Τ.Ε.Ι ΗΠΕΙΡΟΥ
ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ : ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΟΥΔΑΣΤΕΣ : ΠΑΝΑΓΙΩΤΑ ΑΛΜΠΑΝΗ
ΑΛΕΞΑΝΔΡΟΣ ΤΣΙΝΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΑΠΠΑΣ ΑΡΤΑ 2006

Ευχαριστίες-Αφιερώσεις

Ευχαριστούμε τον κύριο Λάππα Κωνσταντίνο για την βοήθεια που μας έδωσε μέσω των οδηγιών και συμβουλών του όσον αφορά τον τρόπο συγκέντρωσης του υλικού, τη συγγραφή και την παρουσίαση της πτυχιακής μας εργασίας.

Θέλω να αφιερώσω την πτυχιακή μου εργασία και το πτυχίο που θα πάρω στη μητέρα μου Ευανθία γιατί με έκανε αυτό που είμαι σήμερα, για την πίστη της σ'εμένα, για την στήριξη που μου παρείχε τα χρόνια που σπούδαζα. Επίσης στους συμφοιτητές και φίλους μου για τις πολλές και αξέχαστες στιγμές!
Αλέξανδρος Τσίνος

Μέσω αυτής της πτυχιακής μου δίνεται η ευκαιρία να ευχαριστήσω τον άνθρωπο που ήταν, είναι και θα είναι πάντα στο πλευρό μου, με βοηθά, με συμβουλεύει και με στηρίζει σε κάθε μου απόφαση. Αφιερώνω το πτυχίο μου στη γιαγιά μου Ευτυχία!
Παναγιώτα Αλμπάνη

Κεφάλαιο 1. Εισαγωγή

Κεφάλαιο 2. Intranets, extranets και vpn

Κεφάλαιο 3. Τα τρωτά σημεία του διαδικτύου

Κεφάλαιο 4. Η αναγκαιότητα της ασφάλειας

Κεφάλαιο 5. Επιθέσεις στην ασφάλεια του δικτύου

Κεφάλαιο 6. Κρυπτογράφηση και Πιστοποίηση

Κεφάλαιο 7. Προτεινόμενη Μεθοδολογία Βελτίωσης της Ασφάλειας

Κεφάλαιο 8. Ιοί, Δούρειοι Ίπποι και Worms

Κεφάλαιο 9. Συστήματα Ανίχνευσης Επιθέσεων Intrusion Detection Systems – IDS

Κεφάλαιο 10. Κανόνες ασφάλειας (Roadmap)

Κεφάλαιο 11. Κοιτώντας στο μέλλον

Κεφάλαιο 1

Εισαγωγή

Ένας τυπικός και ενδεικτικός ορισμός - όχι όμως πλήρης και εκτεταμένος - του όρου «Ασφάλεια Υπολογιστών και Δικτύων» είναι: η αποτροπή επιθέσεων με σκοπό την αποφυγή μη εξουσιοδοτημένης εκμετάλλευσης υπολογιστικών και δικτυακών πόρων και δεδομένων.

Το πρώτο δίκτυο, το ARPANET είχε αρχικά σχεδιαστεί με σκοπό την ευελιξία. Με την πάροδο του χρόνου και όσο προσθέτονταν κόμβοι, άρχισαν τα πρώτα βήματα του hacking. Αρχικά οι ερευνητές που χρησιμοποιούσαν το δίκτυο αντάλλασσαν αστεία και ενοχλητικά μηνύματα. Ήταν σπάνιο εκείνο τον καιρό μία προσπάθεια απομακρυσμένης σύνδεσης σε ένα άλλο κόμβο να θεωρηθεί επίθεση, κύρια λόγω του ότι οι χρήστες του δικτύου, ήταν μία μικρή μάδα ανθρώπων που γνώριζαν προσωπικά ο ένα τον άλλο. Τα πρώτα πραγματικά προβλήματα ασφάλειας εμφανίστηκαν γύρω στο 1980 κύρια λόγω της χρησιμοποίησης των υπολογιστών για διαχείριση απόρρητων δεδομένων και συγκεκριμένα δεδομένων που σχετίζονταν με την περιοχή των στρατιωτικών πληροφοριών. Η αποκορύφωση ήρθε το 1986, που εξαιτίας ενός λογιστικού λάθους που παρατήρησε ο Cliff Stoll, σε ένα τηλεφωνικό λογαριασμό που σύνδεε τους υπολογιστές στο ARPANET, του Lawrence Berkeley National Laboratory στην Βόρεια Καλιφόρνια, ανακάλυψε πως γινόταν μία διεθνής προσπάθεια μέσω του δικτύου να κλαπούν πληροφορίες από στρατιωτικούς κόμβους στην Αμερική.

Η διαμοιραζόμενη χρήση υπολογιστικών και δικτυακών πόρων και πληροφοριών αυξάνεται με εκθετικούς ρυθμούς και στα 1980 είναι αναγκαία η χρήση λειτουργικών συστημάτων που να αποτρέπουν τους χρήστες από ανεπιθύμητη - σκόπιμη ή μη - αλληλεπίδραση καθώς και θωράκιση των δικτύων απέναντι στην ανασφαλή τους φύση. Παράλληλα με τη δυνατότητα απόκρυψης της πληροφορίας (που απαιτείται σε περιπτώσεις μετάδοσης διαβαθμισμένης πληροφορίας), επιβάλλεται και η διατήρηση της ορθότητάς της κατά τη μμεταφορά και την ανάκτησή της (που είναι απαίτηση των επιχειρήσεων και των οργανισμών). ΟΙ υπολογιστές αποτελούν ταυτόχρονα μέσα και στόχους επιθέσεων και η ασφάλεια τους δεν αντιμετωπίζεται ως αυτοσκοπός αλλά σαν το βασικό στοιχείο της διασφάλισης πληροφοριών.

Προκειμένου να διασαφηνιστεί ο όρος ασφάλεια είναι αναγκαίο να οριστούν α) ποιοι πόροι πρέπει να «προστατεύονται» και β) απέναντι σε ποιες «απειλές».

Ως πόροι που πρέπει να προστατεύονται θεωρούνται διεργασίες καθώς και αρχεία ή δεδομένα που αποθηκεύονται ή μμεταφέρονται σε υπολογιστές ή δίκτυα υπολογιστών.

Ως απειλές για την ασφάλεια πληροφοριών θεωρούνται διάφορες μορφές αναπαραγόμενου κώδικα, όπως ιοί (viruses) και σκουλήκια (worms), εκτελέσιμα αρχεία εντολών (shell scripts) που μπορούν να χρησιμοποιήσουν ατέλειες του λογισμικού (bugs) προκειμένου να αλλοιώσουν τα δικαιώματα προσπέλασης διεργασιών, κενά στην διαμόρφωση λογισμικού και των λειτουργικών συστημάτων.

Στα πλαίσια μιας γενικότερης θεώρησης, ασφάλεια θεωρείται η επιτυχής εξουδετέρωση απειλών όπως κλοπή, απάτη, κατασκοπεία, εκβιασμός, τρομοκρατία.

Με βάση το κίνητρο της επίθεσης, που μπορεί να είναι απλή επιθυμία απόκτησης πρόσβασης σε απαγορευμένους πόρους μέχρι την ανορθόδοξη επίτευξη πολιτικών και οικονομικών στόχων, διακρίνονται οι ακόλουθες κατηγορίες εισβολέων:

Hackers: επεμβαίνουν παράνμα σε υπολογιστές επειδή απλά αντιμετωπίζουν τη διαδικασία της προσβολής της ασφάλειας υπολογιστών και δικτύων σαν πρόκληση για τις προγραμματιστικές του ικανότητες.

Κατάσκοποι (Spies): επιδιώκουν την παράνομη απόκτηση πληροφοριών με απώτερο στόχο το πολιτικό όφελος.

Τρομοκράτες (Terrorists): σκοπεύουν να διασπείρουν φόβο σχετικά με πολιτικά ζητήματα χρησιμοποιόντας πληροφορίες που έχουν αποκτήσει με παράνμο τρόπο.

Βιομηχανικοί κατάσκοποι (Corporate Raiders): επιδιώκουν την απόκτηση πρόσβασης σε πληροφορίες και συστήματα ανταγωνιστικών εταιριών και επιχειρήσεων με σκοπό το οικονομικό όφελος εις βάρος τους.

Επαγγελματίες εγκληματίες (Professional Criminals): στοχεύουν στην ικανοποίηση προσωπικών οικονομικών οφελών μέσω παράνομης απόκτησης πληροφοριών ή παραποίησής τους.

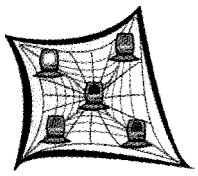
Βάνδαλοι (Vandals): έχουν ως μόνο στόχο την πρόκληση ζημιάς με οποιοδήποτε τρόπο και χωρις κάποιο συγκεκριμένο προσωπικό όφελος.

Ανεξάρτητα από την κατηγοριοποιηση των επιτιθεμένων σε ένα σύσιημα, κύριο πρόβλημα που πρέπει να αντιμετωπιστεί ειναι ο έγκαιρος προσδιορισμός των τρωτών και η βελτίωση της ασφάλειας των συστημάτων πριν από τους επιτιθέμενους.

Κεφάλαιο 2

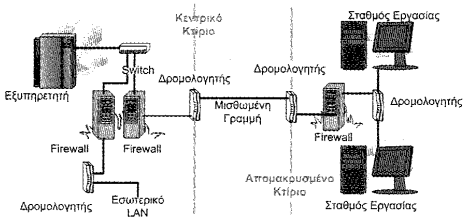
Intranets, extranets και vpn

2.1. Intranets



Το Intranet είναι ένα ιδιωτικό δίκτυο, δομημένο όπως το Internet, που αναπτύσσεται εσωτερικά σε μία εταιρία. Μπορεί να αποτελείται από αρκετά διασυνδεμένα τοπικά δίκτυα χρησιμοποιώντας κύρια την τεχνολογία TCP/IP. Μπορεί να πούμε πως είναι μία ιδιωτική έκδοση του Internet. Τα Intranets παρέχουν βασικά δύο λειτουργίες. Από τη μία παρέχουν ασφαλή πρόσβαση σε πληροφορίες και από την άλλη επιτρέπουν την διαχείριση και επεξεργασία της πληροφορίας κύρια ανάμεσα σε ομάδες του οργανισμού. Το Intranet είναι η ιδανική λύση για οργανισμούς με παραπάνω από 100 εργαζόμενους που βρίσκονται σε διαφορετικά sites. Είναι ο τρόπος για να κοινοποιούνται οι διαρκώς ανανεωμένες πληροφορίες ανάμεσα σε ομάδες εργαζομένων ή σε όλους μαζί. Οι εφαρμογές που αναπτύσσονται έχουν σχέση με την διαχείριση πόρων, την εκπαίδευση, τις πωλήσεις και το μάρκετινγκ, την διακίνηση διοικητικής πληροφορίας, την εταιρική επικοινωνία, την τεκμηρίωση, την έρευνα και τεχνολογία.

Η τεχνολογία που χρησιμοποιείται είναι συνήθως αυτή των ιστοσελίδων (web), γιατί έχει ανοικτή αρχιτεκτονική και υλοποιείται σχετικά εύκολα σε σύντομο χρονικό διάστημα και με μικρό κόστος. Υπάρχουν βέβαια και περιπτώσεις που η συγκέντρωση της πληροφορίας πρέπει να γίνεται αυτόματα και για το λόγο αυτό χρησιμοποιούνται εξειδικευμένες εφαρμογές, που έχουν μεγαλύτερο κόστος σε χρόνο και χρήμα.



Σχήμα 2-7. Σύνδεση sites σε intranet

Η επιτυχία ενός Intranet βασίζεται κύρια στην ικανότητα της άμεσης ενημέρωσης και διακίνησης της πληροφορίας που αφορά κάθε εργαζόμενο. Οι πληροφορίες που διακινούνται μέσα στο Intranet συνήθως είναι για χρήση μόνο από τους εργαζόμενους στον οργανισμό. Ακόμα και μέσα στον ίδιο οργανισμό υπάρχουν πληροφορίες που είναι διαβαθμισμένες. Για παράδειγμα πληροφορίες για τον προϋπολογισμό και τις δαπάνες ενός έργου δεν μπορούν να έχουν παρά συγκεκριμένα άτομα.

Έτσι σε ένα Intranet είναι απαραίτητη η διαβάθμιση του προσωπικού ώστε να μπορεί να έχει μόνο τις απαραίτητες πληροφορίες για να κάνει γρήγορα και σωστά την εργασία του. Η έννοια λοιπόν της ασφάλειας υπάρχει και στα Intranets μόνο που εδώ δεν υπάρχει σαφής ορισμός της περιμέτρου ή για να ακριβολογούμε υπάρχουν διαφορετικές περιμετροι που όμως συχνά έχουν κάποιες επικαλύψεις. Ο τρόπος για να διασφαλίσει κάποιος τις πληροφορίες είναι να εφαρμόσει τεχνικές πιστοποίησης (authentication) και εξουσιοδότησης (authorization, access control), ενώ στις περιπτώσεις κρίσιμης εμπιστευτικής πληροφορίας θα πρέπει να εφαρμόζεται και κρυπτογράφηση των δεδομένων.

2.2. Extranets

Ένα Extranet είναι ένα ιδιωτικό δίκτυο που χρησιμοποιεί τα πρωτόκολλα του Internet και το σύστημα των δημόσιων τηλεπικοινωνιών, για να προσφέρει με ασφάλεια απαραίτητες πληροφορίες έξω από αυτό. Το extranet μπορούμε να το δούμε σαν μέρος του intranet μιας εταιρίας που επεκτείνεται επιλεκτικά σε χρήστες έξω από αυτήν. Είναι κυρίως θέμα ορισμού της περιμέτρου. Για να περιφρουρηθεί η περίμετρος σε ένα extranet χρειάζεται ενίσχυση της ασφάλειας. Αυτά απαιτούν firewalls, ψηφιακή πιστοποίηση (digital certificates), και κρυπτογράφηση μηνυμάτων.

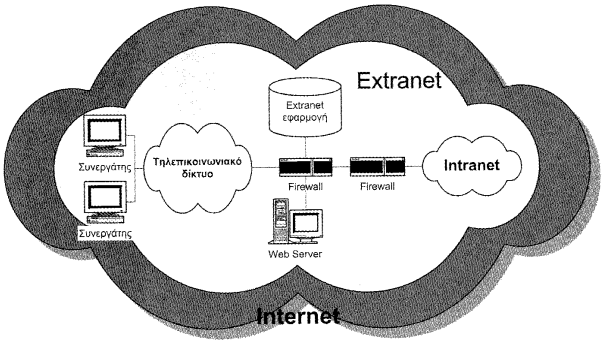
Ένα από τα καλά του κόσμου των δικτύων είναι πως λύσεις σε παλιά προβλήματα, αναπλάθονται με ένα καλύτερο τρόπο. Για παράδειγμα μεταφέροντας μέσα σε ένα οργανισμό το Internet φτιάξαμε τα Intranets. Τώρα διασυνδέουμε με έξυπνο τρόπο τα intranets για να φτιάξουμε extranets. Οι πολλά υποσχόμενες εφαρμογές των extranets φαίνεται πως συνδυάζουν τα καλά των δύο κόσμων. Μπορούμε να έχουμε την ταχύτητα και πληρότητα των εφαρμογών του intranet, να την περάσουμε από το firewall και να έχουμε την έκταση και λειτουργικότητα του internet.

Ο ρόλος ενός extranet είναι να παρέχει μετρήσιμη, ελεγχόμενη και προστατευμένη πληροφορία μεταξύ συνεργαζόμενων εταίρων για την μεγιστοποίηση των ωφελειών που προκύπτουν από την συνεργασία. Στην υλοποίηση του extranet πρέπει να ληφθεί όμως υπόψη πως η συνεργασία είναι μια δυναμική σχέση που αρκετές φορές αλλάζει. Η ροή της πληροφορίας προς τους συνεργάτες δεν μπορεί να εγγυηθεί πως δεν θα υπάρξει διαρροή από κάποιον τελικό παραλήπτη της πληροφορίας. Επίσης δεν είναι δυνατόν να πάρεις πίσω μια πληροφορία που έχει γνωστοποιηθεί. Άρα χρειάζεται σωστός σχεδιασμός τόσο στις πληροφορίες που διαμοιράζονται (τακτικής και όχι στρατηγικής μορφής), όσο και στην

ασφάλεια του extranet, ώστε να μην είναι δυνατή η διείσδυση του συνεργάτη στο Intranet της εταιρείας μας.

Η δημιουργία ενός αποδοτικού και ασφαλούς extranet δεν είναι μία τυπική και εύκολη διαδικασία. Απαιτείται λεπτομερής σχεδιασμός, συνδυασμός και προσαρμογή εμπορικών προϊόντων και ειδικών λύσεων για κάθε περίπτωση. Επιπλέον πρέπει να ενεργοποιηθούν τα απαραίτητα συστήματα ασφάλειας όπως tunneling, απόκρυψη στοιχείων (encryption), ψηφιακά πιστοποιητικά (digital certificates) κλπ.

Συνοψίζοντας, το extranet είναι για τις εταιρίες ένας τρόπος να παρέχουν εταιρικές πληροφορίες στους συνεργάτες και πελάτες τους συνήθως χρησιμοποιώντας IP δίκτυα, συχνά μέσω του διαδικτύου. Είναι επίσης μία ευκαιρία να μειώσουν τα κόστη, να αυξήσουν την αποδοτικότητά τους και να ενισχύσουν της εταιρικές σχέσεις. Είναι όμως και ο εφιάλτης του υπεύθυνου ασφάλειας του οργανισμού. Στο Σχήμα 2.8 φαίνεται πως μέσα στο internet δημιουργούνται intranets και extranets και πως ο ορισμός της περιμέτρου είναι ένα δύσκολο εγχείρημα με πολλά μοντέλα υλοποίησης.



Σχήμα 2-8. Από το internet στο intranet και το extranet

2.3. Από τα Intranets στα Extranets

Ένα extranet έχει πολλά κοινά χαρακτηριστικά με ένα intranet. Αν και αρχικά τα intranets φτιάχτηκαν σαν ασφαλή δίκτυα πίσω από firewalls για να εξυπηρετούν τις εσωτερικές ανάγκες των εταιριών, γρήγορα φάνηκε πως έπρεπε να ανοιχτούν και σε εξωτερικούς χρήστες όπως συνεργάτες, πελάτες, προμηθευτές κλπ. Οι ειδικοί λένε σήμερα πως ένα firewall ανάμεσα στο internet και το intranet είναι «μία ημιπερατή μεμβράνη, που θα γίνεται περισσότερο πορώδης με την πάροδο του χρόνου». Η νέα επανάσταση των extranets έρχεται να επιβεβαιώσει τον ορισμό αυτό.

Από τότε που άρχισαν να κατασκευάζονται εφαρμογές για επικοινωνιακούς λόγους, άρχισε να διαφαίνεται η ανάγκη και για εξωτερική επικοινωνία. Η επικοινωνία είναι σημαντική και απαραίτητη ανάμεσα σε μέλη διαφορετικών οργανισμών που συνεργάζονται. Είναι φανερό πως οι επιτυχημένες εταιρίες που παραμένουν κλειστές στον εαυτό τους μειώνονται συνεχώς. Είναι απαραίτητη η διαρκής επικοινωνία τόσο με τους προμηθευτές όσο και με τους πελάτες τους, προσφέροντας μέρος της εσωτερικής πληροφόρησης σε αυτούς.

Είναι λογικό κάποιος να αναρωτιέται: «αφού το web προσφέρει ένα καλό τρόπο για την διακίνηση της εταιρικής πληροφορίας, γιατί δεν το επεκτείνουμε και παραέξω;». Πράγματι, δημοσιοποιώντας εταιρικές πληροφορίες είναι ένας απλός τρόπος να δημιουργήσει κάποιος ένα extranet. Τέτοιο παράδειγμα είναι να προσφέρονται μέσω εξυπηρετητή ιστοσελίδων (web server) εταιρικές πληροφορίες που έχουν αποθηκευθεί σε βάση δεδομένων. Υπάρχουν πολλά δεδομένα και υπηρεσίες που μία εταιρία και οι συνεργάτες της θα ήθελαν να μοιραστούν. Όπως για παράδειγμα πληροφορίες για τις

προδιαγραφές προϊόντων, τιμοκατάλογοι, τρόποι παράδοσης προϊόντων, τεχνική υποστήριξη, ανανέωση λογισμικού, δημοσίευση και ανταλλαγή πληροφοριών μέσω web φορμών, μηχανών αναζήτησης και ερωτήσεων σε βάσεις δεδομένων, υπηρεσίες τηλεσυνεργασίας. Η ανάγκη αυτή έχει γίνει αντιληπτή κύρια σε εφαρμογές του Ηλεκτρονικού Εμπορίου με δυνατότητες να γίνονται οι παραγγελίες, οι παραδόσεις και οι πληρωμές προϊόντων με ηλεκτρονικό τρόπο.

Υπάρχουν πολλοί τρόποι να φανεί χρήσιμο και αποδοτικό ένα extranet και όλο και περισσότερες εταιρίες το χρησιμοποιούν. Αυτό δημιουργεί βέβαια μία σειρά προβλημάτων ασφάλειας που είναι κοινά για intranet και extranet και εξετάζονται μαζί. Έτσι έχουμε να αντιμετωπίσουμε ένα παράδοξο: με τα extranets επιτρέπουμε σε χρήστες έξω από τον οργανισμό μας να έχουν προσπέλαση σε εταιρικά δεδομένα και υπηρεσίες μέσω του διαδικτύου. Αυτό όμως έρχεται σε αντίθεση με την προσπάθεια να αποφύγουμε τις προσπέλαση έξω από το δίκτυό μας, κατασκευάζοντας ασφαλή δίκτυα με χρήση firewalls.

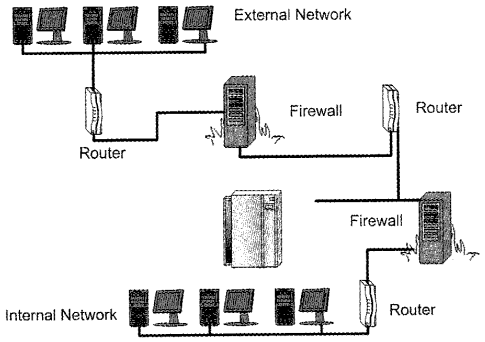
Σε περιπτώσεις δημιουργίας extranets πρέπει να εξετασθούν προσεχτικά οι ακόλουθες περιπτώσεις :

1. Η τεχνολογία που θα χρησιμοποιεί ο ένας συνεργάτης συνεργάζονται με το firewall και τα συστήματα ασφάλειας του άλλου;
2. Υπάρχει κοινή αντιμετώπιση στις επενδύσεις που πρέπει να γίνουν για την ενίσχυση της ασφάλειας και την εκπαίδευση του προσωπικού των δύο οργανισμών;
3. Τι γίνεται σε περιπτώσεις που ο ένας συνεργάτης προσπαθεί να διασπάσει το εσωτερικό δίκτυο του άλλου;
4. Πως αντιμετωπίζουμε την κατάσταση που προκύπτει όταν ένας hacker διασπά την ασφάλεια του ενός συνεργάτη και μέσω αυτού επιτίθεται στα συστήματα του άλλου;

Απάντηση σε αυτά τα προβλήματα έχουμε μόνο με την διαμόρφωση στρατηγικού σχεδιασμού των συστημάτων μας:

1. Πρέπει να ορίσουμε την πολιτική διάθεσης των πόρων του οργανισμού. Ποιες πληροφορίες ή υπηρεσίες είναι διαθέσιμες για κοινή χρήση.
2. Πρέπει να περιορίσουμε ης δυνατότητες του συστήματος στις αναγκαίες. Δεν θέλουμε να φτιάξουμε ένα IPsec VPN όταν χρειαζόμαστε όλο κι όλο ένα ασφαλή web server ή δεν επιτρέπουμε τα interactive logins όταν χρειάζεται μόνο η μεταφορά αρχείων.
3. Πρέπει να μπορούμε να κρυπτογραφήσουμε τα δεδομένα μας. Ακόμα και πάνω από ένα ασφαλές δίκτυο δεν μπορούμε να είμαστε σίγουροι πως τα δεδομένα μας δεν θα καταλήξουν σε κοινή θέα.
4. Πρέπει να μπορούμε να γνωρίζουμε ποιος είναι ο χρήστης που προσπελαύνει το δίκτυό μας άρα τα δεδομένα και ης υπηρεσίες μας. Πρέπει να γίνει χρήση κάποιας μεθόδου πιστοποίησης κατάλληλης για το είδος της ασφάλειας που θέλουμε να πετύχουμε. Μπορεί να είναι ο βασικός συνδυασμός username/password, ψηφιακά πιστοποιητικά και υπογραφές.
5. Πρέπει να απομονώνουμε τα προσφερόμενα προς τους εξωτερικούς χρήστες δεδομένα και υπηρεσίες από το εσωτερικό μας δίκτυο. Δεν θέλουμε οι εξυπηρετητές που τα προσφέρουν να βρίσκονται εσωτερικά στο ιδιωτικό μας δίκτυο, αλλά σε συγκεκριμένη προστατευμένη περιοχή του δικτύου μας.

6. Πρέπει να έχουμε μηχανισμό παρακολούθησης του extranet και του intranet. Είναι σωστό να παρακολουθούνται οι προσπάθειες διείσδυσης στο δίκτυό μας, τα μοτίβα κυκλοφορίας πακέτων, οι προσπάθειες πιστοποίησης σε καταγραφές των logs.



Σχήμα 2-10. Δομικά στοιχεία extranet

Έτοιμες λύσεις για την σωστή δημιουργία extranets δεν υπάρχουν, υπάρχουν όμως τα κατάλληλα συστατικά για να φτιάξουμε την λύση που μας ταιριάζει. Η δημιουργία ενός αποδοτικού και ασφαλούς intranet ή extranet είναι μία δύσκολη διαδικασία που απαιτεί λεπτομερή σχεδιασμό, συνδυασμό εμπορικών προϊόντων και προσαρμοσμένων λύσεων, εφαρμογή τεχνικών όπως tunneling, κρυπτογράφηση, ψηφιακά πιστοποιητικά, Ιδεατά Δίκτυα και συσκευών όπως firewalls, ασφαλείς εξυπηρετητές, proxy applications, κ.ά. Η πολυπλοκότητα αλλά και οι εξεζητημένες γνώσεις που απαιτούνται για τον σχεδιασμό και την υλοποίηση οδηγεί συνήθως σε ανάθεση της εργασίας σε εξειδικευμένο προσωπικό. Στοιχεία που πρέπει να προσεχτούν αφορούν;

1. Παροχή ασφάλειας από άκρο σ' άκρο
2. Πιστοποίηση των χρηστών
3. Λεπτομερή έλεγχο προσπέλασης
4. Διαλειτουργικότητα εφαρμογών και συσκευών
5. Επεκτασιμότητα
6. Ευχρηστία
7. Προσαρμοστικότητα

2.4. Ιδεατά Ιδιωτικά Δίκτυα (VPNs)

Ένα Ιδεατό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN) είναι ένα περιβάλλον επικοινωνίας στο οποίο η πρόσβαση ελέγχεται με τέτοιο τρόπο, ώστε να επιτρέπει συνδέσεις μεταξύ μελών μιας ορισμένης περιοχής ενδιαφέροντος. Το περιβάλλον αυτό κατασκευάζεται μέσα από ένα υπάρχον κοινό μέσο επικοινωνίας, που προσφέρει υπηρεσίες σε μη αποκλειστική βάση. Ένας πιο απλός και πιο κατανοητός ορισμός είναι ο παρακάτω:

«'Ενα VPN είναι ένα ιδιωτικό δίκτυο που κατασκευάζεται χρησιμοποιώντας την υπάρχουσα υποδομή ενός δημοσίου δικτύου, όπως είναι το Internet»,

Στην πραγματικότητα η κατασκευή του είναι ιδεατή καθώς το κομμάτι της υποδομής που χρησιμοποιείται δεν είναι ένα σταθερό σύνολο συσκευών. Κάθε φορά τα δεδομένα που αποστέλλονται μπορεί να ακολουθούν διαφορετική διαδρομή μέχρι να φτάσουν στον προορισμό τους. Αυτή είναι και η βασική διαφορά με ένα πραγματικό ιδιωτικό δίκτυο ενώ

παρουσιάζει τα ίδια χαρακτηριστικά, όπως ασφάλεια, αξιοπιστία, ποιότητα υπηρεσιών (Quality of Service), διαχειρισιμότητα και ανάθεση προτεραιοτήτων στους χρήστες.

Εκτός από την έννοια του ιδεατού υπάρχει και η έννοια της κρυπτογράφησης που χαρακτηρίζει τη φιλοσοφία λειτουργίας ενός VPN. Η κρυπτογράφηση αφορά τη μετατροπή του εκάστοτε μηνύματος σε μια μορφή που είναι δύσκολο ή αδύνατο να κατανοηθεί από κάποιον τρίτο εκτός από το δέκτη. Η διαδικασία της κρυπτογράφησης εκτελείται στον αποστολέα του μηνύματος, ενώ ο δέκτης είναι επιφορτισμένος με την επαναφορά του μηνύματος στην αρχική του μορφή. Πρέπει, επομένως, ο δέκτης να έχει διαθέσιμες όλες τις απαραίτητες πληροφορίες για να διεκπεραιώσει την αντίστροφη διαδικασία.

Ιστορικά ένας πρόγονος των VPN είναι το Public Data Network (PDN). Το περιβάλλον του PDN βασίζεται πάνω σε ένα κοινό τρόπο διευθυνσιοδότησης και σε μια κοινή ιεραρχία δρομολόγησης που επιτρέπει στα switching elements (δρομολογητες) να καθορίσουν τη θέση των διασυνδεδεμένων οντοτήτων. Όλες οι οντότητες του δικτύου έχουν πρόσβαση σε κοινή υποδομή που αποτελείται από στοιχεία δρομολόγησης και κυκλώματα. Τ ο πρόβλημα του παραπάνω δικτύου PDN είναι ότι η ευρεία πρόσβαση που προσφέρει δημιουργεί περιορισμούς στο ποιες ανάγκες των χρηστών μπορούν να καλυφθούν. Η κυριότερη ανάγκη που δεν μπορεί να καλυφθεί είναι αυτή της κρυπτογράφησης των δεδομένων. Συγκεκριμένα το Internet δεν είναι η καλύτερη λύση για οργανισμούς που θέλουν να χρησιμοποιήσουν ένα δίκτυο για ένα κλειστό σύνολο χρηστών και για εφαρμογές ιδιωτικού χαρακτήρα, όπως η διασύνδεση γεωγραφικά απομακρυσμένων γραφείων μιας εταιρείας. Επίσης μια εφαρμογή κάποιου χρήστη μπορεί να έχει διαφορετικές απαιτήσεις διαχείρισης του δικτύου ή απόδοσης από αυτές που προσφέρονται από το PDN. Η εκπλήρωση αυτών των αναγκών οδήγησε στη χρήση ιδιωτικών δικτύων υλοποιημένων με μισθωμένες γραμμές, αλλά αυτή η λύση επιβαρύνει με το κόστος της μίσθωσης γραμμών και της διαχείρισης του δικτύου από ειδικευμένο προσωπικό. Η αύξηση των απομακρυσμένων χρηστών δημιούργησε απαιτήσεις για επέκταση της υπάρχουσας υποδομής και καθώς οι τοποθεσίες τους ήταν γεωγραφικά διεσπαρμένες προκάλεσε δυσανάλογη αύξηση του κόστους χρήσης του δικτύου. Σε τέτοιες περιπτώσεις η διαχείριση του δικτύου γίνεται πολύ δύσκολη.

Η χρήση της υπάρχουσας υποδομής άρχισε να διαφαίνεται σαν η μοναδική λύση μείωσης του κόστους και των προβλημάτων επέκτασης. Η χρήση της έφερε στην επιφάνεια τα ευγενή προβλήματα αξιοπιστίας, και έλλειψης κρυπτογράφησης δεδομένων με αποτέλεσμα να απαιτείται η ανάπτυξη νέων τεχνολογιών. Η νέα τεχνολογία που αντιπροσωπεύεται από τα VPN προσπαθεί να εφαρμόσει τεχνικές κρυπτογραφίας, κατηγοριοποίησης των πληροφοριών και κατανομής υπηρεσιών σε κατηγορίες χρηστών με τέτοιο τρόπο ώστε να αντιμετωπίζει ως ένα βαθμό τα προβλήματα του υποστρώματος το οποίο τελικά αναλαμβάνει την μεταφορά της πληροφορίας. Βέβαια τα VPN δεν αποτελούν πανάκεια καθώς υπάρχουν εφαρμογές με απαιτήσεις που δεν μπορούν να καλυφθούν. Μοναδική λύση τότε αποτελούν τα ιδιωτικά δίκτυα.

2.5. Απαιτήσεις από ένα Ιδεατό Ιδιωτικό Δίκτυο (VPN)

Ασφάλεια	Διαλειτουργικότητα	Ευκολία στη χρήση
Υποστήριξη ,ισχυρής πιστοποίησης , token cards ,smart cards , biometrics, δακτυλικά αποτυπώματα ,X.509, Kerberos	Υποστήριξη βασικών ανοικτών στάνταρ	Εύχρηστο client στους σταθμούς εργασίας. Διαφανή λειτουργία στον χρήστη
Υποστήριξη ισχυρής κρυπτογράφησης με κλειδιά μεγέθους 40,56 και 128 και Μέθοδο Κρυπτογράφησης RC4, DES , Triple DES	Δυνατότητα συνεργασίας Και ολοκλήρωσης Με τη περιμετρική Ασφάλεια του δικτύου Και συσκευές όπως firewall, router	Πιστοποίηση την πρώτη φορά Εισόδου στο δίκτυο και όχι Κάθε φορά που ξεκινά μια εφαρμογή
Υποστήριξη φιλτραρίσματος των datastreams ,συμπεριλαμβανομένων ιών ,τύπων αρχείων Java και ActiveX , πρωτοκόλλων όπως FTP, Telnet κλπ	Συμβατότητα με τα Πρωτόκολλα ipv4, IPSec ,PPTP/L2TP	Επεκτάσιμο σε εκατοντάδες Και χιλιάδες χρήστες
Υποστήριξη σεναρίων προσπέλασης ανάλογα με παραμέτρους όπως ,μέθοδος πιστοποίησης ,κρυπτογράφησης ,ώρα , διεύθυνση προορισμού ,διεύθυνση προέλευσης ,τύπο εφαρμογής	Υποστήριξη των βασικών στάνταρ για πιστοποίηση και κρυπτογράφηση	Υποστήριξη κεντρικής Διαχείρισης της ασφάλειας
Υποστήριξη παρακολούθησης , καταγραφής και ελέγχου της δικτυακής κυκλοφορίας	Υποστήριξη όλων των ειδών των εφαρμογών	Το σύστημα του VPN να τρέχει σε συνήθη λειτουργικά συστήματα όπως Windows NT και UNIX
Υποστήριξη μηχανισμού ειδοποίησης Του διαχειριστή για Συγκεκριμένα περιστατικά	Δυνατότητα λειτουργίας σε Ετερογενές περιβάλλον Με λειτουργικά συστήματα Windows ,UNIX	
	Δυνατότητα συνεργασίας Με βάσεις δεδομένων σε NT , Netware ,RADIUS, ACE	

Τα VPN αποτελούνται από υλικό και λογισμικό το οποίο καλείται να ικανοποιήσει ένα σύνολο απαιτήσεων που θα κάνουν το VPN εύκολο στη χρήση και στη συντήρηση, ασφαλές και διαθέσιμο στους χρήστες. Μέσα από μια μελέτη των αναγκών του

οργανισμού θα προκύψει το σύνολο των χαρακτηριστικών για το VPN που θα πρέπει να εγκαταστήσει. Ο οργανισμός μπορεί είτε να υλοποιήσει το VPN με δικά του μέσα είτε να αναθέσει την εργασία σε έναν πάροχο VPN υπηρεσιών, που μπορεί να είναι ένας πάροχος Internet υπηρεσιών (ISP).

Τα VPN μπορούν να υλοποιούν και άλλα πρωτόκολλα όπως MPLS, για forwarding packets στο δίκτυο και βελτίωση των προσφερόμενων υπηρεσιών τόσο από την πλευρά της ασφάλειας, όσο και από την εγγυημένη ποιότητα των υπηρεσιών, ή το BGP για την μεταφορά των λιστών με εναλλακτικές δρομολογήσεις πάνω στο Ιδεατό Ιδιωτικό Δίκτυο.

Η επιλογή ενός συστήματος VPN πρέπει να έχει τα παρακάτω χαρακτηριστικά:

Τα τρία βασικά χαρακτηριστικά που προσδιορίζουν ένα VPN είναι η κρυπτογράφηση, η πιστοποίηση και ο έλεγχος προσπέλασης. Αν και η κρυπτογράφηση και πιστοποίηση είναι σημαντικά στοιχεία του VPN, είναι σχετικά εύκολο να υλοποιηθούν. Ο έλεγχος της προσπέλασης είναι όμως μάλλον δύσκολος, επειδή ή υλοποίησή του εξαρτάται και από άλλα εργαλεία ασφάλειας. Τελικά το πόσο ασφαλές είναι ένα VPN εξαρτάται από το πόσο συνεργάζονται τα τρία αυτά βασικά χαρακτηριστικά. Αν ένα πάσχει σε υλοποίηση πάσχει όλη η υλοποίηση του VPN.

Όπου στον πραγματικό κόσμο χρησιμοποιούνται οι φυλασσόμενες πόρτες στα VPNs χρησιμοποιούνται τα firewalls. Ο έλεγχος της προσπέλασης μπορεί να είναι διαβαθμισμένος και από τη στιγμή που ένας χρήστης θα πιστοποιηθεί με χρήση token card, digital certificate ή ακόμα και χρήση δακτυλικών αποτυπωμάτων μπορεί να έχει προσπέλαση στους πόρους που του έχουν αντιστοιχιστεί σύμφωνα με το προφίλ του.

Οι λύσεις που υπάρχουν για την υλοποίηση των VPNs περιλαμβάνουν κάποιες από τις συσκευές όπως firewalls, routers, proxy servers, VPN λογισμικό και υλικό ή και όλα αυτά. Ένας συνδυασμός από τον εξοπλισμό αυτό δίνει καλύτερα αποτελέσματα. Κατά την υλοποίηση του VPN πρέπει να ληφθεί μέριμνα για την εξασφάλιση των παρακάτω απαραίτητων προδιαγραφών λειτουργίας:

Διαθεσιμότητα (Availability)

Ένα VPN πρέπει να προσφέρει πρόσβαση καθ' όλη τη διάρκεια του 24ώρου. Αυτό σημαίνει ότι θα πρέπει να ικανοποιεί κάθε αίτηση για σύνδεση, οποτεδήποτε αυτή εμφανιστεί. Η διαθεσιμότητα δεν εξαρτάται μόνο από την ικανότητα του παρόχου να κρατά το δίκτυό του σε συνεχή λειτουργία, καθώς κάποια προβλήματα οφείλονται σε παράγοντες εκτός ελέγχου του. Η περίπτωση χρήσης του Internet ως υποδομή είναι ένα τέτοιο παράδειγμα.

Έλεγχος (Control)

Ένα VPN μπορεί είτε να βρίσκεται κάτω από τον έλεγχο του παρόχου, είτε κάτω από τον έλεγχο του τομέα υποστήριξης δικτύου της εταιρείας. Συνήθως υπάρχει η αντίληψη από τα διοικητικά στελέχη ότι η διαχείριση του VPN από προσωπικό εκτός εταιρείας δημιουργεί περισσότερους κινδύνους επιθέσεων. Στην πραγματικότητα η επιλογή της διαχείρισης από τρίτους και συγκεκριμένα από τον φορέα υλοποίησης του VPN έχει πολλά πλεονεκτήματα. Η μεγάλη εμπειρία και εξειδίκευση των τεχνικών εξασφαλίζει γρήγορη υλοποίηση και καλή λειτουργία του VPN. Οι εφαρμογές επόπτευσης της κυκλοφορίας και συναγερμού μπορούν να εξασφαλίσουν ένα καλό επίπεδο ασφάλειας. Η δεύτερη περίπτωση έχει το πλεονέκτημα του πλήρους ελέγχου του VPN αλλά θα πρέπει να ληφθούν σοβαρά υπόψη ο χρόνος εκπαίδευσης του προσωπικού, το κόστος απόκτησης του εξοπλισμού και ο χρόνος μέχρι να κριθεί επιχειρησιακό το δίκτυο.

Συμβατότητα (Compatibility)

Το VPN πρέπει να είναι συμβατό με το ήδη υπάρχον δίκτυο του χρήστη. Όταν υπάρχει χρήση διαφορετικών πρωτοκόλλων θα πρέπει να γίνουν οι απαραίτητες ενέργειες ώστε να διασυνδεθούν τα δύο δίκτυα. Για παράδειγμα μπορεί το VPN να στηρίζεται στο IP, ενώ το δίκτυο του χρήστη στο IPX. Η χρήση ενός gateway λύνει το πρόβλημα συμβατότητας προσθέτοντας ένα ακόμη επίπεδο στο σχεδιασμό και την υλοποίηση. Επίσης το δίκτυο πρέπει να φτάνει μέχρι το επίπεδο δικτύου (network layer) του προτύπου OSI του οργανισμού ISO.

Ασφάλεια (Security)

Ένα VPN δεν αποτελεί ιδιωτικό δίκτυο του χρήστη όπως ήδη έχει αναφερθεί. Η χρήση της κοινής υποδομής για τη μεταφορά πληροφοριών καθιστά δυνατή την υποκλοπή τους από τρίτους. Η ασφάλεια αναφέρεται σε όλες τις ενέργειες που εκτελούνται από τα στοιχεία του VPN, όπως για παράδειγμα είναι η διαδικασία κρυπτογράφησης των δεδομένων ή η διαδικασία πιστοποίησης των χρηστών του δικτύου. Βέβαια οι απαιτήσεις για ασφάλεια μπορεί να μην ικανοποιούνται αν η πλατφόρμα που θα εγκατασταθεί το λογισμικό του VPN παρουσιάζει αδυναμίες. Αν ένα VPN υλοποιηθεί πάνω σε κάποιο λειτουργικό σύστημα τότε πρέπει να αντιμετωπιστούν τα πιθανά του προβλήματα ασφαλείας, διαφορετικά η χρήση του VPN θα είναι ανώφελη. Είναι φανερό ότι οι απαιτήσεις ασφάλειας δεν αφορούν μόνο την πολιτική του VPN στο θέμα αυτό αλλά και τα μέσα του χρήστη τα οποία θα υποστηρίξουν το δίκτυο.

Διαλειτουργικότητα (Interoperability)

Καθώς τα VPN είναι μια νέα τεχνολογία από πλευράς υλοποίησης προκύπτουν πολλά θέματα συμβατότητας από τη χρήση διαφόρων προτύπων κρυπτογράφησης και ασφαλείας. Υπάρχουν πολλά προϊόντα στην αγορά με αποτέλεσμα να είναι δύσκολη η επιλογή κάποιου από αυτά. Η έλλειψη πιστοποίησης σε κάποια από αυτά δεν εξασφαλίζει το ότι καλύπτουν τα πρότυπα ασφαλείας. Υπάρχουν βέβαια οργανισμοί πιστοποίησης που αναλαμβάνουν τον έλεγχο των προϊόντων και εκδίδουν πιστοποιητικά που δείχνουν τη συμφωνία του προϊόντος με τα διάφορα πρότυπα.

Αξιοπιστία (Reliability)

Ένα VPN πρέπει να προσφέρει εγγυήσεις για αξιόπιστη λειτουργία, ειδικά όταν υλοποιείται από κάποιον ISP, καθώς τότε η λειτουργία του εξαρτάται σε ένα σημαντικό βαθμό από αυτόν. Αν το δίκτυο σταματήσει να λειτουργεί τότε ο χρήστης το μόνο που μπορεί να κάνει είναι να περιμένει από τον ISP να λύσει το πρόβλημα. Ο χρόνος εξυπηρέτησης εξαρτάται από τον αριθμό των χρηστών που υποστηρίζει ο ISP και από το πόσο εύκολα μπορεί να διαθέσει πόρους για τη λύση του προβλήματος.

Πιστοποίηση δεδομένων και χρηστών (Data and User authentication)

Είναι πολύ σημαντικό σε κάθε υλοποίηση VPN να προσφέρονται και οι δύο υπηρεσίες, επειδή αποτελούν σημαντικές πτυχές της ασφάλειας που θα προσφέρεται. Η πιστοποίηση δεδομένων αφορά την επιβεβαίωση ότι τα δεδομένα έχουν ληφθεί στο σύνολό τους και ότι δεν έχουν μεταβληθεί κατά τη μεταφορά τους. Πιστοποίηση χρήστη είναι η διαδικασία χορήγησης άδειας πρόσβασης στο δίκτυο. Αν ο χρήστης βρίσκεται εκτός του εταιρικού δικτύου τότε πρέπει να γίνεται ασφαλής και αξιόπιστη εξακρίβωση της ταυτότητάς του πριν του παραχωρηθεί το δικαίωμα της πρόσβασης. Επίσης πρέπει να εξακριβωθούν και τα δικαιώματα που έχει από τη στιγμή που θα συνδεθεί στο δίκτυο, ώστε να περιορίζεται μόνο στις υπηρεσίες που του έχουν αποδοθεί.

Επιβάρυνση φορτίου (Traffic Overhead)

Σε κάθε τεχνολογία υπάρχει εξισορρόπηση των παραγόντων λειτουργίας της και τα VPN δε θα μπορούσαν να μην ακολουθούν τον κανόνα. Συγκεκριμένα τα αλληλοσυγκρουόμενα χαρακτηριστικά είναι η ευελιξία και ευχρηστία απέναντι στην ασφάλεια, η ταχύτητα απέναντι στην απόδοση της επικοινωνίας. Η επιβάρυνση αφορά είτε το κόστος που υπεισέρχεται από την κρυπτογράφηση των δεδομένων που μεταφράζεται στο πόση υπολογιστική ισχύς καταναλώνεται, είτε στο ποσό του παραπάνω εύρους ζώνης που απαιτείται για τη μετάδοση των μεγαλύτερου μεγέθους πακέτων που προκύπτουν μέσω encapsulation. Θα πρέπει λοιπόν το VPN να μπορεί να είναι ευέλικτο στη διαμόρφωσή του ώστε να καλύπτει τις διάφορες ανάγκες που θα προκύψουν κατά τη διάρκεια χρήσης του. Για παράδειγμα θα μπορούσε να γίνεται κατηγοριοποίηση των δεδομένων ανάλογα με την αξία τους και έτσι άλλα να κρυπτογραφούνται, άλλα απλώς να πιστοποιούνται και άλλα να αποστέλλονται χωρίς να υποστούν καμία επεξεργασία.

Αντιμετώπιση άρνησης πράξεων (non repudiation)

Ένα VPN πρέπει να έχει τη δυνατότητα θετικής αναγνώρισης ενός χρήστη χωρίς αυτός να μπορεί να αρνηθεί την αναγνώριση που έγινε. Η απαίτηση αυτή έχει μεγάλη σημασία για τις εφαρμογές του ηλεκτρονικού εμπορίου γιατί αν υπάρχει έστω και μια μικρή αμφιβολία για το ποιος έχει κάνει μια παραγγελία τότε αυτή δεν μπορεί να εκτελεστεί για ευνόητους λόγους. Η εξασφάλιση αυτής της ιδιότητας μπορεί να γίνει με χρήση ψηφιακών υπογραφών (digital signatures).

2.6.Τοπολογίες VPN

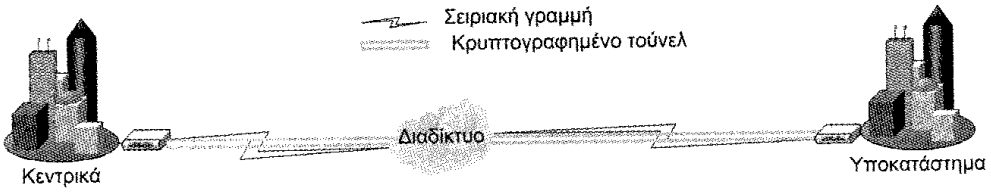
Η χρήση των VPNs έρχεται να δώσει λύσεις σε τέσσερα διαφορετικά σενάρια διασύνδεσης, ορίζοντας αντίστοιχες τοπολογίες:

- Ανάμεσα στον οργανισμό και τα υποκαταστήματά του, δημιουργώντας ένα ***εσωτερικό VPN (Intranet VPN)***
- Ανάμεσα στον οργανισμό και τους απομακρυσμένους εργαζόμενους, δημιουργώντας ένα ***απομακρυσμένης προσπέλασης VPN (remote access VPN)***
- Ανάμεσα στον οργανισμό και τους συνεργαζόμενους πελάτες, προμηθευτές, οργανισμούς, δημιουργώντας ένα ***εξωτερικό VPN (extranet VPN)***
- Ανάμεσα σε τμήματα του ίδιου οργανισμού, δημιουργώντας ένα ***ενδοεπιχειρησιακό VPN (Intranetwork VPN)***

Παρακάτω περιγράφονται οι διαφορετικές τοπολογίες για την υλοποίηση των VPN ανάλογα με την χρήση τους

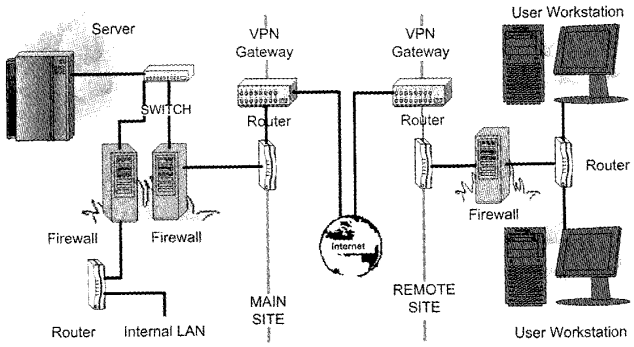
2.7. Intranet VPN

Υπενθυμιζουμε ότι ένα intranet είναι ένα δίκτυο εργασίας το οποίο είναι εσωτερικό σε κάποια εταιρεία επεκτεινόμενο στα διαφορετικά υποκαταστήματά της. Παρέχει τις πιο πρόσφατες πληροφορίες και υπηρεσίες σε όλους τους υπαλλήλους της εταιρείας που συνδέονται σε αυτό ανεξάρτητα από το που βρίσκονται. Τα intranet VPN προσφέρουν ένα κοινό, ανεξάρτητο πλατφόρμας interface, το οποίο είναι λιγότερο ακριβό στην υλοποίηση από μία client/server εφαρμογή. Τα Intranet VPN επιτρέπουν την ίδια ασφάλεια και διασυνδεσιμότητα μεταξύ των κεντρικών γραφείων μιας εταιρείας και απομακρυσμένων γραφείων.



Σχήμα 2-11. Δομικά στοιχεία extranet

Ο τρόπος που έχουν δομηθεί τα δύο δίκτυα ώστε να παρέχουν ασφάλεια στην διασύνδεση φαίνεται στοπαρακάτω Σχήμα 2-12.



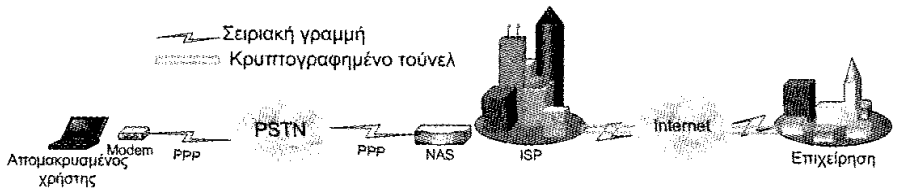
Σχήμα 2-12. Δομικά στοιχεία ενός Intranet VPN

Ιδεατό Ιδιωτικό Δίκτυο απομακρυσμένης προσπέλασης

Ένα VPN αυτής της κατηγορίας εξυπηρετεί απομακρυσμένους κινούμενους (remote mobile) χρήστες. Συγκεκριμένα παρέχει τη δυνατότητα σύνδεσης αυτού του τύπου χρηστών με τα κεντρικά γραφεία της εταιρείας μέσω ενός τούνελ (tunnel) κρυπτογράφησης δεδομένων. Η δημιουργία του τελευταίου μπορεί να γίνει με ειδικό λογισμικό εγκατεστημένο στον εξοπλισμό του χρήστη. Στην άλλη άκρη του τούνελ υπάρχει μια οντότητα που αποτελεί είσοδο στο ιδιωτικό δίκτυο της εταιρείας που μπορεί να είναι και αυτό ένα VPN. Η όλη διαδικασία της δημιουργίας του tunnel πρέπει να είναι εύχρηστη και ο χρήστης θα πρέπει διάφανα να προσπελαύνει τους πόρους του επιχειρησιακού δικτύου σαν να βρισκόταν στο εσωτερικό δίκτυο. Το σημαντικό στοιχείο σε αυτά τα δίκτυα είναι η δυνατότητα της κρυπτογράφησης των δεδομένων που διακινούνται πάνω στο δίκτυο, της πιστοποίησης και της διαχείρισης των δικαιωμάτων των διαφόρων χρηστών. Στο σχεδιασμό της ασφάλειας για τα extranet VPNs ισχύει ότι ο απομακρυσμένος χρήστης θα πρέπει να έχει αυστηρά ελεγχόμενη προσπέλαση, σε αυτούς μόνο τους πόρους που του χρειάζονται για να κάνει από μακριά την εργασία του. Από την στιγμή που ο χρήστης θα κάνει Login στο επιχειρησιακό δίκτυο, θα έχει προσπέλαση στους πόρους που του ορίζει το προκαθορισμένο προφίλ που του έχει οριστεί. Μεγάλη προσοχή χρειάζεται σε super users γιατί έτσι δημιουργούνται κερκόπορτες (back-doors) στο σύστημα της ασφάλειας.

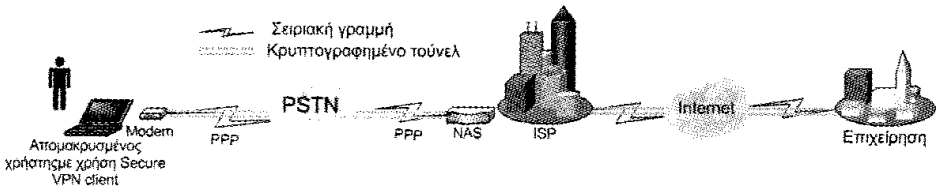
Τα απομακρυσμένης προσπέλασης (remote access) VPNs χωρίζονται σε δύο κατηγορίες: στα δημιουργούμενα από τον πελάτη (client-initiated) και στα δημιουργούμενα από τον εξυπηρετητή δικτυακής πρόσβασης (network access server NAS-initiated).

Ενεργοποίηση από τον εξυπηρετητή προσπέλασης: Στην περίπτωση αυτή οι απομακρυσμένοι χρήστες κάνουν μία κλήση στο Δικτυακό Εξυπηρετητή Προσπέλασης (Network Access Server) του παρόχου (lSP) και αυτό δημιουργεί ένα κρυπτογραφημένο τούνελ με το VPN της εταιρείας. Αυτά τα VPN δίνουν τη δυνατότητα στους χρήστες να συνδεθούν σε διάφορα δίκτυα χρησιμοποιώντας πολλαπλά τούνελ, ενώ η εφαρμογή πελάτης (client application) δεν χρειάζεται να έχει λογισμικό για τη δημιουργία τούνελ Το αρνητικό στοιχείο είναι ότι η σύνδεση μεταξύ χρήστη και ISP δεν είναι κρυπτογραφημένη, συνεπώς στηρίζεται στο PSTN, που δεν παρέχει καμία ασφάλεια. Τ ο διάγραμμα ενός τέτοιου VPN φαίνεται στο Σχήμα 2-13



Σχήμα 2-13. Απομακρυσμένη προσπέλαση VPN ενεργοποιημένη από τον δικτυακό εξυπηρετητή (NAS)

Ενεργοποίηση από τον χρήστη: Στην περίπτωση αυτή, απομακρυσμένοι χρήστες χρησιμοποιούν client εφαρμογές για να δημιουργήσουν κρυπτογραφημένα IP τούνελ, μέσω του δικτύου ενός παρόχου υπηρεσιών διαδικτύου (ISP), προς το δίκτυο κάποιας εταιρείας. Το πλεονέκτημα των δημιουργούμενων από τον πελάτη ιδεατών ιδιωτικών δικτύων (clientinitiated VPN) έναντι των δημιουργούμενων από τον εξυπηρετητή του δικτύου (NAS-initiated) είναι ότι χρησιμοποιούν κρυπτογραφημένο τούνελ για τη σύνδεση μεταξύ της εφαρμογής πελάτη (client) και του παρόχου (ISP) μέσω του δημόσιου τηλεφωνικού δικτύου (PSTN) .

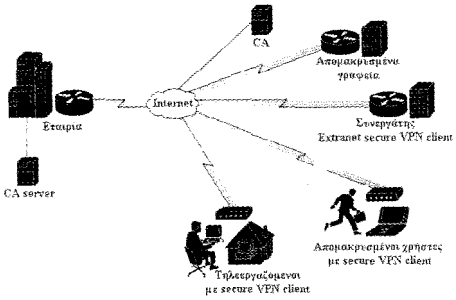


Σχήμα 2-14. Απομακρυσμένη προσπέλαση VPN ενεργοποιημένη από τον χρήστη

Στο Σχήμα 2-14 φαίνεται ένα client-initiated remote access VPN. Η εφαρμογή πελάτης δημιουργεί μία PPP σύνδεση με το NAS του ISP και εν συνεχεία σχηματίζεται ένα κρυπτογραφημένο τούνελ μέσω του δημόσιου τηλεφωνικού δικτύου.

Extranet VPN

Πρόκειται για ένα ιδεατό ιδιωτικό δίκτυο, που επιτρέπει την πρόσβαση σε πελάτες, προμηθευτές και συνεργάτες μιας εταιρείας (Business to business ή B2B VPN). Η υλοποίηση και η διαχείριση της ασφάλειας σε ένα τέτοιο δίκτυο είναι μία επίπονη προσπάθεια που χρειάζεται προσοχή και τα κατάλληλα εργαλεία. Ο σωστός σχεδιασμός αυτού του δικτύου απαιτεί την ιεραρχική σχεδίαση της ασφάλειας με έλεγχο της προσπέλασης σε κάθε επίπεδο.



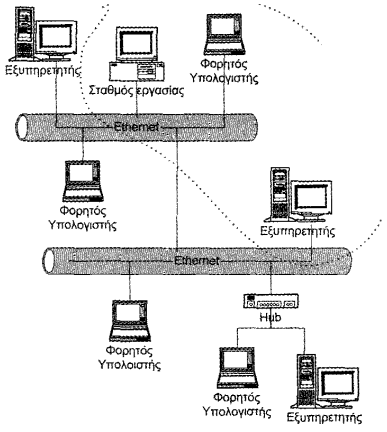
Σχήμα 2-15. Extranet VPN (B2B VPN)

Στο Σχήμα 2-15, φαίνεται μια extranet VPN τοπολογία. Χρησιμοποιώντας ψηφιακά πιστοποιητικά, οι «πελάτες» δημιουργούν μέσω Διαδικτύου, ασφαλή τούνελ προς το δίκτυο μιας εταιρείας. Κάθε «πελάτης» λαμβάνει από την «Αρχή Πιστοποίησης» (Certification Authority - CA) ένα ψηφιακό πιστοποιητικό (digital certificate) το οποίο χρησιμοποιείται για πιστοποίηση από τον CA server της εταιρείας.

Είναι απαραίτητο να υπάρχει μια αξιόπιστη σύνδεση ανάμεσα σε ένα firewall και ένα VPN proxy που θα φιλτράρει την κυκλοφορία που περνά από το firewall σύμφωνα με την πολιτική του οργανισμού.

Intranetwork VPN

Η βασική ιδέα πίσω από τη χρήση τους είναι η δημιουργία ενός VPN μέσα στο δίκτυο της εταιρείας, το οποίο μπορεί να είναι ένα υποδίκτυο, που θα προσφέρει προστασία σε πολύτιμους πόρους και πληροφορίες σημαντικής αξίας για την εταιρεία. Τέτοιες πληροφορίες μπορεί να είναι στοιχεία ερευνών πάνω σε νέα προϊόντα, οικονομικά στοιχεία, πολιτικές παραγωγής και προώθησης προϊόντων, κλπ. Βασική αιτία χρήσης τους είναι το γεγονός ότι πολλές παραβιάσεις στα δίκτυα εταιρειών γίνονται από τους ίδιους τους υπαλλήλους της, οι οποίοι έχουν αποκτήσει πρόσβαση σε μη εξουσιοδοτημένες περιοχές. Οι απώλειες από τέτοιου είδους επιθέσεις δικαιολογούν την υλοποίηση τέτοιων λύσεων.



Σχήμα 2-16. Intranetwork VPN

Το Σχήμα 2-16, δείχνει μια απλή περίπτωση εφαρμογής ενός intranetwork VPN, όπου ένας αριθμός συσκευών έχει συνδεθεί με τέτοιο τρόπο ώστε να αποτελεί ένα εσωτερικό VPN. Όπως φαίνεται οι συσκευές του VPN μπορεί να μην ανήκουν στο ίδιο υποδίκτυο, πράγμα που αποτελεί χαρακτηριστικό της τεχνολογίας αυτής.

2.8. Σύγκριση Κατηγοριών δικτύων

Συγκρίνοντας τα χαρακτηριστικά των διαφορετικών δικτύων ως προς την περίμετρο που ορίζει το «μέσα» και το «έξω» των δικτύων βλέπουμε πως τα χαρακτηριστικά της ασφάλειας γίνονται ασαφή ανάμεσά τους.

Χαρακτηριστικό	intranet	extranet	VPN	internet
Χρήση	εταιρία	Μοιράζεται ανάμεσα σε διαφορετικούς συνεργάτες και ISP's	Εταιρία αλλά υλοποιείται μέσω ISP's	Όλοι ,υλοποιείται κύρια μέσω μεγάλων τηλεπικοινωνιακών οργανισμών
Αξιοπιστία	υψηλή	Μεσαία-Υψηλή	Μεσαία-Υψηλή	Χαμηλή
Ασφάλεια	Συνήθως προφυλάσσεται από τους «έξω»	Συνήθως διαφυλάσσεται από τους «έξω»	Συνήθως προφυλάσσεται από τους «έξω»	Δεν προφυλάσσεται
Τύπος πληροφορίας που διακινείται	ιδιωτική	Επιλεκτική διανομή	Ιδιωτική	Γενικού ενδιαφέροντος
Ταχύτητα	10Mbps-1Gbps	T1-T3	33.6Kbps-T3	33.6Kbps-T1
Κόστος	Υψηλό	Μεσαίο	Μεσαίο-Χαμηλό	Χαμηλό

Κεφάλαιο 3

Τα τρωτά σημεία του διαδικτύου

Ένα σύστημα είναι ασφαλές τόσο, όσο οι άνθρωποι που το χρησιμοποιούν. Κανείς δεν νοιάζεται για την ασφάλεια ενός συστήματος που λειτουργεί συνεχώς και έχει τα απαραίτητα backup για να επανέλθει στην κανονική λειτουργία του, αν συμβεί πρόβλημα στο υλικό.

Το πρόβλημα προκύπτει όταν μία λειτουργική ανάγκη (όπως η εμπιστευτικότητα) πρέπει να υλοποιηθεί. Από την στιγμή που θα αρχίσουν η υλοποιήσεις συστημάτων ασφαλείας, δεν υπάρχει ορατό τέλος στην βελτίωση της ασφάλειας. Όποιος δεν έχει προσπέλαση στο σύστημα, θα προσπαθεί να βρει τρωτό σημείο στην ασφάλεια.

Τρωτό είναι ένα αδύναμο (ασθενικό) σημείο που εκμεταλλεύεται κάποιος που θέλει να βρει ένα τρόπο να εισβάλει, χωρίς εξουσιοδότηση, σε ένα υπολογιστικό/δικτυακό σύστημα. Όταν με χρήση του τρωτού σημείου γίνει εισβολή, τότε μιλάμε για περιστατικό παραβίασης της ασφάλειας. Τα τρωτά σημεία οφείλονται σε σχεδιαστικά και κατασκευαστικά λάθη.

3.1. Γιατί τόσο ενδιαφέρον για την ασφάλεια

Είναι χαρακτηριστικά εύκολο να αποκτήσει κάποιος μη εξουσιοδοτημένη προσπέλαση σε ένα περιβάλλον με χαλαρή ασφάλεια και ταυτόχρονα να μην γίνει ποτέ αντιληπτός. Ακόμα και αν χρήστες του δικτύου δεν έχουν κάτι χρήσιμο σε ένα υπολογιστή, αυτός μπορεί να γίνει η κεκρόπορτα για την εισβολή σε ένα δίκτυο.

Ακόμα και η πιο «αθώα» πληροφορία, όπως τι προγράμματα τρέχουν οι υπολογιστές, τι πρωτόκολλα χρησιμοποιούνται είναι πολύ σημαντικά στοιχεία για τους hackers. Με τη γνώση αυτή μπορούν να δοκιμάσουν γνωστά τρωτά σημεία τους και να αποκτήσουν πρόσβαση σε σημαντικές πληροφορίες.

Το διαδίκτυο είναι ένα μέσο διάδοσης πληροφοριών. Αυτό όμως ισχύει και για τους hackers που μεταδίδουν πληροφορίες για τις αδυναμίες που βρίσκουν σε λειτουργικά συστήματα, πρωτόκολλα και εφαρμογές. Στο διαδίκτυο υπάρχει ένας ανταγωνισμός ταχύτητας, ανάμεσα στο πόσο γρήγορα θα ανηδράσουν οι κατασκευαστές και οι διαχεριστές των υπολογιστικών συστημάτων για να διορθώσουν ένα νέο αδύνατο σημείο στο σύστημά τους, πριν δεχθούν εισβολή και των hackers που θέλουν να εκμεταλλευτούν το αδύνατο σημείο για να εισβάλουν στο σύστημα. Σύμφωνα με στοιχεία του
CERT/CC και τα καθημερινά κρούσματα επιθέσεων, κανένας στο διαδίκτυο δεν μπορεί να θεωρηθεί ασφαλής.

Οι επιπτώσεις μίας παραβίασης στην ασφάλεια μπορεί να είναι ο χαμένος χρόνος για την ανάκτηση της λειτουργικότητας των συστημάτων, η απώλεια χρημάτων και αξιοπιστίας, η αδυναμία συνέχισης της εργασίας, τα νομικά προβλήματα και σε εξαιρετικά σπάνιες περιπτώσεις ο κίνδυνος της ίδιας της ζωής,

Συνήθως οι περιπτώσεις επίθεσης έχουν σκοπό την επίθεση κατά της αξιοπιστίας, της φήμης και της λειτουργικότητας των οργανισμών με αποτέλεσμα την άμεση ή έμμεση χρηματική επιβάρυνση. Επιθέσεις έχουν παρουσιαστεί και σε sites του Ελληνικού χώρου κύρια σε κρατικούς οργανισμούς με σκοπό την δυσφήμησή τους.

3.2. Γιατί το διαδίκτυο είναι τρωτό

Πολλά από τα πρωταρχικά δικτυακά πρωτόκολλα, που τώρα αποτελούν μέρος της υποδομής του διαδικτύου, δεν σχεδιάστηκαν έχοντας κατά νου την ασφάλεια. Χωρίς μία θεμελιώδη ασφαλή υποδομή, η άμυνα του δικτύου γίνεται πιο δύσκολη. Επιπλέον, το διαδίκτυο είναι ένα δυναμικό περιβάλλον. τόσο στην τοπολογία του, όσο και στην τεχνολογία.

Ο στόχος κατά το σχεδιασμό του IP ήταν η δημιουργία ενός πρωτοκόλλου που να διασυνδέει ετερογενή δίκτυα με τέτοιο τρόπο ώστε όλοι οι υπολογιστές να είναι μοναδικά προσδιορισμένοι, να μπορούν να ανταλλάσσουν δεδομένα με μία κοινή μορφοποίηση (format) και τέλος να μεταδώσουν δεδομένα χωρίς να γνωρίζουν στοιχεία για τη δομή και τη μορφή των δικτύων που ανήκουν οι παραλήπτες. Τα διασυνδεόμενα δίκτυα αρχικά αφορούσαν πανεπιστήμια ή ερευνητικά ιδρύματα και στόχος ήταν η διαπανεπιστημιακή συνεργασία. Για αυτόν το λόγο ουδέποτε τέθηκε θέμα ασφάλειας στο σχεδιασμό του IP. Μοιραία λοιπόν οι μηχανισμοί της ασφάλειας απουσιάζουν από εκεί που θα έπρεπε να ήταν ενσωματωμένοι, στο επίπεδο του δικτύου. Όταν αργότερα με την τεράστια εξάπλωση του διαδικτύου και τη χρήση του

για εμπορικούς σκοπούς εμφανίστηκε το θέμα της ασφάλειας, έπρεπε αναγκαστικά να αντιμετωπιστεί σε ένα υψηλότερο επίπεδο, όπως στο επίπεδο εφαρμογής ή σπανιότερα στο επίπεδο μεταφοράς. Για παράδειγμα το πρωτόκολλο Secure Sockets Layer (SSL) λειτουργεί στο επίπεδο μεταφοράς, ενώ το πρωτόκολλο Secure HTTP (SHTTP) λειτουργεί στο επίπεδο εφαρμογής.

Εξαιτίας του κληρονομούμενου ανοικτού περιβάλλοντος του διαδικτύου και του αρχικού σχεδιασμού των πρωτοκόλλων, οι επιθέσεις γενικά είναι γρήγορες, εύκολες,

ανέξοδες και μπορεί να μην είναι δυνατόν να ανακαλυφθούν ή να ανιχνευτούν. Ο εισβολέας δεν χρειάζεται να είναι παρών στο site που επιτίθεται, αλλά αντίθετα μπορεί να βρίσκεται οπουδήποτε στον κόσμο και μάλιστα είναι δυνατό να αποκρυφτεί και το σημείο που βρίσκεται.

Μία άλλη μέθοδος ενίσχυσης της ασφάλειας που εμφανίστηκε τελευταία και χρησιμοποιείται όλο και πιο συχνά είναι αυτή της δημιουργίας ιδεατών ιδιωτικών δικτύων (VPNs) με χρήση κατάλληλου λογισμικού η υλικού. Η βασική φιλοσοφία αυτών των μεθόδων είναι η κωδικοποίηση του πακέτου που πρόκειται να μεταδοθεί και κατόπιν η ενσωμάτωσή του σε ένα νέο πακέτο που αποστέλλεται στον προορισμό. Η μετατροπή δηλαδή του αρχικού IP πακέτου σε δεδομένα ενός άλλου IP πακέτου όπου τα πεδία που αφορούν τις διευθύνσεις αποστολέα και παραλήπτη είναι διαφορετικά από ότι στο αρχικό πακέτο (tunneling).

Παρά τις επιτυχημένες προσπάθειες σε όλες αυτές τις μέθοδες εξακολουθεί να υπάρχει ένα σοβαρό πρόβλημα. Αν χρησιμοποιείται ασφάλεια στο επίπεδο εφαρμογής τότε υπάρχει αρκετή πληροφορία που περιέχεται στην επικεφαλίδα του πακέτου στο οποίο ενσωματώνεται το κωδικοποιημένο πακέτο, που είναι ευάλωτη σε επιθέσεις. Με χρήση προγραμμάτων ανάλυσης της δικτυακής κυκλοφορίας (sniffers) είναι δυνατόν να αποκαλυφθούν οι διεργασίες και τα συστήματα που ανταλλάσσουν πληροφορίες. Επίσης το κόστος της υποστήριξης της ασφάλειας από κάθε εφαρμογή χωριστά στοιχίζει αρκετά σε σχέση με το να παρέχονταν η ασφάλεια στο επίπεδο του δικτύου και κάθε εφαρμογή να έκανε χρήση αυτής.

Αν χρησιμοποιείται ασφάλεια στο επίπεδο μεταφοράς, τότε αυτό σημαίνει ότι οι εφαρμογές που χρησιμοποιούν αυτή τη μέθοδο πρέπει να ξαναγραφτούν, ώστε τόσο ο εξυπηρετητής όσο και ο πελάτης να κάνουν χρήση αυτής της ασφάλειας.

Τέλος η χρήση πρωτοκόλλων tunneling έχει μέτρια απόδοση, αλλά επιπλέον πάσχει από έλλειψη κάποιου πρότυπου που θα μπορέσει να ακολουθηθεί.

Είναι πάντως κοινό στους οργανισμούς να δείχνουν μία ατεκμηρίωτη εμπιστοσύνη στο διαδίκτυο, έχοντας άγνοια των κινδύνων που παραμονευτούν. Πιστεύουν πως το site τους δεν είναι στόχος ή πως έχουν πάρει όλα τα απαραίτητα μέσα για την προστασία τους. Όμως η τεχνολογία αλλάζει ταχύτατα και το ίδιο τα εργαλεία που καιοσκευάζουν οι εισβολείς. Έτσι τα μέτρα που λαμβάνονται δεν ισχύουν μετά την πάροδο σύντομου χρονικού διαστήματος .

. Εξαιτίας του ότι το μεγαλύτερο μέρος της κυκλοφορίας στο διαδίκτυο δεν είναι κρυπτογραφημένο, δεν είναι εφικτή η εμπιστευτικότητα και ακεραιότητα των πληροφοριών. Σαν αποτέλεσμα ένα site μπορεί να δεχθεί επιθέσεις από άλλο με χρήση εργαλείων, όπως ένας packet sniffer, που μπορεί να είναι εγκατεστημένος στο ένα και να μαζεύει στοιχεία για άλλο.

Ένας άλλος παράγοντας που συνεισφέρει στην επιδείνωση του προβλήματος είναι η ραγδαία ανάπτυξη των υπηρεσιών πάνω από το διαδίκτυο. Με χρήση πολύπλοκων εφαρμογών, που δυστυχώς δεν σχεδιάζονται, εγκαθίστανται και συντηρούνται με προσοχή, μένουν τρωτά σημεία στον κώδικα των προγραμμάτων και των λειτουργικών.

Η επιλογή του λειτουργικού συστήματος που εγκαθίσταται στον εξοπλισμό πρέπει να γίνεται με κριτήριο την ενίσχυση της ασφάλειας, και όχι με κριτήριο την ταχύτητα, τις επιδόσεις, την τιμή, την ευκολία χρήσης, την διαχείριση, και την υποστήριξη.

Συνήθως η στάνταρ διαμόρφωση του λειτουργικού, όπως έρχεται από τον κατασκευαστή δεν είναι η κατάλληλη για την διασφάλιση και ενίσχυση της ασφάλειας, δίνοντας την δυνατότητα στους γνώστες να επιχειρήσουν επίθεση αμέσως μετά την πρώτη εγκατάσταση.

Τέλος πρέπει να τονιστεί, πως με την εξέλιξη του διαδικτύου υπάρχει η ανάγκη για εξειδικευμένους τεχνικούς σε θέματα ασφάλειας που θα αναλύουν, σχεδιάζουν, εγκαθιστούν και συντηρούν την ασφάλεια ενός site.

Τύποι τρωτών

Η ακόλουθη ταξινόμηση είναι χρήσιμη για να καταλάβουμε τους τεχνικούς λόγους, πίσω από επιτυχείς τεχνικές παραβίασης της ασφάλειας και να βοηθήσει τους ειδικούς να προσδιορίσουν γενικές λύσεις για τον ίδιο τύπο προβλημάτων.

Ελαττώματα στο λογισμικό ή στο σχεδιασμό των πρωτοκόλλων

Τα πρωτόκολλα ορίζουν του κανόνες και τις μεθόδους για να μπορούν οι υπολογιστές να επικοινωνούν μεταξύ τους στο δίκτυο. Αν το πρωτόκολλο έχει σχεδιαστικό λάθος είναι επισφαλές σε εκμετάλλευση του τρωτού σημείου ανεξάρτητα από το πόσο καλά υλοποιήθηκε. Ένα τέτοιο παράδειγμα είναι το Network File System (NFS), που επιτρέπει στα συστήματα να μοιράζουν αρχεία. Το πρωτόκολλο αυτό δεν περιλαμβάνει έναν τρόπο πιστοποίησης, έτσι ώστε ο χρήστης που συνδέεται δεν πιστοποιείται για το αν είναι αυτό που διατείνεται. Οι NFS servers είναι στόχος για την κοινότητα των εισβολέων.

Όταν σχεδιάζεται το λογισμικό χωρίς η ασφάλεια να συμπεριλαμβάνεται στις αρχικές προδιαγραφές, υπάρχει το ενδεχόμενο το επιπλέον τμήμα που προστίθεται για την ενίσχυση της ασφάλειας, να μην αλληλεπιδρά όπως είχε αρχικά σχεδιαστεί και να προκύπτουν απρόσμενα τρωτά σημεία.

Αδυναμίες στην υλοποίηση του λογισμικού ή του πρωτοκόλλου

Ακόμα και αν ένα πρωτόκολλο έχει σχεδιαστεί σωστά και προσεχτικά, μπορεί να έχει τρωτά σημεία από τον τρόπο υλοποίησής του. Για παράδειγμα, ένα πρωτόκολλο για ηλεκτρονικό ταχυδρομείο, μπορεί να υλοποιηθεί με τέτοιο τρόπο που να επιτρέπει την σύνδεση στο mail port του συστήματος που θα γίνει η επίθεση και να ζητήσει να εκτελέσει συγκεκριμένες εντολές. Έτσι ο εισβολέας μπορεί να γράψει στο πεδίο «To:», αντί την σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου, συγκεκριμένες εντολές και να ζητήσει το password file του συστήματος, χωρίς να χρειάζεται καν λογαριασμός στο σύστημα.

Το λογισμικό μπορεί να έχει τρωτά σημεία, επειδή δεν βρέθηκαν πριν την τελική έκδοση. Οι εισβολείς ψάχνουν και βρίσκουν τα ελαττώματα αυτά με δικά τους εργαλεία. Για παράδειγμα ψάχνουν για ελαττώματα σε περιπτώσεις όπως:

- Ανταγωνιστικές καταστάσεις στην προσπέλαση αρχείων
- Ανυπαρξία ελέγχων για το περιεχόμενο και το μέγεθος των δεδομένων
- Ανυπαρξία ελέγχων γω την ανημετώπιση εσωτερικών λαθών
- Αδυναμία προσαρμογής σε εξάντληση πόρων
- Ελλιπή έλεγχο του λειτουργικού περιβάλλοντος
- Ανάρμοστη χρήση κλήσεων του συστήματος
- Χρήση τμημάτων του λογισμικού για άλλο σκοπό από αυτό που σχεδιάστηκαν.

Κάνοντας χρήση αδυναμιών στο λογισμικό οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε πόρους, χωρίς να χρειάζονται την απαραίτητη εξουσιοδότηση από το σύστημα

Αδυναμίες στην διαμόρφωση των συστημάτων και των δικτύων

Τρωτά σημεία σε αυτή την κατηγορία δεν προέρχονται από προβλήματα στα πρωτόκολλα ή το λογισμικό. Αντίθετα τα προβλήματα αυτά προέρχονται από τον τρόπο που αυτά τα δομικά στοιχεία, εγκαθίστανται και χρησιμοποιούνται Τα προϊόντα παραδίδονται και συνήθως εγκαθίστανται με προκαθορισμένες παραμέτρους, που οι εισβολείς μπορούν να εκμεταλλευτούν. Οι διαχειριστές συστημάτων και οι χρήστες μπορεί να μην αλλάξουν ης προκαθορισμένες παραμέτρους, με αποτέλεσμα το σύστημα να εμφανίζει τρωτά.

Ένα παράδειγμα λανθασμένης διαμόρφωσης που συχνά εκμεταλλεύονται Οι εισβολείς είναι η ανώνυμη χρήση της υπηρεσίας File Transfer Protocol (FTP). Οι οδηγίες για την ασφαλή διαμόρφωση αυτής της υπηρεσίας τονίζουν την ανάγκη το password file, τα βοηθητικά προγράμματα και τα αρχεία δεδομένων να βρίσκονται σε άλλη θέση στο σύστημα από το υπόλοιπο λειτουργικό σύστημα και αυτό να μην μπορεί να προσπελαστεί από τον χώρο αποθήκευσης του FTP. Όταν τα sites δεν προσέξουν την διαμόρφωση του ftp server τότε μη εξουσιοδοτημένοι χρήστες μπορούν να βρουν πληροφορίες πιστοποίησης και να τις εφαρμόσουν για να αποκτήσουν προσπέλαση.

Κεφάλαιο 4

Η Αναγκαιότητα της Ασφάλεια

ΔΕΝ ΧΡΕΙΑΖΕΤΑΙ ΠΑΡΑ να ρίξει κανείς μία ματιά στις ημερήσιες εφημερίδες μεγάλης κυκλοφορίας για να διαπιστώσει ότι οι επιθέσεις σε υπολογιστές παρουσιάζουν ανησυχητική αύξηση. Σχεδόν κάθε ημέρα υπάρχουν δημοσιεύματα για περιστατικά παρενόχλησης ή διείσδυσης στα υπολογιστικά συστήματα κυβερνητικών και άλλων οργανισμών. Ακόμη και οργανισμοί μεγάλου κύρους, όπως ο στρατός των Η.Π.Α. και η Microsoft έχουν δεχτεί επιθέσεις από χάκερ. Θα πρέπει να αναφέρουμε ότι δεν δημοσιεύονται όλες οι επιθέσεις που γίνονται σε υπολογιστικά συστήματα. Ενώ η επίθεση στους υπολογιστές του FBI μπορεί να γίνει πρωτοσέλιδο, πολλές επιθέσεις δεν βλέπουν ποτέ τα φώτα της δημοσιότητας. Το να αποκαλυφθεί ότι μία συγκεκριμένη εταιρεία υπήρξε θύμα κλοπής των οικονομικών δεδομένων της ή των κατασκευαστικών σχεδίων των νέων προϊόντων της μπορεί να έχει σοβαρές οικονομικές επιπτώσεις. Το ίδιο ισχύει και για κάποια τράπεζα που θα ανακοίνωνε ότι παραβιάστηκε η ασφάλεια των υπολογιστικών της συστημάτων και κλάπηκε ένα μεγάλο χρηματικό ποσό. Τέλος, υπάρχει επίσης ένας μεγάλος αριθμός επιθέσεων οι οποίες παραμένουν εντελώς ατεκμηρίωτες. Η πιο κοινή κατηγορία τέτοιων επιθέσεων είναι οι επιθέσεις που γίνονται εκ των έσω: σε τέτοιες περιπτώσεις ο οργανισμός που πέφτει θύμα της επίθεσης μπορεί να μην επιθυμεί να δώσει μεγαλύτερη έκταση στο θέμα, εκτός φυσικά από την απόλυση του υπαλλήλου ή των υπαλλήλων που είναι υπαίτιοι.

Δεν υπάρχουν ρεαλιστικά στατιστικά στοιχεία όσον αφορά στον αριθμό των παραβιάσεων των συστημάτων ασφάλειας που παραμένουν κρυφές. Ωστόσο, είναι σαφές ότι οι επιθέσεις σε υπολογιστικά συστήματα βρίσκονται σε ανησυχητικά ανοδική πορεία και για τον λόγο αυτό κάθε δίκτυο χρειάζεται μία συγκεκριμένη στρατηγική για την αποτροπή τους.

4.1. Το Σκεπτικό ενός Εισβολέα

Εάν θέλετε να εξακριβώσετε ποιος είναι ο καλύτερος τρόπος για να διαφυλάξετε τους πόρους σας, θα πρέπει να προσδιορίσετε ποιος θα ήθελε να τους παραβιάσει, ή να τους κλέψει. Οι περισσότερες επιθέσεις σε υπολογιστικά συστήματα δεν είναι τυχαίες· συνήθως το άτομο που τις εκκινεί πιστεύει ότι έχει να κερδίσει κάτι παρενοχλώντας το δίκτυο σας, ή υποκλέπτοντας τα δεδομένα σας. Το να προσδιορίσετε ποιος θα μπορούσε να έχει όφελος από την υποκλοπή ή την παρενόχληση των πόρων σας είναι το πρώτο βήμα που μπορείτε να κάνετε για να τους προστατέψετε.

Εισβολείς Χάκερ και Cracker

Οι λέξεις "εισβολέας" (attacker) χάκερ (HACKER) και κράκερ (cracker) χρησιμοποιούνται συνήθως με ταυτόσημη σημασία. Ωστόσο, υπάρχουν ορισμένες σημαντικές διαφορές μεταξύ αυτών των τριών όρων. **Εισβολέας** είναι κάποιος ο οποίος αναζητά τρόπους για να κλέψει ή να καταστρέψει τα συστήματα σας. Ένας εισβολέας μπορεί να έχει υψηλό επίπεδο τεχνικών γνώσεων, ή να είναι απλώς ένας επιδέξιος ερασιτέχνης, θα μπορούσαμε να παρομοιάσουμε τους εισβολείς με έναν κατάσκοπο, ή έναν κοινό ληστή.

Όσον αφορά στην λέξη **χάκερ (hacker)**, η αρχική σημασία της ήταν θετική: σαν χάκερ χαρακτηρίζονταν κάποιος ο οποίος είχε βαθιά γνώση των υπολογιστών και της δικτύωσης. Οι χάκερ δεν ικανοποιούνται με την απλή εκτέλεση ενός προγράμματος· θέλουν να γνωρίζουν τα πάντα για τον τρόπο λειτουργίας του ακόμη και την παραμικρή λεπτομέρεια. Ένας χάκερ είναι κάποιος ο οποίος αισθάνεται την ανάγκη να προχωρήσει πέρα από τα προφανή. Η τέχνη των χάκερ μπορεί να είναι είτε θετική, είτε αρνητική, ανάλογα με την προσωπικότητα κάθε ατόμου και τα κίνητρα του.

Δεν εκλαμβάνουν τίποτα ως δεδομένο. Για παράδειγμα, όταν ένας κατασκευαστής ισχυρίζεται "Το προϊόν μου είναι 100% ασφαλές", ένας χάκερ μπορεί να εκλάβει αυτή την δήλωση σαν μία προσωπική πρόκληση την οποία πρέπει οπωσδήποτε να αντιμετωπίσει. Ωστόσο, το τι ακριβώς θα αποφασίσει να κάνει ο χάκερ με τις πληροφορίες που θα αποκαλύψει είναι αυτό που καθορίζει σε ποια πλευρά θα τον κατατάξουμε - στους "καλούς" ή στους "κακούς".

Ένας χάκερ ο οποίος βρίσκει έναν τρόπο για να εκμεταλλευτεί μία "ρωγμή" στην ασφάλεια ενός προγράμματος και την δημοσιοποιεί (αντί να προσπαθήσει να την εκμεταλλευτεί ιδιοτελώς) αποκαλείται "χάκερ με λευκό καπέλο". Εν αντιθέσει, εάν ένας χάκερ εντοπίσει μία ρωγμή στην ασφάλεια ενός προγράμματος και αποφασίσει να την χρησιμοποιήσει έναντι ανυποψίαστων θυμάτων για προσωπικό όφελος, τότε λέμε ότι φοράει μαύρο καπέλο. Το γκρι καπέλο δίνεται στους χάκερ οι οποίοι φορούν λευκό καπέλο την ημέρα, αλλά μαύρο την νύχτα. Με άλλα λόγια, στους χάκερ οι οποίοι απασχολούνται νόμιμα σαν σύμβουλοι ασφάλειας την ημέρα αλλά αναπτύσσουν παράνομη δραστηριότητα στον ελεύθερο χρόνο τους.

