ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ: ΤΡΟΠΟΙ ΕΠΙΘΕΣΗΣ ΚΑΙ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΦΟΙΤΗΤΡΙΑ: ΨΟΥΧΛΟΥ ΙΣΙΔΩΡΑ
Α.Μ. 736

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΛΙΑΡΟΚΑΠΗΣ ΔΗΜΗΤΡΙΟΣ

ΑΡΤΑ ΑΥΓΟΥΣΤΟΣ 2024

CYBERSECURITY: ATTACK METHODS AND PROTECTION MEASURES IN CYBERSPACE

Εγκρίθηκε από τριμελή εξεταστική επιτροπή

Τόπος, Ημερομηνία

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Επιβλέπων καθηγητής

2. Μέλος επιτροπής

3. Μέλος επιτροπής

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Δηλώνω υπεύθυνα ότι το παρόν έγγραφο είναι προϊόν αυθεντικής και πρωτότυπης έρευνας και συγγραφής και δεν περιέχει λογοκλοπή. Όλα τα στοιχεία, ιδέες, κείμενα και πληροφορίες που χρησιμοποιήθηκαν, είτε αναφέρονται αυτούσια, είτε παραφρασμένα και έχουν καταγραφεί με σαφή και κατάλληλο τρόπο στο τέλος της εργασίας, στο παράρτημα της βιβλιογραφίας. Κανένα μέρος της παρούσας εργασίας δεν έχει αντιγραφεί από οποιαδήποτε άλλη πηγή χωρίς την κατάλληλη αναφορά και αναγνώριση της πηγής αυτής.

Περιεχόμενα

ΠΕΡΙΛΗΨΗ

Η κυβερνοασφάλεια (cybersecurity) αποτελεί πλέον έναν κρίσιμο τομέα, αναγκαίο για την προστασία της ψηφιακής μας ζωής και των προσωπικών και επαγγελματικών δεδομένων. Σκοπός της παρούσης εργασίας είναι η μελέτη των κινδύνων που ελλοχεύουν στον κυβερνοχώρο**,** αλλά και των μέτρων προστασίας που μπορούν να εφαρμοστούν για την αντιμετώπισή τους.

Αναλυτικά, στο πρώτο κεφάλαιο παρουσιάζονται οι επίσημοι ορισμοί της κυβερνοασφάλειας καθώς και οι βασικές αρχές που την διέπουν. Επίσης, αναλύονται κατηγορίες απειλών και τύποι τρωτοτήτων που μπορεί να αντιμετωπίσει ένα σύστημα. Για την αντιμετώπιση αυτών των απειλών, η ανάλυση ρίσκου και η διαχείριση κινδύνου αποτελούν σημαντικό παράγοντα. Τέλος, τονίζεται η σημασία της ανάπτυξης πολιτικών ασφαλείας και εκπαίδευσης των χρηστών στην έγκαιρη αναγνώριση και απόκριση σε κυβερνοαπειλές.

Στο δεύτερο κεφάλαιο μελετώνται τύποι τρωτοτήτων που εκμεταλλεύονται οι παραβάτες και διερευνάται η πηγή προέλευσής τους. Ακόμη, παρουσιάζονται αναλυτικά τα είδη των επιθέσεων, η επικινδυνότητά τους, καθώς και οι μέθοδοι μέσω των οποίων οι επιθέσεις αυτές μπορούν να τελεστούν. Το κεφάλαιο κλείνει με την περιγραφή της ανατομίας μιας επίθεσης και των βημάτων που ακολουθούν οι θύτες για την επιτυχημένη εισβολή σε ένα υπολογιστικό σύστημα.

Το τρίτο κεφάλαιο εστιάζει στους βασικούς μηχανισμούς ασφαλείας που θα πρέπει να εφαρμόζει κάθε υπολογιστικό σύστημα ώστε να είναι σε θέσει να προστατεύσει επαρκώς τους πόρους του και να αντιμετωπίζει αποτελεσματικά επερχόμενες απειλές. Στη συνέχεια παρουσιάζεται η κρυπτογραφία ως το βασικό εργαλείο προστασίας του περιεχομένου της διακινούμενης πληροφορίας βρίσκοντας μεγάλη εφαρμογή στις ψηφιακές υπογραφές και στα πρωτόκολλα ασφαλείας δικτύων. Στο τελευταίο μέρος του κεφαλαίου εξετάζονται τα συστήματα ανίχνευσης εισβολών, ενός λογισμικού που εποπτεύει τα δίκτυα για την εξασφάλιση της ομαλής και ασφαλούς λειτουργίας τους.

Στο τέταρτο και τελευταίο κεφάλαιο της εργασίας πραγματοποιείται μια προσομοίωση επίθεσης έγχυσης κώδικα σε ιστοσελίδα που έχει δημιουργηθεί ειδικά για το σκοπό αυτό. Ακολουθούν πρακτικές βελτιστοποίησης της ασφάλειας του κώδικα αλλά και τεχνικές για την ασφάλεια του χρήστη.

Λέξεις – Κλειδιά: κυβερνοασφάλεια, κυβερνοχώρος, κυβερνοαπειλές, τρωτότήτες**,** μηχανισμοί ασφαλείας

ABSTRACT

The field of Cybersecurity has become a critical area, essential for protecting our digital lives, as well as our personal and professional data. The purpose of this paper is to study the risks lurking in cyberspace and the protective measures that can be applied to address them.

Specifically, the first chapter presents the official definitions of Cybersecurity and the basic principles that govern it. Additionally, categories of threats and types of vulnerabilities that a system may face are analyzed. Risk analysis and risk management are significant factors in addressing these threats. Finally, the importance of developing security policies and training users to promptly recognize and respond to cyber threats is emphasized.

In the second chapter, the types of vulnerabilities exploited by offenders are studied, and their origins are investigated. The chapter also presents a detailed analysis of the types of attacks, their severity, and the methods through which these attacks can be executed. The chapter concludes with a description of the anatomy of an attack and the steps perpetrators follow to successfully breach a computing system.

The third chapter focuses on the basic security mechanisms that should be implemented by any computing system to adequately protect its resources and effectively deal with incoming threats. Next, cryptography is presented as the fundamental tool for protecting the content of transmitted information, with significant applications in digital signatures and network security protocols. In the final part of the chapter, intrusion detection systems are examined, which are software solutions that monitor networks to ensure their smooth and secure operation.

In the fourth and final chapter of the paper, a simulation of a code injection attack on a specially created website is conducted. This is followed by practical methods for optimizing code security and techniques for user safety.

Key Words: Cybersecurity, Cyberspace, Cyberthreat, Vulnerability, Security mechanisms

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1 ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΕΙΣΑΓΩΓΗ ΘΕΩΡΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η ραγδαία εξέλιξη της τεχνολογίας τις τελευταίες δεκαετίες έχει οδηγήσει στη δημιουργία μιας ψηφιακής κοινωνίας που επηρεάζει με ποικίλους τρόπους την καθημερινότητα, την εργασία και τις δραστηριότητες των ανθρώπων. Συγκεκριμένα, η επιστήμη της πληροφορικής αναπτύσσεται με ταχύτατους ρυθμούς με τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) , δικτύων και ειδικότερα το διαδίκτυο, να χρησιμοποιούνται καθημερινά και από ιδιώτες και από κρατικούς φορείς για δραστηριότητες όπως εργασία, ψυχαγωγία, εκπαίδευση, ενημέρωση επικοινωνία και εμπορικές συναλλαγές. Η εξέλιξη αυτή έχει ως βασικό σκοπό τη βελτίωση της ποιότητας ζωής του σύγχρονου ανθρώπου με τη χρήση νέων τεχνολογιών να είναι πλέον απαραίτητη για να καλύπτονται βασικές ανάγκες χωρίς όμως οι άνθρωποι πολλές φορές να συνειδητοποιούν τις απειλές που διακυβεύουν την ασφάλεια των υπολογιστικών συστημάτων τους αλλά και των προσωπικών τους δεδομένων κλάδος της επιστήμης της πληροφορικής που ασχολείται με την προστασία των υπολογιστών, των υπολογιστικών συστημάτων και των δικτύων, ονομάζεται **Κυβερνοασφάλεια (Cybersecurity)**.

Ο όρος «Κυβερνοχώρος» (Cyberspace) περιλαμβάνει σε παγκόσμιο επίπεδο ψηφιακές δραστηριότητες που τελούνται εντός ενός ή περισσότερων αλληλοεξαρτώμενων δικτύων, ενσωματωμένων συστημάτων και ελεγκτών και είναι μια έννοια ευρύτερη από αυτή του διαδικτύου. Στη σύγχρονη ψηφιακή εποχή και με την ενσωμάτωση δικτυακών υποδομών και διαδικτυακών εφαρμογών στη καθημερινότητα των ανθρώπων εμφανίζονται συνεχώς νέες προκλήσεις και απειλές για την ασφάλεια των δεδομένων στον κυβερνοχώρο. Απλοί χρήστες αλλά και εταιρίες, στρατιωτικές βάσεις, τράπεζες και κυβερνητικοί οργανισμοί παράγουν σε καθημερινή βάση ανά τον κόσμο, τεράστιο όγκο ευαίσθητων προσωπικών δεδομένων και απόρρητων πληροφοριών που πρέπει να προστατεύονται από μη εξουσιοδοτημένη ή κακόβουλη πρόσβαση με σκοπό την υποκλοπή, την μεταβολή τους ή ακόμη και την εισαγωγή πλαστών δεδομένων. Τέτοιου είδους επιθέσεις όπως θα δούμε και παρακάτω, ονομάζονται Κυβερνοεπιθέσεις (CyberAttacks).

Οι υποδομές στις οποίες βασίζονται τα συστήματα πληροφοριών, επικοινωνιών και δικτύων συνεχώς αλλάζουν και διαμορφώνονται ανάλογα με τις απαιτήσεις των χρηστών και τις ταχύτατες τεχνολογικές εξελίξεις. Οι επιθέσεις που τελούνται στα πλαίσια του κυβερνοχώρου γίνονται ολοένα και πιο σύνθετες και εμφανίζονται με μεγαλύτερη συχνότητα θέτοντας σε κίνδυνο τη σωστή λειτουργία και αποτελεσματικότητα των υποδομών αυτών αλλά και των ψηφιακών υπηρεσιών που μας παρέχουν. Οι πιο επιζήμιες επιθέσεις είναι εκείνες που στοχεύουν κυρίως τις κρίσιμες υποδομές και τα πληροφοριακά συστήματα ενός κράτους και κάνουν την ασφάλεια να αποτελεί μείζον θέμα εθνικού ενδιαφέροντος ώστε να εξασφαλιστούν η ακεραιότητα, η διαθεσιμότητα, η ανθεκτικότητα και η εμπιστευτικότητα της ψηφιακής διακινούμενης πληροφορίας, βασικές αρχές της κυβερνοασφάλειας τις οποίες θα αναλύσουμε στην συνέχεια.

Η Κυβερνοασφάλεια με την πάροδο των χρόνων έχει εξελιχθεί και συνεχίζει να διευρύνεται και η εφαρμογή της κρίνεται πλέον ολοένα και πιο αναγκαία τόσο από τον απλό χρήστη όσο και από μεγάλες εταιρίες και οργανισμούς, αφού στο οπλοστάσιό της διαθέτει αρκετές μεθόδους και τεχνικές που αποβλέπουν στην προστασία των υπολογιστών, υπολογιστικών συστημάτων και δικτύων από διάφορες μορφές επιθέσεων που έχουν ως στόχο την δυσλειτουργία και την υποκλοπή ευαίσθητων δεδομένων από τους επιτιθέμενους αλλά και στον έγκαιρο εντοπισμό των πιθανών απειλών που ελλοχεύουν στον κυβερνοχώρο.

Πριν γίνει εννοιολογική προσέγγιση της κυβερνοασφάλειας, παρακάτω δίνεται μια πιο πρακτική θεώρηση ώστε να γίνει ευκόλως κατανοητό το γνωστικό της αντικείμενο. Δίνεται λοιπόν, ως μια διαδικασία που απαρτίζεται από τρία διακριτά βήματα. Η διαδικασία αυτή ονομάζεται πολιτική ασφαλείας και καθορίζει τις ενέργειες που πρέπει να διεξάγονται για να μειωθούν οι κίνδυνοι νέων επιθέσεων και οι συνέπειες που τις ακολουθούν. Τα βήματα αυτά είναι η πρόληψη (prevention) , η ανίχνευση (detection) και η απόκριση (recovery ή response).

Η **πρόληψη** είναι η διαδικασία λήψης μέτρων και στρατηγικών με σκοπό να αποφευχθούν οι επιπτώσεις από ανεπιθύμητες ενέργειες. Η συγκεκριμένη διαδικασία είναι πολύ σημαντική καθώς οι διαχειριστές έχουν τη δυνατότητα να λαμβάνουν τα κατάλληλα μέτρα ασφαλείας για τους πόρους που θέλουν να προστατεύσουν. Η κρυπτογράφηση και οι ψηφιακές υπογραφές είναι μερικά από τα εργαλεία που χρησιμοποιούνται για να ενισχύσουν την πρόληψη.

Η **ανίχνευση** είναι η διαδικασία έγκαιρης αναζήτησης και εντοπισμού των παράνομων ενεργειών που μπορεί να ελλοχεύουν στον κυβερνοχώρο αλλά και των συνεπειών που τις συνοδεύουν. Είναι μια εξίσου σημαντική διαδικασία καθώς με τη λήψη κατάλληλων μέτρων όπως είναι η συνεχής παρακολούθηση και ανίχνευση μη εξουσιοδοτημένων διεισδύσεων στο σύστημα, η αξία της ασφάλειας αυξάνεται. Συστήματα ανίχνευσης εισβολών (IDS) και αρχεία καταγραφής είναι εργαλεία που χρησιμοποιούνται υπέρ της ανίχνευσης.

Η **απόκριση** είναι η διαδικασία αποκατάστασης των πόρων που έχουν υποστεί ζημιά από προηγούμενες επιθέσεις και η αντιμετώπιση αυτών που βρίσκονται εν εξελίξει. Για να έχει νόημα ωστόσο το προηγούμενο βήμα, θα πρέπει η απόκριση να είναι έγκαιρη και καλά σχεδιασμένη. Εδώ, η διατήρηση αντιγράφων ασφαλείας και εργαλεία αφαίρεσης malware ενισχύουν την απόκριση σε συμβάντα. [1]

ΠΡΟΣΕΓΓΙΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Καθώς η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς, με ανάλογη ταχύτητα μεγαλώνει και η εξάρτηση της κοινωνίας από τα μέσα τεχνολογιών και πληροφορικής. Δημιουργείται έτσι μια αυξανόμενη ανάγκη για προστασία των χρηστών κάτι που κάνει την κυβερνοασφάλεια θέμα παγκοσμίου ενδιαφέροντος και υψίστης σημασίας. Ωστόσο δεν υπάρχει ένας συγκεκριμένος, τυποποιημένος και καθολικά αποδεκτός ορισμός για την κυβερνοασφάλεια καθώς είναι ένας όρος πολυδιάστατος. Πολλά έθνη ανά τον κόσμο έχουν δημοσιεύσει την επίσημη στρατηγική τους στην οποία τοποθετούνται σε ότι αφορά τον κυβερνοχώρο, το κυβερνοέγκλημα και την κυβερνοασφάλεια**.** Ο διαχωρισμός όμως ανάμεσα στις έννοιες **Κυβερνοασφάλεια**, **Ασφάλεια Πληροφοριών** και **Ασφάλεια Πληροφοριακών και Επικοινωνιακών Τεχνολογιών (ICT)**

ακόμη και η μεταξύ τους σχέση, δεν είναι πάντα σαφής. [2] . Για να αποσαφηνίσουμε τις έννοιες αυτές και να κατανοήσουμε καλύτερα πώς αυτές συγχέονται, αλλά και για να έχουμε μια ξεκάθαρη εικόνα της κυβερνοασφάλειας όπως είναι απαραίτητο για τα επόμενα κεφάλαια της εργασίας, παρατείθενται ακολούθως ενδεικτικά κάποιοι από τους ορισμούς που επίσημα έχουν δοθεί. Εάν εμβαθύνουμε περισσότερο, θα δούμε ότι αν και έχουν κοινά, τα όρια της κυβερνοασφάλειας είναι αρκετά μεγαλύτερα από αυτά της ασφάλειας πληροφοριών (ISO/IEC 27032:2012(E)).

Ασφάλεια πληροφοριών

- Σύμφωνα με το CNSS (Committee on National Security Systems) ως ασφάλεια πληροφοριών ορίζεται η διαδικασία προστασίας των πληροφοριών και των βασικών στοιχείων τους, συμπεριλαμβανομένου του λογισμικού (system) και του υλικού (hardware) που χρησιμοποιούν, αποθηκεύουν και μεταφέρουν αυτές τις πληροφορίες . Ωστόσο είναι ένας τομέας που περιλαμβάνει κλάδους της διαχείρισης ασφάλειας πληροφοριών, της ασφάλειας υπολογιστών και δεδομένων καθώς και της ασφάλειας δικτύων.[3]
- Επίσης ως ασφάλεια πληροφοριών ορίζεται και η διατήρηση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας της πληροφορίας η οποία μπορεί να διαφέρει σε μορφή (π.χ. να είναι έντυπη ή ψηφιακή) (ISO/IEC 27002 (2005))

Ασφάλεια Πληροφοριακών και Επικοινωνιακών Τεχνολογιών

- Η ασφάλεια πληροφοριακών και επικοινωνιακών τεχνολογιών αφορά την ασφάλεια των συστημάτων που βασίζονται στην τεχνολογία στα οποία η πληροφορία είναι αποθηκευμένη ή/και μεταδιδόμενη**.** Το 2004, το διεθνές πρότυπο ISO/IEC 13335 όρισε την ασφάλεια πληροφοριακών και επικοινωνιακών τεχνολογιών ως όλα τα ζητήματα που σχετίζονται με τον προσδιορισμό, την επίτευξη και την διατήρηση της ακεραιότητας, της εμπιστευτικότητας, της διαθεσιμότητας, της μη-αποποίησης ευθύνης, της αυθεντικοποίησης και αξιοπιστίας των πηγών πληροφορίας. [5]

Κυβερνοασφάλεια

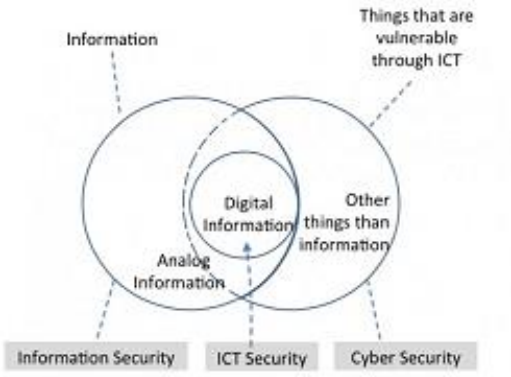
1 Το 2005, η Αμερικανική κυβέρνηση στο 109^{ο} κογκρέσο(h.r 285) ,προς διόρθωση της πράξης Εθνικής Ασφάλειας του 2002 αλλά και ως πολιτική βελτίωσης της κυβερνοασφάλειας, εισάγει στο τέλος μια προσέγγιση του ορισμού της, ως ακολούθως:

Κυβερνοασφάλεια είναι η διαδικασία αποφυγής ζημιάς, προστασίας και αποκατάστασης των υπολογιστών, των ηλεκτρονικών επικοινωνιακών συστημάτων και υπηρεσιών, των ενσύρματων επικοινωνιών και των ηλεκτρονικών επικοινωνιών συμπεριλαμβανομένων των πληροφοριών που εμπεριέχονται, με σκοπό την διασφάλιση της διαθεσιμότητας, της ακεραιότητας, της εμπιστευτικότητας, της αυθεντικότητας και της μη-αποποίησης. [5]

2 Η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union) αποσαφηνίζει την κυβερνοασφάλεια ως εξής (ITU-T X.1205):