Πολλοί άνθρωποι παρεξηγούν τα κίνητρα αυτών που δημοσιεύουν λεπτομέρειες γνωστών σφαλμάτων (bugs) σε εφαρμογές λογισμικού. Πολύ σπάνια γίνεται αυτό με στόχο να εκπαιδευτούν άλλοι εισβολείς. Συνηθέστερα η κοινοποίηση των τρωτών σημείων ενός υπολογιστικού συστήματος ή λογισμικού προειδοποιεί τους κατασκευαστές και τους επόπτες συστημάτων για το πιθανό πρόβλημα και την ανάγκη λύσης του. Πολλές φορές, η δημόσια κοινοποίηση ενός τρωτού σημείου γίνεται από απλή ενόχληση ή από αναγκαιότητα. Η δημοσιοποίηση τέτοιων προβλημάτων έδωσε λανθασμένη εντύπωση σε ορισμένους παρατηρητές. Όταν κάποιος βρίσκει ένα πρόβλημα σχετιζόμενο με την ασφάλεια ενός συστήματος και το αναφέρει στο ευρύ κοινό, ορισμένοι μπορεί να πιστέψουν ότι αυτός που το αναφέρει είναι ένας εισβολέας ο οποίος εκμεταλλεύεται το πρόβλημα για προσωπικό όφελος. Ωστόσο, αυτή η τακτική να κοινοποιούνται και να συζητιούνται ανοικτά τα σχετιζόμενα με την ασφάλεια προβλήματα έχει οδηγήσει στην ανάπτυξη πιο εύρωστου λογισμικού, με υψηλότερο βαθμό ακεραιότητας.

Τα κίνητρα των πιθανών εισβολέων

Ποιο όμως μπορεί να είναι για κάποιον άνθρωπο το κίνητρο να εξαπολύσει μία επίθεση εναντίον του δικτύου σας αυτού του είδους οι επιθέσεις σπάνια είναι τυχαίες. Σχεδόν πάντα υποδηλώνουν ότι ο εισβολέας έχει κάτι να κερδίσει από την επίθεση. Το τι ακριβώς προκαλεί την επίθεση, εξαρτάται από τον οργανισμό και από το άτομο που την εξαπολύει.

Επιθέσεις εκ των Εσω

Μελέτες έχουν δείξει ότι στην συντριπτική πλειοψηφία των περιπτώσεων, οι επιθέσεις που δέχονται οι οργανισμοί προέρχονται εκ των έσω. Στην πραγματικότητα, ορισμένες μελέτες ισχυρίζονται ότι έως και το 70% όλων των επιθέσεων που δέχονται τα υπολογιστικά συστήματα προέρχονται από κάποιον εντός του οργανισμού, ή από κάποιον ο οποίος μπορεί να έχει πληροφόρηση εκ των έσω (π.χ. ένας πρώην υπάλληλος). Αν και η χρήση συστημάτων firewall για την προστασία των δικτύων από εξωτερικές επιθέσεις έχει πλέον καθιερωθεί, ακόμη και σήμερα οι υπάλληλοι είναι υπεύθυνοι για τις μεγαλύτερες καταστροφές που μπορούν να υποστούν τα δεδομένα ενός οργανισμού (δηλαδή, τα άτομα που έχουν άμεση γνώση του τρόπου λειτουργίας του δικτύου σας). Τέτοιου είδους καταστροφές μπορεί να είναι τυχαίες (π.χ. ένα αθώο λάθος ενός χρήστη) ή, σε ορισμένες περιπτώσεις, σκόπιμες.

Η συνηθέστερη αιτία μιας πραγματικής επίθεσης είναι ένας δυσαρεστημένος υπάλληλος ή πρώην υπάλληλος.

Αν και οι περισσότεροι επόπτες συστημάτων καταβάλλουν σημαντικές προσπάθειες γία να προστατέψουν το δίκτυο τους από τις εξωτερικές επιθέσεις, συχνά παραβλέπουν την πολύ μεγαλύτερη απειλή των επιθέσεων εκ των έσω. Ένα άτομο δεν χρειάζεται να είναι χαρακτηρισμένος εισβολέας για να μπορεί να κάνει ζημιά στους πόρους μιας εταιρείας. Σε ορισμένες περιπτώσεις, η ζημιά γίνεται απλά και μόνο από άγνοια.

Μία άλλη απειλή η οποία παρουσιάζεται με ανησυχητική συχνότητα δεν είναι η καταστροφή των δεδομένων, αλλά η κλοπή τους. Αυτό αναφέρεται συνήθως με τον όρο "βιομηχανική κατασκοπεία" και αν και δεν θεωρείται τόσο κοινό όσο η καταστροφή των δεδομένων "εκ των έσω", αποτελεί μία υπαρκτή απειλή για οποιονδήποτε οργανισμό διατηρεί "εμπιστευτικά" δεδομένα κυρίως όταν η υποκλοπή αυτών των δεδομένων θα μπορούσε να αφήσει τον οργανισμό νομικά υπεύθυνο.

Εξωτερικές Επιθέσεις

Οι εξωτερικές επιθέσεις μπορούν να προέρχονται από πολλές και ποικίλες πηγές. Αν και μπορούν επίσης να προέρχονται από δυσαρεστημένους υπαλλήλους, η γκάμα των πιθανών εισβολέων που μπορούν να εκκινήσουν μία εξωτερική επίθεση είναι πολύ μεγαλύτερη. Το μόνο κοινό στοιχείο είναι ότι συνήθως κάποιος έχει να κερδίσει κάτι κάνοντας μία τέτοια επίθεση.

Ανταγωνιστές

Εάν δραστηριοποιείστε σε έναν τομέα της αγοράς στον οποίο υπάρχει μεγάλος ανταγωνισμός, ένας φιλόδοξος ανταγωνιστής σας μπορεί να διαβλέψει πιθανό όφελος κάνοντας μία επίθεση στο δίκτυο σας. Η επίθεση αυτή μπορεί να πάρει την μορφή της κλοπής των πρωτότυπων κατασκευαστικών σχεδίων ενός νέου προϊόντος, ή των οικονομικών στοιχείων της εταιρείας σας. Μία τέτοια επίθεση θα μπορούσε επίσης να έχει σαν στόχο να καταστήσει άχρηστους τους πόρους του δικτύου σας, ώστε να σας προκαλέσει οικονομική ζημιά (διαφυγόντα κέρδη).

Το όφελος από την κλοπή των σχεδίων ενός νέου προϊόντος είναι προφανές. Έχοντας αυτές τις πληροφορίες, ο "κλέφτης" μπορεί να χρησιμοποιήσει τα δικά σας σχέδια για να μειώσει τον χρόνο ανάπτυξης του δικού του ανταγωνιστικού προϊόντος, ή για να το βελτιώσει με περισσότερες και καλύτερες λειτουργίες. Εάν ένας ανταγωνιστής ξέρει ποια προϊόντα σκοπεύετε να κυκλοφορήσετε στο εγγύς μέλλον, μπορεί να σας προλάβει παρουσιάζοντας στην αγορά ένα πιο ελκυστικό προϊόν.

Η κλοπή οικονομικών στοιχείων μπορεί να είναι εξίσου καταστροφική. Αποκτώντας όλα τα δεδομένα του προηγούμενου οικονομικού έτους της εταιρείας σας, ένας ανταγωνιστής σας θα μπορούσε να αποκτήσει σαφές "πλεονέκτημα" στην αγορά. Και σ' αυτή την περίπτωση το πλεονέκτημα απορρέει από την γνώση: της οικονομικής ευρωστίας της εταιρείας σας (ή της έλλειψης της), ή των πηγών από τις οποίες προέρχονται τα έσοδα της εταιρείας σας.

Διαφορά Απόψεων

Η άλλη κατηγορία επιθέσεων υποκινείται συνήθως από κάτι το οποίο δεν έχει σχέση με την απληστία ή την βία. Αποκαλούμενοι συχνά "hacktivists" από τον συνδυασμό των λέξεων hacker και activist τα άτομα αυτά επιτίθενται σε συστήματα με στόχο την διακοπή της παροχής υπηρεσιών, την δυσφήμιση συγκεκριμένων Web sites , ή γενικότερα την προσέλκυση της προσοχής του κοινού στα πιστεύω τους. Αυτή η κατηγορία επιθέσεων έχει καθαρά πολιτικό-στρατιωτικούς στόχους, μεταφέροντας τις πολεμικές συγκρούσεις από τον πραγματικό κόσμο στον κυβερνοχώρο.

Υψηλό Προφίλ

Οργανισμοί οι οποίοι είναι ευρέως γνωστοί ή έρχονται πολύ συχνά στην δημοσιότητα μπορούν να γίνουν στόχοι επιθέσεων απλά και μόνο λόγω της δημοσιότητας που απολαμβάνουν. Ένας υποψήφιος εισβολέας μπορεί να επιχειρήσει να επιτεθεί σε ένα γνωστό site, ελπίζοντας ότι μία επιτυχημένη επίθεση θα του αποφέρει τα λίγα λεπτά δημοσιότητας που του αναλογούν

.

Ηλεκτρονικό Ταχυδρομείο

Αναμφισβήτητα η πιο προσβλητική μορφή επίθεσης είναι η χρήση του συστήματος ηλεκτρονικού ταχυδρομείου του οργανισμού σας σαν αναμεταδότη spam. Ο όρος “spam” χαρακτηρίζει την αποστολή ανεπιθύμητων μηνυμάτων e-mail (διαφημίσεις, σχήματα πυραμίδας, κ.α.). Αυτοί που ασχολούνται με το spam οι spammers ελπίζουν ότι ο τεράστιος όγκος των διαφημίσεων που στέλνουν θα παράγει κάποιο ενδιαφέρον για το προϊόν ή την υπηρεσία που διαφημίζουν. Συνήθως, όταν ένας spammer στέλνει μια διαφήμιση, αυτή φτάνει σε δεκάδες χιλιάδες διευθύνσεις ηλεκτρονικού ταχυδρομείου και ταχυδρομικές λίστες. Όταν ένας spammer χρησιμοποιεί το δικό σας σύστημα e-mail σαν αναμεταδότη, το σύστημα σας γίνεται ο κόμβος από τον οποίο αποστέλλονται όλα αυτά τα μηνύματα στους παραλήπτες.

Το αποτέλεσμα είναι μία κατάσταση άρνησης εξυπηρέτησης (Denial of Service). Κατά την διάρκεια που ο δικός σας server ηλεκτρονικού ταχυδρομείου ξοδεύει τον χρόνο του για την διεκπεραίωση του spam, δεν μπορεί να χειριστεί την εισερχόμενη και εξερχόμενη ηλεκτρονική αλληλογραφία του οργανισμού σας.

Τα περισσότερα σύγχρονα συοτήματα ηλεκτρονικού ταχυδρομείου περιλαμβάνουν πλέον ειδικές ρυθμίσεις για την καταπολέμηση του spam. Αν και οι ρυθμίσεις αυτές δεν μπορούν να εμποδίσουν τα μηνύματα spam να φτάσουν μέχρι την θυρίδα σας, εμποδίζουν την χρήση του συστήματος σας σαν αναμεταδότη spam, κάνοντας δεκτά μόνο τα μηνύματα που προορίζονται για, ή προέρχονται από, το δικό σας domain.

Φοβούμενοι την τιμωρία, οι περισσότεροι spammers προτιμούν να χρησιμοποιούν το δικό σας σύστημα e-mail αντί για το δικό τους. Ένας τυπικός spammer προσπαθεί να κρύψει την πραγματική διεύθυνση αποστολέα· έτσι, οποιοσδήποτε προσπαθήσει να τον εντοπίσει, θα υποθέσει ότι το ανεπιθύμητο μήνυμα προήλθε από το δικό σας δίκτυο.

4.3. Πόση ασφάλεια χρειάζεστε;

Πριν αποφασίσετε ποιος είναι ο καλύτερος τρόπος για να ασφαλίσετε το δίκτυο σας, θα πρέπει να προσδιορίσετε το επίπεδο της προστασίας που θέλετε να επιτύχετε. Συγκεκριμένα, θα πρέπει να ξεκινήσετε αναλύοντας το δίκτυο σας για να εξακριβώσετε το επίπεδο "οχύρωσης" που χρειάζεται πραγματικά. Μπορείτε κατόπιν να χρησιμοποιήσετε αυτή την πληροφορία για να αναπτύξετε την πολιτική ασφάλειας για το δίκτυο σας. Οπλισμένοι μ' αυτή την γνώση, θα είστε σε πολύ καλή θέση για ν' αρχίσετε να λαμβάνετε τις καλύτερες δυνατές αποφάσεις σχετικά με την δομή της ασφάλειας του δικτύου σας.

Ανάλυση κινδύνων

Ανάλυση κινδύνων (irisk analysis) είναι η διαδικασία προσδιορισμού των πόρων που θέλετε να προστατέψετε και των πιθανών απειλών από τις οποίες μπορεί να κινδυνεύουν. Η διεξαγωγή της ανάλυσης κινδύνων με ακρίβεια και σαφήνεια είναι ένα βήμα ζωτικής σημασίας για την ασφάλιση του περιβάλλοντος του δικτύου σας.

Ποιους πόρους θέλω να προστατέψω;

Οποιαδήποτε αποτελεσματική ανάλυση κινδύνων πρέπει να ξεκινά προσδιορίζοντας τους πόρους και τα "κεφάλαια" του οργανισμού σας τα οποία θέλετε να προστατέψτε. Τυπικά, οι πόροι αυτοί εμπίπτουν σε μία από τις ακόλουθες τέσσερις κατηγορίες:

- Φυσικοί πόροι
- Πνευματικοί πόροι
- Σχετιζόμενοι με τον χρόνο πόροι
- Πόροι που σχετίζονται με την αντίληψη των άλλων ανθρώπων για τον οργανισμό σας

Φυσικοί πόροι

Στους φυσικούς πόρους εμπίπτει οτιδήποτε έχει φυσική μορφή. Σ' αυτή την κατηγορία περιλαμβάνονται οι σταθμοί εργασίας του δικτύου, οι servers, τα τερματικά, τα hubs (διανομείς) του δικτύου, καθώς και οι υπόλοιπες περιφερειακές συσκευές. Βασικά, οποιοσδήποτε υπολογιστικός πόρος έχει φυσική μορφή μπορεί να θεωρηθεί φυσικός πόρος.

Όταν διεξάγετε την ανάλυση κινδύνων, δεν θα πρέπει να ξεχνάτε του φυσικούς πόρους.

Ο τελικός στόχος της ανάλυσης κινδύνων είναι η κατάστρωση ενός αποτελεσματικού σε σχέση με το κόστος πλάνου για την διαφύλαξη των πόρων σας. Κατά την πορεία της ανάλυσης δεν θα πρέπει να παραβλέψετε τους πιο προφανείς τομείς προβλημάτων και τις αντίστοιχες λύσεις.

Πνευματικοί πόροι

Οι πνευματικοί πόροι είναι δυσκολότερο να προσδιοριστούν από τους φυσικούς πόρους, επειδή συνήθως υπάρχουν μόνο σε ηλεκτρονική μορφή. Στην κατηγορία των πνευματικών πόρων συγκαταλέγεται οποιαδήποτε μορφή πληροφορίας είναι σημαντική για την λειτουργία του οργανισμού. Πιο συγκεκριμένα, σ' αυτή την κατηγορία μπορεί να περιλαμβάνεται το λογισμικό, τα οικονομικά στοιχεία, οι βάσεις δεδομένων, όπως επίσης και οποιαδήποτε σχέδια προϊόντων.

Σχετιζόμενοι με τον χρόνο πόροι

Ο χρόνος είναι πολύ σημαντικός πόρος για οποιονδήποτε οργανισμό ή επιχείρηση, αλλά πολλές φορές αγνοείται κατά την διεξαγωγή της ανάλυσης κινδύνων. Ωστόσο, για πολλούς οργανισμούς ο χρόνος είναι ένας από τους πολυτιμότερους πόρους που διαθέτουν. Όταν αποτιμάτε το κόστος της απώλειας χρόνου για τον οργανισμό σας, βεβαιωθείτε ότι περιλαμβάνετε στην αξιολόγηση σας όλες τις συνέπειες που θα είχε αυτή η απώλεια.

Πόροι που σχετίζονται με την αντίληψη των άλλων για τον οργανισμό σας

Μετά από τις επιθέσεις άρνησης εξυπηρέτησης τον Φεβρουάριο του 2000, οι περισσότερες εταιρείες-θύματα (Yahoo, AMAZON, eBay και Buy.com μεταξύ άλλων) αντιμετώπισαν πτώση της τιμής των μετοχών τους. Παρά το γεγονός ότι η απώλεια αυτή δεν ήταν μακροπρόθεσμη, ήταν μία υπαρκτή, μετρήσιμη αρνητική επίδραση στην εμπιστοσύνη των καταναλωτών και των μετόχων. Λόγω της δημοσιότητας που έλαβε η διείσδυση κάποιων χάκερ στα συστήματα της Microsoft τον Οκτώβριο του 2000, κάποιοι

αναρωτήθηκαν μήπως οι εισβολείς κατάφεραν να κάνουν αλλαγές σε πολύτιμο πηγαίο κώδικα, οι οποίες πέρασαν απαρατήρητες. Αν και η Microsoft αρνήθηκε οποιαδήποτε ζημιά, απλά και μόνο το γεγονός της παραβίασης των συστημάτων της ήταν αρκετό για να αμαυρώσει την αξιοπιστία της και την εμπιστοσύνη των καταναλωτών όχι μόνο στην εταιρεία, αλλά και στα προϊόντα της.

Ο κίνδυνος καταστροφής της φήμης ενός οργανισμού υπήρξε αιτία σημαντικών μπελάδων για όσους εργάζονται στον τομέα της ασφάλειας (συμπεριλαμβανομένων των υπηρεσιών επιβολής του νόμου), οι οποίοι βασίζονται στις πληροφορίες και την απειρία των συναδέλφων τους για να σχεδιάσουν καλύτερα συστήματα προστασίας, ή για να κάνουν νομικές ενέργειες. Σε μία προσπάθεια να ενθαρρύνει την ελεύθερη ανταλλαγή πολύτιμων τεχνικών λεπτομερειών για τις επιθέσεις που δέχονται οι εταιρείες από χάκερ, χωρίς ωστόσο να ζημιώνεται η φήμη τους, το FBI δημιούργησε μία ομάδα προστασίας των υποδομών και των υπολογιστικών συστημάτων από πιθανές επιθέσεις (Infrastructure Protection and Computer Intrusion Squad, IPCIS), η οποία λειτουργεί σαν ένα ανώνυμο ίδρυμα "συγκέντρωσης τεχνογνωσίας".

Από ποιες οντότητες προσπαθώ να προστατέψω τους πόρους μου;

Οι πιθανές επιθέσεις σε δίκτυα μπορούν να προέρχονται από οποιαδήποτε πηγή η οποία έχει πρόσβαση στο δίκτυο σας. Αυτές οι πηγές μπορούν να ποικίλουν σε μεγάλο βαθμό, ανάλογα με το μέγεθος του οργανισμού σας και τις υπάρχουσες μορφές πρόσβασης στο δίκτυο. Ενδεικτικά, ορισμένες εξ αυτών θα μπορούσαν να είναι:

- Εσωτερικά συστήματα
- Πρόσβαση από υποκαταστήματα, θυγατρικές εταιρείες, ή απομακρυσμένα γραφεία
- Πρόσβαση ενός επαγγελματικού συνεργάτη μέσω μιας σύνδεσης WAN
- Πρόσβαση μέσω του Internet
- Πρόσβαση μέσω δεξαμενών μόντεμ (modem pools)

Να έχετε υπόψη ότι στο στάδιο αυτό δεν προσπαθείτε να εντοπίσετε ποιος μπορεί να θέλει να επιτεθεί στο δίκτυο σας. Αυτό που εξετάζετε είναι ποια είναι τα διαθέσιμα μέσα με τα οποία θα μπορούσε κανείς να αποκτήσει πρόσβαση στους πόρους του δικτύου σας.

Ποιος θα ήθελε να παραβιάσει το δίκτυο μας;

Παραπάνω εξετάσαμε σε θεωρητικό επίπεδο ποιοι θα μπορούσαν να έχουν λόγους για να επιτεθούν στο δίκτυο σας. Όπως ήδη αναφέραμε, πιθανές απειλές θα μπορούσαν να θεωρηθούν οι ακόλουθες:

- Οι μόνιμοι υπάλληλοι του οργανισμού
- Προσωρινοί υπάλληλοι ή συνεργάτες
- Ανταγωνιστές
- Άτομα με απόψεις ή στόχους ριζικά διαφορετικούς από αυτούς του οργανισμού σας
- Άτομα τα οποία έχουν εκδικητική διάθεση έναντι του οργανισμού σας ή συγκεκριμένων υπαλλήλων του
- Άτομα τα οποία επιθυμούν να αποκτήσουν φήμη μέσω της δημόσιας αναγνώρισης του οργανισμού σας

Ανάλογα με τον οργανισμό στον οποίο εργάζεστε, μπορεί να υπάρχουν και άλλες πιθανές απειλές τις οποίες θα πρέπει να προσθέσετε στην παραπάνω λίστα. Δύο είναι τα σημαντικά στοιχεία σ' αυτή την προσπάθεια: να προσδιορίσετε τι έχει να κερδίσει κάποιος εξαπολύοντας μία επιτυχημένη επίθεση στο δίκτυο του οργανισμού σας, και τι μπορεί να αξίζει αυτή η επίθεση για έναν πιθανό εισβολέα.

Πόσες πιθανότητες έχω να δεχτώ επίθεση;

Τώρα που έχετε προσδιορίσει τους πόρους του οργανισμού σας και τις πηγές από τις οποίες μπορούν να προέλθουν επιθέσεις, μπορείτε να εκτιμήσετε το επίπεδο κινδύνου του οργανισμού σας έναντι τέτοιων επιθέσεων. Τι διάταξη έχει το δίκτυο του οργανισμού σας; Είναι εντελώς απομονωμένο, ή έχει πολλά σημεία εισόδου - όπως για παράδειγμα σύνδεση μέσω WAN, δεξαμενή μόντεμ, ή ένα δίκτυο VPN για την διακίνηση πληροφοριών μέσω Internet; Χρησιμοποιείτε για όλα αυτά τα σημεία σύνδεσης ένα ισχυρό σχήμα πιστοποίησης και κάποιο σύστημα προστασίας (firewall); Θα μπορούσε το δίκτυο σας να είναι στόχος για ένα πιθανό εισβολέα; Σαφώς, ένας τέτοιος εισβολέας θα προτιμούσε να εξαπολύσει την επίθεση του σε μία τράπεζα, παρά σε ένα μικρό γραφείο.

Η εκτίμηση της πιθανότητας να δεχθεί επίθεση το δίκτυο σας είναι πολύ υποκειμενική. Δύο διαφορετικοί εργαζόμενοι στον ίδιο οργανισμό θα μπορούσαν να έχουν εντελώς διαφορετική άποψη όσον αφορά στην πιθανότητα επιθέσεων που μπορεί να δεχτεί το δίκτυο τους. Για τον λόγο αυτό καλό θα είναι να ζητήσετε την γνώμη πολλών διαφορετικών τμημάτων του οργανισμού σας σ' αυτό το θέμα. Θα μπορούσατε επίσης να συνεργαστείτε με έναν εξειδικευμένο σύμβουλο ο οποίος έχει πρακτική εμπειρία στην ανάλυση και αξιολόγηση κινδύνων.

Ποιο είναι το άμεσο κόστος;

Για κάθε πόρο που αναφέραμε παραπάνω, θα πρέπει να καταγράψετε την άμεση επίδραση που θα είχε η παραβίαση ή η καταστροφή του σε κόστος. Για παράδειγμα, τι γίνεται εάν η παραβίαση του δικτύου σας επιτρέψει σε έναν ανταγωνιστή να αποκτήσει πρόσβαση σε όλα τα πρωτότυπα σχέδια της νέας σειράς προϊόντων της εταιρείας σας; Αυτό θα έδινε στον ανταγωνιστή σας την δυνατότητα να αναπτύξει ένα καλύτερο προϊόν και να σας προλάβει στην αγορά. Ακόμη πιο δύσκολο να μετρηθεί - αλλά εξίσου υπαρκτή - είναι η απώλεια της εμπιστοσύνης των καταναλωτών, ή η δυσφήμιση σας, που μπορούν να επηρεάσουν πολύ αρνητικά την πορεία της εταιρείας σας.

Ωστόσο, σε ορισμένες περιπτώσεις ο κύριος συντελεστής για τον προσδιορισμό των απωλειών δεν είναι το χρηματικό κόστος. Για παράδειγμα, αν και ένα νοσοκομείο μπορεί να αντιμετωπίσει οικονομικές απώλειες εάν ένας εισβολέας παραβιάσει τις ιατρικές του εγγραφές, η καταστροφή αυτών των εγγραφών θα μπορούσε να συνεπάγεται ακόμη και απώλεια ζωών - κάτι πολύ πιο καταστροφικό. Κατά τον προσδιορισμό του άμεσου κόστους μιας απώλειας θα πρέπει να εξετάζετε οποιαδήποτε μορφή απώλειας - όχι μόνο τα χρήματα.

Ποιο είναι το μακροπρόθεσμο κόστος;

Θα πρέπει επίσης να εκτιμήσετε το κόστος που συνεπάγεται η πλήρης ανάκαμψη του συστήματος από μία βλάβη ή επίθεση. Για τον σκοπό αυτό θα πρέπει να προσδιοριστούν οι οικονομικές επιπτώσεις που συνεπάγονται διάφορες μορφές απωλειών. Βασιζόμενοι σ' αυτά τα στοιχεία μπορείτε να προσδιορίσετε - μέσα σε λογικά πλαίσια - την οικονομική επένδυση που θα πρέπει να γίνει για την διασφάλιση των πόρων του δικτύου σας. Να θυμάστε επίσης ότι ορισμένοι πόροι (όπως για παράδειγμα η φήμη του οργανισμού σας ή η εμπιστοσύνη των καταναλωτών και των επενδυτών) είναι δύσκολο να ποσοτικόποιηθούν, αν και είναι εξίσου υπαρκτοί με τους υπόλοιπους.

Πώς μπορώ να προστατέψω αποτελεσματικά σε σχέση με το κόστος τους πόρους μου;

Θα πρέπει να σκεφτείτε πόσο θα σας κοστίσει η ασφάλεια, όταν καθορίζετε το επίπεδο της προστασίας που είναι κατάλληλο για το δικό σας περιβάλλον δικτύου.

Για την ασφάλιση ενός περιβάλλοντος δικτύου μπορεί επίσης να υπάρχουν κόστη τα οποία δεν είναι άμεσα εμφανή αλλά πρέπει να συνυπολογιστούν, όπως π.χ. η απασχόληση ενός στελέχους, ανάλογα με το μέγεθος του δικτύου σας. Αυξάνοντας το

επίπεδο της λεπτομέρειας που καταγράφεται για τις δραστηριότητες του δικτύου σας ίσως δημιουργήσετε την ανάγκη πρόσληψης ενός επιπλέον στελέχους ειδικά για την ασφάλειά του.
Επίσης, η αυξημένη ασφάλεια συνεπάγεται σε πολλές περιπτώσεις την μείωση της ευκολίας χρήσης ή πρόσβασης στους πόρους του δικτύου, πράγμα το οποίο μπορεί να καταστήσει πιο κουραστική ή χρονοβόρα την εκτέλεση των εργασιών των τελικών χρηστών. Αυτό δεν σημαίνει ότι θα πρέπει να αποφεύγετε με κάθε κόστος αυτή την μείωση ευχρηστίας· μπορεί να είναι αναγκαίο κακό για την ασφάλιση ενός περιβάλλοντος, και πρέπει να καταγραφεί σαν πιθανό κόστος λόγω μειωμένης παραγωγικότας.

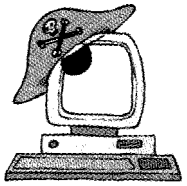
4.4. Κατάρτιση του προϋπολογισμού για τα μέτρα ασφάλειας

Στο σημείο που βρίσκεστε τώρα θα πρέπει να έχετε σχηματίσει μία πολύ καλή άποψη σχετικά με το επίπεδο ασφάλειας του οποίου το κόστος θα κληθείτε να αιτιολογήσετε. Σ' αυτό θα πρέπει να συμπεριλάβετε τις αποσβέσεις των παγίων (ο εξοπλισμός του server, τα συστήματα firewall και η κατασκευή ασφαλών περιοχών μέσα στις εγκαταστάσεις της εταιρείας), καθώς επίσης και οποιοδήποτε περιοδικό κόστος (μισθοδοσία του προσωπικού ασφάλειας, τακτικοί έλεγχοι και συντήρηση του συστήματος).

Όσο περισσότερο μπορείτε να διευρύνετε τον προϋπολογισμό σας, τόσο περισσότερα μέτρα ασφάλειας θα μπορείτε να λάβετε. Η ασφάλεια είναι ένα προληπτικό έξοδο - δηλαδή ζητάτε από τους ιθύνοντες του οργανισμού σας να επενδύσουν χρήματα σε μέτρα και διαδικασίες οι οποίες, εάν όλα πάνε κατ' ευχήν, θα αποδώσουν μόνο και μόνο επειδή δεν θα χρειαστεί να ξοδέψετε περισσότερα χρήματα μελλοντικά για να ανακάμψετε από μία καταστροφή, Όσα περισσότερα μέτρα προφύλαξης μπορείτε να λάβετε, τόσο περισσότερο μειώνετε τις πιθανότητες καταστροφών.

Κεφάλαιο 5

Επιθέσεις στην ασφάλεια του δικτύου



Το πρώτο σημαντικό περιστατικό ασφάλειας παρουσιάστηκε στο διαδίκτυο τα 1988. Ονομάστηκε Morris worm, από το όνομα του φοιτητή του Cornell University, Robert Morris, που έγραψε ένα πρόγραμμα που μπορούσε να συνδεθεί σε έναν άλλο υπολογιστή, να αντιγραφεί σε αυτόν και να αρχίσει να κάνει το ίδιο με τον επόμενο υπολογιστή στο δίκτυο. Αυτό το αυτόματα αναπαραγόμενο πρόγραμμα προκάλεσε μία γεωμετρική έκρηξη επιθέσεων στο διαδίκτυο. Το πρόγραμμα χρησιμοποιούσε τόσους πολλούς πόρους από τα σύστημα που βρισκόταν, ώστε τελικά έπαυε να είναι λειτουργικό. Το αποτέλεσμα ήταν το 10% των υπολογιστών που ήταν συνδεμένοι στο ARPANET (σε σύνολο 88,000) να σταματήσουν την λειτουργία τους την ίδια ώρα. Το δίκτυο που θα μπορούσε να ήταν τα μέσο που θα βοηθούσε στην επίλυση του προβλήματος, είχε πάψει να είναι λειτουργικό. Επιπλέον οι διαχειριστές πολλών sites από φόβο μήπως "μολυνθούν» τα συστήματά τους, σταματούσαν την επικοινωνία τους με τα δίκτυο για να αντιμετωπίσουν την κατάσταση, με αποτέλεσμα να γίνονται περισσότεροι οι κόμβοι που δεν ήταν συνδεμένοι.

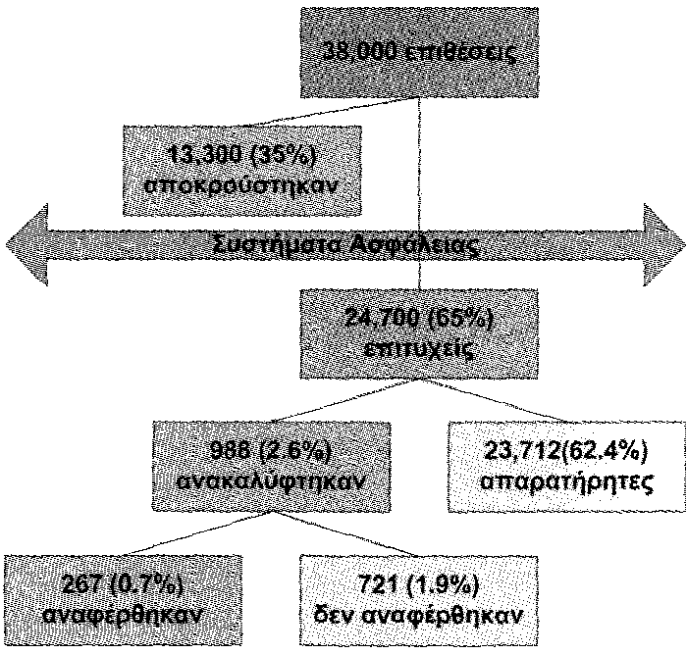
Ήταν τόσο μεγάλη η αίσθηση που προκάλεσε τα Morris worm, που το Υπουργείο Άμυνας αποφάσισε την χρηματαδότηση μίας ομάδας άμεσης αντίδρασης σε προβλήματα ασφάλειας, που τώρα ονομάζεται CERT Coordination Center. Το CERT/CC πρόκειται για ένα καλά οργανωμένα ινστιτούτα ασφάλειας στο διαδίκτυο που παρέχει ενημέρωση, τεχνική υποστήριξη και κάλυψη γενικότερα σε χρήστες του διαδικτύου. Διαθέτει βάσεις

δεδομένων με τα περισσότερα περιστατικά επιθέσεων στο διαδίκτυο, ομάδες εκπαίδευσης και ανάπτυξης λογισμικού και γενικότερα τεχνικών θωράκισης του διαδικτύου και των δικτύων γενικότερα.

Υπάρχουν και άλλοι οργανισμοί και ινστιτούτα όπως τα CERT/CC, μικρότερης όμως εμβέλειας. Στα σύνολό τους αποτελούν το FIRST (Forum of Incident Response and Security Teams), μια μορφή κοινότητας που παρακολουθεί και επινοεί τρόπους άμυνας απέναντι σε επιθέσεις στο διαδίκτυο. Το FIRST αριθμούσε τα 1996, τα 57 μέλη με δράση στον κυβερνητικό, εμπορικό και ακαδημαϊκό τομέα και με σημαντική συμβολή στην ασφάλεια του διαδικτύου.

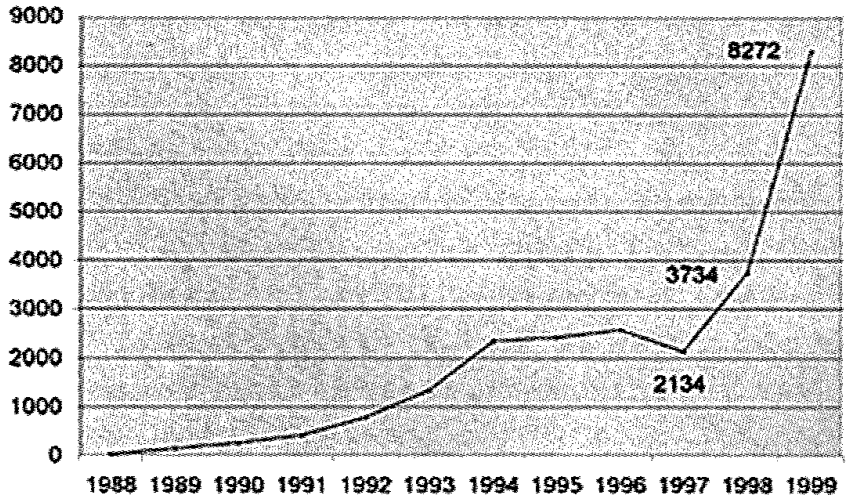
5.1. Επεισόδιο επιθέσεων σε σχέση με την ανάπτυξη του Internet

Για τον έλεγχο της τρωτότητας σε συστήματα, έχουν γίνει πολλές προσπάθειες οι περισσότερες με χρηματοδότηση του υπουργείου άμυνας των ΗΠΑ, με στόχο κόμβους στρατιωτικών υπηρεσιών και υπηρεσιών ασφάλειας. Σε μια τέτοια έρευνα επιστήμονες της DISA (Defense Information Systems Agency) έκαναν επιθέσεις σε υπολογιστές στρατιωτικών υπηρεσιών στο διάστημα από το 1992 ως το 1995. Τα αποτελέσματά της φαίνονται στο Σχήμα 5-1.



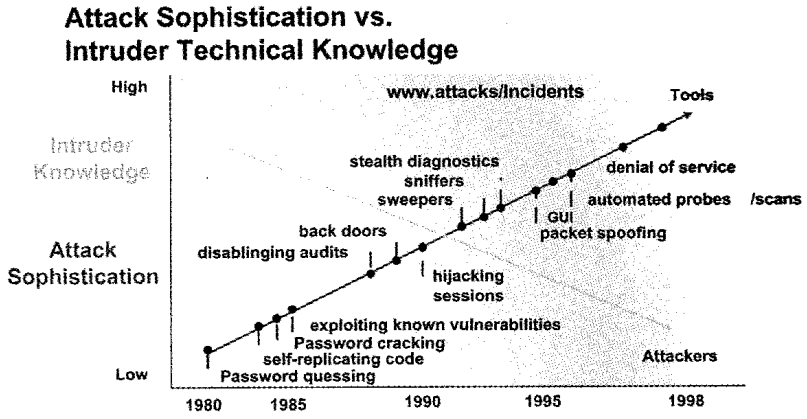
Σχήμα 5-1. Αποτελέσματα επιθέσεων DISA

Σύμφωνα με εκτιμήσεις της DISA τα συστήματα του Υπουργείου Άμυνας, πρέπει να έχουν δεχθεί 250,000 επιθέσεις από το 1992-1995. Υποθέτοντας πως τα συστήματα αυτά αποτελούν το 10% του συνόλου του διαδικτύου εκτιμούν πως 2.5 εκατομμύρια επιθέσεις έγιναν στο διαδίκτυο μόνο το διάστημα 1992-1995. Επίσης συμπεράνουν πως 1 στις 140 επιθέσεις ανακοινώνονται. Έτσι και από το Σχήμα 4-2, προκύπτει πως τα συνολικά περιστατικά το 1999 ήταν περίπου 11.5 εκατομμύρια.



Σχήμα 4-2. Αριθμός περιστατικών που αναφέρθηκαν

5.2. Είδη επιθέσεων και τεχνικές



Σχήμα 4-3. Η εξέλιξη των επιθέσεων σε σχέση με τις γνώσεις των εισβολέων

Επίθεση στις Ιστοσελίδες

Τα sites με σελίδες του διαδικτύου ήταν πάντα ο αγαπημένος στόχος των hackers, ίσως γιατί δεν προσφέρουν ικανοποιητική ασφάλεια και τις σελίδες τους επισκέπτονται πολλοί άνθρωποι κάθε μέρα. Η αλλαγή της κεντρικής σελίδας αυτών των sites γίνεται συνήθως για να διαβαστούν από πολλούς πολιτικά ή αντικυβερνητικά μηνύματα. Δεν είναι λίγες οι περιπτώσεις που οργανισμοί έχουν δει την φήμη τους να πληγώνεται από τέτοιες επιθέσεις. Μεγάλες εταιρίες, κυβερνητικοί οργανισμοί, στρατιωτικά προγράμματα είναι οι κύριοι στόχοι.

Επίθεση στην υπηρεσία ονοματολογίας (DNS)

Ένας άλλος τρόπος για να τροποποιηθούν οι ιστοσελίδες ενός site που βλέπουν οι χρήστες είναι να αλλάξει η IP διεύθυνση που υποτίθεται πως έχει από την υπηρεσία ονοματολογίας (Domain Name Service) ο κόμβος. Για παράδειγμα αν η IP διεύθυνση του κόμβου WWW.victim.com ήταν 66.77.222.33, θα μπορούσε να αλλάξουν τα στοιχεία της βάσης δεδομένων του DNS και να δείχνει σε ένα πορνογραφικού περιεχομένου site.

Επίθεση με Δούρειους Ίππους

Οι Δούρειοι Ίπποι (trojan horses) είναι προγράμματα που προσποιούνται ότι έχουν άλλες λειτουργίες από αυτές που πραγματικά υλοποιούν. Συνήθως κρύβονται σε άλλα προγράμματα, αλλά μπορούν να βρίσκονται και μεμονωμένα. Παράδειγμα Δούρειου Ίππου είναι ο Happy99.exe. Αυτοί αντιπροσωπεύουν ποσοστό 58% του συνόλου των Εργαλείων. Ενδεικτικά, αναφέρονται κάποια ποσοστά για Δούρειους Ίππους από έρευνα που έγινε από το CERT®/CC: login (56%), telnet (16%), ps (12%).

Επίθεση με «σκουλήκια»

Τα «σκουλήκια» (worms) είναι προγράμματα που δρουν αυτόνομα και «σέρνονται» (έτσι προκύπτει το όνομα «σκουλήκι») από site σε site εκμεταλλευόμενα τρύπες του συστήματος. Σε κάθε site το σκουλήκι δρα αυτόνομα και ανεξάρτητα από τα υπόλοιπα sites που προσπαθεί να «συρθεί». Το πιο χαρακτηριστικό σκουλήκι είναι το Internet Worm που το βράδυ της 2ας Νοεμβρίου 1988, κατάφερε να διασπάσει το Διαδίκτυο στην Αμερική, προκαλώντας αντιδράσεις πανικού σε όλο τον κόσμο.

Επίθεση με Ιούς

Οι Ιοί (viruses), τα γνωστά προγράμματα που προσπαθούν (με πονηρές και συνήθως δόλιες τεχνικές) να εγκατασταθούν σε κάποιους υπολογιστές και να προσβάλουν την ακεραιότητα του συστήματος με διάφορους τρόπους (από τους πιο ανώδυνους, αφήνοντας μία υπογραφή-ίχνος της παρουσίας τους ή πιο επώδυνους, με απώλεια δεδομένων, καταστροφή της διαμόρφωσης - configuration του συστήματος). Ένα από τα πιο έγκυρα αντι-ιοικά προγράμματα (το Symantec Norton Antivirus) στην ανανέωση του Μάιου 1999 περιείχε υπογραφές 21753 ιών.

Επίθεση με «Ανιχνευτές»

Οι ανιχνευτές (scanners) δικτυακής κίνησης είναι προγράμματα που χρησιμοποιούνται για τον έλεγχο της ασφάλειας των συστημάτων. Ονομάζονται ανιχνευτές γιατί γνωρίζουν όλα τα πιθανά εξωτερικά σημεία που θα μπορούσε να εκμεταλλευτεί ένας επίδοξος hacker για να προσβάλει την ασφάλεια του συστήματος. Αν και αρχικά δημιουργήθηκαν για χρήση από τους διαχειριστές των συστημάτων, σύντομα έγιναν εργαλεία των hackers για να βρίσκουν πιθανούς στόχους. Τέτοια προγράμματα είναι το ISS, το TCPdump, το Nmap, το SATAN και πολλά άλλα. Το ποσοστό της χρήσης τους είναι 14.3% του συνολικού των εργαλείων.

Επίθεση στο πρωτόκολλο TFTP

Το πρωτόκολλο TFTP (Trivial File Transfer Protocol) σχεδιάστηκε ως πρωτόκολλο για την χωρίς δίσκο εκκίνηση «πελατών» (diskless clients). Ωστόσο, δεν είχε δοθεί αρκετή προσοχή στην πρόσβαση σε συγκεκριμένους καταλόγους του συστήματος με αποτέλεσμα να μπορεί κανείς να αντιγράψει κι άλλα αρχεία, όπως για παράδειγμα, το αρχείο κωδικών πρόσβασης.

Επίθεση στη Δικτυακή Υπηρεσία Πληροφοριών (NIS)

Πρόκειται για την υλοποίηση της Sun Microsystems «Κίτρινων Σελίδων» (Yellow Pages) για κατανεμημένη διαχείριση δικτυακών πληροφοριών (όπως αρχεία κωδικών πρόσβασης, χάρτες του δικτύου κλπ.). Ωστόσο, οι πληροφορίες αυτές περνούσαν πάνω από το δίκτυο και μπορούσε οποιοσδήποτε να τα παρακολουθήσει και να τα υποκλέψει. Το NIS (Network Information Service) αντικαταστάθηκε από το NIS+ (από την Sun Microsystems και πάλι) το οποίο χρησιμοποιεί κρυπτογραφικές μεθόδους για την μεταφορά κάθε είδους ευαίσθητης πληροφορίας.

Επίθεση στο πρωτόκολλο μεταφοράς αρχείων (FTP)

Τα προβλήματα με το FTP (File Transfer Protocol) μπορούν να συνδυαστούν με αυτά του TFTP, των αδυνάτων κωδικών κλπ. Μέσω του FTP και μιας λανθασμένης διαμόρφωσης μπορεί κάποιος να υποκλέψει αρχεία του συστήματος.

Επίθεση στο Σύστημα Δικτυακής Αρχειοθέτησης (NFS)

Το NFS (Network File System) αποτελεί πρωτοποριακή υλοποίηση από την Sun Microsystems (χρησιμοποιήθηκε από όλους τους κατασκευαστές συστημάτων Unix και από τα Windows NT). Ωστόσο, με λάθος διαμόρφωση, μπορεί να «μοιράσει» ένα σύστημα αρχείων (file system) σε κακόβουλους χρήστες.

Επίθεση στο πρωτόκολλο ηλεκτρονικού ταχυδρομείου (SMTP)

Το πρωτόκολλο SMTP (SimpleMail Transfer Protocol) πρόκειται για το TCP/IP πρωτόκολλο επικοινωνίας των MTA (Mail Transfer Agents) της υπηρεσίας του ηλεκτρονικού ταχυδρομείου. Το κυριότερο πρόγραμμα που χρησιμοποιείται και αποτελεί πηγή του προβλήματος (10.4%) είναι το sendmail (σε Berkeley UNIX συστήματα). Πιο πρόσφατα, νέα προγράμματα με μεγαλύτερη ασφάλεια έχουν εμφανιστεί, τόσο για πλατφόρμες UNIX (π.χ. qmail) όσο και για πλατφόρμες Windows (Exchange Server).

Επίθεση στο ηλεκτρονικό ταχυδρομείο

Στην κατηγορία αυτή εμπίπτουν προβλήματα που προκύπτουν από την προβληματική χρήση του SMTP. Τέτοια είναι το mail spoofing (απόκρυψη αποστολέα ή αλλαγή διεύθυνσής του), mail bombs (μεγάλος όγκος μηνυμάτων σε συγκεκριμένο παραλήπτη), binmail, mailrace, mail abuse. Μία πιο πρόσφατη τρωτότητα που μπορεί να κατηγοριοποιηθεί κάτω από τον ευρύτερο όρο "mail" είναι και το spamming, η παράνομη χρήση mail relays για την αποστολή μηνυμάτων ακατάλληλου ή αδιάφορου περιεχομένου, σε ένα μεγάλο αριθμό χρηστών.

Επίθεση με «έμπιστους υπολογιστές»

Η υπηρεσία των «έμπιστων υπολογιστών» (trusted hosts) δημιουργήθηκε αρχικά για την ευκολία των χρηστών που είχαν πολλούς λογαριασμούς σε συστήματα και χρειάζονταν άμεση πρόσβαση χωρίς την καθυστέρηση για ταυτοποίηση μέσω κωδικών πρόσβασης. Το πρόβλημα αυτό παρουσιάζεται σε UNIX συστήματα και συγκεκριμένα στα αρχεία hosts.equiv (πλήρης πρόσβαση από άλλα συστήματα) και .rhosts (πρόσβαση σε λογαριασμό χρήστη που ορίζεται από τον ίδιο το χρήστη).

Επίθεση μέσω διαμόρφωσης (weak configuration)

Επιθέσεις που έχουν καταγραφεί σε αυτή τη κατηγορία οφείλονται σε λάθη και παραλείψεις στη διαμόρφωση του συστήματος και κυρίως στη δικτυακή διαμόρφωση. Σε αυτές τις περιπτώσεις παραμένουν τα αρχικά συνθηματικά (passwords) που δημιουργούνται κατά την εγκατάσταση ενός λογισμικού ή συστήματος και ο διαχειριστής

δεν τα αλλάζει. Επίσης μπορεί να παραμείνουν τα αρχικά δικαιώματα προσπέλασης που δεν είναι κατά ανάγκη ασφαλή.

Επίθεση από εύρεση των κωδικών πρόσβασης

Η τρωτότητα των κωδικών πρόσβασης (password vulnerabilities) είναι η πιο συχνή μορφή παραβίασης της πρόσβασης (ποσοστό 22%). Η εύρεση του κωδικού πρόσβασης ενός χρήστη μπορεί να γίνει με αρκετούς τρόπους: (ί) ανπγραφή του αρχείου κωδικών (password file) και μετέπειτα επεξεργασία αυτού (14%), (ίί) «σπάσιμο» κωδικών πρόσβασης (password cracking) με χρήση προγραμμάτων που προσπαθούν να μαντέψουν passwords κωδικοποιώντας συνήθεις λέξεις (10%), (ίίί) «αδύνατοι κωδικοί» (weak passwords) που μπορεί εύκολα να βρει κανείς γνωρίζοντας το πρόσωπο στο οποίο ανήκει ο λογαριασμός (χρήση του ονόματος, διεύθυνσης, Τηλεφώνου κλπ.) (4%).

Επίθεση με «σπαστήρια» κωδικών

Τα «σπαστήρια κωδικών» (password cracks) είναι προγράμματα τα οποία με είσοδο ένα αρχείο κωδικών πρόσβασης (password file) και με χρήση ενός λεξικού συνηθισμένων λέξεων που χρησιμοποιούνται για κωδικοί, προσπαθούν να ανακαλύψουν όσο το δυνατό περισσότερους κωδικούς για πρόσβαση σε κάποιο σύστημα. Ενδεικτικά αναφέρεται ότι σε ένα UNIX σύστημα 1000 περίπου χρηστών, και υποθέτοντας ότι οι χρήστες δεν έχουν συμβουλευτεί να επιλέγουν δύσκολους κωδικούς (συνήθως συνδυασμό γραμμάτων, αριθμών και σημείων στίξης), ένα «σπαστήρι» μπορεί να ανακαλύψει εύκολα ένα ποσοστό 40% των συνολικών κωδικών. Τα προγράμματα αυτά χρησιμοποιούν και οι διαχειριστές συστημάτων για να προλάβουν παρόμοιες ενέργειες από hackers.

Επίθεση με «ωτακουστές»

Οι «Ωτακουστές» πακέτων (packet sniffers) είναι προγράμματα που μπορούν να παρακολουθούν («ακούν», ή «μυρίζουν» - sniff) την κίνηση του δικτύου σε επίπεδο IP πακέτων. Με κατάλληλες τεχνικές, έχουν τη δυνατότητα να ανακατασκευάσουν τα μηνύματα και να κάνουν αναγνώριση των πρωτοκόλλων που περνούν πάνω από το δίκτυο. Οι sniffers τρέχουν συνήθως σε τοπικά δίκτυα (Ethernet) και «κλέβουν» κωδικούς πρόσβασης ή παρακολουθούν τις πληκτρολογήσεις από συγκεκριμένους σταθμούς εργασίας. Με κατάλληλους μηχανισμούς ανασυνθέτουν τα πακέτα που μπορεί να έχουν χρήσιμη πληροφορία (κωδικούς πρόσβασης, αρχεία, κλπ.) χωρίς όμως να επηρεάζουν το περιεχόμενό τους (ανάγνωση μόνο). Τα γεγονότα που αφορούν sniffers ανταποκρίνονται σε ένα ποσοστό 31 % του συνόλου των εργαλείων. Ο τρόπος επίθεσης με αυτούς δείχνει μία κλιμάκωση στον τρόπο δράσης: ξεκινά από απλή ανίχνευση του στόχου κι αφού εντοπίσει παραλείψεις στην ασφάλεια, εισβάλλει, σβήνει τα ίχνη, αποδυναμώνει την άμυνα του συστήματος (NIS, FTP, sendmail) και εγκαθιστά Trojans για την εξάπλωσή του.

Η χρήση των sniffers αν και μπορεί να έχει θετικά αποτελέσματα για την διαχείριση δικτύου και υπολογιστικών συστημάτων (εντοπισμός bottlenecks, άχρηστης πληροφορίας που μεταδίδεται κλπ.) στα χέρια των hackers μπορεί να έχει καταστροφικά αποτελέσματα. Η χρήση ενός sniffer απαιτεί προνόμια διαχειριστή (superuser privileges), αλλά σήμερα, ο καθένας είναι «διαχειριστής» του προσωπικού του συστήματος και μάλιστα με σύνδεση στο διαδίκτυο. Για τον λόγο αυτό, η ασφάλεια από τα sniffers θα πρέπει να εξασφαλίζεται στο επίπεδο παρόχου υπηρεσιών δικτύου (ISP).

Επίθεση με πλαστογράφηση της IP διεύθυνσης

Η τεχνική αυτή βασίζεται στη δυνατότητα την οποία μπορεί να έχει ένας κόμβος να ισχυρίζεται πως έχει την IP διεύθυνση ενός άλλου. Από την στιγμή που πολλά συστήματα (όπως για παράδειγμα οι access lists σε δρομολογητές) ορίζουν ποια πακέτα επιτρέπονται και ποια όχι να εισέλθουν σε ένα δίκτυο ανάλογα με την IP διεύθυνση του αποστολέα, αυτή είναι μία χρήσιμη τεχνική σε έναν hacker. Με τον τρόπο αυτό είναι δυνατό να διασφαλίσει την προσπέλαση σε υπηρεσίες που επιτρέπονται σε κόμβους με συγκεκριμένες IP διευθύνσεις. Επίσης μπορεί να σταλεί από ένα εξωτερικό δίκτυο ένα πακέτο δεδομένων που να φαίνεται πως έχει σταλεί από εσωτερικό κόμβο ενός προφυλαγμένου δικτύου, δίνοντας έτσι την δυνατότητα να εκτελεστούν εντολές, που επιτρέπονται να εκτελεστούν μόνο από εσωτερικούς κόμβους.

Η πλαστογράφηση της IP διεύθυνσης (IP spoofing) είναι μία νέα (σχετικά) τεχνική επίθεσης σε δικτυωμένους υπολογιστές. Αν και η πιθανότητα τέτοιας επίθεσης είχε προβλεφθεί από το 1989 από τον Steve Bellovin, μόνο από τις αρχές του 1995 άρχισε να χρησιμοποιείται από τους hackers.

Προκειμένου να αποκτήσουν πρόσβαση, οι εισβολείς δημιουργούν πακέτα με ψεύτικες IP διευθύνσεις. Αυτό εκμεταλλεύεται τις εφαρμογές που χρησιμοποιούν ταυτοποίηση (authentication) που βασίζεται στην IP διεύθυνση του αποστολέα και μπορεί να οδηγήσει ακόμα και στην απόκτηση πρόσβασης διαχειριστή στο σύστημα στόχο (για παράδειγμα στις περιπτώσεις χρήσης του /etc/hosts.equiv ή .rhosts). Οι επιθέσεις αυτές μπορούν να αποτραπούν από firewalls που ελέγχουν τις διευθύνσεις πριν μπουν στο τοπικό, έμπιστο (trusted) δίκτυο.

Οι επιθέσεις τύπου "IP spoofing" είναι γενικά δύσκολο να εντοπιστούν, αφού η πρώτη εντύπωση είναι ότι η επίθεση έχει προέλθει από την πλαστή διεύθυνση. Η επαλήθευση συνήθως αργεί, επιτρέποντας στον hacker να δρα ανενόχλητος για κάποιο διάστημα. Η πιο επαρκής «θεραπεία» είναι η χρήση δρομολογητών που έχουν κατάλληλα διαμορφωθεί ώστε να αποτρέπουν είσοδο πακέτων από το εξωτερικό interface με εσωτερικές διευθύνσεις του δικτύου του (δρώντας ως φίλτρο εισόδου).

Επίθεση με «πειρατεία» IP σύνδεσης

Πρόκειται για μία σχετικά σύνθετη επίθεση που περιγράφτηκε πρώτα από τον Steve Bellovin. Με αυτή την επίθεση ένας hacker μπορεί να καταλάβει την σύνδεση ενός χρήστη με έναν εξυπηρετητή (γνωστή και σαν man in the middle) και να εκτελεί εντολές που έχει δικαίωμα ο χρήστης. Επιπλέον μπορεί να βλέπει τι γράφει ο χρήστης. Για παράδειγμα αν ο χρήστης γράφει ένα mail τότε ο hacker μπορεί να διαβάσει το mail του, ενώ αν στέλνει στοιχεία της πιστωτικής του κάρτας μπορεί να τα δει.

Αρχική Αντιμετώπιση: Με την δημιουργία κωδικοποιημένης σύνδεσης του χρήοτη με τον εξυπηρετητή, μπορούμε να εμποδίσουμε το διάβασμα των στοιχείων, δεδομένων ή εντολών καθώς και την χρήση της σύνδεσης από τον hacker που μη έχοντας το κλειδί κρυπτογράφησης του χρήστη βλέπει μόνο «σκουπίδια».

Επίθεση με παραποίηση IP διεύθυνσης

Πρόκειται για ένα είδος επίθεσης που πρωτοεμφανίστηκε στις αρχές του 1998. Βασίζεται στο IP spoofing, ενώ εκμεταλλεύεται και αδυναμίες της υλοποίησης των IP και ICMP (Internet Control MessageProtocol) πρωτοκόλλων σε δικτυακές συσκευές.

Το smurf είναι ένα πρόγραμμα, το οποίο προσποιείται ότι στέλνει πακέτα από άσχετο αποστολέα (εδώ χρησιμοποιούνται οι τεχνικές του IP spoofing). Τα πακέτα αυτά είναι του πρωτοκόλλου ICMP, το οποίο και χρησιμοποιείται από βασικές λειτουργίες του δικτύου (π.χ. τις υπηρεσίες ping και traceroute). Στέλνοντας ένα ping πακέτο στην διεύθυνση εκπομπής (broadcast address) ενός δικτύου, ο αποστολέας δέχεται απάντηση από κάθε

έναν από τους κόμβους που δέχθηκαν το ICMP ping πακέτο (δηλαδή όλους του κόμβους του δικτύου).

Αν και το ping πακέτο δεν είναι μεγάλο σε μέγεθος, εντούτοις ο παράγοντας της ενίσχυση είναι ίσος με τον αριθμό των μηχανημάτων. Σε ένα μεγάλο B-class δίκτυο όπου λ.χ. χρησιμοποιείται το ένα τέταρτο του πεδίου διευθύνσεων, η απάντηση είναι ίση με περίπου 16.000 πακέτα. Είναι προφανές ότι με μερικές εκατοντάδες πακέτα ping μπορούν να κάνουν άχρηστο το δίκτυο, δημιουργώντας μία κατάσταση άρνησης εξυπηρέτησης (Denial-of Service).

Επίθεση με υπερχείλιση προσωρινής μνήμης

Μερικές φορές οι hackers εισβάλουν σε συστήματα χωρίς να χρειάζεται να κάνουν login σε αυτά. Αντίθετα χρησιμοποιούν ένα πρόγραμμα που ήδη υπάρχει στον υπολογιστή και τρέχει στο σύστημα και του δίνουν να εκτελέσει ένα κομμάτι εντολών. Για να το πετύχουν αυτό φτιάχνουν ένα μεγάλο τμήμα από χαρακτήρες που περιέχει τις εντολές που θέλουν να εκτελεστούν, και το εισάγουν σαν παράμετρο εισόδου στο πρόγραμμα. Κανονικά το πρόγραμμα δεν εκτελεί τον κώδικα που περνά σαν παράμετρος. Αν όμως το μήκος του κειμένου της παραμέτρου είναι μεγαλύτερο από το μήκος που έχει δοθεί σαν χώρος (buffer) για το πέρασμα της παραμέτρου, τότε μέρος του περνά στον χώρο του εκτελέσιμου προγράμματος και εκτελείται (Buffer overflow).

Αν λοιπόν μία διεργασία του συστήματος τρέχει με προνόμια διαχειριστή και καταφέρει ο hacker να περάσει με παράμετρο τον κώδικά του, τότε θα μπορέσει να εκτελέσει εντολές που θα του δώσουν διάφορα προνόμια (root access).

Επίθεση μέσω άρνησης παροχής υπηρεσιών (DoS)

Οι επιθέσεις αυτού του τύπου είναι οι πιο μοχθηρές και πιο δύσκολο να αντιμετωπισθούν. Είναι οι πιο μοχθηρές γιατί είναι εύκολο να γίνουν, δύσκολο (μερικές φορές αδύνατο) να εντοπισθούν και το χειρότερο δεν μπορείς να αρνηθείς την υπηρεσία στον επιτιθέμενο χωρίς να κάνεις το ίδιο στις γνήσιες αιτήσεις για την υπηρεσία, από κανονικούς χρήστες.

Η μεθοδολογία της DoS (Denial of Service) επίθεσης είναι απλή: αν σταλούν σε έναν εξυπηρετητή, περισσότερες αιτήσεις από όσες μπορεί να εξυπηρετήσει τότε οι λειτουργίες που επιβάλλουν οι αιτήσεις αυτές, δεσμεύουν πόρους του συστήματος με αποτέλεσμα, μετά από κάποιο σύντομο χρονικό διάστημα, το σύστημα να μην είναι σε θέση να εξυπηρετήσει τους χρήστες και να μη μπορεί να παρέχει αρκετούς πόρους για την εκτέλεση διεργασιών. Παράδειγμα αποτελεί το mail spam, η επαναλαμβανόμενη δηλαδή αποστολή μηνυμάτων προκειμένου να φτάσει το σύστημα στα όρια της χωρητικότητάς του.

Αρχική Αντιμετώπιση: Χρήση packet filtering για την αποτροπή **IP** spoofed πακέτων να εισέλθουν στο σύστημα. Το σύστημα δεν πρέπει να τρέχει στα όρια των δυνατοτήτων του και έχει εγκατεστημένα τα τελευταία security patches.

Η ριζική αντιμετώπιση της επιθέσεως αυτής οδηγεί στην επίλυση του προβλήματος του 'IP traceback", δηλαδή στην γρήγορη ανίχνευση της πηγής της επίθεσης μέσα από την ανάλυση των πακέτων των αιτήσεων. Το πρόβλημα της ανίχνευσης της πηγής επιθέσεων είναι σήμερα ένα σημαντικό ζήτημα σύγχρονης έρευνας.

Κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS)

Η μεθοδολογία αυτού του είδους της επίθεσης είναι ίδια με την μεθοδολογία στο Denial of Service, με μόνη διαφορά την συνδυασμένη προσπάθεια προσβολής σε ένα κόμβο από πολλούς διαφορετικούς επιτιθέμενους. Το είδος αυτό των επιθέσεων έχει σαν στόχο να ξεγελάσει τα συστήματα που παρακολουθούν το δίκτυο για επιθέσεις. Τα

εργαλεία που χρησιμοποιούνται είναι εξειδικευμένα και έχουν αποδείξει πως τα Intrusion Detection Systems δεν τα καταφέρνουν καλά σε αυτές τις επιθέσεις. Χαρακτηριστικό παράδειγμα οι επιθέσεις στο Yahoo, e-Bay, Amazon, e-Trade που έγιναν το καλοκαίρι του 2000.

Επίθεση με «μοχθηρό κώδικα» (Malicious Code)

Πρόκειται για εντολές οι οποίες δείχνουν να ξεκινούν διαδικασίες χρηστών, αλλά στην πραγματικότητα προσπαθούν να μαζέψουν ή να εκμεταλλευτούν ευαίσθητα δεδομένα (password files). Για παράδειγμα στην κατηγορία αυτή μπορούν να ενταχθούν οι προσπάθειες για σύνδεση μέσω του προγράμματος login, μέσω συνδέσεων http και telnet.

Επίθεση με εκμετάλλευση κοινωνικών σχέσεων

Οι hackers πολλές φορές προσπαθούν να βρουν στοιχεία που θα τους επιτρέψουν να εισβάλουν στο σύστημα χρησιμοποιώντας τις κοινωνικές σχέσεις και παριστάνοντας πως είναι κάποιοι άλλοι (Social Engineering). Αυτό το είδος της αναζήτησης πληροφοριών μπορεί να γίνει σε μεγάλους οργανισμούς που οι υπάλληλοι δεν γνωρίζονται μεταξύ τους. Για παράδειγμα μπορούν να παραστήσουν πως είναι νέοι τεχνικοί ή σύμβουλοι ασφάλειας που χρειάζονται ένα password για να φτιάξουν κάτι. Υπολογίζεται πως το 20% των εισβολών προέρχεται από πληροφορίες από social engineering.

Σε μία περίπτωση έχει αναφερθεί πως ο hacker κατάφερε να πάρει πληροφορίες και Passwords, μοιράζονται leaflets σε μία εταιρία για την αλλαγή του τηλεφώνου του help desk. Μόνο που το τηλέφωνο ήταν του σπιτιού του!

Κεφάλαιο 6

Κρυπτογράφηση και Πιστοποίηση

Η ΠΙΣΤΟΠΟΙΗΣΗ ΚΑΙ Η ΚΡΥΠΤΟΓΡΑΦΗΣΗ είναι δύο "διαπλεκόμενες" τεχνολογίες οι οποίες - σε τεχνικό επίπεδο - σας βοηθούν να διασφαλίσετε ότι τα δεδομένα σας παραμένουν ασφαλή. Η πιστοποίηση (authentication) είναι η διαδικασία με την οποία διασφαλίζεται ότι οι οντότητες που βρίσκονται στα δυο άκρα μιας σύνδεσης είναι πράγματι αυτές που ισχυρίζονται ότι είναι. Αυτό δεν ισχύει μόνο για την οντότητα που προσπαθεί να προσπελάσει μία υπηρεσία (π.χ. ένας τελικός χρήστης), αλλά επίσης και για την οντότητα που παρέχει την υπηρεσία (π.χ. ένας file server ή ένα Web site). Η κρυπτογράφηση (encryption) μας βοηθά να διασφαλίσουμε ότι οι πληροφορίες που διακινούνται μέσω μιας συνόδου επικοινωνίας δεν θα παραβιαστούν. Σαν "παραβίαση" δεν θεωρείται μόνο η ανάγνωση των πληροφοριών που μεταδίδονται, αλλά και η τροποποίηση τους επίσης.

Παρά το γεγονός ότι σε ατομικό επίπεδο η πιστοποίηση και η κρυπτογράφηση έχουν συγκεκριμένες, ξεχωριστές ευθύνες για την ασφάλεια μιας συνόδου επικοινωνίας, η μέγιστη προστασία μπορεί να επιτευχθεί μόνο με τον συνδυασμό τους. Για τον λόγο αυτό, πολλά πρωτόκολλα ασφάλειας διαθέτουν προδιαγραφές τόσο για την πιστοποίηση, όσο και για την κρυπτογράφηση.

6.1. Η Ανάγκη για αυξημένη ασφάλεια

Στην δεκαετία του '70, όταν δημιουργήθηκε η έκδοση 4 του πρωτοκόλλου IP η οποία χρησιμοποιείται στο Internet, η ασφάλεια των δικτύων δεν αποτελούσε ζωτικό θέμα. Αν και η ασφάλεια των υπολογιστικών συστημάτων ήταν από τότε σημαντική, ελάχιστη προσοχή δίνονταν στο μέσο μεταφοράς που χρησιμοποιούνταν για την διακίνηση των πληροφοριών. Όταν πρωτοπαρουσιάστηκε το IP δεν διέθετε εγγενείς προδιαγραφές για την ασφάλεια. Οι προδιαγραφές του IP δεν λαμβάνουν υπόψη το γεγονός ότι μπορεί να θέλετε να προστατέψετε τα δεδομένα που μεταφέρει το IP. Το σκεπτικό αυτό άλλαξε στην έκδοση 6 του IP, αλλά απ' ότι φαίνεται δεν έχει φτάσει ακόμη η ώρα για την ευρεία αποδοχή αυτής της νέας προδιαγραφής.

Μετάδοση σε Μορφή Απλού Κειμένου

Επί του παρόντος, το IP μεταδίδει όλα τα δεδομένα σε μορφή απλού κειμένου (clear text). Αυτό σημαίνει ότι δεν γίνεται καμία προσπάθεια αναδιοργάνωσης των δεδομένων με στόχο την απόκρυψη τους από αδιάκριτα μάτια· τα δεδομένα μεταδίδονται απλώς στην αρχική τους μορφή. Αυτό ισχύει τόσο για τα καθαυτό δεδομένα, όσο και για τις πληροφορίες πιστοποίησης.

Παθητική Παρακολούθηση Απλού Κειμένου

Καταγράψαμε την σύνοδο πιστοποίησης ενός χρήστη σε έναν POP3 server χρησιμοποιώντας ένα εργαλείο ανάλυσης δικτύου (network analyzer). Ένα εργαλείο ανάλυσης δικτύου μπορεί να είναι είτε μία ειδική συσκευή, είτε λογισμικό το οποίο τρέχει σ' έναν υπολογιστή του δικτύου. Το κόστος του λογισμικού ανάλυσης δικτύου είναι μικρότερο από $1,000 για τις πλατφόρμες Windows και Mac, ενώ αντίστοιχα εργαλεία λογισμικού είναι ελεύθερα διαθέσιμα για UNIX.

Τα εργαλεία ανάλυσης δικτύου λειτουργούν σαν "παθητικές" συσκευές, πράγμα το οποίο σημαίνει ότι δεν χρειάζεται να μεταδίδουν δεδομένα στο δίκτυο για να μπορούν να παρακολουθούν την κυκλοφορία του. Αν και ορισμένα εργαλεία ανάλυσης παράγουν δική τους κυκλοφορία στο δίκτυο (συνήθως στην προσπάθεια τους να εντοπίσουν έναν σταθμό υπεύθυνο για την διαχείριση του δικτύου), αυτό δεν είναι απαραίτητο. Στην πραγματικότητα, ένα εργαλείο ανάλυσης δεν χρειάζεται καν μία έγκυρη διεύθυνση δικτύου. Αυτό σημαίνει ότι ένα εργαλείο ανάλυσης δικτύου μπορεί να παρακολουθεί το δίκτυο σας χωρίς να είστε ενήμεροι για την ύπαρξη του. Δεν έχετε κανέναν άλλο τρόπο για να ανιχνεύσετε την παρουσία του, εκτός από την φυσική εξέταση των καλωδίων και την μέτρηση των θυρών των hubs και των switches.

Ένας εισβολέας μπορεί επίσης να φορτώσει λογισμικό ανάλυσης δικτύου σε ένα σύστημα το οποίο κατάφερε να παραβιάσει. Αυτό σημαίνει ότι ο εισβολέας δεν χρειάζεται φυσική πρόσβαση στις εγκαταστάσεις σας για να παρακολουθεί την κυκλοφορία του δικτύου σας. Μπορεί απλώς να χρησιμοποιήσει έναν από τους υπάρχοντες υπολογιστές σας για να υποκλέπτει την κυκλοφορία του δικτύου σας. Για τον λόγο αυτό είναι πολύ σημαντικό να εκτελείτε τακτικούς ελέγχους στα συστήματα του δικτύου σας.

Για να μπορέσει ένα εργαλείο ανάλυσης δικτύου να παρακολουθήσει μία σύνοδο επικοινωνίας, πρέπει να συνδεθεί σε κάποιο σημείο κατά μήκος της διαδρομής που ακολουθεί αυτή η σύνοδος. Δηλαδή, θα μπορούσε να συνδεθεί σε κάποιο σημείο του δικτύου σας ανάμεσα στο σύστημα που εκκινεί την σύνοδο επικοινωνίας και στο σύστημα προορισμού. Θα μπορούσε επίσης να συνδεθεί σ' ένα από τα συστήματα που βρίσκονται στα δύο άκρα της σύνδεσης. Αυτό σημαίνει ότι ο εισβολέας δεν μπορεί να υποκλέψει την κυκλοφορία του δικτύου σας από μία απομακρυσμένη θέση, μέσω Internet. Θα πρέπει να τοποθετήσει κάποιο εργαλείο παρακολούθησης μέσα στο ίδιο το δίκτυο σας.

Πρωτόκολλα τα οποία μεταδίδουν τα δεδομένα σε μορφή απλού κειμένου

Το πρωτόκολλο POP3 δεν είναι η μοναδική υπηρεσία του IP η οποία διεξάγει την επικοινωνία σε μορφή απλού κειμένου. Σχεδόν κάθε υπηρεσία του IP η οποία δεν είναι ειδικά σχεδιασμένη ώστε να παρέχει υπηρεσίες πιστοποίησης και κρυπτογράφησης μεταδίδει τα δεδομένα σαν απλό κείμενο. Ακολουθεί μία ενδεικτική λίστα τέτοιων υπηρεσιών:

FTP Οι πληροφορίες πιστοποίησης μεταδίδονται σε μορφή απλού κειμένου.

Telnet Οι πληροφορίες πιστοποίησης μεταδίδονται σε μορφή απλού κειμένου.

SMTP Τα περιεχόμενα των μηνυμάτων ηλεκτρονικού ταχυδρομείου παραδίδονται σαν απλό κείμενο.

HTTP Τα περιεχόμενα των ιστοσελίδων και των πεδίων των ηλεκτρονικών φορμών στέλνονται σαν απλό κείμενο.

IMAP Οι πληροφορίες πιστοποίησης μεταδίδονται σε μορφή απλού κειμένου.

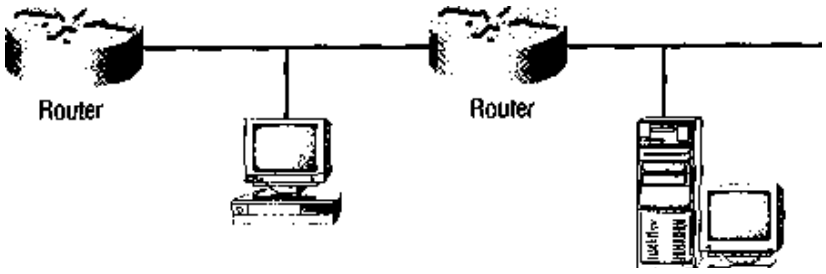
SNMP έκδοση 1 Οι πληροφορίες πιστοποίησης μεταδίδονται σε μορφή απλού κειμένου.

6.2. Η Αναγκαιότητα ενός καλού μηχανισμού πιστοποίησης

Η ανάγκη χρήσης ενός ισχυρού μηχανισμού πιστοποίησης της ταυτότητας οποιουδήποτε συνδέεται στο δίκτυο είναι μάλλον προφανής. Είναι πολύ εύκολο για τον οποιονδήποτε να παρακολουθήσει μία υπηρεσία η οποία μεταδίδει τις πληροφορίες σύνδεσης σε μορφή απλού κειμένου. Η εύκολη υποκλοπή των διαπιστευτηρίων σύνδεσης των χρηστών αποτελεί ακόμη μεγαλύτερο πρόβλημα στα περιβάλλοντα τα οποία δεν απαιτούν συχνές αλλαγές των κωδικών πρόσβασης. Αυτή η προσέγγιση δίνει σ' έναν εισβολέα άφθονο χρόνο για να εκκινήσει μία επίθεση στο δίκτυο σας, χρησιμοποιώντας τα διαπιστευτήρια ενός έγκυρου χρήστη του οποίου τον λογαριασμό κατάφερε να παραβιάσει. Ένα άλλο πρόβλημα είναι το γεγονός ότι οι περισσότεροι χρήστες προσπαθούν να έχουν το ίδιο όνομα σύνδεσης και κωδικό πρόσβασης σε όλους τους λογαριασμούς τους. Αυτό σημαίνει ότι εάν ένας εισβολέας μπορέσει να υποκλέψει τα διαπιστευτήρια ενός χρήστη από μία μη-ασφαλή υπηρεσία (π.χ. το POP3), θα έχει στην διάθεση του ένα έγκυρο όνομα σύνδεσης και κωδικό πρόσβασης για να διεισδύσει σε άλλα συστήματα του δικτύου, όπως π.χ. NT και NetWare servers. Ένας ισχυρός μηχανισμός πιστοποίησης προχωρά πέρα από την απλή επικύρωση της ταυτότητας αυτού που προσπαθεί να προσπελάσει μία υπηρεσία κατά την αρχική φάση της σύνδεσης, θα πρέπει επίσης να διασφαλίζει ότι ο υπολογιστής προέλευσης δεν αντικαθίσταται από ένα επιτιθέμενο σύστημα κατά την διάρκεια της συνόδου επικοινωνίας. Αυτή η μορφή επίθεσης αποκαλείται συνήθως "πειρατεία συνόδου" (session hijacking).

Πειρατεία Συνόδων

Εξετάστε το απλό δίκτυο που παρουσιάζεται σχηματικά στην Εικόνα 6.5. Ένας σταθμός του δικτύου επικοινωνεί με έναν server μέσω μη-ασφαλούς σύνδεσης. Ο σταθμός έχει πιστοποιηθεί ήδη στον server και του έχει παραχωρηθεί πρόσβαση. Ας υποθέσουμε ότι ο συγκεκριμένος σταθμός εργασίας έχει προνόμια ισοδύναμα με αυτά του επόπτη. Ο επίδοξος εισβολέας έχει εγκατασταθεί σ' έναν τομέα του δικτύου ανάμεσα στον συγκεκριμένο σταθμό εργασίας και στον server και παρακολουθεί σιωπηλά την σύνοδο επικοινωνίας. Ο εισβολέας έχει άφθονο χρόνο για να μάθει τον αριθμό θύρας και τον αριθμό ακολουθίας που χρησιμοποιείται για την διεξαγωγή αυτής της συνομιλίας.



ΕΙΚΟΝΑ 6.5: Ένα παράδειγμα επίθεσης από ένα σημείο ανάμεσα σε δύο επικοινωνούντα συστήματα.

Ας υποθέσουμε τώρα ότι ο επίδοξος εισβολέας αποφασίζει να εκμεταλλευτεί αυτή την σύνοδο επικοινωνίας (με προνόμια επόπτη) για να δημιουργήσει ένα νέο λογαριασμό, επίσης με τα προνόμια του επόπτη. Το πρώτο πράγμα που κάνει είναι να υποχρεώσει τον σταθμό να μεταβεί σε μία κατάσταση στην οποία δεν μπορεί να επικοινωνήσει πλέον με τον server. Ο εισβολέας μπορεί να προκαλέσει την κατάρρευση του σταθμού στέλνοντας του ένα "ping του θανάτου", ή χρησιμοποιώντας ένα εργαλείο όπως το WinNuke. Μπορεί επίσης να το πετύχει εκκινώντας μία άλλη μορφή επίθεσης, όπως ο κατακλυσμός πακέτων ICMP. Ανεξάρτητα από το είδος της επίθεσης που θα εκκινήσει ο επίδοξος εισβολέας, ο στόχος του είναι να διασφαλίσει ότι ο σταθμός του δικτύου δεν θα μπορεί να ανταποκριθεί στην κυκλοφορία που του στέλνει ο server.

Τώρα που έχει βγάλει από την μέση τον σταθμό του δικτύου, ο επίδοξος εισβολέας είναι ελεύθερος να επικοινωνήσει με τον server σαν να ήταν ο ίδιος ο σταθμός του δικτύου. Αυτό μπορεί να το κάνει υποκλέπτοντας τις απαντήσεις του server κατά την πορεία τους προς τον σταθμό του δικτύου και χρησιμοποιώντας τις κατάλληλες πληροφορίες από αυτή. Εάν ο επίδοξος εισβολέας γνωρίζει σε βάθος το IP, μπορεί επίσης να αγνοήσει ολοκληρωτικά τις απαντήσεις του server και να μεταδώσει αριθμούς θύρας και ακολουθίας βασιζόμενος στις γνώσεις του για τις αναμενόμενες απαντήσεις από τον server. Σε κάθε περίπτωση, ο επίδοξος εισβολέας είναι πλέον σε θέση να επικοινωνεί με τον server΄ δυστυχώς όμως, ο server πιστεύει ότι συνεχίζει να επικοινωνεί με τον σταθμό εργασίας του δικτύου.

Όπως αντιλαμβάνεστε, ένας καλός μηχανισμός πιστοποίησης θα πρέπει επίσης να ελέγχει ότι η προέλευση παραμένει σταθερή καθ' όλη την διάρκεια της συνόδου επικοινωνίας και δεν έχει αντικατασταθεί από ένα διαφορετικό σύστημα. Αυτό μπορεί να γίνει υποχρεώνοντας τα δύο συστήματα να ανταλλάσσουν ένα "μυστικό" κατά την πορεία της συνόδου επικοινωνίας. Το μυστικό μπορεί να ανταλλάσσεται με κάθε πακέτο που μεταδίδεται, ή σε τυχαία χρονικά διαστήματα κατά την διάρκεια της συνόδου. Προφανώς, η επαλήθευση της προέλευσης σε κάθε πακέτο είναι πολύ πιο ασφαλής από την επαλήθευση σε τυχαία χρονικά διαστήματα. Η σύνοδος επικοινωνίας θα ήταν ακόμη πιο ασφαλής εάν μπορούσατε να διαφοροποιείτε το μυστικό που ανταλλάσσεται με κάθε πακέτο. Κάτι τέτοιο θα βοηθούσε στο να διασφαλιστεί ότι η σύνοδος επικοινωνίας είναι άτρωτη σε οποιαδήποτε μορφή πειρατείας συνόδου.

Επαλήθευση του Προορισμού

Αυτό που μπορεί να μην είναι άμεσα εμφανές είναι η ανάγκη πιστοποίησης του ίδιου του server. Πολλοί άνθρωποι θεωρούν ως δεδομένο ότι όταν επιχειρούν μία σύνδεση είτε θα συνδέονται στον σωστό server, είτε θα λαμβάνουν κάποιο μήνυμα το οποίο θα τους αναφέρει ότι το συγκεκριμένο σύστημα δεν είναι προσπελάσιμο. Δεν αντιλαμβάνονται ότι αυτό που θεωρούν ως server μπορεί στην πραγματικότητα να είναι ένας εισβολέας ο οποίος προσπαθεί να παραβιάσει το δίκτυο τους.

Από τα Windows *95* και μετά, η Microsoft χρησιμοποιεί ισχυρότερα σχήματα πιστοποίησης στα λειτουργικά της συστήματα (όπως θα δείτε παρακάτω σ' αυτό το κεφάλαιο), με αποκορύφωμα το πρωτόκολλο Kerberos το οποίο απαιτεί και από τα δύο επικοινωνούντα συστήματα να πιστοποιούν το ένα την ταυτότητα του στο άλλο.

Δηλητηρίαση του DNS

Μία άλλη μορφή επίθεσης η οποία καταδεικνύει την αναγκαιότητα ενός ισχυρού μηχανισμού πιστοποίησης είναι η δηλητηρίαση του DNS (DNS poisoning). Η δηλητηρίαση DNS (γνωστή επίσης και με τον όρο δηλητηρίαση μνήμης [cache poisoning]) είναι η διαδικασία παράδοσης λανθασμένης διεύθυνσης IP για έναν συγκεκριμένο σταθμό του δικτύου, με στόχο την εκτροπή της κυκλοφορίας σε μία διαφορετική διαδρομή, και όχι στον πραγματικό της προορισμό.

Κάτι τέτοιο ανοίγει την πόρτα για ορισμένες πολύ πιο τρομακτικές δυνατότητες. Στην εποχή των ηλεκτρονικών τραπεζικών συναλλαγών, σκεφτείτε τις επιπτώσεις που θα υπήρχαν εάν κάποιος εξέτρεπε την κυκλοφορία που κατευθύνεται στο Web site μιας τράπεζας. Ένας εισβολέας θα μπορούσε να στήσει έναν πλασματικό δέρνει· ώστε να δείχνει πανομοιότυπος με τον server της τράπεζας και κατόπιν να χρησιμοποιήσει την μέθοδο "δηλητηρίασης" του DNS για να εκτρέψει την προοριζόμενη για την τράπεζα κυκλοφορία σ' αυτό τον ψεύτικο server.

Όταν ένας πελάτης της τράπεζας προσπαθήσει να πιστοποιηθεί στον Web server της για να κάνει οποιεσδήποτε ενέργειες θέλει με τους τραπεζικούς του λογαριασμούς, ο εισβολέας θα μπορούσε να υποκλέψει τις πληροφορίες πιστοποίησης και να παρουσιάσει στον χρήστη μία αρχική οθόνη η οποία θα δηλώνει ότι το σύστημα της τράπεζας είναι επί του παρόντος εκτός λειτουργίας. Εάν δεν χρησιμοποιούνται ψηφιακά πιστοποιητικά (digital certificates), ο πελάτης δεν μπορεί να ξέρει ότι η επικοινωνία του έχει εκτραπεί σε ένα διαφορετικό site παρά μόνο εάν προσέξει την αλλαγή στις διευθύνσεις IP (κάτι το οποίο δεν είναι και τόσο πιθανό).

6.3. Εισαγωγή στην Κρυπτογράφηση

Η *κρυπτογραφία (cryptography)* είναι η επιστήμη που ασχολείται με τον μετασχηματισμό της πληροφορίας σε μία εναλλακτική μορφή, η οποία μπορεί κατόπιν να αντιστραφεί για να επανέλθει στην αρχική της μορφή. Η εναλλακτική μορφή αναφέρεται σαν κρυπτογραφημένο κείμενο (ciphertext) ή απλώς κρυπτογράφημα και συνήθως δημιουργείται με την χρήση ενός αλγορίθμου και ενός κλειδιού κρυπτογράφησης. Ο αλγόριθμος κρυπτογράφησης είναι ένας μαθηματικός τύπος ο οποίος εφαρμόζεται στην πληροφορία που θέλετε να κρυπτογραφήσετε. Το κλειδί κρυπτογράφησης είναι μία επιπλέον μεταβλητή η οποία "εμφυτεύεται" στον αλγόριθμο κρυπτογράφησης για να διασφαλίσει ότι το κρυπτογράφημα δεν θα παράγεται με την ίδια ακριβώς ακολουθία υπολογισμών κάθε φορά που χρησιμοποιείται ο αλγόριθμος.

Επειδή η κρυπτογράφηση χρησιμοποιεί μαθηματικούς τύπους, υπάρχει μία στενή σχέση μεταξύ των ακόλουθων στοιχείων:

- Αλγόριθμος
- Κλειδί κρυπτογράφησης
- Αρχικά δεδομένα
- Κρυπτογράφημα (κρυπτογραφημένο κείμενο)

Αυτό σημαίνει ότι εάν γνωρίζετε οποιαδήποτε τρία από τα παραπάνω στοιχεία, είστε σε θέση να παράγετε το τέταρτο. Η μοναδική εξαίρεση είναι όταν γνωρίζετε τον συνδυασμό των αρχικών δεδομένων και του κρυπτογραφήματος. Εάν έχετε πολλαπλά δείγματα αρχικών δεδομένων και των κρυπτογραφημάτων τους, είναι δυνατό να ανακαλύψετε τον αλγόριθμο και το κλειδί κρυπτογράφησης.

Μέθοδοι Κρυπτογράφησης

Οι δύο βασικές μέθοδοι κρυπτογράφησης είναι:

- Κρυπτογράφηση σε επίπεδο μεμονωμένων ψηφίων (stream cipher)

- Κρυπτογράφηση σε επίπεδο ομάδων χαρακτήρων (block cipher)

Οι δύο μέθοδοι κρυπτογράφησης είναι παρόμοιες, εκτός από την ποσότητα των δεδομένων που κρυπτογραφούν σε κάθε πέρασμα. Τα περισσότερα σύγχρονα σχήματα κρυπτογράφησης χρησιμοποιούν κάποια μορφή κρυπτογράφησης ομάδων χαρακτήρων.

Κρυπτογράφηση σε Επίπεδο Μεμονωμένων Ψηφίων

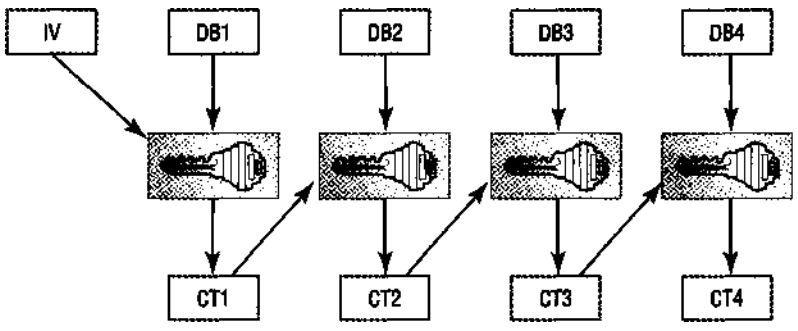
Η κρυπτογράφηση σε επίπεδο μεμονωμένων ψηφίων είναι μία από τις απλούστερες μεθόδους κρυπτογράφησης δεδομένων. Όταν χρησιμοποιείται αυτή η μέθοδος, κάθε ψηφίο (bit) δεδομένων κρυπτογραφείται διαδοχικά, χρησιμοποιώντας ένα ψηφίο (bit) του κλειδιού. Ένα κλασσικό παράδειγμα αυτής της μεθόδου είναι ο κώδικας του Vernam, ο οποίος χρησιμοποιούνταν για την κρυπτογράφηση της επικοινωνίας μέσω τηλετύπου.