Κυβερνοασφάλεια είναι η συλλογή εργαλείων, πολιτικών, εννοιών και μέτρων ασφαλείας, κατευθυντήριων οδηγιών, δράσεων, εκπαίδευσης, καλύτερων πρακτικών και τεχνολογιών που μπορούν να χρησιμοποιηθούν για να προστατεύσουν το περιβάλλον του κυβερνοχώρου όπως επίσης και τα περιουσιακά στοιχεία των χρηστών και των επιχειρήσεων περιουσιακά αυτά στοιχεία μπορεί να είναι συνδεδεμένες ηλεκτρονικές συσκευές, εφαρμογές, υποδομές, υπηρεσίες και οι πληροφορίες στο σύνολό τους που μεταδίδονται ή αποθηκεύονται στον κυβερνοχώρο. [6]

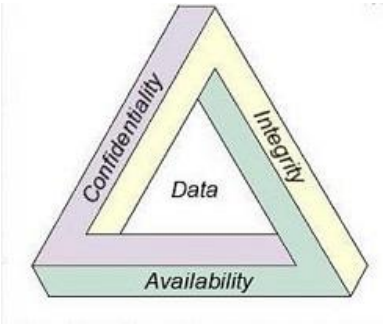
Ρίχνοντας μια δεύτερη ματιά στους ορισμούς, παρατηρούμε ότι στην περίπτωση της ασφάλειας πληροφοριών το στοιχείο που προστατεύεται είναι αυτούσια η πληροφορία. Στην ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων, στόχος είναι η προστασία της τεχνολογίας που χρησιμοποιείται και ως ακόλουθο και οι πληροφορίες που περιέχει. Η κυβερνοασφάλεια από την άλλη, εστιάζει στην ασφάλεια των χρηστών που μπορεί να είναι απλοί χρήστες, οργανισμοί ή και έθνη και κατ'επέκταση οποιοδήποτε περιουσιακό στοιχείο τους μπορεί να προσεγγιστεί μέσω του κυβερνοχώρου. Οι παραπάνω έννοιες σχετίζονται, είναι όμως φανερό ότι η προστασία στην οποία αποσκοπεί η κυβερνοασφάλεια, περιλαμβάνει κατά μια έννοια την ασφάλεια πληροφοριών, αλλά και την ασφάλεια πληροφοριακών και επικοινωνιακών τεχνολογιών, ωστόσο εκτείνεται και πέρα από τα επίσημα όρια της ασφάλειας πληροφοριών και της ασφάλειας πληροφοριακών και επικοινωνιακών τεχνολογιών, δημιουργώντας έτσι ένα πρόσθετο κλάδο στον τομέα της ασφάλειας. Η παρακάτω εικόνα δείχνει τη σχέση μεταξύ τους και τα όρια που καλύπτει καθένας από τους τρείς ορισμούς.



Εικόνα 1 Σχέση ανάμεσα στην ασφάλεια πληροφοριών, στην ασφάλεια πληροφοριών και επικοινωνιακών τεχνολογιών και την κυβερνοασφάλεια.

ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ ΠΟΥ ΔΙΕΠΟΥΝ ΤΗΝ ΑΣΦΑΛΕΙΑ

Στους ορισμούς που δόθηκαν στην προηγούμενη ενότητα έγινε αναφορά σε έννοιες όπως η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα. Οι έννοιες αυτές, όπως και η εξουσιοδότηση, η μη αποποίηση και η αυθεντικοποίηση, όπως θα δούμε παρακάτω, αποτελούν τις θεμελιώδεις αρχές της ασφάλειας στις οποίες στηρίζονται η διαφύλαξη των πόρων αλλά και η προστασία των δεδομένων ενός χρήστη ή ενός συστήματος στα πλαίσια του κυβερνοχώρου. Οι τρείς πρώτες μάλιστα, αποτελούν και το μοντέλο CIA (Confidentiality, Integrity, Availability) που υποδεικνύει τις βασικές λειτουργίες ενός συστήματος ή ενός δικτύου που είναι πιθανότερο να δεχτούν κάποια επίθεση και άρα αυτές που πρέπει οπωσδήποτε πρώτα να προστατευθούν.



Εικόνα 2 Μοντέλο CIA

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ (CONFIDENTIALITY)

Η εμπιστευτικότητα συνεπάγεται την διασφάλιση ότι η προστατευόμενη πληροφορία δεν θα είναι προσπελάσιμη από μη εξουσιοδοτημένους χρήστες, υπηρεσίες ή συνδεδεμένες συσκευές. Πιο συγκεκριμένα σκοπός της εμπιστευτικότητας είναι να αποτρέψει την εκτύπωση, την παρουσίαση ή την εμφάνιση των προστατευόμενων δεδομένων ακόμα και την αποκάλυψη της ύπαρξής τους, εφόσον χρειαστεί, από ομάδες ατόμων που δεν τους Εχουν παραχωρηθεί τα απαραίτητα δικαιώματα. [7] Η εμπιστευτικότητα έχει επίσης να κάνει και με την προστασία της ροής δεδομένων από την ανάλυση της κίνησης. [8] Αυτό σημαίνει ότι σε μια ζεύξη πέρα από τον αποστολέα και τον παραλήπτη σκοπός είναι κανένας άλλος να μην μπορεί να παρεμβάλλει στην επικοινωνία με σκοπό να αποσπάσει πληροφορίες για τη μεταξύ τους σχέση, τη συχνότητα επικοινωνίας ή το μήκος και το περιεχόμενο των μηνυμάτων. Σε αυτή την περίπτωση δημιουργείται το ερώτημα εάν απαιτείται η ασυνδεσιμότητα (unlinkability) ορισμένων γεγονότων ώστε ο επιτιθέμενος να μην είναι σε θέση να διακρίνει επαρκώς εάν υπάρχει κάποια συσχέτιση μεταξύ μηνυμάτων, χρηστών ή δράσεων σε ένα επικοινωνιακό σύστημα. Για να γίνει αυτό εφικτό θα πρέπει οι χρήστες να έχουν την ιδιότητα της ανωνυμίας (anonymity),την κατάσταση δηλαδή της ταυτοποίησης μέσω της οποίας μια οντότητα μπορεί να αναγνωριστεί ως διακριτή χωρίς να υπάρχουν επαρκείς πληροφορίες ταυτοποίησης που να τη συνδέουν με κάποια γνωστή ταυτότητα. [8][9]

ΑΚΕΡΑΙΟΤΗΤΑ (INTEGRITY)

Η ακεραιότητα εξασφαλίζει ότι κανένας μη εξουσιοδοτημένος χρήστης δεν θα έχει τη δυνατότητα να μεταβάλλει (να δημιουργήσει, να τροποποιήσει ή να διαγράψει),σκόπιμα ή μη, την προστατευόμενη πληροφορία. Πρόκειται για την ιδιότητα που αντανακλά τη λογική ορθότητα και την αξιοπιστία του λειτουργικού συστήματος καθώς και την λογική πληρότητα του υλικού και του λογισμικού που εφαρμόζει μηχανισμούς προστασίας. Η ακεραιότητα χαρακτηρίζει επίσης τη συνοχή των δομών δεδομένων και τη λειτουργικότητα των δεδομένων που είναι αποθηκευμένα στο σύστημα . Τα κενά ασφαλείας και οι ευπάθειες στο λογισμικό μπορούν να οδηγήσουν σε απώλεια της ακεραιότητας στα δεδομένα και να καταστήσουν δυνατές μη εξουσιοδοτημένες τροποποιήσεις στο σύστημα. Τυπικά τα προγράμματα περνούν από αυστηρό έλεγχο τα δικαιώματα ανάγνωσης και εγγραφής των χρηστών που ζητούν πρόσβαση σε συγκεκριμένα αρχεία και δεδομένα, ωστόσο μια ευπάθεια του λειτουργικού συστήματος αρκεί για να οδηγήσει σε παράβλεψη αυτού του ελέγχου και να κάνει πιο εύκολη για τον επιτιθέμενο την εξαπόλυση κάποιας επίθεσης (SQL Injection). [7][8]

ΔΙΑΘΕΣΙΜΟΤΗΤΑ (AVAILABILITY)

Η διαθεσιμότητα ορίζεται ως η ιδιότητα που επιτρέπει στο σύστημα ή στους προστατευόμενους πόρους του, να είναι προσβάσιμο και χρησιμοποιήσιμο εφόσον απαιτηθεί από εξουσιοδοτημένες οντότητες. Βασικός σκοπός της διαθεσιμότητας είναι να εξασφαλίσει ότι ένας επιτιθέμενος δεν θα έχει τη δυνατότητα να αποτρέψει τους νόμιμους χρήστες από το να έχουν ορθή πρόσβαση στο σύστημά τους. Η διαθεσιμότητα αντιμετωπίζει θέματα ασφαλείας που ανακύπτουν από επιθέσεις άρνησης εξυπηρέτησης (Denial of Service), δηλαδή από την παρεμπόδιση εισόδου εξουσιοδοτημένων χρηστών ή και την χρονική καθυστέρηση κρίσιμων λειτουργιών του συστήματος. [7][8]

ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ (AUTHENTICATION)

Η ιδιότητα της αυθεντικοποίησης είναι ιδιαίτερα σημαντική στον τομέα της ασφάλειας καθώς αποτελεί το κλειδί για την πιστοποίηση της πηγής ενός συνόλου δεδομένων (πακέτα σε ένα δίκτυο ή e-mail) αλλά και για την επιβεβαίωση της ταυτότητας των οντοτήτων που συμμετέχουν σε μια ζεύξη. Αποτελεί βασικό μέτρο ασφάλειας καθώς καθιερώνει την εγκυρότητα του μεταδιδόμενου μηνύματος, του δημιουργού του και σε ευρύτερα πλαίσια προσδιορίζει το αν θα δοθεί εξουσιοδότηση στην εκάστοτε οντότητα να έχει πρόσβαση σε συγκεκριμένες πληροφορίες. Υπάρχουν διάφοροι μέθοδοι αυθεντικοποίησης ενός χρήστη και σε όλες πρέπει να δοθούν κάποιες πληροφορίες που να τον ταυτοποιούν και που μόνο εκείνος θα γνωρίζει. Οι πληροφορίες αυτές ανήκουν σε τρεις κατηγορίες που θα αναλύσουμε στη συνέχεια και ονομάζονται παράγοντες αυθεντικοποίησης (factors of authentication). Τα συστήματα αυθεντικοποίησης μηνυμάτων ωστόσο δεν μπορούν να βασιστούν μόνο σε αυτούς τους παράγοντες αλλά χρησιμοποιούν και την κρυπτογραφία όπου με την παραγωγή μυστικού κλειδιού που μόνο ο αποστολέας έχει στην κατοχή του, γίνεται η ταυτοποίηση του από τον παραλήπτη. Η αυθεντικοποίηση διακρίνεται σε :