Κρυπτογράφηση σε Επίπεδο Ομάδων Δεδομένων

Αντίθετα με την κρυπτογράφηση σε επίπεδο μεμονωμένων ψηφίων, οι μέθοδοι κρυπτογράφησης σε επίπεδο ομάδων δεδομένων (block cipher) είναι ειδικά σχεδιασμένες ώστε να κρυπτογραφούν ομάδες δεδομένων συγκεκριμένου μεγέθους. Οι προδιαγραφές ενός τέτοιου κώδικα κρυπτογράφησης πρέπει να προσδιορίζουν την ποσότητα των δεδομένων που θα κρυπτογραφούνται σε κάθε πέρασμα (το μπλοκ), καθώς και το μέγεθος του κλειδιού που θα εφαρμόζεται σε κάθε μπλοκ. Για παράδειγμα, το πολύ γνωστό σύστημα κρυπτογράφησης DES (Data Encryption Standard) υπαγορεύει ότι τα δεδομένα πρέπει να κρυπτογραφούνται σε μπλοκ των 64 bit, χρησιμοποιώντας ένα κλειδί μεγέθους 56 bit.

Υπάρχουν πολλοί διαφορετικοί αλγόριθμοι οι οποίοι μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση σε επίπεδο μπλοκ δεδομένων. Στην απλούστερη μορφή του, ένας τέτοιος αλγόριθμος παίρνει απλώς τα δεδομένα, τα διαχωρίζει σε ομάδες και εφαρμόζει το κλειδί σε κάθε ομάδα. Αν και αυτή η μέθοδος είναι αποτελεσματική, μπορεί να παράγει επαναλαμβανόμενα μοτίβα στο κρυπτογράφημα. Εάν δύο ομάδες δεδομένων περιέχουν την ίδια ακριβώς πληροφορία, η κρυπτογράφηση τους μ' έναν τέτοιο αλγόριθμο θα δώσει πανομοιότυπο αποτέλεσμα. Ένας cracker μπορεί να χρησιμοποιήσει τα επαναλαμβανόμενα μοτίβα που συναντά στο κρυπτογράφημα για να βρει το κλειδί κρυπτογράφησης.

Μία καλύτερη λύση θα ήταν να πάρουμε τα πρώτα αποτελέσματα του αλγόριθμου και να τα συνδυάσουμε με επόμενα κλειδιά. Η Εικόνα 6.6 παρουσιάζει μία πιθανή μέθοδο. Τα δεδομένα που θέλουμε να κρυπτογραφήσουμε χωρίζονται σε μπλοκ με τίτλους DB1 έως DB4. Προστίθεται ένας "παράγοντας αρχικοποίησης" (Initialization Vector, IV) στην αρχή των δεδομένων, ο οποίος διασφαλίζει ότι όλα τα μπλοκ μπορούν να κρυπτογραφηθούν σωστά. Ο παράγοντας αρχικοποίησης είναι μία τυχαία ακολουθία χαρακτήρων η οποία διασφαλίζει ότι δεν θα παραχθεί το ίδιο κρυπτογράφημα από δύο πανομοιότυπα αρχικά μηνύματα. Για την δημιουργία του πρώτου κρυπτογραφημένου μπλοκ (CT1) χρησιμοποιείται ένας μαθηματικός τύπος ο οποίος συνδυάζει το κλειδί κρυπτογράφησης, το πρώτο μπλοκ των αρχικών δεδομένων (DB1) και τον παράγοντα αρχικοποίησης (IV).



Κλειδί + IV + DB1 = CT1 Κλειδί + CT1 + DB2 = CT2 Κλειδί + CT2 + DB3 = CT3 Κλειδί + CT3 + DB4 = CT4

ΕΙΚΟΝΑ 6.6: Μία τεχνική κρυπτογράφησης σε επίπεδο ομάδων δεδομένων.

Για την δημιουργία του δεύτερου κρυπτογραφημένου μπλοκ (CT2) ο μαθηματικός τύπος συνδυάζει το κλειδί κρυπτογράφησης, το πρώτο κρυπτογραφημένο μπλοκ (CT1) και το δεύτερο μπλοκ των αρχικών δεδομένων (DB2). Επειδή οι μεταβλητές του αλγορίθμου μας έχουν αλλάξει, τα DB1 και DB2 μπορούν να είναι πανομοιότυπα, αλλά τα παραγόμενα κρυπτογραφήματα (CT1 και CT2) θα περιέχουν διαφορετικές τιμές. Αυτό μας βοηθά να διασφαλίσουμε ότι συνολικά, το παραγόμενο κρυπτογράφημα θα είναι επαρκώς "ανακατεμένο" έτσι ώστε να δείχνει εντελώς τυχαίο. Η χρήση του κρυπτογραφήματος του προηγούμενου μπλοκ για την κρυπτογράφηση του επόμενου μπλοκ δεδομένων συνεχίζεται για ολόκληρο το αρχικό μήνυμα. Το αποτέλεσμα είναι η παραγωγή μιας φαινομενικά τυχαίας ακολουθίας χαρακτήρων στο κρυπτογράφημα.

Δημόσια/Ιδιωτικά Κλειδιά Κρυπτογράφησης

Μέχρι τώρα, όλες οι τεχνικές κρυπτογράφησης που εξετάσαμε χρησιμοποιούν αλγόριθμους οι οποίοι βασίζονται στην ύπαρξη ενός *μυστικού κλειδιού*. Ένας τέτοιος αλγόριθμος βασίζεται στο ίδιο κλειδί για την κρυπτογράφηση των δεδομένων και την αποκρυπτογράφηση τους. Αυτό σημαίνει ότι το κλειδί κρυπτογράφησης πρέπει να παραμείνει μυστικό για να διασφαλιστεί η ακεραιότητα των κρυπτογραφημένων δεδομένων. Εάν ένας εισβολέας μάθει το μυστικό σας κλειδί, θα μπορεί να ξεκλειδώσει όλα τα κρυπτογραφημένα μηνύματα σας. Εδώ προκύπτει ένα ενδιαφέρον πρόβλημα: θα πρέπει να βρείτε μία ασφαλή μέθοδο για την ανταλλαγή του μυστικού κλειδιού με τα άτομα που επικοινωνείτε, έτσι ώστε οι πληροφορίες που ανταλλάσσετε να είναι εξίσου ασφαλείς!

Με απλούς όρους, ένα *δημόσιο κλειδί (public key)* είναι ένα κλειδί κρυπτογράφησης το οποίο παράγεται με μαθηματικό τρόπο από ένα ιδιωτικό (μυστικό) κλειδί κρυπτογράφησης. Οι πληροφορίες που κρυπτογραφούνται με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν με το ιδιωτικό κλειδί του παραλήπτη τους· ωστόσο, οι πληροφορίες που κρυπτογραφούνται με το ιδιωτικό κλειδί δεν μπορούν να αποκρυπτογραφηθούν με το δημόσιο κλειδί. Με άλλα λόγια, τα δύο κλειδιά - δημόσιο και ιδιωτικό - δεν είναι "συμμετρικά". Είναι ειδικά σχεδιασμένα έτσι ώστε το δημόσιο κλειδί να χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και το ιδιωτικό κλειδί να χρησιμοποιείται για τη ν αποκρυπτογράφηση του παραγόμενου κρυπτογραφήματος.

Αυτό εξαλείφει το πρόβλημα της χρήσης συμμετρικών μυστικών κλειδιών, επειδή δεν απαιτεί ένα ασφαλές κανάλι επικοινωνίας για την ανταλλαγή του κλειδιού μεταξύ των ενδιαφερόμενων μερών. Τα δημόσια κλειδιά μπορούν να κοινοποιούνται με οποιαδήποτε μέθοδο, διατηρώντας ωστόσο την μυστικότητα των μηνυμάτων που κρυπτογραφούν. Εάν ένας φίλος σας θέλει να σας στείλει ένα μυστικό μήνυμα, το μόνο που χρειάζεται να κάνει είναι να το κρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί σας. Το παραγόμενο κρυπτογράφημα μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό σας κλειδί.

Η μέθοδος Diffie-Hellman μπορεί επίσης να χρησιμοποιηθεί για σκοπούς πιστοποίησης: Πιστοποιείτε την ταυτότητα σας υπογράφοντας ένα μήνυμα με το ιδιωτικό σας κλειδί, πριν το κρυπτογραφήσετε με το δημόσιο κλειδί του παραλήπτη. Η "υπογραφή" είναι απλώς ένας μαθηματικός αλγόριθμος ο οποίος επεξεργάζεται το ιδιωτικό σας κλειδί και τα περιεχόμενα του μηνύματος σας. Έτσι δημιουργείται μία μοναδική στο είδος της ψηφιακή υπογραφή, η οποία προσαρτάται στο τέλος του μηνύματος. Επειδή για την δημιουργία της υπογραφής χρησιμοποιούνται τα περιεχόμενα του μηνύματος, η ψηφιακή σας υπογραφή θα είναι διαφορετική σε κάθε μήνυμα που στέλνετε.

Για παράδειγμα, ας υποθέσουμε ότι θέλετε να στείλετε ένα ιδιωτικό μήνυμα σ' έναν φίλο σας. Κατ' αρχήν δημιουργείτε μία ψηφιακή υπογραφή χρησιμοποιώντας το ιδιωτικό σας κλειδί και κατόπιν κρυπτογραφείτε το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του φίλου σας. Όταν ο φίλος σας λάβει το κρυπτογραφημένο μήνυμα, κατ' αρχήν το αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί και κατόπιν ελέγχει την

ψηφιακή υπογραφή χρησιμοποιώντας το δικό σας δημόσιο κλειδί. Εάν η υπογραφή ταιριάζει, ο φίλος σας μπορεί να είναι σίγουρος ότι το μήνυμα που έλαβε είναι αυθεντικό και δεν έχει παραποιηθεί. Εάν η υπογραφή δεν ταιριάζει, ο φίλος σας θα πρέπει να υποθέσει είτε ότι το μήνυμα δεν υπογράφτηκε με το ιδιωτικό σας κλειδί, είτε ότι το κρυπτογράφημα τροποποιήθηκε κατά την πορεία προς τον προορισμό του. Σε κάθε περίπτωση, ο παραλήπτης θα ξέρει ότι το περιεχόμενο αυτού του μηνύματος πρέπει να αντιμετωπιστεί τουλάχιστον με επιφύλαξη.

Τα Αδύνατα Σημεία της Κρυπτογράφησης

Τρία είναι τα αδύνατα σημεία της κρυπτογράφησης:

- Λανθασμένος χειρισμός, ή ανθρώπινα σφάλματα
- Αναποτελεσματικότητα του κώδικα κρυπτογράφησης
- Επιθέσεις "ωμής βίας"

Όταν καλείστε να επιλέξετε ποια μέθοδος κρυπτογράφησης ικανοποιεί καλύτερα τις ανάγκες σας, θα πρέπει οπωσδήποτε να εξετάσετε τα αδύνατα σημεία των υποψήφιων επιλογών σας.

Λανθασμένος Χειρισμός ή Ανθρώπινα Σφάλματα

Ανθρώπινα σφάλματα στη διαχείριση των κλειδιών είναι συχνότερα σε ορισμένες μέθοδους κρυπτογράφησης σε σύγκριση με άλλες. Όταν επιλέγετε μία μέθοδο κρυπτογράφησης, βεβαιωθείτε ότι έχετε την σωστή υποδομή που απαιτείται για την διαχείριση των κλειδιών κρυπτογράφησης με τον ενδεδειγμένο τρόπο.

Αν και η κρυπτογράφηση με κλειδιά μιας χρήσης (one-time pad) είναι η ασφαλέστερη μέθοδος που θα μπορούσε να χρησιμοποιήσει κανείς, απαιτεί από εσάς να έχετε την δυνατότητα να παράγετε πολλά κλειδιά για να καλύψετε τις ανάγκες σας στον τομέα της κρυπτογράφησης δεδομένων. Ακόμη κι αν χρησιμοποιείτε έναν συνηθισμένο κώδικα κρυπτογράφησης με μυστικό κλειδί για τις επικοινωνίες μέσω του δικτύου σας, θα πρέπει να διασφαλίσετε ότι έχετε στη διάθεση σας μία απόλυτα ασφαλή μέθοδο για την ανταλλαγή του κλειδιού μεταξύ των υπολογιστών. Ποιο το όφελος να κρυπτογραφήσετε τα δεδομένα σας, εάν πρόκειται να μεταδώσετε το μυστικό σας κλειδί μέσω ενός μη-ασφαλούς καναλιού επικοινωνίας;

Η απλότητα στην διαχείριση των κλειδιών είναι ένας από τους λόγους για τους οποίους έγινε τόσο δημοφιλής η μέθοδος δημόσιου/ιδιωτικού κλειδιού. Η δυνατότητα ανταλλαγής του κλειδιού μέσω του ίδιου μη-ασφαλούς καναλιού που σκοπεύετε να χρησιμοποιήσετε και για την μετάδοση των δεδομένων είναι πολύ ελκυστική πρόταση. Κατ' αρχήν, απλοποιεί σημαντικά την διαχείριση: μπορείτε να κρατάτε το ιδιωτικό σας κλειδί απόρρητο, ενώ μεταδίδετε το δημόσιο κλειδί σας χρησιμοποιώντας οποιαδήποτε μέθοδο επιλέγετε.

Θα πρέπει να διασφαλίσετε ότι τα δημόσια κλειδιά που χρησιμοποιείτε για την κρυπτογράφηση δεδομένων προέρχονται πράγματι από την κατάλληλη πηγή και όχι από έναν εισβολέα ο οποίος άλλαξε ένα ιδιωτικό κλειδί μ' ένα άλλο. Η εγκυρότητα ενός δημόσιου κλειδιού μπορεί εύκολα να πιστοποιηθεί μ' ένα τηλεφώνημα, ή κάποιον άλλο εξίσου εύκολο τρόπο.

Οι Αδυναμίες των Κωδίκων Κρυπτογράφησης

Το να εξακριβώσει κανείς εάν υπάρχουν οποιεσδήποτε αδυναμίες στον αλγόριθμο (κώδικα) μιας συγκεκριμένης μεθόδου κρυπτογράφησης είναι πιθανώς η δυσκολότερη εργασία που μπορεί να ανατεθεί σε έναν μη-ειδικό στην κρυπτογραφία. Υπάρχουν όμως ορισμένα πράγματα τα οποία μπορείτε να ελέγξετε για να βεβαιωθείτε ότι η μέθοδος κρυπτογράφησης που χρησιμοποιείτε είναι ασφαλής:

- Ο αλγόριθμος στον οποίο βασίζεται ο κώδικας κρυπτογράφησης πρέπει να έχει κοινοποιηθεί. Οι αλγόριθμοι που βασίζονται στην μυστικότητα είναι πιθανό να αντιμετωπίζουν προβλήματα τα οποία μπορεί να εκμεταλλευτεί κάποιος για να επιτύχει γρηγορότερα το σπάσιμο του κώδικα κρυπτογράφησης.
- Ο αλγόριθμος κρυπτογράφησης θα πρέπει να έχει υποστεί σχολαστική δημόσια εξέταση. Ο κάθε άνθρωπος θα πρέπει να έχει την δυνατότητα να αξιολογήσει τον αλγόριθμο και να δημοσιεύσει ελεύθερα τα ευρήματα του. Αυτό σημαίνει ότι η ανάλυση και η αξιολόγηση του αλγόριθμου δεν μπορεί να περιορίζεται με συμφωνίες εμπιστευτικότητας, ή με την υπογραφή δεσμευτικών συμφωνιών μη-αποκάλυψης.
- Ο αλγόριθμος κρυπτογράφησης θα πρέπει να είναι διαθέσιμος στο ευρύ κοινό για εύλογο χρονικό διάστημα, έτσι ώστε να γίνει σωστή ανάλυση και αξιολόγηση του. Ένας αλγόριθμος κρυπτογράφησης ο οποίος είναι διαθέσιμος στο κοινό μόνο για λίγους μήνες δεν μπορεί να χαρακτηριστεί σαν "δοκιμασμένος στον χρόνο".

Η δημόσια ανάλυση δεν θα πρέπει να αποκαλύψει "χρήσιμες" (για έναν cracker) αδυναμίες του αλγόριθμου κρυπτογράφησης.

Ακολουθώντας αυτούς τους απλούς κανόνες θα είστε σε θέση να κάνετε εμπεριστατωμένες εκτιμήσεις για την ασφάλεια που παρέχει ένας αλγόριθμος κρυπτογράφησης.

Επιθέσεις Ωμής Βίας

Σαν επίθεση ωμής βίας (brute force attack) χαρακτηρίζεται μία προσπάθεια δοκιμής όλων των πιθανών συνδυασμών για την εύρεση του κλειδιού που θα "ξεκλειδώσει" το κρυπτογράφημα. Αυτός είναι και ο λόγος για τον οποίο η συγκεκριμένη μορφή επίθεσης αναφέρεται επίσης σαν "εξαντλητική αναζήτηση κλειδιού" (exhaustive key search). Ο επίδοξος cracker δεν κάνει πραγματική προσπάθεια να σπάσει το κλειδί, αλλά βασίζεται στην δυνατότητα του να δοκιμάσει όλους τους πιθανούς συνδυασμούς κλειδιών μέσα σε ένα εύλογο χρονικό διάστημα. Όλοι οι αλγόριθμοι κρυπτογράφησης είναι τρωτοί - σε μικρότερο ή μεγαλύτερο βαθμό - στις επιθέσεις ωμής βίας.

Εάν μία εξαντλητική αναζήτηση κλειδιού μπορεί να αποκαλύψει τους αριθμούς "χρυσών" καρτών VISA σε λίγες ώρες, τότε η επίθεση αυτή αξίζει τον κόπο. Εν αντιθέσει, εάν χρειάζονται χρόνια δοκιμών, τότε ίσως μία επίθεση ωμής βίας μάλλον δεν αξίζει ούτε τον κόπο, ούτε τον χρόνο σας.

Το άλλο σημαντικό στοιχείο είναι πόσο τρωτός είναι ένας αλγόριθμος. Αν και όλοι οι αλγόριθμοι κρυπτογράφησης είναι ευπρόσβλητοι σε επιθέσεις ωμής βίας, ορισμένοι απαιτούν τόσο πολύ χρόνο για την δοκιμή όλων των πιθανών κλειδιών, που ο απαιτούμενος χρόνος δεν μπορεί να θεωρηθεί εύλογος. Για παράδειγμα, ένας κώδικας κρυπτογράφησης με κλειδιά μιας χρήσης θα μπορούσε να "σπάσει" με μία επίθεση ωμής βίας, αλλά σε χρόνο που μετράται ίσως σε χιλιετίες, χρησιμοποιώντας την ισχύ των σημερινών υπολογιστών.

Συνεπώς, ο χρόνος που απαιτείται για την εκτέλεση μιας επίθεσης ωμής βίας εξαρτάται από δυο παράγοντες: τον χρόνο που απαιτείται για την δοκιμή ενός συγκεκριμένου κλειδιού και το πλήθος των πιθανών συνδυασμών κλειδιών. Ο χρόνος που απαιτείται για την δοκιμή κάθε κλειδιού εξαρτάται από την συσκευή που παρέχει την επεξεργαστική ισχύ. Ένας τυπικός προσωπικός υπολογιστής μπορεί να δοκιμάζει περίπου πέντε κλειδιά ανά δευτερόλεπτο. Μία συσκευή ειδικά σχεδιασμένη για το σπάσιμο κλειδιών κρυπτογράφησης μπορεί να επεξεργάζεται 200 και πλέον κλειδιά ανά δευτερόλεπτο. Φυσικά, ο συνδυασμός πολλαπλών υπολογιστών θα μπορούσε να επιφέρει ακόμη καλύτερα αποτελέσματα.

Όσον αφορά στο πλήθος των πιθανών συνδυασμών κλειδιών, αυτό είναι ανάλογο με το μέγεθος του κλειδιού κρυπτογράφησης. Στην κρυπτογραφία, το μέγεθος έχει σημασία:

όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο περισσότεροι πιθανοί συνδυασμοί υπάρχουν. Ο Πίνακας 6.1 παρουσιάζει ορισμένες κοινές μεθόδους κρυπτογράφησης μαζί με το αντίστοιχο μέγεθος κλειδιού. Παρατηρήστε ότι καθώς αυξάνεται το μέγεθος του κλειδιού, αυξάνεται εκθετικά το πλήθος των πιθανών συνδυασμών.

ΠΙΝΑΚΑΣ 6.1: Μέθοδοι Κρυπτογράφησης και τα Αντίστοιχα Κλειδιά

Κρυπτογράφηση	**Μέγεθος Κλειδιού**	**Πλήθος Πιθανών Συνδυασμών**
Netscape	40 bits	1.1X10
DES	56 bits	72.1x10
Triple DES (2 κλειδιά)	112 bits	5.2x10
IDEA	128 bits	3.4x10
RC4/128	128 bits	3.4x10
Triple DES (3 κλειδιά)	168 bits	3.7x10
Μελλοντικό πρότυπο;	256 bits	1.2χ10

Φυσικά, όλα αυτά οδηγούν στο εξής ερώτημα: πόσος χρόνος χρειάζεται για την διεξαγωγή μιας εξαντλητικής αναζήτησης κλειδιού για έναν συγκεκριμένο αλγόριθμο κρυπτογράφησης; Η απάντηση θα σας φοβίσει. Το σύστημα κρυπτογράφησης DES (το οποίο θα εξετάσουμε σε μία ειδική ενότητα παρακάτω σ' αυτό το κεφάλαιο) θεωρείται πρότυπο σ' αυτό τον τομέα. Εδώ και κάμποσα χρόνια τα εργαστήρια RSA Laboratories έχουν απευθύνει ανοιχτή πρόσκληση για το "σπάσιμο" ενός κρυπτογραφήματος δημιουργημένου με το DES.

Το 1997, χρειάστηκαν περίπου πέντε μήνες. Στις αρχές του 1998, χρειάστηκαν 39 ημέρες. Μέχρι τον Ιούλιο του 1999, το Electronic Frontier Foundation (EFF) κατάφερε να απαντήσει στην πρόκληση σε λιγότερο από 22 ώρες.

Το EFF κατάφερε αυτό τον εκπληκτικό χρόνο χρησιμοποιώντας μία συσκευή ειδικά σχεδιασμένη για την εκτέλεση επιθέσεων ωμής βίας στο σύστημα κρυπτογράφησης DES. Το κόστος της συσκευής ήταν περίπου 250,000 δολάρια σίγουρα εντός των οικονομικών δυνατοτήτων τόσο του οργανωμένου εγκλήματος, όσο και των πολυεθνικών επιχειρήσεων. Μετά από την επιτυχία του, το EFF δημοσίευσε ένα βιβλίο με

τίτλο Cracking DES («σπάζοντας το DES»), στο οποίο τεκμηριώνεται πλήρως η σχεδίαση της συσκευής που χρησιμοποίησε. Το περιστατικό αυτό άλλαξε εντελώς τις απόψεις των ειδικών σχετικά με το ποια μεγέθη κλειδιών θεωρούνται ασφαλή.

6.4. Η Αναγκαιότητα ενός καλού μηχανισμού κρυπτογράφησης

Εάν χρησιμοποιείτε έναν ισχυρό μηχανισμό πιστοποίησης για οποιαδήποτε μορφή επικοινωνίας στο δίκτυο σας, γιατί χρειάζεστε την κρυπτογράφηση; Η κρυπτογράφηση εξυπηρετεί δύο σκοπούς:

- Την προστασία των δεδομένων από υποκλοπή
- Την προστασία των δεδομένων από τροποποίηση

Έχουμε δει ότι οι περισσότερες υπηρεσίες του IP μεταδίδουν όλη την πληροφορία σε μορφή απλού κειμένου. Αυτό και μόνο το γεγονός είναι αρκετό για να αιτιολογήσει κανείς την αναγκαιότητα χρήσης ενός καλού μηχανισμού κρυπτογράφησης για την προστασία των δεδομένων του από τα αδιάκριτα μάτια.

Η κρυπτογράφηση μπορεί επίσης να σας βοηθήσει να διασφαλίσετε ότι τα δεδομένα δεν υφίστανται κανενός είδους τροποποίηση κατά την μετάδοση τους. Τέτοιες μορφές επίθεσης χαρακτηρίζονται συνήθως με τον όρο "man-in-the-middle" (ένας άνθρωπος ανάμεσα), επειδή βασίζονται στην δυνατότητα ενός εισβολέα να παρεμβληθεί στην

μετάδοση των δεδομένων. Ας υποθέσουμε ότι έχετε έναν Web server διαμορφωμένο ώστε να δέχεται online παραγγελίες από τον κατάλογο των προϊόντων σας. Ο πελάτης συμπληρώνει μία ηλεκτρονική φόρμα, η οποία αποθηκεύεται κατόπιν στον Web server σε μορφή απλού κειμένου. Σε τακτά χρονικά διαστήματα, τα αρχεία αυτά μεταφέρονται σε έναν διαφορετικό υπολογιστή μέσω FTP ή SMTP.

Εάν ένας εισβολέας αποκτήσει πρόσβαση στο σύστημα αρχείων του Web server, θα έχει την δυνατότητα να τροποποιήσει αυτά τα αρχεία κειμένου πριν υποστούν επεξεργασία. Το αποτέλεσμα είναι δυσαρεστημένοι πελάτες. Αν και αυτό το παράδειγμα υποθέτει ότι ο εισβολέας απέκτησε πρόσβαση στο σύστημα αρχείων ενός server, μία ανάλογη επίθεση είναι επίσης δυνατό να εκκινήσει κατά την διάρκεια που οι πληροφορίες βρίσκονται προσωρινά στο δίκτυο.

Σ' αυτή την περίπτωση, αν και ο εισβολέας δεν έκλεψε τίποτα δικό σας, η τροποποίηση που έκανε στα δεδομένα είχε άμεσες αρνητικές επιπτώσεις για την επιχείρηση σας. Εάν τα δεδομένα των παραγγελιών κρυπτογραφούνταν με έναν ισχυρό αλγόριθμο κρυπτογράφησης, η επίθεση αυτή θα ήταν πολύ πιο δύσκολο να επιτύχει, επειδή ο εισβολέας δεν θα ήξερε ποιες τιμές του κρυπτογραφημένου αρχείου πρέπει να αλλάξει. Και ακόμη κι αν κατάφερνε να μαντέψει σωστά μερικές τιμές, ο αλγόριθμος αποκρυπτογράφησης θα εντόπιζε τις αλλαγές στα δεδομένα.

Data Encryption Standard(DES)

Το DES ήταν για πολλά χρόνια το σύστημα κρυπτογράφησης που χρησιμοποιούσε η κυβέρνηση των Η.Π.Α. για την προστασία των ευαίσθητων αλλά όχι διαβαθμισμένων δεδομένων της. Το Ινστιτούτο ANSI και η ομάδα εργασίας IETF (Internet Engineering Task Force) έχουν επίσης ενσωματώσει το DES στα δικά τους πρότυπα ασφάλειας. Το DES είναι εκ του μακρόθεν ο δημοφιλέστερος κώδικας κρυπτογράφησης μυστικού κλειδιού που χρησιμοποιείται σήμερα.

Για την κρυπτογράφηση των δεδομένων, το αρχικό πρότυπο του DES χρησιμοποιεί ένα κλειδί μεγέθους 40 bit (για τα προϊόντα που εξάγονται εκτός των Η.Π.Α), ή 56 bit. Η πιο πρόσφατη έκδοση του προτύπου, με όνομα Triple DES, κρυπτογραφεί το απλό κείμενο τρεις φορές χρησιμοποιώντας δύο ή τρία διαφορετικά κλειδιά μεγέθους 56 bit. Η διαδικασία αυτή παράγει ένα κρυπτογράφημα ισοδύναμο με το κρυπτογράφημα που θα παρήγαγε η χρήση ενός κλειδιού μεγέθους 112 bit ή 168 bit, διατηρώντας ωστόσο προς τα πίσω συμβατότητα με τις προηγούμενες εκδόσεις του προτύπου.

Το DES είναι σχεδιασμένο με τέτοιο τρόπο, έτσι ώστε ακόμη κι αν κάποιος γνωρίζει ένα μέρος των αρχικών δεδομένων και την αντίστοιχη κρυπτογραφημένη μορφή τους, να μην υπάρχει κανένας τρόπος για να βρεθεί το κλειδί χωρίς να δοκιμαστούν όλα τα πιθανά κλειδιά. Η ισχύς της βασιζόμενης στο DES κρυπτογράφησης βασίζεται στο κλειδί και στην σωστή προστασία του. Αν και το αρχικό πρότυπο του DES έχει "σπάσει" από επιθέσεις ωμής βίας μέσα σε 56 και μόνο ώρες, το νέο πρότυπο Triple DES θεωρείται ότι θα είναι ασφαλές για αρκετά χρόνια.

Advanced Encryption Standard (AES)

Από τις 26 Μαΐου του 2002, το νέο πρότυπο κρυπτογράφησης που χρησιμοποιεί η κυβέρνηση των Η.Π.Α. για την προστασία ευαίσθητων αλλά όχι διαβαθμισμένων δεδομένων είναι το AES (Advanced Encryption Standard). Αυτό το νέο πρότυπο είναι ο νικητής ενός διαγωνισμού στον οποίο συμμετείχαν πολλοί αλγόριθμοι κρυπτογράφησης (MARS, RC6, Rijndael, Serpent, Twofish) οι οποίοι αξιολογήθηκαν όχι μόνο ως προς την αντοχή τους σε επιθέσεις "ωμής βίας", αλλά επίσης ως προς την ταχύτητα, την συντήρηση και την ευκολία διαχείρισης. Σαν αποτέλεσμα αυτής της διαδικασίας, επιλέχτηκε ο αλγόριθμος Rijndael σαν "επίσημος" αλγόριθμος του νέου προτύπου.

Ο αλγόριθμος Rijndael (όπως υλοποιείται στο AES) είναι ένας συμμετρικός κώδικας κρυπτογράφησης ομάδων χαρακτήρων ο οποίος χρησιμοποιεί κλειδιά μεγέθους 128, 192 και 256 bits (σε μπλοκ των 128 bit). Αν και όλοι οι αλγόριθμοι που υποβλήθηκαν στην κυβέρνηση των Η.Π.Α. θεωρήθηκαν κατάλληλοι - από άποψη ισχύος - για το AES, ο αλγόριθμος Rijndael αρίστευσε μεταξύ αυτών στους τομείς της απόδοσης, της αποτελεσματικότητας και της ευελιξίας. Αυτοί οι τομείς έχουν εξαιρετική σημασία, εάν λάβει κανείς υπόψη ότι το σύστημα κρυπτογράφησης πρέπει να υλοποιηθεί σε συστήματα

(hardware και software) με ισχύ μικρότερη από αυτή ενός τυπικού προσωπικού υπολογιστή όπως π.χ. πομποδέκτες, αναγνώστες κλειδιών/καρτών και άλλες συσκευές.

Ποια είναι η γνώμη της IETF σχετικά με το AES και τον αλγόριθμο που χρησιμοποιεί; Μετά από ενδελεχή επανεξέταση των καθιερωμένων από την ίδια πρωτοκόλλων (συμπεριλαμβανομένων των SSL, S/MIME, SSH και kerberos μεταξύ άλλων), η IETF κατέληξε ότι τα περισσότερα πρωτόκολλα, τα οποία χρησιμοποιούν ήδη κρυπτογράφηση, μπορούν να τροποποιηθούν σχετικά εύκολα ώστε να υποστηρίζουν το νέο πρότυπο AES. Σαν αποτέλεσμα, μέχρι τα τέλη του 2003, όλα τα πρωτόκολλα της IETF θα υποστηρίζουν το AES, αν και θα συνεχίσουν να παρέχουν υποστήριξη για τα παλαιότερα πρότυπα DES/3DES για λίγο καιρό ακόμη.

Servers Ψηφιακών Πιστοποιητικών

Όπως είδατε στην ενότητα που ασχολήθηκε με τα δημόσια και ιδιωτικά κλειδιά κρυπτογράφησης, ένα ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί για την δημιουργία μιας μοναδικής ψηφιακής υπογραφής. Η υπογραφή αυτή μπορεί κατόπιν να επαληθεύεται με το δημόσιο κλειδί, για να διασφαλίζεται η αυθεντικότητα της. Η διαδικασία αυτή παρέχει μία πολύ ισχυρή μέθοδο πιστοποίησης της ταυτότητας ενός χρήστη. Ένας server ψηφιακών πιστοποιητικών (digital certificate server) παρέχει ένα κεντρικό σημείο διαχείρισης πολλαπλών δημόσιων κλειδιών. Έτσι, ο κάθε χρήστης δεν είναι υποχρεωμένος να διατηρεί και να διαχειρίζεται αντίγραφα των δημόσιων κλειδιών κάθε άλλου χρήστη. Για παράδειγμα, ένας server στον οποίο τρέχει το λογισμικό Lotus Notes μπορεί να λειτουργήσει σαν διακομιστής ψηφιακών πιστοποιητικών, επιτρέποντας στους χρήστες να υπογράφουν μηνύματα χρησιμοποιώντας τα ιδιωτικά τους κλειδιά. Κατά την παράδοση του μηνύματος, ο server πληροφορεί τον παραλήπτη εάν το Lotus Notes μπόρεσε να πιστοποιήσει την ψηφιακή υπογραφή.

Οι servers ψηφιακών πιστοποιητικών γνωστοί επίσης και σαν φορείς παροχής/ελέγχου πιστοποιητικών (certificate authorities, CA), παρέχουν υπηρεσίες πιστοποίησης των ψηφιακών υπογραφών. Για παράδειγμα, εάν ο Χρήσης Α λάβει ένα ψηφιακά υπογεγραμμένο μήνυμα από τον Χρήστη Β αλλά δεν έχει ένα αντίγραφο του δημόσιου κλειδιού κρυπτογράφησης του Χρήστη Β, ο Χρήστης Α μπορεί να αποκτήσει ένα αντίγραφο του δημόσιου κλειδιού του Χρήστη Β από το server ψηφιακών πιστοποιητικών για να επιβεβαιώσει την αυθεντικότητα του μηνύματος. Ας υποθέσουμε επίσης ότι ο Χρήστης Α θέλει αν απαντήσει στο μήνυμα του Χρήστη Β, αλλά θέλει να κρυπτογραφήσει το μήνυμα του για να το προστατέψει από τα αδιάκριτα μάτια. Ο Χρήστης Α μπορεί και πάλι να αποκτήσει ένα αντίγραφο του δημόσιου κλειδιού του Χρήστη Β από τον server ψηφιακών πιστοποιητικών, έτσι ώστε να μπορέσει να κρυπτογραφήσει το μήνυμα του χρησιμοποιώντας το δημόσιο κλειδί του Χρήστη Β. Οι servers ψηφιακών πιστοποιητικών μπορούν επίσης να χρησιμοποιούνται σαν ένας κεντρικός μηχανισμός για την σύνδεση και τον έλεγχο της πρόσβασης των χρηστών. Τα ψηφιακά πιστοποιητικά μπορούν να αντιστοιχίζονται σε λίστες ελέγχου πρόσβασης οι οποίες θα εφαρμόζονται για τα αρχεία που αποθηκεύονται σ' έναν server. Όταν ένας χρήστης προσπαθήσει να προσπελάσει ένα τέτοιο αρχείο, ο server ελέγχει μέσω του πιστοποιητικού ότι ο χρήστης έχει τα κατάλληλα δικαιώματα πρόσβασης. Αυτό επιτρέπει σ' έναν server ψηφιακών πιστοποιητικών να διαχειρίζεται σχεδόν στην ολότητα της την ασφάλεια των εγγράφων ενός οργανισμού.

Η χρήση ενός συστήματος παροχής/ελέγχου ψηφιακών πιστοποιητικών το οποίο υποστηρίζει το X.509 - ένα καθιερωμένο πρότυπο για τα ψηφιακά πιστοποιητικά - είναι ακόμη πιο επωφελής υπό το πρίσμα της ασφάλειας. Ένα τέτοιο σύστημα επιτρέπει την επαλήθευση των πιστοποιητικών και την κρυπτογράφηση των πληροφοριών που διακινούνται μεταξύ οργανισμών. Εάν η βασική μέθοδος ανταλλαγής πληροφοριών μεταξύ δύο domain είναι το ηλεκτρονικό ταχυδρομείο, ένα σύστημα παροχής/ελέγχου ψηφιακών πιστοποιητικών μπορεί να είναι πολύ πιο αποτελεσματικό σε σχέση με το κόστος από το να επενδύσετε σ' ένα εικονικό ιδιωτικό δίκτυο (VPN).

Το IPSEC (IP Security)

Το IP Security (IPSEC) είναι μία ομάδα πρωτοκόλλων τα οποία αναπτύχθηκαν από την IETF για την υποστήριξη της κρυπτογράφησης και πιστοποίησης δεδομένων στο επίπεδο του πρωτοκόλλου IP του μοντέλου αναφοράς OSI. Για τον λόγο αυτό αποτελεί μία πολύ σημαντική τεχνολογία για την υλοποίηση εικονικών ιδιωτικών δικτύων. Το IPSEC περιλαμβάνει τα ακόλουθα πρωτόκολλα:

AH (Authentication Header) Το πρωτόκολλο αυτό χρησιμοποιείται για την πιστοποίηση και την επικύρωση των πακέτων με άλλα λόγια, για την ψηφιακή υπογραφή κάθε πακέτου. Ο υπολογιστής προορισμού μπορεί να επαληθεύσει όχι μόνο την ταυτότητα του αποστολέα του μηνύματος, αλλά και την ακεραιότητα των δεδομένων δηλαδή, μπορεί να επαληθεύσει ότι τα δεδομένα που λαμβάνονται δεν έχουν αλλοιωθεί, είτε λόγω προβλημάτων στην επικοινωνία, είτε σκόπιμα από έναν εισβολέα.

ESP (Encapsulating Security Protocol) Αυτό το πρωτόκολλο κρυπτογραφεί τον τομέα δεδομένων ενός πακέτου, έτσι ώστε μόνο ο αποστολέας και ο παραλήπτης να γνωρίζουν το περιεχόμενο του.

Ipcomp (IP payload compression) Το πρωτόκολλο IPcomp συμπιέζει τα δεδομένα πριν τα παραδώσει στο ESP, για μεγαλύτερη αποτελεσματικότητα.

IKE (Internet Key Exchange) Επειδή τα πρωτόκολλα AH και ESP χρησιμοποιούν ιδιωτικά/δημόσια κλειδιά για την παραγωγή και ανταλλαγή ενός συμμετρικού κλειδιού συνόδου (session key), το πρωτόκολλο IKE είναι αυτό που διαπραγματεύεται πώς θα λάβει χώρα αυτή η διαδικασία.

Το IpSEC λειτουργεί σε δύο καταστάσεις, τις transport (μεταφορά) και tunnel (σήραγγα, τούνελ). Η κατάσταση transport κρυπτογραφεί απλώς την επικοινωνία μεταξύ δύο υπολογιστών. Η κατάσταση tunnel, η οποία χρησιμοποιείται για την υποστήριξη των εικονικών ιδιωτικών δικτύων (VPN), ενθυλακώνει ολόκληρο το κρυπτογραφημένο πακέτο IP μέσα σ' ένα άλλο πακέτο IP, έτσι ώστε τα κρυπτογραφημένα δεδομένα να φτάνουν στον προορισμό τους μέσα από ένα εικονικό "τούνελ". Τα πρωτόκολλα AH και ESP μπορούν να λειτουργούν είτε σε κατάσταση transport, είτε σε κατάσταση tunnel.

Όταν υλοποιείτε το IPSEC θα πρέπει να δώσετε στο σύστημα σας τις κατάλληλες οδηγίες, έτσι ώστε να ξέρει ποια πακέτα πρόκειται να χειρίζεται το IPSEC. Για τον σκοπό αυτό θα πρέπει να καθορίσετε μία πολιτική για το IPSEC, η οποία εκφράζει απλώς την απόφαση σας σχετικά με το εάν το IPSEC θα εφαρμόζεται σ' έναν συγκεκριμένο τύπο πακέτων ή σε μία υπηρεσία συνολικά.

Σαν παράδειγμα, υποθέστε ότι ένας κανόνας στην πολιτική του IPSEC ισχύει για όλα τα πακέτα που στέλνονται σ' ένα συγκεκριμένο δίκτυο. Η προσέγγιση αυτή είναι πιο κοινή όταν χρησιμοποιείται ένας "ενήμερος" για το IPSEC router για την υλοποίηση μιας ασφαλούς σύνδεσης (πιθανώς μιας σύνδεσης VPN αλλά αυτό δεν είναι απαραίτητο) από ένα δίκτυο προς ένα άλλο. Σ' αυτή την περίπτωση κρυπτογραφούνται όλα τα πακέτα, ανεξάρτητα από την υπηρεσία ή τον σταθμό του δικτύου από τον οποίο προέρχονται, εφόσον προορίζονται για το συγκεκριμένο δίκτυο.

Εάν θέλετε να εγκαταστήσετε μία υπηρεσία ενήμερη για το IPSEC (π.χ. έναν server ηλεκτρονικού ταχυδρομείου), θα μπορούσατε επίσης να καθορίσετε ότι το IPSEC θα χειρίζεται όλα τα πακέτα που στέλνονται ή λαμβάνονται από μία συγκεκριμένη θύρα ανεξαρτήτως της προέλευσης ή του προορισμού τους. Σ' αυτή την περίπτωση λέγεται ότι η εφαρμογή του IPSEC γίνεται ανά server.

Επιπρόσθετα με την ευελιξία των λειτουργιών που εκτελεί το IPSEC, αυτό το πρότυπο προβλέπει επίσης την δυνατότητα χρήσης αλγόριθμων κρυπτογράφησης από τα πρωτόκολλα AH, ESP και IKE. Η δυνατότητα αυτή είναι ιδιαίτερα σημαντική εάν θέλετε να συνδυάσετε το IPSEC με άλλες λύσεις για την ασφάλεια, από διάφορους κατασκευαστές.

Kerberos

Το Kerberos είναι μία ακόμη λύση πιστοποίησης, ειδικά σχεδιασμένη ώστε να παρέχει ένα και μόνο σημείο "εισόδου" σ' ένα ετερογενές περιβάλλον. Το Kerberos επιτρέπει την

αμοιβαία πιστοποίηση και την κρυπτογράφηση της επικοινωνίας μεταξύ χρηστών και υπηρεσιών. Ωστόσο, ανόμοια με την χρήση "διαπιστευτηρίων" (tokens) ασφάλειας, το Kerberos βασίζεται στο γεγονός ότι κάθε χρήστης θα διατηρεί και θα θυμάται έναν μοναδικό κωδικό πρόσβασης.

Όταν ένας χρήστης πιστοποιείται στο λειτουργικό σύστημα του τοπικού υπολογιστή, μία ειδική υπηρεσία (agent) αυτού του συστήματος στέλνει μία αίτηση πιστοποίησης στον Kerberos server. Ο server ανταποκρίνεται στέλνοντας κρυπτογραφημένα τα διαπιστευτήρια του χρήστη που προσπαθεί να πιστοποιηθεί στο σύστημα. Κατόπιν η υπηρεσία αυτή προσπαθεί να αποκρυπτογραφήσει τα διαπιστευτήρια χρησιμοποιώντας τον παρεχόμενο από τον χρήστη κωδικό πρόσβασης. Εάν ο χρήστης παρέχει τον σωστό κωδικό πρόσβασης, πιστοποιείται και του παρέχονται τα κατάλληλα "εισιτήρια πιστοποίησης" (authentication tickets), τα οποία του δίνουν την δυνατότητα να προσπελάζει άλλες υπηρεσίες οι οποίες βασίζονται στην πιστοποίηση του Kerberos. Στον χρήστη δίνεται επίσης ένα σύνολο κλειδιών τα οποία μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση όλων των συνόδων μετάδοσης δεδομένων.

Μετά από την αρχική πιστοποίηση του χρήστη, δεν είναι απαραίτητο να πιστοποιηθεί ξανά η ταυτότητα του σε οποιουσδήποτε servers ή εφαρμογές υποστηρίζουν το kerberos. Τα "εισιτήρια" που παρέχει ο Kerberos server δίνουν στον χρήστη όλα τα διαπιστευτήρια που χρειάζεται για να προσπελάσει άλλους πόρους του δικτύου. Αν και ο χρήστης πρέπει να θυμάται τον κωδικό πρόσβασης του, χρειάζεται μόνο έναν κωδικό πρόσβασης για να προσπελάζει όλα τα συστήματα του δικτύου στα οποία του έχει παραχωρηθεί πρόσβαση. Ένα από τα μεγαλύτερα πλεονεκτήματα του kerberos είναι το γεγονός ότι διατίθεται ελευθέρα. Μπορείτε να μεταφέρετε τον πηγαίο κώδικα του και να τον χρησιμοποιήσετε χωρίς καμία επιβάρυνση. Υπάρχουν επίσης πολλές εμπορικές εφαρμογές, όπως το προϊόν Global Sign-On (GSO) της IBM, οι οποίες είναι συμβατές με το Kerberos αλλά διαθέτουν επιπλέον λειτουργίες και βελτιωμένο περιβάλλον διαχείρισης. Με την πάροδο του χρόνου ανακαλύφθηκαν ορισμένα τρωτά σημεία στην ασφάλεια του Kerberos, αλλά τα περισσότερα εξ αυτών (αν όχι όλα) διορθώθηκαν μέχρι την έκδοση kerberos V.

PPTP/L2TP

Ένα κεφάλαιο αφιερωμένο στις τεχνικές κρυπτογράφησης δεν θα μπορούσε να θεωρηθεί πλήρες χωρίς να κάνει τουλάχιστον μία αναφορά στα πρωτόκολλα PPTP (Point-to-Point Tunneling Protocol) και L2TP (Layer Two Tunneling Protocol). Δημιουργημένο από την Microsoft, το πρωτόκολλο PPTP χρησιμοποιεί πιστοποίηση βασιζόμενη στο πρωτόκολλο PPP (Point to Point Protocol, πρωτόκολλο για επικοινωνία από σημείο σε σημείο) και κρυπτογράφηση βασισμένη σε έναν αλγόριθμο της Microsoft. Η Microsoft ενσωμάτωσε υποστήριξη για το PPTP σε όλες τις εκδόσεις των Windows.

Ωστόσο, αν και αυτή η τεχνολογία συνέβαλλε στην γρήγορη και εύκολη υλοποίηση εικονικών ιδιωτικών δικτύων με προϊόντα της Microsoft, το PPTP δεν θεωρήθηκε ποτέ ασφαλές πρωτόκολλο. Σαν αποτέλεσμα, η Microsoft πήρε τα καλύτερα χαρακτηριστικά του PPTP και τα συνδύασε με τα καλύτερα χαρακτηριστικά του πρωτοκόλλου L2F (Layer Two Forwarding, προώθηση στο επίπεδο 2) της Cisco, δημιουργώντας το πρωτόκολλο L2TP (το οποίο υιοθετήθηκε αργότερα από την IETF). Το πρωτόκολλο L2TP μπορεί να χρησιμοποιεί το IPSEC για πιστοποίηση και κρυπτογράφηση, και επειδή οι υλοποιήσεις του IPSEC έχουν δυνατότητα επιλογής μεταξύ διάφορων αλγόριθμων, είναι πιο ευέλικτο (και πιο ασφαλές). Υπάρχει βέβαια ένα επιπλέον κόστος για την υλοποίηση και την συντήρηση του, λόγω του γεγονότος ότι το IPSEC βασίζεται στην χρήση δημόσιων κλειδιών.

Αλλά το L2TP μπορεί επίσης να λειτουργεί χωρίς το IPSEC σ' αυτή την κατάσταση χρησιμοποιεί τους μηχανισμούς πιστοποίησης και ελέγχου πρόσβασης του πρωτοκόλλου PPP - PAP (Password Authentication Protocol) και CHAP (Challenge Handshake Authentication Protocol), μαζί με το NCP (Network Control Protocol) - για τον χειρισμό της ανάθεσης διευθύνσεων IP σε απομακρυσμένους σταθμούς ενός VPN. (Στο τοπικό δίκτυο, ο σταθμός του VPN μπορεί να φαίνεται ότι έχει διεύθυνση IP από το ίδιο ή ένα συμπληρωματικό υπο-δίκτυο). Η υλοποίηση του L2TP από την Microsoft μπορεί επίσης

να χρησιμοποιείτο πρωτόκολλο EAP (το οποίο θα εξετάσουμε στην συνέχεια) για ακόμη πιο ευέλικτη και ισχυρή πιστοποίηση.

EAP (Extensible Authentication Protocol)

Το πρωτόκολλο EAP είναι μία επέκταση του PPP η οποία επιτρέπει την χρήση πολλαπλών μεθόδων πιστοποίησης, όπως για παράδειγμα κωδικοί πρόσβασης μιας χρήσης, πιστοποίηση δημόσιου κλειδιού (μέσω "έξυπνων" καρτών [smart cards]), Kerberos και RADIUS (δείτε την επόμενη ενότητα). Στην υλοποίηση του EAP, η Microsoft ενσωμάτωσε υποστήριξη για τόσο για το πρωτόκολλο CHAP, όσο και για το TLS (Transport Layer Security). Το TLS είναι ένα σχήμα αμοιβαίας πιστοποίησης (όπως και το Kerberos), το οποίο απαιτεί τόσο από τον server όσο και από τα client συστήματα να αποδεικνύουν την ταυτότητα τους (μέσω πιστοποιητικών) και αποτελεί μία επέκταση (και βελτίωση) του γνωστού SSL.

Remote Access Dial-In User Service (RADIUS)

Το RADIUS επιτρέπει σε πολλαπλές συσκευές απομακρυσμένης πρόσβασης να μοιράζονται την ίδια βάση δεδομένων με στοιχεία πιστοποίησης. Το RADIUS παρέχει ένα κεντρικό σημείο διαχείρισης για όλες τις μορφές απομακρυσμένης προσπέλασης ενός δικτύου. Όταν ένας χρήστης προσπαθεί να συνδεθεί σε έναν υπολογιστή ο οποίος χρησιμοποιεί τις υπηρεσίες ενός RADIUS server (π.χ. ένα σύστημα που παρέχει υπηρεσίες απομακρυσμένης πρόσβασης σε πολλαπλούς χρήστες), του ζητείται όνομα σύνδεσης και κωδικός πρόσβασης. Ο υπολογιστής προωθεί κατόπιν τα διαπιστευτήρια του χρήστη στον RADIUS server. Εάν τα διαπιστευτήρια είναι έγκυρα, ο server επιστρέφει μία καταφατική απάντηση και ο χρήστης αποκτά πρόσβαση στο δίκτυο. Εάν τα διαπιστευτήρια δεν ταιριάζουν με κάποια εγγραφή της βάσης δεδομένων, ο Radius server θα απαντήσει απορρίπτοντας την αίτηση, υποχρεώνοντας τον υπολογιστή να κλείσει την σύνδεση του χρήστη.

Στο παρελθόν, το Radius χρησιμοποιούνταν κυρίως για την απομακρυσμένη πρόσβαση σε ένα δίκτυο μέσω μόντεμ. Με την πάροδο του χρόνου άρχισε να απολαμβάνει ευρύτερης υποστήριξης από κατασκευαστές όπως οι 3COM, Cisco και Ascend. Το RADIUS άρχισε επίσης να γίνεται ευρέως αποδεκτό σαν μία μέθοδος πιστοποίησης των απομακρυσμένων χρηστών που προσπαθούν να προσπελάσουν το τοπικό δίκτυο μέσω ενός firewall. Υποστήριξη για το RADIUS έχει ενσωματωθεί σε προϊόντα firewall όπως το firewall-1 της Check Point και το PIX της Cisco.

Το μεγαλύτερο μειονέκτημα της χρήσης του RADIUS για την παροχή πρόσβασης σ' ένα δίκτυο μέσω firewall είναι ότι η προδιαγραφή του δεν περιλαμβάνει κρυπτογράφηση. Αυτό σημαίνει ότι αν και το RADIUS παρέχει έναν ισχυρό μηχανισμό πιστοποίησης, δεν έχει κανένα τρόπο για να διασφαλίσει την ακεραιότητα των δεδομένων αφού υλοποιηθεί η σύνοδος επικοινωνίας. Εάν χρησιμοποιήσετε πιστοποίηση μέσω RADIUS στο firewall, θα χρειαστείτε μία επιπλέον λύση για να παρέχετε δυνατότητα κρυπτογράφησης.

Κρυπτογράφηση RSA

Ο αλγόριθμος κρυπτογράφησης K5A δημιουργήθηκε από τους Ron Rivest, Adi Shamir και Leonard Adleman το 1977. Το RSA θεωρείται σαν το ντε φάκτο πρότυπο στην κρυπτογράφηση δημόσιου/ιδιωτικού κλειδιού: έχει ενσωματωθεί σε προϊόντα εταιρειών όπως οι Microsoft, Apple, Novell, Sun και Lotus. Σαν ένας μηχανισμός κρυπτογράφησης δημόσιου/ιδιωτικού κλειδιού, έχει επίσης δυνατότητα να εκτελεί πιστοποίηση.

Το γεγονός ότι ο αλγόριθμος RSA χρησιμοποιείται ευρύτατα είναι πολύ σημαντικό για όσους ενδιαφέρονται ιδιαίτερα το θέμα της συνεργασίας (interoperability) μεταξύ ανομοιογενών συστημάτων. Δεν μπορείτε να πιστοποιήσετε ή να αποκρυπτογραφήσετε ένα μήνυμα, εάν χρησιμοποιείτε έναν αλγόριθμο διαφορετικό από αυτόν που χρησιμοποιήθηκε για την δημιουργία του. Η επιλογή ενός προϊόντος που υποστηρίζει το RSA σας βοηθά να διασφαλίσετε ότι θα μπορείτε να ανταλλάσσετε πληροφορίες με πολύ περισσότερους χρήστες. Η μεγαλύτερη εγκατεστημένη βάση του RSA σημαίνει επίσης ότι ο αλγόριθμος αυτός έχει δοκιμαστεί, και άντεξε στον χρόνο. Αυτό είναι ένα πολύ

σημαντικό θέμα όταν καλείστε να επιλέξετε έναν αλγόριθμο για την προστασία των δεδομένων σας.

Αρχικός κάτοχος του αλγόριθμου κρυπτογράφησης RSA ήταν η RSA laboratiries, αλλά από τον Σεπτέμβριο του 2000 ο RSA είναι ελεύθερα διαθέσιμος. Αυτή η κίνηση εκ μέρους της RSA laboratories ενισχύει ακόμη περισσότερο την ήδη ισχυρή θέση του αλγόριθμου RSA και είναι σίγουρο ότι θα αυξήσει την παρουσία του σε διάφορα προϊόντα και υπηρεσίες.

Secure Shell (SSH)

Το Secure Shell (SSH) είναι μία ισχυρή μέθοδος για την πιστοποίηση των σταθμών του δικτύου και την ασφάλιση πολλαπλών συνόδων επικοινωνίας μεταξύ δύο συστημάτων. Γραμμένο από έναν Φιλανδό φοιτητή, το SSH απολαμβάνει ευρύτατης αποδοχής στον κόσμο του UNIX. Το ίδιο πρωτόκολλο έχει επίσης μεταφερθεί στις πλατφόρμες των Windows και OS/2.

Τα συστήματα που τρέχουν το SSH ακροάζονται στην θύρα 22 για εισερχόμενες αιτήσεις σύνδεσης. Οταν δύο συστήματα στα οποία τρέχει το SSH υλοποιήσουν μία σύνδεση μεταξύ τους, επαληθεύει το καθένα τα διαπιστευτήρια του άλλου εκτελώντας μία ανταλλαγή ψηφιακών πιστοποιητικών με την χρήση του RSA. Αφού επαληθευτούν τα διαπιστευτήρια των δύο υπολογιστών, χρησιμοποιείται το σύστημα Triple DES για την κρυπτογράφηση όλης της πληροφορίας που διακινείται μεταξύ των δύο συστημάτων. Τα δύο συστήματα πιστοποιούν το ένα την ταυτότητα του άλλου κατά την εξέλιξη της επικοινωνίας τους και περιοδικά αλλάζουν κλειδιά κρυπτογράφησης. Αυτό διασφαλίζει σε μεγάλο βαθμό ότι οι επιθέσεις που βασίζονται σε ωμή βία ή σε πειρατεία συνόδων δεν θα μπορούν να είναι αποτελεσματικές.

Το πρωτόκολλο SSH είναι μία θαυμάσια μέθοδος για την "θωράκιση" των πρωτοκόλλων που είναι γνωστό ότι δεν είναι ασφαλή. Για παράδειγμα, τα telnet και FTP ανταλλάσσουν όλες τις πληροφορίες πιστοποίησης σε μορφή απλού κειμένου. Το SSH μπορεί να "ενθυλακώσει" αυτές τις συνόδους επικοινωνίας για να διασφαλίσει ότι οι μεταδιδόμενες πληροφορίες δεν θα είναι ποτέ ορατές σαν απλό κείμενο.

Secure Sockets Layer (SSL)

Δημιουργημένο από την εταιρεία Netscape, το πρωτόκολλο Secure Sockets Layer (SSL) παρέχει κρυπτογράφηση RSA στο επίπεδο συνόδου του μοντέλου OSI. Παρέχοντας κρυπτογράφηση στο επίπεδο συνόδου, το πρωτόκολλο SSL έχει την δυνατότητα να είναι ανεξάρτητο από την υπηρεσία. Αν και το SSL δουλεύει εξίσου καλά με το FTP, το http, ή ακόμη και το telnet, η βασική χρήση του είναι για την θωράκιση των Web servers που χρησιμοποιούνται για ηλεκτρονικό εμπόριο (e-commerce). Επειδή ο αλγόριθμος RSA εκτελεί κρυπτογράφηση δημόσιου/ιδιωτικού κλειδιού, υποστηρίζονται επίσης τα ψηφιακά πιστοποιητικά. Αυτό επιτρέπει την πιστοποίηση του server και, προαιρετικά, του client συστήματος. Η Netscape περιλαμβάνει το SSL στα βασικά προϊόντα της (την εφαρμογή Web browser και τα προϊόντα Web server. Η Netscape διαθέτει ελεύθερα τον πηγαίο κώδικα του SSL έτσι ώστε να μπορέσει να προσαρμοστεί και σε άλλες πλατφόρμες Web server. Οποιοσδήποτε αναπτύσσει μία ιστοσελίδα μπορεί να καθορίσει ότι για την ανάκτηση της από τον server θα απαιτείται σύνδεση μέσω του SSL για όλες τις εφαρμογές Web browser. Αυτή η δυνατότητα επιτρέπει την διεξαγωγή online εμπορικών συναλλαγών με σχετικά ασφαλή τρόπο.

Το SSL δημιουργήθηκε από την Netscape, η οποία πέρασε κατόπιν αυτό το πρότυπο στην ομάδα IETF. Η IETF δημιούργησε το TLS (Transport Layer Security) από το SSL, διατηρώντας ταυτόχρονα "συμβατότητα προς τα πίσω". Σαν αποτέλεσμα, το HTTPS (Hypertext Transfer Protocol Secure) υποστηρίζει τόσο το SSL, όσο και το TLS.

Συσκευές Ασφάλειας

Οι συσκευές ασφάλειας (security tokens) είναι συσκευές παραγωγής κωδικών πρόσβασης οι οποίες μπορούν να χρησιμοποιούνται για την πρόσβαση σε τοπικά συστήματα ή υπηρεσίες του δικτύου. Από φυσικής απόψεως είναι μικρές συσκευές με μία LCD οθόνη η οποία παρουσιάζει τον τρέχοντα κωδικό πρόσβασης και το χρονικό διάστημα που απομένει μέχρι να λήξει. Αφού λήξει ο τρέχων κωδικός πρόσβασης,

παράγεται ένας νέος. Αυτό παρέχει υψηλό βαθμό ασφάλειας κατά την πιστοποίηση, δεδομένου ότι ακόμη κι αν υποκλαπεί ένας κωδικός πρόσβασης, έχει πολύ μικρή διάρκεια ζωής. Η Εικόνα 6.7 παρουσιάζει δείγματα τέτοιων συσκευών της εταιρείας Security Dynamics Technologies. Οι συσκευές αυτές αναφέρονται σαν κάρτες SecureID.

ΕΙΚΟΝΑ 6.7: Συσκευές ασφάλειας της Security Dynamics Technologies.

Οι συσκευές ασφάλειας δεν πιστοποιούν απευθείας τον χρήστη σ' ένα λειτουργικό σύστημα ή μία εφαρμογή. Απαιτείται μία ειδική υπηρεσία (agent) για να ανακατευθύνει την αίτηση σύνδεσης σε έναν διακομιστή πιστοποίησης. Για παράδειγμα το FireWall-1 υποστηρίζει πιστοποίηση μέσω καρτών SecureID. Οταν ένας χρήστης θέλει να προσπελάζει από το Internet υπηρεσίες του εσωτερικού δικτύου τις οποίες προστατεύει το FireWall-1, μπορεί να χρησιμοποιήσει μία κάρτα SecureID για να πιστοποιήσει την ταυτότητα του στο firewall. Το FireWall-1 δεν χειρίζεται μόνο του την πιστοποίηση· αντίθετα, μία ειδική υπηρεσία (agent) που τρέχει στο firewall προωθεί την αίτηση σύνδεσης σε έναν διακομιστή πιστοποίησης καρτών SecureID γνωστό με τον όρο ACE/Server. Εάν τα διαπιστευτήρια είναι έγκυρα, η επικύρωση τους επιστρέφεται στην ειδική υπηρεσία (agent) μέσω κρυπτογραφημένης συνόδου επικοινωνίας και ο χρήστης αποκτά πρόσβαση στο εσωτερικό δίκτυο.

Κάθε συσκευή ασφάλειας προσδιορίζεται με έναν κωδικό αριθμό. Ο κωδικός αυτός προσδιορίζει με μονοσήμαντο τρόπο κάθε συσκευή ασφάλειας στον server. Επίσης, ο κωδικός αυτός χρησιμοποιείται για την τροποποίηση του αλγόριθμου παραγωγής όλων των κωδικών πρόσβασης της συσκευής, έτσι ώστε να μην παράγεται η ίδια ακολουθία κωδικών πρόσβασης από πολλαπλές συσκευές. Επειδή οι κωδικοί πρόσβασης λήγουν σε τακτά χρονικά διαστήματα (συνήθως 60 δευτερόλεπτα), η συσκευή πρέπει να συγχρονιστεί αρχικά με τον διακομιστή πιστοποίησης.

Υπάρχουν αρκετά πλεονεκτήματα σ' αυτό το είδος πιστοποίησης. Κατ' αρχήν, οι χρήστες δεν είναι πλέον υποχρεωμένοι να θυμούνται κωδικούς πρόσβασης. Διαβάζουν απλώς τον τρέχοντα κωδικό πρόσβασης από την συσκευή τους και τον χρησιμοποιούν για την πιστοποίηση τους. Προφανώς, σ' αυτή την περίπτωση οι χρήστες δεν είναι υποχρεωμένοι να αλλάζουν τους κωδικούς τους σε τακτά χρονικά διαστήματα, επειδή η εργασία αυτή γίνεται αυτόματα από την συσκευή. Επίσης, οι πιθανότητες ανταλλαγής κωδικών πρόσβασης μεταξύ των χρηστών ελαχιστοποιούνται, επειδή κάθε χρήστης είναι υποχρεωμένος να χρησιμοποιεί την συσκευή του σε κάθε απόπειρα πιστοποίησης που κάνει. Ακόμη κι αν ο χρήστης πει προφορικά τον κωδικό πρόσβασης που εμφανίζει η έξυπνη κάρτα του σε ένα άλλο άτομο, οι συνέπειες θα είναι μικρές επειδή ο κωδικός πρόσβασης είναι έγκυρος μόνο για ένα πολύ μικρό χρονικό διάστημα.

Οι συσκευές ασφάλειας είναι ένας θαυμάσιος τρόπος για να παρέχετε υπηρεσίες πιστοποίησης. Η μόνη αδυναμία τους είναι ότι δεν παρέχουν καμία μορφή κρυπτογράφησης. Βασίζονται στο υποκείμενο λειτουργικό σύστημα ή στην υποκείμενη εφαρμογή για την παροχή αυτής της δυνατότητας. Αυτό σημαίνει ότι τα δεδομένα της πιστοποίησης θα μπορούσαν να διαβαστούν σαν απλό κείμενο εάν ένας εισβολέας υποκλέψει μία σύνοδο επικοινωνίας telnet. Ωστόσο, η περιορισμένη διάρκεια ζωής οποιουδήποτε κωδικού πρόσβασης δυσχεραίνει σημαντικά την εκμετάλλευση αυτής της πληροφορίας, ακόμη κι αν υποκλαπεί.

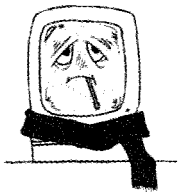
SKIP (Simple Key Management for Internet Protocols)

Το πρωτόκολλο SKIP (Simple Key Management for Internet Protocols) είναι παρόμοιο με το SSL στο ότι λειτουργεί στο επίπεδο συνόδου του μοντέλου OSI. Όπως ισχύει και με το SSL, το χαρακτηριστικό αυτό δίνει στο SKIP την δυνατότητα να υποστηρίζει υπηρεσίες του IP, ανεξάρτητα από το εάν αυτές υποστηρίζουν κρυπτογράφηση. Αυτό είναι εξαιρετικά χρήσιμο όταν θέλετε να τρέχετε πολλαπλές υπηρεσίες του IP μεταξύ δύο υπολογιστών.

Το χαρακτηριστικό που καθιστά το SKIP μοναδικό είναι ότι δεν απαιτεί την ύπαρξη πρότερης επικοινωνίας για τον ορισμό ή την ανταλλαγή κλειδιών σε βάση σύνοδο προς σύνοδο. Ο αλγόριθμος δημόσιου/ιδιωτικού κλειδιού των Diffie-Hellman χρησιμοποιείται για την παραγωγή ενός "μυστικού" το οποίο μοιράζονται τα δύο συμβαλλόμενα μέρη. Αυτό το "κοινό μυστικό" χρησιμοποιείται για να παρέχει κρυπτογράφηση και πιστοποίηση στο επίπεδο των πακέτων IP. Αν και το SKIP είναι εξαιρετικά αποτελεσματικό στην κρυπτογράφηση δεδομένων, πράγμα το οποίο θα βελτίωνε την απόδοση ενός εικονικού ιδιωτικού δικτύου, βασίζεται στην μακροπρόθεσμη προστασία του "κοινού μυστικού" για την διατήρηση της ακεραιότητας κάθε συνόδου. Το SKIP δεν παράγει συνεχώς νέες τιμές κλειδιών όπως το SSH. Αυτό καθιστά ευάλωτη την κρυπτογράφηση του SKIP, εάν τα κλειδιά δεν προστατεύονται σωστά.

Κεφάλαιο 7

Προτεινόμενη Μεθοδολογία Βελτίωσης της Ασφάλειας



Η ύπαρξη ασφάλειας στο intranet και το extranet απαιτεί την δημιουργία εμποδίων στην φυσική προσπέλαση του εξοπλισμού, το δίκτυο, αλλά και τις εφαρμογές. Τι είναι όμως αυτό που θέλουμε να διαφυλάξουμε; Μία γενική απάντηση της μορφής «τον οργανισμό ή εταιρία μου από αυτούς που θέλουν να χρησιμοποιήσουν την τεχνολογία για να κάνουν κακό», αφήνει περιθώρια για μία μόνο λύση στο πρόβλημα: μην χρησιμοποιείτε υπολογιστές. Αυτή την στιγμή δεν υπάρχει 100% ασφαλές σύστημα προστασίας ενός intranet ή extranet. Μάλιστα όσο πλησιάζουμε προς την απόλυτη ασφάλεια το ίδιο ασυμπτωτικά διογκώνεται το κόστος για την δημιουργία ενός τέτοιου συστήματος ασφάλειας.

Για να είναι εφικτή μια υλοποίηση, δηλαδή το κόστος υλοποίησης του συστήματος ασφάλειας να είναι μικρότερο από το κόστος μιας επίθεσης, πρέπει να γίνουν μία σειρά από ενέργειες που έχουν σκοπό την ανάλυση, τον σχεδιασμό, την υλοποίηση και την λειτουργία του συστήματός μας, για την αντιμετώπιση περιστατικών επιθέσεων.

Έτσι Χρειάζεται:

- Να γίνει ανάλυση των κινδύνων που έχουμε να αντιμετωπίσουμε και καταγραφή των πόρων που πρέπει να διαφυλάξουμε,
- να προσδιοριστεί η πολιτική ασφάλειας που θα εφαρμόσουμε,
- να σχεδιάσουμε την αρχιτεκτονική του υπολογιστικού και πληροφοριακού συστήματος που θα αναπτύξουμε,
- να αποφασίσουμε για τις υπηρεσίες ασφάλειας που θα υιοθετήσουμε για την προστασία του intranet/extranet,
- να γνωρίζουμε τα εργαλεία και τις μεθόδους επιθέσεων καθώς και τα αντίμετρα που πρέπει να εφαρμόζονται,
- να έχουμε σχεδιάσει τον τρόπο αντιμετώπισης ενός περιστατικού επίθεσης

- να ενημερώνουμε τους χρήστες μας
- να είμαστε πάντα ενήμεροι για τα τελευταία νέα σε θέματα ασφάλειας παρακολουθώντας λίστες και ανακοινώσεις κατασκευαστών υπολογιστικών συστημάτων, οργανισμών ασφάλειας, χρηστών, ακόμα και hackers.

Για να έχουμε ένα ικανοποιητικό επίπεδο ασφάλειας πρέπει να αναλύσουμε τα παραπάνω για να ικανοποιήσουμε την ύπαρξη έξι βασικών σημείων της ασφάλειας :

1. Την εμπιστευτικότητα της πληροφορίας: διασφαλίζοντας πως η πληροφορία είναι προσπελάσιμη από τους σωστούς χρήστες (π.χ. τα σχέδια για το νέο προϊόν είναι προσπελάσιμα σε ορισμένους μόνο χρήστες)
2. Την πιστοποίηση αυθεντικότητας: επαληθεύοντας την αυθεντικότητα ενός χρήστη ή υπολογιστικού συστήματος (π.χ. πως είναι πράγματι ο χρήστης που ζητά προσπέλαση)
3. Την αποφυγή άρνησης πράξεων: εξασφαλίζοντας πως οι χρήστες δεν μπορούν να αρνηθούν τις ηλεκτρονικές πράξεις τους (π.χ. ότι αντέγραφαν ένα αρχείο)
4. Την ακεραιότητα των δεδομένων: διασφαλίζοντας πως τα δεδομένα δεν έχουν αλλάξει και είναι τα ίδια με αυτά που αρχικά τοποθετήθηκαν (π.χ. τα περιεχόμενα της μελέτης δεν έχουν αλλάξει από κάποιο τρίτο)
5. Τον έλεγχο προσπέλασης: διασφαλίζοντας πως οι πόροι βρίσκονται κάτω από τον αποκλειστικό έλεγχο εξουσιοδοτημένων χρηστών, βεβαιώνοντας πως ο χρήστης που ζητά την προσπέλαση έχει την άδεια να το κάνει (π.χ. η αλλαγή στο αρχείο ενός υπαλλήλου επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα)
6. Την διαθεσιμότητα των πόρων: εξασφαλίζοντας πως τα δεδομένα οι υπηρεσίες και οι εξυπηρετητές είναι διαθέσιμα όποτε ζητηθούν (π.χ. άμεση αποκατάσταση δεδομένων και υπηρεσιών μετά από επίθεση).

7.1. Αποτίμηση κινδύνων

Γενικά

Είναι πολύ σημαντικό να καταλάβουμε πως στην υλοποίηση της ασφάλειας δεν μπορεί κανείς να κάνει την ερώτηση «ποιο είναι το καλύτερο firewall, να το εγκαταστήσω». Υπάρχουν δύο άκρα: απόλυτη ασφάλεια και απόλυτη ελευθερία πρόσβασης. Μία καλή προσέγγιση προς την απόλυτη ασφάλεια έχουμε όταν ο υπολογιστής μας δεν είναι συνδεμένος με το δίκτυο, δεν είναι συνδεμένος στο ηλεκτρικό ρεύμα, είναι κλειστός, κλειδωμένος σε ένα χρηματοκιβώτιο, κτισμένο με τεράστιες ποσότητες τσιμέντου σε πολύ μεγάλο βάθος, με μοναδική είσοδο που φυλάσσεται από ακριβοπληρωμένους φρουρούς. Δυστυχώς έτσι δεν είναι και τόσο χρήσιμος.

Από την άλλη πλευρά ένας υπολογιστής με πλήρη ελευθερία πρόσβασης είναι μεν τρομερά εύχρηστος, αλλά μπορεί να καταλήξει άχρηστος αφού χωρίς κανόνες χρήσης ο καθένας μπορεί να κάνει ότι θέλει καταστρέφοντας την λειτουργικότητά του είτε εσκεμμένα, είτε από άγνοια.

Οι περισσότεροι άνθρωποι έχουν μία εικόνα για το ανεκτό επίπεδο κινδύνου για κάθε ενέργειά τους (όσο και αν είναι προσιτό δεν πηδάμε από το παράθυρο του σπιτιού μας για να κατέβουμε γρήγορα στο δρόμο να προλάβουμε το λεωφορείο για την δουλειά, ενώ μπορεί να το επιχειρήσουμε αν κινδυνεύει η ζωή μας).

Ο κάθε οργανισμός λοιπόν πρέπει να αποφασίσει για τα συστήματά του, το σημείο που χρειάζεται να βρίσκεται, ανάμεσα στην απόλυτη ασφάλεια και την απόλυτη ευκολία προσπέλασης. Μία πολιτική ασφάλειας πρέπει να προσδιορίσει τους πόρους που έχουν αξία για τον οργανισμό, τις πιθανές απειλές και κατόπιν να προτείνει ων κατάλληλη πολιτική ασφάλειας για το πως θα διασφαλιστούν οι πόροι από τις πιθανές απειλές.

Προσδιορισμός των πόρων

Είναι σημαντικό να προσδιοριστούν όλοι οι πόροι που θα πρέπει να προστατευθούν. Η κατηγοριοποίηση των πόρων που θα προστατευθούν έχει ως εξής :

- Υλικό: Κεντρική Μονάδα Επεξεργασίας, τερματικοί σταθμοί εργασίας, προσωπικοί υπολογιστές, εκτυπωτές, δίσκοι, γραμμές επικοινωνίας, εξυπηρετητές, δρομολογητές.
- Λογισμικό: Πηγαίος κώδικας, αντικείμενος κώδικας, εργαλεία, διαγνωστικά προγράμματα, λειτουργικά συστήματα, προγράμματα επικοινωνίας.
- Δεδομένα: Αρχειοθετημένα off-line, αποθηκευμένα on-line, κατά την διάρκεια ως επεξεργασίας τους, αντίγραφα ασφαλείας.
- Ανθρώπινο δυναμικό: Χρήστες, διαχειριστές, τεχνικοί κ.λπ.
- Τεκμηρίωση: Προγραμμάτων, υλικού, συστημάτων, τοπικών διαδικασιών διαχείρισης.
- Υλικό Υποστήριξης: Δημοσιεύσεις, φόρμες, μαγνητικά μέσα κ.α.

Προσδιορισμός των απειλών

Αφού καταγραφούν οι πόροι που πρέπει να προστατευτούν θα πρέπει να προσδιοριστούν πιθανές απειλές τους. Κλασικές απειλές που μπορεί να δεχθεί ένα σύστημα είναι οι ακόλουθες:

- Σκόπιμη απειλή (Hacking, Denial of Service, κατασκοπία)
- Απροσχεδίαστη απειλή (π.χ. λανθασμένη αποστολή με mail κρίσιμων στοιχείων σε μια ομάδα αποδεκτών)
- Φυσικές περιβαλλοντικές απειλές (σεισμός)
- Μη φυσικές απειλές (εμπρησμός, διακοπή ρεύματος)
- Μη εξουσιοδοτημένη προσπέλαση των μέσων και / ή της πληροφορίας.
- Αγνώστου ταυτότητας και / ή μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας.
- Κατάργηση / άρνηση των προσφερόμενων υπηρεσιών.

Η εμπιστοσύνη παίζει σημαντικό ρόλο στην υλοποίηση της πολιτικής ασφάλειας. Το πρώτο βήμα είναι να αποφασιστεί ποιος έχει προσπέλαση, σε ποιους πόρους, τι είδους (διαχειριστή, απλού χρήστη, χειριστή) και να περιγραφεί το μοντέλο υλοποίησης με ομάδες χρηστών.

7.2. Πολιτική ασφάλειας

Τι είναι πολιτική ασφάλειας και γιατί πρέπει να έχω

Η πολιτική ασφάλειας είναι το σύνολο των κανόνων που ρυθμίζουν την πρόσβαση που έχει κάθε χρήστης στα πληροφοριακά συστήματα ενός οργανισμού.

Χωρίς την ύπαρξη πολιτικής ασφάλειας δεν υπάρχει ένα γενικό πλαίσιο για την ασφάλεια. Με την πολιτική ορίζουμε ποια συμπεριφορά είναι επιτρεπόμενη μέσα στον οργανισμό ως προς την χρήση των προσφερόμενων υπηρεσιών, μέσα από διαδικασίες που πρέπει να ακολουθηθούν από όλους.

Η πολιτική ασφάλειας είναι μία καλή μέθοδος για την δημιουργία συναντίληψης ανάμεσα στα στελέχη του οργανισμού.

Οι χρήστες ανημετωπίζουν τις πολιτικές σαν ένα φρένο της παραγωγικότητας ή ένα τρόπο να ελέγχεται η συμπεριφορά των εργαζομένων, αρνούμενοι να υποκύψουν στην παρακολούθηση (σύνδρομο του Μεγάλου Αδελφού).

Προσδιορισμός της πολιτικής ασφάλειας

Οι αποφάσεις που λαμβάνονται για την ασφάλεια ενός δικτύου από τον διαχειριστή του, καθορίζουν το πόσο ασφαλές είναι ένα δίκτυο καθώς και την ευκολία στη χρήση του.

Καταρχήν θα πρέπει να αποφασιστεί τι είναι σκόπιμο να διαφυλαχτεί.

Όταν γίνει αυτό θα πρέπει να οριστούν οι περιορισμοί που θα πρέπει να τεθούν ώστε να έχουμε το επιθυμητό αποτέλεσμα.

Οι στόχοι καθορίζονται από τους ακόλουθους παράγοντες:

1. Προσφερόμενες υπηρεσίες σε σχέση με την ασφάλεια του δικτύου. Υπάρχουν περιπτώσεις που η χρήση κάποιων υπηρεσιών αυξάνει τον κίνδυνο για την άρση της ασφάλειας ενός δικτύου, με αποτέλεσμα το κόστος των υπηρεσιών αυτών να είναι μεγαλύτερο από τα οφέλη τους. Σε τέτοιες περιπτώσεις είναι προτιμότερη η κατάργηση της υπηρεσίας.
2. Ευκολία χρήσης σε σχέση με τη προσφερόμενη ασφάλεια. Το ευκολότερο σύστημα στη χρήση είναι αυτό που προσφέρει άμεση πρόσβαση χωρίς την ύπαρξη συνθηματικών. Παρόλα αυτά ένα τέτοιο σύστημα δεν προσφέρει καμία απολύτως ασφάλεια. Με την χρήση συνθηματικών (password) το σύστημα γίνεται λίγο πιο δύσκολο αφού κάθε χρήστης θα πρέπει να θυμάται τον κωδικό του, αλλά ταυτόχρονα γίνεται και πιο ασφαλές.
3. Κόστος ασφάλειας ενάντια στον κίνδυνο απώλειας. Υπάρχουν διάφορα είδη που προσδιορίζουν το κόστος της ασφάλειας όπως :

- Κόστος αγοράς υλικού ή λογισμικού, όπως firewalls και on-time password generators
- Απόδοση (η κωδικοποίηση και η αποκωδικοποίηση χρειάζονται κάποιο χρόνο) καθώς και ευκολία στην χρήση.

- Υπάρχουν επίσης διάφορα επίπεδα κινδύνου όπως :
    - Άρση του απορρήτου (π.χ. ανάγνωση πληροφορίας από τρίτους),
    - Απώλεια δεδομένων (διαγραφή δεδομένων) ή
    - Απώλεια υπηρεσιών (χρήση των πηγών του δικτύου, άρνηση πρόσβασης στο δίκτυο κ.α.).

Για την υλοποίηση της ασφάλειας του δικτύου θα πρέπει να ληφθούν υπόψη όλα τα παραπάνω.

Ποιοι θα εμπλακούν στον προσδιορισμό της πολιτικής

Μια πολιτική ασφάλειας για να είναι κατάλληλη για τον οργανισμό θα πρέπει να είναι αποδεκτή από όλους τους εργαζομένους. Επίσης θα πρέπει να υπάρχει υποστήριξη της πολιτικής και από τη διεύθυνση του οργανισμού ώστε να επιτύχει στους στόχους της. Οι ομάδες εργαζομένων που εμπλέκονται σε μια πολιτική ασφάλειας είναι:

- Απλοί χρήστες - η πολιτική ασφάλειας αφορά αυτούς ως επί το πλείστον
- Προσωπικό υποστήριξης - είναι αυτοί που θα υλοποιήσουν και θα υποστηρίξουν την πολιτική ασφάλειας
- Διοικητικό προσωπικό - καθορίζουν το βαθμό προστασίας των περισσότερων δεδομένων και αναλαμβάνουν το οικονομικό κόστος της πολιτικής που θα υλοποιηθεί
- Νομικοί σύμβουλοι - που ενδιαφέρονται για την φήμη και την νομική κάλυψη του οργανισμού

Τα συστατικά της καλής πολιτικής ασφάλειας

Μια πολιτική ασφάλειας θα πρέπει να είναι:

υλοποιήσιμη: Να υπάρχουν ρεαλιστικοί κανόνες διαχείρισης των συστημάτων για κάθε τμήμα του οργανισμού, οδηγίες χρήσης των διάφορων πόρων, εγκατεστημένα συστήματα ασφάλειας.

Θα πρέπει να ακολουθείται απ' όλους: Οι χρήστες θα πρέπει να κατανοήσουν πως δε γίνονται παρακάμψεις για τη διευκόλυνσή τους. Θα πρέπει οι ίδιοι να προσαρμόσουν τις καθημερινές δραστηριότητές τους στους κανόνες ασφάλειας. Δεν θα πρέπει όμως να είναι και υπερβολικά αυστηροί γιατί τότε οι χρήστες θα προσπαθούν να βρουν τρόπους για να ξεπεράσουν τους κανόνες.

Ευέλικτη: Για να είναι βιώσιμη μια πολιτική ασφάλειας θα πρέπει να εξαρτάται από το υλικό και το λογισμικό που υπάρχει, ώστε να μπορεί να αναπροσαρμόζει τους κανόνες της σύμφωνα με τις προδιαγραφές τους. Επίσης θα πρέπει να αναγνωρίζει τις εξαιρέσεις που είναι δυνατό να γίνουν στους κανόνες ασφάλειας ανάλογα με τις ανάγκες που θα παρουσιαστούν. Για παράδειγμα ο διαχειριστής ενός συστήματος μπορεί να χρειαστεί τον κωδικό πρόσβασης κάποιου χρήστη για ένα σύστημα.

Θα πρέπει να ισοσταθμίζει την προστασία του οργανισμού με την παραγωγικότητα. Αν οι κανόνες είναι πολύ αυστηροί οι χρήστες θα βρουν τρόπους να μην τους εφαρμόζουν. Οι τεχνικοί έλεγχοι δεν είναι πάντα εφικτοί.

Αναβαθμίσιμη: Οι κανόνες που τίθενται θα πρέπει να αναπροσαρμόζονται και να ακολουθούν την εξέλιξη του οργανισμού.

Την πολιτική ασφάλειας που θα εφαρμόσουμε πρέπει να έχουν την ευκαιρία να την σχολιάσουν και όσοι θα δεχτούν τις επιπτώσεις της. Πολλά παραδείγματα πολιτικής μπορούν να βρεθούν στις ιστοσελίδες:

http://www.eff.orglpub/CAF/policies
http://www.gatech.edu/itis/policy/usage/contents.html
http://csrc.ncsl.nisiogov/secplcy/

Κανόνες ασφάλειας

1. Κανόνες ασφάλειας για το δίκτυο

Η πολιτική ασφάλειας για το δίκτυο καθορίζει:

- Ποιος εγκαθιστά καινούριες συσκευές στο δικτυο
- Ποιος ειδοποιείται για κάθε τέτοια εγκατάσταση
- Πώς τεκμηριώνεται μια τέτοια αλλαγή
- Ποιες είναι οι αλλαγές στο «χάρτη» του δικτύου
- Ποιες οι νέες απαιτήσεις σε ασφάλεια
- Πώς αντιμετωπίζονται μη ασφαλείς συσκευές

2. Κανόνες ασφάλειας για την προστασία των δεδομένων

Η πολιτική ασφάλειας για την προστασία των δεδομένων - πληροφοριών του οργανισμού, καθορίζει:

- Επίπεδα κρισιμότητας των πληροφοριών που κυκλοφορούν
- Ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες
- Τα επίπεδα πρόσβασης σε τέτοιες πληροφορίες που έχουν οι ομάδες των χρηστών
- Πώς αποθηκεύεται και μεταδίδεται τέτοιου είδους πληροφορία
- Σε ποια συστήματα αποθηκεύεται τέτοια πληροφορία
- Σε ποια συστήματα εκτυπώνονται τέτοια δεδομένα

3. Κανόνες ασφάλειας των χρηστών
Η πολιτική ασφάλειας για τους χρήστες θα πρέπει να καθορίζει:

- Την ευθύνη των χρηστών για την προστασία των δεδομένων που έχουν στους προσωπικούς λογαριασμούς τους
- Αν οι χρήστες μπορούν διαβάζουν και να αντιγράφουν αρχεία που δεν τους ανήκουν αλλά έχουν πρόσβαση
- Αν οι χρήστες μπορούν να μεταβάλλουν αρχεία που δεν τους ανήκουν αλλά έχουν δικαίωμα εγγραφής σ' αυτά
- Αν οι χρήστες μπορούν να πάρουν αντίγραφα βασικών αρχείων (configuration files) από τα βασικά συστήματα του οργανισμού
- Αν οι χρήστες μπορούν να μοιράζουν αρχεία για κοινή χρήση
- Αν οι χρήστες μπορούν να δημιουργούν αντίγραφα νόμιμα αγορασμένου λογισμικού
- Το επίπεδο χρήσης του Mail, Web, News από τους χρήστες ή από ομάδες χρηστών

4. Κανόνες ασφάλειας των λογαριασμών των χρηστών
Η πολιτική ασφάλειας για τους λογαριασμούς των χρηστών θα πρέπει να καθορίζει:

- Ποιος έχει τη δικαιοδοσία να δέχεται αιτήσεις ανοίγματος λογαριασμών
- Ποιος επιτρέπεται να κάνει χρήση των πόρων του οργανισμού
- Αν οι χρήστες μοιράζονται το λογαριασμό τους με άλλους ή αν έχουν περισσότερους από έναν λογαριασμούς σε συστήματα του οργανισμού
- Τ α δικαιώματα και τις υπευθυνότητες των χρηστών για τη χρήση των πόρων που τους διατίθενται
- Πότε ο λογαριασμός ενός χρήστη απενεργοποιείται
- Τους κανόνες που ακολουθούν οι κωδικοί πρόσβασης των χρηστών

5. Κανόνες ασφάλειας για την απομακρυσμένη πρόσβαση
Η πολιτική ασφάλειας για την απομακρυσμένη πρόσβαση θα πρέπει να καθορίζει:

- Ποιος έχει το δικαίωμα της απομακρυσμένης πρόσβασης (Authentication)
- Ποιες είναι οι επιτρεπόμενες μέθοδοι για απομακρυσμένη πρόσβαση
- Αν επιτρέπονται dial-out modems
- Αν θα υπάρχει καταγραφή των χρηστών που χρησιμοποιούν την υπηρεσία αυτή
- Αν θα δίνεται η δυνατότητα για callback
- Σε ποια δεδομένα επιτρέπεται η απομακρυσμένη πρόσβαση

6. Διαδικασία Configuration Management
Η πολιτική ασφάλειας στη διαδικασία του configuration management καθορίζει:

- Πώς ελέγχεται και εγκαθίσταται καινούριο υλικό και λογισμικό στα συστήματα του οργανισμού
- Πώς τεκμηριώνονται οι αλλαγές σε υλικό και λογισμικό
- Ποιος ενημερώνεται για τυχόν αλλαγές σε υλικό και λογισμικό
- Ποιος έχει τη δικαιοδοσία να κάνει αλλαγές στο υλικό ή το λογισμικό των συστημάτων του οργανισμού
- Με ποια διαδικασία μπορεί να υπάρξει εξαίρεση σε ένα κανόνα για ορισμένο χρονικό διάστημα

- Πως γίνεται η διαχείριση των firewalls, πως ζητούνται αλλαγές και πως εγκρίνονται

7. Διαδικασία αντιμετώπισης προβλημάτων
Η πολιτική ασφάλειας στην περίπτωση που παρουσιαστεί κάποιο πρόβλημα (εισβολή) καθορίζει:

- Διαδικασία άμεσης υποστήριξης από εξειδικευμένο προσωπικό
- Τις πρώτες, άμεσες ενέργειες που πρέπει να γίνουν
- Τον τρόπο που θα αντιμετωπιστεί μια εισβολή
- Ποιες πληροφορίες θα πρέπει να καταγραφούν για να χρησιμοποιηθούν αργότερα
- Ποιος θα πρέπει να ενημερωθεί και πότε

8. Διαδικασία Backup
Η πολιτική ασφάλειας για τη διαδικασία του backup καθορίζει:

- Ποια είναι τα αρχεία τα οποία παίρνονται backup (αρχεία συστήματος, αρχεία χρηστών)
- Πόσο συχνά πραγματοποιείται η διαδικασία του backup
- Αν υπάρχει Disaster Recovery το όποιο είναι άμεσα εκτελέσιμο μετά από κάποια δυσλειτουργία.
- Που φυλάγονται τα μαγνητικά μέσα.

7.3. Ένα μοντέλο περιμετρικής ασφάλειας

Σχεδιασμός μοντέλου

Πλήρης προσδιορισμός των πλάνων ασφάλειας

Όλα τα sites θα πρέπει να καθορίζουν ένα περιεκτικό πλάνο ασφαλείας. Αυτό το πλάνο θα πρέπει να είναι σε ένα υψηλότερο επίπεδο από τις πολιτικές ασφαλείας που συζητούνται στο αντίστοιχο κεφάλαιο και θα πρέπει να κατασκευάζεται όπως ένα πλαίσιο γενικότερης κατεύθυνσης, στο οποίο θα ανήκουν οι ειδικές πολιτικές ασφαλείας.

Είναι σημαντικό να υπάρχει αυτό το πλαίσιο εργασίας, έτσι ώστε ξεχωριστές πολιτικές να μπορούν να συμφωνούν με την ολική αρχιτεκτονική ασφαλείας ενός site. Για παράδειγμα έχοντας μία σκληρή πολιτική και έχοντας ελευθερίες χρήσης για τα modems, έχουμε ασυμφωνία με την ολική φιλοσοφία του σκληρού περιορισμού.

Σε ένα πλάνο ασφαλείας θα πρέπει να ορίζονται η λίστα των δικτυακών υπηρεσιών που θα παρέχονται, ποιες περιοχές του οργανισμού θα παρέχουν την υπηρεσία, ποιος θα έχει πρόσβαση σε αυτή την υπηρεσία, ποιος θα διαχειρίζεται την υπηρεσία κλπ.

Για sites συνδεμένα στο Διαδίκτυο, η ανεξέλεγκτα μεγάλη χρήση του Διαδικτύου, και τα σχετικά με αυτή επεισόδια ασφαλείας μπορεί να επισκιάσουν ένα περισσότερο σοβαρό εσωτερικό πρόβλημα ασφαλείας. Ομοίως, οργανισμοί οι οποίοι δεν έχουν ποτέ συνδεθεί στο Διαδίκτυο, ενώ ενδέχεται να έχουν ισχυρές και καλά ορισμένες πολιτικές ασφαλείας, είναι δυνατό να σφάλουν στο να υιοθετήσουν μια επιτυχημένη πολιτική εξωτερικής διασύνδεσης.

Διαχωρισμός των υπηρεσιών

Υπάρχουν πολλές υπηρεσίες που μπορεί να προσφέρει ένα site στους χρήστες του. Κάποιες από αυτές μπορεί να είναι και εξωτερικές. Τόσο για λόγους ασφάλειας όσο και

για λόγους απόδοσης, συνιστάται κάθε υπηρεσία να «στήνεται» στο δικό της εξυπηρετητή.

Οι υπηρεσίες που παρέχονται από ένα site θα πρέπει να έχουν διαφορετικά επίπεδα προσπέλασης. Υπηρεσίες που είναι άμεσα συνδεδεμένες , την ασφάλεια του site θα πρέπει να βρίσκονται σε ξεχωριστούς hosts έχουν περιορισμένη πρόσβαση, και όχι σε συστήματα που φιλοξενούν υπηρεσίες που θα χρησιμοποιούνται από την πλειοψηφία των χρηστών.

Στο σημείο αυτό θα πρέπει να επισημάνουμε ότι οι εισβολείς δεν φέρονται τόσο για την ίδια την υπηρεσία (π.χ. ανάγνωση ηλεκτρονικού ταχυδρομείου) αλλά χρησιμοποιούν τις υπηρεσίες προκειμένου να αποκτήσουν πρόσβαση στους πόρους του συστήματος.

Επιλογή μοντέλου Deny all/Allow all

Υπάρχουν δυο διαμετρικά αντίθετες φιλοσοφίες που μπορούν να υιοθετηθούν κατά το σχεδιασμό της ασφάλειας ενός site. Η φιλοσοφία που θα ακολουθηθεί εξαρτάται από το site και τις ανάγκες του.

Στο πρώτο μοντέλο προτείνεται η κατάργηση όλων των υπηρεσιών και η επιλεκτική ενεργοποίηση τους ανάλογα με τις εκάστοτε ανάγκες. Το μοντέλο αυτό γνωστό σαν «deny all» είναι πιο ασφαλές αλλά και πιο δύσκολο στην εφαρμογή του. Για να εφαρμοστεί το μοντέλο αυτό απαιτείται γνώση των υπηρεσιών και των αντιστοίχων πρωτοκόλλων.

Το δεύτερο μοντέλο γνωστό σαν «allow all», είναι πολύ πιο εύκολο στην εφαρμογή του αλλά και λιγότερο ασφαλές από τον τύπο «deny all». Στο μοντέλο αυτό ενεργοποιούνται από την αρχή όλες οι υπηρεσίες και επιτρέπονται όλα τα πρωτόκολλα σε επίπεδο δικτύου. Ανάλογα με τα προβλήματα που παρουσιάζονται κατά την εφαρμογή αυτού του μοντέλου γίνονται περιορισμοί τόσο σε επίπεδο host όσο και σε επίπεδο δικτύου.

Σε ένα site είναι δυνατό να ακολουθηθούν και τα δυο μοντέλα. Για παράδειγμα το μοντέλο «allow all» μπορεί να υιοθετηθεί για την επικοινωνία δύο τοπικών δικτύων ενώ το δεύτερο μοντέλο «deny all» για τη σύνδεση, ενός site με το Διαδίκτυο.

Συνήθως όμως υπάρχει ο μέσος δρόμος με το μοντέλο εμπιστοσύνης σε κάποιους ανθρώπους κάποιες χρονικές στιγμές.

Προσδιορισμός των πραγματικών αναγκών για υπηρεσίες

Υπάρχουν πολλές υπηρεσίες οι οποίες είτε λειτουργούν εσωτερικά σε ένα δίκτυο είτε έχουν σχέση με το Διαδίκτυο. Έλεγχος για την ασφάλεια ενός site σημαίνει ελεγχόμενη πρόσβαση των εσωτερικών υπηρεσιών καθώς και ελεγχόμενη πρόσβαση των υπηρεσιών που βρίσκονται σε απομακρυσμένα sites.

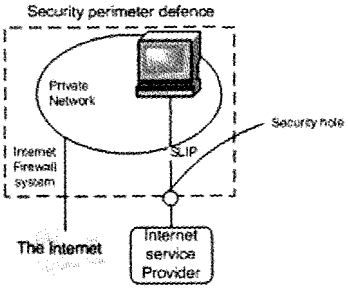
Το Διαδίκτυο προσφέρει ένα μεγάλο αριθμό υπηρεσιών όπως anonymous FTP, gopher, DB access, WWW κ.α. Πολλές φορές γίνεται αλόγιστη χρήση των υπηρεσιών αυτών. Προτού τεθεί μια υπηρεσία σε λειτουργία, καλό θα ήταν να διερευνηθεί αν είναι πραγματικά αναγκαία.

Θα πρέπει να λαμβάνεται υπόψη πάντα ότι ο βαθμός πολυπλοκότητα ς της ασφάλειας του συστήματος αυξάνεται εκθετικά όταν μπαίνουν σε λειτουργία διάφορες υπηρεσίες. Οι filtering routers που χρησιμοποιούνται θα πρέπει να τροποποιούνται ώστε να υποστηρίζουν τα καινούργια πρωτόκολλα. Κάποια από τα πρωτόκολλα αυτά όπως το RPC είναι από τη φύση τους δύσκολο να ελεγχθούν. Είναι προφανές ότι η αλληλεπίδραση υπηρεσιών που βρίσκονται στην ίδια συσκευή μπορεί έχει καταστροφικά αποτελέσματα.

Υλοποίηση με «Τοίχους Ασφαλείας» (firewalls)

Τεχνολογίες «Τοίχων Ασφαλείας»

Όπως είναι γνωστό η σύνδεση ενός συστήματος στο διαδίκτυο δίνει την δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Η δυνατότητα αυτή δεν είναι πάντα επιθυμητή αφού εμπιστευτικές πληροφορίες που βρίσκονται στα συστήματα ενός οργανισμού μπορούν να διαρρεύσουν.



Σχήμα 7-1.

Για να υπάρξει ένα είδος διαχωρισμού ανάμεσα στο Intranet του οργανισμού και το Internet υπάρχει μία ομάδα συστημάτων που δημιουργεί έναν τοίχο ασφαλείας ανάμεσα στα δύο δίκτυα. Η χρήση τους βέβαια βοηθά την ενίσχυση της ασφάλειας, αλλά δεν την εγγυάται. Ο σωστός σχεδιασμός της περιμέτρου και της διαμόρφωσης των συστημάτων είναι απαραίτητος για την σωστή λειτουργία τους (βλ σχήμα 7-1).

Ένα firewall μπορεί να μας προσφέρει:

- Ένα σημείο εφαρμογής των αποφάσεων που αφορούν την ασφάλεια
- Ένα μέσο για την εφαρμογή της πολιτικής ασφάλειας
- Έναν τρόπο καταγραφής της δικτυακής κίνησης
- Ένα φράγμα σε ανεπιθύμητες επιθέσεις

Αντίθετα ένα firewall δεν μπορεί να μας προφυλάξει από:

- Εσωτερικούς χρήστες που σκοπεύουν να επιτεθούν
- Συνδέσεις που δεν περνούν από αυτό
- Εντελώς νέους τύπους απειλών-επιθέσεων
- Ιούς, αποδοτικά
- Λάθη στην διαμόρφωση

Παρόλα αυτά ούτε με τη χρήση firewall μπορούμε να έχουμε απόλυτη ασφάλεια στο δίκτυο. Όταν μιλάμε για ασφάλεια θα πρέπει να λάβουμε υπόψη μας το κόστος που απαιτείται για την προστασία, το βαθμό πολυπλοκότητας του συστήματός μας καθώς και την ευκολία στη χρήση. Το firewall αλληλεπιδρά με το internet και χρειάζεται ιδιαίτερη προσοχή στην εγκατάστασή του και την σωστή διαμόρφωσή του.

Firewall λοιπόν, είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Ένα firewall λειτουργεί σαν μία πύλη από την οποία περνάει όλη η κίνηση από και προς το εξωτερικό δίκτυο. Με την χρήση ενός Firewall περιορίζεται η επικοινωνία ανάμεσα στο προστατευόμενο δίκτυο και ένα οποιοδήποτε άλλο δίκτυο.

Γενικά ένα firewall θα μπορούσαμε να το παρομοιάσουμε με έναν τοίχο ανάμεσα στο εσωτερικό δίκτυο και ένα εξωτερικό δίκτυο (π.χ. το Διαδίκτυο).

Το βασικό χαρακτηριστικό αυτού του τοίχου είναι να βρεθούν οι δρόμοι- πύλες από τους οποίους θα μπορεί να περάσει συγκεκριμένη πληροφορία. Το πιο δύσκολο κομμάτι για την υλοποίηση του firewall είναι η εύρεση των κριτηρίων που θα προσδιορίσουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν μέσα από αυτές τις πύλες.

Ένα firewall μπορεί να είναι ο συνδυασμός δρομολογητών (routers), υποδικτύων (network segments) και υπολογιστών που έχουν ρόλο host.

Ανάλογα με τον τρόπο λειτουργίας της συσκευής υπάρχουν διαφορετικά είδους εγκαταστάσεις. Παρακάτω αναφέρουμε μερικά στοιχεία των firewall:

Bastion host: Ένας υπολογιστής γενικού σκοπού που χρησιμοποιείται για να ελέγξει την προσπέλαση ανάμεσα στο εσωτερικό (ιδιωτικό) δίκτυο (intranet) και το Internet. Συνήθως το λειτουργικό τους σύστημα είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητές του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται

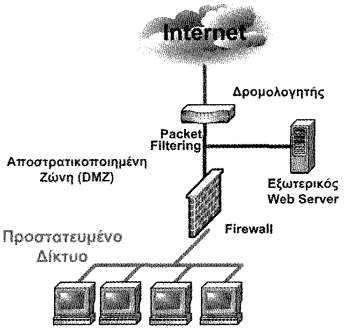
Δρομολογητής (Router): Ένας υπολογιστικό σύστημα ειδικού σκοπού, που διασύνδεει δύο δίκτυα. Διαχειρίζεται τα πακέτα που διακινούνται ανάμεσα στα δίκτυα, δρομολογώντας την κυκλοφορία στα κατάλληλα δίκτυα.

Ελεγκτής Λίστας Προσπέλασης (Access Control List-ACL): Πολλοί δρομολογητές έχουν την δυνατότητα να επεξεργάζονται τα πακέτα που δρομολογούν και να επιτρέπουν (ή όχι) την κυκλοφορία τους ανάλογα με το αν πληρούν (ή όχι) ορισμένες συνθήκες. Αυτές συμπεριλαμβάνουν την διεύθυνση του αποστολέα, του παραλήπτη, το port που απαντά η υπηρεσία κλπ. Έτσι μπορούν να δημιουργηθούν λίστες με κανόνες που πρέπει να ικανοποιούνται για να μπορεί να γίνει προσπέλαση ενός εξυπηρετητή ή μιας υπηρεσίας.

Η αποστρατικοποιημένη ζώνη (Demilitarized Zone-DMZ): είναι ένα κρίσιμο συστατικό του δικτύου που βρίσκεται ανάμεσα στο ιδιωτικό δίκτυο που προφυλάσσει το firewall και το διαδίκτυο. Είναι μία περιοχή που ανήκει μεν στην εσωτερική δομή του δικτύου μας, αλλά οι κόμβοι του δεν απολαμβάνουν την εμπιστοσύνη που έχουν οι κόμβοι του υπόλοιπου δικτύου. Ο σκοπός της ζώνης αυτής είναι στρατηγικής σημασίας για την ασφάλεια του δικτύου μας και επιτρέπει στην ουσία την προσπέλαση σε κόμβους και υπηρεσίες του εσωτερικού δικτύου. Οι εξωτερικοί χρήστες του διαδικτύου μπορούν να προσπελάσουν μόνο τους κόμβους της ζώνης αυτής, ενώ αυτοί μπορούν να προσπελάσουν και κόμβους του εσωτερικού δικτύου. Σε περίπτωση επίθεσης ο hacker θα πρέπει να αντιμετωπίσει και δεύτερο «τείχος» άμυνας.

Proxy: Όταν ένας εξυπηρετητής δρα σαν να ήταν κάποιος άλλος. Για παράδειγμα ένας κόμβος που μπορεί να φέρει μια σελίδα από το διαδίκτυο πρέπει να στηθεί σαν proxy server και ένας κόμβος που ζητά την σελίδα αυτή αλλά βρίσκεται στο εσωτερικό του δικτύου πρέπει να στηθεί σαν proxy client. Με τον τρόπο αυτό όταν ένας κόμβος από το εσωτερικό μας δίκτυο ζητά μια σελίδα από το διαδίκτυο, ο proxy server την ζητά για λογαριασμό του client και την παραδίδει σε αυτόν. Με τον τρόπο αυτό μόνο οι proxy servers έρχονται σε επικοινωνία με το διαδίκτυο, ενισχύοντας την ασφάλεια του εσωτερικού μας δικτύου.

Διαμόρφωση Firewall



Σχήμα 7-2. Η διαμόρφωση των firewalls

Τρόποι λειτουργίας των firewalls

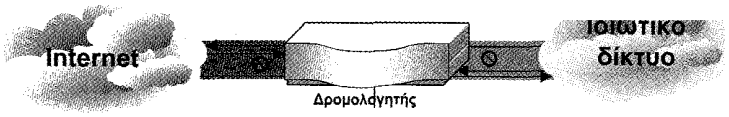
Η λειτουργία των firewalls μπορεί να είναι ένα ή περισσότερα από τα ακόλουθα: Packet-filtering router, Application-level gateway (ή proxy server).

Δρομολογητές φιλτραρίσματος πακέτων (Packet-Filtering Routers)

Αυτό που γίνεται αντιληπτό πιο εύκολα σε ένα firewall είναι η λειτουργία που σχετίζεται με ένα filtering router. Ένας δρομολογητής κινεί δεδομένα από και προς ένα ή περισσότερα δίκτυα. Ένας κανονικός δρομολογητής παίρνει ένα πακέτο από ένα δίκτυο «Α» και το δρομολογεί προς τον προορισμό του ένα δίκτυο «Β». Ένας δρομολογητής φιλτραρίσματος (filtering router) κάνει ακριβώς το ίδιο με ένα απλό δρομολογητή, επιπλέον όμως αποφασίζει για το αν θα δρομολογήσει ή όχι ένα πακέτο. Αυτό επιτυγχάνεται με την εγκατάσταση κάποιων φίλτρων βάση των οποίων ο δρομολογητής αποφασίζει για το τι θα κάνει με οποιοδήποτε πακέτο φτάνει σε αυτόν.

Επιπλέον στοιχεία που θα πρέπει να λαμβάνονται υπόψη, ώστε να κατασκευάσουμε ένα ασφαλές filtering πλάνο, είναι αν ο δρομολογητής επαναπροσδιορίζει τις εντολές φιλτραρίσματος και αν είναι δυνατή η εφαρμογή φίλτρων για εισερχόμενα ή εξερχόμενα πακέτα σε κάθε διεπαφή (interface). Ένα άλλο σημαντικό θέμα είναι η ικανότητα ανάπτυξης φίλτρων που βασίζονται σε επιλογές του IP header και στον τεμαχισμό των πακέτων. Η κατασκευή ενός καλού φίλτρου είναι πολύ δύσκολη και απαιτείται η πλήρης κατανόηση των πρωτοκόλλων που θέλουμε να φιλτράρουμε.

Ένας δρομολογητής φιλτραρίσματος πακέτων (βλ Σχήμα 7-3) παίρνει αποφάσεις για το αν θα περάσει ή όχι το κάθε πακέτο. Ο δρομολογητής εξετάζει το κάθε datagram για να αποφασίσει αν ταιριάζει με κάποιον από τους κανόνες φιλτραρίσματος των πακέτων. Οι πληροφορίες είναι η IP αποστολέα, IP παραλήπτη, το πρωτόκολλο (TCP, UDP, ICMP, ή IPTunnel), το TCP/UDP port προέλευσης, το TCP/UDP port προορισμού, το ICMP μήνυμα κλπ.



Σχήμα 7-3. Packet filtering router

Τα πλεονεκτήματα του τύπου αυτού είναι το μικρό κόστος υλοποίησης, για WAN συνδέσεις χωρίς πρόβλημα στην απόδοση, είναι διάφανο στους χρήστες και στις εφαρμογές. Στα μειονεκτήματα πρέπει να υπολογίσουμε την δυσκολία εξακρίβωσης της ορθότητας των κανόνων φιλτραρίσματος. Για πολύπλοκες εγκαταστάσεις η απόδοση του συστήματος πέφτει όσο αυξάνουν οι κανόνες φιλτραρίσματος. Τέλος η εγκατάσταση αυτού του είδους δεν είναι σε θέση να πάρει αποφάσεις σε σχέση με την εφαρμογή ή το περιεχόμενο των δεδομένων.

Πύλες εφαρμογών (Application level gateways)

Οι πύλες εφαρμογών επιτρέπουν στο διαχειριστή, να υλοποιήσει μία αυστηρότερη πολιτική ασφάλειας. Στο σύστημα εγκαθίστανται proxies των εφαρμογών που επιτρέπουν την προσπέλαση σε εξωτερικούς χρήστες μόνο μέσα από αυτές, ενώ κάθε άλλη χρήση αποτρέπεται από το firewall. Οι χρήστες επιτρέπεται να προσπελαύνουν τις υπηρεσίες του gateway αλλά δεν επιτρέπεται να κάνουν Login σε αυτόν. Για την καλύτερη ασφάλεια του δικτύου τα φίλτρα περιορίζουν την πρόσβαση δυο συνδεδεμένων δικτύων σε ένα μόνο host ο οποίος λέγεται bastion host. Για να φτάσει κάποιο πακέτο στο δευτερεύον δίκτυο θα πρέπει να περάσει από το bastion host. Έτσι περιορίζεται ο αριθμός των άμεσα προσπελάσιμων κόμβων των δικτύων με αποτέλεσμα να επιτυγχάνεται περισσότερη ασφάλεια. Στην περίπτωση αυτή οι υπηρεσίες προωθούνται ξανά από τον bastion host.

Οι proxy servers χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Διάφορες εφαρμογές συγκεντρώνονται σε μια μηχανή, η μηχανή αυτή αποτελεί το βασικό κόμβο (bastion host) που λειτουργεί σαν proxy server για διάφορες υπηρεσίες όπως (Telnet, SMTP, FTP, HTTP κ.α.). Παρόλα αυτά είναι δυνατό να χρησιμοποιούνται διαφορετικοί host για καθεμία από τις παραπάνω υπηρεσίες. Σε αυτή την περίπτωση ο πελάτης αντί να συνδέεται απευθείας με έναν εξωτερικό server συνδέεται με τον proxy server, ο οποίος με τη σειρά του συνδέεται με τον εξωτερικό server.

Από τη χρήση ενός proxy server είναι δυνατό να αποκομιστούν σημαντικά οφέλη. Καταρχήν είναι δυνατή η προσθήκη μιας λίστας ελέγχου προσπέλασης (access control list) για τις διάφορες υπηρεσίες, απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης (authentication) προτού τους επιτραπεί πρόσβαση σε κάποιο από τις υπηρεσίες. Υπάρχουν επίσης και οι «έξυπνοι» proxy servers που λέγονται Application Layer Gateways (ALGs), οι οποίοι μπορούν να μπλοκάρουν συγκεκριμένα τμήματα (subsections) ενός πρωτοκόλλου. Για παράδειγμα ένας ALG για FTP μπορεί να διαχωρίζει την εντολή "put" από την εντολή "get". Έτσι ένας οργανισμός μπορεί να επιτρέπει στους χρήστες του να «κατεβάζουν» αρχεία αλλά να μην αφήνει τους έξω να παίρνουν τα αρχεία των δικών του συστημάτων.

Επίσης, οι proxy servers μπορούν να διαμορφωθούν με τέτοιο τρόπο ώστε να κωδικοποιούνται οι ροές των δεδομένων με βάση διάφορες παραμέτρους. Τέτοιες δυνατότητες μπορούν να χρησιμοποιηθούν από οργανισμούς για να επιτύχουν ασφαλή διασύνδεση των sites τους μέσω του Διαδικτύου.

Τα πλεονεκτήματα αυτού του τύπου είναι η μεγαλύτερη ασφάλεια αφού τα συστήματα αυτά «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα. Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο από τον proxy εμποδίζοντας έτσι την απευθείας σύνδεση. Οι κανόνες φιλτραρίσματος είναι αρκετά πιο εύκολοι να υλοποιηθούν και να εξακριβωθούν για την ορθότητά τους. Το μεγαλύτερο μειονέκτημα είναι πως πρέπει οι χρήστες να αλλάξουν την συμπεριφορά τους ή να στηθεί εξειδικευμένο λογισμικό που θα δίνει μεγαλύτερη ευελιξία στους εσωτερικούς χρήστες χωρίς να μειώνεται η προσφερόμενη ασφάλεια.

Παρακάτω φαίνεται η ακολουθία εντολών για να γίνει μία σύνδεση telnet.

Outside-Client > telnet bastion_host
Username: John Smith
Challenge Number "237936"
Challenge Response: 723456
Trying 200.43.67.17
Hostos UNIX (bastion_host)
Bh-telnet-proxy>help
Valid commands are:

Connect hostname
Help/?
Quit/exit

Bh-telnet-proxy> connect inside server

Hostos UNIX (inside_server)

Login: John Smith
Password: ######
Last login: Wednesday April 15 11:17:15

Υβριδικά συστήματα

Ο συνδυασμός των δύο περιπτώσεων οδηγεί σε καλύτερα αποτελέσματα και συνήθως η υλοποίηση περιλαμβάνει και packet filtering και proxy applications. Τα firewalls εκτός από την ιδιότητα που έχουν να διαφυλάσσουν ένα δίκτυο από διάφορους τρίτους δίνουν δυνατότητα πρόσβασης από απόσταση στους νόμιμους χρήστες του. Το καλύτερο firewall σε ένα δίκτυο επιτυγχάνεται με το συνδυασμό δυο screening routers με ένα ή περισσότερους proxy servers που τοποθετούνται ανάμεσα στους δυο routers. Με την μέθοδο αυτή ο εξωτερικός router εμποδίζει την μη εξουσιοδοτημένη πρόσβαση σε επίπεδο IP (IP spoofing, source routing, packet fragments) ενώ επιτρέπει στον proxy server να παρέχει ασφάλεια στα πρωτόκολλα υψηλότερων επιπέδων. Ο σκοπός του εσωτερικού router είναι να μπλοκάρει όλη την κίνηση εκτός από αυτή του proxy server.

Πολλά firewalls είναι δυνατό να κρατάνε log file για την ενημέρωση των διαχειριστών. Πολλές φορές οι εισβολείς προσπαθούν να παραποιήσουν τα log file. Είναι λοιπόν σκόπιμο να διαφυλάσσονται αυτές οι πληροφορίες. Για το σκοπό αυτό υπάρχουν διάφορες μέθοδοι όπως:

- Μονή εγγραφή (Write-once)
- Μονή εγγραφή-πολλαπλή ανάγνωση (WORM drives)
- Paper logs
- Κεντρικός έλεγχος του logging μέσα από χρήσιμα εργαλεία όπως το syslog.
- Διαφύλαξη της πληροφορίας που κρατείται μέσω log με την σύνδεση μέσω σειριακής θύρας σε ένα υπολογιστή που κρατά το Log σε αρχείο.

Υπάρχουν διάφορα εμπορικά πακέτα για firewalls με κυμαινόμενο κόστος. Σε κάθε περίπτωση η σωστή αρχικοποίηση ενός firewall απαιτεί καλή γνώση του TCP/IP πρωτοκόλλου. Επιπλέον, ένα firewall θα πρέπει να συντηρείται σωστά και ανά τακτά

χρονικά διαστήματα να εγκαθίστανται patches και updates και να γίνεται συχνός έλεγχος για τη σωστή του λειτουργία.

Όταν κάποιος θελήσει να τοποθετήσει κάποιο firewall στον αρχικό του προϋπολογισμό θα πρέπει να συμπεριλάβει ό,τι προαναφέρθηκε. Σε κάθε περίπτωση θα πρέπει να γνωρίζουμε ότι η χρήση ενός firewall δεν εγγυάται την απόλυτη ασφάλεια ενός δικτύου.

Αρχιτεκτονικές Firewalls

Παρακάτω εξετάζονται διαφορετικές αρχιτεκτονικές στην υλοποίηση των συστημάτων firewalls.

Αρχιτεκτονικές με χρήση μίας συσκευής

Η απλούστερη περίπτωση εγκατάστασης firewall είναι με μία μοναδική συσκευή που αναλαμβάνει την λειτουργία του firewall. Το πλεονέκτημα αυτής της λύσης είναι πως υπάρχει ένα σημείο στο οποίο πρέπει κάποιος να επικεντρωθεί ώστε να κάνει σωστή διαμόρφωση, ενώ σαν μειονέκτημα μπορεί να θεωρηθεί ακριβώς το ότι η ασφάλεια εξαρτάται μόνο από μία συσκευή. Στην πράξη το πλεονέκτημα των αρχιτεκτονικών με μία συσκευή δεν είναι στην ασφάλεια, που δεν είναι σε πολλαπλά επίπεδα, αλλά σε πρακτικά θέματα. Η λύση αυτή είναι φτηνότερη, ευκολότερη στην υλοποίηση και στη συντήρηση κάνοντάς την κατάλληλη για μικρά sites.

Δρομολογητής ελέγχου κίνησης (screening router)

Είναι δυνατό να χρησιμοποιηθεί η μέθοδος του φιλτραρίσματος πακέτων σε ένα δρομολογητή, σαν firewall για να προστατέψει ολόκληρο το δίκτυο. Είναι μία φτηνή λύση, αφού πάντα υπάρχει ένας δρομολογητής για να συνδέει το εσωτερικό δίκτυο με το Internet. Οι κατάλληλες χρήσεις περιλαμβάνουν περιπτώσεις όπου:

- Στο δίκτυο που προστατεύουν υπάρχει ένα καλό επίπεδο ασφάλειας κόμβων
- Ο αριθμός των πρωτοκόλλων που χρησιμοποιούνται είναι περιορισμένος
- Απαιτείται μέγιστη απόδοση από το δίκτυο

Οι screening routers είναι χρήσιμοι σε εσωτερικά firewalls και για δίκτυα που παρέχουν υπηρεσίες στο internet. Δεν είναι ασύνηθες σε παρόχους υπηρεσιών διαδικτύου να χρησιμοποιούν αυτή την λύση ανάμεσα στους κόμβους τους και το διαδίκτυο.

Υπολογιστής με διπλή κάρτα δικτύου (dual-homed host)

Η αρχιτεκτονική αυτή στηρίζεται σε έναν υπολογιστή που έχει τουλάχιστον δύο κάρτες δικτύου και λειτουργεί σαν δρομολογητής για την κίνηση ανάμεσα στα πακέτα που διακινούνται στα δύο υποδίκτυα που είναι συνδεμένα στις δύο κάρτες. Απενεργοποιούμε την αυτόματη δρομολόγηση και επιτρέπουμε μόνο σε συγκεκριμένα πακέτα που τηρούν τους κανόνες ασφάλειας, που έχουμε ορίσει να περάσουν στο άλλο υποδίκτυο. Τα dual-homed hosts προσφέρουν υπηρεσίες μέσω proxy (αντιπροσώπων), χωρίς δυστυχώς να υπάρχουν υλοποιήσεις για όλες τις υπηρεσίες. Η χρήση τους ενδείκνυται σε περιπτώσεις όπου:

- Η κίνηση στο δίκτυο είναι μικρή
- Η κίνηση προς το διαδίκτυο δεν είναι κρίσιμη για την λειτουργία του site
- Δεν παρέχονται υπηρεσίες σε χρήστες του διαδικτύου
- Το δίκτυο που προστατεύεται δεν έχει πολύτιμα δεδομένα

Συσκευές πολλαπλής χρήσης

Οι συσκευές αυτές είναι υλοποιήσεις κατασκευαστών που συνδυάζουν τα πλεονεκτήματα και μειονεκτήματα των δύο προηγούμενων λύσεων. Πρόκειται για συσκευές που χρησιμοποιούν ιδιόκτητες εσωτερικές αρχιτεκτονικές και πρωτόκολλα και μπορούν να δώσουν τις λειτουργίες του proxying και packet filtering ταυτόχρονα.

Αρχιτεκτονικές με διαχωρισμό υπηρεσιών

Σε αυτή την περίπτωση για ορισμένες υπηρεσίες η σύνδεση του διαδικτύου με το εσωτερικό δίκτυο γίνεται μέσω ενός εσωτερικού κόμβου, τον ενδιάμεσο (proxy), που παίζει το ρόλο της αντίστασης σε επιθέσεις (bastion σημαίνει οχυρό αντίστασης σε επίθεση).

Ο δρομολογητής αναλαμβάνει να υλοποιήσει είτε τον διαχωρισμό των πακέτων ανάμεσα σε αυτά που επιτρέπονται να προχωρήσουν στο εσωτερικό δίκτυο, από αυτά που πρέπει να πάνε στον bastion host και αφορούν υπηρεσίες που υποστηρίζει είτε να απαγορεύσει πλήρως τη δρομολόγησή τους στο εσωτερικό δίκτυο.

Έτσι για παράδειγμα, οι χρήστες του διαδικτύου προσπελαύνουν συγκεκριμένες υπηρεσίες του εσωτερικού δικτύου μόνο μέσα από τον κόμβο αυτό. Κάθε άλλη προσπάθεια για προσπέλαση σε άλλο κόμβο απορρίπτεται ή όχι ανάλογα με την πολιτική που υλοποιεί ο δρομολογητής.

Ο δρομολογητής μπορεί να επιτρέπει στους εσωτερικούς κόμβους, για συγκεκριμένες υπηρεσίες, να επικοινωνούν με κόμβους στο διαδίκτυο (packet filtering) ή να απαγορεύει όλες τις συνδέσεις με το διαδίκτυο παρά μόνο με χρήση ενδιάμεσου (proxy) μέσω του bastion host. Η χρήση αυτής της αρχιτεκτονικής συνίσταται όταν:

Υπάρχουν λίγες εισερχόμενες συνδέσεις. Για την ακρίβεια δεν είναι σωστή η υλοποίηση αυτή όταν ο διαχωρισμός γίνεται για web server .

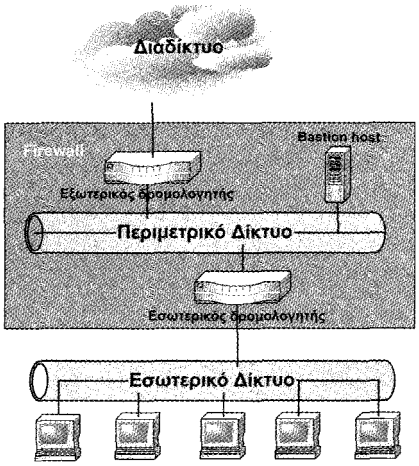
Το δίκτυο που προστατεύεται έχει σχετικά μεγάλο επίπεδο ασφάλειας στους κόμβους.

Αρχιτεκτονικές με διαχωρισμό υποδικτύων

Η αρχιτεκτονική του διαχωρισμού των υποδικτύων προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Με την υλοποίηση ενός περιμετρικού δικτύου (DeMilitary Zone-DMZ) απομονώνεται ακόμα περισσότερο το εσωτερικό δίκτυο από τους χρήστες του διαδικτύου. Τι κερδίζουμε με αυτό;

Το ***περιμετρικό δίκτυο*** αποτελεί ένα ακόμα επίπεδο ασφάλειας ανάμεσα στο διαδίκτυο και το εσωτερικό δίκτυο. Σε πολλά Ethernet δίκτυα είναι δυνατό να παρακολουθούνται τα πακέτα που διακινούνται με σκοπό να γίνει υποκλοπή κρίσιμων πληροφοριών. Με τον διαχωρισμό των υποδικτύων προσπαθούμε να διαφυλάξουμε τις πληροφορίες αυτές, σε περίπτωση που κάποιος καταφέρει να εισέλθει στον bastion host, αφού ανήκει σε άλλο υποδίκτυο και ο εσωτερικός δρομολογητής απορρίπτει την κίνηση από το εσωτερικό δίκτυο.

Ο ***bastion host*** χρησιμοποιείται για να δέχεται συνδέσεις από το διαδίκτυο που αφορούν πληροφορία που πρέπει να παραδοθεί στο site, όπως για παράδειγμα εισερχόμενο mail, ftp συνδέσεις ή ερωτήσεις για ονοματολογία κόμβων (DNS). Επίσης στις περιπτώσεις που χρειάζεται να γίνουν συνδέσεις από εσωτερικούς κόμβους με το διαδίκτυο δεν επιτρέπεται η απευθείας σύνδεση, αλλά χρησιμοποιείται σαν ενδιάμεσος (proxy server) για υπηρεσίες όπως η προσπέλαση ιστοσελίδων.



Από την φύση τους τα bastion hosts είναι τα πιο τρωτά συστήματα. Για την ακρίβεια σε μία επίθεση είναι ο πρώτος στόχος, αφού αν έχει σχεδιαστεί σωστά το φιλτράρισμα των πακέτων είναι ο μόνος κόμβος που προσπελαύνεται από το διαδίκτυο. Για να επιτύχει να εισχωρήσει στο εσωτερικό δίκτυο ένας hacker πρέπει να καταφέρει να περάσει και από τους δύο δρομολογητές. Στο Σχήμα 7-7 παρουσιάζεται μία τυπική εγκατάσταση firewall με την αρχιτεκτονική του διαχωρισμού των υποδικτύων.

Σχήμα 7-7. Αρχιτεκτονική διαχωρισμού υποδικτύων.

Ο ***εσωτερικός δρομολογητής*** κάνει το κύριο φιλτράρισμα των πακέτων στο firewall. Επιτρέπει σε επιλεγμένες υπηρεσίες να κάνουν συνδέσεις προς το διαδίκτυο είτε απευθείας, είτε με χρήση του ενδιάμεσου. Πρόκειται για τις υπηρεσίες πού είναι απαραίτητες για την λειτουργία του site και είναι αυτές που θεωρούνται ασφαλείς. Η επιλογή του τι θεωρείται ασφαλές ορίζεται από το κάθε site ξεχωριστά και συνδυάζει ης ανάγκες, δυνατότητες και περιορισμούς που έχει το κάθε ένα. Οι απαραίτητες υπηρεσίες που επιτρέπονται από το εσωτερικό προς το περιμετρικό δίκτυο πρέπει να περιλαμβάνουν το SMTP για το ηλεκτρονικό ταχυδρομείο, DNS για ης ερωτήσεις ονοματολογίας, και HTTP για ης προσπέλαση του web server.

Τέλος ο ***εξωτερικός δρομολογητής*** είναι αυτός που προστατεύει καταρχήν το περιμετρικό και εσωτερικό υποδίκτυο. Σε αυτόν δεν ορίζονται πολύπλοκοι κανόνες που πρέπει συχνά να αλλάζουν. Οι κύριοι κανόνες αφορούν ελέγχους για την αυθεντικότητα της προέλευσης των πακέτων. Για παράδειγμα δεν μπορεί να εισέρχεται ένα πακέτο από το διαδίκτυο, που έχει διεύθυνση αποστολέα το εσωτερικό δίκτυο, ή να φεύγει προ το διαδίκτυο ένα πακέτο που δεν έχει αποστολέα κόμβο του περιμετρικού ή του εσωτερικού δικτύου για ορισμένες υπηρεσίες.

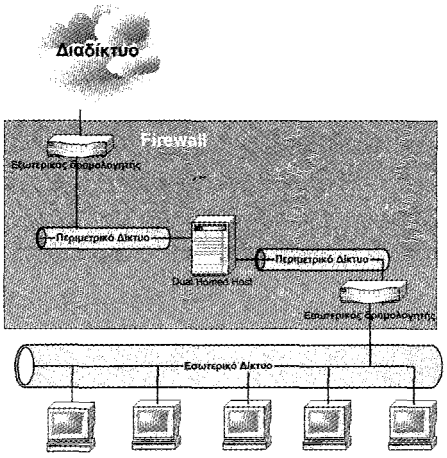
Η αρχιτεκτονική αυτή είναι η καταλληλότερη για τις περισσότερες περιπτώσεις δικτύων και firewalls.

Αρχιτεκτονικές με διαχωρισμό πολλαπλών υποδικτύων

Υπάρχουν περιπτώσεις που χρειάζεται κάτι παραπάνω από αυτά που προσφέρει η αρχιτεκτονική του διαχωρισμού υποδικτύων. Στις περιπτώσεις αυτές προσφέρονται πιο σύνθετες αρχιτεκτονικές διπλού διαχωρισμού δικτύων. Σε αυτό τον τύπο υπάρχουν ο εξωτερικός και εσωτερικός δρομολογητής αλλά υπάρχουν δύο περιμετρικά υποδίκτυα που συνδέονται μεταξύ τους με διαφορετικούς τρόπους.

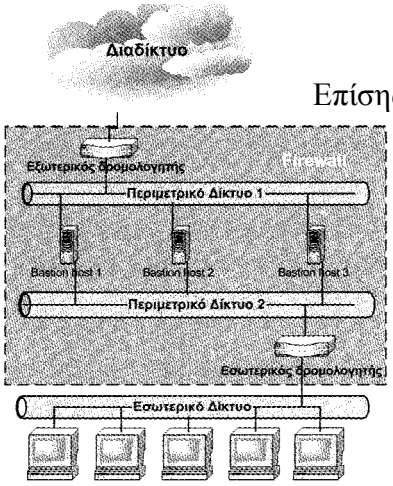
Διπλός διαχωρισμός υποδικτύων με χρήση υπολογιστή διπλής κάρτας δικτύου (dual-homed host)

Σε αυτή την περίπτωση ανάμεσα στον εσωτερικό και τον εξωτερικό δρομολογητή υπάρχουν περισσότερα υποδίκτυα που διασυνδέονται μεταξύ τους με ένα ή περισσότερους υπολογιστές με διπλές κάρτες δικτύου (dual-homed host) και όχι με έναν επιπλέον δρομολογητή. Μερικά sites χρησιμοποιούν αυτήν την αρχιτεκτονική (βλ. Σχήμα 7-8) για να προσθέσουν βάθος στην άμυνα τους και να προστατέψουν τους ενδιάμεσους (proxies) των υπηρεσιών. Ο υπολογιστής με τις δύο κάρτες δικτύου παρέχει καλύτερο έλεγχο στην δρομολόγηση των πακέτων ανάμεσα στα δύο υποδίκτυα, ενισχύοντας έτσι την ασφάλεια. Με την χρήση αυτής της αρχιτεκτονικής οι διαχειριστές μπορούν να «κόψουν» επικίνδυνα πρωτόκολλα όπως αυτά που αφορούν την απομακρυσμένη προσπέλαση για την διαχείριση των κόμβων, χωρίς να βασιστούν αποκλειστικά στον εξωτερικό δρομολογητή που δεν προσφέρει αρκετή λεπτομέρεια στην διαχείριση αυτών των πρωτοκόλλων.



Σχήμα 7-8. Διαχωρισμός υποδικτύων με dual-homed host

Επίσης υπάρχει η δυνατότητα για τον διαχωρισμό των δύο περιμετρικών υποδικτύων με χρήση homed hosts που υλοποιούν διάμεσους (proxies) λειτουργώντας ως bastion hosts. Η υλοποίηση αυτή (βλ. Σχήμα 7-9) είναι απαραίτητη περιπτώσεις που απαιτείται υψηλή απόδοση σε εξυπηρετητές που κάνουν έντονη χρήση του δικτύου, περιορίζοντας τα πρωτόκολλα διαχείρισης που απαιτούν αρκετό εύρως φάσματος (bandwidth). Αυτού του είδους firewall επιτρέπει εξαιρετική πολυεπίπεδη προοτασία, αν και χρειάζεται ιδιαίτερη προσοχή στην διαμόρφωση .

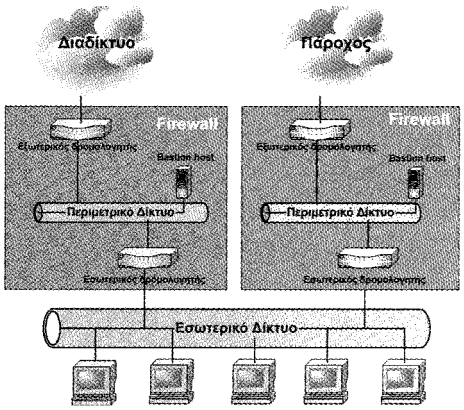


Σχήμα 7-9. Διπλός διαχωρισμός υποδικιύων χωρίς ενδιάμεση κίνηση

Η χρήση αυτής της αρχιτεκτονικής είναι κοτάλληλη για δίκτυα που απαιτείται υψηλή ασφάλεια, ιδιαίτερα αν παρέχονται υπηρεσίες στο διαδίκτυο.

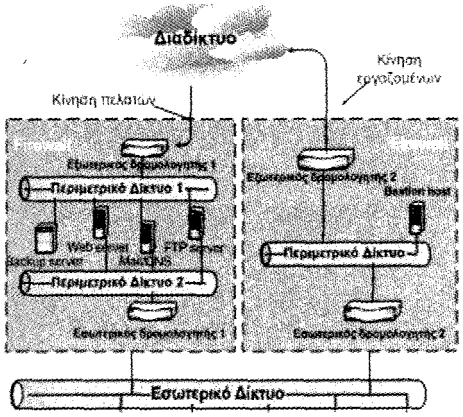
Διπλός διαχωρισμός σε ανεξάρτητα υποδίκτυα

Σε ορισμένες περιπτώσεις χρειάζεται να έχουμε πολλά ανεξάρτητα διαχωρισμένα υποδίκτυα με ξεχωριστούς εξωτερικούς δρομολογητές. Το Σχήμα 7-10 δείχνει αυτή την υλοποίηση.Η λύση αυτή προτιμάται σε περιπτώσεις που χρειάζεται να υπάρχει εναλλακτική λύση στην διασύνδεση με το διαδίκτυο μέσω κάποιου άλλου παρόχου. Δεν είναι λογικό να πληρώνει κάποιος το κόστος των δύο συνδέσεων και να τοποθετεί τα δύο άκρα στον ίδιο εξωτερικό δρομολογητή. Με την εγκατάσταση των δύο συνδέσεων σε δύο διαφορετικούς εξωτερικούς δρομολογητές , δύο περιμετρικά υποδίκτυα και εσωτερικούς δρομολογητές διασφαλίζει πως δεν υπάρχει ένα σημείο αποτυχίας ανάμεσα στο site και στο διαδίκτυο. Αρκεί βέβαια, οι γραμμές που χρησιμοποιούνται να περνούν από διαφορετική όδευση και να έχουμε επιλέξει διαφορετικούς παρόχους.



Σχήμα 7-10 Πολλαπλά περιμετρικά υποδίκτυα

Σε κάποιες περιπτώσεις που οι δύο διασυνδέσεις είναι ταυτόχρονα ενεργές, και χρειάζεται η απομόνωση του ενός από το άλλο αν για παράδειγμα στο ένα υποδίκτυο διακινούνται εμπιστευτικές πληροφορίες, μπορούμε να συνδέσουμε τα δύο περιμετρικά υποδίκτυα με ένα εσωτερικό δρομολογητή με τις κατάλληλες οδηγίες για το φιλτράρισμα των πακέτων. Επίσης μπορούμε να χρησιμοποιήσουμε αυτή την αρχιτεκτονική όταν παρέχουμε εισερχόμενες υπηρεσίες στο διαδίκτυο (π.χ. ιστοσελίδες στο διαδίκτυο) και ταυτόχρονα προσφέρουμε εξερχόμενες υπηρεσίες σε εσωτερικούς χρήστες (π.χ. ενδιάμεσο proxy για προσπέλαση ιστοσελίδων από το διαδίκτυο), για να αυξήσουμε την ασφάλεια. Διαχωρίζοντας σε δύο ανεξάρτητα περιμετρικά υποδίκτυα τις εξερχόμενες από τις εισερχόμενες υπηρεσίες αυξάνουμε κατά πολύ την ασφάλεια του site.

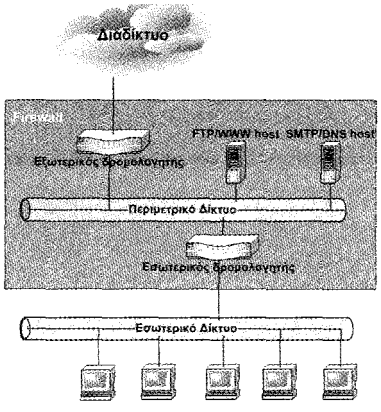


Σχήμα 7-11 Μία πολύπλοκη εγκατάσταση firewall

Το να διατηρούμε διαφορετικά περιμετρικά υποδίκτυα είναι λιγότερο επικίνδυνο από το να έχουμε μοιρασμένο το εσωτερικό δίκτυο, αλλά εξακολουθεί να είναι πρόβλημα στην διαχείριση.

Μία πιο σύνθετη αρχιτεκτονική υπάρχει στο Σχήμα 7-11 που παρουσιάζεται το firewall που (θα έπρεπε να) χρησιμοποιούν αρκετοί πάροχοι με αρκετά περιμετρικά δίκτυα και πολλαπλές συνδέσεις στο διαδίκτυο.

Η χρήση αυτών των αρχιτεκτονικών ενδείκνυται σε περιπτώσεις που έχει μεγάλη σημασία η εναλλακτική όδευση της επικοινωνίας, ή απαιτήσεις για υψηλή ασφάλεια και διαφορετικές ανεξάρτητες χρήσεις του διαδικτύου.

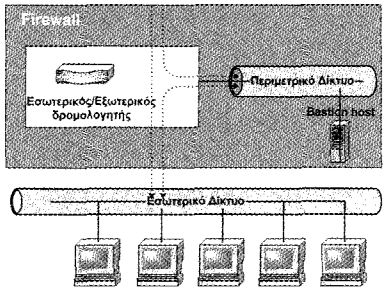


Διαφοροποιήσεις στις αρχιτεκτονικές firewall

Παρακάτω παρουσιάζονται σχηματικά ορισμένες υλοποιήσεις που συναντώνται στην πράξη αλλά παρουσιάζουν (κατά την άποψή μας) λάθη στην διαμόρφωση.

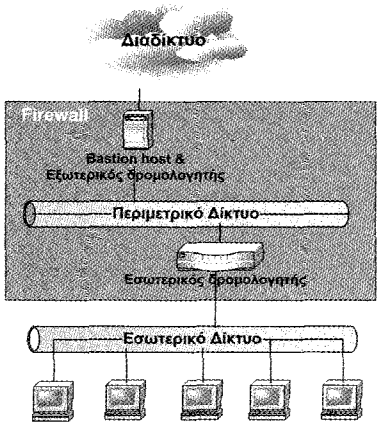
Αν και μέχρι τώρα μιλήσαμε για εγκαταστάσεις με ένα bastion host υπάρχουν περιπτώσεις που επιβάλλεται η χρήση περισσοτέρων, είτε για βελτίωση της απόδοσης, είτε ως εναλλακτική λύση σε περίπτωση αστοχίας, είτε λόγω της ανάγκης για λειτουργικό διαχωρισμό των δεδομένων ή των εξυπηρετητών (βλ. Σχήμα 7-12).

Μία άλλη περίπτωση διαμόρφωσης παρουσιάζεται όταν ο εσωτερικός και εξωτερικός δρομολογητής είναι μία συσκευή (βλ. Σχήμα 7-13). Αυτό είναι δυνατόν μόνο αν ο δρομολογητής είναι ισχυρός, έχει δυνατότητες και ευελιξία στην διαμόρφωση της πολιτικής ασφάλειας. Στην περίπτωση αυτή είναι δυνατή η εγκάτασταση της εξωτερικής σύνδεσης, της εσωτερικής και του περιμετρικού υποδικτύου σε διαφορετικά interfaces. Η αρχιτεκτονική αυτού του είδους δημιουργεί ένα σημείο αποτυχίας σε περίπτωση αστοχίας του υλικού, ενώ ταυτόχρονα δημιουργεί προβλήματα αν ένας hacker καταφέρει να έχει πρόσβαση στον δρομολογητή, αφού τώρα είναι και εσωτερικός.



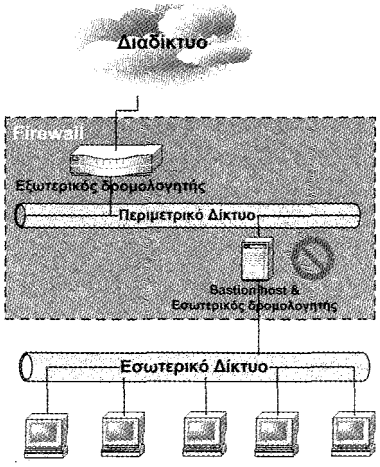
Σχήμα 7-13 εσωτερικός και εξωτερικός δρομολογητής σε μια συσκευή

Υπάρχουν, επίσης περιπτώσεις όπου γίνεται χρήση ενός εξυπηρετητή με δύο κάρτες δικτύου (dual-homed host) σαν εξωτερικός δρομολογητής και ενδιάμεσος (proxy). Για παράδειγμα, αν υπάρχει μόνο μία dial-up SLIP ή PPP σύνδεση 010 διαδίκτυο, τότε μπορούμε να «τρέχουμε» PPP 010v bastion-host και να λειτουργεί σαν bastion host και εξωτερικό δρομολογητή. Σε αυτή την περίπτωση (βλ. Σχήμα 7-14) μία συσκευή λειτουργεί σαν τρεις: bastion, εσωτερικός εξωτερικός δρομολογητής. Η χρήση αυτή δεν θα δώσει την απόδοση, ή ευελιξία ενός δρομολογητή, αλλά δεν χρειάζεται τίποτα περισσότερο στην περίπτωση μιας απλής σύνδεσης χαμηλής ταχύτητας. Επιπλέον αυτή η υλοποίηση, αν και δεν έχει περισσότερα προβλήματα ασφάλειας, από ότι η χρήση εσωτερικού και εξωτερικού δρομολογητή σε μία συσκευή, αφήνει πιο εκτεθειμένο τον bastion host με μόνο ης δυνατότητες που έχει ο ίδιος για φιλτράρισμα πακέτων.



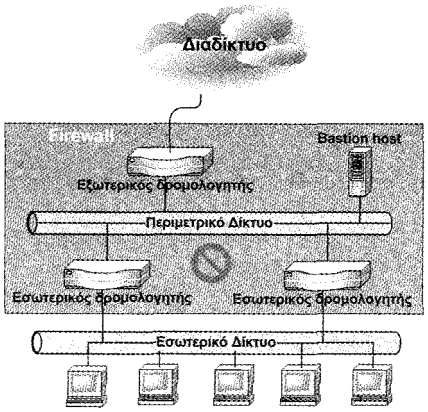
Σχήμα 7-14. Bastion host και εξωτερικός δρομολογητής σε μια συσκευή

Αν και οι υλοποιήσεις που έχουν τον bastion host και τον εξωτερικό δρομολογητή σε μία συσκευή είναι κάτι που είναι αποδεκτό η ύπαρξη του bastion και του εσωτερικού δρομολογητή σε μία συσκευή (βλ. Σχήμα 7-15) προτείνεται να αποφεύγονται. Σε αυτή την υλοποίηση μειώνεται δραστικά η ασφάλεια του site. Αυτό γίνεται γιατί όταν ο bastion host δεχτεί επίθεση και αποκτηθεί πρόσβαση σε αυτόν τότε ο hacker έχει προσπέλαση στον εσωτερικό δρομολογητή. Αντίθετα στην προηγούμενη περίπτωση ο εσωτερικός μπορούσε να δράσει ανασταλτικά αν κάτι τέτοιο συνέβαινε και ο hacker είχε προσπέλαση στον εξωτερικό δρομολογητή. Μία κύρια χρήση του περιμετρικού υποδικτύου είναι η διαφύλαξη της δικτυακής κίνησης του εσωτερικού δικτύου από τον bastion host, γεγονός που στην συγκεκριμένη υλοποίηση αυτό δεν ισχύει.



Σχήμα 7-15. Bastion host και εσωιερικός δρομολογητής σε μια συσκευή

Είναι επίσης επικίνδυνη η χρήση δύο εσωτερικών δρομολογητών για την διασύνδεση του περιμετρικού υποδικτύου με το εσωτερικό δίκτυο (βλ. Σχήμα 7-16). Για παράδειγμα μπορεί μία εσωτερική συσκευή να διαπιστώσει πως είναι γρηγορότερο να προσπελάσει μία άλλη εσωτερική συσκευή μέσω του περιμετρικού υποδικτύου. Αν είμαστε προσεκτικοί αυτή η κίνηση θα σταματήσει από το φιλτράρισμα των πακέτων που κάνουν οι δρομολογητές. Αν όμως δεν έχει γίνει σωστή διαμόρφωση (πράγμα όχι απίθανο σε πολύπλοκες εγκαταστάσεις) τότε η εσωτερική πληροφορία θα διακινείται στο περιμετρικό υποδίκτυο, δίνοντας την ευκαιρία για λαθρανάγνωση κρίσιμων δεδομένων.



Σχήμα 7-16. εγκατάσταση με πολλαπλούς εσωτερικούς δρομολογητές

Αυτή η εγκατάσταση μπορεί να προκύψει από την απαίτηση για αποφυγή ενός σημείου αστοχίας στην σύνδεση ενός μεγάλου εσωτερικού δικτύου με το διαδίκτυο ή για την βελτίωση της απόδοσης.

Η σύνδεση ενός ίδιου δρομολογητή όσο αφορά το υλικό και την διαμόρφωση συστήματος είναι η εύκολη λύση, αλλά και αυτή που θα δημιουργήσει προβλήματα στην ασφάλεια με μεγάλη πιθανότητα. Η σωστή λύση είναι η σύνδεση των εσωτερικών δρομολογητών σε διαφορετικά περιμετρικά δίκτυα και εξωτερικούς δρομολογητές, γεγονός που έχει μεν αρκετά μεγαλύτερο κόστος, αλλά βελτιώνει σαφέστατα την ασφάλεια (βλ σχήματα 7-10 και 7-11).

Αν όντως παρουσιαστούν προβλήματα στην απόδοση της διασύνδεσης του εσωτερικού δικτύου με το διαδίκτυο μέσω της συνδεσμολογίας με έναν εσωτερικό δρομολογητή (βλ. Σχήμα 7-7) είναι αρκετά δύσκολο να τεκμηριωθεί το παραπάνω κόστος της χρήσης διπλών περιμετρικών δικτύων και εξωτερικών δρομολογητών όπως στην περίπτωση των σχημάτων 7-10 και 7-11. Σε αυτή την περίπτωση το πρόβλημα δεν οφείλεται συνήθως στον εσωτερικό δρομολογητή, μπορεί όμως να συμβαίνει κάτι από τα ακόλουθα:
είτε αρκετή από την κυκλοφορία που πηγαίνει στο περιμετρικό υποδίκτυο, δεν χρειάζεται να δρομολογηθεί από τον εξωτερικό προς το διαδίκτυο. Σε αυτή την πρώτη περίπτωση

είναι πιθανό να έχει γίνει λάθος στην διαμόρφωση. Ούτως ή άλλως όμως, περιστασιακά, υπάρχει κυκλοφορία από το εσωτερικό προς το περιμετρικό υποδίκτυο που δεν δρομολογείται προς το διαδίκτυο από τον εξωτερικό δρομολογητή, και αφορά κύρια ενημέρωση εξυπηρετητών (π.χ. για πληροφορίες ονοματολογίας - DNS).
είτε ο εξωτερικός δρομολογητής είναι ταχύτερος από τον εσωτερικό, οπότε σε αυτή την περίπτωση πρέπει να εξεταστεί η ενίσχυση του εσωτερικού δρομολογητή (upgrade) ώστε να γίνει ίσων δυνατοτήτων με τον εξωτερικό.

Μία άλλη περίπτωση όπου πιθανά χρειάζονται δύο εσωτερικοί δρομολογητές είναι να υπάρχουν πολλαπλά εσωτερικά δίκτυα με διαφορετικό επίπεδο ασφάλειας ή για άλλους λόγους να απαιτείται ο φυσικός διαχωρισμός των εσωτερικών δικτύων. Στην περίπτωση αυτή και για να αποφύγουμε την λανθασμένη εγκατάσταση, πρέπει πρώτα να εξεταστεί να δοθούν διαφορετικά Interfaces του ίδιου δρομολογητή σε κάθε εσωτερικό δίκτυο. Αν παρ' όλα αυτά γίνει χρήση διαφορετικών εσωτερικών δρομολογητών θα πρέπει να επικοινωνούν μόνο μέσω του περιμετρικού υποδικτύου, δημιουργώντας προβλήματα σε ορισμένους χρήστες, αφού τα δύο δίκτυα θα πρέπει να θεωρούν το ένα το άλλο σαν μη ασφαλή. Άλλη λύση, στην οποία το ένα δίκτυο αποδέχεται το άλλο σαν ασφαλές, πιθανά θα δημιουργήσει προβλήματα στην ασφάλεια του site.

Αν τελικά παρθεί απόφαση να υπάρχουν διαφορετικοί εσωτερικοί δρομολογητές, τότε θα πρέπει να ανατεθεί η λειτουργία και συντήρησή τους στην ίδια ομάδα, ώστε να επιλυθούν τα όποια προβλήματα παρουσιαστούν στη διαμόρφωση χωρίς μείωση της ασφάλειας. Σε αυτή την περίπτωση πρέπει να υπάρχει συνεχής παρακολούθηση της κυκλοφορίας που μεταφέρεται μέσα από το περιμετρικό υποδίκτυο, για την διαπίστωση σφαλμάτων στην διαμόρφωση των δρομολογητών.

Σχεδιασμός Firewalls

Στα προηγούμενα ασχοληθήκαμε με τις τεχνολογίες και τις αρχιτεκτονικές που χρησιμοποιούνται συνήθως για την υλοποίηση των firewalls. Η καταλληλότερη λύση σπάνια είναι μία μόνο τεχνολογία ή μία συσκευή. Συνήθως αποτελείται από προσεκτική επιλογή και συνδυασμό διαφορετικών τεχνολογιών και συσκευών που επιλύουν διαφορετικά προβλήματα.

1.Σχεδιασμός

1.1. Τεκμηρίωση του περιβάλλοντος. Όταν σχεδιάζεται ένα firewall χρειάζεται να γνωρίζουμε τα όρια ανάμεσα στα διαφορετικά τμήματα ασφάλειας σε ένα site

1.2. Επιλογή των λειτουργιών του firewall ανάμεσα σε packet filtering, application proxies, dynamic packet fi1tering. Προτείνουμε τον ακόλουθο πίνακα σαν οδηγό για την επιλογή τους

1.3. Επιλογή της αρχιτεκτονικής του firewall

1.4. Προστασία του συστήματος από μη εξουσιοδοτημένη προσπέλαση

2. Επιλογή λογισμικού και υλικού για firewalls.

2.1. Προσδιορισμός των απαραίτητων τμημάτων υλικού (υπολογιστές, δρομολογητές,επεξεργαστές, μνήμη, δίσκος, κάρτες, καλώδιο κλπ)

2.2. Προσδιορισμός των απαραίτητων τμημάτων λογισμικού

2.3. Προσδιορισμός των εργαλείων ελέγχου και διαχείρισης

3.Επιλογή του υλικού τεκμηρίωσης, της εκπαίδευσης και της υποστήριξης

3.1. Προσδιορισμός των απαιτήσεων εκπαίδευσης.

3.2. Προσδιορισμός των αναγκών σε υποστήριξη. Επιλογή υποστήριξης σε 24ωρη, 3 ημερών, ανά κλήση, κ.λ.π.

4.Εγκατάσταση του υλικού και του λογισμικού του firewall

5. Διαμόρφωση της δρομολόγησης IP.

6.Διαμόρφωση του φιλτραρίσματος πακέτων στο firewall

6.1. Σχεδιασμός των κανόνων φιλτραρίσματος των πακέτων, με κριτήρια στοιχεία από την επικεφαλίδα του πακέτου, όπως διεύθυνση αποστολέα, παραλήπτη, πρωτόκολλο, θύρα αποστολής, θύρα παραλαβής, μήκος πακέτου, πληροφορία κατάστασης σύνδεσης. Σαν αρχή για την δημιουργία κανόνων για πρώτη φορά έχουμε τα ακόλουθα:

- Γενικά ο κανόνας είναι deny all packets
- Σχεδιάζουμε κανόνες anti-spoofing και τους τοποθετούμε στην αρχή της λίστας των κανόνων
- Δημιουργούμε ένα πίνακα με τους αποστολείς και παραλήπτες πακέτων με τα πρωτόκολλα και τις θύρες που χρησιμοποιούνται στην συνήθη λειτουργία τους, ώστε να διαπιστώσουμε πως δεν έχουμε αποκλείσει την επικοινωνία κάποιου χρήστη με άλλον ή με υπηρεσία
- Ταξινομούμε τον πίνακα ως προς το πρωτόκολλο και μετά την θύρα (port)
- Συγκεντρώνουμε τα ίδια πρωτόκολλα σε μια γραμμή και στις επόμενες συνεχόμενα τις θύρες
- Μετατρέπουμε τον πίνακα σε σετ από κανόνες και ης τοποθετούμε ανάμεσα στους κανόνες anti-spoofing και στον κανόνα deny all

6.2. Προσοχή χρειάζεται στις ακόλουθες περιπτώσεις:

- Σε ορισμένα συστήματα κενή λίστα κανόνων σημαίνει πως δεν επιτρέπεται να περάσει κυκλοφορία
- Μερικά συστήματα έχουν προκαθορισμένους κανόνες
- Μερικά συστήματα έχουν ξεχωριστούς κανόνες για εισερχόμενα και εξερχόμενα πακέτα.
- Για να λειτουργήσουν κανόνες anti-spoofing πρέπει το firewall να αντιλαμβάνεται την εισερχόμενη και εξερχόμενη κίνηση σε κάθε interface. Χρειάζεται να τεθούν οι κανόνες ανάλογα με την φορά. Το φιλτράρισμα πακέτων πρέπει να Βασίζεται σε IP διευθύνσεις και όχι σε ονόματα κόμβων
- Αν χρειάζεται έλεγχος στα πακέτα UDP (που είναι connectionless πρωτόκολλο), τότε ορισμένες υπηρεσίες πρέπει να «τρέχουν» σε proxies, αλλιώς αν δεν επιτρέψουμε UDP κάποιες υπηρεσίες δεν θα λειτουργούν (π.Χ. το DNS «τρέχει» στο port UDP 53)

6.3. Τεκμηρίωση των κανόνων φιλτραρίσματος πακέτων

7.Εγκατάσταση των μηχανισμών καταγραφής και συναγερμού

7.1. Επιλογή των περιπτώσεων φιλτραρίσματος πακέτων που θα καταγράφονται

7.3. Σχεδιασμός του συστήματος συναγερμού

8.Έλεγχος στο σύστημα firewall

8.1. Δημιουργία πλάνου ελέγχων για πρωτόκολλα, θύρες, υπηρεσίες και χρήστες

8.2. Προμήθεια εργαλείων ελέγχου

8.3. Έλεγχος των λειτουργιών του firewall στο περιβάλλον εργαστηρίου

8.3.1.Απενεργοποίηση του φιλτραρίσματος πακέτων

8.3.2.Εισαγωγή πακέτων που θα εξετάσουν όλους τους κανόνες δρομολόγησης και να σταλούν μέσα από το firewall

8.3.3.Επιβεβαίωση πως τα πακέτα στάλθηκαν σωστά αντιπαραβάλλοντας τα στοιχεία των καταγραφών του firewall και τα ευρήματα του scanner

8.3.4.Ενεργοποίηση του packet filtering

8.3.5.Εισαγωγή πακέτων που περιέχουν δείγμα από όλες τις πιθανές διευθύνσεις αποστολέων, παραληπτών για όλα τα πρωτόκολλα και όλες τις θύρες

8.3.6.Επιβεβαίωση πως τα πακέτα που έπρεπε να αποκλειστούν (deny) αποκλείστηκαν και όλα όσα έπρεπε να περάσουν πέρασαν. Εξετάζουμε τις καταγραφές του firewall και συγκρίνουμε αποτελέσματα.

8.3.7. Διενέργεια ανίχνευσης για ανοικτά και μπλοκαρισμένα ports, για να διαπιστώσουμε πως το firewall λειτουργεί όπως το σχεδιάσαμε.

8.3.8. Αντιπαραβάλουμε όλη την κίνηση που καταγράφηκε σαν συναγερμός αντιστοιχεί με αυτή που έπρεπε να έχει καταγραφεί από τους κανόνες

Εξετάζουμε αν όλοι οι κανόνες που ενεργοποιούν συναγερμούς αποστέλλονται.

8.4. Έλεγχος του firewall στο παραγωγικό περιβάλλον

8.5. Επιλογή και εξέταση λειτουργιών που σχετίζονται με την καταγραφή

8.6. Ανίχνευση για τρωτά σημεία

8.7. Επιλογή επαναλαμβανόμενων τεστ για την επιβεβαίωση της ορθής λειτουργίας σε τακτά χρονικά διαστήματα

8.8. Προετοιμασία για παραγωγική χρήση

8.9. Προετοιμασία για παρακολούθηση της λειτουργίας

9.Εγκατάσραση του firewall

10. Φάση ενεργοποίησης λειτουργίας του συστήματος

10.1. Προετοιμασία μεταγωγής στο νέο σύστημα

10.2. Ενημέρωση χρηστών

10.3. Ενεργοποίηση της ιδιωτικής κίνησης πάνω από το firewall

- Εγκατάσταση των συνδέσεων του διαδικτύου και του ιδιωτικού δικτύου στο firewall
- Αλλαγή των defau1t gateways
- Ενημέρωση των πινάκων δρομολόγησης (Update routing table)

7.4. Πρωτόκολλα, Υπηρεσίες και Διαδικασίες για την ασφάλεια

Προκειμένου να ασφαλισουμε ένα δικτύο υπάρχουν κάποια βασικά σημεία τα οποία θα πρέπει να μελετήσουμε και να υλοποιήσουμε. Θα πρέπει να καταβάλλεται προσπάθεια για την προστασία όλων των κρίσιμων στοιχείων του δικτύου. Πολλοί διαχειριστές ασχολούνται μόνο με την ασφάλεια των κόμβων. Προτιμάται να προστατεύονται μόνο οι κόμβοι για δύο λόγους:

είναι κάτι που μπορεί να επιτευχθεί εύκολα

οι hosts είναι τα «στοιχεία» του δικτύου που δέχονται τις περισσότερες επιθέσεις

Παρόλα αυτά είναι εξίσου σημαντική η προστασία όλων των συσκευών του δικτύου. Αν το δίκτυο είναι «ανοιχτό» σε τρίτους, μπορεί κάποιος να αλλάξει την δρομολόγηση των πακέτων και να υποκλέψει κρίσιμη πληροφορία (π.χ. passwords). Μπορεί επίσης να έχει πρόσβαση στο σύστημα διαχείρισης του δικτύου ή σε διάφορες υπηρεσίες του όπως (DNS, NFS, NTP, WWW).

Ένας άλλος παράγοντας που θα πρέπει να λαμβάνεται υπόψη είναι το ανθρώπινο λάθος. Κάποιος διαχειριστής μπορεί να μην κάνει σωστή διαμόρφωση ενός κόμβου, με αποτέλεσμα η προβληματική λειτουργία να επηρεάζει τους χρήστες που χρησιμοποιούν τον συγκεκριμένο host. Το πρόβλημα αυξάνεται όταν γίνει λάθος configuration σε κάποια βασική συσκευή (π.χ. router), όπου επηρεάζονται άμεσα όλοι οι χρήστες του δικτύου.

Υπάρχουν κάποια κλασικά προβλήματα τα οποία κάνουν τρωτό ένα δίκτυο. Ένα από αυτά είναι η μη διαθεσιμότητα της υπηρεσίας μετά από κάποια επίθεση. Στην περίπτωση αυτή δεν είναι δυνατή η μμεταφορά δεδομένων. Ένα δίκτυο έρχεται στην κατάσταση αυτή με δύο τρόπους:

- ✓ Επίθεση στους δρομολογητές.
- ✓ Συμφόρηση (flooding) του δικτύου.

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι με τον όρο δρομολογητής εκτός από τις κλασσικές συσκευές δρομολόγησης εννοούνται και «στοιχεία» όπως firewalls, proxy servers κ.α.

Η επίθεση σε ένα δρομολογητή έχει σκοπό τη διακοπή της μεταφοράς των πακέτων ή την προώθηση τους σε λάθος σημείο. Σε αυτήν την κατάσταση μπορεί να βρεθεί ένας δρομολογητής όταν δεν έχει σωστό configuration ή όταν βομβαρδίζεται με πακέτα που δεν προλαβαίνει να δρομολογήσει με αποτέλεσμα να μειώνεται σταδιακά η απόδοσή του.

Η συμφόρηση ενός δικτύου διαφέρει από αυτή του δρομολογητή γιατί τα πακέτα απευθύνονται σε όλες τις συσκευές του δικτύου (broadcast). Η «ιδανική» συμφόρηση επιτυγχάνεται όταν ένα πακέτο πηγαίνει σε όλους τους κόμβους του δικτύου οι οποίοι το στέλνουν πάλι ή δημιουργούν προβληματικά πακέτα τα οποία συλλέγονται από τους hosts που με τη σειρά τους τα προωθούν ξανά.

Ένα άλλο κλασικό πρόβλημα είναι αυτό του spoofing (υποκλοπή της πληροφορίας). Στην περίπτωση του spoofing τα πακέτα, προτού φτάσουν στον παραλήπτη, περνούν από κάποιον ενδιάμεσο host. Η διάγνωση του spoofing είναι γενικά δύσκολη, γιατί τις περισσότερες φορές η πληροφορία που φτάνει στον παραλήπτη δεν αλλοιώνεται.

Για την επίλυση των προαναφερόμενων προβλημάτων χρησιμοποιούνται γνωστά πρωτοκόλλα όπως το RIP-2 και το OSPF.

Με τη χρήση password επιτυγχάνεται η ελάχιστα απαιτούμενη προστασία του δικτύου αφού δεν είναι δυνατή η άμεση πρόσβαση στους πόρους του από κάποιον τρίτο. Υπάρχουν τα ακόλουθα επίπεδα προστασίας:

- ✓ CIear text password
- ✓ Cryptographic checksum
- ✓ Encryption

Με τη χρήση συνθηματικών δεν επιβαρύνονται η CPU και το bandwidth. Με τον έλεγχο ισοτιμίας (checksum) δεν είναι δυνατό να περάσουν πακέτα που δεν ανήκουν στο δίκτυο ακόμη και όταν ο εισβολέα ς έχει άμεση πρόσβαση στους πόρους του δικτύου. Η καλύτερη προστασία του δικτύου επιγχάνεται με την κρυπτογράφηση όλης της πληροφορίας καθώς και των routing updates. Με τον τρόπο αυτό ένας εισβολέας είναι δύσκολο να καταλάβει την τοπολογία του δικτύου. Το μειονέκτημα της κρυπτογράφησης είναι το overhead που έχουμε κατά την διαδικασία των updates.

Τόσο το RIP-2 όσο και το OSPF υποστηρίζουν την χρήση των συνθηματικών (clear text password). Ορισμένες φορές είναι δυνατόν να υποστηρίzουν και MO5 κρυπτογράφηση.

Δυστυχώς δεν υπάρχει ακόμη σίγουρη προστασία σε περιπτώσεις συμφόρησης του δικτύου. Το θετικό στην περίπτωση αυτή είναι ότι η συμφόρηση είναι άμεσα εμφανής και μπορεί να αντιμετωπιστεί με σχετικά απλούς τρόπους.

Σε περίπτωση που μας ενδιαφέρει η διασύνδεση επιχειρήσεων, οργανισμών, καταναλωτών και πελατών πρέπει να υπάρχει ένα είδος συνεννόησης για τα standards που θα χρησιμοποιηθούν στην επέκταση του επιχειρηματικού δικτύου μέχρι τον πελάτη. Τα standards που έχουν συμφωνηθεί αφορούν διαμορφώσεις των firewalls, μηχανισμούς ψηφιακής πιστοποίησης, πρακτικές διακίνησης εφαρμογών και δομές για την ανταλλαγή δεδομένων. Όλο και περισσότερες εταιρίες εγκαταλείπουν τα ιδιόκτητα κλειστά πρωτόκολλα και εφαρμογές και υιοθετούν τα συνήθη ανοικτά πρωτόκολλα του Internet, με τα οποία μπορούν να παρέχουν σελίδες στο διαδίκτυο, δυνατότητα ηλεκτρονικού ταχυδρομείου για συνεργασία με τους πελάτες τους, να κάνουν χρήση client-server εφαρμογών.

Προσπαθώντας να οδηγήσουμε το δίκτυο στο επόμενο επίπεδο ασφάλειας, έχουμε σαν σύμμαχους την τεχνολογία του διαδικτύου και τα ανοικτά πρωτόκολλα.

Επιπλέον υπάρχουν πολλά είδη υπηρεσιών που προσφέρονται καθεμία με τις δικές της απαιτήσεις για ασφάλεια. Για παράδειγμα μία υπηρεσία που χρησιμοποιείται μόνο εσωτερικά σε ένα site (π.χ. NFS) μπορεί να απαιτεί διαφορετικούς μηχανισμούς προστασίας από μια άλλη που χρησιμοποιείται για πρόσβαση από εξωτερικούς χρήστες. Πολλές φορές ο αποκλεισμός των εξωτερικών προσπελάσεων σε ένα εξυπηρετητή μπορεί λόγω της φύσης της προσφερόμενης υπηρεσίας να αρκεί. Παρόλα αυτά ένας εξυπηρετητής παγκόσμιου ιστού (Web Server), ο οποίος είναι προσπελάσιμος από όλο τον κόσμο, απαιτεί εσωτερική προστασία. Αυτό σημαίνει ότι η υπηρεσία, τα πρωτόκολλα επικοινωνίας και ο εξυπηρετητής πρέπει να προστατεύονται με τέτοιο τρόπο ώστε να αποφεύγεται οποιαδήποτε μη επιτρεπτή πρόσβαση και τροποποίηση των αρχείων από τα οποία αντλείται η προς δημοσίευση πληροφορία.

Από τα παραπάνω φαίνεται ότι οι υπηρεσίες που παρέχονται εσωτερικά πρέπει να διαφοροποιούνται από αυτές που παρέχονται εξωτερικά, γιατί έχουν διαφορετικές απαιτήσεις προστασίας. Αυτό σημαίνει ότι οι δύο αυτοί τύποι των υπηρεσιών πρέπει να είναι εγκατεστημένες ανεξάρτητα σε διαφορετικούς εξυπηρετητές. Ορισμένες φορές, προκειμένου να επιτευχθεί καλύτερο επίπεδο ασφάλειας, σε κάποια sites Ορίζονται ακόμη και διαφορετικά υποδίκτυα άλλα προσβάσιμα από τους εσωτερικούς χρήστες και άλλα προσβάσιμα από οποιονδήποτε για την παροχή των υπηρεσιών αυτών. Στις περιπτώσεις αυτές, πολλές φορές υπάρχει κάποιο firewall το οποίο ενώνει τα διαφορετικά υποδίκτυα. Ιδιαίτερη προσοχή πρέπει να δοθεί στην κατάλληλη λειτουργία του firewal1.

Σε μεγάλους οργανισμούς παρατηρείται το φαινόμενο να υπάρχει αυξανόμενο ενδιαφέρον για τη χρήση intranets, μέσω των οποίων επιτυγχάνεται η διασύνδεση διαφορετικών τμημάτων ενός οργανισμού (π.χ. τομείς μιας εταιρείας). Μολονότι υπάρχει μία γενική διαφοροποίηση ανάμεσα σε εξωτερικές και εσωτερικές υπηρεσίες, τα sites, που χρησιμοποιούν intranets θα πρέπει να λαμβάνουν υπόψη ότι πρόκειται για μία υπηρεσία που δε θα είναι δημόσια, ούτε τόσο αποκλειστικά ιδιωτική. Επομένως, μια τέτοια υπηρεσία χρειάζεται το δικό της σύστημα για να την υποστηρίζει, το οποίο θα είναι διαφοροποιημένο από τα συστήματα υποστήριξης των εξωτερικών και εσωτερικών υπηρεσιών.

Ένας τύπος εξωτερικών υπηρεσιών που χρήζει ιδιαίτερης αναφοράς, είναι αυτός των υπηρεσιών που επιτρέπουν ανώνυμη πρόσβαση (anonymous ή guest). Τέτοιες υπηρεσίες είναι το ανώνυμο ftp (anonymous ftp) και η μη πιστοποιημένη πρόσβαση (guest login). Είναι εξαιρετικά σημαντικό να διασφαλιστεί ότι οι εξυπηρετητές αυτών των υπηρεσιών είναι προσεκτικά απομονωμένοι από τους υπόλοιπους εξυπηρετητές και ότι στα συστήματα αρχείων δε θα πρέπει να έχουν πρόσβαση εξωτερικοί χρήστες.

Επίσης, ιδιαίτερη μνια χρειάζεται να γίνει για τις υπηρεσίες ανώνυμης πρόσβασης που δίνουν δικαιώματα εγγραφής στους χρήστες (anonymous writable access). Επειδή το site που φιλοξενεί μια υπηρεσία είναι υπεύθυνο για το περιεχόμενο των πληροφοριών που

δημοσιεύει, απαιτείται προσεκτική παρακολούθηση της πληροφορίας που εισάγουν οι ανώνυμοι χρήστες.

Οι πιο δημοφιλείς υπηρεσίες στην κοινωνία των δικτύων και του Διαδικτύου είναι: name service, password key service, authentication / proxy server, electronic mail, www, file transfer & NFS. Εφόσον αυτές είναι οι πιο συχνά χρησιμοποιούμενες υπηρεσίες είναι και τα πιο προφανή σημεία επίθεσης. Επιπλέον, πρέπει να τονιστεί ότι μία επιτυχημένη επίθεση σε μία από αυτές τις υπηρεσίες μπορεί να επιφέρει γενικότερα προβλήματα.

Πρωτόκολλα και υπηρεσίες δικτύων για την ασφάλεια

Ipsec

Ο αρχικός σχεδιασμός του IPv4 δεν είχε λάβει υπόψη του κανένα θέμα ασφάλειας λόγω της φύσης του δικτύου (επιδίωκε να συνδέσει ακαδημαϊκά ιδρύματα). Μετά την τεράστια εξάπλωση που γνώρισε το διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε ένα από τα πιο απαιτητικές ανάγκες στο διαδίκτυο. Για να καλύψει τις ανάγκες αυτές η IETF δημιούργησε το IP Security Working Group με στόχο να σχεδιάσει μία αρχιτεκτονική ασφάλειας και τα αντίστοιχα πρωτόκολλα ώστε να παρέχεται ασφάλεια βασισμένη στην κρυπτογραφία για το IPv6 πρωτόκολλο. Η αρχιτεκτονική αυτή είναι γνωστή και ως IPsec και περιγράφεται στο RFC 182565. Καθώς προχωρούσαν οι εργασίες διαπιστώθηκε ότι η προτεινόμενη αρχιτεκτονική ασφαλείας για το IPv6 μπορούσε να ενσωματωθεί και στο IPv4 και έτσι το τελευταίο ορίστηκε σαν επιπλέον στόχος. Πρέπει να τονιστεί ότι αυτή η αρχιτεκτονική αφορά το πρωτόκολλο IP και δεν προτείνει μία αρχιτεκτονική ασφάλειας για το διαδίκτυο. Ορίζει τις υπηρεσίες ασφάλειας που μπορούν να χρησιμοποιηθούν στο επίπεδο δικτύου τόσο από το IPv4 όσο και από το IPv6. Η υλοποίηση βέβαια αυτών των υπηρεσιών διαφέρει, αφού στο IPv4 θα πρέπει να υπάρχουν οι κατάλληλες AH και ESP επικεφαλίδες στο πεδίο IP Options, κάτι που είναι αρκετά πιο δύσκολο σε σχέση με το IPv6 που αυτές οι λειτουργίες υλοποιούνται εύκολα γιατί έλαβε υπόψη του αυτές τις απαιτήσεις στο σχεδιασμό του.

Οι στόχοι της ασφάλειας στο IP

Η ασφάλεια επιτυγχάνεται αν έχουν επιτευχθεί οι παρακάτω στόχοι:

1. **Πιστοποίηση παραλήπτη**: Αφορά τη δυνατότητα ελέγχου των δεδομένων και της πιστοποίησης ότι ο αποστολέας που μετέδωσε αυτά τα δεδομένα είναι αυτός που φαίνεται στο αντίστοιχο πεδίο του πακέτου.
2. **Ακεραιότητα δεδομένων**: Αφορά τη δυνατότητα ελέγχου των δεδομένων και πιστοποίησης ότι αυτά δεν έχουν αλλαχθεί κατά τη μετάδοσή τους από τον αποστολέα στον παραλήπτη.
3. **Δυνατότητα απορρήτου**: Αφορά τη δυνατότητα μετάδοσης των δεδομένων με τέτοιο τρόπο ώστε να μπορούν να διαβαστούν μόνο από τον ορισμένο παραλήπτη και όχι από τους ενδιάμεσους κόμβους στο μονοπάτι από τον αποστολέα στον παραλήπτη.

Η πιστοποίηση και η ακεραιότητα είναι συχνά στενά συνδεμένες ενώ η δυνατότητα του απορρήτου της μηνύματος επιτυγχάνεται με χρήση κωδικοποιησης με δημόσια κλειδιά, μια μέθοδο με την οποία εξασφαλίζεται ταυτόχρονα και η πιστοποίηση του αποστολέα.

Το πιο σημαντικό πρόβλημα με την ασφάλεια στο διαδίκτυο είναι το γεγονός ότι πρόκειται για ένα εντελώς ανοιχτό δίκτυο, όπου τα πακέτα θα πρέπει να περάσουν από διάφορους κόμβους για τους οποίους κανείς δεν μμπορεί να εγγυηθεί. Έτσι πιθανά είναι να υπάρχουν διάφοροι ανιχνευτές - υποκλοπείς πακέτων (packet sniffers). Ένα τέτοιο περιβάλλον είναι πολύ δύσκολο να ασφαλιστεί έστω και με τη χρήση κωδικοποιήσεων και

ψηφιακών υπογραφών. Η ασφάλεια θα πρέπει να αντιμετωπίζει και θέματα όπως οι επιθέσεις τύπου Denial Of Service, όπου στόχος είναι η δέσμευση όλων των διαθέσιμων πόρων μίας υπηρεσίας ώστε αυτή να μην μπορεί να δοθεί σε άλλους χρήστες, ή οι επιθέσεις τύπου Spoofing, όπου έχει γίνει αλλαγή της διεύθυνσης του αποστολέα ενός πακέτου.

Η ασφάλεια που ορίζει το IPsec

Το IPsec πρότυπο ορίζει τους μηχανισμούς ασφάλειας που μπορούν να χρησιμοποιηθούν από το IP πρωτόκολλο ανεξαρτήτως έκδοσης ώστε να επιτυγχάνεται ασφάλεια στο επίπεδο δικτύου. Ένα σύστημα χρησιμοποιεί το IPsec για να απαιτήσει από τους κόμβους που επικοινωνεί να κάνουν χρήση συγκεκριμένων αλγορίθμων και πρωτοκόλλων ασφαλείας. Το IPsec παρέχει και τα εργαλεία με τα οποία ένα σύστημα μπορεί να διαπραγματευτεί με άλλα συστήματα για να καταλήξουν για παράδειγμα σε κοινή χρήση ενός αλγόριθμου κωδικοποίησης.

Οι υπηρεσίες που μπορούν να θεωρηθούν μέρος του IPsec περιλαμβάνουν:

Έλεγχο πρόσβασης: Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί τον κατάλληλο κωδικό. Υπάρχουν διάφορα πρωτόκολλα ασφάλειας που μπορούν να χρησιμοποιηθούν για να ορίσουν μία ασφαλή ανταλλαγή κλειδιών.