- Αυθεντικοποίηση ομότιμης οντότητας (Peer entity authentication) : Σε αυτή την περίπτωση μια οντότητα δεν μπορεί να προσποιηθεί ότι είναι μια άλλη
- Αυθεντικοποίηση προέλευσης δεδομένων (Data origin authentication) : Η πηγή προέλευσης του μηνύματος είναι αυτή που ισχυρίζεται. [8]

ΕΞΟΥΣΙΟΔΟΤΗΣΗ (AUTHORIZATION)

Ενώ όπως προαναφέρθηκε, η αυθεντικοποίηση έχει άμεση σχέση με την ταυτοποίηση οντοτήτων, η εξουσιοδότηση είναι το αμέσως επόμενο βήμα. Πρόκειται για την αρχή εκείνη που προσδιορίζει αν μια ταυτοποιημένη οντότητα θα έχει πρόσβαση στο σύστημα, διευκρινίζει ποιά θα είναι τα ακριβή δικαιώματα της και ποιές ενέργειες θα επιτρέπονται. [7][8]

ΜΗ ΑΠΟΠΟΙΗΣΗ (NON-REPUDIATION)

Πρόκειται για την ιδιότητα που εμποδίζει τον αποστολέα ή τον παραλήπτη από το να απαρνηθεί ένα μήνυμα που έχει μεταδοθεί. Για την ακρίβεια ο αποστολέας διαθέτει αποδείξεις για την ταυτότητα του παραλήπτη και ο παραλήπτης διαθέτει πληροφορίες για την ταυτότητα του αποστολέα ώστε καμία πλευρά να μην μπορέσει να αμφισβητήσει την επεξεργασία της πληροφορίας. Εργαλεία για την ενίσχυση της μη αποποίησης αποτελούν οι ψηφιακές υπόγραφες. Στην ασφάλεια επικοινωνιών η μη αποποίηση μπορεί να είναι:

- Μη αποποίηση με απόδειξη προελεύσεως (Non-repudiation with proof of origin): Παρέχει πιστοποίηση προέλευσης των ληφθέντων μηνυμάτων
- Μη αποποίηση με απόδειξη παραδόσεως (Non-repudiation with proof of delivery) : Παρέχει πιστοποίηση παράδοσης των μηνυμάτων στον αποστολέα. [7][8]

ΑΝΑΓΚΑΙΟΤΗΤΑ ΓΙΑ ΑΣΦΑΛΕΙΑ ΣΕ ΕΝΑ ΚΟΣΜΟ ΣΥΝΕΧΟΜΕΝΩΝ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΞΕΛΙΞΕΩΝ

Οι τεχνολογικές εξελίξεις εξυπηρετούν τη βελτίωση των συνθηκών και την ποιότητα ζωής του ανθρώπινου είδους και σαφώς διαμορφώνουν τις κοινωνικές σχέσεις και τον τρόπο επικοινωνίας μεταξύ των ανθρώπων. Η χρήση των διάφορων τεχνολογικών μέσων και του διαδικτύου έχει πλέον γίνει επιτακτική ανάγκη αφού συνδέεται με αναρίθμητες καθημερινές δραστηριότητες. Με την χρήση εξελιγμένων υπολογιστικών συστημάτων είναι σήμερα εφικτό να μεταφέρουμε απομακρυσμένα χρήματα και να κάνουμε πληρωμές, να παρακολουθούμε λειτουργίες του ανθρώπινου σώματος στον τομέα της υγείας, να ελέγχουμε από πτήσεις αεροπλάνων μέχρι την λειτουργία απλών συσκευών μέσα στο σπίτι (IoT) ακόμα και την κίνηση στον δρόμο .Χιλιάδες είναι ακόμη οι δραστηριότητες που επηρεάζουν τις ζωές, την υγεία και την οικονομία σε διεθνές και παγκόσμιο επίπεδο. Εν τούτοις, τα ευεργετήματα αυτών των εξελίξεων είναι η μια όψη του νομίσματος καθώς υπάρχει και η αρνητική πλευρά κατά την οποία εάν δεν γίνεται σωστή χρήση των τεχνολογιών αυτών, μπορούν εύκολα να μετατραπούν σε επικίνδυνα όπλα που στρέφονται ενάντια στον χρήστη.

Σύμφωνα με τον Γ. Μπαμπινιώτη, η λέξη ασφάλεια περιγράφει την κατάσταση στην οποία αισθάνεται κανείς ότι δεν απειλείται, την αποτροπή κινδύνου ή απειλής. Στην επιστήμη της πληροφορικής η ασφάλεια ορίζει τη προστασία του συνόλου των δεδομένων που έχουν αξία για τον χρήστη. Τα δεδομένα αυτά ονομάζονται πόροι ή αγαθά (assets) του υπολογιστικού συστήματος και μπορεί να είναι υλικό, λογισμικό, δεδομένα, διεργασίες, άτομα ή και συνδυασμός των ανωτέρω. Για να καταλάβουμε όμως τι είναι ακριβώς αυτό που πρέπει να προστατέψουμε, πρέπει πρώτα να καθορίσουμε τι αξία (value) έχει και σε ποιόν. Κατά πόσο εύκολο είναι δηλαδή, κάτι να αντικατασταθεί ή όχι.

Για παράδειγμα, ένας κενός ηλεκτρονικός υπολογιστής αποτελεί αγαθό που μπορεί εύκολα να αντικατασταθεί. Αν όμως περιέχει αρχεία, εικόνες, βίντεο, σημειώσεις ή οτιδήποτε άλλο (και αυτά αποτελούν πόρους επίσης), η αξία του ανεβαίνει γιατί το περιεχόμενό του είναι αυτό που δεν μπορεί να αντικατασταθεί και που τον καθιστά μοναδικό. Πόροι του υλικού και του λογισμικού όπως είναι παραδείγματος χάριν υπολογιστές, περιφερειακές συσκευές, λειτουργικά συστήματα και εμπορικές εφαρμογές, είναι «τυποποιημένοι» πόροι και είναι εύκολο να αντικατασταθούν, συνεπώς έχουν χαμηλή αξία. Δεδομένα όμως, όπως προσωπικά έγγραφα, φωτογραφίες, μουσική, e-mail και εφαρμογές δημιουργούμενες από τον χρήστη είναι πόροι μοναδικοί και αναντικατάστατοι συνεπώς έχουν υψηλή αξία και πρέπει να προστατευθούν.

Πολλές φορές οι πόροι ενός υπολογιστικού συστήματος είναι δυνατό να εκτεθούν σε κάποιο κίνδυνο (exposure). Ο κίνδυνος αποτελεί την αιτία να περιοριστεί η αξία του αγαθού και αυτό μπορεί να οδηγήσει σε κάποιας μορφής απώλεια (loss) ή ζημιά (damage). Παράδειγμα έκθεσης σε κίνδυνο είναι η μη εξουσιοδοτημένη αποκάλυψη δεδομένων ή και η τροποποίησή τους καθώς επίσης και η άρνηση θεμιτής προσπέλασης υπολογιστικών πόρων. Απώλειες και ζημιές είναι εφικτό να προκληθούν ως αποτέλεσμα της εκμετάλλευσης μιας ευπάθειας (vulnerability) του υπολογιστικού συστήματος, ενός τρωτού σημείου στο σύστημα δηλαδή που μπορεί να αφορά σε αδυναμία στις ρυθμίσεις ή τη διαχείριση του συστήματος ή ένα ευάλωτο σημείο σε ένα υποσύστημα ασφάλειας. Για παράδειγμα ένα σύστημα μπορεί να είναι τρωτό σε μη εξουσιοδοτημένη χρήση δεδομένων, επειδή δεν εξακριβώνει την ταυτότητα των χρηστών πριν την παραχώρηση του δικαιώματος πρόσβασης σε αυτά τα δεδομένα.

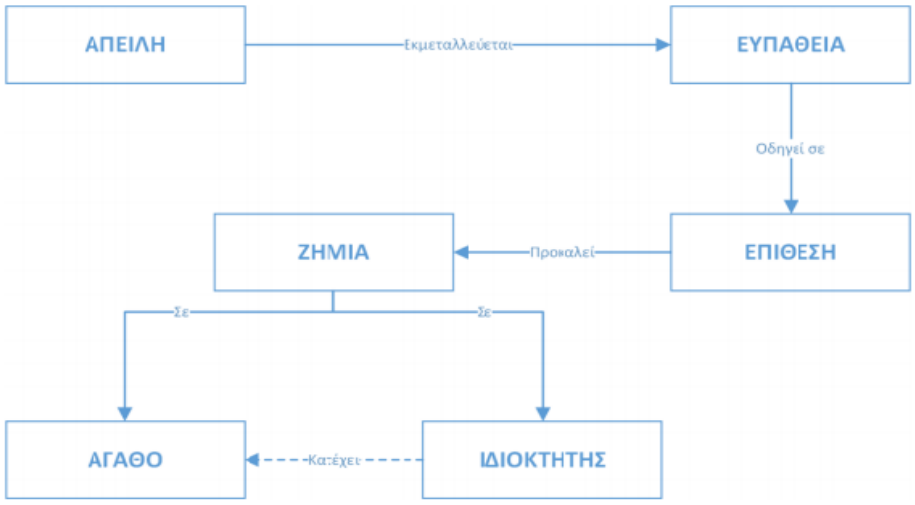
Πρώτου προστατευθεί ένας πόρος, πρέπει να προσδιοριστεί το είδος της ζημίας από το οποίο πρέπει να το διαφυλάξουμε. Μια κατάσταση στην οποία υπάρχει το ενδεχόμενο πρόκλησης απώλειας ή ζημίας αποτελεί απειλή (threat). Οι απειλές μπορεί να είναι κακόβουλες ή και όχι εσκεμμένες ή τυχαίες, σε κάθε περίπτωση ωστόσο έχουν ανεπιθύμητες επιπτώσεις για τους προστατευόμενους πόρους του συστήματος.