Ακεραιότητα δεδομένων: Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου χωρίς την ανάγκη να ελεγχθεί άλλο πακέτο πριν ή μετά από το πακέτο που πρέπει να ελεγχθεί. Αυτό μμπορεί να επιτευχθεί με χρήση τεχνικών hashing.

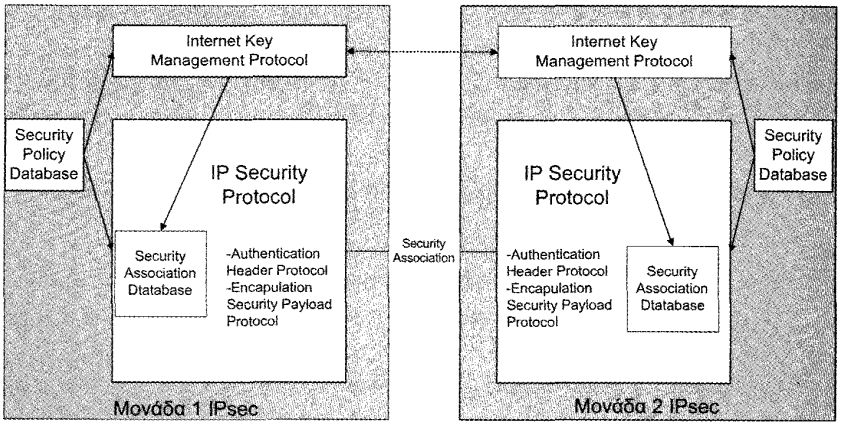
Πιστοποίηση των αποστολέα: Είναι δυνατή η πιστοποίηση του αποστολέα με χρήση των κατάλληλων αλγορίθμων ψηφιακών υπογραφών.

Προστασία εναντίον επιθέσεων τύπου packet replay: Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις όπου ο επιτιθέμενος προσπαθεί να βλάψει τη διαθεσιμότητα του συστήματος, υποκλέπτοντας ένα πακέτο και στέλνοντάς το πολλές φορές στον αποστολέα,

Κωδικοποίηση των δεδομένων: Παρέχονται μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων.

Εξασφάλιση απορρήτου της ροής των δεδομένων: Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων ώστε ο επιτιθέμενος να μην μπορεί να βγάλει συμπεράσματα παρακολουθώντας ένα προς ένα τα πακέτα (που μπορεί να είναι κωδικοποιημένα).

Στην εικόνα που ακολουθεί περιγράφεται η προτεινόμενη από το IPsec αρχιτεκτονική. Γενικά τα πρωτόκολλα του IPsec «τρέχουν» σε ένα δρομολογητή ή σε κάποια πύλη ασφάλειας (secure gateway, πχ ένα σύστημα firewall). Μπορούν φυσικά να υλοποιηθούν σε κόμβους και τελικά συστήματα αλλά κάτι τέτοιο είναι πιο σπάνιο. Κάθε μονάδα του IPsec περιλαμβάνει υλοποιήσεις των IP Security και Internet Key Management πρωτοκόλλων.



Σχήμα 7-17. Η αρχιτεκτονική του IPsec

Εξυπηρετητές Ονοματολογίας (Name Servers) (DNS, NIS(+))

Στο Διαδικτυο η υπηρεσία DNS χρησιμοποιείται για την αντιστοίχηση διευθύνσεων στο δίκτυο IP σε ονόματα υπολογιστών. ΟΙ υπηρεσίες NIS και NIS+ δε χρησιμοποιούνται στο Διαδίκτυο, αλλά υπόκεινται στους ίδιους κινδύνους με αυτούς ενός DNS εξυπηρετητή. Η αντιστοίχηση ενός ονόματος σε μία διεύθυνση είναι κρίσιμη για την ασφαλή λειτουργία ενός δικτύου. Ένας εισβολέας που μπορεί να ελέγξει επιτυχώς ή να απενεργοποιήσει ένα DNS εξυπηρετητή (DNS spoofing), μπορεί να επαναδρομολογήσει τη ροή των πακέτων και να υπονομεύσει τους μηχανισμούς ασφαλείας.

Ένας οργανισμός θα πρέπει να δημιουργεί προστατευμένους κόμβους στα sites για να ενεργούν σαν δευτερεύοντες name servers και να προστατεύουν τους βασικούς DNS servers από επιθέσεις με τη χρήση fittering routers.

Μια υπηρεσία DNS γενικά είναι δύσκολο να προστατευτεί και το αποτέλεσμα σε μια αίτηση δεν είναι δυνατόν να ελεγχθεί αν έχει τροποποιηθεί ή αλλοιωθεί από κάποιον τρίτο.

Μία μέθοδος για την προστασία των DNS υπηρεσιών είναι η ενσωμάτωση ψηφιακών υπογραφών (digital signature) στο πρωτόκολλο, που όταν εφαρμόζεται επιτρέπει τον έλεγχο της ακεραιότητας της πληροφορίας χρησιμοποιώντας κρυπτογράφηση (RFC 2065).

LDAP (Lightweight Directory Access Protocol)

Αυτό το πρότυπο δίνει την δυνατότητα για την καταχώρηση, αποθήκευση και διανομή πληροφοριών επικοινωνίας (contact information), ψηφιακής πιστοποίησης (digital certification), δεδομένων διαμόρφωσης συσκευών (configuration data), κατάσταση εξυπηρετητών (server state information). Με την χρήση αυτού του πρωτοκόλλου είναι δυνατή η προσπέλαση των Χρηστών σε εφαρμογές και υπολογιστές, μέσω του διαδικτύου με πιστοποίηση της ταυτότητάς του.

Κύρια πλεονεκτήματα:

Οι χρήστες μπορούν να αναζητήσουν πληροφορίες για επικοινωνία με στελέχη επιχειρήσεων με τον ίδιο τρόπο που το κάνουν οι εργαζόμενοι στην επιχείρηση.

Υπάρχει τυποποιημένος τρόπος για την αποθήκευση και ανταλλαγή στοιχείων και δεδομένων όπως των X.509 ψηφιακών πιστοποιητικών και των S/MIME πληροφοριών .

Υπάρχει η δυνατότητα για την ασφαλή αντιγραφή των πληροφοριών και σε άλλους εξυπηρετητές συνεργαζόμενων δικτύων.

Επιτρέπει οι εφαρμογές extranet να μπορούν με ένα αξιόπιστο και ταχύ τρόπο να κάνουν ερωτήσεις σε δομημένη πληροφορία.

vCards

Παρέχεται δομημένος τρόπος ανταλλαγής προσωπικών στοιχείων επικοινωνίας. Κάτι σαν ψηφιακή κάρτα στοιχείων που δίνει την δυνατότητα να κοινοποιούνται τα στοιχεία χωρίς να τα γράφουμε συνεχώς κάθε φορά που χρειάζεται.

Στιγμιαίο Συνθηματικό (One-time password)

Προκειμένου να επιτευχθεί η ασφάλεια του δικτύου αποφεύγεται η χρήση passwords που είναι εύκολα προβλέψιμα ή επαναλαμβάνονται με μεγάλη συχνότητα. Πολλές φόρες κάποια προγράμματα γνωστά σαν Δούρειοι Ίπποι (Trojans) καθώς και προγράμματα sniffing υποκλέπτουν password τα οποία χρησιμοποιούνται συχνά ή μεταδίδονται με την μορφή clear text. Προκειμένου να αντιμετωπιστεί αυτό το πρόβλημα αναπτύχθηκαν διάφορες τεχνικές όπως η χρήση συνθηματικών που έχουν ισχύ μόνο μια φορά τα λεγόμενα one-time password. Στην αγορά κυκλοφορούν αρκετά προϊόντα για το σκοπό αυτό.

Kerberos

Το Kerberos είναι ένα κατανεμημένο σύστημα ασφάλειας δικτύου. Τα κύρια χαρακτηριστικά του είναι η παροχή ακεραιότητας (integrity) και κρυπτογράφησης (encryption). Το Kerberos αναπτύχθηκε από το MIT στα μέσα της δεκαετίας του 80. Υπάρχουν δύο βασικές εκδόσεις του Kerberos (4 και 5), οι οποίες για καθαρά πρακτικούς λόγους δεν είναι συμβατές.

Το Kerberos στηρίζεται σε μια βάση συμμετρικών κλειδιών. Υπάρχει ένα κέντρο διανομής κλειδιών (key distribution center - KDC) το οποίο είναι γνωστό σαν Kerberos Server. Σε ένα χρήστη ή μια συσκευή που επικοινωνεί με το KDC παραχωρείται ένα ηλεκτρονικό εισιτήριο. Το εισιτήριο αυτό χρησιμοποιείται για την πιστοποίηση των αρχικών χρηστών / συσκευών. Τα εισιτήρια αυτά έχουν περιορισμένο χρόνο Ζωής.

Η πρακτική σημασία του Kerberos είναι η συμβατότητα του με το επίπεδο εφαρμογών. Κάποιες βασικές εφαρμογές (FTP, Telnet, POP και NFS) συνεργάζονται με το σύστημα αυτό.

Η πιστοποίηση Kerberos στα Windows 2000 υλοποιείται ως εξής:

Όταν ξεκινά η διαδικασία Logon σε ένα σταθμό με Windows 2000 professional, τρέχει το πρόγραμμα Winlogon που αφού του δώσουμε το username/password το περνά στον client Kerberos που είναι ενσωματωμένος στο υποσύστημα ασφάλειας. Αυτός τρέχει μία one-way hashing function (συνάρτηση κρυπτογράφησης) στο password για να δημιουργήσει το CryptoKey. Το CryproKey είναι πολύ ασφαλές, δημιουργείται μόνο μία φορά για κάθε login και δεν στέλνεται πάνω από το δίκτυο. Σκοπός του είναι να συνεισφέρει στην διαδικασία απόκτησης του Ticket Granting Ticket (TGT), ενός ειδικού Session Ticket (ST) που επιτρέπει την πιστοποίηση του client κάθε φορά που ο σταθμός εργασίας ζητά STs για προσπέλαση σε άλλες υπηρεσίες.

Για να πάρει το TGT ο Kerberos client επικοινωνεί με τον Kerberos Distribution Center (KDC), που διαχειρίζεται την διαδικασία πιστοποίησης και την διανομή των κλειδιών. Ο Kerberos client μεταφέρει το username και Ζητά το TGT. Ο KDC εκτελεί τα εξής βήματα:

- ✓ Κοιτά στην Active Directory database για το username που έλαβε και βρίσκει το CryptoKey που του αντιστοιχεί

- ✓ Το KDC φτιάχνει 2 αντίγραφα του Session Key (SK) το μοναδικό κλειδί που χρησιμοποιείται για την επικοινωνία του client με τον KDC.
- ✓ KDC κρυπτογραφεί το ένα αντίγραφο του SK με την χρήση του CryptoKey που βρήκε από την βάση.
- ✓ Ο KDC κρυπτογραφεί το άλλο αντίγραφο του SK με το δικό του CryptoKey. Αυτό είναι το πραγματικό TGT
- ✓ Ο KDC τοποθετεί τα δύο κρυπτογραφημένα μέρη σε ένα datagram (βλ. Σχήμα 7-18) και το στέλνει στον Kerberos client

Όταν ο client λάβει το datagram κάνει τα ακόλουθα:

- ✓ Αποκρυπτογραφεί το πρώτο μέρος του datagram κάνοντας χρήση του CryptoKey του χρήστη και εξάγει το SK Από την στιγμή που το TGT είναι κωδικοποιημένο με το CryptoKey του KDC ο client δεν μπορεί να το αποκωδικοποιήσει μόνος του.
- ✓ Ο kerberos client τοποθετεί το Session Key και το TGT στην cache για μελλοντική χρήση.

Αφού τώρα ο client έχει το TGT όταν χρειάζεται να προσπελάσει μία υπηρεσία το παρουσιάζει στον KDC που με την σειρά του πιστοποιεί τον client και του στέλνει ένα ST για την συγκεκριμένη υπηρεσία. Η διαδικασία που ακολουθείται έχει ως εξής:

1) Ο kerberos client ζητά ένα ST για μια συγκεκριμένη υπηρεσία, π.χ. προσπέλαση σε μία βάση.
2) Ο kerberos client φτιάχνει ένα πακέτο πιστοποίησης και το κωδικοποιεί με το Session Key που έχει λάβει από τον KDC
3) Ο Kerberos client κατόπιν φτιάχνει ένα datagram για αποστολή στον KDC, που περιέχει την κωδικοποιημένη αίτηση, το TGT που έχει στην cache και την αίτηση για την συγκεκριμένη υπηρεσία.

Όταν ο KDC λάβει το TGT πρέπει να επιβεβαιώσει πως προέρχεται πράγματι από ων χρήστη που έχει το Session Key. Μετά μπορεί να στείλει ένα ST για την υπηρεσία στον client. Αυτό γίνεται ως εξής:

1) Ο KDC λαμβάνει το datagram και αποκωδικοποιεί το TGT που περιέχεται σε αυτό. Χρησιμοποιεί το TGT για να εξάγει το Session Key που είχε κωδικοποιήσει νωρίτερα. Αυτό μπορεί να το πετύχει γιατί είναι ο ιδιοκτήτης του CryptoKey. Έτσι ακόμα και αν κάποιος έκλεβε το datagram θα ήταν άχρηστο.
2) Αφού ο KDC αποκτήσει το Session Key το χρησιμοποιεί για να αποκωδικοποιήσει το πακέτο πιστοποίησης που υπήρχε στο datagram. Το γεγονός ότι αυτό το Session Key είναι ικανό να αποκωδικοποιήσει το πακέτο πιστοποίησης αποδεικνύει πως προήλθε από τον client πού κατέχει το Session Key για αυτή τη συνεδρία με ων KDC.
3) Ο KDC διαβάζει την αίτηση για την υπηρεσία, βρίσκει την υπηρεσία που ο client Ζητά προσπέλαση και φτιάχνει ένα ST για την υπηρεσία.

Το ST κατασκευάζει από το KDC με τον ακόλουθο τρόπο:

1) Ο KDC κοιτά στην AD βάση για την υπηρεσία που ζητήθηκε και βρίσκει το CryptoKey για αυτήν.
2) Ο KDC καιοσκευάζει δύο αντίγραφα ενός μοναδικού Session Key για την συνομιλία του client με την υπηρεσία.
3) Ο KDC κωδικοποιεί το ένα αντίγραφο αυτού το Session Key μέσα σε ένα άλλο Session Key που είναι μοναδικό για την συνομιλία του client με το KDC.
4) Ο KDC εξάγει την πληροφορία πιστοποίησης και την κωδικοποιεί μαζί με το άλλο αντίγραφο του Session Key χρησιμοποιώντας το CryptoKey της υπηρεσίας. Αυτό το τμήμα είναι το πραγματικό ST.
5) Ο KDC πακετάρει τα δύο κωδικοποιημένα τμήματα σε ένα datagram και το στέλνει στον Kerberos client.

Όπως ακριβώς στην προηγούμενη περίπτωση, το datagram που παραλήφθηκε από τον clίent περιέχει δύο αντίγραφα του Session Key. Αυτή τη φορά το Session Key είναι μοναδικό για την συνομιλία με την υπηρεσία.

Τώρα, όταν ο client είναι έτοιμος να ανοίξει μία συνομιλία με την υπηρεσία, θα δημιουργήσει μία αίτηση και θα στείλει μία πιστοποίηση και το ST. Αυτή η διαδικασία είναι η ίδια με αυτή που ο clίent Ζήτησε ένα ST για την συνομιλία του clίent με την υπηρεσία, με την εξαίρεση ότι χρησιμοποιεί μία νέα πιστοποίηση και το κωδικοποιεί με το Session Key που είναι μοναδικό για την συνομιλία.

Επιλογή και προφύλαξη των μυστικών κωδικών (Secret Tokens) και των προσωπικών αριθμών αναγνώρισης (PINs)

Η επιλογή των secret tokens θα πρέπει να γίνεται πολύ προσεκτικά ώστε να μην μπορεί εύκολα κάποιος να τα μαντέψει Θα πρέπει να είναι αρκετά μεγάλου μήκους και να αποτελούνται από συνδυασμό μικρών και κεφαλαίων γραμμάτων, ψηφίων και άλλων Χαρακτήρων.

Από τη στιγμή που επιλέγουμε ένα secret token το επόμενο σημαντικό βήμα είναι η λήψη μέτρων για την προστασία του. Κάποια από αυτά χρησιμοποιούνται σαν PINs σε κάποια συσκευή υλικού (Hardware Device - token cards). Αυτά δε θα πρέπει να τοποθετούνται μαζί με το device στο οποίο αντιστοιχούν.

Άλλα όπως τα Pretty Good Privacy (PGP) κλειδιά θα πρέπει να προστατεύονται από ανεπιθύμητη πρόσβαση. Μια σημαντική επισήμανση όταν χρησιμοποιούνται προϊόντα κρυπτογράφησης όπως το PGP είναι πως πρέπει να καθορίζεται το μήκος του κλειδιού και να εκπαιδεύονται οι χρήστες για την σωστή χρήση του.

Εξασφάλιση των συνθηματικών

Υπάρχουν κάποιες γενικές οδηγίες ώστε να αποφευχθούν οι ανεπιθύμητες καταστάσεις που προκύπτουν από τη χρήση κλασικών και επαναχρησιμοποιήσιμων passwords. OI οδηγίες αυτές είναι οι ακόλουθες:

• **Λεξικά συνθηματικών**: Τις περισσότερες φορές προκειμένου να εισχωρήσει σε ένα σύστημα ένας εισβολέας, αυτό που χρειάζεται είναι η πρόσβαση σε ένα λογαριασμό οποιουδήποτε χρήστη. Έτσι αυτό που προσπαθεί να βρει είναι ο κωδικός ενός νόμιμου χρήστη. Αυτό συνήθως γίνεται με την εκτέλεση ενός προγράμματος το οποίο έχει ένα λεξικό με τα πιο κοινά χρησιμοποιούμενα password. Το πρόγραμμα αυτό ελέγχει το αρχείο που κρατά τα passwords των χρηστών του συστήματος (password file) για να βρει κάποιο τετριμμένο αλφαριθμητικό. Για την αποφυγή τέτοιου είδους εισβολών προτείνεται η χρήση δύσκολων και μεγάλου μήκους password.

• **Αλλαγή default passwords**: Πολλά λειτουργικά συστήματα ή προγράμματα εφαρμογών εγκαθίστανται με κάποιους defau1t λογαριασμούς και passwords, τα οποία θα πρέπει να αντικαθιστώνται άμεσα με συνθηματικά που δεν είναι εύκολο να μαντέψει κάποιος.

• **Περιορισμός της πρόσβαση στο password file**: Είναι φανερό πως ένας υπεύθυνος ασφάλειας θέλει να προστατεύσει όλα εκείνα τα αρχεία που περιέχουν κρυπτογραφημένα passwords. Μια αποτελεσματική τακτική που συνήθως εφαρμόζεται είναι η χρήση των shadow passwords, όπου στο αρχείο των passwords υπάρχουν τεχνητά (dummy) ή ψεύτικα password. Το αρχείο με τα κανονικά password προστατεύεται σε κάποιο άλλο σημείο του συστήματος.

• **Χρόνος ισχύος Password**: Ένα θέμα για το οποίο διίστανται οι απόψεις είναι το πότε και πως θα λήγει ένα password. Είναι γενικά αποδεκτή η λήξη ενός password όταν ο αντίστοιχος λογαριασμός γίνεται ανενεργός. Υπάρχουν όμως διαφορετικές απόψεις για το πότε θα αλλάζει ένα password που ανήκει σε κάποιον ενεργό λογαριασμό. Ένας τρόπος είναι η συχνή εναλλαγή του password από το χρήστη. Παρόλα αυτά έχει παρατηρηθεί ότι οι χρήστες που αλλάζουν συχνά το password τους το καταγράφουν συνήθως σε κάποιο εμφανές σημείο για να το θυμούνται ή χρησιμοποιούν εύκολες λέξεις. Γενικά συνιστάται η αλλαγή των passwords των χρηστών τουλάχιστον μια φορά το χρόνο. Αλλαγή θα πρέπει να γίνεται και σε περίπτωση που παραβιασθεί κάποιος λογαριασμός. Τέλος, αν παραβιασθεί κάποιος «προνομιούχος» λογαριασμός (π.χ. ο λογαριασμός του διαχειριστή) είναι καλό να γίνει αλλαγή σε όλα τα password των χρηστών του συστήματος.

• **Password/account blocking**: Σε μερικά site οι λογαριασμοί γίνονται ανενεργοί ύστερα από ένα προκαθορισμένο αριθμό άγονων προσπαθειών πιστοποίησης. Αν κάποιος εφαρμόσει την τακτική αυτή είναι καλό να κρατά το λογαριασμό ανενεργό ακόμη και αν τελικά δοθεί το σωστό password. Προκειμένου ο λογαριασμός να γίνει ξανά ενεργός ο χρήστης θα πρέπει να επικοινωνεί με το διαχειριστή συστήματος.

• **Finger daemon**: Εξορισμού το finger εμφανίζει πολλές σημαντικές πληροφορίες για το σύστημα και το χρήστη. Για παράδειγμα μπορεί να δείξει όλους τους χρήστες που είναι συνδεδεμένοι τη στιγμή εκείνη στο σύστημα ή πληροφορία για ένα συγκεκριμένο χρήστη. Η πληροφορία αυτή χρησιμοποιείται από τους εισβολείς προκειμένου να αναγνωρίσουν τα ονόματα των χρηστών και να μαντέψουν τα passwords τους. Ενδείκνυται η τροποποίηση του finger ώστε η πληροφορία που θα εμφανίζεται για τους χρήστες να περιορίζεται στο ελάχιστο.

Βιομετρικά συστήματα αναγνώρισης

Αν και ο όρος «Βιομετρικά Συστήματα Αναγνώρισης» μπορεί να ακούγεται σαν να προέρχεται από σειρά επιστημονικής φαντασίας, σήμερα, με την βοήθεια της σύγχρονης τεχνολογίας, οι βιομετρικές μέθοδοι προσφέρουν το υψηλότερο επίπεδο ασφάλειας, από τα δίκτυα ATM των μεγαλύτερων τραπεζών μέχρι το προσωπικό υπολογιστικό σας σύστημα.

Παρ' όλο που τα περισσότερα λεξικά ορίζουν τη βιομετρική ως τη στατιστική ανάλυση των βιολογικών χαρακτηριστικών του ανθρώπου, τα τελευταία χρόνια ο όρος τείνει να ταυτιστεί με την επιστήμη που αναλύει τα ανθρώπινα χαρακτηριστικά για σκοπούς ασφαλείας. Πράγματι, το ανθρώπινο σώμα είναι μια τεράστια πηγή μοναδικών γνωρισμάτων που θα μπορούσαν να χρησιμοποιηθούν για αναγνώριση ταυτότητας. Ένα από αυτά μάλιστα, τα δακτυλικά αποτυπώματα, ήδη χρησιμοποιείται χρόνια, για τέτοιους σκοπούς. Με τη βοήθεια όμως που της προσφέρουν τα σύγχρονα μέσα, η βιομετρική έρευνα μπορεί να αναλύσει και να βεβαιώσει και άλλα χαρακτηριστικά του ανθρώπινου σώματος, όπως η ίριδα του ματιού, το σχήμα του προσώπου, του χεριού και η χροιά της φωνής, παρέχοντας μεγαλύτερη ακρίβεια και ασφάλεια. Ενώ όλες οι ανώτερες

βιομετρικές μέθοδοι ασχολούνται με τα φυσικά χαρακτηριστικά ενός ατόμου, σιγά-σιγά αρχίζουν να αναπτύσσονται ορισμένες οι οποίες έχουν ως βάση συμπεριφορές, όπως ο ρυθμός πληκτρολόγησης ή η υπογραφή. Όπου και να βασίζονται πάντως (φυσικό χαρακτηριστικό ή συμπεριφορά) οι βιομετρικές μέθοδοι θεωρούνται, αυτή την στιγμή, ότι προσφέρουν το υψηλότερο επίπεδο ασφάλειας από όλα τα υπάρχοντα συστήματα, όπως είναι τα PINs (Personal Identification Numbers Προσωπικοί Αριθμοί Αναγνώρισης), οι κάρτες και τα συνθηματικά.

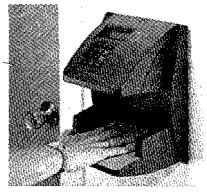
Πολλοί μεγάλοι οργανισμοί, όπως τράπεζες ή κρατικές υπηρεσίες, αρχίζουν δειλά-δειλά να υιοθετούν τη νέα τεχνολογία με σκοπό την αύξηση της ασφάλειας των συστημάτων τους αλλά και την καλύτερη εξυπηρέτηση των πελατών τους. Βέβαια η αγορά έχει και εκπλήξεις. Αν κάνετε μια αναζήτηση στις ηλεκτρονικές αγορές του Internet θα διαπιστώσετε ότι πολλές εταιρείες έχουν κυκλοφορήσει πλήθος από βιομετρικά συστήματα για προσωπικούς υπολογιστές, σε ιδιαίτερα προσιτές τιμές για το μέσο χρήστη (100-150 δολάρια).

Όπως έχουμε πει η αναγνώριση γίνεται κύρια με τρεις τρόπους: με κάτι που ο χρήστης ξέρει (π.χ. λέξη κωδικό), με κάτι που έχει (π.χ. μια ταυτότητα ή μια έξυπνη κάρτα), με κάτι που είναι (π.χ. δακτυλικό αποτύπωμα, ίριδα) ή με συνδυασμούς τους (π.χ. μια έξυπνη κάρτα κι έναν κωδικό).

Αν προσπαθούσαμε να κατατάξουμε τα είδη των συστημάτων ασφάλειας με βάση την αποδοτικότητά τους, θα καταλήγαμε σίγουρα στο εξής συμπέρασμα: στο χαμηλότερο επίπεδο ασφάλειας είναι τα συστήματα όπου το προς αναγνώριση άτομο είναι κάτοχος κάποιου αναγνωριστικού, όπως μια ταυτότητα με φωτογραφία. Τέτοια συστήματα είναι κυριολεκτικά γεμάτα μειονεκτήματα, αφού το αναγνωριστικό μπορεί να χαθεί, καταστραφεί ή και να παραποιηθεl ή αναπαραχθεl πολύ εύκολα στα χέρια κάποιου ειδικού. Ένα από τα βασικότερα μειονεκτήματα του συστήματος, λοιπόν, είναι το γεγονός ότι ο ελεγκτής δεν μπορεί να είναι σίγουρος ούτε αν το αναγνωριστικό είναι γνήσιο ούτε αν αυτός που το έχει είναι ο πραγματικός.

Στα αμέσως επόμενο επίπεδο βρίσκονται τα συστήματα όπου ο χρήστης γνωρίζει κάτι Εδώ τα πράγματα είναι κάπως καλύτερα, αλλά το κύριο πρόβλημα παραμένει με κάποια παραλλαγή. Ενώ το μέσο αναγνώρισης (ο κωδικός ή το συνθηματικό) δεν υπάρχει περίπτωση να είναι πλαστό, κανένας δεν μπορεί να διαβεβαιώσει τον ελεγκτή ότι αυτός που το γνωρίζει είναι το εξουσιοδοτημένο άτομο.

Στο τρίτο επίπεδο υπάρχουν τα συστήματα που αποτελούν συνδυασμό των δύο προηγούμενων. Εδώ, όπως είναι φανερό κατατάσσεται το σύστημα των τραπεζικών καρτών με τα PINs. Αν και υπάρχει σαφής βελτίωση στην αποτελεσματικότητα, κανένα τέτοιο σύστημα δεν είναι πλήρως ασφαλές και αδιάβλητο.



Στο τελευταίο επίπεδο, αυτό της υψηλότερης ασφάλειας, η αναγνώριση γίνεται από κάτι το οποίο ο χρήστης είναι ή κάτι που ο χρήστης κάνει (αναγνώριση με βάση την συμπεριφορά) Τα δακτυλικά αποτυπώματα, για παράδειγμα, είναι μοναδικά για κάθε άνθρωπο. Έτσι, αντί να είστε υποχρεωμένοι να πληκτρολογείτε το PIN σας κάθε φορά που πηγαίνετε στην τράπεζα για να κάνετε ανάληψη από το ATM, θα μπορούσατε να τοποθετείτε τον δείκτη σας στην ειδική υποδοχή.

Αποτελούν, λοιπόν οι Βιομετρικές μέθοδοι τα τέλεια συστήματα ασφάλειας; Δυστυχώς, κανένα σύστημα δεν είναι τέλειο. Τα φυσικά χαρακτηριστικά των ανθρώπων αλλάζουν είτε από το χρόνο είτε από αστάθμητους παράγοντες, όπως ατυχήματα. Φαντασθείτε στο παραπάνω σενάριο με το ATM, ο δείκτης σας να τραυματιζόταν με κάποιο τρόπο. Το μηχάνημα δεν θα μπορούσε να αναγνωρίσει πια το δακτυλικό σας αποτύπωμα! Παρόμοιο πρόβλημα θα είχε και κάποιος εργαζόμενος που θα δοκίμαζε να κάνει ανάληψη με τα χέρια του υπερβολικά λερωμένα από την δουλειά.

Για να καταστεί δυνατή η βιομετρική αναγνώριση κάποιου ατόμου, προηγείται -όπως είναι φυσικό- μια διαδικασία λήψης του βιομετρικού δείγματος. Στην πραγματικότητα, λαμβάνεται από το άτομο ένας αριθμός δειγμάτων (συνήθως 3), τα οποία συνδυάζονται βελτιώνοντας και συμπληρώνοντας το ένα το άλλο, ώστε το αποτέλεσμα που θα προκύψει να είναι όσο το δυνατό τελειότερο. Με αυτόν τρόπο κατασκευάζεται ένα βιομετρικό πρότυπο, με το οποίο θα συγκρίνεται κάθε φορά το δείγμα που θα λαμβάνεται όταν ο χρήστης ζητά την είσοδο του στο προστατευμένο σύστημα. Το βήμα αυτό είναι από τα σημαντικότερα, αφού η ποιότητα του προτύπου θα κρίνει κατά το μεγαλύτερο ποσοστό την αξιοπιστία του όλου συστήματος. Τη δημιουργία του Βιομετρικού προτύπου ακολουθεί το στάδιο της αποθήκευσής του.

Τέλος, έχουμε την διαδικασία εισόδου του χρήστη στο σύστημα, κατά την οποία λαμβάνεται ένα νέο βιομετρικό δείγμα προκειμένου να συγκριθεί με το βιομετρικό πρότυπο. Αν το δείγμα ταιριάζει έστω και με μικρές αποκλίσεις (εξαρτάται πόσο αυστηρά έχει ρυθμιστεί να συμπεριφέρεται το σύστημα), η είσοδος επιτρέπεται.

Δακτυλικά αποτυπώματα

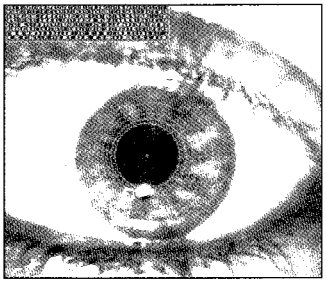
Χωρίς να προσφέρουν τη μέγιστη ακρίβεια, τα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων αποτελούν μια παλιά μέθοδο εξακρίβωσης ταυτότητας. Τα δακτυλικά αποτυπώματα κλείνουν σχεδόν έναν αιώνα πρακτικής εφαρμογής. Ακριβώς αυτή η τεχνογνωσία και το γεγονός ότι δεν απαιτείται ακριβός εξοπλισμός για αυτή τη μέ θοδο βιομετρικής αναγνώρισης, οι πρώτες εφαρμογές ήταν αυτές που έκαναν χρήση δακτυλικών αποτυπωμάτων. Για την αναγνώριση του αποτυπώματος χρησιμοποιούνται διάφορες μμέθοδοι.

Οπτική ανάγνωση: Η μέθοδος μοιάζει αρκετά με την διαδικασία των κοινών scanners. Ο χρήστης αρχικά τοποθετεί το δάκτυλό του στην γυάλινη πλάκα. Στην συνέχεια, και αφού η άκρη του δακτύλου φωτιστεί κατάλληλα, λαμβάνεται η εικόνα του δακτυλικού αποτυπώματος. Οι οπτικοί αναγνώστες δακτυλικών αποτυπωμάτων είναι σήμερα οι πιο συνηθισμένοι. Στο Σχήμα 7-21. φαίνονται τα κύρια σημεία στην αναγνώριση των δακτυλικών αποτυπωμάτων. Πάντως στο διαδίκτυο περιγράφεται διαδικασία που με χρήση μεθόδων ανάλογων των αστυνομικών αρχών είναι δυνατή η «υποκλοπή» και παράνομη χρήση δακτυλικών αποτυπωμάτων, από το γυαλί του scanner.

Ανάγνωση με υπέρηχους: Η μέθοδος αυτή χρησιμοποιεί κύματα υπερήχων. Τα κύματα αυτά «βομβαρδίζουν» το δάκτυλο του χρήστη μετρώντας την πυκνότητα των δακτυλικών αποτυπωμάτων. Το εμφανές πλεονέκτημα της μεθόδου είναι ότι δεν απαιτεί άμεση επαφή του δακτύλου με τον scanner. Κάτι τέτοιο σημαίνει ότι δεν επηρεάζεται από πολύ λερωμένα δάκτυλα.

Θερμική ανάγνωση και ανάγνωση αφής: Η μέθοδος αυτή κάνει χρήση εξελιγμένων chips με αποτέλεσμα να αυξάνεται το κόστος του εξοπλισμού. Ο χρήστης τοποθετεί το δάκτυλό του σε κάποιον αισθητήρα, ο οποίος λαμβάνει την θερμότητα ή την πίεση από το δάκτυλο και την μετατρέπει σε δεδομένα. Βέβαια υπάρχουν προβλήματα όταν ο χρήστης έχει πυρετό ή έχει παγωμένα χέρια. Παρόλα αυτά όμως η μέθοδος είναι αρκετά ακριβής στην αναγνώριση.

Εξέταση ίριδας και αμφιβληστροειδούς



Λέγεται πως τα μοναδικά χαρακτηριστικά της ίριδας και του αμφιβληστροειδούς καθιστούν την τεχνητή αναπαραγωγή τους αδύνατη. Δεν αποτελεί, λοιπόν, έκπληξη το γεγονός ότι τα βιομετρικά συστήματα που βασίζονται στα δύο αυτά μέρη του ματιού είναι τα ακριβέστερα και προσφέρουν τη μεγαλύτερη ασφάλεια.

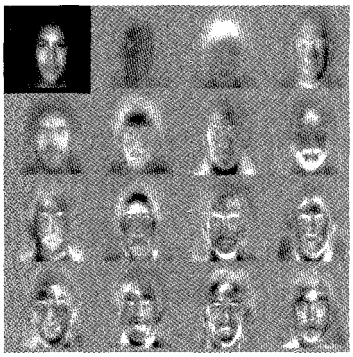
Εκτός από τη μοναδικότητα τους, η ίριδα και ο αμφιβληστροειδής χιτώνας συγκεντρώνουν και ορισμένες άλλες ιδιότητες: τα καθιστούν θαυμάσια επιλογή για την αναγνώριση της ταυτότητας ενός ατόμου αφού επηρεάζονται ελάχιστα από το πέρασμα του χρόνου, ενώ δεν υφίστανται εύκολα τραυματισμούς ή δεν επηρεάζονται από την κούραση. Η εξέταση αμφιβληστροειδούς, θεωρείται η ασφαλέστερη βιομετρική μέθοδος με πρακτικά μηδενικές πιθανότητες παραβίασης.

Εξέταση ίριδας: Η διαδικασία εξέτασης της ίριδας είναι σχετικά απλή:

Μία κάμερα συλλαμβάνει την εικόνα της ίριδας την μετατρέπει σε ψηφιακή μορφή και εφαρμόζει έναν αλγόριθμο που τη μετατρέπει σε ένα είδος μοναδικού μαθηματικού κώδικα, τον οποίο συγκρίνει στη συνέχεια με το βιομετρικό πρότυπο.

Εξέταση αμφιβληστροειδούς: Αν και η εξέταση αμφιβληστροειδούς θεωρείται αυτή τη στιγμή η ασφαλέστερη βιομετρική μέθοδος, η μεγάλη συμμετοχή πού απαιτεί από την πλευρά του χρήστη, την κάνει να θεωρείται η πιο δύσχρηστη. Ο χρήστης τοποθετείται γύρω στους 7 πόντους μπροστά από ένα προσοφθάλμιο και προσπαθεί να εστιάσει μέσα από αυτό για μερικά δευτερόλεπτα σε μία πράσινη κουκίδα. Κάποια στιγμή το μάτι αποκτά τη σωστή εστίαση και ένας scanner συλλαμβάνει τη διάταξη των αιμοφόρων αγγείων που βρίσκονται στο κέντρο του αμφιβληστροειδούς. Από το σημείο αυτό η διαδικασία είναι ίδια με αυτή που ακολουθείται κατά την εξέταση ίριδας.

Αναγνώριση φωνής



Η αναγνώριση φωνής είναι ένα υβριδικό σύστημα που συνδυάζει φυσικά χαρακτηριστικά με συμπεριφορές. Η χροιά και ο τόνος της φωνής εξαρτώνται από πολλά στοιχεία, όπως το μήκος των φωνητικών χορδών, το σχήμα της ρινικής κοιλότητας, του στόματος και του λάρυγγα. Στις χαρακτηριστικές φυσικές ιδιότητες της φωνής για κάθε άνθρωπο, προστίθενται και χαρακτηριστικά συμπεριφοράς, όπως η ταχύτητα ομιλίας και ο τονισμός, που διασφαλίζουν επιπλέον την μοναδικότητα του δείγματος. Τα προβλήματα που πρέπει να αντιμετωπιστούν έχουν να κάνουν με την αλλοίωση της χροιάς και του τόνου, όταν ένας άνθρωπος είναι κρυωμένος, (σε αυτό βοηθά το δεύτερο τμήμα ανάλυσης της συμπεριφοράς) ή όταν υπάρχει θόρυβος από το περιβάλλον.

Γεωμετρία προσώπου

Με τη μέθοδο αυτή εξετάζονται τα χαρακτηριστικά του προσώπου ενός ανθρώπου για να βεβαιώσουν την ταυτότητά του. Η μέθοδος προσπαθεί να εντοπίσει μερικά βασικά σημεία της εικόνας που συλλαμβάνει, όπως μέγεθος ματιών, αποστάσεις από τα άκρα, θέση στο πρόσωπο, σχήμα μύτης και στόματος αποστάσεις μεταξύ του κλπ. Το σύστημα έχει να αντιμετωπίσει αρκετά προβλήματα που έχουν να κάνουν με την γήρανση, την αύξηση του βάρους, την αλλαγή στην εμφάνιση με μούσι ή μουστάκι, τα μαλλιά. Ο τρόπος αντιμετώπισης των προβλημάτων αυτών γίνεται με μεθόδους τεχνικής νοημοσύνης και αυτοεκπαίδευσης, συγκρίνοντας τα χαρακτηριστικά με το πρότυπο και διορθώνοντας με την πάροδο του χρόνου το πρότυπο (προφανώς υπάρχουν και προβλήματα που δεν λύνονται όπως μία πλαστική προσώπου!).

Εξακρίβωση υπογραφής

Το σύστημα αυτό εξετάζει βιομετρικές παραμέτρους στην διαδικασία της υπογραφής και δεν προσπαθεl να συγκρινει την εικόνα της υπογραφής με ένα αποθηκευμένο πρότυπο. Οι παράμετροι που εξετάζονται έχουν να κάνουν με το χρόνο που χρειάζεται ο χρήστης να τελειώσει την υπογραφή του, την γωνια κλισης του στυλό, τις αλλαγές στην επιτάχυνση κατά την διάρκεια γραφής, την πιεση πάνω στην επιφάνεια γραφής, αλλά και

πόσες φορές σηκώθηκε το στυλό από το χαρτί. Η μέθοδος αυτή έχει την μεγαλύτερη αποδοχή, αλλά ακόμα δεν έχει μεγάλη ακρίβεια.

Το μέλλον της βιομετρικής αναγνώρισης

Αν και η μέθοδοι της βιομετρικής αναγνώρισης είναι πρόσφατες, ήδη γίνεται έρευνα σε νέες πιο εξωτικές μεθόδους, όπως ο έλεγχος DNA, n αναγνώριση της σωματικής οσμής, η αναγνώριση της φλεβικής δομής του επάνω μέρους της παλάμης, η αναγνώριση της παλάμης μέσω των γραμμώσεων και των δακτυλικών αποτυπωμάτων, η αναγνώριση της γεωμετριας του αυτιού κλπ.

Δεν υπάρχει ένα τέλειο σύστημα στην βιομετρική τεχνολογια για κάθε εφαρμογή. Το διάγραμμα του Zephyr (βλ. Σχήμα 7-24) δειχνει τα πλεονεκτήματα και τα μειονεκτήματα των εμπορικών προϊόντων που υπάρχουν διαθέσιμα. Τα τέσσερα κριτήρια είναι αυτά που περιγράφουν οι χρήστες και αυτά που επιβάλει η τεχνολογία (Πίνακας 7-1).

ΚριτήριαΧρηστών	**ΚριτήριαΤεχνολογίας**
1. **Προσπάθεια** - Πόσος χρόνος και πππ προσπάθεια χρειάζεται να καταβάλει ο χρήστης	1. **Κόστος** - Το κόστος της συσκευής αναγνώρισης
2. **Διακριτικότητα** - Πόσο διακριτικό πιστεύει ο χρήστης πως είναι το σύστημα.	2**. Ακρίβεια** - Πόσο καλά το σύστημα αναγνωρίζει τα άτομα Πίνακας 7-1. Κριτήρια αξιολόγησης βιομετρικών συστημάτων

Πίνακας 7-1 .Κριτήρια αξιολόγησης βιομετρικών συστημάτων

Κριτήρια χρηστών: Για να απαντήσουμε στην ερώτηση ποιο είναι το καλύτερο βιομετρικό σύστημα, πρέπει να έχουμε στο μυαλό μας την εφαρμογή. Για παράδειγμα, δεν είναι υπερβολικό αν πρόκειται να προσπελάσει ο χρήστης μία εγκατάσταση πυρηνικού αντιδραστήρα, να θεωρήσει ανεκτό να περάσει από μια διαδικασία αναγνώρισης 30", χωρίς να θεωρήσει ενοχλητική την όλη διαδικασία. Αντίθετα αν πρόκειται να εφαρμοστεί ένα βιομετρικό σύστημα για τον έλεγχο ταυτότητας στον κάτοχο ενός εισιτηρίου διαρκείας σε ένα πάρκο αναψυχής, τότε μπορεί να αισθανθεί άβολα και προσβλημένος.

Κριτήρια τεχνολογίας: Οι απαιτήσεις ασφάλειας εξαρτώνται πάλι από την εφαρμογή. Η ακρίβεια του συστήματος μετράται με τους ακόλουθους δείκτες: FAR (False Acceptance Rate - Πιθανότητα λανθασμένης αποδοχής χρήστη) που δίνει την πιθανότητα να γίνει αποδεκτός ένας που προσπαθεί *να* εισέλθει χωρίς προνόμια, FRA (False Rejection Rate - Πιθανότητα λανθασμένης απόρριψης χρήστη) που δίνει την πιθανότητα να απορριφθεί ένα διαπιστευμένος χρήστης και FER (Failure to Enroll Rate- Πιθανότητα αδυναμίας αναγνώρισης) που μετρά την πιθανότητα να μην μπορεί το σύστημα να αναγνωρίσει κάποιον λόγω κακής ποιότητας προτύπου δείγματος.

Το διάγραμμα Zephyr (βλ. Σχήμα 7-24) δείχνει τα δυνατά και αδύνατα σημεία της κάθε τεχνολογίας. Οι επτά βασικές βιομετρικές τεχνολογίες σχεδιάζονται περιμετρικά και τα τέσσερα κριτήρια αξιολόγησης τοποθετούνται από έξω (καλύτερα) προς τα μέσα (χειρότερα).

Σχήμα 7-24. Αξιολόγηση βιομετρικών συστημάτων κατά Zephyr

X.509 v3 Digital Certificates

Με το πρότυπο αυτό προσφέρεται ισχυρή πιστοποίηση δύο μερών, περιεχομένου ή συσκευών συνδεμένων στο δίκτυο, όπως εξυπηρετητές ασφάλειας (secure servers), firewalls, ηλεκτρονικό ταχυδρομείο, ηλεκτρονικές συναλλαγές. Είναι η βάση για την ασφαλή πιστοποίηση στο S/MIME και την ηλεκτρονική διακίνηση εγγράφων στο internet (Electronic Document Interchange over the internet –EDI INT).

Τα ψηφιακά πιστοποιητικά μπορούν να έχουν ισχύ είτε μέσα στο intranet μιας επιχείρησης ή στο extranet ανάμεσα από συνεργαζόμενες επιχειρήσεις μέσω δημόσιων πιστοποιητικών (public certificates) που έχουν εκδοθεί από την επιχείρηση ή από ένα κοινά αποδεκτό οργανισμό πιστοποίησης όπως η VeriSign.

Τα πιστοποιητικά είναι ανώτερα από την χρήση λέξεων κλειδιών (passwords) γιατί παρέχουν ισχυρή πιστοποίηση λόγω της πιστοποίησης της ταυτότητας, της πιστοποίησης της αυθεντικότητας του περιεχομένου ενός μηνύματος (ότι πράγματι έχει σταλεί το συγκεκριμένο περιεχόμενο από το συγκεκριμένο αποστολέα), διασφαλίζει το απόρρητο, διασφαλίζει την προσπέλαση από εξουσιοδοτημένους χρήστες, διασφαλίζει τις συναλλαγές και υποστηρίζει την επικύρωση των πράξεων μη δίνοντας τη δυνατότητα αποποίησης ευθυνών (non-repudiation).

Κύρια πλεονεκτήματα:

- Τα ψηφιακά πιστοποιητικά εξαλείφουν την διαδικασία συμπλήρωσης των στοιχείων του διαλόγου login-password, όταν επιχειρείται η σύνδεση σε μία υπηρεσία.
- Το κάθε μέρος της ηλεκτρονικής συναλλαγής (είτε πρόκειται για προσπέλαση σε υπηρεσία, είτε για αγορά και πληρωμή υπηρεσιών) είναι σίγουρο για την ταυτότητα του άλλου.
- Τα ψηφιακά πιστοποιητικά διασφαλίζουν πως μόνο ο σωστός παραλήπτης μπορεί να διαβάσει τα μηνύματα που στέλνουμε.
- Μπορούν να φτιαχτούν εξεζητημένα προνόμια προσπέλασης σε υπηρεσίες, ώστε να είναι δυνατή η δημιουργία διαφορετικών επιπέδων συνδιαλλαγών στο internet.

S/MIME

Χρησιμοποιείται για την αποστολή μηνυμάτων ανάμεσα σε χρήστες και εφαρμογές κάνοντας χρήση ψηφιακής πιστοποίησης και κωδικοποίησης. Το πρωτόκολλο αυτό δίνει την δυνατότητα ανταλλαγής εμπιστευτικών μηνυμάτων, χωρίς τον φόβο να διαβαστεί από λάθος άτομα. Χρησιμοποιείται κύρια στο ηλεκτρονικό ταχυδρομείο.

Signed objects

Επιτρέπει την ασφαλή διακίνηση και εκτέλεση εφαρμογών ή applets από χρήστες ή κόμβους που εμπιστευόμαστε. Με την ταυτόχρονη χρήση ψηφιακού πιστοποιητικού του αποστολέα μπορούμε να επιτρέπουμε αυτόματα την λήψη και εκτέλεση εφαρμογών μέσα από το διαδίκτυο.

EDI INT

Το πρότυπο αυτό δίνει οδηγίες για την συνδυασμένη χρήση υπαρχόντων EDI standards για την μετάδοση δεδομένων συναλλαγών μέσω της ομάδας πρωτοκόλλων του internet. Με ταυτόχρονη χρήση S/MIME και ψηφιακών πιστοποιητικών, οι συναλλαγές ηλεκτρονικού εμπορίου μπορούν να εκτελούνται με ασφαλή και προκαθορισμένο τρόπο.

Εξυπηρετητές Πιστοποίησης (Authentication/Proxy Servers) (SOCKS, FWTK)

Ένας proxy εξυπηρετητής μπορεί να δώσει πολλές εναλλακτικές λύσεις για την ασφάλεια ενός δικτύου. Επιτρέπει σε ένα site να συγκεντρώσει κάποιες υπηρεσίες σε ένα host και να διαφυλάξει την εσωτερική του δομή. Η ασφάλεια που απαιτείται για ένα proxy εξυπηρετητή είναι άμεσα συνδεδεμένη με τα proxy πρωτόκολλα που χρησιμοποιούνται καθώς και με τις υπηρεσίας που θα πρέπει να περάσουν μέσα από τον proxy. Ένας γενικός κανόνας που ακολουθείται είναι η περιορισμένη πρόσβαση σε συγκεκριμένους hosts καθώς και η πρόσβαση σε συγκεκριμένες υπηρεσίες.

Εξυπηρετητές Συνθηματικών/Κλειδιών (Password/Key Servers, Digital Signature-NIS+, KDC)

Οι password / key servers προστατεύουν ζωτικής σημασίας πληροφορίες (password ή κλειδιά), χρησιμοποιώντας αλγορίθμους κρυπτογράφησης. Παρόλα αυτά ακόμη και ένα κρυπτογραφημένο password μπορεί να βρεθεί, όταν περάσει μέσα από ένα λεξικό (κάποιες πολύ γνωστές λέξεις κρυπτογραφούνται και ο εισβολέα ς που διαθέτει ένα τέτοιο λεξικό βλέπει αν το password ταιριάζει με κάποιες από αυτές τις λέξεις). Για το λόγο αυτό θα πρέπει να απαγορεύεται η πρόσβαση σε τρίτους σε τέτοιους εξυπηρετητές (π.χ. οι υπηρεσίες Telnet, Ftp δε θα πρέπει να επιτρέπονται σε κανένα άλλο εκτός από τους διαχειριστές).

Ηλεκτρονικό Ταχυδρομείο (Electronic mail)

Τα συστήματα που χρησιμοποιούνται για το ηλεκτρονικό ταχυδρομείο είναι πόλος έλξης για τους εισβολείς και αυτό γιατί το ηλεκτρονικό ταχυδρομείο είναι από τις παλαιότερες και τις ευρύτερα εφαρμοσμένες υπηρεσίες. Επίσης ένας εξυπηρετητής ηλεκτρονικού ταχυδρομείου θα πρέπει να είναι προσπελάσιμος από τον έξω κόσμο και να δέχεται δεδομένα από οποιαδήποτε πηγή. Τα συστατικά ενός εξυπηρετητή ηλεκτρονικού ταχυδρομείου είναι τα εξής:

- Πράκτορας λήψης / αποστολής (receiving / sending agent) .
- Πράκτορας επεξεργασίας (processing agent).

Από τη στιγμή που το ηλεκτρονικό μήνυμα παραδίδεται σε όλους τους χρήστες ο πράκτορας επεξεργασίας «processing agent» απαιτεί συνήθως δικαιώματα διαχειριστή (root privileges) ώστε να παραδώσει το μήνυμα. Καλό θα είναι για την ασφάλεια του συστήματος ηλεκτρονικού ταχυδρομείου να είναι ο πράκτορας επεξεργασίας «processing agent» διαφορετικός από τον πράκτορα λήψης/αποστολής «receiving/sending agent». Γενικά απαιτείται μεγάλη προσοχή κατά την εγκατάσταση του συστήματος ηλεκτρονικού ταχυδρομείου ώστε να αποφευχθούν προβλήματα ασφαλείας.

Παγκόσμιος Ιστός (World Wide Web)

Υπάρχει μία εκθετική αύξηση των εξυπηρετητών παγκόσμιου ιστού που οφείλεται στην ευκολία της χρήσης τους καθώς και στην ικανότητα που έχουν να συγκεντρώνουν υπηρεσίες παροχής πληροφοριών. Ορισμένοι χρήστες που προσπελαύνουν αυτούς τους εξυπηρετητές είναι δυνατό να εκτελέσουν κάποιες λειτουργίες όπως για παράδειγμα όταν επιθυμούν να κάνουν μία αίτηση, ο εξυπηρετητής για να ανταποκριθεί στις απαιτήσεις της αίτησης πρέπει εκτελέσει κάποιο πρόγραμμα. Ορισμένοι προγραμματιστές που υλοποιούν αυτά τα προγράμματα δε λαμβάνουν τα απαιτούμενα μέτρα ασφαλείας γι' αυτές τις περιπτώσεις, με αποτέλεσμα να κάνουν το σύστημα ευάλωτο σε εξωτερικές επιθέσεις. Όταν κάποιος υπολογιστής φιλοξενεί έναν εξυπηρετητή παγκόσμιου ιστού, δε θα πρέπει να φυλάσσονται απόρρητες πληροφορίες σε αυτό το μηχάνημα.

Σε πολλά sites χρησιμοποιείται ο ίδιος υπολογιστής σαν FTP εξυπηρετητής ή WWW εξυπηρετητής. Στην περίπτωση αυτή θα πρέπει ο FTP εξυπηρετητής να απαντά μόνο σε «get» αιτήσεις, διαφορετικά (αιτήσεις put) είναι δυνατό να αντικαταστήσουν αρχεία του εξυπηρετητή web.

Μεταφορά Αρχείων (File transfer FTP, TFTP)

Το FTP όπως και το TFTP προσφέρουν υπηρεσίες μεταφοράς αρχείων. Το FTP απαιτεί πιστοποίηση (authentication), ενώ το TFTP όχι. Για το λόγο αυτό είναι καλό να αποφεύγεται το TFTP.

Οι FTP εξυπηρετητές που δεν έχουν σωστή διαμόρφωση (configuration), δίνουν την δυνατότητα σε εισβολείς να αντιγράφουν, να αντικαθιστούν ή να σβήνουν αρχεία του υπολογιστή που φιλοξενεί την εν λόγω υπηρεσία. Από τα πιο συνηθισμένα φαινόμενα που μπορεί να παρουσιαστούν σε έναν εξυπηρετητή με λάθος διαμόρφωση είναι η πρόσβαση σε κρυπτογραφημένα αρχεία password και ιδιωτικά αρχεία, καθώς και η εισαγωγή Δούρειων Ίππων (Trojan Horses).

Μία βασική αρχή για την ασφάλεια ενός δικτύου είναι ότι «Οι υπηρεσίες που προσφέρονται εσωτερικά σε ένα site δε θα πρέπει να συνυπάρχουν με τις υπηρεσίες που προσφέρονται εξωτερικά». Το TFTP δεν παρέχει καμία απολύτως ασφάλεια, είναι μία υπηρεσία για εσωτερική και μόνο χρήση και θα πρέπει να είναι πολύ καλά ορισμένη (μέσω του TFTP εξυπηρετητή να επιτρέπεται πρόσβαση μόνο σε προκαθορισμένα αρχεία). Ένας TFTP εξυπηρετητής χρησιμοποιείται κυρίως για να γίνονται download τα αρχεία για τη διαμόρφωση των Δρομολογητών.

Δικτυακές Υπηρεσίες Αρχειοθέτησης (NFS)

Το NFS (Network File Service) δίνει τη δυνατότητα σε διάφορους hosts να διαμοιράζονται κοινούς δίσκους. Το NFS χρησιμοποιείται συχνά από υπολογιστές οι οποίοι δεν έχουν σκληρούς δίσκους αλλά εξαρτώνται από κάποιο disk server. Το NFS δεν έχει ενσωματωμένο σύστημα ασφάλειας. Ένας εξυπηρετητής συνιστάται να είναι προσπελάσιμος μόνο από τους υπολογιστές που χρησιμοποιούν τις υπηρεσίες του. Αυτό μπορεί να επιτευχθεί με τον προσδιορισμό του υπολογιστή του οποίου το σύστημα αρχείων είναι προσπελάσιμο και με ποια δικαιώματα. (π.χ. read-only, read-write κ.α.). Η

διαμοίραση των συστημάτων αρχείων είναι μια υπηρεσία που πρέπει να προσφέρεται μόνο εσωτερικά σε ένα δίκτυο. Γενικά, η εξωτερική πρόσβαση στο διαμοιραζόμενο σύστημα αρχείων μπορεί να περιοριστεί με τη χρήση Firewalls.

Πιστοποίηση (Authentication)

Για πολλά χρόνια η μέθοδος της πιστοποίησης των χρηστών εφαρμοζόταν με τη χρήση γνωστών, συχνά χρησιμοποιούμενων συνθηματικών (passwords). Αυτά τα συνθηματικά χρησιμοποιούνταν αρχικά από χρήστες τερματικών που ήθελαν να έχουν πρόσβαση σε κάποιο κεντρικό υπολογιστή. Την εποχή εκείνη δεν υπήρχαν ούτε τοπικά δίκτυα αλλά ούτε και δίκτυα ευρείας περιοχής και έτσι δεν υπήρχε κίνδυνος για την ανακάλυψη ενός συνθηματικού. Σήμερα με την εκτεταμένη χρήση των δικτύων η αποστολή επαναχρησιμοποιούμενων password σε μορφή απλού κειμένου (clear text) δίνει την δυνατότητα σε οποιονδήποτε να τα βρίσκει με σχετικά εύκολο τρόπο. Στοιχεία που προέρχονται από τον οργανισμό CERT δείχνουν ότι μεγάλος αριθμός από clear text password εντοπίζονται εύκολα από sniffers πακέτων.

Οι τελευταίες τεχνολογικές τάσεις στο χώρο της πιστοποίησης είναι η χρήση one-time passwords (S/key), PGP και η πιστοποίηση συσκευών να βασίζεται στην χρήση «κουπονιών» (token). Οι χρήστες χρησιμοποιούν αλφαριθμητικά συνθηματικά σαν κρυφά token και pins. Τα token αυτά συνήθως δεν επιλέγονται προσεκτικά ούτε προστατεύονται. Έτσι μπορεί εύκολα να υπονομευθεί η πιστοποίηση.

Εμπιστευτικότητα (Confidentiality)

Σε κάποιο site τις περισσότερες φορές υπάρχουν πληροφορίες οι οποίες δε θα πρέπει να προσπελαστούν από μη εξουσιοδοτημένους χρήστες. Τα λειτουργικά συστήματα διαθέτουν συνήθως ενσωματωμένους μηχανισμούς για την προστασία των αρχείων. Οι μηχανισμοί αυτοί δίνουν τη δυνατότητα σε ένα διαχειριστή να ελέγχει ποιος θα έχει πρόσβαση στα περιεχόμενα των αρχείων αυτών.

Η εμπιστευτικότητα μπορεί να επιτευχθεί και με την κρυπτογράφηση. Η κρυπτογράφηση επιτυγχάνεται με την παρεμβολή χαρακτήρων στα δεδομένα, έτσι ώστε να είναι δύσκολη και χρονοβόρα η εύρεση της αρχικής πληροφορίας για οποιονδήποτε άλλο έκτος από τους εξουσιοδοτημένους παραλήπτες. Οι εξουσιοδοτημένοι παραλήπτες και οι ιδιοκτήτες της πληροφορίας κατέχουν τα κλειδιά για την αποκρυπτογράφηση της πληροφορίας.

Ακεραιότητα (Integrity)

Ένας διαχειριστής πρέπει να εξασφαλίζει την ακεραιότητα της πληροφορίας που υπάρχει στο σύστημα του. Ένας τρόπος για να επιτευχθεί ο έλεγχος της ακεραιότητας των δεδομένων είναι να παράγουμε το checksum του αναλλοίωτου αρχείου και να το αποθηκεύουμε off-line, και περιοδικά να συγκρίνουμε το checksum που αποθηκεύτηκε off-line με αυτό του αρχείου που χρησιμοποιείται online.

Υπάρχουν λειτουργικά συστήματα τα οποία έχουν ενσωματωμένα checksumming προγράμματα όπως το unix sum. Παρόλα αυτά είναι καλύτερο να χρησιμοποιούνται ισχυρές μέθοδοι και προγράμματα κρυπτογράφησης όπως το message digest-MD5. Υπάρχουν επίσης προγράμματα τα οποία χρησιμοποιούνται για να ελέγχουν την ακεραιότητα των δεδομένων που ανταλλάσσονται μεταξύ διαφόρων εφαρμογών όπως το e-mail, όπου θέλουμε ένα μήνυμα να φτάσει αναλλοίωτο από τον αποστολέα στον παραλήπτη.

Εξουσιοδότηση (Authorization)

Εξουσιοδότηση είναι η διαδικασία κατά την οποία εκχωρούνται στους χρήστες δικαιώματα για την προσπέλαση κάποιου πόρου. Η εξουσιοδότηση διαφέρει από την πιστοποίηση. Κατά την πιστοποίηση ελέγχεται αν ο χρήστης ανήκει ή όχι στο σύστημα. Από τη στιγμή που αναγνωρίζεται ως νόμιμος χρήστης εξουσιοδοτείται για τα δικαιώματα που έχει στο σύστημα.

Μια πολύ δημοφιλής προσέγγιση για εξουσιοδότηση είναι αυτή του συστήματος Unix, όπου υπάρχουν τρεις κατηγορίες χρηστών: owner, group και world.

Owner μπορεί να είναι κάποιος που δημιουργεί κάποιο αντικείμενο ή ο χρήστης που ορίζεται από τον supervisor σαν owner. Τα δικαιώματα του owner είναι τα (read, write, execute) και ανήκουν μόνο σε αυτόν.

Group είναι μια ομάδα χρηστών οι οποίοι μπορούν να χρησιμοποιούν κάποιο αντικείμενο και να έχουν δικαιώματα πρόσβασης σε αυτό. Και εδώ τα δικαιώματα όλων των χρηστών που ανήκουν στο group είναι (read, write, execute).

Στο world ανήκουν όλοι οι υπόλοιποι που έχουν πρόσβαση στο σύστημα. Μια άλλη προσέγγιση είναι η χρήση λίστας ελέγχου προσπέλασης (Access Control List ACL) όπου αναφέρονται όλοι οι χρήστες ή τα group που έχουν πρόσβαση σε κάποιον πόρο. Το πλεονέκτημα της χρήσης ACL είναι ότι μπορεί εύκολα να ελεγχθεί ποιος έχει πρόσβαση σε τι. Το μειονέκτημα είναι ο χώρος που απαιτείται για να αποθηκευτούν οι λίστες.

Προσπέλαση (Access)

Είναι σημαντικό να ελέγχεται η πρόσβαση στους hosts. Η προσπέλαση θα πρέπει να επιτρέπεται μόνο σε εκείνους που πρέπει να χρησιμοποιούν τους hosts. Θα πρέπει επίσης να κρατούνται αντίγραφα ασφαλείας, τα οποία θα βρίσκονται σε προστατευόμενους χώρους. Υψηλό κίνδυνο για κλοπή δεδομένων παρουσιάζουν οι φορητοί υπολογιστές. Θα πρέπει να λαμβάνονται όλα τα μέτρα ώστε σε περίπτωση κλοπής κάποιου φορητού να μην δίνεται χρήσιμη πληροφορία για το σύστημα.

Επίσης, θα πρέπει να ελέγχεται η πρόσβαση στα rack όπου βρίσκονται τα ενεργά στοιχεία του δικτύου καθώς και σε μέρη που υπάρχουν file servers, name servers και hosts.

Κοινόχρησrες Δικτυακές Συνδέσεις (Walk-up Network Connections)

Με τον όρο "walk-up" συνδέσεις εννοούμε τα σημεία σύνδεσης του δικτύου που χρησιμοποιούνται για φορητούς host. Θα πρέπει να λαμβάνουμε υπόψη ότι με την παροχή αυτής της υπηρεσίας μπορεί οποιοσδήποτε μη εξουσιοδοτημένος host να συνδεθεί στο δίκτυο. Με τη υπηρεσία αυτή αυξάνεται ο κίνδυνος για επιθέσεις όπως IP address spoofing, packet sniffing κ.α.

Η πιστοποίηση σε ένα walk-up host θα πρέπει να γίνεται προτού επιτραπεί στο χρήστη η πρόσβαση στους πόρους του δικτύου. Επίσης μπορούν να χρησιμοποιηθούν διαφορετικά υποδίκτυα για εξωτερικούς χρήστες.

Άλλες δικτυακές τεχνολογίες

Ένας συνηθισμένος στόχος των εισβολέων είναι τα πρωτόκολλα που χρησιμοποιούνται για τη φυσική σύνδεση του δικτύου (X.25, ISDN, SMDS, DDS και Frame Relay). Ένας υποψήφιος εισβολέας προσπαθεί να παρέμβει και να αλλοιώσει την πληροφορία όταν αυτή περνά μέσα από το φυσικό μέσο.

Διαχείριση των τηλεφωνικών γραμμών modems

Για την ασφάλεια του δικτύου θα πρέπει να ελέγχονται και οι γραμμές των modems. Παρόλο που τα modems είναι ένας εύκολος τρόπος πρόσβασης σε ένα site μπορούν να προκαλέσουν αρκετά προβλήματα στην ασφάλεια.

Οι γραμμές modem θα πρέπει να εγκαθίστανται μετά από κατάλληλη εξουσιοδότηση. Για τις γραμμές αυτές θα πρέπει να τηρείται αρχείο το οποίο θα ενημερώνεται τακτικά για όλες τις ενέργειες που έχουν προηγηθεί. Για την σωστή διαχείριση και διατήρηση της ασφάλειας πρέπει να τηρούνται τα παρακάτω:

Πιστοποίηση των *Dial-In χρηστών*

Οι dial-in χρήστες θα πρέπει να πιστοποιούνται πριν από την προσπέλαση οποιασδήποτε συσκευής του συστήματος. Σε κάθε περίπτωση μια τηλεφωνική γραμμή μπορεί να μπλοκαριστεί και ο εισβολέας να δει την πληροφορία που περνάει από την γραμμή. Ενδείκνυται η one-time αλλαγή password.

Πολλές φορές οι χρήστες δίνουν λάθος τον

κωδικό τους. Στην περίπτωση αυτή θα πρέπει να δίνεται στο χρήστη δυνατότητα επανάληψης της διαδικασίας μέχρι τρεις φορές. Αν τελικά ο χρήσrης δεν συνδεθεί είναι καλό να μην αναφέρεται σε ποιο σημείο (login ή password) έγινε το λάθος.

Χρήση Callback

Μια άλλη δυνατότητα που μπορεί να δώσει ο διαχειριστής στο dial-in server είναι αυτή του call-back (ο χρήστης καλεί και αφού πιστοποιηθεί η αυθεντικότητα του, το σύσrημα τον αποσυνδέει και καλεί το χρήσrη σε συγκεκριμένο αριθμό. Με το call-back μπορεί να ελεγχθεί κάποιος εισβολέας αφού κατά το call-back υπάρχει το νούμερο του δικαιούχου χρήστη μόνο.

Καταγραφή όλων των login

Θα πρέπει όλο το σύμπλεγμα των dial-in συσκευών και συνδέσεων να καταγράφεται τόσο για τα dial-in όσο και τα dial-out τηλεφωνήματα που γίνονται. Αυτό γίνεται με καταγραφικό σύσrημα σro τηλεφωνικό κέντρο.

Επιλογή του κατάλληλου μηνύματος στην σύνδεση

Θα πρέπει να ελέγχεται η πληροφορία που εμφανίζεται στα banner. Θα πρέπει να είναι σύντομη χωρίς να δίνει στοιχεία σχετικά με τον τύπο του υλικού του host ή το λειτουργικό σύστημα που είναι εγκατεστημένο sro host. Θα μπορούσε να χρησιμοποιηθεί και ένα blind password (π.χ. να μην δίνεται καμία απάντηση σε μια εισερχόμενη κλήση μέχρι ο χρήστης πληκτρολογήσει κάποιο password). Η διαδικασία αυτή εξομοιώνει ένα dead modem.

Πιστοποίηση Dial-0ut

Σημαντικό ζητήματα είναι η πιστοποίηση της αυθεντικότητας των dial-out χρηστών κύρια για λόγους ασφάλειας αλλά και γιατί ο οργανισμός πληρώνει τις κλήσεις.

Ποτέ δεν πρέπει να επιτρέπεται dial-out δυνατότητα από ένα σημείο που δεν ελέγχεται η δυνατότητα για dial-in. Είναι πολύ δύσκολο να ανιχνευτούν οι κινήσεις ενός hacker που περνά από πολλά διαφορετικά σημεία σrον οργανισμό.

Τουλάχιστον δεν πρέπει να επιτρέπεται το ίδιο modem να λειτουργεί με δυνατότητα dial-in και dial-out.

7.5. Καταγραφή και Επαλήθευση (Auditing)

Η ενίσχυση της ασφάλειας σε ένα site επιβάλει τον ορισμό των διαδικασιών συλλογής δεδομένων που παράγονται από τη δικτυακή δραστηριότητα σε ένα site. Η ανάλυση των δεδομένων αυτών μπορεί να αποβεί χρήσιμη στην αντιμετώπιση προβλημάτων που μπορεί να προκύψουν από την παραβίαση της ασφάλειάς του.

Τι συλλέγεται

Τα δεδομένα που συλλέγονται πρέπει να περιλαμβάνουν κάθε προσπάθεια παραβίασης των επιπέδων ασφάλειας από ένα άτομο, διεργασία ή άλλη οντότητα του δικτύου. Αυτό περιλαμβάνει είσοδο στο σύστημα (login) έξοδο από το σύστημα (logout), πρόσβαση με δικαιώματα «super user», δημιουργία εισιτηρίων (π.χ. για το Kerberos) και κάθε άλλη δραστηριότητα κατά τη διαδικασία πρόσβασης ή αλλαγή της κατάστασης. Είναι ιδιαίτερα σημαντικό να καταγράφεται πότε γίνεται "anonymous" ή "guest" πρόσβαση σε δημόσιους εξυπηρετητές.

Γενικότερα, η πληροφορία που πρέπει να συλλεχθεί περιλαμβάνει: username και hostname για login και logout, δικαιώματα προηγούμενης και νέας πρόσβασης για αλλαγή των δικαιωμάτων πρόσβασης, και timestamp. Φυσικά, υπάρχει πολύ περισσότερη πληροφορία που μπορεί να συγκεντρωθεί, και η οποία εξαρτάται από το τι κάνει το σύστημα και πόσος είναι ο προσφερόμενος χώρος για την αποθήκευση της συλλεγόμενης πληροφορίας.

Είναι πολύ σημαντικό να μη συγκεντρώνονται πληροφορίες για τα passwords. Αυτό δημιουργεί ενδεχόμενη καταπάτηση της ασφάλειας αν οι συλλεγόμενες εγγραφές προσπελαύνονται από μη εξουσιοδοτημένους χρήστες.

Διαδικασία λήψης αντιγράφων ασφαλείας

Μια κλασική διαδικασία που εφαρμόζεται σε υπολογιστικά συστήματα είναι αυτή της λήψης αντιγράφων ασφαλείας. Για να είναι σωστός ο σχεδιασμός που γίνεται για την ασφάλεια ενός site, η διαδικασία λήψης αντιγραφών θα πρέπει να αποτελεί αναπόσπαστο κομμάτι του. Κατά την δημιουργία αντιγράφων ασφαλείας θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα:

- Να είναι δυνατή η δημιουργία αντιγράφων ασφαλείας .
- Τα αντίγραφα θα πρέπει να αποθηκεύονται off-site. Ο αποθηκευτικός χώρος θα πρέπει να επιλέγεται προσεκτικά σύμφωνα με τα ακόλουθα κριτήρια: την ασφάλεια και τη διαθεσιμότητα του.
- Προκειμένου να έχουμε επιπρόσθετη ασφάλεια τα αντίγραφα θα πρέπει να κρυπτογραφούνται. Η ανάκτηση της πληροφορίας θα πρέπει να είναι δυνατή από οποιαδήποτε σημείο οποιαδήποτε στιγμή. Επίσης άμεσα διαθέσιμα θα πρέπει να είναι και τα προγράμματα αποκρυπτογράφησης.
- Τα αντίγραφα θα πρέπει να ελέγχονται ανά τακτά χρονικά διαστήματα τόσο για την ορθότητα όσο και για την πληρότητα τους.

7.6. Αντιμετώπιση ενός περιστατικού ασφάλειας

Για να αντιμετωπιστεί σωστά ένα περιστατικό ασφάλειας πρέπει να υπάρχει κάποιο σχέδιο δράσης. Σχέδιο δράσης θα πρέπει να υπάρχει τόσο για την περίπτωση που η παραβίαση είναι αποτέλεσμα μίας εξωτερικής επίθεσης από κάποιον εισβολέα, όσο και όταν οφείλεται σε ακούσια ζημιά, ή κατά τον έλεγχο κάποιου νέου προγράμματος από κάποιον που προσπαθεί να εκμεταλλευτεί τις αδυναμίες ενός λογισμικού, ή όταν προκαλείται από κάποιον δυσαρεστημένο υπάλληλο.

Οι παραδοσιακοί τρόποι που ακολουθούνται για την ασφάλεια ενός συστήματος δεν προβλέπουν τρόπους άμεσης αντίδρασης σε περίπτωση που συμβεί η επίθεση. Αυτό έχει

σαν αποτέλεσμα τη λήψη βιαστικών αποφάσεων όταν η επίθεση είναι σε εξέλιξη. Οι αποφάσεις αυτές μπορεί να είναι ζημιογόνες στον εντοπισμό της πηγής του περιστατικού, στη συλλογή στοιχεί ων για να χρησιμοποιηθούν σε πιθανές διώξεις που θα γίνουν, καθώς και στην προετοιμασία ανάκτησης του συστήματος και προστασίας των πολύτιμων δεδομένων του συστήματος.

Μια καλή προσέγγιση για τον αποτελεσματικό χειρισμό τέτοιων περιστατικών, θα πρέπει να είναι ο οικονομικός παράγοντας. Η ύπαρξη διαχειριστών και τεχνικών που ασχολούνται αποκλειστικά με την αντιμετώπιση των παραβιάσεων του συστήματος είναι οικονομικά ασύμφορη, για τα συνήθη μεγέθη των εταιριών και οργανισμών. Για το λόγο αυτό θα πρέπει το προσωπικό του κέντρου διαχείρισης να είναι εκπαιδευμένο και να χειρίζεται ανάλογες καταστάσεις.

Εξαιτίας του Διαδικτύου οι περισσότερες παραβιάσεις δεν περιορίζονται σε ένα μόνο site. Οι «τρύπες» των λειτουργικών συστημάτων που είναι εγκατεστημένα σε πολλά εκατομμύρια συστήματα, γίνονται αντικείμενο εκμετάλλευσης από το ίδιο το δίκτυο. Για αυτό, είναι κρίσιμο όλα τα εμπλεκόμενα sites να ενημερώνονται όσο πιο γρήγορα γίνεται.

Με την αποτελεσματική αντιμετώπιση των παραβιάσεων είναι δυνατόν να προκύψουν οφέλη που σχετίζονται με νομικά ζητήματα.

Προετοιμασία και σχεδιασμός της αντιμετώπισης περιστατικών ασφάλειας

Ο τρόπος αντίδρασης σε περίπτωση παραβίασης θα πρέπει να έχει προετοιμαστεί εκ των προτέρων. Σε κάθε δίκτυο υπάρχει ένα βασικό επίπεδο προστασίας. Έχοντας ορίσει ένα πρώτο επίπεδο προστασίας στο δίκτυο μπορούν να περιοριστούν ενδεχόμενες καταστροφές. Στο σχεδιασμό της προστασίας θα πρέπει να περιλαμβάνονται γενικές οδηγίες για την αντιμετώπιση παραβιάσεων, που μπορεί να δεχτεί το δίκτυο. Η τήρηση των διαδικασιών οδηγεί στην καλύτερη αντιμετώπιση του προβλήματος. Είναι πάρα πολύ σημαντικό το προτεινόμενο σχέδιο να ελεγχθεί προτού συμβεί μία παραβίαση.

Το να γνωρίζει κανείς πως να ανταποκρίνεται άμεσα και αποτελεσματικά σε μία παραβίαση είναι σημαντικό γιατί επιτυγχάνεται:

1. Η προφύλαξη των στοιχείων μιας εταιρείας τα οποία μπορούν να εκτεθούν
2. Η διαφύλαξη των πόρων που μπορεί να αξιοποιηθούν πιο κερδοσκοπικά
3. Η συμμόρφωση με κυβερνητικούς και άλλους κανονισμούς
4. Η ελαχιστοποίηση ενδεχόμενης αρνητικής έκθεσης

Κατά την σχεδίαση μιας διαδικασίας, πρέπει να καθορίζονται οι στόχοι που θα τεθούν για την αντιμετώπιση μιας παραβίασης. Αυτοί οι στόχοι μπορούν να ταξινομηθούν κατά προτεραιότητα ανάλογα με το site. Τα ζητήματα που σχετίζονται με τους διάφορους τύπους παραβιάσεων είναι τα ακόλουθα:

1. Η κατανόηση του τρόπου με τον οποίο έγινε η παραβίαση
2. Η αποφυγή έκθεσης του συστήματος στον ίδιο κίνδυνο
3. Αποφυγή κλιμάκωσης του προβλήματος και περαιτέρω παραβιάσεων
4. Εκτίμηση της επίδρασης και τη ζημιάς που προκάλεσε η παραβίαση
5. Αποκατάσταση του συστήματος από την παραβίαση
6. Εκσυγχρονισμός ακολουθούμενων πολιτικών και διαδικασιών
7. Εύρεση του υπαιτίου (αν αυτό είναι δυνατόν)

Οι ενέργειες που γίνονται κατά τη διάρκεια μίας παραβίασης πρέπει να εκτελεστούν με μια σειρά προτεραιότητας. Μερικές φορές μία παραβίαση μπορεί να είναι τόσο σύνθετη και πολύπλοκη που να είναι ασύμφορη η αντιμετώπιση της. Η τήρηση σειράς

προτεραιότητας είναι απαραίτητη. Παρόλο που οι προτεραιότητες μπορεί να διαφέρουν από οργανισμό σε οργανισμό, η ακόλουθη προτεινόμενη σειρά μπορεί να αποτελέσει σημείο έναρξης για τον καθορισμό του τρόπου αντίδρασης:

1. Η προστασία της ανθρώπινης ζωής και της ασφάλειας των ανθρώπων. Η ανθρώπινη ζωή έχει πάντα τη μέγιστη προτεραιότητα
2. Η προστασία των ευαίσθητων δεδομένων.
3. Η προστασία άλλων δεδομένων, όπως δεδομένα χρηστών, επιστημονικά, διαχειριστικά, γιατί η απώλεια δεδομένων είναι δαπανηρή όσο αφορά τους πόρους.
4. Η προστασία άλλων συστημάτων, δικτύων ή sites από παρόμοια περιστατικά.
5. Η πρόβλεψη καταστροφής των συστημάτων (π.χ. χάσιμο ή μετατροπή αρχείων του συστήματος, καταστροφή του δίσκου κλπ).
6. Ελαχιστοποίηση της ζημιάς κατά την παραβίαση των υπολογιστικών πόρων. Σε πολλές περιπτώσεις προτιμάται το «κατέβασμα» ή η αποσύνδεση του συστήματος από το δίκτυο προκειμένου να περιοριστεί η ζημιά.

Από τη στιγμή που έχουν προστατευθεί η ανθρώπινη ζωή και η εθνική ασφάλεια το αμέσως σημαντικότερο πράγμα είναι η διαφύλαξη των δεδομένων και όχι του λογισμικού ή του υλικού του συστήματος. Παρόλο που δεν είναι επιθυμητό να έχουμε ζημιά ή απώλεια κατά τη διάρκεια μίας παραβίασης, τα συστήματα μπορούν να αντικατασταθούν. Ωστόσο, η απώλεια ή έκθεση δεδομένων δεν είναι αποδεκτή.

Ένα άλλο σημαντικό πράγμα που πρέπει να ληφθεί υπόψη είναι η επίδραση της παραβίασης σε τρίτους. Μέσα στα όρια που επιβάλλονται από κρατικούς κανονισμούς, είναι σημαντική η άμεση πληροφόρηση των προσβεβλημένων ομάδων.

Κάθε σχέδιο που αντιστοιχεί σε παραβιάσεις ασφάλειας πρέπει να καθοδηγείται από τοπικές πολιτικές και κανονισμούς. Κυβερνητικά και ιδιωτικά sites που έχουν κρίσιμη πληροφορία ακολουθούν συγκεκριμένους κανόνες.

Λίστα ατόμων προς ενημέρωση

Για την επίλυση κάποιου προβλήματος είναι πιθανό να χρειάζεται και η συμμετοχή κάποιων τρίτων. Ως τρίτοι θεωρούνται οι τοπικοί διευθυντές και διαχειριστές, άλλα sites στο Διαδίκτυο καθώς και διάφοροι ερευνητικοί οργανισμοί. Για την πιο αποδοτική αντιμετώπιση της παραβίασης είναι σημαντικό όλοι οι συμμετέχοντες στην επίλυση κάποιου προβλήματος να βρίσκονται σε συνεχή επαφή. Ωστόσο πολλά προβλήματα μπορούν να επιλυθούν εσωτερικά.

Για κάθε είδους επαφή, πρέπει να καθοριστούν συγκεκριμένοι εργαζόμενοι, που θα δρουν ως σημεία επαφής και οι οποίοι θα ασχολούνται με τεχνικά ή διαχειριστικά θέματα περιλαμβανομένων νομικών ή ερευνητικών ομάδων (agencies) καθώς και παρόχων υπηρεσιών ή πωλητών προϊόντων. Στην περίπτωση αυτή πρέπει να καθορίζεται πόση πληροφορία θα γνωστοποιείται στον καθένα. Είναι ιδιαίτερα σημαντικό να καθορίσουμε, τι είδους πληροφορία θα μοιραστεί στους χρήστες ενός site, στο κοινό (συμπεριλαμβανομένου και του τύπου) καθώς και σε άλλα sites.

Υπεύθυνοι και προσωπικό

Κατά τον σχεδιασμό μιας πολιτικής ασφάλειας θα πρέπει να ορίζεται οπωσδήποτε ένας υπεύθυνος συντονισμού. Ένα μεγάλο λάθος που μπορεί να γίνει, είναι να έχουμε ένα μεγάλο αριθμό ανθρώπων όπου ο καθένας εργάζεται ανεξάρτητα. Αυτό μπορεί να οδηγήσει σε σύγχυση και αναποτελεσματικές προσπάθειες.

Ο Υπεύθυνος Ασφάλειας μπορεί να μην είναι το υπεύθυνο άτομο για να αντιμετωπίσει την παραβίαση. Υπάρχουν δύο διακριτοί ρόλοι για τον Υπεύθυνο Ασφάλειας και το άτομο που είναι υπεύθυνο για την παραβίαση. Το υπεύθυνο άτομο θα πάρει τις αποφάσεις σύμφωνα με την ακολουθούμενη πολιτική, σε αντίθεση, ο Υπεύθυνος Ασφάλειας πρέπει να συντονίζει την προσπάθεια όλων των ομάδων που εμπλέκονται στην αντιμετώπιση του προβλήματος.

Ο Υπεύθυνος Ασφάλειας πρέπει να είναι ένα άτομο με άρτια τεχνική κατάρτιση ώστε να συντονίσει επιτυχώς τις προσπάθειες των διαχειριστών των συστημάτων και των χρηστών που αναμιγνύονται στην παρακολούθηση και την αντίδραση στην επίθεση. Αυτό το άτομο πρέπει να επιλεγεί με προσοχή. Δεν χρειάζεται απαραίτητα να είναι το ίδιο άτομο που έχει την ευθύνη για τη διαχείριση του συστήματος καθώς συχνά τα άτομα αυτά έχουν γνώση μόνο για την καθημερινή λειτουργία του συστήματος, και στερούνται τεχνική εξειδίκευση σε βάθος.

Τέλος, οι χρήστες θα πρέπει να ξέρουν πως να περιγράφουν τυχόν παραβιάσεις. Τα sites πρέπει να παρέχουν διαδικασίες αναφοράς που θα δουλεύουν καθ' όλη τη διάρκεια της μέρας. Το Help Desk χρησιμοποιείται συχνά για να παραλαμβάνει αυτές τις αναφορές κατά τη διάρκεια κανονικών ωρών εργασίας, ενώ οι beepers και τα τηλέφωνα μπορούν να χρησιμοποιηθούν εκτός του κανονικού ωραρίου.

Ενημέρωση των αρχών – Νομικές συνέπειες

Όταν συμβεί μία παραβίαση που έχει νομικές συνέπειες, είναι σημαντικό να έρθουμε σε επαφή με τις αρχές το συντομότερο. Πρέπει επίσης να ενημερωθούν οι υπεύθυνοι από την πλευρά της πολιτείας. Ένας σημαντικός λόγος για τον καθορισμό ενός σημείου επαφής είναι το ότι όταν μία επίθεση είναι σε εξέλιξη υπάρχει πολύ λίγος χρόνος για να κληθούν οι αρχές. Κάποια γνωστά νομικά θέματα που θα πρέπει να λαμβάνονται υπόψη είναι:

1. Ο κίνδυνος δυσφήμησης κάποιου οργανισμού
a. Η χρέωση ευθυνών σε περίπτωση που κάποιο τρίτο σύστημα υποστεί ζημία εξαιτιας του συστήματος του οργανισμού
2. Η διάχυση της πληροφορίας

Ομάδες αντιμετώπισης περιστατικών

Αυτή τη στιγμή υπάρχει ένας αριθμός ομάδων αντιμετώπισης παραβιάσεων ασφαλείας υπολογιστών (CSIRTs) όπως το Κέντρο Συντονισμού CERT, το γερμανικό DFN-CERT, και άλλες ομάδες στον κόσμο. Οι ομάδες αυτές υπάρχουν στα πλαίσια σημαντικών κρατικών προσπαθειών και μεγάλων εταιρειών για την αντιμετώπιση των hackers. Αν είναι διαθέσιμη μία τέτοια ομάδα, τότε θα πρέπει να ειδοποιηθεί άμεσα όταν γίνει αντιληπτή κάποια παράβαση. Αυτές οι ομάδες είναι υπεύθυνες να συντονίσουν την αντιμετώπιση των παραβιάσεων ασφαλείας σε Η/Υ, σε μεγάλο αριθμό από sites.

Αν διαπιστωθεί ότι η διακοπή της ασφάλειας συνέβη εξαιτίας ενός ελαττώματος του λογισμικού ή του υλικού του συστήματος, ο πωλητής (ή προμηθευτής) και η ομάδα αντιμετώπισης παραβιάσεων της ασφάλειας ενός υπολογιστή, θα πρέπει να ειδοποιηθούν άμεσα. Η διάδοση κάποιου προβλήματος elναι ιδιαίτερα σημαντική γιατl πολλά άλλα συστήματα που είναι ευάλωτα, μπορούν να βοηθηθούν από τους προμηθευτές ή τις ομάδες απόκρισης.

Επηρεαζόμενα και εμπλεκόμενα sites

Αν μία παραβιαση είναι προφανές ότι δεν θα περιοριστεί μόνο στο τοπικό site αλλά θα έχει συνέπειες και σε άλλα sites, είναι καλή πρακτική να ενημερωθούν από την αρχή. Κάθε site πρέπει να επιλέξει να έρθει σε επαφή με άλλα sites κατευθείαν ή να δώσει πληροφορίες σε μια κατάλληλη ομάδα αντιμετώπισης.

Τα νομικά θέματα και τα θέματα υπευθυνότητας που προκύπτουν από μια παραβίαση ασφαλείας διαφέρουν από χώρα σε χώρα.

Πληροφορία που αφορά συγκεκριμένα άτομα μπορεί να είναι ιδιαίτερα κρίσιμη, και να χρήζει ειδικής μεταχείρισης. Οι ομάδες αντιμετώπισης όταν δίνουν πληροφορίες σε υπεύθυνους ασφάλειας, μπορούν να προστατέψουν την ανωνυμία της αρχικής πηγής. Σε πολλές όμως περιπτώσεις η ανάλυση των logs και της πληροφορίας άλλων sites μπορεί να αποκαλύψει στοιχεία του site.

Όλα τα παραπάνω προβλήματα δεν πρέπει να αποτελέσουν αφορμή για να μην αναμειχθούν άλλα sites. Στην πραγματικότητα, οι εμπειρίες των ήδη υπαρχόντων ομάδων, δείχνουν, ότι πολλά sites που πληροφορούνται για προβλήματα ασφαλείας, δεν είναι καν ενήμερα ότι το site τους έχει εκτεθεί. Χωρίς έγκαιρη πληροφόρηση τα άλλα sites είναι συχνά ανίκανα να αναλάβουν δράση ενάντια στους εισβολείς.

Εσωτερική ενημέρωση

Είναι πολύ σημανηκό όταν διαγνωστεί μια μεγάλη παραβίαση να ενημερώνονται οι χρήστες για ης ενέργειες που έγιναν, καθώς και το πως αναμένεται να αντιδράσουν οι χρήστες ή τα διάφορα τμήματα. Συγκεκριμένα, πρέπει να γίνει ξεκάθαρο στους χρήστες αν θα πρέπει να μιλήσουν ή όχι στον έξω κόσμο (συμπεριλαμβανομένων και των άλλων τμημάτων). Σε περίπτωση προβλήματος οι χρήστες θα πρέπει να είναι ενήμεροι και να δίνουν πληροφορίες μη επιζήμιες για τον οργανισμό. Η επικοινωνία με πελάτες και εταίρους που έχουν κλείσει συμβόλαια πρέπει να αντιμετωπιστεί με έναν λογικό αλλά και ευαίσθητο τρόπο.

Δημόσιες σχέσεις - Ανακοινώσεις

Ένα από τα πιο σημαντικά θέματα που πρέπει να ληφθεί υπόψη είναι πότε, ποιος και πόσο συχνά θα δημοσιοποιεί πληροφορίες στο ευρύ κοινό μέσω του τύπου. Αν δεν υπάρχει γραφείο δημοσίων σχέσεων πρέπει να μελετηθεί προσεχτικά η πληροφορία που θα δημοσιευτεί στον τύπο. Αν η πληροφορία είναι ευαίσθητη, είναι προτιμότερο να παρέχεται στον τύπο η ελάχιστη δυνατή. Στο σημείο αυτό θα πρέπει να γίνει η εξής σημαντική παρατήρηση: η παραπληροφόρηση του τύπου μπορεί να προκαλέσει μεγαλύτερη ζημιά από την δημοσίευση ευαίσθητης πληροφορίας. Γενικά πρέπει να λαμβάνεται υπόψη:

1. Να μην γίνει εκτενής αναφορά σε τεχνικό επίπεδο. Λεπτομερής πληροφορία για την παραβίαση μπορεί να παρέχει σημαντική πληροφορία σε άλλους για να λανσάρουν παρόμοιες επιθέσεις σε άλλα sites.
2. Διάφοροι συλλογισμοί για το ποιος προκάλεσε τη βλάβη ή τα κίνητρα του θα πρέπει να μην φτάσουν στον τύπο. Πολλές φορές οι συλλογισμοί αυτοί μπορεί να δώσουν μία λανθασμένη εικόνα του γεγονότος
3. Η διαφύλαξη των ενοχοποιητικών στοιχείων.
4. Η αποφυγή συνεντεύξεων πριν από μία καλή και μεθοδική προετοιμασία.
5. Η αποφυγή αποπροσανατολισμού του κοινού.

Προσδιορίζοντας ένα περιστατικό

Πολλές φορές τα σημάδια μιας παραβίασης που μοιάζουν να προέρχονται από έναν ιό, μια εισβολή στο σύστημα, κ.λ.π. είναι απλά ανωμαλίες, όπως λάθη στο υλικό ή μη αρμόζουσα συμπεριφορά ενός χρήστη του συστήματος. Για την αναγνώριση μιας πραγματικής επίθεσης απαιτείται η προμήθεια κατάλληλου λογισμικού. Επίσης, πολύ χρήσιμη μπορεί να φανεί κάποιου είδους πληροφορία επαλήθευσης, κυρίως στο να καθορίσουμε αν συμβαίνει πράγματι επίθεση στο δίκτυο. Πολλές παραβιάσεις προκαλούν μία δυναμική αλυσίδα γεγονότων, και ένα αρχικό στιγμιότυπο του συστήματος μπορεί να είναι το πιο χρήσιμο εργαλείο στο να αναγνωριοτεί το πρόβλημα και η οποιαδήποτε πηγή της επίθεσης. Τέλος, είναι πολύ σημαντική η διατήρηση log πληροφορίας. Το να καταγράφονται τα γεγονότα (events) του συστήματος, οι τηλεφωνικές συνδιαλέξεις κ.λ.π., μπορεί να οδηγήσει σε μία άμεση και συστηματική αναγνώριση του προβλήματος και αποτελεί τη βάση για άλλα επιμέρους στάδια σιην αντιμετώπιση της παραβίασης.

Υπάρχουν συγκεκριμένες ενδείξεις ή συμπτώματα όταν συμβαίνει μία παραβίαση, που αξίζουν ειδικότερης προσοχής:

1. Αδικαιολόγητη διακοπή της λειτουργίας του συστήματος (crash).
2. Άνοιγμα νέων λογαριασμών χρηστών ή υψηλή δραστηριότητα σε έναν λογαριασμό με προηγούμενη χαμηλή χρήση.
3. Νέα αρχεία με συνήθως περίεργα ονόματα.
4. Ασυμφωνίες λογαριασμών
5. Αλλαγές στα μεγέθη των αρχείων και των ημερομηνιών.
6. Προσπάθειες να γράψει κάποιος στο σύστημα.
7. Μετατροπές ή σβησίματα αρχείων.
8. Άρνηση των εξυπηρετητών να παρέχουν τις υπηρεσίες που υποστηρίζουν
9. Ανεξήγητα χαμηλή απόδοση του συστήματος
10. Εκτύπωση ακατανόητων χαρακτήρων στην κονσόλα των χρηστών.
11. Ύποπτες συστηματικές έρευνες στα αρχεία
12. Αδυναμία των χρηστών να μπουν στους λογαριασμούς τους λόγω αλλαγών στη διαμόρφωσή τους.

Αντιμετώπιση της επίθεσης

Κατά τη διάρκεια της αντιμετώπισης μίας παραβίασης πρέπει να γίνουν κάποια συγκεκριμένα βήματα. Σε όλες τις ενέργειες που σχετίζονται με την ασφάλεια, το πιο σημαντικό πράγμα που πρέπει να γίνει, είναι όλα τα sites να έχουν από μία πολιτική. Χωρίς καθορισμένες πολιτικές και στόχους, οποιεσδήποτε ενέργειες θα παραμείνουν χωρίς αντίκρισμα.

Ένας από τους πιο καθοριστικούς στόχους είναι να αποκατασταθεί ο έλεγχος των προσβεβλημένων συστημάτων και να περιοριστούν οι συνέπειες και η ζημιά. Στη χειρότερη περίπτωση, ίσως να επιβάλλεται και η διακοπή της λειτουργίας του συστήματος.

Τρόποι ενημέρωσης και ανταλλαγής πληροφοριών

Όταν επιβεβαιωθεί μία παραβίαση, πρέπει να ειδοποιηθεί το κατάλληλο προσωπικό. Η διαδικασία με την οποία επιτυγχάνεται αυτή η ενημέρωση είναι πολύ σημαντικό για τη διατήρηση της κατάστασης υπό έλεγχο, τόσο από τεχνικής όσο και από συναισθηματική άποψη. Οι περιστάσεις πρέπει να περιγραφούν όσο το δυνατό πιο λεπτομερειακά, με σκοπό την άμεση αναγνώριση και κατανόηση του προβλήματος.

Καταρχήν, κάθε ειδοποίηση σε προσωπικό εντός ή εκτός του site πρέπει να είναι σαφής. Μία άλλη σημαντική θεώρηση όταν επικοινωνούμε για μία παραβίαση είναι η απόδοση της πραγματικότητας. Το να γίνονται προσπάθειες απόκρυψης στοιχείων της παραβίασης με το να παρέχονται λάθος ή ελλιπείς πληροφορίες μπορεί όχι μόνο να

εμποδίσει μία επιτυχή ανάλυση της παραβίασης, αλλά μπορεί και να χειροτερέψει την κατάσταση. Είναι πολύ σημαντική η διατήρηση της ψυχραιμίας τόσο στις γραπτές όσο και στις προφορικές επικοινωνίες.

Προφύλαξη των στοιχείων/αρχείων καταγραφής της επίθεσης

Όταν αντιμετωπιστεί αποτελεσματικά μία παραβίαση, θα πρέπει να τηρείται ένα λεπτομερές αρχείο με οποιαδήποτε πληροφορία σχετίζεται με την παραβίαση. Αυτό μπορεί να παρέχει μια πολύ σημαντική βοήθεια ώστε να διαλευκανθεί μια σειρά γεγονότων σε σύντομο σχετικά χρόνο. Αν για παράδειγμα δεν γίνει καταγραφή όλων των τηλεφωνημάτων, είναι πολύ πιθανόν να παραβλεφθεί ένα σημαντικό κομμάτι πληροφορίας. Την ίδια στιγμή, η καταγραφή των παραβιάσεων μπορεί να παρέχει τεκμήρια σε περίπτωση δικαστικής διένεξης. Η καταγραφή μίας παραβίασης μπορεί να βοηθήσει στην εκτίμηση της ζημιάς.

Κατά τη διάρκεια των αρχικών σταδίων μίας παραβίασης, συχνά δεν είναι πρακτικό να καθοριστεί αν θα γίνει μήνυση, έτσι θα πρέπει να καταγρά φονται και να συγκεντρώνονται οποιαδήποτε στοιχεία μπορούν μελλοντικά να φανούν χρήσιμα. Θα πρέπει να γίνει καταγραφή για:

- όλα τα events του συστήματος
- όλες τις ενέργειες που έγιναν
- όλες τις εξωτερικές συνομιλίες (περιλαμβάνοντας το άτομο με το οποίο έγινε η συνομιλία, την ημερομηνία, την ώρα και το περιεχόμενο της συνομιλίας)

Ο καλύτερος τρόπος για την καταγραφή των στοιχείων είναι η τήρηση ενός ημερολογίου. Αυτό επιτρέπει την καλή αρχειοθέτηση της πληροφορίας μας. Πολλή από αυτή την πληροφορία μπορεί να χρησιμοποιηθεί σε ένα δικαστήριο.

Αν είναι εφικτό θα πρέπει να ακολουθηθούν τα παρακάτω βήματα:

- τακτικά (π.χ. κάθε μέρα) να παραδίδουμε επικυρωμένα αντίγραφα του ημερολογίου σε ένα άτομο που θα έχει οριστεί σαν επιβλέπων.
- ο επιβλέπων θα πρέπει να αποθηκεύει αυτές τις φωτοτυπημένες σελίδες σε ένα ασφαλές μέρος (π.χ. ένα χρηματοκιβώτιο).
- κατά την παράδοση της πληροφορίας για φύλαξη, θα πρέπει να επιστρέφεται μία υπογεγραμμένη απόδειξη από τον επιστάτη όπου θα αναφέρεται η παραλαβή και η ημερομηνία παραλαβής.

Πιθανό λάθος κατά την τήρηση αυτών των διαδικασιών μπορεί να καταλήξει σε ακύρωση κάθε στοιχείου που θα παραδοθεί σε ένα δικαστήριο.

Λήψη μέτρων περιορισμού ζημιών

Ο σκοπός της λήψης μέτρων είναι ο περιορισμός της έκτασης μίας επίθεσης. Ένα σημαντικό μέρος του αφορά τη λήψη αποφάσεων (π.χ. καθορισμός για το αν θα γίνει τερματισμός του συστήματος, ή αποσύνδεση από το δίκτυο, αν θα παρακολουθείται η δραστηριότητα του συστήματος ή του δικτύου, αν θα απενεργοποιηθούν λειτουργίες του, όπως μεταφορά απομακρυσμένου αρχείου, κ.λ.π.)

Ορισμένες φορές αυτή η απόφαση είναι εύκολο να ληφθεί. Αν η πληροφορία είναι ομαδοποιημένη, ευπαθής ή ιδιόκτητη θα πρέπει να γίνεται τερματι σμός του συστήματος. Πρέπει να λαμβάνεται υπόψη ότι η άρνηση πρόσβασης σε όλους τους χρήστες όταν μία παραβίαση βρίσκεται σε εξέλιξη ειδοποιεί όλους τους χρήστες, συμπεριλαμβανομένων και των χρηστών που έχουν το υπτιθέμενο πρόβλημα, ότι οι διαχειριστές είναι ενήμεροι

του προβλήματος. Αυτό μπορεί να έχει επιβλαβείς επιδράσεις στην έρευνα. Σε ορισμένες περιπτώσεις, είναι συνετή η αφαίρεση όλων των προσβάσεων, και κατόπιν η αποκατάσταση της κανονικής λειτουργίας σε περιορισμένα στάδια. Σε άλλες περιπτώσεις, αξίζει να προκληθεί κάποια ζημιά στο σύστημα αν αυτό έχει σαν αποτέλεσμα την εύρεση του εισβολέα.

Αυτό το στάδιο περιλαμβάνει την εκτέλεση προκαθορισμένων διαδικασιών. Ο οργανισμός ή το site θα πρέπει εκ των προτέρων να έχει ορίσει τα αποδεκτά ρίσκα για την περίπτωση που πραγματοποιηθεί μία παραβίαση και θα υπαγορεύει συγκεκριμένες ενέργειες. Αυτό είναι πολύ σημαντικό όταν χρειάζεται μία γρήγορη απόφαση και δεν είναι δυνατή η επαφή με όλα τα εμπλεκόμενα άτομα προκειμένου να ληφθεί η απόφαση αυτή. Κατά την απουσία προκαθορισμένων διαδικασιών, το άτομο που είναι υπεύθυνο για την παραβίαση, συχνά δεν έχει τη δύναμη να πάρει δύσκολες διαχειριστικές αποφάσεις. Μία τελευταία ενέργεια που θα συμβεί κατά τη διάρκεια του σταδίου αντιμετώπισης της παραβίασης, είναι να ειδοποιηθούν οι αμόδιες αρχές.

Απαλλαγή

Η κατάλληλη στιγμή για την απαλλαγή από τα κατάλοιπα μιας παραβίασης είναι όταν αυτή προσδιοριστεί με ακρίβεια. Πριν από την εξάλειψη μιας αιτίας, πρέπει να δοθεί μεγάλη προσοχή στη συγκέντρωση όλης της απαραίτητης πληροφορίας για το εκτεθειμένο σύστημα καθώς και την αιτία της παραβίασης, η οποία είναι πολύ πιθανόν να χαθεί κατά ων καθαρισμό του συστήματος.

Υπάρχει διαθέσιμο λογισμικό για να μας βοηθήσει στη διεργασία εξυγίανσης του συστήματος, όπως προγράμματα anti-virus. Αν έχουν δημιουργηθεί «πλαστά» (bogus) αρχεία, προτού σβηστούν θα πρέπει να αρχειοθετηθούν. Στην περίπτωση προσβολής από ιό, είναι πολύ σημαντικός ο καθαρισμός και η αναδιάταξη όλων των μέσων που περιέχουν προσβεβλημένα αρχεία. Τέλος, θα πρέπει να βεβαιώνεται η καλή κατάσταση των αντιγράφων ασφαλείας. Πολλά συστήματα που έχουν προσβληθεί από ιούς, περιοδικά προσβάλλονται ξανά επειδή απλά οι άνθρωποι δεν απομακρύνουν συστηματικά τους ιούς από τα backups. Μετά από την απομάκρυνση πρέπει να ληφθεί ένα νέο backup.

Η εξάλειψη όλων των ευάλωτων σημείων μετά από μια παραβίαση είναι σχεδόν αδύνατη.

Ίσως είναι απαραίτητη η επιστροφή στο αρχικό σύστημα διανομής και η επαναφορά του συστήματος από την αρχή. Για να γίνει αυτό θα πρέπει να διατηρούνται μια εγγραφή αρχικοποίησης του γνήσιου συστήματος και κάθε αλλαγή που μεσολάβησε.

Ανάκαμψη λειτουργιών και υπηρεσιών

Όταν έχει εξυγιανθεί η αιτία μίας παραβίασης, το επόμενο στάδιο είναι η φάση της ανάκαμψης των συστημάτων. Ο στόχος της ανάκαμψης είναι η επιστροφή του συστήματος στην αρχική του κατάσταση. Αυτό θα πρέπει να γίνει ενοχλώντας τους χρήστες το λιγότερο δυνατό.

Συνεχής ενημέρωση (follow-up)

Από τη στιγμή που το σύστημα έχει επιστρέψει σε μία σταθερή κατάσταση, είναι πολύ πιθανόν να υπάρχουν «τρύπες» που να απειλούν το σύστημα. Στο σημείο αυτό θα πρέπει να γίνει έλεγχος του συστήματος για πιθανή απώλεια δεδομένων κατά το στάδιο του καθαρισμού του συστήματος.

Το πιο σημαντικό στοιχείο του follow-up είναι να γίνει μία ανάλυση που θα ακολουθεί τα γεγονότα. Τι έγινε ακριβώς και ποιες στιγμές; Πόσο καλά αντέδρασαν τα στελέχη στην παραβίαση; Τι είδους πληροφορία χρειάζεται αμέσως το προσωπικό και πως θα μπορούσαν να την πάρουν όσο πιο γρήγορα γίνεται; Τι θα πρέπει να γίνει με

διαφορετικό τρόπο την επόμενη φορά; Μετά την παραβίαση, είναι σκόπιμη η συγγραφή μιας αναφοράς στην οποία θα περιγράφεται η ακριβής ακολουθία των γεγονότων: η μέθοδος ανακάλυψης, η διαδικασία διόρθωσης, η διαδικασία παρακολούθησης και τέλος μία γενική περίληψη. Αυτό θα βοηθήσει στην απόλυτη κατανόηση του προβλήματος.

Είναι επίσης σημαντικό, το συντομότερο δυνατό να αποκτήσουμε μία οικονομική εκτίμηση της ζημιάς που προκάλεσε η παραβίαση. Αυτή η εκτίμηση θα περιλαμβάνει έξοδα που σχετίζονται με κάθε απώλεια σε λογισμικό και αρχεία δεδομένων, τη ζημιά του υλικού, καθώς και έξοδα σε ανθρώπινο δυναμικό που χρησιμοποιήθηκε για την επαναφορά των αρχείων που είχαν αλλοιωθεί. Μια τέτοια εκτίμηση μπορεί να αποτελέσει τη βάση για περαιτέρω ενέργειες δίωξης-μήνυσης.

Ενέργειες μετά την επίθεση

Ακριβώς μετά την παραβίαση διάφορες ενέργειες πρέπει να λάβουν χώρα:

- Πρέπει να κρατηθεί ένας κατάλογος απογραφής των πόρων του συστήματος (π.χ. μία προσεκτική εξέταση θα καθορίσει πως προσβλήθηκε το σύστημα) .
- Τα αποτέλεσμα ενός περιστατικού πρέπει να θεωρηθούν πηγή μάθησης και να συμπεριληφθούν στο αναθεωρημένο σχέδιο ασφαλείας για να αποτραπεί η επανεμφάνιση του φαινομένου.
- Μία νέα ανάλυση ρίσκου πρέπει να αναπτυχθεί.

Όταν ένα site έχει συνέλθει από μία παραβίαση, η πολιτική και οι διαδικασίες πρέπει να αναθεωρηθούν και να περικλείσουν αλλαγές έτσι ώστε να αποφευχθούν παρόμοια περιστατικά. Οι αναθεωρήσεις επιβάλλονται εξαιτίας των σημερινών υπολογιστικών περιβαλλόντων που συνεχώς αλλάζουν. Ο απότερος σκοπός της διαδικασίας που ακολουθεί το γεγονός της παραβίασης είναι η βελτίωση των μέτρων ασφαλείας, έτσι ώστε να προστατευθεί το site από μελλοντικές επιθέσεις. Όσο και να ακούγεται οξύμωρο, ένας οργανισμός ή ένα site έχει, ως αποτέλεσμα μίας παραβίασης, το κέρδος της πρακτικής γνώσης.

7.7. Τα λάθη της διοίκησης που οδηγούν σε προβλήματα ασφάλειας

Τα προβλήματα ασφάλειας δεν ευθύνονται, αποκλειστικά στη διαχείριση και τη διαμόρφωση των συστημάτων. Πολλά προβλήματα προέρχονται κύρια από οργανωτικά και διοικητικά θέματα που μία διοίκηση πρέπει να φροντίζει να επιλύσει. Παρακάτω αναφέρονται τα κύρια λάθη της διοίκησης ενός οργανισμού που οδηγούν σε προβλήματα ασφάλειας:

1. Ανάθεση της διαχείρισης της ασφάλειας σε ανεκπαίδευτους τεχνικούς, χωρίς να τους παρέχεται ο χρόνος και η εκπαίδευση για να μπορέσουν να φέρουν σε πέρας την εργασία.
2. Αδυναμία κατανόησης της σχέσης της ασφάλειας πληροφοριών και των προβλημάτων που προκύπτουν στην επιχείρηση.
3. Αποτυχία στο να αντιμετωπιστούν τα λειτουργικά θέματα της ασφάλειας. Οι περιστασιακές διορθώσεις αφήνονται στην τύχη τους και μετά από κάποιο χρονικό διάστημα είναι ξεπερασμένες.
4. Εμπιστοσύνη του σχήματος ασφάλειας μόνο σε ένα firewall
5. Αδυναμία αξιολόγησης του κόστους που έχει η φήμη του οργανισμού από επίθεση στο πληροφοριακό σύστημα.
6. Εφαρμογή διορθωτικών μέτρων περιορισμένης έκτασης μετά από κάθε επίθεση

7. Εφαρμογή της τακτικής «όσο δεν ενισχύω την ασφάλεια δεν προκαλώ τις επιθέσεις».

7.8. Η ασφάλεια για τους χρήστες

Οι χρήστες πρέπει να γνωρίζουν μερικά βασικά θέματα που θα βελτιώσουν την ασφάλεια του site. Ο ενημερωμένος χρήστης:

1. Γνωρίζει ποιος είναι υπεύθυνος για την ασφάλεια στο site του
2. Κρατά κρυφό το συνθηματικό του
3. Χρησιμοποιεί την προστασία οθόνης με συνθηματικό
4. Δεν επιτρέπει σε οποιονδήποτε να χρησιμοποιεί τον σταθμό εργασίας του ή το δίκτυο
5. Γνωρίζει τι λογισμικό εκτελεί στο σταθμό εργασίας του και την προέλευσή του
6. Δεν πανικοβάλλεται, αλλα ενημερώνει τον υπεύθυνο ασφάλειας
7. Προσέχει τι «κατεβάζει» από το διαδίκτυο και πάντα χρησιμοποιεί το πρόγραμμα προστασίας από ιούς
8. Δεν ανοίγει εκτελέσιμα attachments σε ηλεκτρονικά μηνύματα αν δεν έρθει πρώτα σε επαφή με τον αποστολέα
9. Δεν ανοίγει μόνος του μία κερκόπορτα στήνοντας dial in επικοινωνία χωρίς να ενημερώσει τον υπεύθυνο ασφάλειας
10. Δεν αφήνει το σταθμό εργασίας του ανοικτό χωρίς προστασία με συνθηματικό

ΚΕΦΑΛΑΙΟ 8

Ιοί, Δούρειοι Ίπποι και Worms

8.1. Τι Είναι Ένας Ιός;

Για πολλά χρόνια κανείς δεν μπορούσε να δώσει με ακρίβεια έναν ορισμό για τους ιούς

υπολογιστών, και υπήρξαν σημαντικές διαμάχες μεταξύ των ειδικών. Η δυσκολία εντοπίζονταν κυρίως στην περιγραφή εκείνων των συγκεκριμένων ιδιοτήτων που χαρακτηρίζουν έναν πραγματικό ιό και τον διαχωρίζουν από τους άλλους τύπους προγραμμάτων. Πολλοί συνηθίζουν να χαρακτηρίζουν τους ιούς, τα worms ("σκουλήκια"), τους Δούρειους Ίππους (Trojan Horses), κ.λ.π., με τον γενικευμένο όρο "ιός". Σήμερα ένας γενικά αποδεκτός ορισμός για τους ιούς υπολογιστών είναι ο εξής: Ένας ιός υπολογιστών είναι ένα πρόγραμμα το οποίο μπορεί να διαιρεθεί σε τρία λειτουργικά μέρη:

- Αναπαραγωγή (Replication)
- Απόκρυψη (Concealment)
- Βόμβα (Bomb)

Ο συνδυασμός αυτών των τριών ιδιοτήτων χαρακτηρίζει ένα πρόγραμμα σαν ιό.

Αναραγωγή

Ένας ιός πρέπει να διαθέτει κάποια μέθοδο αναπαραγωγής - έναν τρόπο για να αναπαράγει τον εαυτό του. Όταν ένας ιός αναπαράγει τον εαυτό του σ' ένα αρχείο, το αποτέλεσμα αναφέρεται με τον όρο "μόλυνση" (infection). Η αναπαραγωγή διασφαλίζει την εξάπλωση του ιού και συμβαίνει όταν ο ιός φορτώνεται στην μνήμη και έχει πρόσβαση στην CPU. Ένας ιός δεν μπορεί να εξαπλωθεί υπάρχοντας απλώς και μόνο σε έναν σκληρό δίσκο. Για να μπορέσει να ενεργοποιηθεί ένας ιός, θα πρέπει να εκτελεστεί ένα αρχείο μολυσμένο μ' αυτόν. Ο όρος "εκτέλεση" εδώ είναι γενικευμένος, Για παράδειγμα, ο χρήστης μπορεί να τρέξει ένα μολυσμένο εκτελέσιμο αρχείο από την γραμμή εντολών ή να ανοίξει ένα μολυσμένο έγγραφο στο Microsoft Word ή σε ένα άλλο πρόγραμμα το οποίο υποστηρίζει μακροεντολές ενσωματωμένες σε έγγραφα.

Μόλυνση αρχείων

Η μέθοδος αναπαραγωγής μπορεί να είναι αποτέλεσμα της μόλυνσης ενός αρχείου, ή της μόλυνσης του τομέα εκκίνησης (boot sector) ενός δίσκου. Η μόλυνση αρχείων βασίζεται στην δυνατότητα του ιού να προσαρτά τον εαυτό του σε ένα αρχείο. Θεωρητικά, οποιοσδήποτε τύπος αρχείου είναι ευάλωτος σ' αυτή την μορφή μόλυνσης. Ωστόσο, οι εισβολείς συνηθίζουν να επικεντρώνουν την προσοχή τους σε αρχεία τα οποία παρέχουν κάποια μορφή πρόσβασης στις λειτουργίες της CPU. Η πρόσβαση αυτή μπορεί να παρέχεται με την άμεση εκτέλεση ενός προγράμματος, ή με την εκτέλεση μιας δευτερεύουσας διεργασίας η οποία ενεργοποιεί τον κώδικα του ιού.

Για παράδειγμα, ένα έγγραφο του Word δεν εκτελεί άμεσα καμία εντολή στην μνήμη. Ωστόσο, το Word μπορεί να διαβάζει τις εντολές που περιέχει μία μακροεντολή ενσωματωμένη σ' ένα έγγραφο και να τις εκτελεί στην μνήμη. Συνεπώς, αν και στην πραγματικότητα είναι μολυσμένο το έγγραφο, η εφαρμογή (το Word) είναι αυτή που παρέχει το όχημα για την αναπαραγωγή του ιού. Για να ενεργοποιήσετε έναν βασιζόμενο σε μακροεντολή ιό, το μόνο που χρειάζεται να κάνετε είναι να ανοίξετε ένα μολυσμένο έγγραφο στο Word ή σε οποιαδήποτε άλλη εφαρμογή υποστηρίζει μακροεντολές.

Ένας παρόμοιος τύπος ιού ο οποίος υπήρξε δημοφιλής πολλά χρόνια πριν, εκμεταλλεύονταν τα τρωτά σημεία του προγράμματος οδήγησης ANSI.SYS του DOS. Οποιοδήποτε αρχείο κειμένου μπορεί να περιέχει ενσωματωμένες εντολές ANSI. Εάν ένας χρήστης φορτώσει το πρόγραμμα οδήγησης ANSI.SYS, οι εντολές αυτές μπορούν να διαβαστούν από το αρχείο κειμένου, να διερμηνευτούν και να εκτελεστούν, ακόμη κι αν η μοναδική ενέργεια που κάνει ο χρήστης είναι η ανάγνωση των περιεχομένων του αρχείου. Ορισμένοι ιοί μπορούν επίσης να ενσωματώνονται σε αρχεία πηγαίου κώδικα. Όταν τελικά μεταγλωττίζεται ο πηγαίος κώδικας σε εκτελέσιμη μορφή, ο ιός αποκτά πρόσβαση στην CPU και μπορεί να αναπαραχθεί.

Ωστόσο, οι γνωστότεροι τύποι ιών είναι αυτοί που μολύνουν τα εκτελέσιμα αρχεία (αρχεία με επεκτάσεις COM, EXE, PIF, ή BAT). Ένας ιός προσθέτει ένα μικρό κομμάτι κώδικα στην αρχή του εκτελέσιμου αρχείου· όταν το αρχείο αυτό εκτελείται, ο ιός φορτώνεται στην μνήμη πριν από την πραγματική εφαρμογή. Κατόπιν ο ιός τοποθετεί τον υπόλοιπο κώδικα του στο μέσον ή στο τέλος του αρχείου.

Αφού μολυνθεί ένα αρχείο, η μέθοδος αναπαραγωγής του ιού μπορεί να βασίζεται στην μνήμη ή όχι. Στην πρώτη περίπτωση, αφού φορτωθεί ο ιός στην μνήμη, περιμένει να εκτελεστούν άλλα προγράμματα και τότε τα μολύνει. Ιοί όπως ο Cabanas έχουν αποδείξει ότι αυτό είναι εφικτό ακόμη και σε συστήματα που χρησιμοποιούν προστατευόμενες περιοχές μνήμης, όπως τα Windows NT. Στην δεύτερη περίπτωση, ο ιός επιλέγει ένα ή περισσότερα εκτελέσιμα αρχεία στον δίσκο και τα μολύνει άμεσα, χωρίς να περιμένει μέχρι να φορτωθούν στην μνήμη. Αυτή η μόλυνση λαμβάνει χώρα κάθε φορά που εκκινεί το μολυσμένο εκτελέσιμο αρχείο.

Σε ορισμένες περιπτώσεις ένας ιός μπορεί να εκμεταλλευτεί την σειρά αναζήτησης αρχείων που έχει καθοριστεί στο λειτουργικό σύστημα για να διευκολύνει την φόρτωση του κώδικα του χωρίς να μολύνει πραγματικά το υπάρχον αρχείο. Αυτός ο τύπος ιών αναφέρεται με τον όρο "ιοί συνοδείας" (companion virus). Ένας ιός συνοδείας λειτουργεί διασφαλίζοντας ότι το εκτελέσιμο αρχείο του εκκινεί πριν από την εκκίνηση του έγκυρου εκτελέσιμου αρχείου.

Όταν εισάγετε μία εντολή για να τρέξετε ένα πρόγραμμα, τα windows αναζητούν κατ' αρχήν ένα αρχείο με επέκταση COM, κατόπιν ένα αρχείο με επέκταση EXE και τέλος ένα αρχείο με επέκταση BAT (υποθέτοντας ότι τα αρχεία βρίσκονται στην ίδια θέση του συστήματος αρχείων αλλιώς, το λειτουργικό σύστημα βασίζεται στην διαδρομή καταλόγων για τον εντοπισμό τους). Αφού βρεθεί ένα αρχείο, το λειτουργικό σύστημα τερματίζει την αναζήτηση του και εκτελεί το πρόγραμμα. Στο παράδειγμα μας, το λειτουργικό σύστημα θα έβρισκε και θα εκτελούσε το αρχείο του ιού (με επέκταση COM) πριν από το πραγματικό εκτελέσιμο του προγράμματος (με επέκταση EXE).

Αναπαραγωγή μέσω του τομέα εκκίνησης

Οι ιοί που αναπαράγονται μέσω του τομέα εκκίνησης (boot sector) μολύνουν την περιοχή συστήματος του δίσκου, η οποία διαβάζεται κατά την εκκίνηση του υπολογιστή ή την πρώτη φορά που προσπελάζεται ο δίσκος. Αυτή η περιοχή μπορεί να περιλαμβάνει την κύρια εγγραφή εκκίνησης (master boot record), τον τομέα εκκίνησης του λειτουργικού συστήματος, ή και τα δύο.

Ένας ιός που μολύνει αυτές τις περιοχές παίρνει συνήθως τις οδηγίες συστήματος που βρίσκει εκεί και τις μετακινεί σε κάποια άλλη περιοχή του δίσκου. Έτσι ο ιός είναι ελεύθερος να τοποθετήσει τον δικό του κώδικα στην εγγραφή εκκίνησης. Όταν εκκινεί το σύστημα, ο ιός φορτώνεται στην μνήμη και δείχνει απλώς στην νέα θέση στην οποία έχει μεταφέρει τις οδηγίες συστήματος. Έτσι το σύστημα εκκινεί κανονικά - εκτός από το γεγονός ότι ο ιός είναι πλέον εγκατεστημένος στην μνήμη.

Για την αναπαραγωγή τους, οι ιοί που μολύνουν τον τομέα εκκίνησης βασίζονται στην επαφή μεταξύ των μονάδων δίσκων. Οι δύο μονάδες δίσκων πρέπει να είναι συνδεδεμένες στον ίδιο υπολογιστή. Για παράδειγμα, εάν προσπελάσετε έναν κοινόχρηστο κατάλογο σ' έναν υπολογιστή μολυσμένο με έναν ιό του τομέα εκκίνησης, ο ιός δεν μπορεί να αναπαράγει τον εαυτό του στον τοπικό σας υπολογιστή επειδή οι δύο υπολογιστές δεν μοιράζονται περιοχές της μνήμης ή κύκλους της CPU.

Ωστόσο, μία κατηγορία προγραμμάτων τα οποία χαρακτηρίζονται με τον όρο droppers (σταγονόμετρα) μπορούν να υποβοηθήσουν την διανομή ιών του τομέα εκκίνησης ακόμη και σ' ένα δίκτυο. Ουσιαστικά, ένα τέτοιο πρόγραμμα λειτουργεί σαν ρουτίνα εγκατάστασης του ιού. Αυτά τα προγράμματα γράφονται συνήθως με τρόπο ώστε να κρύβουν τον ιό που περιέχουν και να διαφεύγουν τον εντοπισμό τους από τα προγράμματα ανίχνευσης/εξάλειψης ιών (antivirus).Επίσης, έχουν συνήθως την μορφή ενός χρήσιμου βοηθήματος για να δελεάσουν τον χρήστη να τα τρέξει. Όταν εκτελείται ένα τέτοιο πρόγραμμα, εγκαθιστά τον ιό στο τοπικό σύστημα.

Κοινά χαρακτηριστικά των ιών που μολύνουν αρχεία και τον τομέα εκκίνησης

Ένα κοινό χαρακτηριστικό των ιών που μολύνουν αρχεία και τον τομέα εκκίνησης δίσκων είναι το γεγονός ότι ο ιός πρέπει να έχει κάποια μέθοδο για να ανιχνεύει τον εαυτό του, έτσι ώστε να αποφεύγει την αυτο-καταστροφή του (μολύνοντας τον εαυτό του). Εάν ο ιός μολύνει τον εαυτό του καθίσταται άχρηστος, ή ο χρήστης μπορεί να υποψιαστεί ότι κάτι πάει στραβά. Και στις δύο περιπτώσεις παύει να υπάρχει δυνατότητα αναπαραγωγής

του ιού. Εάν η αναπαραγωγή του ιού δεν μπορεί να συνεχιστεί, ο ιός είναι καταδικασμένος να πεθάνει όπως και οποιοσδήποτε ζωντανός οργανισμός.

Μια ενδιαφέρουσα προσέγγιση

Μία από τις μεθόδους που χρησιμοποιούν οι δημιουργοί ιών για να διασφαλίσουν ότι ο ιός δεν πρόκειται να μολύνει τον εαυτό του (προκαλώντας την αυτοκαταστροφή του) μπορεί επίσης να χρησιμοποιηθεί για την ανίχνευση του ιού και την παρεμπόδιση του. Πολλοί δημιουργοί ιών χρησιμοποιούν ένα κωδικοποιημένο αλφαριθμητικό το οποίο γνωρίζουν ότι είναι μοναδικό στον δικό τους συγκεκριμένο ιό. Έτσι προγραμματίζουν τον ιό τους ώστε να αναζητά αυτό το αλφαριθμητικό πριν μολύνει ένα αρχείο. Εάν ο ιός βρει αυτό το αλφαριθμητικό σ' ένα αρχείο, δεν το μολύνει.

Τα προγράμματα ανίχνευσης/εξάλειψης ιών μπορούν επίσης να προγραμματιστούν ώστε να αναζητούν αυτό το συγκεκριμένο αλφαριθμητικό - την υπογραφή του ιού. Αυτά τα αλφαριθμητικά δίνουν στο λογισμικό ανίχνευσης/εξάλειψης ιών την δυνατότητα να εντοπίζει γρήγορα και εύκολα την ύπαρξη ιών. Επίσης, η προσθήκη ενός τέτοιου αλφαριθμητικού σ' ένα αρχείο, χωρίς όμως τον πραγματικό κώδικα του ιού, σας δίνει την δυνατότητα να θωρακίσετε αυτό το αρχείο έναντι πιθανής μόλυνσης από τον συγκεκριμένο ιό.

Απόκρυψη

Για να διευκολύνει την αναπαραγωγή του, ένας ιός πρέπει να διαθέτει μία ή περισσότερες μεθόδους για να κρατά κρυφή την ύπαρξη του. Εάν ένας ιός εμφάνιζε ένα εικονίδιο για τον εαυτό του στην γραμμή εργασιών των Windows, κάθε χρήστης θα αντιλαμβάνονταν αμέσως ότι υπάρχει κάποιο πρόβλημα. Οι ιοί χρησιμοποιούν διάφορες μεθόδους για να καμουφλάρουν την παρουσία τους.

Μικρό αποτύπωμα

Συνήθως, ο κώδικας των ιών έχει πολύ μικρό μέγεθος. Ενδεικτικά, το μέγεθος ακόμη και ενός μεγάλου ιού μπορεί να μην υπερβαίνει τα 2KB. Ένα τόσο μικρό "αποτύπωμα" διευκολύνει έναν ιό να κρατά κρυφή την παρουσία του αφού εγκα-τασταθεί σ' ένα αποθηκευτικό μέσο του τοπικού συστήματος, καθώς και κατά την διάρκεια που τρέχει στην μνήμη. Για να διασφαλίσουν ότι οι ιοί τους θα έχουν όσο το δυνατόν μικρότερο μέγεθος, οι περισσότεροι δημιουργοί ιών γράφουν τον κώδικα τους σε γλώσσα assembly.

Εάν ένας ιός έχει αρκετά μικρό μέγεθος μπορεί να προσαρτήσει τον εαυτό του σ' ένα αρχείο χωρίς να επηρεάσει το συνολικό μέγεθος του αρχείου σε τέτοιο βαθμό, ώστε το γεγονός αυτό να γίνει αντιληπτό από τους χρήστες. Μία κατηγορία ιών οι οποίοι χαρακτηρίζονται σαν cavity viruses (ιοί που τοποθετούνται μέσα σε κοιλότητες) αναζητούν επαναλαμβανόμενες ακολουθίες χαρακτήρων μέσα σε ένα αρχείο και τοποθετούνται σ' αυτές τις περιοχές. Έτσι ο ιός μπορεί να αποθηκεύσει το μεγαλύτερο μέρος του κώδικα του σ' ένα αρχείο χωρίς να επηρεάσει το μέγεθος του αρχείου.

Τροποποίηση των ιδιοτήτων των αρχείων

Για να προστατέψουν τα αρχεία από πιθανή μόλυνση από ιούς, οι πρώτοι χρήστες υπολογιστών με το λειτουργικό σύστημα DOS ενεργοποιούσαν την ιδιότητα "μόνο ανάγνωσης" (read only) για τα εκτελέσιμα αρχεία τους. Το σκεπτικό στο οποίοβασίζονταν ήταν ότι εάν ένα αρχείο δεν είχε δυνατότητα τροποποίησης, ο ιός δεν θα μπορούσε να το μολύνει. Φυσικά, οι δημιουργοί ιών απάντησαν σ' αυτό το μέτρο προφύλαξης προσθέτοντας στους ιούς τους κώδικα ο οποίος τους επέτρεπε να ελέγχουν τις ιδιότητες των αρχείων πριν τα μολύνουν. Εάν ένα αρχείο ήταν ορισμένο σαν "μόνο ανάγνωσης", ο ιός απενεργοποιούσε την ιδιότητα αυτή, μόλυνε το αρχείο και κατόπιν επανέφερε τις

ιδιότητες του στην αρχική τους κατάσταση. Δεν χρειάζεται να πούμε ότι αυτή η μέθοδος αντιμετώπισης έχει ελάχιστη αξία για την προστασία των αρχείων από τους σημερινούς ιούς.

Ωστόσο, η κατάσταση είναι διαφορετική σε ένα πραγματικό περιβάλλον πολλαπλών χρηστών, στο οποίο το επίπεδο δικαιωμάτων μπορεί να ορίζεται για κάθε χρήστη ατομικά. Εάν απαιτούνται τα προνόμια του επόπτη για την αλλαγή των δικαιωμάτων προσπέλασης ενός αρχείου, ο ιός δεν μπορεί να αλλάξει αυτές τις ιδιότητες όταν τρέχει από τον λογαριασμό ενός κανονικού χρήστη.

Τυπικά, στους κανονικούς χρήστες ενός δικτύου με τα Windows 2000 (ή, όσον αφορά σ' αυτό το θέμα, οποιουδήποτε άλλου λειτουργικού συστήματος δικτύων) παρέχεται πρόσβαση για εγγραφή και ανάγνωση σε έναν "δημόσιο" κατάλογο. Εάν ο υπολογιστής ενός χρήστη κολλήσει ιό, ο ιός μπορεί να εξαπλωθεί στους υπόλοιπους υπολογιστές μολύνοντας αρχεία τα οποία περιέχονται στον δημόσιο κατάλογο, επειδή ο ιός μπορεί να τροποποιήσει αυτά τα αρχεία. Επίσης, εάν μολυνθεί ο υπολογιστής του επόπτη, τα πάντα έχουν χαθεί - ο λογαριασμός αυτός έχει πρόσβαση για εγγραφή στον δημόσιο κατάλογο. Ο ορισμός ενός ελάχιστου απαιτούμενου επιπέδου δικαιωμάτων όχι μόνο επαυξάνει την ασφάλεια, αλλά μπορεί επίσης να σας βοηθήσει να αποτρέψετε την εξάπλωση ιών.

Μαζί με τις ιδιότητες που σχετίζονται με τα δικαιώματα πρόσβασης, οι ιοί μπορούν επίσης να τροποποιήσουν την ημερομηνία/ώρα ενός αρχείου. Η αλλαγή αυτή διασφαλίζει ότι ο χρήστης δεν θα έχει στην διάθεση του κανένα στοιχείο για να αντιληφθεί το πρόβλημα. Τα πρώτα προγράμματα ανίχνευσης ιών έψαχναν για αλλαγές στις ημερομηνίες των αρχείων. Επειδή οι περισσότεροι σημερινοί ιοί επαναφέρουν την αρχική ημερομηνία/ώρα αφού μολύνουν τα αρχεία, αυτή η μέθοδος ανίχνευσης ιών δεν είναι πλέον αποτελεσματική.

Stealth

Το χαρακτηριστικό stealth (απόκρυψη) επιτρέπει σε έναν ιό να κρύψει τις αλλαγές που κάνει σε ένα αρχείο ή στον τομέα εκκίνησης ενός δίσκου. Όταν ο ιός φορτώνεται στην μνήμη, παρακολουθεί τις κλήσεις συστήματος για αρχεία και τομείς δίσκων. Αφού παγιδεύσει μία τέτοια κλήση, ο ιός τροποποιεί τις πληροφορίες που επιστρέφονται στην διεργασία που έκανε την κλήση, έτσι ώστε αυτή να βλέπει τις αρχικές, μη-μολυσμένες πληροφορίες. Αυτό βοηθά τον ιό να αποφεύγει τον εντοπισμό του.

Για παράδειγμα, πολλοί ιοί που μολύνουν τον τομέα εκκίνησης έχουν το χαρακτηριστικό stealth. Εάν το σύστημα εκκινήσει από τον μολυσμένο δίσκο (με αποτέλεσμα ο ιός να φορτωθεί στην μνήμη), προγράμματα όπως το FDISK αναφέρουν ότι η εγγραφή εκκίνησης του δίσκου είναι εντάξει. Ο ιός υποκλέπτει τις κλήσεις που κάνει η εντολή FDISK και επιστρέφει τις αρχικές πληροφορίες του τομέα εκκίνησης του δίσκου. Ωστόσο, εάν εκκινήσετε το σύστημα από μία "καθαρή" δισκέτα, ο μολυσμένος δίσκος θα είναι απροσπέλαστος. Εάν τρέξετε τώρα το FDISK, αυτό θα σας αναφέρει ότι ο τομέας εκκίνησης του συγκεκριμένου δίσκου είναι κατεστραμμένος.

Η απόκρυψη του ιού μπορεί επίσης να επιτευχθεί τροποποιώντας τις πληροφορίες που αναφέρουν εντολές όπως οι DIR και MEM. Δηλαδή, ένας ιός μπορεί να κρατήσει κρυφή την ύπαρξη του τόσο στο τοπικό μέσο αποθήκευσης, όσο και στην φυσική μνήμη. Βέβαια, για να λειτουργήσει σαν stealth ένας ιός πρέπει να τρέχει στην μνήμη· αυτό σημαίνει ότι τουλάχιστον το τμήμα του ιού που είναι υπεύθυνο για την λειτουργία stealth μπορεί να ανιχνεύεται από προγράμματα ανίχνευσης/ εξάλειψης ιών.

Τα αντίμετρα που διαθέτουν οι ιοί για το πρόγραμμα ανίχνευσης/εξάλειψης ιών

Ορισμένοι ιοί διαθέτουν αντίμετρα για την άμυνα τους έναντι οποιασδήποτε μορφής ανίχνευσης. Οι ιοί αυτοί παρακολουθούν το σύστημα συνεχώς για ενδείξεις ενεργών προγραμμάτων ανίχνευσης/εξάλειψης ιών και λαμβάνουν προληπτικά μέτρα για να

διασφαλίσουν ότι θα παραμείνουν απαρατήρητοι, θεωρήστε τα αντίμετρα των ιών σαν μια παραλλαγή της δυνατότητας stealth, αλλά με πιο προχωρημένη άποψη.

Για παράδειγμα, ορισμένοι ιοί παρακολουθούν την δραστηριότητα του συστήματος αφού φορτωθούν στην μνήμη. Εάν ο ιός ανιχνεύσει ότι έχει εκκινήσει ένα πρόγραμμα ανίχνευσης ιών, προσπαθεί να το ξεγελάσει κάνοντας το να πιστεύει ότι υπάρχει κάποιος άλλος ιός στο σύστημα. Συνήθως, για την εξάλειψη του ιού που αναφέρεται σαν "δόλωμα" απαιτείται κάποια καταστροφική διαδικασία εκκαθάρισης, η οποία καθιστά άχρηστο το σύστημα εάν ο ιός αυτός δεν υπάρχει πραγματικά. Κατόπιν, ο πραγματικός ιός προσπαθεί να εξαπλώσει τον εαυτό του στο σύστημα αρχείων, έτσι ώστε ακόμη κι αν γίνει προσπάθεια επαναφοράς, ο ιός να έχει την δυνατότητα να μολύνει την νέα διαμόρφωση του συστήματος.

Όμοια με την δυνατότητα stealth, τα αντίμετρα για τα προγράμματα ανίχνευσης/εξάλειψης ιών βασίζονται στο γεγονός ότι ο ιός είναι ενεργός στην μνήμη και μπορεί να παρακολουθεί την δραστηριότητα που λαμβάνει χώρα στο σύστημα. Για τον λόγο αυτό είναι σημαντικό να εκκινείτε το σύστημα από μία "καθαρή" δισκέτα πριν επιχειρήσετε οποιαδήποτε προσπάθεια επαναφοράς του. Σε υπολογιστές με το DOS είναι επίσης σημαντικό να χρησιμοποιείτε τον διακόπτη ηλεκτρικής τροφοδοσίας για να σβήνετε τον υπολογιστή: πολλοί ιοί μπορούν να παγιδεύουν τον συνδυασμό πλήκτρων CTRL+ALT+DEL, προκαλώντας μία ψεύτικη επανεκκίνηση του συστήματος. Έτσι ο ιός μπορεί να παραμείνει ενεργός στην μνήμη, αν και φαινομενικά το σύστημα έχει επανεκκινήσει.

Κρυπτογράφηση

Οι δημιουργοί ιών δεν έχουν παραβλέψει τα πλεονεκτήματα της κρυπτογράφησης. Η κρυπτογράφηση δίνει σ' έναν δημιουργό ιών την δυνατότητα να κρύψει τις κλήσεις συστήματος και τα αλφαριθμητικά που θα μπορούσαν να προδώσουν την ύπαρξη ενός ιού. Κρυπτογραφώντας τον κώδικα ενός ιού, ο δημιουργός του καθιστά πολύ πιο δύσκολη την ανίχνευση του ιού.

Ωστόσο η ανίχνευση δεν είναι εντελώς αδύνατη, επειδή πολλοί ιοί χρησιμοποιούν μια απλή μορφή κρυπτογράφησης και το ίδιο κλειδί για όλο τον κώδικα τους. Αν και η ανάκτηση του πραγματικού κώδικα του ιού μπορεί να είναι δύσκολη, η ακολουθία αποκρυπτογράφησης είναι πανομοιότυπη για όλα τα μολυσμένα αρχεία. Εάν μπορείτε να βρείτε το κλειδί αποκρυπτογράφησης, μπορείτε επίσης να το χρησιμοποιήσετε για να ανιχνεύσετε όλες τις μελλοντικές εμφανίσεις του ιού. Ακόμη κι αν δεν καταφέρετε να βρείτε το κλειδί αποκρυπτογράφησης, το κρυπτογραφημένο αλφαριθμητικό είναι μία υπογραφή την οποία μπορούν να χρησιμοποιήσουν τα προγράμματα ανίχνευσης/εξάλειψης ιών για να ανιχνεύσουν την ύπαρξη του ιού.

Η αποτελεσματικότητα αυτής της μεθόδου ανίχνευσης κρυπτογραφημένων ιών εξαρτάται από το κρυπτογραφημένο αλφαριθμητικό. Να θυμάστε ότι τα προγράμματα ανίχνευσης/εξάλειψης ιών δεν μπορούν να γνωρίζουν εκ των προτέρων εάν αυτό που αναζητούν είναι κρυπτογραφημένες πληροφορίες ή απλό κείμενο. Εάν το κρυπτογραφημένο αλφαριθμητικό του ιού μπορεί να διαμορφωθεί ώστε να μοιάζει με κάποια αθώα μορφή κώδικα, τα προγράμματα ανίχνευσης/εξάλειψης ιών θα δυσκολευτούν πολύ να ξεχωρίσουν τα μολυσμένα από τα μη-μολυσμένα αρχεία.

Πολυμορφικές μεταλλαγές

Ένας πολυμορφικός ιός μπορεί να αλλάζει την υπογραφή του σε κάθε αρχείο που μολύνει, παραμένοντας ωστόσο λειτουργικός. Πολλά προγράμματα ανίχνευσης ιών μπορούν να ανιχνεύσουν την ύπαρξη ενός ιού ψάχνοντας για προδοτικό κώδικα (την υπογραφή του ιού). Επειδή ένας πολυμορφικός ιός μπορεί να αλλάζει την υπογραφή του μεταξύ διαδοχικών μολύνσεων, η ανίχνευση του είναι πολύ πιο δύσκολη.

Ένας τρόπος για την δημιουργία ενός πολυμορφικού ιού είναι η χρήση πολλών διαφορετικών σχημάτων κρυπτογράφησης, τα οποία χρησιμοποιούν διαφορετικές ρουτίνες αποκρυπτογράφησης. Μόνο μία από αυτές τις ρουτίνες είναι διαθέσιμη σε κάθε

εμφάνιση του ιού. Συνεπώς, ένα πρόγραμμα ανίχνευσης ιών δεν μπορεί να ανιχνεύσει όλες τις εμφανίσεις του ιού παρά μόνο εάν είναι γνωστές όλες οι ρουτίνες αποκρυπτογράφησης του.

Η εύρεση των ρουτινών αποκρυπτογράφησης μπορεί να είναι σχεδόν αδύνατη εάν ο ιός χρησιμοποιεί τυχαίο κλειδί, ή τυχαία ακολουθία χαρακτήρων όταν εκτελεί την κρυπτογράφηση. Για παράδειγμα, πολλοί ιοί περιλαμβάνουν αθώο ή αδρανή κώδικα ο οποίος μπορεί να μεταφέρεται σε διαφορετικές θέσεις μέσα στον ιό πριν από την κρυπτογράφηση, χωρίς να επηρεάζει την ικανότητα λειτουργίας του ιού. Το παραγόμενο κρυπτογράφημα διαφέρει σε κάθε εμφάνιση του ιού επειδή διαφέρει η ακολουθία χαρακτήρων του κωδικού κρυπτογράφησης.

Ο αποτελεσματικότερος τρόπος δημιουργίας ενός πολυμορφικού ίου είναι η ενσωμάτωση ειδικού κώδικα σε ένα εκτελέσιμο αρχείο, ο οποίος αναφέρεται σαν μηχανισμός μεταλλαγής (mutation engine). Επειδή ο μηχανισμός αυτός είναι σπονδυλωτός, μπορεί εύκολα να προστεθεί στον κώδικα οποιουδήποτε υπάρχοντος ιού. Ο μηχανισμός μεταλλαγής περιλαμβάνει μία γεννήτρια τυχαίων αριθμών η οποία συμβάλλει ακόμη περισσότερο στην παράλλαξη του κρυπτογραφημένου κώδικα. Επειδή χρησιμοποιείται μία γεννήτρια τυχαίων αριθμών, το παραγόμενο κρυπτογράφημα είναι απρόβλεπτο - διαφέρει σε κάθε μολυσμένο αρχείο. Το τελικό αποτέλεσμα είναι ότι η ανίχνευση ενός τέτοιου ιού καθίσταται σχεδόν αδύνατη.

Ο ιός μας κατάφερε με επιτυχία να αναπαράγει τον εαυτό του και να αποφύγει την ανίχνεύση. Το ερώτημα τώρα είναι, τι θα κάνει ο ιός στην συνέχεια; Οι περισσότεροι ιοί προγραμματίζονται με τέτοιο τρόπο ώστε να αναμένουν για ένα συγκεκριμένο συμβάν. Το συμβάν αυτό θα μπορούσε να είναι οτιδήποτε - π.χ. η έλευση μιας συγκεκριμένης ημερομηνίας, η μόλυνση συγκεκριμένου αριθμού αρχείων, ή ο εντοπισμός μιας προκαθορισμένης δραστηριότητας.

Αφού λάβει χώρα το συγκεκριμένο συμβάν, εκρήγνυται η βόμβα - φανερώνεται ο πραγματικός σκοπός του ιού. Ο σκοπός του ιού θα μπορούσε να είναι κάτι τόσο αθώο

όσο η αναπαραγωγή ενός ηχητικού σήματος μέσω του μεγαφώνου ή των ηχείων του υπολογιστή, ή κάτι τόσο καταστροφικό όσο η εξάλειψη όλων των αρχείων από τον σκληρό δίσκο. Οι περισσότεροι ιοί-βόμβες μπορούν να εκτελούν καταστροφικές ενέργειες επειδή τα σημερινά περιβάλλοντα με τα Windows δεν παρέχουν επαρκή "απομόνωση" μεταξύ λειτουργικού συστήματος και των προγραμμάτων που τρέχουν στον υπολογιστή.

Ένας ιός μπορεί να έχει απευθείας πρόσβαση στις χαμηλού επιπέδου λειτουργίες του συστήματος. Η δυνατότητα αυτή υπάρχει επειδή το λειτουργικό σύστημα αναμένει ότι τα προγράμματα που τρέχουν σ' αυτό είναι έμπιστα. Για παράδειγμα, οι Windows εφαρμογές μπορούν να προσπελάζουν απευθείας την μνήμη και τον πίνακα διακοπών (interrupt table) του συστήματος. Αν και αυτές οι δυνατότητες μπορούν να βελτιώσουν την απόδοση μιας εφαρμογής – επιτρέποντας της να παρακάμπτει το λειτουργικό σύστημα - παρέχουν επίσης μεγάλο μερος της λειτουργικότητας που χρειάζεται ένας ιός για να λειτουργήσει σαν stealth. Αν και οι περισσότερες "βόμβες" δεν μπορούν να προκαλέσουν φυσική ζημιά, μπορούν να αφήσουν τον υπολογιστή σε μη-χρησιμοποιήσιμη κατάσταση. Το BIOS των περισσότερων σημερινών motherboard περιέχει τον αρχικό κώδικα που χρησιμοποιείται για την εκκίνηση του συστήματος. Επειδή το λειτουργικό σύστημα μπορεί να ενημερώσει τις εντολές του BIOS, ένας ιός μπορεί να διαγράψει ολοκληρωτικά τα περιεχόμενα του BIOS αφήνοντας το motherboard νεκρό, χωρίς καμία δυνατότητα ανάκαμψης.

Ιοί κοινωνικής μηχανικής

Αν και με την αυστηρή έννοια του όρου ένας ιός κοινωνικής μηχανικής (social-engineering virus) δεν είναι πραγματικός ιός, μπορεί να προκαλέσει τόσα προβλήματα όσα κι ένας πραγματικός ιός. Οι ιοί κοινωνικής μηχανικής ικανοποιούν όλα τα κριτήριαενός κανονικού ίου, εκτός από το γεγονός ότι η εξάπλωση τους βασίζεται στους ανθρώπους και όχι σ' έναν υπολογιστή. Ένα καλό παράδειγμα ίου κοινωνικής μηχανικής είναι η φάρσα (hoax) Good Times που κυκλοφορούσε στο Internet για πολλά χρόνια. Ουσιαστικά ήταν ένα μήνυμα e-mail το οποίο πληροφορούσε τους παραλήπτες του ότι κυκλοφορεί ένας επικίνδυνος ιός μέσω e-mail, ο οποίος έχει την δυνατότητα να σβήσει όλα τα αρχεία από τον υπολογιστή τους. Το μήνυμα ισχυρίζονταν επίσης ότι η ύπαρξη του ιού είχε επιβεβαιωθεί από την AOL (την παγκόσμια αυθεντία στους ιούς). Οι παραλήπτες του μηνύματος που ενδιαφέρονταν να μην μολυνθούν *ο* υπολογιστές των φίλων τους

προωθούσαν αυτό το μήνυμα-φάρσα σε όλα τα άτομα που ήταν καταχωρισμένα στα βιβλία διευθύνσεων τους.

Αλλά πώς ικανοποιεί ένας ιός κοινωνικής μηχανικής τα κριτήρια που ορίζουν έναν πραγματικό ιό;

Αναπαραγωγή

Για την εξάπλωση τους, οι ιοί κοινωνικής μηχανικής βασίζονται σε δύο χαρακτηριστικά της ανθρώπινης φύσης: καλές προθέσεις και ευπιστία. Επειδή είναι στην φύση μας να βοηθάμε τους συνανθρώπους μας, είμαστε κάτι περισσότερο κι από πρόθυμοι να κοινοποιήσουμε οτιδήποτε δείχνει σαν προειδοποίηση για ιούς σε άλλους χρήστες υπολογιστών. Επίσης, επειδή είναι στην φύση μας να πιστεύουμε όσα διαβάζουμε -χωρίς να μπαίνουμε στον κόπο να τα επαληθεύσουμε - θα μπορούσαμε κάλλιστα να προωθούμε έναν ιό χωρίς να το γνωρίζουμε.

Απόκρυψη

Για να αποκρύψουν την απειλητική τους φύση, οι ιοί χρησιμοποιούν γλώσσα η οποία καθιστά το μήνυμα πιστευτό για τον μέσο χρήστη. Για παράδειγμα, το μήνυμα μπορεί να ισχυρίζεται ότι μία εταιρεία όπως η AOL, η IBM ή η Microsoft επαλήθευσε την ύπαρξη του ιού για τον οποίο υποτίθεται ότι μας προειδοποιεί. Επειδή όλες αυτές οι εταιρείες σχετίζονται με τους υπολογιστές και είναι γνωστές στον μέσο χρήστη, το μήνυμα δείχνει έγκυρο.

Βόμβα

Αυτός είναι ο τομέας των ιών κοινωνικής μηχανικής που περνάει απαρατήρητος από τους περισσότερους ανθρώπους. Σ' αυτή την περίπτωση η "βόμβα" είναι σπατάλη εύρους ζώνης και αχρείαστη ανησυχία. Επειδή το μήνυμα είναι απάτη, σπαταλιέται εύρος ζώνης κάθε φορά που προωθείται σε έναν επόμενο παραλήπτη. Επειδή ο αποστολέας δίνει την αίσθηση του επείγοντος στο μήνυμα, ο ιός στέλνεται συνήθως μαζικά. Και επειδή το μήνυμα περιλαμβάνει συνήθως προειδοποίηση για μία καταστροφή, προκαλείται αχρείαστη ανησυχία ή φόβος στους παραλήπτες. Δηλαδή, η βόμβα έγκειται στον τρόπο με τον οποίο επηρεάζουν αυτά τα μηνύματα τόσο τους πόρους των υπολογιστών, όσο και τους χειριστές τους.

Κανένα πρόγραμμα ανίχνευσης ιών δεν μπορεί να ανιχνεύσει τους ιούς κοινωνικής μηχανικής. Μόνο η εκπαίδευση και η επαλήθευση των πληροφοριών που πέφτουν στα μάτια μας μπορεί να μας βοηθήσει να αποτρέψουμε την εξάπλωση τέτοιων ιών.

8.2. Από πού προέρχονται οι ιοί

Οι αρχικοί ιοί υπολογιστών ήταν συνήθως φάρσες ανάμεσα σε προγραμματιστές σε συστήματα μεγάλων ή μίνι υπολογιστών στην δεκαετία του 60. Όταν εμφανίστηκε ο πρώτος προσωπικός υπολογιστής, ήταν φυσικό οι έξυπνοι, τεχνικά καταρτισμένοι άνθρωποι που τους αγόραζαν να σκέφτονται διάφορα έξυπνα και αναπάντεχα προγράμματα, ακόμη και φάρσες.

Αυτό το είδος της δραστηριότητας ήταν ακίνδυνο στην αρχή. Αλλά όσο όλο και περισσότεροι άνθρωποι άρχισαν να χρησιμοποιούν προσωπικούς υπολογιστές, και τα εργαλεία για προγραμματιστές και για άσχετους έγιναν πιο δυνατά και έξυπνα, τα πράγματα άρχισαν να ξεπερνούν τα αστεία και τις φάρσες.

Οι ιοί υπολογιστών ήταν μάλλον σπάνιοι μέχρι τα μέσα της δεκαετίας του 80. (Υποπτεύομαι ότι οι άνθρωποι που γράφουν προγράμματα ιών, προηγουμένως προσπαθούσαν να σπάσουν κλειδωμένα προγράμματα.) Μέχρι τότε, τα μέσα διανομής ιών ήταν μηδαμινά. Καθώς όμως άρχισε να αναπτύσσεται η κοινή χρήση λογισμικού - με δισκέτες ή με μόντεμ - άρχισαν να αυξάνονται οι επιθέσεις με ιούς στους προσωπικούς υπολογιστές.

Αρκετά είδη ζωντανών ή αυτοαναπαραγόμενων ιών υπολογιστών εμφανίστηκαν εκείνη την εποχή, εισβάλλοντας σε μεγάλους και σε μίνι υπολογιστές, όπως και σε εξειδικευμένα δίκτυα εταιρικών υπολογιστών και άρχισαν να διακόπτουν την

αλληλογραφία και άλλες επικοινωνίες. (Ανάμεσα τους ήταν και ο διάσημος ιός του δικτύου της IBM, που μπορούσε να αναπαραχθεί και να μετακινηθεί μέσα σε δίκτυα, σχεδόν σαν να ήταν ένα ζωντανό, αυτοκατευθυνόμενο πράγμα.)

Καθώς οι ιοί υπολογιστών άρχισαν να συζητούνται στις ειδήσεις στα τέλη της δεκαετίας του 80, ακόμη περισσότεροι άρχισαν να εμφανίζονται. Αρκετοί ήταν ιδιαίτερα δημιουργικοί στην σύλληψη τους και "κακοί" στην υλοποίηση τους. Τουλάχιστον ένας ιός ανακοινώθηκε εκ των προτέρων από τον κατασκευαστή του, ο οποίος υποσχέθηκε ότι δεν θα κάνει τίποτε περισσότερο από το να εμφανίσει ένα μήνυμα για ειρήνη σε όλο τον κόσμο, μια συγκεκριμένη ημερομηνία. Υπήρχαν ακόμη και μερικοί ιδιαίτερα ύπουλοι ιοί, που μεταμφιέστηκαν σαν προγράμματα προστασίας από ιούς.

Σήμερα, υπολογίζουμε ότι τουλάχιστον δύο ή τρεις νέοι ιοί εμφανίζονται κάθε μέρα.

Λίγα λόγια για την προφύλαξη

Οι συναντήσεις που είχα με ιούς είναι σχετικά λίγες και σπάνιες, αν λάβουμε υπόψη μας τον αριθμό των φορών που έχω εκτεθεί σε κινδύνους μέσω φορτώσεων και κοινής χρήσης δίσκων. Σε περισσότερα από 20 χρόνια που έχω φορτώσει χιλιάδες αρχεία και έχω πάρει πολύ δωρεάν διανεμόμενο λογισμικό στον δίσκο μου, έχω υποστεί μόνο δύο επιθέσεις από ιούς, και τις δύο στα τέλη της δεκαετίας του 80. Ο ένας βρισκόταν σε ένα φαινομενικά νόμιμο πρόγραμμα βάσεων δεδομένων κοινής χρήσης, και απλώς εμφάνιζε το μήνυμα "Gotcha!" από καιρού σε καιρό. Ξεφορτώθηκα αυτό τον ιό διαγράφοντας το πρόγραμμα βάσης δεδομένων. Ένα άλλο πρόγραμμα ιός ήταν πολύ χειρότερο. Άλλαζε τα μεγέθη αρχείων - περιλαμβανομένων και των αόρατων αρχείων συστήματος επάνω στον σκληρό μου δίσκο - με σκοπό να γεμίσει τον δίσκο. Χρειάστηκε να αναμορφοποιήσω τον σκληρό δίσκο για να ξεφορτωθώ αυτό τον ιό.

Μερικοί από τους φίλους μου δεν ήταν ούτε τόσο τυχεροί, ούτε τόσο προσεκτικοί, όσο εγώ. Ένας έχει ένα νέο ιό στον υπολογιστή του κάθε μήνα, και ένας άλλος βρίσκει δύο ή τρεις στον υπολογιστή του κάθε φορά που κάνει ένα έλεγχο νια ιούς (κάτι που δεν κάνει συχνά).

Το θέμα είναι ότι προσέχω πάντα τι φορτώνω, και πώς χειρίζομαι τα φορτωμένα προγράμματα - και αυτό συμβαίνει επειδή η ιστορία μου με τους υπολογιστές προηγείται των προγραμμάτων προστασίας από ιούς. Έχω κάνει το ίδιο με αρχεία δίσκων. Με λίγη προσοχή και φρόνηση στις εργασίες σας με τους υπολογιστές, μπορείτε να μειώσετε κατά πολύ το βαθμό κινδύνου από ιούς και ίσως να μην χρειαστεί να ασχοληθείτε ποτέ με επιθέσεις από ιούς. Με αυτό το θέμα ασχολούμαστε σε αυτό το κεφάλαιο.

Γιατί υπάρχουν οι ιοί

Οι άνθρωποι δημιουργούν ιούς υπολογιστών για διάφορους λόγους. Τα κίνητρα περιλαμβάνουν, χωρίς να παίζει ρόλο η σειρά που τα αναφέρουμε:

- Εκδίκηση εναντίον ενός συγκεκριμένου συστήματος ή ομάδας χρηστών υπολογιστών
- Επιθυμία να ακουστεί το όνομα τους (αν και είναι ανώνυμοι)
- Φάρσες
- Πολιτικές πράξεις
- Πειραματισμούς ("να δω αν μπορώ να το κάνω")

Ο λαϊκός τύπος έχει σκιαγραφήσει τους δημιουργούς ιών σαν έξυπνους παλιάνθρωπους. Ταυτόχρονα, άλλοι δημοσιογράφοι έχουν δηλώσει ότι ορισμένοι δημιουργοί ιών είναι ανικανοποίητοι στις προσωπικές τους ζωές και ενεργούν από μια βαθιά ανάγκη να έχουν τον έλεγχο των πραγμάτων.

Όποιος και να είναι ο λόγος που οι προγραμματιστές δημιουργούν ιούς και προγράμματα Δούρειους Ίππους, οι λόγοι αυτοί δεν παίζουν κανένα ρόλο αν εσείς κολλήσετε ένα ιό. Έτσι, πρέπει να πάρετε κάθε δυνατή προφύλαξη για να τους αποφύγετε.

8.3. Πώς μπορεί να μπει ένας ιός στο σύστημα μου;

Ένας ιός συνήθως εισέρχεται σε ένα σύστημα μεταμφιεσμένος σε πρόγραμμα ή μακροεντολή. Για παράδειγμα, μπορείτε να φορτώσετε ένα αρχείο που αναφέρεται σαν παιχνίδι και ονομάζεται FUNGAME.EXE. Μπορείτε να το εκτελέσετε και, ενώ προσπαθείτε να καταλάβετε πώς να παίξετε το παιχνίδι, το πρόγραμμα μπορεί να εργάζεται στο φόντο διαγράφοντας όλα τα αρχεία στον τρέχοντα κατάλογο - ή σε όλους τους καταλόγους - ή να προσαρτά ένα ιό στο αρχείο εκκίνησης. (Όπως αναφέραμε προηγουμένως, Δούρειος Ίππος είναι ένα άλλο, παλιότερο και πιο κατάλληλο όνομα γι' αυτό το είδος ιού.)

Η πλειοψηφία των ιών και των προγραμμάτων Δούρειων ίππων μεταμφιέζονται σε προγράμματα δημόσιας περιοχής ή δημόσιας χρήσης για να ενθαρρύνουν την διανομή τους. Όπως όμως αναφέραμε προηγουμένως, μερικά μεταμφιέζονται σε ή ενσωματώνονται μέσα σε νόμιμα ή παράνομα αντίτυπα εμπορικού λογισμικού. Επίσης, μερικά προγράμματα ιών έχουν σχεδιαστεί ώστε να εκμεταλλεύονται την ανθρώπινη απληστία, προσποιούμενα ότι είναι προγράμματα που σας βοηθούν να εισβάλετε σε δικτυακούς τόπους ή να πάρετε δωρεάν χρόνο από ένα παροχές υπηρεσιών ή από μια online υπηρεσία, ή προσφέροντας κάποιο άλλο κέρδος.

Φορτώσεις

Για τους περισσότερους ιούς, οι φορτώσεις είναι ο κύριος τρόπος για να μπουν μέσο σε ένα υπολογιστή, εν μέρει επειδή τόσο πολλά αρχεία στις μέρες μας δίνονται με φορτώσεις. Ο κύριος λόγος όμως, είναι ότι ένα αρχείο που μεταφέρει ένα ιό διαδίδεται ταχύτερα online σε σχέση με την μετάδοση σε άλλα μέσα. Επειδή αυτοί που δημιουργούν ιούς υπολογιστών θέλουν να γίνουν γνωστοί, οι περισσότεροι στοχεύουν στον online κόσμο, σαν σημείο διανομής των δημιουργιών τους.

Οι ιοί που διαχέονται online έχουν επίσης την μεγαλύτερη πιθανότητα μακροβιότητας. Χρειάζεται πολύς χρόνος από την αρχική ανακάλυψη ενός ιού σε μια φόρτωση πριν να καταστραφεί και η τελευταία του εμφάνιση. Πολλοί άνθρωποι που τον φορτώνουν δεν εργάζονται online ή δεν δίνουν σημασία σε online πηγές πληροφοριών, και μερικοί από αυτούς τον εκφορτώνουν κάπου αλλού, βάζοντας τον σε online υπηρεσίες ή σε δικτυακούς τόπους, από όπου άλλοι ανυποψίαστοι χρήστες μπορούν να τον φορτώσουν. Έτσι, κάθε νέα εκφόρτωση πολλαπλασιάζει τον πιθανό αριθμό υπολογιστών που εκτίθενται στον ιό. Μερικοί επίσης μπορεί να στείλουν τον ιό με e-mail σε φίλους τους.

Προσαρτήσεις E-mail

Οι ιοί μπορούν να βρεθούν σε προγράμματα ή αρχεία που προσαρτώνται σε μηνύματα email. Η απλή ανάγνωση ενός μηνύματος δεν θα ενεργοποιήσει τον ιό, αλλά όμως το άνοιγμα του προσαρτημένου μολυσμένου αρχείου και/ή η εκτέλεση του προσαρτημένου προγράμματος (ή μακροεντολής) θα τον ενεργοποιήσουν.θα δείτε ότι τα προγράμματα που προσαρτώνται σε μηνύματα email αυξάνονται σε συχνότητα τις περιόδους των μεγάλων διακοπών. Αν και τέτοιες προσαρτήσεις μπορεί να φαίνονται αβλαβείς και κατάλληλες για την συγκεκριμένη περίοδο, είναι καλύτερο να τις διαγράψετε. Ακόμη και αν ξέρετε ποιος σας έστειλε το αρχείο, πρέπει να έχετε υπόψη σας ότι πιθανώς να προωθεί κάτι που του στάλθηκε με τον ίδιο τρόπο και μπορεί να μην έχει ελέγξει για να δει αν το αρχείο είναι ένας ιός.

Αρχεία κοινής χρήσης σε ένα δίκτυο

Τα αρχεία κοινής χρήσης σε ένα δίκτυο συχνά διαχέουν ιούς γρήγορα. Προσέξτε την πολιτική του διαχειριστή του συστήματος σας σε ότι αφορά αρχεία κοινής χρήσης απειλές από ιούς και σχετικά θέματα. Φροντίστε να αποφεύγετε την εκτέλεση προσαρτήσεων email στο δίκτυο, και ειδοποιήστε τον διαχειριστή του συστήματος αμέσως μόλις βρείτε ένα ύποπτο αρχείο.

Δίσκοι κοινής χρήσης

Αντίθετα, οι ιοί που διαχέονται σε δίσκους, διαχέονται πολύ αργά. Οι ιδιοκτήτες υπολογιστών δεν μοιράζονται προγράμματα σε δίσκους όσο έκαναν παλιότερα, τώρα που ό,τι θέλετε βρίσκεται online, δωρεάν. Αλλά η διάχυση ιών μέσω δίσκων κοινής χρήσης δεν έχει εξαλειφθεί.

Ένας φίλος ή συνεργάτης σας μπορεί, χωρίς να το ξέρει, να έχει φορτώσει ένα μολυσμένο πρόγραμμα και να σας το δώσει σε μια δισκέτα, πριν να καταλάβει τι είναι. Επίσης, κάποιος μπορεί να δίνει αντίγραφα ενός δημοφιλούς προγράμματος κοινής χρήσης, χωρίς να ξέρει ότι το πρόγραμμα είναι μολυσμένο.

Στις σπάνιες περιπτώσεις που ένας ιός εισδύσει μέσα σε μια δισκέτα ή ένα CD-ROM που έχει παραχθεί εμπορικά, τότε σχεδόν κάθε αντίγραφο του μπορεί να καταστραφεί γρήγορα, επειδή οι εκδότες του λογισμικού παρακολουθούν προσεκτικά, πού πηγαίνουν τα προϊόντα τους. (Αυτό συνέβη ήδη. Πολλές φορές, ένας κακόβουλος υπάλληλος μιας εταιρίας έχει τροποποιήσει ένα εμπορικό προϊόν, πριν να αναπαραχθεί για πώληση.

Τώρα που τα συστήματα αντιγραφής CD είναι φθηνά, *πρέπει* να είστε προσεκτικοί με τα προγράμματα που εκτελείτε από ένα CD που έχει κατασκευαστεί στο σπίτι.

Worms

Κατά παράδοση, ένα worm (σκουλήκι) θεωρούνταν σαν μία εφαρμογή η οποία μπορούσε να αναπαράγει τον εαυτό της μέσω μιας μόνιμης ή dial-up σύνδεσης δικτύου. Ανόμοια με έναν ιό ο οποίος εξαπλώνει τον εαυτό του στον σκληρό δίσκο ή στο σύστημα αρχείων ενός υπολογιστή, ένα worm είναι ένα αυθύπαρκτο και αυτό-υποστηριζόμενο πρόγραμμα. Ενα τυπικό worm διατηρεί μόνο ένα λειτουργικό αντίγραφο του εαυτού του ενεργό στην μνήμη· δεν χρειάζεται καν να γραφτεί στον δίσκο.

Ωστόσο, τα τελευταία χρόνια η διαχωριστική γραμμή ανάμεσα στα worms και στους ιούς έγινε πολύ θολή, ξεκινώντας από την πολύ γνωστή περίπτωση της Melissa. Η Melissa ήταν ένα υβρίδιο worm/ιού το οποίο μπορούσε να μολύνει ένα σύστημα (σαν ένας ιός), τροποποιώντας τα έγγραφα ώστε να περιέχουν αποσπάσματα από την τηλεοπτική εκπομπή The Simpsons. Αλλά μπορούσε επίσης να χρησιμοποιήσει το Βιβλίο Διευθύνσεων του Microsoft Outlook και του Outlook Express για να στείλει τον εαυτό της (σαν ένα worm) σε άλλα συστήματα του δικτύου, τα οποία μολύνονταν από ένα έγγραφο συνημμένο στο μήνυμα. Το 2000 ο ιός ILOVEYOU, ένα ακόμη υβρίδιο ιού/worm, προκάλεσε σημαντική ζημιά διαγράφοντας αρχεία μορφής JPEG και MP3 από υπολογιστές σε όλο τον κόσμο. (Ορισμένοι ισχυρίζονται ότι ο ιός ILOVEYOU ήταν επίσης μία μορφή Δούρειου Ίππου επειδή παρουσίαζε τον εαυτό του σαν ένα καθ' όλα έγκυρο μήνυμα e-mail). Επίσης, ενώ η Melissa περιόριζε τον εαυτό της στις πρώτες 50 διευθύνσεις του Βιβλίου Διευθύνσεων ενός χρήστη, ο ιός I LOVE YOU χρησιμοποιούσε όλες τις διευθύνσεις που έβρισκε.

Το Code Red, ένα worm το οποίο γνώρισε αρκετή δημοσιότητα (μαζί με τον διάδοχο του Code Red II), ήταν επίσης μία συνδυασμένη μορφή απειλής η οποία περιλάμβανε επιθέσεις άρνησης εξυπηρέτησης, παραποίηση ιστοσελίδων και έναν Δούρειο Ίππο ο οποίος εκτελούνταν μετά από την κύρια επίθεση. Ο Nimda ένας από τους ιούς με συχνή παρουσία το 2001, είχε πρωτοποριακή συμπεριφορά όσον αφορά στον τρόπο με τον οποίο τροποποιούσε υπάρχοντα web sites ώστε να παρέχουν μολυσμένο κώδικα σε client

συστήματα. Αφού μολύνονταν τα client συστήματα αναζητούσαν άλλα ευάλωτα web sites και ο κύκλος της μόλυνσης συνεχίζονταν.

Στα τέλη του 2001 άρχισε να κυκλοφορεί ένα νέο worm με όνομα Klez (το οποίο συνεχίζει να είναι αρκετά ενεργό την στιγμή που γράφονται αυτές οι γραμμές, το καλοκαίρι του 2002). Έχοντας δυνατότητα να απενεργοποιεί τα προγράμματα ανίχνευσης/εξάλειψης ιών (μαζί με άλλα, καθ' όλα έγκυρα προγράμματα), το worm klez μπορεί να παρουσιάσει τον εαυτό του στους χρήστες ακόμη και σαν μία διόρθωση (patch) για την θωράκιση των συστημάτων τους έναντι του εαυτού του!

Το worm vampire

Τα worms δεν θεωρούνταν πάντα κακό πράγμα. Στην δεκαετία του '80, οι John Shock και Jon Hepps της Xerox έκαναν μία θαυμάσια έρευνα για τα worms, με στόχο να δείξουν πόσο ευεργετικά θα μπορούσαν να είναι αυτά τα προγράμματα. Για τον σκοπό αυτό δημιούργησαν πολλά προγράμματα worms και τα χρησιμοποίησαν για την εποπτεία και διαχείριση του δικτύου υπολογιστών της ίδιας της Xerox. Το αποτελεσματικότερο από αυτά ήταν το worm vampire. Αυτό το worm κάθονταν αδρανές κατά την διάρκεια της ημέρας, όταν ο βαθμός χρήσης του δικτύου ήταν υψηλός. Την νύχτα όμως το worms ξυπνούσε και χρησιμοποιούσε τον άεργο χρόνο της CPU για να ολοκληρώσει πολύπλοκες εργασίες. Το επόμενο πρωί το worm vampire αποθήκευε την δουλειά του και πήγαινε για ύπνο.

Το worm vampire ήταν εξαιρετικά αποτελεσματικό, μέχρι την ημέρα που οι υπάλληλοι της Xerox έφτασαν στην δουλειά τους και διαπίστωσαν ότι όλα τα συστήματα υπολογιστών είχαν καταρρεύσει λόγω κάποιας διεργασίας η οποία δεν λειτουργούσε σωστά. Όταν επανεκκίνησαν τα συστήματα, κατέρρευσαν αμέσως και πάλι από το worm. Αυτό είχε σαν αποτέλεσμα την απομάκρυνση του worm απ' όλα τα συστήματα του δικτύου και τον τερματισμό της σχετικής έρευνας.

The great internet worm

Μέχρι τις 3 Νοεμβρίου του 1988, ελάχιστη ήταν η προσοχή που έδιναν οι άνθρωτοι στα worms. Αυτή ήταν η ημέρα που παρουσιάστηκε το "Μεγάλο Σκουλήκι' στο Internet. Σε λιγότερο από έξι ώρες, αυτό το 99 γραμμών πρόγραμμα κατάφερε κυριολεκτικά να θέσει εκτός λειτουργίας 6,000 συστήματα SUN και VAX συνδεδεμένα στο Internet.

Το πρόγραμμα αυτό γράφτηκε από τον Robert Morris, γιο ενός από τους πλέον αξιόλογους ειδικούς στην ασφάλεια που υπήρχαν στις Η.Π.Α. εκείνη την εποχή. Έχει ειπωθεί ότι η συγγραφή του worm δεν ήταν μία κακόβουλη ενέργεια, αλλά η προσπάθεια ενός γιου να βγει από την σκιά του πατέρα του. Το σκεπτικό αυτό υποστηρίζεται και από τον ίδιο τον κώδικα του worm, επειδή το πρόγραμμα αυτό δεν εκτελούσε σκόπιμα καταστροφικές ενέργειες.

Αυτό που έκανε το συγκεκριμένο worm ήταν απλό: εκκινούσε μία μικρή διεργασία, η οποία έτρεχε στο παρασκήνιο, σε κάθε μηχανή που συναντούσε. Το πείραμα αυτό θα περνούσε πιθανώς εντελώς απαρατήρητο, εάν δεν υπήρχε μία μικρή αβλεψία στον προγραμματισμό του worm. Πριν μολύνει ένα σύστημα, το worm δεν έλεγχε εάν το σύστημα ήταν ήδη μολυσμένο. Αυτή η αβλεψία οδήγησε στην πολλαπλή μόλυνση συστημάτων. Ενώ η μία εμφάνιση του worm έθετε ελάχιστο φόρτο στον επεξεργαστή, οι δεκάδες - ή πιθανώς εκατοντάδες - απανωτές μολύνσεις μπορούσαν να "γονατίσουν" ένα σύστημα.

Οι επόπτες συστημάτων βρέθηκαν μπλεγμένοι σε μία άνιση μάχη. Αφού καθάριζαν και επανεκκινούσαν ένα σύστημα, αυτό μολύνονταν ξανά, πολύ γρήγορα. Όταν ανακάλυψαν ότι το worm χρησιμοποιούσε τρωτά σημεία του Sendmail για να μεταφερθεί από σύστημα σε σύστημα, πολλοί επόπτες αντέδρασαν αποσυνδέοντας τα συστήματά τους από το Internet, ή θέτοντας εκτός λειτουργίας τα συστήματα ηλεκτρονικού ταχυδρομείου. Κατά πάσα πιθανότητα η αντίδραση αυτή έκανε περισσότερη ζημιά παρά καλό, επειδή ουσιαστικά απομόνωνε τα συστήματα καθιστώντας αδύνατή την λήψη ενημερωμένων πληροφοριών για το worm, συμπεριλαμβανομένων πληροφοριών για την αποτροπή περαιτέρω μόλυνσης.

Απ΄όλο το χάος που ακολούθησε μετά από αυτό το περιστατικό, προέκυψαν αρκετά

καλά πράγματα. Χρειάστηκε ένα επεισόδιο τόσο μεγάλου εύρους για να αλλάξει το σκεπτικό των ανθρώπων όσον αφορά στα τρωτά σημεία των υπολογιστικών τους συστημάτων. Εκείνη την εποχή τέτοιου είδους τρωτά σημεία θεωρούνταν απλώς “σφάλματα"(bugs) δευτερεύουσας σημασίας. Το περιστατικό με το "Μεγάλο Σκουλήκι" του Internet βοήθησε στο να προσδιοριστούν με σαφέστερο τρόπο αυτές οι αδυναμίες. Χάρη σ' αυτό το περιστατικό δημιουργήθηκε ο οργανισμός CERT (Computer Emergency Response Team), ο οποίος είναι υπεύθυνος για την τεκμηρίωση των προβλημάτων που σχετίζονται με την ασφάλεια των υπολογιστών και βοηθά άλλες εταιρείες και οργανισμούς να λύνουν τέτοια προβλήματα.

Το worm wank

Αν και το "Μεγάλο Σκουλήκι" του Internet είναι το πιο γνωστό παράδειγμα, σίγουρα δεν είναι το χειρότερο worm που είδαμε ποτέ. Τον Οκτώβριο του 1989, το worm WANK (Worms Against Nuclear Killers) άρχισε να διαδίδεται σε ανυποψίαστα συστήματα. Αν και εξαιρετικά καταστροφικό, το worm αυτό ήταν μοναδικό στο είδος του επειδή μόλυνε μόνο συστήματα DEC και χρησιμοποιούσε μόνο το πρωτόκολλο DECnet (δηλαδή δεν μεταδίδονταν μέσω του IP). Αυτό το worm έκανε τα ακόλουθα:

Έστελνε e-mail (κατά πάσα πιθανότητα στον δημιουργό του) με το οποίο προσδιόριζε σε ποια συστήματα είχε επιτεθεί, μαζί με τα ονόματα σύνδεσης και τους κωδικούς πρόσβασης που είχε χρησιμοποιήσει. Άλλαζε τους κωδικούς πρόσβασης υπαρχόντων λογαριασμών. Άφηνε "πίσω πόρτες" για την πρόσβαση στο σύστημα.Έβρισκε χρήστες σε τυχαίους κόμβους του δικτύου και τους καλούσε χρησιμοποιώντας το βοήθημα phone. Μόλυνε τα COM αρχεία του τοπικού συστήματος έτσι ώστε να έχει την δυνατότητα να ενεργοποιηθεί εκ νέου μελλοντικά, ακόμη και μετά από τον καθαρισμό του συστήματος,

Άλλαζε την αρχική οθόνη χαιρετισμού, αναφέροντας την ύπαρξη του.

Τροποποιούσε το script σύνδεσης, έτσι ώστε να δείχνει σαν να είχαν διαγραφεί όλα τα αρχεία ενός χρήστη.Έκρυβε τα αρχεία μετά από την σύνδεση, προσπαθώντας να πείσει τον χρήστη ότι τα αρχεία του είχαν διαγραφεί.