Όταν ένας χρήστης εκμεταλλεύεται μια ευπάθεια σε ένα σύστημα, τότε διαπράττει μια επίθεση (attack) σε αυτό. Ωστόσο μια επίθεση είναι δυνατό να πραγματοποιηθεί και από ένα άλλο, ξεχωριστό σύστημα το οποίο στέλνει καταιγισμό μηνυμάτων στο πρώτο με αποτέλεσμα αυτό να μην είναι σε θέση να ανταποκριθεί και να λειτουργήσει σωστά. Αυτή είναι η γνωστή ως επίθεση άρνησης εξυπηρέτησης που κατακλύζει τους servers με πληθώρα μηνυμάτων θέτοντάς τους έτσι σε αδράνεια, η οποία θα αναλυθεί εκτενέστερα στο κεφάλαιο των επιθέσεων. Η μείωση της αξίας του πόρου και η προξένησα βλάβης ή και διακοπής στο σύστημα έπειτα από μια επιτυχημένη επίθεση, ονομάζεται επίπτωση (impact).

Για να αντιμετωπιστούν επαρκώς ευπάθειες, απειλές και επιθέσεις, χρησιμοποιείται ένα σύνολο αντιμέτρων (countermeasures) ή ελέγχων (control) ως μέτρο προστασίας. Τα αντίμετρα που χρησιμοποιούνται μπορεί να είναι κάποια ενέργεια, συσκευή, διαδικασία ή τεχνική που μειώνει ή εξαλείφει τελείως μια ευπάθεια. Ωστόσο, η διαφορετικότητα τους δημιούργησε την ανάγκη ανάλυσης των συνιστωσών της ασφάλειας ώστε να είναι πιο ευδιάκριτοι οι τομείς στους οποίους θα πρέπει να εφαρμόζεται. Πιο συγκεκριμένα, είναι η φυσική ασφάλεια του συστήματος, η ασφάλεια του υπολογιστικού συστήματος, η ασφάλεια των βάσεων δεδομένων και η ασφάλεια δικτύων επικοινωνιών. Η εφαρμογή των αντιμέτρων έχει ως επακόλουθο ένα επιπρόσθετο κόστος (cost) για τον οικείο οργανισμό, την επιχείρηση ή τον ιδιώτη. [10]

Η σχέση απειλής, ελέγχου και ευπάθειας μπορεί να περιγραφεί πιο συγκεκριμένα ως το σύνολο των ελέγχων και των αντιμέτρων που χρησιμοποιούνται σε ένα σύστημα, αποτρέπει τις απειλές από το να εκμεταλλεύονται τις ευπάθειες του. [11]

Συνοψίζοντας τις έννοιες που αναφέρθηκαν στο σχεδιάγραμμα που ακολουθεί, έχουμε πλέον μια ευρύτερη εικόνα της ασφάλειας στον κόσμο της πληροφορικής. Βασικός σκοπός της ασφάλειας είναι να επιτευχθεί ισορροπία μεταξύ του κόστους των αντιμέτρων προστασίας, της επίθεσης και τη ζημιάς που μπορεί να προκαλέσει. Αυτό ωστόσο, απαιτεί τη βάση μιας εμπεριστατωμένης μελέτης καθώς η ικανοποίηση των απαιτήσεων της ασφάλειας είναι από τις βασικές προϋποθέσεις για την εισαγωγή και την αξιοποίηση νέων τεχνολογιών στον τομέα της πληροφορικής.



Εικόνα 3 Συσχέτιση εννοιών

ΚΑΤΗΓΟΡΙΕΣ ΑΠΕΙΛΩΝ ΚΑΙ ΤΥΠΟΙ ΤΡΩΤΟΤΗΤΩΝ

Είδαμε ως τώρα, ότι απειλή είναι μια κατάσταση στην οποία υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή και ζημιάς σε ένα σύστημα και τους πόρους του. Υπάρχουν ποικίλοι

τρόποι κατηγοριοποίησης των απειλών κυρίως με βάση τα αίτια ή την πηγή τους. Οι απειλές σε ευρύτερο πλαίσιο, μπορεί να είναι φυσικές ή ανθρώπινες, κακόβουλες ή μη και τυχαίες ή στοχευμένες.

Οι φυσικές απειλές είναι εκείνες που προκύπτουν μέσα στο περιβάλλον στο οποίο αναπτύσσονται και λειτουργούν. Τέτοιες είναι οι πυρκαγές, οι πλημμύρες, οι διακοπές ρεύματος ακόμη και η αδυναμία λειτουργίας εξαρτημάτων όπως για παράδειγμα ένα κομμένο καλώδιο ή ένας χαλασμένος σκληρός δίσκος. Από την άλλη, οι ανθρώπινες απειλές είναι αυτές που έχουν ως παράγοντα τον ίδιο τον χρήστη του οποίου οι ενέργειες μπορεί να είναι κακόβουλες ή και απρόθυμες. Τέτοιου τύπου απρόθυμων απειλών, είναι για παράδειγμα αν κάποιος ρίξει κατά λάθος καφέ στον υπολογιστή ή διαγράψει κατά λάθος ένα αρχείο. Αντίθετα, αν υπάρχει πρόθεση πρόκλησης κάποιας βλάβης, πρόκειται δηλαδή για κακόβουλη ενέργεια, τότε χρησιμοποιείται ο όρος επίθεση.

Ως τυχαίες χαρακτηρίζονται οι απειλές στις οποίες ναι μεν υπάρχει πρόθεση πρόκλησης ζημιάς αλλά όχι προς κάποιο συγκεκριμένο άτομο. Ένα παράδειγμα τέτοιας απειλής είναι ένα κακόβουλο κομμάτι κώδικα που δημοσιεύεται σε κάποια ιστοσελίδα και μπορεί να το επισκευτεί οποιοσδήποτε. Στις στοχευμένες απειλές αντιθέτως, οι επιτιθέμενοι (ας μου επιτραπεί ο όρος εφόσον η πρόθεση είναι ξεκάθαρη) έχουν σκοπό να βλάψουν συγκεκριμένους υπολογιστές ή ομάδες αυτών όπως κρατικούς οργανισμούς και φορείς.

Επίσημα, τα είδη των απειλών χωρίζονται σε δυο πιο γενικές κατηγορίες. Αν υποθέσουμε ότι πρόκειται για έναν οργανισμό ή μια επιχείρηση:

- Εξωτερικές απειλές (Outsiders) : Σε αυτή τη κατηγορία ανήκουν hackers, crackers, hacktivists, vandals καθώς και κοινωνικοί μηχανικοί (social engineering) .
- Εσωτερικές απειλές (Insiders) : Εδώ ανήκουν όσοι κάνουν παράκαμψη της πρόσβασης εκ των έσω (όσοι δηλαδή εργάζονται εκεί ή δούλευαν παλιότερα και υπήρξαν δυσαρεστημένοι) [11]

Οι επιπτώσεις των απειλών , από την άλλη, μπορούν να ταξινομηθούν και αυτές, σε τέσσερις διακριτές κατηγορίες με βάση τα αποτελέσματα που επιφέρουν. Αυτές είναι:

- Υποκλοπή (Interception) : Μια μη εξουσιοδοτημένη οντότητα καταφέρνει να προσπελάσει κάποιο πόρο
- Μεταβολή (Modification) : Μια μη εξουσιοδοτημένη οντότητα τροποποιεί την κατάσταση ενός πόρου
- Διακοπή (Interruption) : Μια μη εξουσιοδοτημένη οντότητα καταστρέφει έναν πόρο ή τον καθιστά μη προσπελάσιμο
- Πλαστογραφία (Fabrication) : Μια μη εξουσιοδοτημένη οντότητα πλαστογραφεί έναν πόρο [11]

Οι απειλές εκμεταλλεύονται τις τρωτότητες, τις ευπάθειες δηλαδή ενός υπολογιστικού συστήματος που μπορεί να υπάρχουν σε διαδικασίες στον σχεδιασμό και στην εφαρμογή ώστε να διεξαχθεί μια επίθεση που μπορεί να είναι επιζήμια. Οι ευπάθειες κατηγοριοποιούνται και αυτές ως εξής:

- Ανθρώπινες ευπάθειες: Συχνά είναι το πιο αδύναμο σημείο ασφαλείας των υπολογιστικών συστημάτων. Οι άνθρωποι που τα χειρίζονται νόμιμα αποτελούν τη μεγαλύτερη απειλή για αυτό, καθώς από αυτούς εξαρτάται η ασφάλεια του συστήματος. Σε εταιρίες και οργανισμούς για παράδειγμα, η έλλειψη εκπαίδευσης, η επιπολαιότητα στο χειρισμό ευαίσθητων δεδομένων και ο δόλος πιθανών δυσαρεστημένων υπαλλήλων, αποτελούν από τις πλέον μεγαλύτερες απειλές για την ασφάλεια (insiders).
- Ευπάθειες επικοινωνιών: Αφορά τις συνδέσεις συσκευών σε ανοιχτό δίκτυο όπως είναι το Διαδίκτυο. Ο κίνδυνος εισβολής στο δίκτυο, μη εξουσιοδοτημένων οντοτήτων αυξάνεται και έτσι υπάρχει πιθανότητα πακέτα που μεταδίδονται, να υποκλαπούν, να καταστραφούν ή να αλλάξουν διαδρομή.
- Ευπάθειες υλικού και λογισμικού: Αφορούν κατασκευαστικές δυσλειτουργίες και λανθασμένες ρυθμίσεις στο υλικό και το λογισμικό. Εσφαλμένη εγκατάσταση ή ενδογενή σφάλματα στα επιμέρους τμήματα του συστήματος μπορεί να αποβούν σε διακοπή παροχής των υπηρεσιών.
- Ευπάθειες μέσων: Αφορά την λανθασμένη διαχείριση των μέσων όπως μαγνητικές ταινίες, εκτυπωτές, έντυπα ή οπτικά έγγραφα με τρόπο τέτοιο ώστε να καταστραφούν ή να κλαπούν.
- Φυσικές ευπάθειες: Αφορούν τον χώρο στον οποίο εγκαθιδρύονται και λειτουργούν τα συστήματα (π.χ. χώροι μηχανογραφικών κέντρων, datacenters)
- Εκ φύσεως ευπάθειες: Αφορά κυρίως φυσικές καταστροφές (π.χ. πυρκαγιές, καταποντισμοί, κεραυνοί, διακοπές ρεύματος) και περιβαλλοντικές απειλές όπως η σκόνη, η υγρασία και οι ακραίες θερμοκρασιακές συνθήκες που επηρεάζουν αρνητικά τα υπολογιστικά συστήματα.
- Ευπάθειες εκπομπών: Αφορά την υποκλοπή και αποκωδικοποίηση των εκπεμπόμενων σημάτων μέσα σε ένα δίκτυο ή υπολογιστικό σύστημα από μη εξουσιοδοτημένα άτομα με σκοπό την εξόρυξη κρίσιμων πληροφοριών και δεδομένων ή την πρόκληση δυσλειτουργιών στο ίδιο το σύστημα. [11]

ΑΝΑΛΥΣΗ ΡΙΣΚΟΥ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ

Σε καθημερινή βάση προκύπτουν ολοένα και περισσότερα περιστατικά όπου τα δεδομένα οργανισμών, φορέων και ιδιωτών τίθενται σε κίνδυνο. Περιπτώσεις απώλειας ή κλοπής του φορητού υπολογιστή ή η παραβίαση ενός ιδιωτικού εξυπηρετητή (server), μπορεί να οδηγήσει σε απώλεια ευαίσθητων και εμπιστευτικών δεδομένων. Η σύγχρονη κοινωνία στηρίζεται πλέον σε μέσα που οφείλουν να είναι αξιόπιστα για την ασφαλή αποθήκευση, μετάδοση και χρήση των πληροφοριών οι οποίες αποτελούν πολύτιμους πόρους και πρέπει να προστατεύονται επαρκώς. Ωστόσο, είναι ουτοπική η θεώρηση ότι ένας πόρος μπορεί ποτέ να είναι απόλυτα ασφαλής ενάντια σε κάθε μορφής επίθεση. Όσες άμυνες και μηχανισμοί ασφαλείας και αν εφαρμοστούν στο εκάστοτε σύστημα, πάντα θα υπάρχει η πιθανότητα (likelihood) μιας επιτυχημένης επίθεσης. Είναι αδύνατο να γνωρίζουμε εκ των προτέρων τις επιθέσεις που πρόκειται να συμβούν όμως εφόσον υπάρχει έστω και μια τρωτότητα, η πιθανότητα εκμετάλλευσής της, δημιουργεί ρίσκο (risk). Γενικά ισχύει:

ΡΙΣΚΟ = ΠΙΘΑΝΟΤΗΤΑ Χ ΕΠΙΠΤΩΣΗ

Η διαχείριση των απειλών μπορεί να είναι κατευθυντήρια οδηγός στον περιορισμό του ρίσκου. Σε πολύπλοκα υπολογιστικά συστήματα όμως κάτι τέτοιο δεν είναι πρακτικό. Μια στρατηγική προσέγγιση είναι η δημιουργία αμυντικών μηχανισμών η οποία θα περιορίζει το ρίσκο σε αποδεκτά επίπεδα. Για να γίνει αυτό εφικτό είναι αναγκαίο να εφαρμοστεί μεθοδική ανάλυση του ρίσκου. [12][13]

ISO 27001

Το ISO 27001 αποτελεί ένα διεθνώς αναγνωρισμένο πρότυπο το οποίο προσδιορίζει τις απαιτήσεις και τις προδιαγραφές για την εφαρμογή και την συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Το εν λόγω πρότυπο βρίσκει εφαρμογή σε οργανισμούς και εταιρίες ανεξαρτήτως μεγέθους και σκοπός του είναι η διασφάλιση των εταιρικών δεδομένων και των ευαίσθητων πληροφοριών. Πιο συγκεκριμένα παρέχει:

- Ασφάλεια σε λογικό επίπεδο: Σύνολο μέτρων για την προστασία της ακεραιότητας και της εμπιστευτικότητας των ψηφιακών πληροφοριών
- Ασφάλεια σε φυσικό επίπεδο: Σύνολο λύσεων που στοχεύουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης σε φυσικές τοποθεσίες
- Ασφάλεια σε οργανωτικό επίπεδο: Σύνολο ρόλων, καθηκόντων και υποχρεώσεων που ορίζουν τις πολιτικές και διαδικασίες ασφαλείας σε έναν οργανισμό

Βασική συστημική απαίτηση του προτύπου αποτελεί η διαχείριση ρίσκου (Risk assessment & Treatment Plan). Πρόκειται για το έντυπο στο οποίο πραγματοποιείται αναλυτική καταγραφή και αξιολόγηση των κινδύνων, έτσι ώστε να γίνει επιλογή των κατάλληλων ελέγχων για την ασφάλεια των πληροφοριών όπως φαίνεται και στην παρακάτω εικόνα. [12]

CATEGORY	RISK	IMPACT OF RISK (Scale of 1-10)	MITIGATING CONTROLS AND MEASURES	LIKELIHOOD, POST CONTROLS (0-100%)	RESIDUAL RISK	RISK TREATMENT DECISION
Data	Confidential data could be accessed by unauthorized parties because staff/internal stakeholders are unaware of how to identify and classify confidential data	10	Established a Data Classification Policy, which has a defined information classification scheme for the labeling and handling of data. Data is classified into three levels: Public, Company Confidential, and Customer Confidential	20%	2.0	Accept
Fraud Risk	Risk associated with financial fraud within the organization	9	Independent financial audits performed on an annual basis	20%	1.8	Accept
Vendors	Risks associated with dependence on Vendors to achieve the organization's objectives	8	Established a Vendor Management Policy that outlines a process for managing vendor relationships for key vendors. The SOC2 / ISO reports are collected from key vendors to ensure they provide enough guarantees on security, availability and confidentiality	20%	1.6	Accept

Εικόνα 4 Διαχείριση Ρίσκου στο ISO 27001

Αναλυτικότερα, καταγράφεται η κατηγορία του ρίσκου και γίνεται η περιγραφή του (μπορεί η κατηγορία να αφορά και σε στοιχεία όπως π.χ. ψηφιακά αρχεία, προμηθευτές ή κίνδυνο απάτης). Στη συνέχεια, αποτιμάται σε μια κλίμακα από το 1 έως το 10 ο αντίκτυπος του συμβάντος (οι κλίμακες μπορεί να διαφέρουν). Έπειτα, περιγράφονται οι ενέργειες που λαμβάνουν χώρα για τον περιορισμό του ρίσκου και υπολογίζεται η πιθανότητα εμφάνισης σχετικού συμβάντος (λαμβάνεται υπόψη αν το συμβάν έχει συμβεί ξανά στο παρελθόν). Εφόσον έχουν αποδοθεί τιμές στην πιθανότητα και στον αντίκτυπο, υπολογίζεται το ρίσκο ως το γινόμενο των δύο προαναφερθέντων τιμών. Ανάλογα με την τιμή που θα έχει το ρίσκο , οι κίνδυνοι κατατάσσονται σε χαμηλού, μεσαίου, υψηλού ή πολύ υψηλού επιπέδου και στην συνέχεια χαρακτηρίζονται ως ‘αποδεκτοί’ και ‘μη αποδεκτοί’. Οι χαμηλού επιπέδου κίνδυνοι, γίνονται αποδεκτοί από την εταιρία και δεν απαιτούνται περεταίρω μέτρα ελέγχου, ενώ οι μεσαίου επιπέδου γίνονται αποδεκτοί και επανεξετάζονται έπειτα από ένα χρονικό διάστημα. Από την άλλη, οι κίνδυνοι υψηλού και πολύ υψηλού επιπέδου δεν γίνονται αποδεκτοί και πρέπει να καταγραφούν τα προληπτικά μέτρα που θα εφαρμοστούν για την αντιμετώπισή τους.

ΤΟ ΣΚΕΠΤΙΚΟ ΕΝΟΣ ΕΙΣΒΟΛΕΑ- ΜΙΑ ΜΑΤΙΑ ΑΠΟ ΤΗ ΣΚΟΠΙΑ ΤΟΥ ΕΠΙΤΙΘΕΜΕΝΟΥ

Είναι αντιληπτό ότι όσο μεγαλύτερη είναι η αξία των πόρων που θέλουμε να διαφυλάξουμε, τόσο μεγαλύτερη είναι και η ανάγκη για ασφάλεια. Προτεραιότητα κατά τη διαδικασία του σχεδιασμού και της εφαρμογής των μηχανισμών ασφαλείας είναι ο εντοπισμός των απειλών ώστε να μπορέσουμε να σχηματίσουμε ένα προφίλ για τον επιτιθέμενο. Το προφίλ αυτό έχει άμεση σχέση με τους πόρους που βρίσκονται υπό προστασία αφού όσο πιο πολύτιμοι είναι, τόσο πιο στοχευμένες, έξυπνες και πολύπλοκες θα είναι αντίστοιχα και οι επιθέσεις που θα εξαπολύονται από τους εισβολείς. Υπάρχουν διάφορα κίνητρα που μπορούν να υποκινήσουν επιθέσεις όπως είναι τα οικονομικά, τα πολιτικά, τα στρατιωτικά ή οι ιδεολογικές αντιλήψεις. Οι στόχοι που μπορεί να έχει μια επίθεση μπορεί να είναι προσωπικά ή χρηματοπιστωτικά δεδομένα, απόρρητες πληροφορίες και έγγραφα μιας επιχείρησης ή προγράμματα. Με βάση τα κίνητρά των επιτιθέμενων, οι κατηγορίες των εισβολών διακρίνονται ως εξής:

- Κυβερνο- ακτιβισμός (Cyber activism): Στην κατηγορία των κυβερνο ακτιβιστών συγκαταλέγονται οι βανδαλιστές (vandals) και οι hackers που τελούν ακτιβιστικές ενέργειες στα πλαίσια του κυβερνοχώρου οι οποίες χαρακτηρίζονται από ηλεκτρονική απείθεια κατά των αρχών. Σε γενικές γραμμές, οι hackers είναι άτομα με υψηλό επίπεδο γνώσεων προγραμματισμού που εντοπίζουν και διορθώνουν κενά ασφαλείας σε υπολογιστικά συστήματα χωρίς να έχουν σκοπό να προκαλέσουν κάποια βλάβη ή ζημιά στα δεδομένα. Οι hackers που διαπράττουν ακτιβιστικές ενέργειες με σκοπό να εξυπηρετήσουν πολιτικές, ιδεολογικές ή κοινωνικές απόψεις, ονομάζονται hactivists. Από την άλλη, οι βανδαλιστές είναι και αυτοί hackers που εισβάλλουν σε ένα σύστημα με μοναδικό σκοπό να καταστρέψουν ή να κλέψουν πληροφορίες, υπολογιστές ή και ολόκληρα δίκτυα.
- Κυβερνο- έγκλημα (Cyber crime): Η Επιτροπή Ευρωπαικών κοινοτήτων αποσαφηνίζει το κυβερνοέγκλημα ως το σύνολο των εγκληματικών πράξεων που τελούνται στον κυβερνοχώρο με τη χρήση δικτύων επικοινωνιών και πληροφοριακών συστημάτων ή εναντία αυτών. Πιο συγκεκριμένα προσανατολίζεται σε τρείς κατηγορίες. Η πρώτη αφορά σε ληστείες και απάτες που λαμβάνουν χώρα στον κυβερνοχώρο. Παράδειγμα αυτής της κατηγορίας είναι οι απάτες σε τραπεζικές συναλλαγές και η πώληση κλεμμένων πληροφοριών στην μαύρη αγορά. Η δεύτερη κατηγορία κυβερνοεγκλήματος είναι η δημοσιοποίηση και διακίνηση παράνομου περιεχομένου όπως υλικό παιδικής πορνογραφίας και η πρόκληση φυλετικού μίσους. Η τελευταία κατηγορία περιλαμβάνει τα εγκλήματα που απεθύνονται αποκλειστικά σε συστήματα διασυνδεδεμένων ηλεκτρονικών συσκευών. Τέτοια μπορεί να είναι οι επιθέσεις σε πληροφοριακά συστήματα ή οι επιθέσεις άρνησης εξυπηρέτησης και μπορούν να εξαπολυθούν και σε κρίσιμες υποδομές προκαλώντας καταστροφικά αποτελέσματα.
- Κυβερνο- κατασκοπεία (Cyber espionage): Η κατασκοπεία στον κυβερνοχώρο περιλαμβάνει πράξεις που αποβλέπουν στην απόκτηση μυστικών πληροφοριών από ιδιώτες (απλούς χρήστες), ομάδες ατόμων, κυβερνήσεις και ανταγωνιστές εταιριών με πολιτικό στρατιωτικό ή οικονομικό όφελος χρησιμοποιώντας αθέμιτες μεθόδους. Οι ενέργειες αυτές λαμβάνουν χώρα στο Διαδίκτυο, σε δικτυωμένα συστήματα, υπολογιστές και προγράμματα.
- Κυβερνο- τρομοκρατία (Cyber terrorism): Οι τρομοκράτες του κυβερνοχώρου είναι ένα φαινόμενο που έκανε την εμφάνισή του τα τελευταία χρόνια. Η εξέλιξη της τεχνολογίας, των δικτύων και των δικτυακών εφαρμογών ευνόησε την ανάπτυξη των δεξιοτήτων τους. Η βασική τους διαφορά με τους τρομοκράτες είναι ότι επιτίθενται απομακρυσμένα χωρίς να διατρέχουν

κάποιο φυσικό κίνδυνο. Στόχος τους είναι να εκτελούν επιθέσεις σε κρίσιμα συστήματα τεχνολογίας πληροφοριών και η δράση τους επικεντρώνεται στο να προκαλέσουν φυσικές ζημιές στο σύστημα και τον εξοπλισμό του.

- Κυβερνο- πόλεμος (Cyber warfare): Πρόκειται για τη διαδικασία του ίδιου του πολέμου σε ένα ηλεκτρονικό πεδίο μάχης κάνοντας χρήση ψηφιακών όπλων (όπως για παράδειγμα το StuxNet). Περιλαμβάνει επιθετικές αλλά και αμυντικές διεργασίες που σχετίζονται με τις απειλές των κυβερνοεπιθέσεων, της κατασκοπείας και της δολιοφθοράς. Πραγματεύεται τις ενέργειες ενός έθνους να διεισδύσει σε υπολογιστές και δίκτυα άλλων εθνών με σκοπό την προξένιση βλαβών ή και διακοπής λειτουργίας των συστημάτων. Ωστόσο υπάρχουν και άλλοι ορισμοί στους οποίους περιλαμβάνονται μη πολιτειακοί παράγοντες όπως ομάδες τρομοκρατών, εταιρίες, πολιτικοί ή ιδεολογικοί εξτρεμιστές και διεθνικοί εγκληματικοί οργανισμοί. Για ορισμένες κυβερνήσεις ο κυβερνοπόλεμος αποτελεί θέμα μείζονος σημασίας στον σχεδιασμό της στρατιωτικής στρατηγικής τους, με κάποιες να έχουν επενδύσει πολλά στην ανάπτυξη των ικανοτήτων τους. [14]

ΚΕΦΑΛΑΙΟ 2 ΑΠΕΙΛΕΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

ΕΥΠΑΘΕΙΕΣ ΠΟΥ ΕΚΜΕΤΑΛΛΕΥΟΝΤΑΙ ΟΙ ΠΑΡΑΒΑΤΕΣ

Η ανάγκη των ανθρώπων να χρησιμοποιούν ψηφιακές πλατφόρμες και διασυνδεδεμένες συσκευές για την περάτωση των καθημερινών τους υποχρεώσεων, εγείρει καθημερινά νέα ζητήματα ασφάλειας. Με την εμφάνιση νέων τεχνολογιών αλλά και την εξέλιξη αυτών που υπάρχουν ήδη (όπως είναι οι έξυπνες συσκευές, το διαδίκτυο των πραγμάτων και οι εφαρμογές cloud) εμφανίζονται νέες προκλήσεις και απειλές για την κυβερνοασφάλεια. Οι επιτιθέμενοι αναγκάζονται να εμπλουτίσουν τις γνώσεις τους και να εξελίξουν τις ικανότητές τους ανακαλύπτοντας συνεχώς καινούριες τεχνικές και τεχνάσματα για να επιτύχουν τον σκοπό τους. Αυτό αποτελεί και τη μεγαλύτερη απειλή στον κυβερνοχώρο καθώς ο αριθμός των επιθέσεων αυξάνεται με τον χρόνο, παράλληλα, αυξάνεται και η ένταση της καταστροφής που αυτές επιφέρουν. Σκοπός των κυβερνοεπιθέσεων είναι να αποκτήσουν πρόσβαση σε υπολογιστικά συστήματα ή και να διακόψουν τελείως τη λειτουργία τους.
Η προδιαγραφή RFC2828 , ορίζει την επίθεση ως την προσβολή της ασφάλειας του συστήματος που προέρχεται από μια έξυπνη απειλή. Πρόκειται δηλαδή, για μια ευφυή πράξη που αποτελεί σκόπιμη απόπειρα (ειδικά με την έννοια μιας μεθόδου ή τεχνικής) για την παράκαμψη των υπηρεσιών ασφαλείας και τη παραβίαση ενός συστήματος.
Η ίδια προδιαγραφή, ορίζει την απειλή ως τη δυνατότητα για παραβίαση της ασφάλειας, η οποία υπάρχει όταν μπορεί να υφίσταται κάποιο περιστατικό, δυνατότητα, ενέργεια ή συμβάν που επιτρέπει την παραβίαση της ασφάλειας με πιθανές αρνητικές συνέπειες. Με άλλα λόγια η απειλή είναι ο κίνδυνος να εκμεταλλευτεί κάποιος μια ευπάθεια.
Πρώτου όμως ταξινομήσουμε και αναλύσουμε τα είδη των επιθέσεων που τελούνται στα πλαίσια του κυβερνοχώρου, θα πρέπει πρώτα να μελετήσουμε τις τρωτότητες που πιθανόν να υπάρχουν σε ένα υπολογιστικό σύστημα, σε τι οφείλονται και πώς μια απειλή μπορεί να καταλήξει σε επίθεση αν κάποιος την εκμεταλλευτεί. Οι τρωτότητες ή αλλιώς ευπάθειες όπως τις έχουμε ήδη αναφέρει, μπορεί να είναι αδυναμίες στην τεχνολογία, στο σχεδιασμό του υπολογιστικού συστήματος ή ακόμη και στην πολιτική ασφαλείας του, σε οποιαδήποτε περίπτωση θα πρέπει να αναφέρονται και να γνωστοποιείται όταν εντοπίζονται ώστε να αποφεύγονται απειλές που θα μπορούσαν να τις εκμεταλλευτούν. [15]

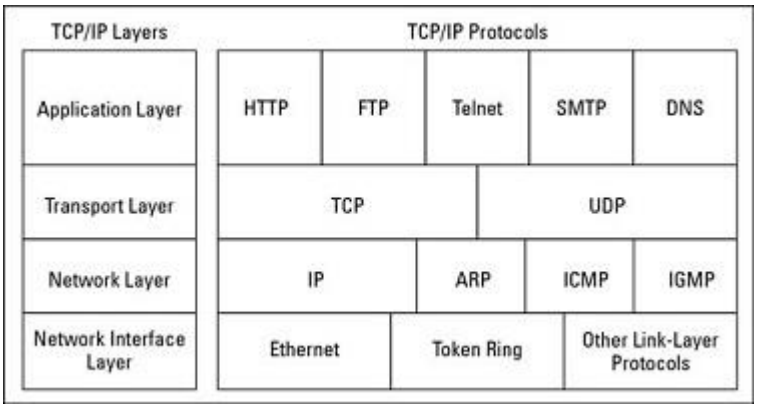
ΕΥΠΑΘΕΙΕΣ ΣΤΑ ΤΕΧΝΟΛΟΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Οι τεχνολογίες υπολογιστών και δικτύων έχουν εγγενείς αδυναμίες στην ασφάλεια που μπορεί να αφορούν:

- Αδυναμίες στη λειτουργία του πρωτοκόλλου TCP/IP
- Αδυναμίες του λειτουργικού συστήματος
- Αδυναμίες στον εξοπλισμό