Όπως ίσως φαντάζεστε, το worms αυτό κατέστρεψε κάτι περισσότερο από την ημέρα μερικών εποπτών συστημάτων. Χρειάστηκε αρκετός καιρός για την επιτυχημένη εξάλειψη αυτού του worm απ' όλα τα μολυσμένα συστήματα.

8.4. Δούρειοι Ίπποι

Ένας Δούρειος Ίππος (Trojan horse), όπως υποδηλώνει το όνομα του, είναι μία εφαρμογή η οποία κρύβει μία δυσάρεστη έκπληξη. Πρόκειται συνήθως για μία διεργασία ή λειτουργία η οποία προστίθεται σκόπιμα από τον δημιουργό του Δούρειου Ίππου και εκτελεί μία δραστηριότητα για την οποία δεν είναι ενήμερος ο χρήστης (και την οποία κατά πάσα πιθανότητα δεν θα ενέκρινε). Η κρυφή λειτουργία είναι αυτή που κάνει ένα τέτοιο πρόγραμμα Δούρειο Ιππο.

Επειδή ο ιός ILOVEYOU παρουσίαζε τον εαυτό του σαν ένα έγκυρο μήνυμα e-mail (ο κώδικας του ιού ήταν αποθηκευμένος σ' ένα αρχείο συνημμένο στο μήνυμα), ορισμένοι τον αντιμετώπισαν σαν Δούρειο Ιππο, αν και ένα μήνυμα e-mail δεν είναι εφαρμογή. Άλλα παραδείγματα εχθρικού κώδικα θολώνουν ακόμη περισσότερο την διαχωριστική γραμμή· ένα τέτοιο παράδειγμα είναι μία επίθεση στην οποία ο τύπος MIME ενός συνημμένου δήλωνε τον ιό σαν ένα πρόγραμμα πολυμέσων, όταν στην πραγματικότητα ήταν εκτελέσιμος κώδικας (και διατηρούσε την επέκταση .EXE). Επειδή εξ ορισμού τα Windows ενεργοποιούν τα αρχεία πολυμέσων το εκτελέσιμο κατάφερε να περάσει από τους συνήθεις ελέγχους ασφάλειας των συνημμένων, και επειδή είχε επέκταση .exe τα Windows το εκτέλεσαν όπως και οποιοδήποτε άλλο πρόγραμμα πράγμα το οποίο οδήγησε στην μόλυνση του συστήματος.

Σε τι διαφέρουν οι δούρειοι ίπποι από τους ιούς;

Ένας Δούρειος Ίππος διαφέρει από έναν ιό στο ότι δεν αναπαράγεται και δεν προσαρτά τον εαυτό του σε άλλα αρχεία. Ένας Δούρειος Ίππος είναι μία αυτόνομη εφαρμογή της οποίας η "βόμβα" περιλαμβάνεται στον αρχικό πηγαίο κώδικα. Δεν απαιτείται η εκτέλεση ενός άλλου προγράμματος για να γίνει καταστροφική.

Στο UNIX έχουν δημιουργηθεί ορισμένοι Δούρειοι Ίπποι για την αντικατάσταση υπαρχουσών εφαρμογών δικτύου. Ένας εισβολέας μπορεί να αντικαταστήσει την διεργασία του Telnet Server (telnetd) με μία άλλη διεργασία, δικής του έμπνευσης. Αν και το πρόγραμμα λειτουργεί πανομοιότυπα με το telnetd, στο παρασκήνιο υποκλέπτει όλα τα ονόματα σύνδεσης και τους κωδικούς πρόσβασης των χρηστών που πιστοποιούνται στο σύστημα. Επίσης, ένας εισβολέας θα μπορούσε να αντικαταστήσει την client εφαρμογή Telnet δίνοντας έγκυρες πληροφορίες λογαριασμών σε απομακρυσμένα συστήματα. Δηλαδή, ο εισβολέας μπορεί να διεισδύσει συστηματικά σε κάθε server ενός δικτύου.

Υπήρξαν επίσης παραδείγματα Δούρειων Ίππων οι οποίοι σχεδιάστηκαν με στόχο να είναι εξαιρετικά καταστροφικοί. Για παράδειγμα, τον Απρίλιο του 1997 πολλοί άνθρωποι έπεσαν θύματα του Δούρειου Ίππου AOL4FREE.COM. Ενώ οι χρήστες πίστευαν ότι είχαν βρει ένα βοήθημα το οποίο θα τους παρείχε έναν δωρεάν λογαριασμό στην AOL, στην πραγματικότητα αυτό που λάμβαναν ήταν ένα θαυμάσιο εργαλείο για την διαγραφή όλων των αρχείων που υπήρχαν στον τοπικό τους δίσκο. Αμέσως μόλις έτρεχαν το πρόγραμμα, αυτό διέγραφε μόνιμα όλα τα αρχεία από την μονάδα δίσκου C.

Μήπως μόλις αγόρασα έναν δούρειο ίππο;

Φυσικά, δεν γράφονται όλοι οι Δούρειοι Ίπποι από κακόβουλους χάκερ. Για παράδειγμα, ορισμένοι χρήστες διαπίστωσαν με μεγάλη τους έκπληξη ότι όταν έμπαιναν στο Microsoft Network, το λογισμικό αυτής της υπηρεσίας έκανε μία πλήρη καταγραφή του εξοπλισμού και του λογισμικού τους, συμπεριλαμβανομένων των εφαρμογών της Microsoft αλλά και άλλων ανταγωνιστικών προϊόντων. Όταν ο χρήστης συνδέονταν στο δίκτυο οι πληροφορίες αυτές προωθούνταν αυτόματα στην Microsoft, η οποία θα μπορούσε έτσι να ελέγξει εάν έχουν αποκτηθεί οι απαιτούμενες άδειες χρήσης των προϊόντων της. Αν και η Microsoft ισχυρίστηκε ότι οι πληροφορίες αυτές συλλέγονταν με μοναδικό σκοπό την τεχνική υποστήριξη, πολλοί άνθρωποι θεώρησαν αυτή την ενέργεια καθαρή παραβίαση της ιδιωτικότητάς τους.

Σε πολλές άλλες περιπτώσεις οι κατασκευαστές εξοπλισμού και λογισμικό προσθέτουν επιπλέον λειτουργικότητα στα προϊόντα τους, με αντίτιμο την παραβίαση της ασφάλειας των συστημάτων των πελατών τους. Για παράδειγμα, τον Μάιο του 1998 έγινε γνωστό ότι η 3COM, καθώς και ορισμένοι άλλοι κατασκευαστές εξοπλισμού δικτύωσης συμπεριλάμβαναν λογαριασμούς υπό μορφή "πίσω πόρτας" για την πρόσβαση στα switches και στους routers που διέθεταν. Αυτοί οι μη-τεκμηριωμένοι λογαριασμοί είναι συνήθως αόρατοι για τον τελικό χρήστη και δεν μπορούν να διαγραφούν ή να απενεργοποιηθούν. Και σ' αυτή την περίπτωση, οι κατασκευαστές των προϊόντων ισχυρίστηκαν ότι είχαν δημιουργήσει τις "πίσω πόρτες" για λόγους που σχετίζονταν με την τεχνική υποστήριξη (π.χ. στην περίπτωση που ένας επόπτης ξεχάσει έναν κωδικό πρόσβασης). Ωστόσο, αυτές οι "πίσω πόρτες" αφήνουν τα προϊόντα τους εντελώς εκτεθειμένα και τους επόπτες ανυποψίαστους.

Τέτοιου είδους δραστηριότητες κυμαίνονται σε μία "γκρίζα" ζώνη, μεταξύ της τεχνικής

υποστήριξης και των Δούρειων Ίππων. Αν και αυτές οι μη-τεκμηριωμένες "πίσω πόρτες" προστίθενται από καθ' όλα αξιόπιστους και έγκριτους κατάσκευαστές, αποτελούν κίνδυνο για την ασφάλεια και αφήνουν εντελώς ανυποψίαστο τον πελάτη για τους πιθανούς κινδύνους. Η δυνατότητα πρόσβασης μέσω "πίσω πόρτας" είναι κάτι το οποίο πολλοί επόπτες συστημάτων θα ήθελαν να απενεργοποιήσουν, αλλά για να γίνει αυτό θα πρέπει πρώτα να μάθουν την ύπαρξη τους.

8.5. Αποτρεπτικά Μέτρα

Τώρα που έχετε δει τις αρνητικές επιπτώσεις που μπορούν να έχουν αυτά τα κακόβουλα προγράμματα για το δίκτυο σας, τι μπορείτε να κάνετε για να αμυνθείτε; Ο

μόνος αλάνθαστος τρόπος για να εντοπίσετε ένα εχθρικό πρόγραμμα είναι να ζήσετε από έναν έμπειρο προγραμματιστή να εξετάσει τον πηγαίο κώδικα του. Επειδή όμως οι περισσότερες εφαρμογές διατίθενται μόνο σε εκτελέσιμη μορφή, θα έπρεπε να καταφύγετε σε μεθόδους αντίστροφης μηχανικής για την εξέταση του περιεχομένου των αρχείων. Προφανώς, η προσέγγιση αυτή είναι υπερβολικά χρόνο βάρα και ακριβή για να αποτελεί βιώσιμη λύση για έναν τυπικό οργανισμό.

Οποιοδήποτε άλλο αποτρεπτικό μέτρο απέχει πολύ από το να θεωρηθεί 100 τοις εκατό αποτελεσματικό. Θα πρέπει να διεξάγετε μία ανάλυση κίνδυνων για να εξακριβώσετε πόση προστασία χρειάζεστε πραγματικά. Υπάρχουν πολλές διαφορετικές τεχνικές τις οποίες μπορείτε να χρησιμοποιήσετε για αποτρέψετε την μόλυνση των υπολογιστών του δικτύου σας από ιούς. Κάθε μία έχει τα ισχυρά και τα αδύνατα σημεία της, αλλά η χρήση τους σε συνδυασμό παρέχει συνήθως τα καλύτερα αποτελέσματα.

Έλεγχος Πρόσβασης

Η καθιέρωση μιας πολιτικής ελέγχου πρόσβασης δεν είναι μόνο ένα καλό μέτρο για την ασφάλεια· μπορεί επίσης να σας βοηθήσει να αποτρέψετε την εξάπλωση καταστροφικών προγραμμάτων στους υπολογιστές του δικτύου σας. Δεν θα πρέπει να μπερδεύετε τον έλεγχο πρόσβασης με τις ιδιότητες των αρχείων (π.χ. μόνο ανάγνωσης ή συστήματος), οι οποίες μπορούν να αλλαχτούν εύκολα από έναν ιό. Η διαχείριση της πρόσβασης των χρηστών θα πρέπει να γίνεται μέσω ενός λειτουργικού συστήματος για περιβάλλοντα πολλαπλών χρηστών, το οποίο δίνει στον επόπτη του δικτύου τη δυνατότητα να καθορίζει τα δικαιώματα προσπέλασης αρχείων ατομικά για κάθε χρήστη.

Ο έλεγχος πρόσβασης δεν είναι κάτι το οποίο μπορεί να αντιληφθεί την παρουσία εχθρικών προγραμμάτων, ή να τα εξαλείψει από το σύστημα. Είναι απλώς μία στρατηγική μέσω της οποίας βοηθάτε τα συστήματα σας να αποφύγουν πιθανή μόλυνση από ιούς. Για παράδειγμα, οι περισσότεροι ιοί βασίζονται στο ότι ο μολυσμένος υπολογιστής έχει πλήρη πρόσβαση σε όλα τα αρχεία (όπως ισχύει στην προκαθορισμένη διαμόρφωση των Windows NT). Εάν ένας προνοητικός επόπτης αλλάξει τα προκαθορισμένα δικαιώματα ώστε οι χρήστες να έχουν πρόσβαση μόνο για ανάγνωση στα εκτελέσιμα που χρησιμοποιούν, ένας ιός δεν θα έχει τη δυνατότητα να μολύνει αυτά τα αρχεία.

Επαλήθευση του Ελεγκτικού Αθροίσματος

Ένα ελεγκτικό άθροισμα (checksum), ή έλεγχος CRC (Cyclic Redundancy), είναι ένας μαθηματικός τρόπος για την επαλήθευση της ακεραιότητας των δεδομένων ενός αρχείου. Μέσω του ελεγκτικού αθροίσματος, τα περιεχόμενα ενός αρχείου μπορούν να εκφράζονται σαν μία αριθμητική τιμή. Εάν αλλάξει έστω κι ένα byte από τα δεδομένα του αρχείου αλλάζει επίσης η τιμή του ελεγκτικού αθροίσματος, ακόμη κι αν παραμείνει σταθερό το μέγεθος του αρχείου. Συνήθως εκτελείται ένας αρχικός έλεγχος σ' ένα μη-μολυσμένο σύστημα για να δημιουργηθεί μία τιμή "βάσης". Κατόπιν έλεγχος CRC εκτελείται σε τακτά διαστήματα, αναζητώντας οποιεσδήποτε αλλαγές έχουν γίνει στα αρχεία. Αυτή η μέθοδος έχει ορισμένες αδυναμίες. Κατ' αρχήν, ο έλεγχος CRC δεν μπορεί να ανιχνεύσει πραγματικά την μόλυνση ενός αρχείου· το μόνο που κάνει είναι να αναζητά αλλαγές. Γι' αυτό τον λόγο τα αυτοαποσυμπιεζόμενα εκτελέσιμα αποτυγχάνουν συνήθως στον έλεγχο CRC. Επίσης, ακόμη και όταν η αλλαγή οφείλεται πράγματι σε έναν ιό, ο έλεγχος CRC δεν έχει δυνατότητα να "καθαρίσει" το αρχείο. Τέλος, πολλοί ιοί γράφονται σκόπιμα με τέτοιο τρόπο ώστε να ξεγελούν τους ελέγχους CRC, κάνοντάς σας να πιστεύετε ότι οι πληροφορίες του αρχείου δεν έχουν αλλάξει.

Παρακολούθηση Διεργασιών

Μία άλλη μέθοδος με την οποία μπορείτε να εμποδίσετε οποιαδήποτε επιβλαβή προγράμματα να αναλάβουν τον έλεγχο ενός υπολογιστή είναι η παρακολούθηση διεργασιών (process monitoring). Η παρακολούθηση διεργασιών παρακολουθεί διαρκώς την δραστηριότητα του συστήματος και "συλλαμβάνει" οποιεσδήποτε ενέργειες δείχνουν ύποπτες. Για παράδειγμα, στα περισσότερα σημερινά PCs, το BIOS περιλαμβάνει μία ειδική ρύθμιση κατά των ιών. Όταν ενεργοποιηθεί, η ρύθμιση αυτή δίνει στον υπολογιστή

την δυνατότητα να "συλλαμβάνει" όλες τις απόπειρες τροποποίησης της κύριας εγγραφής εκκίνησης (master boot record). Εάν ένας ιός που μολύνει τον τομέα εκκίνησης επιχειρήσει να αποθηκεύσει τον εαυτό του σ' αυτή την περιοχή, το BIOS διακόπτει την αίτηση και ζητά την έγκριση του χρήστη. Και σ' αυτή την περίπτωση όμως υπάρχουν ορισμένα προβλήματα. Το πρώτο είναι ότι οι ιοί και τα κανονικά προγράμματα έχουν πολλά κοινά χαρακτηριστικά: είναι εξαιρετικά δύσκολο να ξεχωρίσει κανείς το ένα από το άλλο. Για παράδειγμα, εάν ενεργοποιήσετε την ρύθμιση κατά των ιών στο BIOS, η εκτέλεση του βοηθήματος FDISK θα έχει σαν αποτέλεσμα την εμφάνιση ενός προειδοποιητικού μηνύματος όπως αναφέραμε παραπάνω. Αν και το FDISK δεν είναι ιός (εκτός κι αν συμμερίζεστε το σκεπτικό ότι όλα τα προγράμματα της Microsoft είναι ιοί), προκαλεί την εμφάνιση αυτού του προειδοποιητικού μηνύματος επειδή οι δραστηριότητες του θεωρούνται ύποπτες. Το αποτέλεσμα είναι ένας ψεύτικος συναγερμός - το BIOS πιστεύει ότι έχει ανιχνεύσει έναν ιό, όταν στην πραγματικότητα αυτό δεν ισχύει.

Ένα δεύτερο πρόβλημα της παρακολούθησης διεργασιών είναι το γεγονός ότι απαιτεί την παρέμβαση του χρήστη και αυξημένο επίπεδο γνώσεων εκ μέρους του. Για παράδειγμα, ένας χρήστης ο οποίος αντιμετωπίζει τον ψεύτικο συναγερμό που αναφέραμε παραπάνω πρέπει να γνωρίζει αρκετά πράγματα για τους υπολογιστές ώστε να καταλάβει ότι αυτό που προκάλεσε την προειδοποίηση δεν ήταν η ανίχνευση ενός πραγματικού ιού, αλλά η κανονική λειτουργία του FDISK.

Ας το δούμε όμως και από την άλλη πλευρά: μπορεί να υπάρχει πράγματι ένας ιός που μολύνει τον τομέα εκκίνησης στην δισκέτα στην οποία είναι αποθηκευμένο το FDISK. Κατ' επέκταση, ο χρήστης θα μπορούσε να υποθέσει ότι αυτό που αντιμετωπίζει είναι ένας ψεύτικος συναγερμός, όταν στην πραγματικότητα πρόκειται για έναν ιό. Αν και σ' αυτή την περίπτωση το BIOS θα εμφάνιζε το μήνυμα προειδοποίησης για ιό σε διαφορετικό σημείο της διαδικασίας (κατά την διάρκεια που φορτώνεται το FDISK και όχι όταν κλείνει), ο τελικός χρήστης πρέπει να έχει υψηλό επίπεδο γνώσεων και εμπειρίας στους υπολογιστές για να προσδιορίσει με ακρίβεια ποια προβλήματα οφείλονται πράγματι σε ιούς και ποια όχι.

Το πρόβλημα της διαφοροποίησης μεταξύ ενός ιού και μιας κανονικής εφαρμογής γίνεται ακόμη πιο εμφανές όταν αρχίζετε να παρακολουθείτε άλλους τύπους δραστηριοτήτων. Θα πρέπει να θεωρείτε ύποπτες τις ενέργειες διαγραφής αρχείων Όλοι χρησιμοποιούμε βοηθήματα διαχείρισης αρχείων και περιστασιακά διαγράφουμε αρχεία από τον υπολογιστή μας· τέτοιου είδους ενέργειες θα έπρεπε να παράγουν ψεύτικους συναγερμούς; Το ίδιο ισχύει για την παρακολούθηση των αλλαγών που γίνονται στα αρχεία, τις λειτουργίες μεταγωγής μνήμης, κ.λ.π. Όλες αυτές οι δραστηριότητες μπορεί να εκτελούνται από κάποιον ιό, αλλά εκτελούνται επίσης και από κανονικές εφαρμογές.

Σχεδόν η μόνη χρήσιμη άποψη της παρακολούθησης διεργασιών είναι η προειδοποίηση για ιούς που επιτίθενται στο BIOS, όπως περιγράψαμε παραπάνω. Αν και συνεχίζει να υπάρχει πιθανότητα ψεύτικων συναγερμών, στην πραγματικότητα είναι μάλλον σπάνιο ένας χρήστης να τρέχει το FDISK ή κάποια άλλη έγκυρη εφαρμογή η οποία επιχειρεί να γράψει στον τομέα εκκίνησης του δίσκου. Συνήθως αυτό συμβαίνει μόνο εάν ο χρήστης εγκαθιστά ένα νέο λειτουργικό σύστημα στον υπολογιστή του. Κατά συνέπεια, η συχνότητα εμφάνισης ψεύτικων συναγερμών είναι πολύ μικρή.

Προγράμματα ανίχνευσης ιών

Ο δημοφιλέστερος τρόπος ανίχνευσης των ιών είναι η χρήση ειδικών προγραμμάτων ανίχνευσης ιών. Τα προγράμματα ανίχνευσης ιών (virus scanners) χρησιμοποιούν ειδικά αρχεία υπογραφών (signature files) για να εντοπίζουν ιούς σε μολυσμένα αρχεία. Ένα αρχείο υπογραφών δεν είναι τίποτα περισσότερο από μία βάση δεδομένων στην οποία έχουν καταχωριστεί όλοι οι γνωστοί ιοί μαζί με τα συγκεκριμένα χαρακτηριστικά τους. Στα χαρακτηριστικά αυτά περιλαμβάνονται δείγματα του κώδικα κάθε ιού, οι τύποι των αρχείων που μολύνει και οποιεσδήποτε άλλες πληροφορίες θα μπορούσαν να είναι χρήσιμες για τον εντοπισμό του ιού. Χρησιμοποιώντας ένα ξεχωριστό αρχείο για την αποθήκευση αυτών των πληροφοριών, μπορείτε να ενημερώνετε το πρόγραμμα που χρησιμοποιείτε έτσι ώστε να έχει την δυνατότητα να εντοπίζει ακόμη και τους νεότερους ιούς που κυκλοφορούν, αντικαθιστώντας αυτό και μόνο αυτό το αρχείο. Δεν χρειάζεται να

αναβαθμίσετε ολόκληρο το πρόγράμμα. Η πρακτική αυτή είναι ιδιαίτερα χρήσιμη, δεδομένου ότι σχεδόν κάθε μήνα παρουσιάζονται νέοι ιοί.

Όταν ένα πρόγραμμα ανίχνευσης ιών ελέγχει ένα αρχείο, εξετάζει εάν οποιοδήποτε μέρος του κώδικα του αρχείου ταιριάζει με οποιαδήποτε από τις καταχωρίσεις που υπάρχουν στο αρχείο υπογραφών. Εάν βρεθεί ένα ταίριασμα, το πρόγραμμα ανίχνευσης ιών ειδοποιεί τον χρήστη ότι έχει εντοπιστεί ένας ιός. Στην πλειονότητα τους αυτά τα προγράμματα μπορούν κατόπιν να εκτελέσουν μία ξεχωριστή διεργασία για την εκκαθάριση των αρχείων από τους ιούς.

Ο μεγαλύτερος περιορισμός των προγραμμάτων ανίχνευσης ιών είναι ότι μπορούν να ανιχνεύουν μόνο τους γνωστούς ιούς. Εάν το σύστημα σας μολυνθεί από έναν ιό που μόλις έχει δημιουργηθεί, είναι πολύ πιθανό τα προγράμματα ανίχνευσης ιών να μην τον πάρουν είδηση. Το πρόβλημα αυτό είναι ακόμη πιο ανησυχητικό στις περιπτώσεις των πολυμορφικών ιών. Όπως αναφέραμε παραπάνω σ' αυτό το κεφάλαιο, οι πολυμορφικοί ιοί μπορούν να αλλάζουν την υπογραφή τους σε κάθε μόλυνση. Για να μπορεί ένα πρόγραμμα ανίχνευσης ιών να είναι 100% αποτελεσματικό έναντι αυτής της κατηγορίας ιών, πρέπει να είναι εφοδιασμένο με ένα αρχείο υπογραφών το οποίο θα περιλαμβάνει όλες τις πιθανές παραλλαγές του πολυμορφικού ιού. Εάν λείπει έστω και μία παραλλαγή, το πρόγραμμα ανίχνευσης ιών μπορεί να μην έχει την δυνατότητα να καθαρίσει ένα μολυσμένο αρχείο, οπότε ο ιός μπορεί να μολύνει ξανά το σύστημα.

Τα αποσυμπιεσμένα ή κρυπτογραφημένα αρχεία μπορούν επίσης να προκαλέσουν προβλήματα όταν χρησιμοποιείτε ένα πρόγραμμα ανίχνευσης ιών. Επειδή οι διαδικασίες αποσυμπίεσης και αποκρυπτογράφησης αλλάζουν τον τρόπο αποθήκευσης των δεδομένων, ένα πρόγραμμα ανίχνευσης ιών μπορεί να μην έχει την δυνατότητα να ανιχνεύσει ιούς οι οποίοι κρύβονται μέσα σ' ένα τέτοιο αρχείο.Για παράδειγμα, ας υποθέσουμε ότι χρησιμοποιείτε το PKZIP ή το WinZip για να συμπιέσετε μία ομάδα αρχείων έτσι ώστε να τα μεταφέρετε σε δισκέτα. Κατόπιν χρησιμοποιείτε ένα πρόγραμμα ανίχνευσης ιών για να ελέγξετε την δισκέτα και να βεβαιωθείτε ότι κανένα από τα συμπιεσμένα αρχεία σας δεν περιέχει ιό. Εκτός κι αν το πρόγραμμα ανίχνευσης ιών που χρησιμοποιείτε αναγνωρίζει την μορφή άρχειου ZIP (πράγμα το οποίο δεν ισχύει για όλα), δεν θα μπορέσει να ανιχνεύσει ιούς κρυμμένους μέσα στα συμπιεσμένα αρχεία.

Το πρόβλημα αυτό είναι ακόμη πιο οξύ στα κρυπτογραφημένα αρχεία. Επειδή ένα πρόγραμμα ανίχνευσης ιών δεν έχει τρόπο για να αποκρυπτογραφήσει ένα κρυπτογραφημένο αρχείο, κατά πάσα πιθανότητα δεν θα μπορέσει επίσης να εντοπίσει οποιουσδήποτε ιούς περιέχει. Θα πρέπει πρώτα να αποκρυπτογραφήσετε το αρχείο και κατόπιν να το ελέγξετε για ιούς.

Κατηγορίες προγραμμάτων ανίχνευσης ιών

Υπάρχουν δύο βασικοί τύποι προγραμμάτων ανίχνευσης ιών:

- Προγράμματα τα οποία εκτελούν τον έλεγχο για ιούς κατ' απαίτηση του χρήστη.
- Προγράμματα τα οποία ενεργοποιούνται και παραμένουν μόνιμα στην μνήμη

Ένα πρόγραμμα ανίχνευσης ιών κατ' απαίτηση εκκινεί από τον χρήστη, ή μέσω κάποιας αυτοματοποιημένης διαδικασίας. Όταν εκκινείτε ένα τέτοιο πρόγραμμα αυτό ψάχνει συνήθως για ιούς σε έναν ολόκληρο δίσκο, ή σε όλο το σύστημα. Στους ελέγχους που διενεργεί περιλαμβάνεται επίσης η μνήμη RAM, καθώς και συσκευές αποθήκευσης όπως οι σκληροί δίσκοι ή οι δισκέτες.

Τα μόνιμα στην μνήμη προγράμματα ανίχνευσης ιών είναι προγράμματα τα οποία τρέχουν σαν διεργασίες παρασκηνίου σε ένα σύστημα. Συνήθως εκκινούν κατά την εκκίνηση του ίδιου του συστήματος και παραμένουν διαρκώς ενεργά. Οποτεδήποτε γίνεται μία αίτηση για την προσπέλαση ενός αρχείου στο σύστημα, το μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών "συλλαμβάνει" την αίτηση και πιστοποιεί ότι δεν υπάρχουν ιοί, πριν επιτρέψει την φόρτωση του αρχείου στην μνήμη.

Και με τις δύο μεθόδους γίνονται ορισμένοι συμβιβασμοί. Τα προγράμματα ανίχνευσης ιών κατ' απαίτηση λειτουργούν μετά από το γεγονός. Εκτός κι αν συνηθίζετε

να τρέχετε ένα τέτοιο πρόγραμμα πριν προσπελάσετε οποιοδήποτε αρχείο (πράγμα απίθανο εκτός κι αν είστε αρρωστημένα σχολαστικοί), το σύστημα σας είναι πιθανό να έρθει σε επαφή μ' έναν ιό πριν αυτός ανιχνευθεί. Εν αντιθέσει, ένα μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών μπορεί να εντοπίσει έναν ιό πριν αυτός μολύνει το σύστημα σας, αλλά με ανάλογο κόστος στην απόδοση. Ο έλεγχος κάθε αρχείου μειώνει την ταχύτητα προσπέλασης, επιβραδύνοντας την συνολική απόδοση του συστήματος.

Οι κατασκευαστές μόνιμων στην μνήμη προγραμμάτων ανίχνευσης ιών ξέρουν ότι η ταχύτητα προσπέλασης αρχείων είναι σημαντική και αναγνωρίζουν ότι πολλοί χρήστες θα προτιμούσαν να απενεργοποιήσουν το πρόγραμμα ανίχνευσης ιών αντί να υποστούν οποιαδήποτε μείωση στην απόδοση. Για τον λόγο αυτό, πολλά μόνιμα στην μνήμη προγράμματα ανίχνευσης ιών δεν εκτελούν τόσο "σχολαστικούς" ελέγχους όσοτα προγράμματα ανίχνευσης ιών που εκτελούνται κατ' απαίτηση. Συνήθως, αυτά τα προγράμματα πετυχαίνουν καλύτερη απόδοση επειδή ελέγχουν μόνο τις πιο πιθανές υπογραφές ιών, ή μόνο τα αρχεία που είναι πιο πιθανό να μολυνθούν από ιούς (π.χ. τα αρχεία με επέκταση COM).

Προβλήματα σε μεγάλα περιβάλλοντα

Περιοδικά, όλοι οι κατασκευαστές προγραμμάτων ανίχνευσης ιών κυκλοφορούν ενημερωμένα αρχεία υπογραφών με στόχο να διασφαλίσουν ότι τα προϊόντα τους θα μπορούν να ανιχνεύσουν όσο το δυνατόν περισσότερους από τους γνωστούς ιούς. Η ενημέρωση των αρχείων με τις υπογραφές των ιών μπορεί να σημαίνει σημαντικά αυξημένο φόρτο εργασίας για τους επόπτες που είναι υπεύθυνοι για την διατήρηση της ασφάλειας σε μεγάλα περιβάλλοντα δικτύων. Εάν έχετε PCs με τα λειτουργικά συστήματα DOS, Windows ή Macintosh, θα πρέπει να ενημερώνετε τα αρχεία υπογραφών των προγραμμάτων ανίχνευσης ιών για κάθε λειτουργικό σύστημα.

Πολλοί κατασκευαστές έλαβαν ιδιαίτερα μέτρα για την μείωση αυτού του προβλήματος. Για παράδειγμα, το LANDesk Virus Protect της Intel χρησιμοποιείτο σκεπτικό των virus domains για την ομαδοποίηση πολλαπλών servers και σταθμών εργασίας του δικτύου. Έτσι, ο επόπτης του δικτύου μπορεί να ενημερώνει τα αρχεία υπογραφών, να εξετάζει τα προειδοποιητικά μηνύματα, ή ακόμη και να ελέγχει τις παραμέτρους για την ανίχνευση των ιών από έναν και μόνο υπολογιστή. Μία τέτοια προσέγγιση μπορεί να μειώσει δραματικά τον φόρτο εργασίας που απαιτείται για την διαχείριση της προστασίας των συστημάτων από ιούς σ' ένα μεγάλο περιβάλλον.

Μία κλιμακούμενη ανάλογα με το περιβάλλον λύση για την προστασία των υπολογιστών από ιούς σας βοηθά όχι μόνο να μειώσετε το συνολικό κόστος, αλλά επίσης να διασφαλίσετε ότι το περιβάλλον σας θα είναι καλά προστατευμένο ανά πάσα στιγμή. Όπως αναφέραμε, περιοδικά οι κατασκευαστές προγραμμάτων ανίχνευσης ιών κυκλοφορούν ενημερωμένα αρχεία υπογραφών. Ωστόσο, αυτά τα αρχεία υπογραφών έχουν ελάχιστη χρησιμότητα εάν δεν τα εγκαταστήσετε σε κάθε σύστημα το οποίο τα χρειάζεται. Μία κλιμακούμενη λύση αποτελεί μία απλή μέθοδο για την διανομή των ενημερωμένων αρχείων υπογραφών σε όλα τα συστήματα που τα χρειάζονται. Επίσης, μία καλή λύση για μεγάλα περιβάλλοντα θα πρέπει να περιλαμβάνει κάποια προηγμένη λειτουργία προειδοποίησης (συναγερμού) έτσι ώστε ο επόπτης του δικτύου να μπορεί να ειδοποιείται για όλα τα περιστατικά ιών που εντοπίζονται σε οποιονδήποτε σταθμό εργασίας του δικτύου.

Ευριστικοί σαρωτές

Τα προγράμματα ανίχνευσης ιών που λειτουργούν σαν "ευριστικοί σαρωτές" (heuristic scanners) εκτελούν μία στατιστική ανάλυση για να εξακριβώσουν πόσο πιθανό είναι ένα αρχείο να περιέχει κώδικα ο οποίος υποδεικνύει την παρουσία ενός ιού. Ένα πρόγραμμα το οποίο λειτουργεί σαν ευριστικός σαρωτής δεν συγκρίνει τον κώδικα έναντι ενός αρχείου υπογραφών, όπως κάνει ένα απλό πρόγραμμα ανίχνευσης ιών αντίθετα, χρησιμοποιεί μία κλίμακα βαθμολόγησης για να καθορίσει πόσο πιθανό είναι ο κώδικας του εξεταζόμενου προγράμματος να ανήκει σε ιό. Εάν ο κώδικας του εξεταζόμενου προγράμματος πάρει αρκετούς βαθμούς ο ευριστικός σαρωτής ειδοποιεί τον χρήστη ότι

έχει ανιχνεύσει έναν ιό. Τα περισσότερα σημερινά εργαλεία ανίχνευσης ιών περιλαμβάνουν μία λειτουργία ευριστικής σάρωσης. Ένα από τα μεγαλύτερα πλεονεκτήματα των ευριστικών σαρωτών είναι ότι δεν χρειάζονται ενημέρωση. Επειδή αξιολογούν τα αρχεία με βάση ένα σύστημα βαθμολόγησης, δεν απαιτούνται αρχεία υπογραφών για σκοπούς σύγκρισης. Συνεπώς, ένας ευριστικός σαρωτής έχει πολλές πιθανότητες να ανιχνεύσει έναν πρωτοεμφανιζόμενο ιό. Αυτό μπορεί να είναι εξαιρετικά χρήσιμο εάν για οποιοδήποτε λόγο δεν μπορείτε να ενημερώνετε τακτικά τα αρχεία υπογραφών.

Η μεγαλύτερη αδυναμία των ευριστικών σαρωτών είναι η τάση τους να αναφέρουν ψεύτικους συναγερμούς. Όπως αναφέραμε παραπάνω, ο κώδικας ενός ιού δεν διαφέρει και τόσο πολύ από τον κώδικα ενός κανονικού προγράμματος. Η διαφοροποίηση μεταξύ των δύο μπορεί να είναι εξαιρετικά δύσκολη. Σαν επόπτες συστημάτων μπορεί να βρεθείτε στην άχαρη θέση να κυνηγάτε την ουρά σας εάν χρησιμοποιείτε έναν κακοφτιαγμένο ευριστικό σαρωτή ο οποίος έχει την τάση να αναφέρει συχνά ανύπαρκτους ιούς.

Εργαλεία ανίχνευσης ιών σε επίπεδο εφαρμογής

Τα εργαλεία ανίχνευσης ιών σε επίπεδο εφαρμογής (application-level virus scanners) είναι μία δημοφιλής κατηγορία εργαλείων προστασίας από ιούς. Αντί να είναι υπεύθυνα για την ασφάλιση ενός συγκεκριμένου συστήματος από ιούς, τα εργαλεία ανίχνευσης ιών σε επίπεδο εφαρμογής είναι υπεύθυνα για την ασφάλιση μιας συγκεκριμένης υπηρεσίας σε όλη την έκταση ενός οργανισμού. Για παράδειγμα, το ηλεκτρονικό ταχυδρομείο αποτελείτο ιδανικό όχημα για την διάδοση ιών μέσω των συνημμένων. Η Trend Micro κατασκεύασε ένα προϊόν με όνομα InterScan VirusWall, το οποίο μπορεί να λειτουργήσει σαν αναμεταδότης της κυκλοφορίας του SMTP (Simple Mail Transfer Protocol) αλλά με μία ιδιομορφία. Αντί να λαμβάνει απλώς τα εισερχόμενα μηνύματα και να τα προωθεί στο κατάλληλο σύστημα ηλεκτρονικού ταχυδρομείου το InterScan VirusWall μπορεί να εκτελεί έναν πλήρη έλεγχο για ιούς σε όλα συνημμένα, πριν αναμεταδώσει τα μηνύματα στα συστήματα ηλεκτρονικού ταχυδρομείου του δικτύου.

Μαζί με τον έλεγχο της κυκλοφορίας του SMTP, το InterScan VirusWall μπορείνα ελέγχει οτιδήποτε διακινείται μέσω των πρωτοκόλλων FTP (File Transfer Protocol) και HTTP (Hypertext Transfer Protocol), αρχεία δεδομένων, καθώς επίσης και πολλές μορφές αρχειοθέτησης/συμπίεσης, όπως η μορφή του PKZIP. Αυτό σας βοηθά να διασφαλίσετε ότι όλα τα αρχεία που λαμβάνετε από το Internet είναι εντελώς απαλλαγμένα από ιούς.

8.6. Προστατευτείτε από ιούς

Η προστασία είναι πάντα η καλύτερη θεραπεία. Μπορείτε να κάνετε πολλά πράγματα για να αποτρέψετε προγράμματα ιών από το να μπουν στα δεδομένα ή στο σύστημα σας.

Πριν να προχωρήσουμε, πρέπει να σημειώσω ότι ο υπολογιστής σας δεν μπορεί να πιάσει ιό ή να προσβληθεί με την απλή κλήση σε μια online υπηρεσία ή σε ένα παροχέα υπηρεσιών Internet. Οι ιοί και τα προγράμματα Δούρειοι ίπποι που έχουν φορτωθεί δεν είναι επικίνδυνα παρά μόνο αν τα *εκτελέσετε*. (Υπάρχει η πιθανότητα ένα απομακρυσμένο σύστημα να στέλνει εντολές στο σύστημα σας μέσω ορισμένων ειδών λογισμικού επικοινωνιών, αλλά οι online υπηρεσίες και οι παροχείς υπηρεσιών δεν έχουν καθοριστεί ώστε να καταστρέφουν τα δεδομένα σας.)

Αφού σας τα είπαμε αυτά, να μερικές σημαντικές συμβουλές για προστασία από ιούς:

Αν δεν υπάρχει πρόγραμμα προστασίας από ιούς στο σύστημα σας, εγκαταστήστε ένα τέτοιο πρόγραμμα και ενημερώνετε το συχνά.

Αν το πρόγραμμα σας προστασίας από ιούς παρέχει αυτόματη, πλήρη προστασία, ενεργοποιήστε την. θα σαρώνει αυτόματα τις φορτώσεις που κάνετε, και θα παρακολουθεί τα αρχεία και τα προγράμματα μέσα στο σύστημα σας.

Να είστε προσεκτικοί με αυτά που φορτώνετε. Αν έχετε απορίες για ένα πρόγραμμα σε μια βάση δεδομένων φόρτωσης, ρωτήστε ένα διαχειριστή συστήματος (δηλαδή το άτομο που λειτουργεί ένα δικτυακό τόπο ή μια online υπηρεσία όπου βρήκατε το πρόγραμμα) αν έχει χρησιμοποιήσει το πρόγραμμα και το βρήκε ασφαλές. Ρωτήστε άλλους χρήστες για το πρόγραμμα. (Γενικά αν ένα πρόγραμμα έχει πολλές φορτώσεις - οι μετρητές φορτώσεων για προγράμματα σε βάσεις δεδομένων είναι ορατοί σε μερικά συστήματα - και δεν έχετε δει παράπονα για αυτό σε κανένα ηλεκτρονικό πίνακα ανακοινώσεων τότε μάλλον μπορείτε να το φορτώσετε με ασφάλεια.)

Αν δεχθείτε ένα email με ένα προσαρτημένο αρχείο από κάποιον που δεν τον ξέρετε, τότε διαγράψτε το αρχείο αμέσως. Αν το αρχείο είναι από κάποιον που ξέρετε, ρωτήστε τον από που το πήρε και αν το έχει εξετάσει για ιούς. (Ίσως να θέλετε να το ελέγξετε και μόνοι σας.)

Αν ένας φίλος ή ένας συνεργάτης σας έδωσε μια δισκέτα με ένα πρόγραμμα, ρωτήστε τον αν ξέρει αν το πρόγραμμα είναι ασφαλές. Το έχει εκτελέσει αυτός; Το έχει ελέγξει για ιούς; Ξέρει από πού πήρε το πρόγραμμα;

Πριν να εκτελέσετε ένα πρόγραμμα, εξετάστε προσεκτικά τα αρχεία στην αρχειοθήκη του προγράμματος και διαβάστε τα τυχόν αρχεία READ,ME ή παρόμοια - οι συγγραφείς προγραμμάτων δημόσιας περιοχής ή δημόσιας χρήσης συνήθως περιλαμβάνουν μια περιγραφή με μεγέθη αρχείων, των αρχείων που περιέχονται μέσα σε μια αρχειοθήκη προγράμματος. Αν δείτε αρχεία που δεν περιλαμβάνονται στην περιγραφή, μην χρησιμοποιήσετε το πρόγραμμα

Ακόμη και αν ένα πρόγραμμα δεν είναι άμεσα ύποπτο, σαρώστε το χρησιμοποιώντας ένα από τα προγράμματα προστασίας από ιούς. (Ορισμένα μπορούν να τεθούν ώστε να σαρώνουν αρχειοθήκες και προγράμματα ενώ τις φορτώνετε.)

Αν είναι δυνατό, εκτελέστε το πρόγραμμα από δισκέτα την πρώτη φορά.

Αν υποπτεύεστε ότι ένα πρόγραμμα μεταφέρει ιούς, μην το χρησιμοποιήσετε Σαρώστε το με ένα ή περισσότερα προγράμματα προστασίας από ιούς.

Όταν αγοράζετε ένα εμπορικό πρόγραμμα, βεβαιωθείτε ότι τη ταινία ασφαλείας δεν είναι σπασμένη - ούτε στο εξωτερικό πακέτο, ούτε στο εσωτερικό που περιέχει τις δισκέτες ή το CD-ROM.

Λογισμικό Προστασίας από Ιούς

Πριν να μπούμε σε λεπτομέρειες για λογισμικό προστασίας από ιούς, θέλουμε να σας δώσουμε μια ιδέα του τι μπορεί να κάνει για σας ένα τέτοιο πρόγραμμα. Παρακάτω αναφέρουμε τις λειτουργίες που μπορούν να προσφέρουν προγράμματα προστασίας από ιούς:

- Αναζήτηση σε ύποπτα προγράμματα ιών για ενσωματωμένα μηνύματα που εμφανίζονται συνήθως από προγράμματα ιών
- Αναζήτηση σε ύποπτα προγράμματα ιών για συναρτήσεις και λειτουργίες που μπορούν να καταστρέψουν τα δεδομένα σας (όπως εντολές διαγραφής ή μορφοποίησης δίσκων)
- Έλεγχο των αρχείων συστήματος για αλλαγές
- Μπλοκάρισμα ύποπτου προγράμματος ιού από έκδοση πιθανώς καταστροφικών εντολών
- Τοποθέτηση προγραμμάτων ιών σε "καραντίνα", όπου δεν μπορούν να εκτελεστούν
- Κατάργηση ιών από το σύστημα σας
- Επιδιόρθωση αρχείων καταστραμμένων από ένα ιό (αυτό περιλαμβάνει νόμιμα προγράμματα, που μερικές φορές λειτουργούν σαν "ξενιστές" για ιούς, όπως και αρχεία δεδομένων)

- Σάρωση φορτωμένων αρχείων και προσαρτήσεων email για ιούς
- Σάρωση καθορισμένων μονάδων δίσκων, φακέλων και/ή αρχείων κατ'απαίτηση, ή με βάση ένα προκαθορισμένο πρόγραμμα
- Ενημέρωση όταν τους το δηλώνετε, ή με βάση ένα προκαθορισμένο πρόγραμμα
- Αυτόματη προστασία του συστήματος σας, όπως το χρησιμοποιείτε, παρακολουθώντας προγράμματα, αρχεία και πόρους συστήματος
- Ανέφερα ήδη δύο προγράμματα προστασίας από ιούς που εστιάζονται στην προστασία του συστήματος σας από απειλές από το Internet. Τώρα, ας εξετάσουμε τα πιο αξιόλογα γενικά προγράμματα προστασίας από ιούς.

8.7. Μία στρατηγική για την προστασία από ιούς

Στο σημείο αυτό γνωρίζετε πολύ περισσότερα πράγματα για τον τρόπο λειτουργίας των ιών, καθώς και για τα εργαλεία που είναι διαθέσιμα για την αποτροπή της μόλυνσης των αρχείων σας από ιούς. Στη συνέχεια θα αναφέρουμε ορισμένες μεθόδους με τις οποίες μπορείτε να ασφαλίσετε το δίκτυο σας έναντι των ιών.

Το σχηματικό διάγραμμα της Εικόνας 8.1 παρουσιάζει ένα περιβάλλον δικτύου στο οποίο χρησιμοποιούνται πολλά ανομοιογενή συστήματα - servers και σταθμοί εργασίας με διαφορετικά λειτουργικά συστήματα. Ας υποθέσουμε ότι έχετε προσληφθεί σαν σύμβουλοι στον οργανισμό στον οποίο είναι εγκατεστημένο αυτό το δίκτυο και σας έχει ανατεθεί το έργο της προστασίας του από ιούς, Δούρειους Ίππους και worms. Σας ζητήθηκε επίσης να φέρετε σε πέρας αυτή την εργασία με την ελάχιστη δυνατή επίδραση στην απόδοση του δικτύου. Αφιερώστε λίγο χρόνο για να μελετήσετε το σχηματικό διάγραμμα και σκεφτείτε ποιες συστάσεις θα κάνατε στους ιθύνοντες αυτού του οργανισμού.

Προστασία των σταθμών εργασίας

Αν και οι σταθμοί εργασίας του δικτύου χρησιμοποιούν διάφορα λειτουργικά συστήματα, η πλατφόρμα τους είναι ίδια (PCs). Συνεπώς, όλοι οι σταθμοί εργασίας του δικτύου είναι ευάλωτοι περίπου στους ίδιους τύπους ιών. Καλό θα είναι να προτυποποιήσετε όσο το δυνατόν περισσότερο τις προτάσεις σας για τους σταθμούς του δικτύου, ακόμη κι αν χρησιμοποιούνται πολλαπλά λειτουργικά συστήματα.

Ενεργοποίηση της προστασίας του τομέα εκκίνησης μέσω BIOS

Μία από τις πιο αποτελεσματικές σε σχέση με το κόστος υποδείξεις που μπορείτε να κάνετε στον οργανισμό, είναι η ενεργοποίηση της προστασίας του τομέα εκκίνησης (boot sector) μέσω του BIOS του εκάστοτε συστήματος. Αυτός είναι ένας γρήγορος αλλά αποτελεσματικός τρόπος για να διασφαλίσετε ότι θα παραμένει ασφαλής ο τομέας εκκίνησης όλων των συστημάτων του δικτύου. Συνδυάστε αυτή την υπόδειξη με την κατάλληλη εκπαίδευση των τελικών χρηστών σχετικά με το τι σημαίνουν τα προειδοποιητικά μηνύματα για τον τομέα εκκίνησης και πώς θα πρέπει να ανταποκρίνονται σ' αυτά οι χρήστες. Οι ψεύτικοι συναγερμοί δεν θα πρέπει να αποτελέσουν πρόβλημα παρά μόνο εάν κάποιος χρήστης προσπαθήσει να αναβαθμίσει το λειτουργικό του σύστημα.

Έλεγχος ιών κατ'απαίτηση

Κάθε PC θα πρέπει να χρησιμοποιεί ένα πρόγραμμα ανίχνευσης ιών κατ' απαίτηση, διαμορφωμένο ώστε να εκτελεί πλήρη έλεγχο όλων των τοπικών μονάδων δίσκων σε τακτά χρονικά διαστήματα. Μπορείτε να προγραμματίσετε την εκτέλεση αυτών των ελέγχων κατά την διάρκεια της νύχτας, εάν συνηθίζετε να αφήνετε αναμμένους τους σταθμούς εργασίας του δικτύου σας. Εάν ο νυχτερινός έλεγχος για ιούς δεν είναι βιώσιμη επιλογή, μπορείτε να τον εκτελείτε κατά την διάρκεια μιας διαφορετικής περιόδου εργασιακής αδράνειας (π.χ. κατά την διάρκεια του μεσημεριανού διαλείμματος), ή σε εβδομαδιαία βάση σαν μέρος του script σύνδεσης στον server.

Το πρόγραμμα ανίχνευσης ιών κατ' απαίτηση πρέπει να ελέγχει όλα τα τοπικά αρχεία για να διασφαλίζει ότι δεν κατάφερε να παρεισφρήσει κανένας ιός. Ένα σωστό πρόγραμμα ανίχνευσης ιών κατ' απαίτηση θα πρέπει επίσης να περιλαμβάνει δυνατότητα ευριστικής σάρωσης. Τέλος, θα πρέπει να διαθέτει κάποιο τρόπο για να αναφέρει τα αποτελέσματα των ελέγχων του σε μία κεντρική θέση, από την οποία θα μπορεί να τα εξετάσει ο επόπτης του συστήματος.

Μόνιμα στη μνήμη προγράμματα ανίχνευσης ιών

Κάθε υπολογιστής του δικτύου θα πρέπει επίσης να χρησιμοποιεί ένα μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών το οποίο θα φορτώνεται κατά την εκκίνηση του συστήματος για να εντοπίζει οποιουσδήποτε ιούς πριν μπορέσουν να αποθηκευτούν στο τοπικό σύστημα αρχείων ή να φορτωθούν στην μνήμη. Για να ελαχιστοποιήσετε την μείωση της απόδοσης θα μπορούσατε να επιλέξετε ποια αρχεία θα ελέγχονται από το μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών.

Δεδομένου ότι σκοπεύετε να εκτελείτε επίσης έναν έλεγχο για ιούς κατ' απαίτηση σε τακτά χρονικά διαστήματα, μπορείτε να μην είστε ιδιαίτερα σχολαστικοί όσον αφορά στην επιλογή των αρχείων που θα ελέγχονται από το μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών. Ελέγχοντας μόνο εκείνα τα αρχεία που μολύνονται συνηθέστερα από ιούς, μπορείτε να μειώσετε την αρνητική επίδραση στην απόδοση του συστήματος. Αν και η προσέγγιση αυτή αποδυναμώνει λίγο την στάση σας στον τομέα της ασφάλειας, το κέρδος στην απόδοση του συστήματος είναι τέτοιο που αξίζει να το διακινδυνέψετε. Ένα μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών θα πρέπει να ελέγχει τα ακόλουθα:

- Μόνο τις αιτήσεις για ανάγνωση αρχείων
- Την ύπαρξη worms
- Εκτελέσιμα αρχεία, όπως για παράδειγμα τα αρχεία με επεκτάσεις COM και EXE
- Έγγραφα τα οποία περιέχουν μακροεντολές, όπως για παράδειγμα τα έγγραφα των Microsoft Word και ExceI

Θα πρέπει να ελέγχετε τις απόπειρες ανάγνωσης αρχείων αλλά όχι τις απόπειρες εγγραφής δεδομένων, επειδή ο έλεγχος των αρχείων που γράφονται στον δίσκο είναι πλεονασμός. Εάν ένα πρόγραμμα ανίχνευσης ιών αποτύχει να εντοπίσει έναν ιό κατά την διάρκεια που διαβάζεται το αρχείο στην μνήμη, είναι μάλλον απίθανο να καταφέρει να εντοπίσει τον ιό όταν γράφεται το αρχείο στον δίσκο. Ένα τέτοιο πρόγραμμα θα πρέπει επίσης να εκτελεί έναν έλεγχο για worms, επειδή πολλά από αυτά δεν αποθηκεύουν καθόλου πληροφορίες στον δίσκο· συνεπώς, μπορεί να περάσουν απαρατήρητα από τα προγράμματα ανίχνευσης ιών κατ' απαίτηση. Τέλος, θα θέλετε να διαμορφώσετε το μόνιμο στην μνήμη πρόγραμμα ανίχνευσης ιών ώστε να ελέγχει τα αρχεία με τις μεγαλύτερες πιθανότητες μόλυνσης. Σ' αυτά περιλαμβάνονται τα εκτελέσιμα αρχεία, καθώς επίσης και τα αρχεία που μπορούν να αποθηκεύουν -μακροεντολές.

Επιπλέον επιλογές

Δεν θα αναφερθούμε καθόλου στην τροποποίηση των ιδιοτήτων των αρχείων ή στην χρήση ελεγκτικών αθροισμάτων (checksums), επειδή όπως είδατε παραπάνω αυτές οι μέθοδοι δεν είναι αποτελεσματικές για πολλές κατηγορίες ιών. Επίσης δεν θα ασχοληθούμε με άλλες μορφές παρακολούθησης διεργασιών (εκτός της προειδοποίησης για την μόλυνση του τομέα εκκίνησης) για τον ίδιο ακριβώς λόγο. Οι υποδείξεις μας είναι ειδικά σχεδιασμένες ώστε να παρέχουν το υψηλότερο επίπεδο προστασίας με τον λιγότερο δυνατό φόρτο.

Ωστόσο, μία επιπλέον δυνατότητα είναι η χρήση των δικαιωμάτων αρχείων στους σταθμούς εργασίας του δικτύου για να εμποδίσετε τους χρήστες να έχουν πρόσβαση για εγγραφή σε οποιαδήποτε εκτελέσιμα αρχεία. Αν και αυτό μειώνει τις πιθανότητες μόλυνσης από ιούς στα συγκεκριμένα συστήματα, αποκλίνει από την τυπική διαμόρφωση που χρησιμοποιείται στους υπόλοιπους υπολογιστές του δικτύου. Σημαίνει επίσης ότι οι συγκεκριμένοι χρήστες δεν θα μπορούν να ενημερώσουν τα συστήματα που χρησιμοποιούν. Αυτό μπορεί να είναι αποδεκτό στο δικό σας δίκτυο, ή μπορεί και όχι. Τα

πάντα εξαρτώνται από την υποδομή σας στον τομέα της υποστήριξης και την πολιτική ασφάλειας που έχει υιοθετήσει ο οργανισμός σας.

Η παραπάνω τακτική δεν διευθετεί το πρόβλημα με τους ιούς μακροεντολών, οι οποίοι είναι μία από τις συνηθέστερες μορφές ιών σήμερα. Αυτοί οι ιοί κρύβονται μέσα σε αρχεία εγγράφων. Προφανώς, οι χρήστες πρέπει να έχουν δικαίωμα εγγραφής για να μπορούν να αποθηκεύουν τα έγγραφα τους. Με δύο λόγια, η επιλογή αυτή μπορεί να προκαλέσει περισσότερα προβλήματα από αυτά που λύνει.

Προστασία των λειτουργικών συστημάτων των Servers

Επειδή οι βασιζόμενοι στα Windows NT, UNIX και OS X servers παρέχουν κοινόχρηστους πόρους στο δίκτυο, απαιτούν ελαφρώς διαφορετική μέθοδο προστασίας από αυτή που χρειάζονται οι σταθμοί εργασίας του δικτύου. Η προστασία αυτών των συστημάτων από ιούς είναι πολύ πιο σημαντική, επειδή οι servers μπορούν να χρησιμοποιούνται σαν όχημα για την διάδοση των ιών στους σταθμούς εργασίας του δικτύου.

Ανίχνευση ιών κατ'απαίτηση

Όπως ισχύει και με τους σταθμούς εργασίας του δικτύου, μπορείτε να διαμορφώσετε ένα πρόγραμμα ανίχνευσης ιών κατ' απαίτηση ώστε να εκτελεί έναν πλήρη έλεγχο όλων των αρχείων κάθε νύχτα. Τα περισσότερα προϊόντα ανίχνευσης ιών που τρέχουν σε server περιλαμβάνουν ένα ειδικό εργαλείο χρονικού προγραμματισμού γι' αυτό τον σκοπό. Εάν λαμβάνετε backup του δικτύου κάθε βράδυ, διαμορφώστε το πρόγραμμα ανίχνευσης ιών έτσι ώστε να ελέγχει το σύστημα αρχείων πριν από την εκτέλεση του backup. Η προσέγγιση αυτή διασφαλίζει ότι όλα τα αρχεία που αρχειοθετούνται στο backup είναι απαλλαγμένα από ιούς.

Μόνιμα στην μνήμη προγράμματα ανίχνευσης ιών

Τα μόνιμα στην μνήμη προγράμματα ανίχνευσης ιών ελέγχουν την μνήμη του server και τα αρχεία που είναι αποθηκευμένα στο τοπικό σύστημα αρχείων. Ένα τέτοιο πρόγραμμα θα πρέπει να ελέγχει τα ακόλουθα:

- Την τοπική μνήμη για worms και Δούρειους Ίππους
- Τα εισερχόμενα από το δίκτυο εκτελέσιμα αρχεία
- Τα εισερχόμενα από το δίκτυο έγγραφα με μακροεντολές

Όπως ισχύει και με τους σταθμούς εργασίας του δικτύου, η "υποβάθμιση" του ελέγχου αρχείων σ' αυτό το ελάχιστο επίπεδο γίνεται για χάρη της καλύτερης απόδοσης Ακόμη κι αν καταφέρει να παρεισφρήσει κάποιος ιός, μπορεί να εντοπιστεί από το πρόγραμμα ανίχνευσης ιών που τρέχετε κάθε βράδυ.

Δικαιώματα αρχείων

Όπως αναφέραμε παραπάνω σ' αυτό το κεφάλαιο, η χρήση των κατάλληλων δικαιωμάτων σε επίπεδο μεμονωμένων χρηστών σας επιτρέπει να διασφαλίσετε ότι τα εκτελέσιμα αρχεία σας δεν πρόκειται να μολυνθούν από ιούς. Τα πλεονεκτήματα αυτής της προσέγγισης εξαρτώνται σε μεγάλο βαθμό από τον τρόπο αποθήκευσης των εφαρμογών στο δίκτυο σας. Εάν η στρατηγική σας είναι να αποθηκεύετε όλες τις εφαρμογές τοπικά σε κάθε σταθμό εργασίας, δεν θα υπάρχουν εκτελέσιμα αρχεία στον server για να τα προστατέψετε καθορίζοντας πρόσβαση μόνο για ανάγνωση. Εν αντιθέσει, εάν όλες οι εφαρμογές είναι εγκατεστημένες σε έναν-δύο servers και εκκινούν από αυτούς, μπορείτε να μειώσετε τις πιθανότητες μόλυνσης από ιούς ορίζοντας τα δικαιώματα των χρηστών ώστε να έχουν το ελάχιστο απαιτούμενο επίπεδο πρόσβασης.

Επιπλέον επιλογές

Δεν προτείναμε την παρακολούθηση διεργασιών ή τον έλεγχο CRC επειδή αυτές οι μέθοδοι είναι λιγότερο αποτελεσματικές από την χρήση προγραμμάτων ανίχνευσης ιών. Να θυμάστε ότι ο στόχος σας είναι να παρέχετε τον μέγιστο βαθμό προστασίας με την μικρότερη δυνατή επιβάρυνση στην διαχείριση και συντήρηση του δικτύου. Οι υποδείξεις μας προσανατολίζονται σ' αυτό τον στόχο.

Προστασία συστημάτων UNIX

Εδώ λείπει ένα σημαντικό κομμάτι πληροφορίας: σε τι ακριβώς χρησιμοποιείται ένα σύστημα UNIX; Πρόκειται για έναν απλό αναμεταδότη ηλεκτρονικού ταχυδρομείου, ή για έναν πλήρως λειτουργικό server ο οποίος δέχεται και διεκπεραιώνει μία πλήρη γκάμα υπηρεσιών δικτύωσης; Η απάντηση σ' αυτή την ερώτηση θα μπορούσε να επηρεάσει σε μεγάλο βαθμό τις προτάσεις σας. Για τους σκοπούς του παραδείγματος μας ας υποθέσουμε ότι το σύστημα με το UNIX χρησιμοποιείται μόνο από ορισμένους προγραμματιστές για την μεταγλώττιση κώδικα γραμμένου σε C. Οι χρήστες συνδέονται σ' αυτό το σύστημα μέσω telnet και FTP.

Έλεγχος της ακεραιότητας των αρχείων

Σ΄ένα σύστημα UNIX, ένα από τα σημαντικότερα θέματα που πρέπει να σας απασχολήσουν είναι η πιθανότητα κάποιος να επιχειρήσει να φορτώσει έναν Δούρειο Ίππο στο σύστημα, για να υποκλέψει πληροφορίες πιστοποίησης. Αντικαθιστώντας

Τον telnet server του συστήματος σας μ' έναν server δικής του έμπνευσης, ένας εσβολέας θα μπορούσε να υποκλέψει τα διαπιστευτήρια κάθε χρήστη ο οποίος συνδέεται στο σύστημα.

Ο ευκολότερος τρόπος για να εντοπίσετε τέτοιου είδους δραστηριότητα είναι η εκτέλεση τακτικών ελέγχων ακεραιότητας των αρχείων. Σ' αυτούς περιλαμβάνεται και ο έλεγχος CRC, μέσω του οποίου μπορούν να εντοπίζονται οποιεσδήποτε αλλαγές, ακόμη κι αν το αρχείο έχει την ίδια ημερομηνία/ώρα. Θα πρέπει επίσης να ελέγχετε τους telnet και FTP servers, καθώς και οποιαδήποτε άλλη διεργασία δέχεταιεισερχόμενες συνδέσεις. Ο έλεγχος αυτός θα πρέπει να εκτελείται σαν μία αυτοματοποιημένη διεργασία και τα αποτελέσματα του θα πρέπει να εξετάζονται σε ένα διαφορετικό σύστημα. Χρησιμοποιώντας ένα διαφορετικό σύστημα για την ανάλυση και εξέταση μειώνεται σημαντικά η πιθανότητα τροποποίησης των αποτελεσμάτων από κάποιον ο οποίος κατάφερε να παραβιάσει το σύστημα.

Παρακολούθηση διεργασιών

Ένα άλλο πρόβλημα το οποίο θα πρέπει να σας ανησυχεί όταν αντιμετωπίζετε ένα σύστημα UNIX είναι ότι κάποιος μπορεί να διεισδύσει στο σύστημα χρησιμοποιώντας ένα worm. Μία τέτοια επίθεση θα εμφανίζονταν σαν μία νέα διεργασία που εκτελείται στο σύστημα. Όπως ισχύει και με τον έλεγχο ακεραιότητας των αρχείων, μπορείτε να αυτοματοποιήσετε αυτό τον έλεγχο και να αναλύετε τα αποτελέσματα του σε ένα ξεχωριστό σύστημα. Γνωρίζοντας ποιες διεργασίες πρέπει να τρέχουν ανά πάσα στιγμή στο σύστημα, μπορείτε να κάνετε τις απαιτούμενες ενέργειες εάν εμφανιστεί ξαφνικά μία νέα διεργασία.

Δικαιώματα αρχείων

Εξ ορισμού, μόνο ο χρήστης root μπορεί να αντικαθιστά προγράμματα τα οποία τρέχουν σαν server σ' ένα σύστημα UNIX. Ένας εισβολέας θα έπρεπε πρώτα να παραβιάσει τον λογαριασμό του root ή να αποκτήσει προνόμια επιπέδου root πριν μπορέσει να αντικαταστήσει οποιοδήποτε από τα προγράμματα που τρέχουν στον server. Μειώνοντας τα δικαιώματα πρόσβασης των χρηστών στα αρχεία αυτών των προγραμμάτων μπορείτε να μειώσετε τις πιθανότητες μόλυνσης από ιούς. Μην παραχωρείτε δικαίωμα εγγραφής γι' αυτά τα αρχεία στους λογαριασμούς των απλών χρηστών.

Επιπλέον επιλογές

Τι γίνεται με τα προγράμματα ανίχνευσης ιών; Στο UNIX, οι ιοί είναι μάλλον σπάνιοι. Με δεδομένη την χρήση του συγκεκριμένου συστήματος όπως την περιγράψαμε

παραπάνω, είναι μάλλον απίθανο να αντιμετωπίσετε μόλυνση από ιό. Η μεγαλύτερη ανησυχία σας θα πρέπει να είναι οι Δούρειοι Ίπποι και τα worms.

8.8. Ανασκόπηση

Σ' αυτό το κεφάλαιο εξετάσαμε τις διαφορές μεταξύ των ιών, των Δουρείων Ίππων και των worms, και πώς επηρεάζει κάθε μία από αυτές τις κατηγορίες προγραμμάτων ένα μολυσμένο σύστημα. Μάθατε ποια προληπτικά μέτρα είναι διαθέσιμα, καθώς και την αποτελεσματικότητα τους. Χρησιμοποιώντας σαν παράδειγμα ένα περιβάλλον δικτύου με ανομοιογενή συστήματα, εξετάσαμε επίσης ποια είναι η καλύτερη προσέγγιση για την προστασία του δικτύου από ιούς.

Στο επόμενο κεφάλαιο θα ασχοληθούμε με το θέμα των εφεδρικών αντιγράφων (backups) και της ανάκαμψης του δικτύου σας από καταστροφές. Αυτή είναι η τελευταία γραμμή άμυνας που έχετε όταν συμβαίνει οτιδήποτε καταστροφικό. Από την άποψη της ασφάλειας είναι πάντα συνετό να προετοιμάζεστε για το χειρότερο, ακόμη κι αν αυτό δεν συμβεί ποτέ.

Κεφάλαιο 9

Συστήματα Ανίχνευσης Επιθέσεων Intrusion Detection Systems - IDS

Τα τελευταία χρόνια έχει δοθεί ιδιαίτερη σημασία στο πεδίο της ανίχνευσης εισβολών σε δίκτυα και την ανάπτυξη συστημάτων ανίχνευσης εισβολών. Αυτά τα συστήματα προσπαθούν με διαφορετικές μεθόδους να ανιχνεύσουν την όποια παράνομη δραστηριότητα, χωρίς όμως να το πετυχαίνουν πάντοτε. Σχεδόν όλα τα Συστήματα Ανίχνευσης Επιθέσεων μέχρι σήμερα χρησιμοποιούν είτε κεντρική ανάλυση δεδομένων, δηλαδή ένα σύστημα συλλέγει πληροφορίες για το δίκτυο συνεχώς και προσπαθεί να αποφανθεί για το αν το δίκτυο είναι υπό επίθεση ή όχι, είτε host-based ανάλυση, δηλαδή στον υπολογιστή του δικτύου συλλέγονται και επεξεργάζονται πληροφορίες για να αποφασίσει το σύστημα αν βρίσκεται υπό επίθεση.

9.1. Επιθυμητά χαρακτηριστικά ενός συστήματος ανίχνευσης επιθέσεων (IDS)

Τα χαρακτηριστικά του ιδανικού Συστήματος Ανίχνευσης Επιθέσεων παρατίθενται παρακάτω:

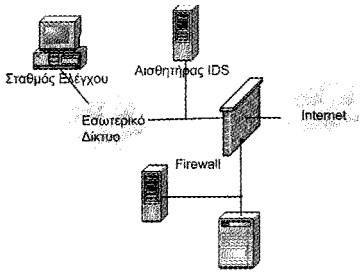
1. Πρέπει να τρέχει συνεχώς με ελάχιστη ανθρώπινη παρακολούθηση
2. Πρέπει να μπορεί να αντιμετωπίσει σφάλματα που μπορεί να συμβούν
3. Το σύστημα πρέπει να μπορεί να επανέλθει από αποτυχίες του συστήματος, είτε προέρχονται από λάθος είτε σκόπιμες .
4. Μετά από μια τέτοια αποτυχία πρέπει να μπορεί να επανέλθει ακριβώς στην προηγούμενη κατάστασή του, σαν να μην είχε συμβεί τίποτε.
5. Πρέπει να μην μπορεί να «καταστραφεί»
6. Πρέπει να είναι σχεδόν αδύνατο να τροποποιήσει ή να αχρηστεύσει κάποιος το Σύστημα Ανίχνευσης Επιθέσεων.
7. Πρέπει να υπάρχει τρόπος το Σύστημα να ελέγχει τον εαυτό του και να μπορεί να ανιχνεύσει αν είναι αυτό που δέχτηκε επίθεση.
8. Πρέπει να επηρεάζει ελάχιστα την απόδοση των υπολογιστών στα οποία τρέχει, ώστε να μην παρεμποδίζει την κανονική τους λειτουργία

9. Πρέπει να είναι διαμορφώσιμο ώστε να προσαρμόζεται με ακρίβεια στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
10. Πρέπει να είναι ανεξάρτητο λειτουργικού συστήματος, δηλαδή πρέπει να υπάρχει τρόπος να λειτουργήσει για ανίχνευση επίθεσης σε οποιοδήποτε λειτουργικό σύοιημα
11. Πρέπει να μπορεί να προσαρμοστεί σε αλλαγές στο δίκτυο και στο υπολογιστικό σύστημα που παρακολουθεί.
12. Πρέπει να μπορεί να ανιχνεύσει επιθέσεις

13. δεν πρέπει να χαρακτηρίζει σαν επίθεση περιπτώσεις καλής λειτουργίας του δικτύου (**false positive**)
14. δεν πρέπει να αποτυγχάνει στην ανίχνευση οποιασδήποτε επίθεσης. Πρέπει να είναι πολύ δύσκολο για τον εισβολέα να «καμουφλαριστεί» έτσι ώστε να μην γίνει αντιληπτός σαν εισβολέας από το σύστημα
15. πρέπει να ανιχνεύει και να αναφέρει τις επιθέσεις όσο πιο γρήγορα γίνεται.
16. πρέπει να είναι αρκετά γενικό ώστε να ανιχνεύει πολλούς διαφορετικούς τύπους επιθέσεων, ακόμα και άγνωστους τύπους επιθέσεων.

Παρακάτω αναλύονται τα χαρακτηριστικά των network-based και host-based Συστημάτων Ανίχνευσης Επιθέσεων που έχουν προταθεί και υλοποιηθεί μέχρι σήμερα.

9.2. Ιδιαίτερα χαρακτηριστικά συστημάτων ανίχνευσης επιθέσεων (IDS) ανάλογα με τον τρόπο ανίχνευσης



Ένα σύστημα ανίχνευσης επιθέσεων (IDS) εξετάζει την δραστηριότητα σε ένα σύστημα ή δίκτυο με στόχο να βρει πιθανές εισβολές ή επιθέσεις. Τα IDS βασίζονται σε δύο τεχνολογίες, στις Network-Based και στις Host-Based. Τα Network Based συστήματα είναι τα πιο διαδεδομένα και εξετάζουν τη διερχόμενη δικτυακή κίνηση (traffic) για ίχνη εισβολής.

Σχημα 9-1 διαταξη δικτυακού IDS

Το Σχήμα 9-1 δείχνει τη διάταξη ενός παραδοσιακού Δικτυακού (Network Based) IDS με δύο αισθητήρες σε ξεχωριστά δικτυακά τμήματα που επικοινωνούν με ένα σταθμό παρακολούθησης δεδομένων στο εσωτερικό δίκτυο. Τα Κομβικά (Host-Based) συστήματα IDS παρακολουθούν τη δραστηριότητα χρηστών και εφαρμογών στο τοπικό μηχάνημα για ίχνη εισβολής. Γενικά υπάρχουν τρία είδη μηχανισμών ανάλυσης που χρησιμοποιεί:

- Ανάλυση με βάση γεγονότα ή υπογραφές (events ή signatures)
- Στατιστική ανάλυση
- Προσαρμόσιμα συστήματα

Τα συστήματα που βασίζονται σε γεγονότα ή υπογραφές λειτουργούν παρόμοια με τα antivirus προγράμματα, που είναι αρκετά διαδεδομένα μεταξύ των χρηστών.

Ο κατασκευαστής παράγει μία λίστα με «υπογραφές» δηλαδή χαρακτηριστικά τμήματα που θεωρεί ότι είναι ύποπτα ή ενδεικτικά μιας επίθεσης. Το IDS ερευνά και αναλύει το περιβάλλον ελέγχοντας για γνωστές υπογραφές. Το IDS μπορεί τότε να αντιδράσει εκτελώντας μια προκαθορισμένη ενέργεια, όπως να στείλει alert ή να συνεχίσει επιπλέον έλεγχο. Αυτό είναι και το πιο διαδεδομένο είδος ενός συστήματος ανίχνευσης επιθέσεων.

Τα συστήματα που βασίζονται στην στατιστική ανάλυση κατασκευάζουν στατιστικά πρότυπα του περιβάλλοντος, όπως τη μέση διάρκεια μιας συνόδου telnet και στη συνέχεια κοιτάζει για αποκλίσεις από το «σύνηθες». Μετά από περίπου 10 χρόνια έρευνας, αρχίζουν και γίνονται οι πρώτες υλοποιήσεις σε εμπορικά προϊόντα.

Τα προσαρμόσιμα συστήματα ξεκινούν με γενικούς κανόνες για το περιβάλλον και στη συνέχεια μαθαίνουν ή προσαρμόζονται σε τοπικές καταστάσεις που διαφορετικά θα τις θεωρούσαν ασυνήθιστες. Μετά από την αρχική περίοδο μάθησης, το σύστημα καταλαβαίνει την αλληλεπίδραση ανθρώπων-περιβάλλοντος και προειδοποιεί τους υπεύθυνους για ασυνήθιστες δραστηριότητες. Η έρευνα σε αυτόν τον τομέα συνεχίζεται διαρκώς.

Δικτυακά συστήματα ανίχνευσης επιθέσεων (Network based IDS)

Το δικτυακό IDS συνήθως αποτελείται από δύο μέρη: τους αισθητήρες και τον σταθμό διαχείρισης / ανάλυσης. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον administrator του συστήματος.

Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα, δηλαδή λαμβάνουν όλη την δικτυακή κίνηση, όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και το διερχόμενο από αυτούς traffic με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στον σταθμό διαχείρισης/ανάλυσης. Ο σταθμός διαχείρισης/ανάλυσης μπορεί να δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες ή να πραγματοποιήσει επιπλέον ανάλυση.

Πλεονεκτήματα

1. Τα δικτυακά συστήματα ανίχνευσης επιθέσεων μπορούν να ανιχνεύσουν κάποιες από τις επιθέσεις που χρησιμοποιούν το δίκτυο. Είναι επαρκή για την ανίχνευση πρόσβασης διαδικασίες είναι πολύ μικρότερος με ένα network σύστημα, παρά με ένα host based σύστημα.
2. Τα network based συσιήματα έχουν την τάση να είναι καλύτερα αυτόδιατηρούμενα από ότι τα host based.Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάστασή τους είναι απλή.
3. Ένα Network Based IDS δεν απαιτεί μετατροπές στους server μιας επιχείρησης ή στους hosts για να εγκατασταθεί.
4. Το IDS δεν αποτελεί κρίσιμο παράγοντα για την λειτουργικότητα του δικτύου, γιατί δεν λειτουργεί ως router ή κάποια άλλη κρίσιμη συσκευή. Άρα, τυχόν αποτυχία στο σύστημα του IDS δε θα έχει σημαντική επίδραση στην επιχείρηση. Ένα επιπλέον όφελος είναι ότι πιθανότατα θα συναντήσουμε λιγότερη αντίδραση από ανθρώπους εντός του εργασιακού περιβάλλοντος.

Μειονεκτήματα

1. Ένα network based IDS απλά εξετάζει τη δικτυακή σύνδεση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μία επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου.

2. Τα network based IDS συνήθως χρησιμοποιούν ανάλυση signatures για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι, ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για πιο πολύπλοκα είδη επιθέσεων.
3. Ένα σύστημα ανίχνευσης επιθέσεων μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Κάποιες φορές αυτό σημαίνει ότι οποιοδήποτε εξεταζόμενο πακέτο παράγει μια μεγάλη ποσότητα κίνησης δεδομένων.
4. Ένα network based IDS πιθανόν να αντιμετωπίσει δυσκολίες στο χειρισμό επιθέσεων στη διάρκεια κρυπτογραφημένων συνόδων. Ευτυχώς, είναι πολύ λίγες οι επιθέσεις που πραγματοποιούνται εντός μιας κρυπτογραφημένης συνόδου, εκτός από τις επιθέσεις εναντίον ευπαθών Web servers. Αυτό το γεγονός θα γίνει περισσότερο εμφανές με την μετάβαση στο IPv6.

Συστήματα ανίχνευσης επιθέσεων εγκατεστημένο σε υπολογισρές (Host based IDS)

Τα συστήματα που είναι host based ψάχνουν για ίχνη εισβολής στο τοπικό σύστημα του host. Χρησιμοποιούν συχνά το μηχανισμό ελέγχου και καταγραφής του host σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό host, όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιομάτων ή μετατροπές σε δικαιώματα του συστήματος.

Πλεονεκτήματα

1. Ένα host based IDS μπορεί να αποτελέσει πολύ δυνατό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, είναι σε θέση μερικές φορές να πει τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι προσπάθησε να εκτελέσει μια επικίνδυνη εντολή. Άρα τα host based IDS συνήθως παρέχουν πολύ πιο λεπτομερείς και σχετικές πληροφορίες από ότι τα network based IDS.
2. Μπορούν να χρησιμοποιηθούν σε περιβάλλοντα όπου δεν χρειάζεται πλήρης ανίχνευση εισβολών ή όταν δεν υπάρχει διαθέσιμη χωρητικότητα δικτύου για επικοινωνία αισθητήρα - σταθμού ανάλυσης.
3. Τέλος, σε ένα host based σύστημα είναι ευκολότερο να σχηματιστεί μία ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη.

Μειονεκτήματα

1. Τα host based συστήματα απαιτούν εγκατάσταση στην συγκεκριμένη συσκευή που θέλουμε να προστατεύσουμε. Αν, για παράδειγμα έχουμε ένα server που πρέπει να τον προστατέψουμε θα πρέπει να εγκατασταθεί το IDS στον server αυτόν. Όπως αναφέρθηκε και παραπάνω, αυτό μπορεί να προκαλέσει προβλήματα χωρητικότητας.
2. Ένα άλλο πρόβλημα είναι ότι έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής (logging system) και ελέγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, θα πρέπει να γίνει αλλαγή στο configuration. Αυτό αποτελεί τεράστιο πρόβλημα αλλαγής στη διαχείριση του server.
3. Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την οικονομική δυνοτότητα να προστατέψουν ολόκληρα δικτυακά τμήματα με τη χρήση network based IDS, αναγκάζονται να επιλέξουν ποια συστήματα θα

προστατέψουν και ποια όχι και αυτό το γεγονός αφήνει μεγάλα κενά στην κάλυψη της ανίχνευσης εισβολών στο δίκτυο.

4. Τέλος, ο χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των host που προστοτεύονται. Για παράδειγμα αν ένας άνθρωπος χρειάζεται t χρόνο για να ερευνήσει ένα περιστατικό σε ένα σύστημα, θα χρειαστεί 2t για δύο συστήματα, 3t για τρία κοκ.

9.3. Τεχνικές ανίχνευσης επιθέσεων

Μία άλλη κατηγοριοποίηση των IDS γίνεται αντίστοιχα με την τεχνική που ανιχνεύονται οι εισβολές.

Υπάρχουν 6 κατηγορίες εισβολών:

1) Προσπάθεια εισόδου στο σύστημα, που ανιχνεύεται από τυπικά προφίλ συμπεριφοράς ή παραβιάσεις περιορισμών ασφαλείας.
2) Κρυφή επίθεση, που ανιχνεύεται επίσης από τα τυπικά προφίλ συμπεριφοράς.
3) Διείσδυση στο σύστημα ελέγχου ασφαλείας, οι οποία ανιχνεύεται με συνεχή παρακολούθηση συγκεκριμένων προτύπων δραστηριότητας.
4) Διαρροή, που γίνεται αντιληπτή με μια τυπική χρήση των πόρων του συστήματος.
5) Denial of service (άρνηση εκτέλεσης εφαρμογής), που επίσης γίνεται αντιληπτή από χρήση πόρων του συστήματος.
6) Κακόβουλη χρήση, που ανιχνεύεται μέσω τυπικής συμπεριφοράς προφίλ, παραβιάσεων κανόνων ασφαλείας, ή με χρήση ειδικών προνομίων.

Οι τεχνικές που χρησιμοποιούνται στην ανίχνευση εισβολών χωρίζονται σε δύο είδη:

Ανίχνευση διαταραχών (Anomaly Detection)

Οι τεχνικές ανίχνευσης διαταραχών καταλήγουν στο συμπέρασμα ότι όλες οι επιθετικές δραστηριότητες είναι αναγκαστικά ανωμαλίες. Αυτό σημαίνει ότι αν μπορούσαμε να καθιερώσουμε ένα "σύνηθες προφίλ δραστηριότητας" για ένα σύστημα, θα ήμασταν σε θέση, θεωρητικά, να σημαδέψουμε όλες τις καταστάσεις του συστήματος που διαφέρουν από το καθιερωμένο προφίλ. Αυτό θα γίνει με βάση ένα, στατιστικά, σημαντικό νούμερο προσπαθειών εισβολής. Παρόλα αυτά αν συλλογιστούμε ότι το σύνολο των επιθετικών δραστηριοτήτων αλλάζει την κατάσταση του σύνολο των δραστηριοτήτων διαταραχής παρά να το αφήνει στην αρχική μορφή, βγάζουμε κάποιες ενδιαφέρουσες εκδοχές:

- Ασυνήθεις δραστηριότητες, που δεν έχουν χαρακτήρα εισβολής χαρακτηρίζονται ως επιθετικές.
- Επιθετικές δραστηριότητες που δεν είναι ασυνήθεις, καταλήγουν σε false negatives (γεγονότα δεν χαρακτηρίζονται επιθέσεις, ενώ στην πραγματικότητα είναι).

Αυτό είναι ένα ιδιαίτερα επικίνδυνο πρόβλημα και αποτελεί περισσότερο σοβαρό από το πρόβλημα των ***false positive*** (γεγονότα που χαρακτηρίζονται ως επιθέσεις, ενώ στην πραγματικότητα δεν είναι).

Το κυριότερο στην ανίχνευση διαταραχών σε συστήματα ανίχνευσης επιθέσεων, είναι να γίνονται οι επιλογές στα επίπεδα των ορίων έτσι, ώστε κανένα από τα δύο παραπάνω προβλήματα να μη μεγιστοποιείται. Σημαντική είναι, επίσης και η επιλογή των χαρακτηριστικών στην παρακολούθηση δεδομένων. Τα συστήματα ανίχνευσης

διαταραχών είναι υπολογιστικά ακριβά, λόγω του κόστους του ελέγχου και της συνεχούς ανανέωσης (updating) των μετρικών του προφίλ ενός συστήματος.

Ανίχνευση κακής συμπεριφοράς (Misuse Detection)

Η ιδέα πίσω από την misuse detection είναι ότι υπάρχουν τρόποι αναπαράστασης επιθέσεων με τη μορφή ενός προτύπου ή signature, ώστε ακόμα και παραλλαγές της επίθεσης να μπορούν να ανιχνευτούν. Άρα τα συστήματα αυτά μοιάζουν πολύ με τα antivirus προγράμματα, μπορούν να ανιχνεύσουν πολλά ή όλα τα γνωστά πρότυπα εισβολής, αλλά δεν είναι αποτελεσματικά σε άγνωστες τεχνικές επίθεσης.

9.4. Συστήματα ανίχνευσης διαταραχών (Anomaly Detection)

Μερικές από τις σημαντικές προσεγγίσεις στα συστήματα ανίχνευσης διαταραχών αναλύονται παρακάτω:

Στατιστική προσέγγιση

Στην μέθοδο αυτή, αρχικά δημιουργούνται τα πρότυπα συμπεριφοράς για τα υπό εξέταση αντικείμενα. Καθώς το σύστημα συνεχώς τρέχει, ο ανιχνευτής διαταραχών συνεχώς παράγει την διακύμανση του παρόντος προφίλ σε σχέση με την αρχική κατάσταση. Παρατηρούμε ότι, σε αυτήν την περίπτωση, υπάρχουν πολλοί παράγοντες που επηρεάζουν το προφίλ συμπεριφοράς όπως ο χρόνος χρήσης του επεξεργαστή, ο αριθμός των δικτυακών συνδέσεων στη μονάδα του χρόνου κλπ. Σε μερικά συστήματα το παρόν προφίλ και το προηγούμενο συνενώνονται ανά διαστήματα, ενώ σε άλλα η παραγωγή προφίλ γίνεται σε μια χρονική περίοδο. Το κυριότερο πλεονέκτημα των στατιστικών συστημάτων είναι ότι συνεχώς προσαρμόζονται καλύτερα στην παρακολούθηση της συμπεριφοράς των χρηστών. Συνεπώς είναι πιο ευαίσθητα από τον ανθρώπινο παράγοντα. Πάντως, υπάρχουν μερικά προβλήματα με αυτά τα συστήματα, γιατί μπορούν σταδιακά να κατευθυνθούν με τέτοιο τρόπο από εισβολείς, ώστε να οδηγούνται σε λάθος εκτιμήσεις. Για παράδειγμα, γεγονότα εισβολής να εκτιμηθούν ως φυσιολογικά, όταν το όριο ύπαρξης ή μη ύπαρξης διαταραχής (threshold) να είναι πολύ μικρό ή μεγάλο αντίστοιχα και σχέσεις μεταξύ γεγονότων να μην αναφερθούν λόγω της μικρής ευαισθησίας των στατιστικών παραγόντων που χρησιμοποιούνται.

Πρόβλεψη προτύπων

Αυτή η μέθοδος ανίχνευσης εισβολών προσπαθεί να προβλέψει μελλοντικά γεγονότα με χρήση γεγονότων που ήδη έχουν συμβεί. Χάριν παραδείγματος, μπορούμε να θέσουμε τον εξής κανόνα:

$$E1 - E2 \rightarrow (E3 = 80\%, E4 = 15\%, E5 = 5\%)$$

Αυτό σημαίνει ότι με δεδομένα τα γεγονότα E1 και E2 και με το E2 να ακολουθεί το E1 στο χρόνο, υπάρχει 80% πιθανότητα να ακολουθήσει το γεγονός E3, 15 % να ακολουθήσει το E4 και 5% να ακολουθήσει το E5. Το πρόβλημα είναι ότι μερικά επιθετικά σενάρια που δεν έχουν προβλεφθεί από το σύστημα δε θα χαρακτηριστούν ως εισβολή. Δηλαδή, αν μια ακολουθία γεγονότων A-B-C υπάρχει και είναι εισβολή, αλλά δεν βρίσκεται στη βάση των κανόνων, θα καταχωρηθεί απλά ως άγνωστη. Αυτό το πρόβλημα μπορεί να λυθεί μερικώς με ων χαρακτηρισμό οποιοδήποτε αγνώστου γεγονότος ως εισβολή (αυξάνοντας έτσι τον αριθμό των false negatives).Στην

φυσιολογική περίπτωση, ένα γεγονός χαρακτηρίζεται ως εισβολή εάν ταιριάζει με το αριστερό μέρος του κανόνα ανάλυσης και το δεξί μέρος είναι πολύ διαφορετικό από το αποτέλεσμα της πρόβλεψης.

Νευρωνικά δίκτυα

Μια διαφορετική προσέγγιση στα συστήματα εντοπισμού εισβολής είναι η χρήση νευρωνικών δικτύων. Η ιδέα εδώ είναι να «εκπαιδεύσουμε» ένα νευ ρωνικό δίκτυο με τέτοιο τρόπο, ώσιε να μπορεί να προβλέψει την επόμενη εντολή ή ενέργεια ενός χρήσιη, με βάση προηγούμενες εντολές και ενέργειες. Το δίκτυο λειτουργεί με βάση ένα σύνολο εντολών, αντιπροσωπευτικών του χρήστη. Μετά την περίοδο εκμάθησης το δίκτυο προσπαθεί να ταιριάξει πραγματικές εντολές με το πραγματικό προφίλ του χρήστη, που ήδη υπάρχει στο δίκτυο. Κάποια πλεονεκτήματα των νευρωνικών δικτύων είναι ότι τα καταφέρνουν καλά με πολύπλοκα δεδομένα, η επιτυχία τους δεν εξαρτάται από καμία στατιστική υπόθεση για την φύση των δεδομένων και είναι πιο εύκολο να μετατραπούν για διαφορετικές ομάδες χρησιών. Όμως υπάρχουν και προβλήματα. Πρώτα, ένα μικρό σύνολο πληροφοριών θα οδηγήσει σε πολλά false positives, ενώ ένα μεγάλο σύνολο θα οδηγήσει σε άσχετα δεδομένα και στην αύξηση των false negatives. Δεύτερο, η τοπολογία του δικτύου αποφασίζεται μετά από πολλές διαδοχικές δοκιμές και λάθη. Τρίτο, ο εισβολέας μπορεί να «εκπαιδεύσει» το δίκτυο κατά την φάση εκμάθησης.

9.5. Συστήμαια ανίχνευσης κακής χρήσης (Misuse Detection)

Η έρευνα στον χώρο των misuse detection συστημάτων και παραδείγματα τέτοιων συστημάτων παρουσιάζονται παρακάτω:

Ειδικά συστήματα

Διαχωρίζουν την φάση του ταιριάσματος των κανόνων συμπεριφοράς από την φάση εκτέλεσης. Το ταίριασμα γίνεται ανάλογα με τα γεγονότα που συμβαίνουν. Ακολουθούν υβριδικές τεχνικές ανίχνευσης επιθέσεων που αποτελούνται από στοιχεία misuse και anomaly detection. Ο anomaly detector βασίζεται στην στατιστική προσέγγιση και χαρακτηρίζει γεγονότα ως επιθέσεις αν διαφέρουν πολύ από την αναμενόμενη συμπεριφορά. Ο misuse detector κωδικοποιεί γνωστές περιπτώσεις εισβολών και πρότυπα επιθέσεων. Η βάση των κανόνων μπορεί να αλλάζει για διαφορετικά συστήματα. Το πλεονέκτημα είναι ότι περιλαμβάνουν τόσο στατιστικό στοιχείο, όσο και στοιχείο ειδικού συστήματος. Αυτό σημαίνει ότι έχουμε αυξημένες πιθανότητες να αναγνωρίσουμε μια εισβολή, αφού αν δεν την αναγνωρίσει το ένα στοιχείο θα την εντοπίσει το άλλο.

Υπάρχουν και κάποια μειονεκτήματα στην προσέγγιση ειδικών συστημάτων. Για παράδειγμα, το σύστημα πρέπει να συσταθεί από κάποιον ειδικό στο θέμα ασφάλειας, που σημαίνει ότι το σύστημα είναι τόσο ισχυρό όσο και το προσωπικό ασφαλείας που το προγραμματίζει. Αυτό οδηγεί στο συμπέρασμα πως υπάρχει σοβαρή πιθανότητα το σύστημα να αποτύχει να χαρακτηρίσει τις εισβολές.

Παρακολούθηση πληκτρολόγησης

Είναι μια απλή τεχνική η οποία παρακολουθεί χτυπήματα πλήκτρων για πρότυπα επίθεσης. Δυστυχώς το σύστημα αυτό έχει πολλά ελαττώματα. Δυνατότητες των shells, όπως bash, ksh, tcsh στις οποίες ο χρήστης χρησιμοποιεί aliases, ξεπερνούν την τεχνική αυτή εύκολα. Επίσης, η μέθοδος δεν αναλύει την εκτέλεση της εντολής, αλλά μόνο την πληκτρολόγηση. Αυτό σημαίνει ότι ένα κακόβουλο πρόγραμμα δεν μπορεί να χαρακτηριστεί ως επιθετική δραστηριότητα.

9.6. Συστήματα ανίχνευσης εισβολών βασισμένα σε μοντέλα

Η ιδέα στα συστήματα αυτά είναι ότι συγκεκριμένα σενάρια συμπεραίνονται από άλλες συγκεκριμένες φανερές δραστ:ηριότητες. Αν αυτές οι δραστηριότητες παρακολουθούνται, είναι δυνατό να εντοπίσουμε προσπάθειες εισβολής με εξέταση των δραστηριοτήτων που εξάγονται από συγκεκριμένα σενάρια εισβολής. Το βασικό μοντέλο του συστήματος αποτελείται από τρία modules.

Ο **προβλέπτης** χρησιμοποιεί ενεργά μοντέλα και μοντέλα σεναρίων και προσπαθεί να προβλέψει το επόμενο βήμα σε ένα σενάριο που αναμένεται να συμβεί. Ένα μοντέλο σεναρίου είναι μια βάση δεδομένων με προδιαγραφές επιθετικών σεναρίων.

Ο **σχεδιαστής** στη συνέχεια, μεταφράζει αυτήν την υπόθεση σε μία ένδειξη της συμπεριφοράς, όπως θα πρέπει να συμβεί μετά. Χρησιμοποιεί την πληροφορία πρόβλεψης για να σχεδιάσει το επόμενο βήμα αναζήτησης.

Ο **διερμηνέας** χρησιμοποιεί την πληροφορία από τον σχεδιαστή και ψάχνει για αυτήν στα δεδομένα που έρχονται. Το σύστημα προχωρά με αυτόν τον τρόπο, συγκεντρώνοντας όλο και περισσότερες αποδείξεις για μια προσπάθεια εισβολής μέχρι να συναντήσει ένα όριο (threshold). Σε αυτό το σημείο στέλνει alert για προσπάθεια εισβολής.

Η προσέγγιση αυτή είναι πολύ καλή. Επειδή ο σχεδιαστής και ο διερμηνέας γνωρίζουν τι πρέπει να αναζητήσουν σε κάθε βήμα, οι άχρηστες πληροφορίες φιλτράρονται και οδηγούμαστε σε εξαιρετικά αποτελέσματα. Επιπλέον, το σύστημα μπορεί να προβλέψει την επόμενη κίνηση του επιτιθέμενου, σύμφωνα με το μοντέλο εισβολής. Αυτές οι προβλέψεις χρησιμοποιούνται για να επαληθεύσουμε μια υποψία εισβολής, για να πάρουμε προληπτικά μέτρα ή για να αποφασίσουμε ποια δεδομένα να αναζητήσουμε στη συνέχεια.

Όμως, υπάρχουν κάποια κρίσιμα θέματα σχεηκά με το παραπάνω σύστημα. Πρώτα, τα πρότυπα για τα σενάρια εισβολής πρέπει να αναγνωρίζονται εύκολα. Δεύτερο, τα πρότυπα πρέπει πάντα να συμβαίνουν σύμφωνα με το μοντέλο συμπεριφοράς για την οποία αναζητούνται. Τρίτο τα πρότυπα πρέπει να είναι μοναδικά και να μην συνδέονται με καμία άλλη φυσιολογική συμπεριφορά.

Ανάλυση μετάβασης καταστάσεων

Στην τεχνική αυτή το σύστημα παρακολούθησης αναπαρίσταται σαν ένα διάγραμμα μετάβασης καταστάσεων. Καθώς τα δεδομένα αναλύονται το σύστημα πραγματοποιεί μεταβάσεις από μία κατάσταση σε άλλη. Η μετάβαση γίνεται αν κάποια λογική (Boolean) κατάσταση είναι αληθής (π.χ, ο χρήστης ανοίγει ένα αρχείο). Η προσέγγιση είναι να έχουμε μεταβάσεις από ασφαλείς σε μη ασφαλείς καταστάσεις σύμφωνα με γνωστά πρότυπα επιθέσεων. Για να φτάσουμε στην τελική κατάσταση εισβολής, πρέπει να εκπληρώνονται κάποιες καταστάσεις. Αν αυτές οι καταστάσεις προστασίας είναι αληθείς, τότε έχουμε εισβολή σχεδόν σίγουρα. Αν κάποια από αυτές τις καταστάσεις δεν είναι αληθής, η πιθανότητα εισβολής μειώνεται. Παρατηρούμε ότι αυτές οι καταστάσεις προστασίας υπάρχουν για να ξεχωρίζουν τις δρα στηριότητες εισβολής από τις φυσιολογικές δραστηριότητες. Μερικά πλεονεκτήματα αυτής της προσέγγισης είναι:

- μπορεί να ανιχνεύσει συνεργατικές επιθέσεις,
- μπορεί να εντοπίσει επιθέσεις που γεννώνται σε πολλές συνόδους χρηστών
- μπορεί να προβλέψει επικίνδυνες καταστάσεις σύμφωνα με την παρούσα κατάσταση του συστήματος και να λάβει προληπτικά μέτρα.

Παρόλα αυτά υπάρχουν και προβλήματα με τα συστήματα μετάβασης καταστάσεων. Τα πρότυπα επιθέσεων μπορούν να ορίσουν μόνο μια αλληλουχία γεγονότων, παρά περισσότερο πολύπλοκες φόρμουλες. Δεν μπορούν να ανιχνεύσουν επιθέσεις τύπου

denial of service, failed logins, διαφοροποιήσεις από την φυσιολογική χρήση και παθητική παρακολούθηση. Αυτό γίνεται, γιατί τα αντικείμενα αυτά δεν καταγράφονται από μηχανισμό ανίχνευσης ή δεν μπορούν να αναπαρασταθούν με διαγράμματα μετάβασης καταστάσεων. Κάποιες από τις αδυναμίες του συστήματος διορθώνονται με το μοντέλο σύγκρισης προτύπων που αναφέρουμε παρακάτω.

Μοντέλο σύγκρισης προτύπων

Το μοντέλο αυτό κωδικοποιεί γνωστές ενδείξεις εισβολών ως πρότυπα, που στη συνέχεια συγκρίνονται με τα δεδομένα ελέγχου. Όπως και στο σύστημα μετάβασης δεδομένων, το μοντέλο προσπαθεί να συγκρίνει επερχόμενα γεγονότα με πρότυπα που αντιπροσωπεύουν σενάρια εισβολής. Η υλοποίηση πραγματοποιεί μεταβάσεις σε συγκεκριμένα γεγονότα, που καλούνται ετικέτες και μεταβλητές Boolean που ονομάζονται έλεγχοι-φύλακες μπορούν να τοποθετηθούν σε κάθε μετάβαση. Η διαφορά μεταξύ του συγκεκριμένου μοντέλου και του μοντέλου ανάλυσης μεταβάσεων είναι ότι στο δεύτερο οι έλεγχοι-φύλακες συσχετίζονται με τις καταστάσεις, παρά με τις μεταβάσεις όπως έχουμε εδώ. Τα σημαντικότερα πλεονεκτήματα του μοντέλου είναι:

1. Χρειάζεται απλά να ξέρουμε ποια πρότυπα να συγκρίνουμε, όχι το πώς να τα συγκρίνουμε.
2. Πολλαπλές ροές γεγονότων μπορούν να χρησιμοποιηθούν για τη σύγκριση προτύπων για κάθε ροή, χωρίς την ανάγκη να συνδυάσουμε τις ροές. Αυτό σημαίνει ότι μπορεί να γίνει ανεξάρτητα η επεξεργασία και τα αποτελέσματα να αναλυθούν μαζί για να δώσουν αποδείξεις επιθετικής δραστηριότητας.
3. Μεταφερσιμότητα: Από τη στιγμή που τα signatures εισβολών γράφονται σε ένα script που είναι ανεξάρτητο από το σύστημα, δεν χρειάζεται να ξαναγραφτούν πάλι για δωφορετικά ίχνη πληροφοριών. Οι προδιαγραφές των προτύπων τους δίνουν τη δυνατότητα να ανταλλαχθούν μεταξύ διαφορετικών λειτουργικών συστημάτων.
4. Έχει εξαιρετικές δυνατότητες ελέγχου σε πραγματικό χρόνο, αφού η χρήση CPU είναι περίπου 5-6%, για έλεγχο 100 διαφορετικών προτύπων.
5. Μπορεί να ανιχνεύσει κάποια επιθετικά signatures όπως τα αποτυχημένα logins, που το μοντέλο μετάβασης καταστάσεων δεν μπορεί.

Ένα πρόβλημα με αυτό το μοντέλο είναι ότι μπορεί να εντοπίσει επιθέσεις που βασίζονται σε γνωστές ευπάθειες μόνο (αποτελεί και γενικότερο πρόβλημα των misuse detection συστημάτων). Επίσης, δεν μπορεί να ανιχνεύσει επιθέσεις από μηχάνημα που προσποιείται ότι είναι άλλο μηχάνημα χρησιμοποιώντας την IP διεύθυνσή του (spoofing attack).

9.7. Ασυνήθιστα IP πακέτα που πρέπει να ανιχνεύουν τα IDS

Καθώς η χρήση των συστημάτων ανίχνευσης επιθέσεων συνεχώς εξαπλώνεται πρέπει να αναφέρουμε τα χαρακτηριστικά των ασυνήθιστων IP πακέτων. Αυτό είναι απαραίτητο για την εκτίμηση ενός συναγερμού (alert) από τον διαχειριστή του συστήματος, αφού υπάρχουν περιπτώσεις που ακόμα και αν το IDS παράγει alert για συγκεκριμένες διερευνήσεις (scans) και επιθέσεις, να μην μπορούμε να καταλάβουμε η σημαίνει αυτό το alert.

Ορίζουμε ως ασυνήθιστα πακέτα εκείνα που παραβιάζουν τα IP protocol standards όπως αυτά ορίζονται στο σύνολο των προδιαγραφών RFC (Requests For Comments). Δημιουργούνται από τυχαία γεγονότα, όπως από ένα router που δεν λειτουργεί σωστά, αλλά συνήθως κατασκευάζονται ειδικά από επιτιθέμενους για να πετύχουν τους σκοπούς

τους. Η ανωμαλία εισάγεται συχνά στο πακέτο με σκοπό να αποφευχθεί το μπλοκάρισμα του πακέτου από ένα firewall ή από ένα σύστημα ανίχνευσης επιθέσεων (IDS). Επίσης, τα πακέτα αυτά χρησιμεύουν σε προσπάθειες για αποτροπή της λειτουργίας συστημάτων.

Τύποι IP πρωτοκόλλων

Υπάρχουν πολλοί διαφορετικοί τύποι IP πρωτοκόλλων. Τα τρία πιο συνηθισμένα είναι: το Transmission Control (TCP), το User Datagram (UDP) και το Internet Message (ICMP). Υπάρχουν δεκάδες άλλα πρωτόκολλα όπως τα IGRP, EIGRP, OSPF κλπ. Κάθε ένα έχει την δική του τιμή, που ονομάζεται Internet Protocol Number. Είναι σημαντικό να ης γνωρίζουμε γιατί κάποια συστήματα καταγράφουν τα πακέτα με βάση αυτό το νούμερο.

IP διευθύνσεις

Συγκεκριμένες IP διευθύνσεις έχουν ανατεθεί ειδικά από την IANA (Internet Assigned Numbers Authority) ως δεσμευμένες για εσωτερική χρήση εσωτερικού δικτύου μόνο και όχι για χρήση στο internet. Οι δεσμευμένες ζώνες διευθύνσεων είναι: 10.0.0.0 - 10.255.255.255,172.16.0.0 - 172.31.255.255 και 192.168.0.0 - 192.168.255.255.

Αν και οι παραπάνω διευθύνσεις δεν θα έπρεπε ποτέ να εμφανιστούν στο Internet, παρόλα αυτά υπάρχουν. Κάποιες φορές αυτό οφείλεται σε εξοπλισμό που έχει αρχικοποιηθεί λάθος. Για παράδειγμα, ένα firewall μπορεί κατά λάθος να επιτρέψει σε εσωτερικές διευθύνσεις να διαρρεύσουν στο internet. Επίσης, μηχανήματα που προσπαθούν αποτυχημένα να αποκτήσουν IP διεύθυνση μέσω ενός DHCP server, τυπικά τους ανατίθενται διευθύνσεις στο υποδίκτυο 169.254. Ένας επιπλέον λόγος είναι ότι οι

hackers δημιουργούν τέτοια πακέτα με ψεύτικες IP διευθύνσεις. Αυτή η τεχνική ονομάζεται όπως έχουμε αναφέρει IP spoofing.

Ο κυριότερος λόγος για την εφαρμογή του IP spoofing είναι να καταστήσουνε αδύνατη την ανίχνευση της πραγματικής IP διεύθυνσης. Οι εισβολείς μπορεί να χρησιμοποιήσουνε διευθύνσεις στις ζώνες που αναφέρθηκαν παραπάνω. Πιο συχνά χρησιμοποιούν πραγματικές διευθύνσεις που ανήκουν σε κάποιον άλλον. Εάν το σύστημά μας δεχτεί επίθεση, εμείς θα εντοπίσουμε την IP διεύθυνσης ενός «αθώου» συστήματος. Ένας άλλος τύπος IP spoofing επίθεσης ονομάζεται Land επίθεση και χρησιμοποιεί πακέτα με πηγή και προορισμό την ίδια διεύθυνση. Τα πακέτα πρέπει πάντα να έχουν διαφορετική διεύθυνση πηγής και προορισμού και οι δικτυακές συσκευές μας πρέπει να απορρίπτουν πακέτα που οι τιμές αυτές είναι οι ίδιες.

Για να αποφύγουμε IP spoofing επιθέσεις που δημιουργούνται στο δίκτυό μας πρέπει να επιτρέπουμε εισερχόμενα πακέτα με διεύθυνση πηγής εκτός της δικτυακής μας ζώνης και διεύθυνση προορισμού εντός της δικτυακής μας ζώνης. Επίσης, πακέτα που έχουν IP διεύθυνση σε ζώνες μη επιτρεπόμενες πρέπει να απορρίπτονται άμεσα από τις Internet based συσκευές μας.

TCP πακέτα

Το TCP είναι ένα πρωτόκολλο που βασίζεται στις αμφίδρομες συνδέσεις. Χρησιμοποιεί διάφορα flags για να δείξει ότι μια σύνδεση έχει αρχίσει ή τελείωσε, ή ότι τα δεδομένα είναι υψηλής προτεραιότητας. Πολλές επιθέσεις βασίζονται στην αλλοίωση των TCP flags. Συγκεκριμένοι παράνομοι συνδυασμοί flags μπορούν να βοηθήσουν πακέτα να αποφύγουν τον εντοπισμό από firewalls ή IDS.

Οι λειτουργικές προδιαγραφές για το TCP ορίζονται στο RFC 793. Εκεί ορίζεται το πώς θα πρέπει να απαντούν τα συστήματα σε νόμιμα πακέτα, αλλά δεν εξηγούν το πώς θα πρέπει να χειρίζονται παράνομους συνδυασμούς flags. Συνεπώς, διαφορετικά λειτουργικά συστήματα δεν αντιδρούν με τον ίδιο τρόπο σε αυτούς τους συνδυασμούς. Οι

επιτιθέμενοι χρησιμοποιούν αυτό για να διαπιστώσουν το είδος του λειτουργικού που ένα σύστημα ή συσκευή χρησιμοποιεί.

TCP Header
Ο header ενός TCP πακέτου παρατίθεται παρακάτω:

<table>
<tr><td colspan="8">16bits</td><td>32 bits</td></tr>
<tr><td colspan="8">Source port</td><td>Destination port</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgement number</td></tr>
<tr><td>Offset</td><td>Resrvd</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="8">Checksum</td><td>Urgent pointer</td></tr>
<tr><td colspan="9">Option + Padding</td></tr>
<tr><td colspan="9">Data</td></tr>
</table>

Τουλάχιστον ένα από τα έξι flags πρέπει να έχει τιμή σε κάθε TCP πακέτο. Κάθε flag αντιστοιχεί σε ένα συγκεκριμένο bit στο TCP header. Τα έξι Ξags είναι:

- SYN (Synchronization) - Ξεκινάει μια TCP σύνδεση.
- ACK (Acknowledgment) - Δείχνει ότι η τιμή στο πεδίο επιβεβαίωσης τιμής είναι έγκυρη
- FIN (Finish) - Ομαλή λήξη μιας σύνδεσης.
- RST (Reset) - Απότομη λήξη μιας σύνδεσης.
- PSH (Push) - Πληροφορεί τον δέκτη να τελειώσει με τα δεδομένα όσο γίνεται πιο γρήγορα.
- URG (Urgent) - Δείχνει ότι ο δείκτης άμεσης προτεραιότητας είναι έγκυρος, συχνά προκαλείται από ένα διακόπτη.

Πριν αναφέρουμε τους ανώμαλους συνδυασμούς flags ας ρίξουμε μια ματιά στους κανονικούς:

- SYN, SYN ACK και ACK χρησιμοποιούνται κατά τη διάρκεια του three-way handshake που εγκαθιστά μια TCP σύνδεση.
- Εκτός από το αρχικό SYN πακέτο, κάθε πακέτο στη σύνδεση πρέπει να έχει το ACK bit ενεργοποιημένο.
- FIN ACK και ACK χρησιμοποιούνται κατά τη διάρκεια μια φυσιολογικής συνόδου λήξης μιας υπάρχουσας σύνδεσης.
- RST ACK μπορεί να χρησιμοποιηθεί για να κλείσει άμεσα μια υπάρχουσα σύνδεση.
- Πακέτα κατά τη διάρκεια της συνομιλίας σε μια σύνδεση (αμέσως μετά το three-way handshake, αλλά πριν τη λήξη της) περιέχουν μόνο ACK Προαιρετικά, μπορούν να περιέχουν PSH και /ή URG.

Πακέτα με οποιονδήποτε διαφορετικό συνδυασμό flags χαρακτηρίζονται ως ανώμαλα. Μερικοί από τους πιο συνηθισμένους συνδυασμούς παρουσιάζονται παρακάτω:

- SYN FIN είναι πιθανότατα ο πιο γνωστός παράνομος συνδυασμός. Το SYN χρησιμοποιείται για την έναρξη μιας σύνδεσης, ενώ το FIN για την λήξη μιας σύνδεσης. Είναι παράλογο να εκτελούμε και τις δύο πράξεις ταυτόχρονα. Πολλά εργαλεία port scanning χρησιμοποιούν SYN FIN πακέτα, γιατί πολλά συστήματα ανίχνευσης επιθέσεων δεν μπορούσαν να τα εντοπίσουν στο παρελθόν, αν και πλέον τα περισσότερα μπορούν. Μπορούμε να υποθέσουμε πως κάθε SYN FIN πακέτα που βλέπουμε είναι κακόβουλα.
- Υπάρχουν ως παραλλαγές του SYN FIN τα SYN FIN PSH, SYN FIN RST, SYN FIN RST PSH. Αυτά τα πακέτα χρησιμοποιούνται από εισβολείς που γνωρίζουν ότι αρκετά IDS συστήματα για να βελτιώσουν τους χρόνους επεξεργασίας κοιτάνε για πακέτα με μόνο το SYN και το FIN bit ενεργοποιημένα, και όχι τα επιπλέον. Και πάλι τα πακέτα αυτά είναι ιδιαίτερα επικίνδυνα.
- Τ α πακέτα δεν πρέπει ποτέ να περιέχουν μόνο ένα FIN flag. Τα FIN πακέτα συχνά χρησιμοποιούνται για port scan, network mapping και άλλες ύποπτες δραστηριότητες.
- Μερικά πακέτα δεν έχουν κανένα flag ενεργοποιημένο. Αυτά ονομάζονται "null" πακέτα και είναι παράνομο να υπάρχει πακέτο τέτοιας μορφής.

Εκτός από τα έξι flag bits που περιγράψαμε, τα TCP πακέτα έχουν και δύο επιπλέον bits που δεσμεύονται για μελλοντική χρήση και αναφέρονται ως «δεσμευμένα bits». Οποιοδήποτε πακέτο που έχει ένα ή και τα δύο δεσμευμένα bits ενεργοποιημένα είναι σίγουρα ύποπτο.

Υπάρχουν και κάποια άλλα χαρακτηριστικά της TCP κίνησης όπου οι ανωμαλίες γίνονται αντιληπτές:

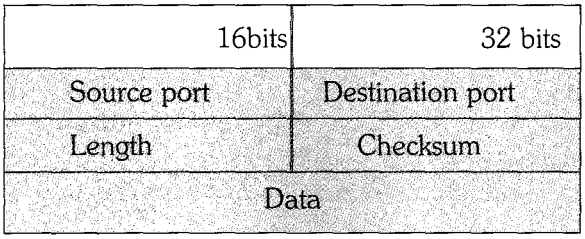
- Τα πακέτα δεν πρέπει να έχουν ποτέ port της πηγής ή του προορισμού στην τιμή 0.
- Ο αριθμός βεβαίωσης λήψης δεν πρέπει ποτέ να είναι Ο όταν το ACK flag είναι ενεργοποιημένο.
- Ένα SYN μόνο πακέτο, που συναντάται μόνο όταν ξεκινάει μια νέα σύνδεση, δεν πρέπει να περιέχει δεδομένα.
- Πακέτα δεν πρέπει να χρησιμοποιούν διευθύνσεις προορισμού που αποτελούν διευθύνσεις εκπομπής και συνήθως τελειώνουν σε .0 ή σε .255. Οι εκπομπές κανονικά δεν πραγματοποιούνται με χρήση του TCP.

Πολλά από τα εργαλεία που χρησιμοποιούν οι επιτιθέμενοι για να σαρώσουν και να εξετάσουν ένα δίκτυο βασίζονται στη χρήση παράνομων συνδυασμών πακέτων. Ένα μεγάλο ποσοστό alerts που εντοπίζονται από IDS περιλαμβάνουν και αυτούς τους τύπους των πακέτων, επομένως είναι κρίσιμο να μπορέσουμε να τα αναγνωρίσουμε και να καταλάβουμε τη λειτουργία τους. Με το να στήσουμε το IDS έτσι ώστε να αναγνωρίζει αυτά τα πακέτα είμαστε σε θέση να βρούμε ασυνήθιστη δραστηριότητα που αγνοούσαμε μέχρι τότε.

UDP πακέτα

Αντίθετα με το TCP, το UDP είναι πρωτόκολλο που δε βασίζεται στην αμφίδρομη σύνδεση μεταξύ hosts. Δεν έχει flag και τα δεσμευμένα bits που έχει το TCP. Όμως, και τα δύο βασίζονται στα ports της πηγής και του προορισμού. Όπως στο TCP, τα UDP πακέτα δεν πρέπει να έχουν port πηγής ή προορισμού στην τιμή Ο. Για την δημιουργία ασυνήθιστων UDP πακέτων χρησιμοποιείται η τεχνική του θρυμματισμού (fragmentation) που αναφέρουμε παρακάτω.

Ο UDP header αποτελείται από 4 πεδία, με μήκος 2 bytes το καθένα.



ICMP πακέτα

Το ICMP χρησιμοποιείται για να μεταβιβάσει ένα μήνυμα λάθους μεταξύ δύο συστημάτων (hosts), ή από ένα σύστημα σε μια δικτυακή συσκευή όπως είναι ένας δρομολογητής. Από τη στιγμή που το UDP, δε βασίζεται στην αμφίδρομη σύνδεση, χρησιμοποιείται το ICMP για να μεταδίδει τα μηνύματα λάθους εκ μέρους τους. Για να αποφευχθούν πιθανές επαναλήψεις μηνυμάτων λαθών, οι απαντήσεις ποτέ δεν στέλνονται στα μηνύματα λάθους του ICMP, γιατί δεν έχει αριθμούς ports. Αντίθετα, χρησιμοποιεί τύπους μηνυμάτων και κωδικούς. Ένα άλλο αξιοπρόσεχτο χαρακτηριστικό του ICMP είναι ότι υποστηρίζει κίνηση εκπομπής. Αφού τα ICMP πακέτα δεν είναι πολύπλοκα, δεν υπάρχουν πολλοί τρόποι να αλλοιωθούν για άλλους σκοπούς.

Ένας τύπος ICMP μηνύματος που χρησιμοποιείται κακόβουλα είναι η ανακατεύθυνση (redirect). Το ICMP ανακατευθύνει τα μηνύματα που πρόκειται να σταλούν από έναν δρομολογητή σε έναν κόμβο. Αυτό γίνεται για να τον ενημερώσει πως υπάρχει πιο κατάλληλος δρομολογητής για την επικοινωνία με μια συγκεκριμένη διεύθυνση προορισμού. Κάποια είδη επιθέσεων όπως το Winfreeze χρησιμοποιεί ψεύτικες ανακατευθύνσεις μηνυμάτων για να πετύχει να πείσει ένα host να χρησιμοποιήσει τον εαυτό του ως βέλτιστο δρομολογητή. Προφανώς, όποιο πακέτο λέει σε μια συσκευή να δρομολογεί τα πάντα στον εαυτό του πρέπει να θεωρείται ιδιαίτερα επικίνδυνο.

Τα περισσότερα ICMP πακέτα αποτελούνται από έναν μικρό header και την ωφέλιμη πληροφορία τους. Για παράδειγμα, τα περισσότερα ICMP echo requests πακέτα έχουν έναν 8 byte header και 56 bytes δεδομένων. ICMP πακέτα που είναι αρκετά μεγαλύτερα από το κανονικό πρέπει να θεωρούνται ύποπτα.

Επίσης, κάποια είδη ICMP όπως echo requests δεν πρέπει να περιέχουν δεδομένα, Κάποιες κακόβουλες εφαρμογές, όπως προγράμματα denial of

service και tunneling, χρησιμοποιούν ICMP πακέτα σαν κλωβούς που κρύβουν άλλη κίνηση. Άρα, μία ICMP echo απάνωση μπορεί να περιέχει ένα εντελώς διαφορετικό IP πρωτόκολλο στα δεδομένα της, για παράδειγμα. Εάν παρακολουθούμε τα συστήματά μας για μεγάλα ICMP πακέτα ή για πακέτα ICMP συγκεκριμένου τύπου που περιέχουν δεδομένα, ενώ δε θα έπρεπε, θα είμαστε σε θέση να εντοπίσουμε αυτόν τον τύπο της κίνησης.

Κατάτμηση (Fragmentation)

Όταν ένα IP πακέτο είναι πολύ μεγάλο για να μεταδοθεί με τη μία, πρέπει να χωριστεί σε δύο η περισσότερα κομμάτια που μπορούν να σταλούν κατά μήκος των δικτύων. Κάθε μέρος ενός πακέτου αναφέρεται ως fragment. Αυτή η διαδικασία συμβαίνει για όλα τα πρωτόκολλα που αναφέραμε - TCP, UDP και ICMP- αν και κυρίως πραγματοποιείται για το TCP. Όμως, οι επιτιθέμενοι μπορούν να δημιουργήσουν τεχνητά κομματιασμένα πακέτα. Σε ιερικές περιπτώσεις, αυτό γίνεται για να οδηγήσει σε crash του συστήματος. Άλλες φορές γίνεται για να αποφευχθεί ο εντοπισμός από συστήματα ανίχνευσης

επιθέσεων. Κάποια firewalls και IDS δεν εκτελούν επανασυναρμολόγηση των πακέτων, οπότε μπορούν απλά να ελέγξουν το κάθε κομμάτι ξεχωριστά και όχι ως σύνολο.

Ένας τύπος κακόβουλου fragmentation περιλαμβάνει κομμάτια που έχουν παράνομα offset. Μία τιμή offset υποδεικνύει που θα πρέπει να τοποθετηθούν τα δεδομένα όταν το πακέτο επανασυναρμολογηθεί. Το πρώτο κομμάτι φαίνεται φυσιολογικό, εκτός από το ότι είναι πολύ μικρό. Το δεύτερο έχει μία τιμή offset δεδομένων που είναι μικρότερη από το μήκος των δεδομένων στο πρώτο πακέτο. Δηλαδή, αν το πρώτο κομμάτι είχε 24 bytes δεδομένων, το δεύτερο μπορεί να ισχυριστεί ότι έχει ένα offset της τάξης των 20 bytes. Αυτό σημαίνει ότι τα δεδομένα στο δεύτερο κομμάτι θα επαναγράψουν τα 4 τελευταία bytes δεδομένων από το πρώτο κομμάτι. Αν το fragmented πακέτο ήταν TCP, τότε το πρώτο κομμάτι θα περιέχει τον TCP header. Ο σκοπός ως τιμής offset στο δεύτερο κομμάτι θα ήταν να επαναγράψει μέρος του TCP header του πρώτου κομματιού, όπως το port της διεύθυνσης προορισμού. Έτσι, ένας επιτιθέμενος μπορεί να στείλει ένα fragmented πακέτο μέσω του firewall στον web server στο port 80, αλλά όταν ο web server επανασυναρμολογήσει το πακέτο, η τελική μορφή θα κατευθυνθεί σε ένα εντελώς διαφορετικό port.

Ο ίδιος τύπος επίθεσης μπορεί να χρησιμοποιηθεί για την διακοπή λειτουργίας των συστημάτων. Σε μερικά παλιότερα λειτουργικά συστήματα, όταν το μηχάνημα που λαμβάνει πακέτα προσπαθήσει να ξαναφτιάξει τέτοιο πακέτο, υπολογίζει αρνητικό μήκος για το δεύτερο κομμάτι. Αυτή η τιμή μεταφέρεται σε μία συνάρτηση που θα πρέπει να αντιγράψει από την μνήμη. Δυστυχώς, η αντιγραφή δεν μπορεί να χειριστεί αρνητική τιμή, με αποτέλεσμα να νομίσει πως η αρνητική τιμή είναι στην πραγματικότητα μία πολύ μεγάλη θετική τιμή.

Ένας δεύτερος τύπος επιθέσεων που περιέχει fragments είναι γνωστός και ως επίθεση tiny fragment. Δύο TCP fragments δημιουργούνται. Το πρώτο κομμάτι είναι τόσο μικρό, ώστε δεν περιέχει ούτε καν ολόκληρο το TCP header, και ειδικότερα το port προορισμού. Το δεύτερο κομμάτι περιέχει το υπόλοιπο μέρος του TCP header, μαζί με τον αριθμό του port. Κάποια firewall και IDS, ίσως επιτρέψουν σε ένα ή και στα δύο κομμάτια να περάσουν, ειδικά εάν δεν εκτελούν επανασυναρμολόγηση πακέτων.

Επίθεση πραγματοποιείται στέλνοντας ένα fragmented και ασυνήθιστα μεγάλο πακέτο. Ο επιτιθέμενος ελπίζει ότι όταν ο host λάβει τα κομμάτια, θα καταρρεύσει στην προσπάθεια να ξαναφτιάξει το αρχικό πακέτο, αφού το μέγεθός του είναι παράνομο (τα πακέτα έχουν ένα ελάχιστο και μέγιστο μέγεθος). Ο πιο γνωστός τρόπος επίθεσης είναι το διάσημο Ping of death. Δημιουργεί ένα ICMP echo request πακέτο που είναι μεγαλύτερο από το μέγιστο επιτρεπόμενο μέγεθος των 65,535 bytes.

Κάποιες επιθέσεις χρησιμοποιούν πακέτα που δεν είναι παράνομα, αλλά είναι εξαιρετικά ύποπτα. Για παράδειγμα, ας υποθέσουμε ότι λαμβάνουμε ένα TCP πακέτο που έχει μόνο το SYN flag ενεργοποιημένο. Από τη στιγμή που ένα τέτοιο πακέτο δεν επιτρέπεται να μεταφέρει δεδομένα, δεν θα πρέπει να είναι αρκετά μεγάλο ώστε να χρειάζεται fragmentation. Εάν συναντήσουμε τέτοιο πακέτο πρέπει να το μεταχειριστούμε με υποψία.

Επομένως, πώς μπορούμε να προστατέψουμε το δίκτυο μας σε επιθέσεις fragmentation; Όπως αναφέραμε προηγουμένως, πρέπει να χρησιμοποιήσουμε firewalls και συστήματα ανίχνευσης επιθέσεων που μπορούν να εκτελέσουν επανασυναρμολόγηση πακέτων. Πρέπει επίσης, να

στέλνουν alert όταν συναντώνται πολύ μικρά κομμάτια, διαφορετικά από το τελικό κομμάτι σε ένα πακέτο. Σε φυσιολογικές συνθήκες, δεν πρέπει να παρατηρούμε μικρά αρχικά κομμάτια, τα οποία είναι συνήθως κακόβουλα. Επίσης, πρέπει να κρατάμε το σύστημά μας updated με τα κατάλληλα patches και security fixes.

9.8. Οδηγίες για επιλογή προϊόντων IDS

Οι τεχνικές δυνατότητες αποτελούν σίγουρα ένα σοβαρό λόγο για την αγορά ενός IDS, αλλά δεν είναι το μόνο. Υπάρχει ένας αριθμός οργανωτικών και περιβαλλοντικών λόγων επίσης. Θα παραθέσουμε τρία διαφορετικά δέντρα απόφασης για να βοηθηθεί κάποιος που θέλει να επιλέξει ένα IDS. Τα δέντρα αυτά παρέχουν βασικές αρχές προς την κατεύθυνση της σωστής επιλογής, ανάλογα με ης ανάγκες μας. Έτσι έχουμε τα εξής δέντρα σχετικά με: management, technical issues και web sites.

Το πρώτο βήμα στην αξιολόγηση ενός σχεδίου ανίχνευσης επιθέσεων είναι να αποφασίσουμε το κατά πόσο είναι διαθέσιμη η διοίκηση του οργανισμού να υποστηρίξει το σχέδιο. Σκοπός ενός IDS δεν είναι απλά να εντοπίσει ης εισβολές, αλλά να «κάνει κάτι» για αυτές. Επομένως, η ανίχνευση επιθέσεων πρέπει να θεωρηθεί ως τμήμα μιας μεγαλύτερης διαδικασίας απάντησης σε γεγονότα. Η διοίκηση πρέπει να αποφασίσει ποιος τύπος απάντησης είναι ο κατάλληλος και πώς να επιλύσει τέτοιες καταστάσεις.

Επιπλέον, η απάντηση μπορεί να περιλαμβάνει ένα σημαντικό αριθμό ανθρώπων που ασχολούνται με νομικά θέματα, δημόσιες σχέσεις, δικτυακή υποδομή και διαχείριση. Επίσης, θα πρέπει να γνωρίζουμε ότι θα υπάρξει μείωση παραγωγικότητας και καθυστέρηση του συστήματος ως εταιρείας. Η έκταση ως παρεχόμενης υποστήριξης θα έχει ουσιαστικό αποτέλεσμα στην τελική απόφαση. Συστήματα που είναι δύσκολο να υλοποιηθούν και να υποστηριχθούν θα απαιτήσουν πολύ μεγαλύτερη υπομονή και δουλειά από άλλα, πιο απλά. Όμως δυνατοί συνδυασμοί IDS και καταρτισμένου προσωπικού μπορούν να εμπνεύσουν την εμπιστοσύνη ενός ασφαλούς συστήματος.

Ένα άλλο σημείο που απαιτεί προσοχή αφορά τα τεχνικά θέματα που προκύπτουν κατά την εγκατάσταση ενός IDS. Τυπικά, το πιο σημαντικό θέμα είναι η επιπλέον δικτυακή κίνηση (traffic) που θα προκαλείται από ένα σύστημα ανίχνευσης επιθέσεων. Ένα άλλο θέμα είναι η δημιουργία μια διαδικασίας για την ερμηνεία των αποτελεσμάτων από το IDS. Οι οργανισμοί πρέπει να αποφασίσουν για το πώς θα χειριστούν τα αποτελέσματα της ανάλυσης και πώς θα ενσωματώσουν τα αποτελέσματα αυτά σε ένα γενικότερο σχέδιο αντίδρασης και διόρθωσης.

Αρχικά πρέπει να αναγνωρίσουμε τις κρίσιμες πηγές πληροφορίας, για την αποθήκευση και ης επικοινωνίες. Με άλλα λόγια, να κάνουμε μια λίστα με όσα θέλουμε να προστατέψουμε. Αφού γίνει αυτό, πρέπει να εκτιμήσουμε τη δυνατότητα να διατηρήσουμε την ασφάλεια σε αυτές τις πηγές.

Η πρόσβαση στα μηχανήματα αποτελεί έναν κρίσιμο παράγοντα. Τα Host Based IDS απαιτούν περισσότερη προσοχή, από ότι τα Network Based συστήματα ανίχνευσης. Από τη στιγμή, που ένα host based IDS απαιτεί πρόσβαση με αυξημένα δικαιώματα στο λειτουργικό του host, μία host based υλοποίηση απαιτεί σημαντική υποστήριξη από την υπεύθυνη ομάδα για το IDS. Αυτός ο παράγοντας είναι και ο σημαντικότερος όταν εγκαθιστούμε ένα host based IDS.

Όταν εγκαθιστούμε ένα IDS για κάποιον web server παρουσιάζονται ειδικές συνθήκες. Από τη στιγμή που γνωρίζουμε ότι οι web servers είναι περισσότερο επιρρεπείς σε επιθέσεις, θα πρέπει να τους δοθεί ιδιαίτερη προσοχή από την ομάδα διαχείρισης του IDS. Ίσως η σκέψη για περισσότερους από έναν τύπο IDS να είναι εφαρμόσιμη και σωστή σε αυτήν την περίπτωση.

9.9. Στοιχεία που προέρχονται από τα συστήματα IDS για την διαχείριση και ανάλυση των επιθέσεων

Το IDS σύστημα συνήθως αποτελείται από το υποσύστημα συλλογής στοιχείων και από το υποσύστημα ανάλυσης των δεδομένων και διαχείρισης των συμβάντων. Για την αναγνώριση επίθεσης χρησιμοποιούνται οι παρακάτω γενικές τεχνικές από το σύστημα ανάλυσης δεδομένων:

- Ταίριασμα ακολουθιών, εκφράσεων ή ψηφιολέξεων
- Συχνότητες ή όρια γεγονότων
- Συσχέτιση γεγονότων
- Ανιχνευση στατιστικών ανωμαλιών

Από τη στιγμή που η επίθεση έχει ανιχνευθεl, το σύστημα διαχείρισης της επίθεσης δίνει μια ποικιλία στις επιλογές για πληροφόρηση, προειδοποίηση και λήψη μέτρων απέναντι στην επίθεση. Συνήθως, ενημερώνεται ο διαχειριστής, γίνεται τερματισμός της σύνδεσης μεταξύ επιτιθέμενου και host ή και καταγραφή της συνόδου με σκοπό τη συλλογή πληροφοριών για περαιτέρω ανάλυση και συγκέντρωση αποδελξεων.

Οι δυνατότητες για αντιμετώπιση των επιθέσεων και απειλών είναι κρίσιμο χαρακτηριστικό για οποιαδήποτε IDS. Τα περισσότερα network based ή host based IDS μοιράζονται τις ίδιες επιλογές απάντησης/αντιμετώπισης των επιθέσεων. Οι αντιδράσεις αυτές χωρlζονται σε τρεις κατηγορίες:

- Κοινοποίησης της επίθεσης
- Αποθήκευσης στοιχείων
- Ενεργής απάντησης

Αναλυτικά για κάθε μία κατηγορία έχουμε:

Κοινοποίηση της επίθεσης

Περιλαμβάνει αποστολή σήματος κινδύνου στην κονσόλα ή στο σύστημα του διαχειριστή για την πιθανή επίθεση. Ένας άλλος τρόπος ειδοποίησης είναι μέσω ηλεκτρονικού ταχυδρομείου στον διαχειριστή, σε χρήστες που να τους αφορά άμεσα το θέμα ή σε οποιοδήποτε άλλο ενδιαφερόμενο πρόσω πο. Ακόμη, μέσω SNMP traps μηνυμάτων, που στέλνονται σε διάφορους hosts και περιλαμβάνουν πληροφορίες για το είδος της επίθεσης. Τα μηνύματα αυτά είναι ιδιαίτερα ενδιαφέρονται για τους διαχειριστές συστημάτων και δικτύων.

Αποθήκευση στοιχείων

Για κάθε σύστημα ανίχνευσης επιθέσεων η αποθήκευση των δεδομένων είναι το ποιο βασικό σημείο. Έτσι, το σύστημα ανάλυσης αποθηκεύει το αρχείο καταγραφής συμβάντων (log) το οποίο περιέχει το σύνολο όλων των πακέτων, διευθύνσεων και ενεργειών που καταγράφηκαν από τον υποσύστημα συλλογής δεδομένων. Επίσης, μπορεί να αποθηκεύσει και τη συνεχή ροή πληροφοριών που κινείται σε ένα δίκτυο ανεξάρτητα από το αν χαρακτηρίζονται αυτές ως ύποπτες ή όχι. Αυτό γίνεται για περαιτέρω ανάλυση της δικτυακής κυκλοφορίας.

Ενεργή απάντηση

Εδώ έχουμε το σύνολο εκείνων των ενεργειών που αποτελούν την απάντηση του συστήματος μας στον εισβολέα. Η πιο συνηθισμένη είναι ο τερματισμός της σύνδεσης μεταξύ του εισβολέα και του κόμβου που υφίσταται την επίθεση με τη χρήση ενός TCP Reset πακέτου. Σε περίπτωση που υπάρχει firewall μπορεί να γίνει νέα αρχικοποίηση χρησιμοποιώντας τα καινούργια δεδομένα (ip διεύθυνση του επιτιθέμενου κλπ) για την καλύτερη προστασία του δικτύου μας.

Τέλος πρέπει να υποστηρίζεται από το σύστημα η επιλογή από τον διαχειριστή προκαθορισμένων πράξεων ανάλογα με την κρίση του.

Ανάλυση δεδομένων για τον χαρακτηρισμό μιας επίθεσης

Από τη στιγμή που έχουμε ειδοποίηση (alert) από το σύστημα IDS για πιθανη επίθεση χρειάζεται να ελέγξουμε τα υπολογιστικά και δικτυακά συστήματα και τα δεδομένα μας, καθώς και να καθορίσουμε τις αντιδράσεις μας. Η πληροφορία που συλλέγεται και επεξεργάζεται μέσω της ανάλυσης αποτελεί κλειδί στις αποφάσεις και τις πράξεις κατά τη διάρκεια της διαδικασίας απάντησης στην επίθεση.

Ο σκοπός της ανάλυσης είναι να βρεθεί:

- Το είδος των επιθέσεων που χρησιμοποιήθηκαν
- Ποια συστήματα και τι δεδομένα προσβλήθηκαν από τον εισβολέα
- Οι κινήσεις του εισβολέα μετά την είσοδο στα συστήματα
- Το τι κάνει τώρα ο εισβολέας, σε περίπτωση που η εισβολή δεν έχει περιοριστεί ή τερματιστεί

Κατά τη διάρκεια της ανάλυσης, θα μπούμε στον πειρασμό να συλλέξουμε επιπλέον πληροφορίες για το σύστημα που ο επιτιθέμενος χρησιμοποίησε για να μπει στο σύστημά μας. Τέτοιες ενέργειες μπορεί να γίνουν αντιληπτές από τον εισβολέα. Σε περίπτωση που το σύστημα από το οποίο προέρχεται η επίθεση ανήκει σε κάποιον άλλον οργανισμό, αυτή η συλλογή στοιχείων μπορεί να ερμηνευτεί ως ενέργεια εισβολής.

Συνεπώς η αξία της συλλογής όσο το δυνατόν περισσότερων στοιχείων πρέπει να είναι σε ισορροπία με τον πιθανό κίνδυνο να καταλάβουν οι επιτιθέμενοι ότι έγιναν αντιληπτοί. Συνέπεια αυτού μπορεί να είναι οι βεβιασμένες ενέργειες από μέρους τους για να διαγράψουν τα ίχνη των δραστηριοτήτων τους, που σημαίνει επιπλέον ζημιά στα συστήματα που προσπαθούμε να διασώσουμε. Κάποιοι πιθανότητα να μην επιστρέψουν, πράγμα που σημαίνει ότι δε θα λάβουμε πληροφορίες από μελλοντική επίσκεψη τους στα συστήματα μας, που ίσως να αποδεικνύονταν πολύ σημαντικές.

Για να αντιμετωπιστεί μια εισβολή αποτελεσματικά πρέπει να καθοριστεί ο σκοπός και η επίδρασή της και να βάλουμε σε σειρά προτεραιότητας τις ενέργειες αντίδρασης. Αυτό θα γίνει δυνατό μόνο με ανάλυση όλων των διαθέσιμων δεδομένων. Για παράδειγμα, οι ενέργειές μας θα εξαρτηθούν από το βαθμό πρόσβασης που απέκτησε ο εισβολέας και από το βαθμό εμπιστοσύνης που έχουμε στην ανάλυση αυτής της πληροφορίας από το σύστημα,

Η αντίδραση πρέπει να περιλαμβάνει την εγγραφή της κατάστασης του συστήματος που είναι ο στόχος και περιέχει καταγραφή των εξής:

- Όλες τις τρέχουσες δικτυακές συνδέσεις
- Όλες τις εν ενεργεία διαδικασίες
- Τους ενεργούς χρήστες που είναι εντός συστήματος
- Όλα τα αρχεία που βρίσκονται σε χρήση (αρχεία πιθανότατα να σβηστούν αν μια διαδικασία τελειώσει με τη διακοπή της δικτυακής σύνδεση)
- Δεδομένα από την κύρια μνήμη ή την cache, που αλλάζουν συνεχώς

Backup των υπό επίθεση συστημάτων

Λήψη τουλάχιστον δύο backup του συστήματος ή των συστημάτων που τους έχει γίνει επίθεση, καθώς και των αρχείων των χρηστών στα συστήματα αυτά. Κατόπιν, η επανάκτηση των δεδομένων μπορεί να γίνει από το backup μέσο για επιπλέον ανάλυση και μελέτη. Επίσης, το backup θα αποτελέσει και το αποδεικτικό στοιχείο για αυτές τις ενέργειες.

Χρειάζεται ιδιαίτερη προσοχή στα παρακάτω:

- Ασυνήθης μεγάλη δραστηριότητα του σκληρού δίσκου, που συμβαίνει στη διάρκεια του backup, μπορεί να γίνει αντιληπτή
- Ο εισβολέας είναι πιθανό να έχει εγκαταστήσει πρόγραμμα Trojan που θα σβήσει τα log αρχεία. Για παράδειγμα, μπορεί να έχει γίνει μετατροπή στο πρόγραμμα backup έτσι ώστε αν δεν απαντήσει στο ping κάποιος router, τότε να δοθεί εντολή για καταστροφή των δεδομένων του δίσκου. Αν το σύστημα βγει εκτός δικτύου για έλεγχο, τότε ίσως να χαθούν όλα τα log αρχεία.

Απομόνωση των υπό επίθεση συστημάτων
Αυτό μπορεί να επιτευχθεί με:

Μεταφορά των backup δεδομένων σε ένα προσωρινό σύστημα (test system) που είναι απομονωμένο από τα λειτουργικά μας συστήματα και αποκατάσταση (restore) του υπό επίθεση συστήματος στο test σύστημα

Αποσύνδεση των συστημάτων στα οποία υπάρχει εισβολή και ανάλυση δεδομένων απευθείας στους hosts, έχοντας πάντα στο μυαλό μας ότι αυτό θα καταστρέψει την αρχική πηγή πληροφορίας

Αναζήτηση σε άλλα συστήματα για ίχνη εισβολής

Οι εισβολείς συχνά δημιουργούν πολλά σημεία εισόδου σε ένα δίκτυο, από τη στιγμή που θα αποκτήσουν πρόσβαση. Εάν ανιχνευτεί μια επίθεση ή εισβολή, πρέπει να ελέγξουμε όλα τα άλλα συστήματα που είναι "παρόμοια" με το σύστημα που έχει προσβληθεί.

Ο όρος παρόμοια μπορεί να έχει ποικίλες ερμηνείες ανάλογα με το λειτουργικό περιβάλλον και περιλαμβάνει

- Συστήματα που βρίσκονται στο ίδιο διάστημα IP διευθύνσεων ή στο ίδιο υποδίκτυο. Οι εισβολείς πραγματοποιούν σαρώσεις (scans) σε πολλαπλά διαστήματα δικτυακών διευθύνσεων για να εντοπίσουν τρωτά σημεία στην ασφάλεια των συστημάτων.
- Συστήματα που βρίσκονται στο ίδιο "ασφαλές" domain. Τα συστήματα αυτά παρέχουν πρόσβαση σε χρήστες άλλων συστημάτων εντός του domain χωρίς να χρειάζεται επιπλέον authentication.
- Συστήματα που έχουν τουλάχιστον μια κοινή δικτυακή υπηρεσία (service). Οι εισβολείς συνήθως ελέγχουν για τις πιο γνωστές υπηρεσίες όπως το DNS (Domain Name System), FTP (File Transfer Protocol), HTTP (Hyper-Text Transfer Protocol) και SMTP (Simple Mail Transfer Protocol).
- Συστήματα που έχουν το ίδιο λειτουργικό σύστημα.
- Συστήματα τα οποία μοιράζονται το ίδιο σύστημα αρχείων δίνοντας χώρο αποθήκευσης σε προσβεβλημένα συστήματα ή χρησιμοποιώντας χώρο αρχείων από τέτοια συστήματα.

Εξέταση ηλεκτρονικών αρχείων συμβάντων που δημιουργούνται από firewalls, συστήματα δικτυακών αισθητήρων και δρομολογητές

Οι επιθέσεις συχνά αφήνουν ίχνη πληροφορίας που είναι σε θέση να οδηγήσουν τον έμπειρο αναλυτή, στο σύστημα που χρησιμοποίησε ο εισβολέας για να πετύχει την επίθεση. Τέτοια ίχνη περιλαμβάνουν logs και αρχεία επαλήθευσης, αρχεία που

δημιούργησε και άφησε ο εισβολέας, πληροφορία για την χρήση εξυπηρετητών και εφαρμογών που χρησιμοποιήθηκαν για την επίθεση μέσα στο δίκτυο.

Τα logs από firewall, συστήματα δικτυακών αισθητήρων και δρομολογητές μένουν συνήθως άθικτα και περιέχουν πολύτιμες πληροφορίες, ακόμα και αν ο εισβολέας αποκτήσει τοπική πρόσβαση στο σύστημα και δικαιώματα διαχειριστή (administrator), διαγράφοντας τα τοπικά logs για να αποκρύψει πληροφορίες. Αν γίνει σωστή χρήση και αρχικοποίηση, αυτά τα συστήματα εύκολα καταγράφουν τις συνδέσεις και την κίνηση μηνυμάτων, που δημιουργούνται από τον εισβολέα.

Χρησιμοποιώντας πληροφορίες από το παραπάνω βήμα ανάλυσης (μαζί με ημερομηνία, χρόνο και τα υπό επίθεση συστήματα) μπορούμε να εντοπίσουμε σχετικές εγγραφές στα logs που αποκαλύπτουν περισσότερο λεπτομερείς πληροφορίες για την εισβολή. Καλό θα ήταν να ελέγχουμε για παρεμφερείς συνδέσεις, που συμπεριλαμβάνουν συνδέσεις από την ίδια πηγή ή που έχουν τον ίδιο προορισμό.

Αναγνώριση των μεθόδων που χρησιμοποιήθηκαν στην επίθεση.

Συνήθως το είδος της επίθεσης που χρησιμοποιήθηκε το βρίσκουμε με μελέτη των logs εξυπηρετητών δρομολογητών και firewalls.

Οι εισβολείς πραγματοποιούν έναν αριθμό διαφορετικών επιθέσεων ή σαρώσεων για την παρουσία μιας συγκεκριμένης ευπάθειας, πριν αποκτήσουν πρόσβαση στον κόμβο. Ανάλογα με το πόσο καλά έχει στηθεί το σύστημα ανίχνευσης τα logs του συστήματος και του δικτυακού ανιχνευτή πιθανότατα θα περιέχουν:

- Μηνύματα άρνησης πρόσβασης εάν ο εισβολέας προσπαθήσει να μαντέψει κωδικούς
- Μηνύματα που υποδεικνύουν γνωστά τρωτά όπως η εντολή του UNIX sendmail "wiz"
- Άρνηση πρόσβασης σε συγκεκριμένες εφαρμογές που συλλέγεται από κάποιο εγκατεστημένο εργαλείο, όπως το TCP Wrapper

Επίσης στοιχεία όπως ημερομηνία, ώρα και πηγή μπορούν να αποδειχτούν χρήσιμα.

Υπάρχει η δυνατότητα ανίχνευσης της διαγραφής των logs,σε περίπτωση που ο εισβολέας επιχειρήσει να σβήσει τα logs και να εξαφανίσει τα ίχνη

του. Σε αυτήν την περίπτωση μας ειδοποιεί ότι κάτι ύποπτο συμβαίνει στο σύστημα και χρειάζεται να αναλύσουμε περαιτέρω.

Αναγνώριση των ενεργειών του εισβολέα κατά την πρόσβαση στο σύστημα

Είναι απαραίτητο η ανάλυση να μας οδηγήσει στον τρόπο με τον οποίο ο εισβολέας επιτέθηκε και απέκτησε πρόσβαση στα συστήματα μας. Αυτό δεν μπορεί να γίνει όμως, παρά μόνο με την σωστή αξιολόγηση της διαθέσιμης πληροφορίας. Σε πολλά συστήματα μπορούμε εύκολα να ανιχνεύσουμε προσπάθειες εγγραφής και μετατροπής αρχείων, ενώ δυστυχώς η ανάγνωση (πιθανά κρίσιμων δεδομένων) σπανίως καταγράφεται λόγω της μεγάλης αλληλεπίδρασης αυτής της πρόσβασης (read access).

Χωρίς να χρειαστούμε επιπλέον πληροφορίες, πρέπει να υποθέσουμε ότι αν ο εισβολέα ς αποκτήσει πρόσβαση στο σύστημα, είναι σε θέση να έχει πλήρη έλεγχο στον προσβεβλημένο κόμβο. Για αυτό πρέπει να αναλύσουμε το χειρότερο δυνατό σενάριο για την ζημιά που θα δημιουργηθεί.

Για να ανιχνεύσουμε το τι έκανε ο εισβολέας στο σύστημα μπορούμε να:

- Αναλύσουμε διαφορεηκά log αρχεία
- Συγκρίνουμε τα checksums γνωστών και έμπιστων αρχείων με τα αρχεία στο σύστημα που έχει προσβληθεί

- Χρησιμοποιήσουμε επιπλέον εργαλεία ανίχνευσης και ανάλυσης επιθέσεων
-

Είναι ιδιαίτερα σημαντικό να έχουμε ένα ασφαλές και κρυπτογραφημένο checksum για να κάνουμε τη σύγκριση με αρχεία που ίσως να έχουν αλλοιωθεί. Έτσι μπορούμε να διαπιστώσουμε αν ο εισβολέας αλλοίωσε τον πυρήνα του λειτουργικού συστήματος.

Παραδείγματα ιχνών που αφήνουν οι εισβολείς περιλαμβάνουν:

- αλλαγές στα log αρχεία για να αποκρύψουν την παρουσία τους
- ενέργειες για την αλλοίωση ενός εργαλείου του συστήματος, ώστε να μην καταγραφούν εφαρμογές, που ο εισβολέας εγκατέστησε με σκοπό ων προστασία από εύκολη ανίχνευση του
- Εφαρμογές Trojan, back doors ή νέες εκδόσεις εντολών του συστήματος.

Κεφάλαιο 10

Κανόνες ασφάλειας (Roadmap)

Στο κεφάλαιο αυτό παραθέτουμε μερικούς βασικούς κανόνες τόσο για την ενίσχυση της ασφάλειας, όσο και για την αντιμετώπιση των επιθέσεων μέσα από τον προσδιορισμό των "πολύτιμων πόρων" την εκτέλεση ελέγχων ασφαλείας και την δημιουργία διαδικασιών αντιμετώπισης. Με την επεξεργασία των στοιχείων που μπορούν να συγκεντρωθούν μετά από τον έλεγχο με τα εργαλεία που αναφέρονται μπορούμε να προχωρήσουμε στην περιγραφή κανόνων για τον σχεδιασμό, υλοποίηση, βελτίωση και αναθεώρηση της ασφάλειας.

10.1. Σχεδιασμός της ασφάλειας στο site

Τεκμηρίωση της ανάγκης για επένδυση στην ασφάλεια

- Εύρεση των πόρων που πρέπει να προφυλαχτούν, ανάλυση της αξίας των πόρων, ανάλυση των κινδύνων που μπορεί να αντιμετωπίσουν οι πόροι
- Τεκμηρίωση της δημιουργούμενης απειλής από προσπάθειες εισβολής στο site. Καταγραφή των περιπτώσεων εισβολής με ένα παθητικό δικτυακό αναλυτή στον κορμό του δικτύου (passive network sniffer)
- Έλεγχος με εργαλεία εξακρίβωσης προβλημάτων ασφάλειας (π.Χ. ISS, Netsonar, SATAN) , εναντίον του site από την εξωτερική πλευρά της περιμέτρου
- Συζήτηση για τον αντίκτυπο στην φήμη, λειτουργία, αξιοπιστία και κέρδη του επιχειρηματικού οργανισμού από την κοινοποίηση αναφορών περιστατικών επιθέσεων και εισβολή στο site
- Συζήτηση για τον αντίκτυπο στην φήμη, λειτουργία, αξιοπιστία και κέρδη από πιθανή επίθεση άρνησης παροχής υπηρεσίας (denial of service attack)
- Συλλογή και παρουσίαση στοιχείων για την συχνότητα των επιθέσεων στο Internet, τις εταιρίες που έχουν δεχτεί επιθέσεις και την ζημιά που έπαθαν

Προσδιορισμός του σκοπού της ασφάλειας και των πόρων που θα διαφυλάξει

Πρέπει να γίνουν ερωτήσεις και συζητήσεις μέσα στον οργανισμό για τα ακόλουθα:

- Τι περιμένουν οι χρήστες και οι πελάτες από την υλοποίηση των διαδικασιών διαφύλαξης της ασφάλειας;

- Αν δεν λάβουμε σοβαρά υπόψη μας την ασφάλεια θα χάσουμε πελάτες; Ή αν λάβουμε πολύ σοβαρά την ασφάλεια η λειωυργικότητα είναι ανεκτή;
- Πόσος χρόνος ή πόσα χρήματα χάθηκαν όσο διάστημα έμειναν τα συστήματά μας εκτός λειτουργίας τον περασμένο χρόνο;
- Υπάρχει ανησυχία για επιθέσεις από το εσωτερικό της περιμέτρου; Πόσο εμπιστεύεσαι τους χρήστες σου;
- Οι περισσότεροι χρήστες σου είναι μέσα ή έξω από την περίμετρο;
- Πόσο ευπαθή δεδομένα υπάρχουν στα υπολογιστικά συστήματα; Τι θα χάσει ο οργανισμός αν η πληροφορία αυτή αλλοιωθεί ή κλαπεί;
- Υπάρχει η ανάγκη διαφορετικού επιπέδου ασφάλειας στα διάφορα τμήματα του οργανισμού (λογιστήριο, τμήμα προσωπικού, τμήμα έρευνας, τμήμα υποστήριξης πελατών, εργαστήρια κλπ);
- Πόσο έχει υποφέρει ο οργανισμός από αρνητική δημοσιότητα λόγω έλλειψης ενός σχεδιασμένου συστήματος προστασίας;
- Υπάρχουν οδηγίες και κανονισμοί ασφάλειας στον οργανισμό; Γίνεται προσπάθεια να τηρηθούν;
- Επικρατούν σε περίπτωση σύγκρουσης οι απαιτήσεις της δουλειάς σε σχέση με τις απαιτήσεις της ασφάλειας; Αν ναι είναι αυτό που θέλουμε;
- Πόσο σημαντικό για την λειτουργία του οργανισμού είναι η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων και πληροφοριών;
- Είναι οι επιλογές που έχουμε κάνει συνεπείς με ης επιχειρησιακές ανάγκες και τα οικονομικά του οργανισμού;

Ορισμός των κύριων σημείων επιτυχούς προγράμματος επαγρύπνησης για την ασφάλεια

- Εξασφάλιση της εκπαίδευσης του προσωπικού μέσω διαφορετικών μέσων (σεμινάρια, ιστοσελίδες, online τεκμηρίωση, video, πρακτική)
- Παροχή εκπαίδευσης σε σταθερή βάση και μέσω του προγράμματος ενημέρωσης νέων υπαλλήλων
- Παροχή εκπαίδευσης στο προσωπικό υποστήριξης, στους χρήστες και τους managers
- Μέρος της εκπαίδευσης πρέπει να είναι τα εικονικά συμβάντα επίθεσης για την εξακρίβωση της ικανότητας αντιμετώπισης, από το προσωπικό υποστήριξης και τους χρήστες, των περιστατικών επιθέσεων στην ασφάλεια.
- Διαρκή ενημέρωση των χρηστών και του προσωπικού υποστήριξης με οδηγίες διάγνωσης και αντιμετώπισης περιστατικών και την τρέχουσα τάση των επιθέσεων σε υπολογιστικά και δικτυακά συστήματα.
- Συχνή αναθεώρηση των διαδικασιών εκπαίδευσης ώστε να είμαστε σίγουροι πως είναι σχετικές και ενημερωμένες.

Προσδιορισμός των κύριων στοιχείων μίας καλής υποδομής ασφάλειας

- Ισχυρή δέσμευση της διοίκησης για την παροχή των απαραίτητων πόρων για την υλοποίηση του σχήματος ασφάλειας και της διασφάλισης της σχετικής πολιτικής και των διαδικασιών
- Ύπαρξη προσωπικού αφοσιωμένο ειδικά στην ασφάλεια
- Ύπαρξη ενός καλώς ορισμένου πλάνου ασφάλειας
- Δημιουργία ενός καλοσχεδιασμένου προγράμματος ενημέρωσης-εκπαίδευσης
- Σχεδιασμός, υλοποίηση και τεκμηρίωση ξεκάθαρης πολιτικής και διαδικασιών ασφάλειας και ενημέρωση όλων στον οργανισμό

- Δημιουργία καναλιών επικοινωνίας ανάμεσα στις σχετικές με ασφάλεια ομάδες
- Ύπαρξη ομάδας αντιμετώπισης επιθέσεων
- Προσδιορισμένη περίμετρος και έλεγχος της ασφάλειας στην εσωτερική και εξωτερική προσπέλαση
- Δημιουργία ενός ολοκληρωμένου συστήματος από υπολογιστικά και δικτυακά εργαλεία για την παρακολούθηση και βελτίωση της ασφάλειας

Κοινά προβλήματα στην υλοποίηση του πλάνου ασφάλειας

- Έλλειψη προσωπικού αποκλειστικά για την υλοποίηση, παρακολούθηση και βελτίωση της ασφάλειας
- Το προσωπικό υποστήριξης δεν έχει την απαραίτητη υποστήριξη από την διοίκηση, αλλά και την ισχύ να εφαρμόσει τα απαραίτητα μέτρα ασφάλειας
- Δεν εφαρμόζονται τα patches των κατασκευαστών για την αντιμετώπιση γνωστών προβλημάτων ασφάλειας
- Δεν ελέγχεται η προσπέλαση στους εσωτερικούς κόμβους
- Δεν εφαρμόζονται ικανοποιητικά συστήματα πιστοποίησης και εξουσιοδότησης για την απομακρυσμένη πρόσβαση
- Δεν εφαρμόζονται οι προκαθορισμένες διαδικασίες όταν εγκαθίστανται νέες δικτυακές συσκευές στον οργανισμό
- Δίνεται έμφαση στην μέθοδο της "ασφάλειας μέσω της αφάνειας"
- Δεν γίνεται χρήση υπολογιστικών και δικτυακών εργαλείων παρακολούθησης και εξακρίβωσης διείσδυσης.

10.2. Υλοποίηση της ασφάλειας

Ορισμός των τυπικών καθηκόντων του προσωπικού ασφαλείας

- Προτείνουν και υλοποιούν τα εσωτερικά standard ασφάλειας
- Σχεδιάζουν, υλοποιούν, διασφαλίζουν και τεκμηριώνουν την επίσημη πολιτική ασφάλειας
- Ελέγχουν, παρακολουθούν και δοκιμάζουν τα υπολογιστικά και δικτυακά συστήματα για πιθανά προβλήματα παραβίασης της ασφάλειας
- Παρακολουθούν τις ηλεκτρονικές λίστες και τα νέα (lists, newsgroups και ανταποκρίνονται κάνοντας ρυθμίσεις στα συστήματα, για την αντιμετώπιση στις νέες επιθέσεις και τάσεις που εμφανίζονται διεθνώς.

- Επιθεωρούν σε καθημερινή βάση, τα αρχεία με τις καταγραφές παραβίασης ασφαλείας των συστημάτων (security logs) και διερευνούν τυχόν ανωμαλίες
- Δοκιμάζουν, εγκαθιστούν και συντηρούν εργαλεία για την ασφάλεια της υποδομής.
- Δοκιμάζουν και εγκαθιστούν patches κατασκευαστών που διορθώνουν προβλήματα ασφάλειας.
- Παραμένουν ενήμεροι στην τεχνολογία ασφάλειας και στις πιθανές απειλές
- Παρέχουν διερεύνηση, συντονισμό, αναφορές και συνεχή παρακολούθηση σε περιστατικά παραβίασης της δικτυακής ασφάλειας
- Συμμετέχουν στην επιθεώρηση και ανάλυση εσωτερικών projects που μπορεί να έχουν επιπτώσεις στην ασφάλεια του οργανισμού
- Συνεισφέρουν στην ενημέρωση των εσωτερικών και εξωτερικών συνεργατών και πελατών για την πολιτική και τις διαδικασίες ασφάλειας που έχει ο οργανισμός.

Διασφάλιση και τεκμηρίωση της αποτελεσματικότητας της υποδομής ασφάλειας μέσω μεθοδικών και λεπτομερών εξετάσεων (audits)

- Έλεγχος της διαδικασίας διατήρησης της ασφάλειας κατά την εγκατάσταση νέου εξοπλισμού, ώστε να επιβεβαιώνεται η συμμόρφωση με την υπάρχουσα πολιτική και τα standards που αφορούν εγκατάσταση νέου εξοπλισμού
- Τακτική αυτόματη εξέταση συστημάτων για την διαπίστωση της μη εξουσιοδοτημένης "επισκεψης" από εισβολέα
- Δημιουργία τυχαίων ελέγχων για την διαπίστωση της συμμόρφωσης με την πολιτική ασφάλειας και την αντιμετώπιση μιας κατηγορίας προβλημάτων (π.χ. η παρουσία τρωτών σημείων στην ασφάλεια που ανακοινώθηκε από κάποιον κατασκευασή).

  Δημιουργία νυχτερινών αυτόματων έλεγχων σε κρίσιμα αρχεία, (π.χ. password file, αρχεία μισθοδοσίας, ιστοσελίδες κ.ά) με δημιουργία αντιγράφων των αρχείων αυτών, ώστε να μπορεί να εξακριβωθεί η πε ρίπτωση παραβίασης της ασφάλειας τις νυχτερινές ώρες και πριν προλάβει ο επιτιθέμενος να αλλοιώσει τα στοιχεία του log file.

Έλεγχοι στην κίνηση των λογαριασμών των χρηστών, για τον εντοπισμό ανενεργών, άκυρων ή παράνομων λογαριασμών

Περιοδικές εικονικές επιθέσεις για τον έλεγχο της συνολικής ασφάλειας του οργανισμού.

Εργαλεία που μπορούν να χρησιμοποιηθούν για την ασφάλεια

- Εργαλεία ελέγχου βασισμένα σε εξυπηρετητές, όπως COPS, NCARP, crack, Tiger, Tripwire, logcheck, tklogger, Safesuite, NetSonar
- Εργαλεία ανάλυσης δικτυακής κίνησης και ανίχνευσης εισβολής, όπως tcpdump, sysniff, NetRanger, NOCOL, NFR, RealSecure, Shadow
- Εργαλεία διαχείρισης και βελτίωσης ασφάλειας, όπως crack, localmail, smrsh, logdaemon, npasswd, ορ, passwd +, S4-kit, sfingerd, sudo, swatch, watcher. Wuftpd, LPRng
- Εργαλεία φιλτραρίσματος (filtering), firewall, proxy, όπως fwtk, ipfilter, ipfirewall, portmap v3, SOCKS, tcp _ wrappers, smapd
- Εργαλεία ελέγχου βασισμένα στο δίκτυο, όπως nmap, nessus, SATAN, Safesuite
- Εργαλεία κρυπτογράφησης, όπως md5, md5chech, PGP, rpem, UFCcrypt
- Εργαλεία για password μίας χρήσης, όπως OPIE, S/Key
- Εργαλεία απομακρυσμένης εξουσιοδοτημένης προσπέλασης, όπως RADIUS, TACACS+, SSL, SSH, Kerberos

Ορισμός των κύριων σημείων που πρέπει να τηρηθούν στην αντιμετώπιση ενός περιστατικού ασφάλειας

- Πρέπει να ακολουθηθούν η πολιτική και οι διαδικασίες του οργανισμού
- Η επικοινωνία με τους υπεύθυνους, πρέπει να γίνεται εκτός δικτύου δεδομένων (π.χ. τηλέφωνο) για την περίπτωση που ο εισβολέας μπορεί να παρακολουθεί την δικτυακή κίνηση
- Πρέπει να καταγράφονται όλες οι ενέργειες (τα αρχεία που τροποποιήθηκαν, οι διεργασίες του συστήματος που σταμάτησαν κλπ)
- Πρέπει να αντιγραφούν τα αρχεία που έχουν καταγραφεί κινήσεις των εισβολέων σε offline χώρο

Εφαρμογή άμεσων και οικονομικών λύσεων για την βελτίωση της ασφάλειας

- Τεκμηρίωση και δημοσιοποίηση των διαδικασιών που αναμένεται να ακολουθήσει η ομάδα ασφάλειας
- Διαμόρφωση του configuration των περιμετρικών δρομολογητών, να αρνούνται την περιττή εισερχόμενη κυκλοφορία
- Συντήρηση του sendmail σε ενημερωμένη έκδοση με σωστή διαμόρφωση. Χρήση φίλτρων για την προστασία από attachments με ιούς
- Χρήση δωρεάν εργαλείων για τον έλεγχο της ασφάλειας με προσπάθεια εισβολής στα συστήματα του οργανισμού.
- Εγκατάσταση δωρεάν εργαλείων σε εξυπηρετητές και στο δίκτυο για την παρακολούθηση, έλεγχο και ανάλυση της δικτυακής κυκλοφορίας σε κρίσιμους κόμβους.
- Παρακολούθηση σε καθημερινή βάση των εγγραφών του συστήματος (logs)

10.3. Παγίδες και τρωτά σημεία

Τα εκτελέσιμα και οι κατάλόγοι που συχνά γίνονται στόχος εισβολέων

Αν υπάρχει υποψία πως τα συστήματα του οργανισμού έχουν δεχθεί εισβολή, υπάρχει σοβαρό ενδεχόμενο κάποιο από τα παρακάτω αρχεία του συστήματος να έχει αλλοιωθεί:

/bin/login
/usr/ etc/in.telnetd
/usr/ etc/in. ftpd
/usr/ etc/in. tftpd
/usr/ucb/netstat
/bin/ps
/bin/ls
/usr/sbin/ifconfig
/bin/df
/usr/lib/libc.a
/usr/ucb/cc

Ή μπορεί να έχει αλλοιωθεί κάηοιο από τα παρακάτω αρχεία:
/.rhosts
/ etc/hosts.equiv
/bin/.rhosts
/etc/passwd
/etc/group
/var/yp/67 (nis maps)
root environment files (.login, .cshrc, .profile, .forward)

Οι εισβολείς συνήθως κρύβουν τα αρχεία τους σε προσωρινά directories όπως: /tmp, /var/tmp, /etc/tmp, /usr/spool, and /usr/líb/cron.

Γνώση των συνήθων τρόπων επιθέσεων

- Εκμετάλλευση τρωτών σημείων στον κώδικα του λογισμικού κατασκευαστών
- Εκμετάλλευση των τρωτών σημείων σε cgi-bin
- Βομβαρδισμός με emails, spamming, relaying μέσω άλλων sites
- Εκμετάλλευση ftp και web εξυπηρετητών που η εγκατάσταση και διαμόρφωση δεν έχει γίνει προσεκτικά

- Εκμετάλλευση των τρωτών σημείων στο named/BIND
- Εκμετάλλευση των agents μεταφοράς email και των προγραμμάτων ανάγνωσης email (n.x.MS-OutIook, Pine)
- Επίθεση τύπου "άρνηση παροχής υπηρεσίας" (Denial oí Service attack) με διάφορες μεθόδους
- Αποστολή σε email attachments εκτελέσιμου κώδικα που "τρέχει" χωρίς την συγκατάθεση του χρήστη

Αντιμετώπιση των κοινών προβλημάτων στην υλοποίηση της ασφάλειας της περιμέτρου

- Η διοίκηση και το προσωπικό ασφάλειας, συχνά υποθέτουν πως με την χρήση ενός firewall έχουν ικανοποιητική ασφάλεια, χωρίς να χρειάζεται περαιτέρω έλεγχος στο εσωτερικό δίκτυο.
- Μέλη του οργανισμού ζητούν την εγκατάσταση τηλεφωνικών γραμμών και modem στο χώρο εργασίας τους ώστε να μπορούν να επικοινωνούν είτε με ISPs, είτε για να εγκαταστήσουν δυνατότητα τηλεφωνικής προσπέλασης στο σταθμό εργασίας τους από το σπίτι. Με τον τρόπο αυτό υπάρχει αποφυγή της όποιας ασφάλειας έχει εγκατασταθεί για την ασφάλεια της περιμέτρου.
- Μερικές δικτυακές υπηρεσίες (π.χ. ftp, tftp, http, sendmail) που προορίζονται για εσωτερικούς κόμβους, περνούν από τα σημεία ελέγχου της περιμετρικής ασφάλειας χωρίς έλεγχο.
- Οι firewall κόμβοι ή δρομολογητές δέχονται συνδέσεις τόσο από το εσωτερικό δίκτυο όσο και από το DMZ (DeMilitarized Zone) δίκτυο.
- Επειδή οι access lists στους δρομολογητές συνήθως ρυθμίζονται λανθασμένα (λόγω πολυπλοκότητας των κανόνων όταν αυξάνει το μέγεθος τους), επιτρέπεται να περάσουν άγνωστες και επικίνδυνες υπηρεσίες.
- Οι καταγραφές των αρχείων του συστήματος για τις εξωτερικές συνδέσεις στην περίμετρο είτε δεν είναι επαρκείς, είτε δεν ελέγχονται σε τακτική βάση
- Συχνά δημιουργούνται κωδικοποιημένα τούνελ επικοινωνίας από την περίμετρο του δικτύου χωρίς να λαμβάνεται υπόψη η ασφάλεια των άκρων του τούνελ.

Κεφάλαιο 11

Κοιτώντας στο μέλλον

11.1. Internetworking Protocols - Σύγχρονη Κρυπτογραφία

Τα περισσότερα από τα πρωτόκολλα που χρησιμοποιούνται σήμερα δεν έχουν αλλάξει από τότε που ορίστηκαν, την εποχή του ARPA του ερευνητικού και εκπαιδευτικού δικτύου, που η εμπιστοσύνη ήταν ο κανόνας. Για να έχουμε μία ασφαλή βάση για τις κρίσιμες μελλοντικές εφαρμογές του διαδικτύου, πρέπει να αντιμετωπιστούν τα σοβαρά ελαττώματα που υπάρχουν σήμερα. Κύρια η έλλειψη της απόκρυψης (encryption) για την ασφαλή μετάδοση δεδομένων και την διασφάλιση της αυθεντικότητας της πληροφορίας, η έλλειψη της κρυπτογραφικής πιστοποίησης για την διασφάλιση της αυθεντικότητας της πηγής που προέρχεται η πληροφορία και η έλλειψη της δυνοτότητας cryptographic checksum για την διασφάλιση της ακεραιότητας των αποθηκευμένων δεδομένων, αλλά και της ίδιας της πληροφορίας δρομολόγησης. Τα νέα πρωτόκολλα που προτείνονται από την IETF (lnternet Engineering Task Force), όπως το Ipng ή αλλιώς Ipv6 μπορούν να οδηγήσουν σε δημιουργία

ασφαλέστερου περιβάλλοντος. Στο μέλλον, τα πρωτόκολλα πιστοποίησης θα υπόστηρίζονται σταδιακά από τεχνολογίες που σήμερα πιστοποιούν άτομα (π.χ. *στο* εργασιακό τους περιβάλλον), με την χρήση έξυπνων καρτών, αναγνώστες δακτυλικών αποτυπωμάτων, αναγνώριση προσώπου, ίριδας, φωνής κλπ.

Ο σχεδιασμός, η ανάλυση και η υλοποίηση πρωτοκόλλων θα είναι το αντικείμενο συνεχούς έρευνας. Ο στόχος, που είναι ένα 100% ασφαλές πρωτόκολλο (ασφαλές όσο και ο κρυπτογραφικός αλγόριθμος που το υποστηρίζει), δεν είναι μακριά.

11.2. Ανίχνευση Εισβολής

Η έρευνα σε αυτό τον τομέα διεξάγεται για την βελτίωση της δυνατότητας των δικτυακών συστημάτων να διακρίνουν πως δέχτηκαν επίθεση. Η ανίχνευση των παραβιάσεων αναγνωρίζεται σαν μια δύσκολη ερευνητική περιοχή που βρίσκεται ακόμα στην αρχή της. Υπάρχουν δύο περιοχές στον τομέα αυτό, η ανίχνευση ανωμαλιών και η αναγνώριση προτύπων.

Η έρευνα στην ανίχνευση ανωμαλιών βασίζεται στον ορισμό προτύπων «κανονικής» συμπεριφοράς, σε δίκτυα, εξυπηρετητες, χρήστες και στην ανίχνευση συμπεριφορών που είναι κατά πολύ διαφορετικές (ανωμαλία). Τα πρότυπα της κανονικής συμπεριφοράς συνήθως προσδιορίζονται συγκεντρώνοντας στοιχεία για ένα χρονικό διάστημα κατάλληλο για την εξασφάλιση ενός τυπικού δείγματος συμπεριφοράς των εξουδιοδοτημένων χρηστών και των διαδικασιών (processes) των συστημάτων. Η βασική δυσκολία που πρέπει να αντιμετωπιστεί, είναι πως η κανονική συμπεριφορά είναι ευμετάβλητη εξαιτίας πληθώρας αβλαβών ενεργειών που μπορούν να επιτρέψουν παραβιάσεις. Πολλές από τις ενέργειες ενός εισβολέα δεν διαφοροποιούνται από τις ενέργειες εξουσιοδοτημένων χρηστών.

Η δεύτερη μεγάλη περιοχή είναι η αναγνώριση προτύπων. Ο στόχος εδώ είναι να αναγνωριστούν ακολουθίες γεγονότων στην συμπεριφορά του δικτύου, των εξυπηρετητών και των χρηστών,που προέρχονται από γνωστά σενάρια επιθέσεων. Ένα πρόβλημα σε αυτή την προσέγγιση είναι η πληθώρα των διαφορετικών σεναρίων που προκύπτουν από την διαφοροποίηση της στρατηγικής που εφαρμόζει ο κάθε εισβολέας κάνοντας χρήση της ίδιας μεθόδου. Ένα δεύτερο πρόβλημα είναι πως νέα είδη επιθέσεων που δεν είναι γνωστά τα μοτίβα επίθεσης, δηλαδή η «υπογραφή» τους, δεν μπορουν να αντιμετωπιστούν με αυτή την προσέγγιση.

Τέλος πρέπει να αναφερθεί πως υπάρχει ανάγκη να βρεθούν εργαλεία και τεχνικές για την αναγνώριση επιθέσεων που προέρχονται από διαφορετικά μέρη του Internet αλλά συντονίζονται από ένα σημείο (Distributed Denial of Service-DdoS), καθώς και πρωτόκολλα που να επιτρέπουν την ιχνηλασία της αρχής των επιθέσεων.

11.3. Software Engineering και ικανότητα επιβίωσης των συστημάτων

Οι τρέχουσες μέθοδοι δημιουργίας λογισμικού δεν έχουν να επιδείξουν αξιόλογα επιτεύγματα, σε ότι αφορά θέματα ασφάλειας. Τις περισσότερες φορές το θέμα της ασφάλειας είναι μεταγενέστερο του βασικού σχεδιασμού του λογισμικού. Η δημιουργία ασφαλών λογισμικών, πρέπει να έχει την δυνατότητα να επιδεικνύει το λογισμικό συμπεριφορά που συνεισφέρει στην ικανότητα επιβίωσης του συστήματος παρά τις επιθέσεις που δέχεται.

Σαν ικανότητα επιβίωσης, ορίζεται η ικανότητα ενός συστήματος να συνεχίζει να εκτελεί τις κρίσιμες λειτουργίες ,με τον χρονοπρογραμματισμό που έχει οριστεί ,ακόμα και αν μέρος των πόρων του συστήματος έχουν δεχτεί επίθεση ή έχουν βλάβη .Ο όρος σύστημα έχει ευρεία έννοια και περιλαμβάνει και συστάδες από συστήματα και δίκτυα.

Αν και αρχές και μεθόδοι που έχουν να κάνουν με την ικανότητα επιβίωσης είναι χαρακτηριστικά των έμβιων όντων ,μπορούν να υλοποιηθούν με παραδοσιακές τεχνικές

της περιοχής της δημιουργίας λογισμικού και των υπολογιστικών συστημάτων ,όπως αξιοπιστία ,αντιμετώπιση σφαλμάτων ,επιβεβαίωση ορθότητας ,απόδοση και ασφάλεια συστημάτων .Η έρευνα κατευθύνεται σε δημιουργία μεθόδων ανοσοποίησης που θα διακινούν αυτόματα τις διορθώσεις των τρωτών ,σε ένα ολόκληρο δίκτυο ,για να διαφυλαχτούν όλα τα συστήματα από ένα νέο πρόβλημα ασφάλειας .Η έννοια της ανοσοποίησης μπορεί να γενικευθεί ώστε να συμπεριλάβει προσαρμόσιμα δίκτυα ,που αποτελούνται από

κατανεμημένα συνεργαζόμενα δικτυακά στοιχεία ,που ανταλλάσουν πληροφορίες για προβλήματα ασφαλείας και δραστικά αλλάζουν και προσαρμόζονται σαν αντίδραση απειλών εναντίον της ασφάλειας

11.4 Προγραμματισμός ιστοσελίδων και γλώσσες κειμένου (scripting languages)

Το να «κατεβάσεις» ενδιαφέρον ,πληροφοριακό και ψυχαγωγικό περιεχόμενο από τις σελίδες κόμβων του διαδικτύου ,τοπικά στον υπολογιστή είναι μία κύρια ενέργεια του net surfing .Το περιεχόμενο που έχει ενδιαφέρον από τη πλευρά της ασφάλειας έχει να κάνει με το «κατέβασμα»κώδικα που εκτελείται τοπικά .Το εκτελέσιμο περιεχόμενο μπορεί να παρέχει την αναμετάδοση μίας συνάντησης ,μουσική ,τρισδιάστατα γραφικά ή επικίνδυνο κώδικα που μπορεί να διαγράψει τα περιεχόμενα του δίσκου από τον

σταθμό εργασίας .Ο κώδικας είναι γραμμένος σε JAVA ή ActiveX και ονομάζεται applet(JAVA) ή Control Panel(ActiveX).

Οι γλώσσες προγραμματισμού για web,εισάγουν νέα προβλήματα στην ασφάλεια του διαδικτύου ,γιατί «κατεβαίνουν» ,αποθηκεύονται και εκτελούνται χωρίς να ελέγξεις το source code .Αυτό γίνεται απλά «σερφάροντας» στο διαδίκτυο ,χωρίς πολλές φορές ο χρήστης να αντιλαμβάνεται το γεγονός .Η JAVA έχει εσωτερικούς μηχανισμούς ασφάλειας ,αλλά οι ειδικοί στην ασφάλεια γνωρίζουν πώς να τους ξεπερνούν .Ο μηχανισμός για την εξασφάληση του κώδικα είναι η κρυπτογράφηση του checksum του κώδικα και η πιστοποίηση του από τον κατασκευαστή .Πάντως τα επόμενα χρόνια το πρόβλημα αυτό θα ενταθεί και ο μόνος εμφανής τρόπος προφύλαξης είναι η κρυπτογράφηση και η ετοιμότητα των χρηστών .

Βιβλιογραφία-Πηγές ενημέρωσης

Actually Useful Internet Security Techniques by LarryJ.Hughes Jr.
Applied Cryptography: Protocols, Algorithms and Source Code in C by Bruce Schneier
Building Internet Firewalls by Brent Chapman & Elizabeth D. Zwicky
Cisco IOS Network Security by Cisco Systems
DesigningNetwork Security by Mike Kaeo
Firewalls and Internet Security by Bill Cheswick &Steve Bellovin
Web Security Sourcebook by Avi rubin,Dan Geer and Marcus Ranum

http://www.itpolicy.gsa.gov/
http://www.cit.nih.gov/security.html
http://cs-www.ncsl.nist.gov/
http://www.phrack.com/
http://www.2600.com/
http://www.cert.org/