Αδυναμίες στη λειτουργιά του πρωτοκόλλου TCP/IP

Η σουίτα πρωτοκόλλων του TCP/IP είναι μια ομάδα από διαφορετικά πρωτόκολλα επικοινωνίας που λειτουργούν μέσω του διαδικτύου και άλλων ιδιωτικών επικοινωνιακών δικτύων. Το πρότυπο TCP/IP είναι ένα σύστημα από κανόνες που ορίζουν την επικοινωνία σε δίκτυα TCP/IP. Η αντίστοιχη υλοποίηση (implementation), είναι το λογισμικό που χρησιμοποιείται για την εκτέλεση της μορφοποίησης και επεξεργασίας των μεταδόσεων και αποτελεί τη διεπαφή ανάμεσα στον κόμβο και στο δίκτυο. Το TCP/IP φέρνει σε πέρας τις βασικότερες υπηρεσίες του διαδικτύου καθώς παρέχει συνδεσιμότητα από άκρο σε άκρο εγκαθιδρύοντας, διατηρώντας και απελευθερώνοντας συνδέσεις μεταξύ του αποστολέα και του παραλήπτη. Η προσπάθεια δημιουργίας ενός ευέλικτου συστήματος πρωτοκόλλου που θα μπορούσε να υποστηρίξει μεγάλη ποικιλία υλικού και να παρέχει ένα ευπροσάρμοστο, εφεδρικό και αποκεντρωμένο σύστημα παράδοσης δεδομένων σε παγκόσμια κλίμακα ήταν η πρώιμη εμφάνιση του TCP/IP (προηγουμένως είχε την ονομασία Arpanet).
Το TCP/IP αποτελείται από μια διαστρωματοποιημένη αρχιτεκτονική τεσσάρων επιπέδων, το επίπεδο εφαρμογής, το επίπεδο μεταφοράς, το επίπεδο δικτύου και το επίπεδο πρόσβασης δικτύου. Κάθε επίπεδο έχει τα δικά του πρωτόκολλα και επιτελεί συγκεκριμένες λειτουργίες. Οι λειτουργίες αυτές αφορούν τον έλεγχο ροής, τον έλεγχο λαθών, τη λογική διευθυνσιοδότηση και την δρομολόγηση της κίνησης σε ένα δίκτυο.
Ωστόσο η σχεδίασή του, όπως αναφέρθηκε, έδινε περισσότερη έμφαση στην ευελιξία του και στην δυνατότητά του να εξυπηρετεί την επικοινωνία μεταξύ ανομοιογενών υπολογιστικών συστημάτων και λιγότερη στην ασφάλεια, που τότε δεν αποτελούσε μεγάλο πρόβλημα. [16][17][18]



Εικόνα 5 TCP/IP και τα πρωτόκολλα που το συνοδεύουν ανά επίπεδο

Σήμερα η λειτουργία του Internet στηρίζεται σε αυτή τη σουίτα πρωτοκόλλων αν και έχουν βρεθεί αρκετά τρωτά σημεία στα επιμέρους πρωτόκολλα. Κάποια από αυτά αναφέρθηκαν και διορθώθηκαν σε νεότερες εκδόσεις (όπως για παράδειγμα το IPv4 σε IPv6) ενώ κάποια άλλα εξακολουθούν να υπάρχουν με αποτέλεσμα να τα εκμεταλλεύονται οι εισβολείς εξαπολύοντας νέες μορφές επιθέσεων.

ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ (APPLICATION LAYER)

Παρέχει εφαρμογές για αντιμετώπιση προβλημάτων δικτύου, μεταφορά αρχείων, απομακρυσμένο έλεγχο και δραστηριότητες στο Internet. Υποστηρίζει επίσης τα API (Application Programming Interface ή διεπαφή) δικτύων που επιτρέπουν σε προγράμματα που είναι γραμμένα για ένα συγκεκριμένο λειτουργικό σύστημα να έχουν πρόσβαση στο δίκτυο. Οι εφαρμογές αυτές οφείλουν να παρέχουν ασφάλεια στα ευαίσθητα δεδομένα που είναι προς αποστολή στο δίκτυο, ωστόσο ήταν ελλιπείς. Οι ευπάθειες ασφαλείας αφορούν τα δύο πιο γνωστά πρωτόκολλα αυτού του επιπέδου.

HTTP (Hypertext Transfer Protocol): Είναι το προεπιλεγμένο πρωτόκολλο επικοινωνίας πελάτη-εξυπηρετητή και χρησιμοποιείται από όλα τα προγράμματα περιήγησης. Το πρωτόκολλο αυτό, καθορίζει τον τρόπο με τον οποίο θα μορφοποιούνται και θα αποστέλλονται τα μηνύματα κατά την επικοινωνία, αλλά και τον τρόπο με τον οποίο θα πρέπει να ανταποκρίνονται οι εξυπηρετητές και οι φυλλομετρητές σε κάθε εντολή που εκτελείται. Η μεταφορά των δεδομένων και των αρχείων στις φόρμες των ιστοσελίδων γίνεται σε μορφή απλού κειμένου. Είναι ωστόσο επιρρεπές σε επιθέσεις κατά της ασφάλειας. Μερικές από αυτές είναι οι παρακάτω:

- Session Hijacking: Για κάθε σύνδεση που εγκαθιδρύεται, υπάρχει ένας μοναδικός αριθμός που την χαρακτηρίζει (session ID)
- Caching
- Cookie poisoning
- Replay attack
- Cross-site Scripting (XSS)

DNS (Domain Name System): Είναι το πρωτόκολλο που μεταφράζει τα ονόματα των διακομιστών σε τις IP διευθύνσεις. Εδώ οι επιθέσεις έχουν να κάνουν με την διαχείριση ή και ανακατεύθυνση της κίνησης σε ένα δίκτυο, σε λάθος προορισμούς. Μερικά παραδείγματα τέτοιων επιθέσεων έχουν ως εξής:

- DNS cache poisoning
- DNS spoofing
- DNS ID hijacking

ΕΠΙΠΕΔΟ ΜΕΤΑΦΟΡΑΣ (TRANSPORT LAYER)

Κύριος σκοπός αυτού του επιπέδου είναι να ελέγχει τη ροή των δεδομένων μεταξύ πελάτη και εξυπηρετητή αποφεύγοντας επαναλήψεις ή παρακάμψεις τμημάτων των δεδομένων. Παρέχει υπηρεσίες γνωστοποίησης για το διαδίκτυο και αποτελεί τη διασύνδεση για τις εφαρμογές του δικτύου. Το TCP πρωτόκολλο αυτού του επιπέδου δημιούργησε ανησυχίες όσον αφορά την αξιοπιστία και την ολοκληρωμένη παράδοση των δεδομένων στον παραλήπτη. Αυτή η ανησυχία έδωσε προβάδισμα στους επιτιθέμενους ώστε να εξαπολύσουν επιθέσεις όπως θα αναλύσουμε και στη συνέχεια.

- TCP (Transmission Control Protocol): Είναι ένα πρωτόκολλο προσανατολισμένο στις συνδέσεις. Παρέχει εκτενή έλεγχο λαθών και ροής για να διασφαλίσει την επιτυχή παράδοση των δεδομένων. Οι ευπάθειές του οφείλονται κυρίως σε σχεδιαστικές αδυναμίες του πρωτοκόλλου αφού δεν περιλάμβανε επαρκείς μηχανισμούς ασφαλείας. Μερικές από αυτές είναι οι εξής:
    - TCP "SYN" attack
    - TCP land attack
    - TCP & UDP port scanning technique
    - TCP sequence number prediction
    - IP half scan attack
    - TCP sequence number generation attack

ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ (INTERNET LAYER)

Παρέχει τη λογική διευθυνσιοδότηση που είναι ανεξάρτητη από το υλικό, έτσι ώστε τα δεδομένα να μπορούν να περνούν σε υποδίκτυα που έχουν διαφορετικές αρχιτεκτονικές. Επίσης παρέχει δρομολόγηση προκειμένου να περιοριστεί η κίνηση και υποστηρίζει παράδοση σε όλο το μήκος του διαδικτύου. Τέλος, συσχετίζει φυσικές με λογικές διευθύνσεις. Τα πρωτόκολλα που χρησιμοποιούνται σε αυτό το επίπεδο είναι το IP, το ARP, το ICMP και το IGMP όπως θα δούμε και στη συνέχεια. Σε αυτό το επίπεδο γίνεται προσπάθεια από τους εισβολείς να αντλήσουν πληροφορίες από τα πακέτα και να έχουν μια εικόνα για την τοπολογία, τους κόμβους και τις διαδρομές εντός ενός δικτύου. Παρακάτω παρατίθενται επιγραμματικά τα πρωτόκολλα που αναφέρθηκαν και επιθέσεις που λαμβάνουν χώρα σε κάθε ένα από αυτά:

- IP (Internet Protocol): Οι βασικότερες λειτουργίες του είναι η διευθυνσιοδότηση, η δρομολόγηση και η μετάδοση των πακέτων μέσα στο δίκτυο.
    - IP Spoofing Attacks
    - .HTTP flooding
    - Password brute-force attempts
    - Web scraping/data harvesting by grey marketers
    - Web scraping/data harvesting by competitors
    - Click jacking

- ARP (Address Resolution Protocol): Εδώ οι κύριες λειτουργίες είναι η απεικόνιση και η αντιστοίχηση των IP διευθύνσεων σε φυσικές διευθύνσεις
    - Connection hijacking and interception
    - Connection reseating
    - Packet sniff
    - Denial of service (DoS)

- ICMP (Internet Control Message Protocol): Είναι πρωτόκολλο που χρησιμοποιείται για λειτουργίες διάγνωσης και αντιμετώπισης προβλημάτων. Είναι υπεύθυνο για την ανίχνευση λαθών στο δίκτυο και την αναφορά τους. Μπορεί να χρησιμοποιηθεί

για ανίχνευση της κίνησης σε ένα δίκτυο και την καταγραφή των διαθέσιμων κόμβων του.
    - ICMP tunnelling
    - Smurf Attack
    - Fraggle attack
- IGMP (Internet Group Management Protocol):
    - Distributed denial of service (DDoS)
    - Multicast routing

Αδυναμίες του λειτουργικού συστήματος

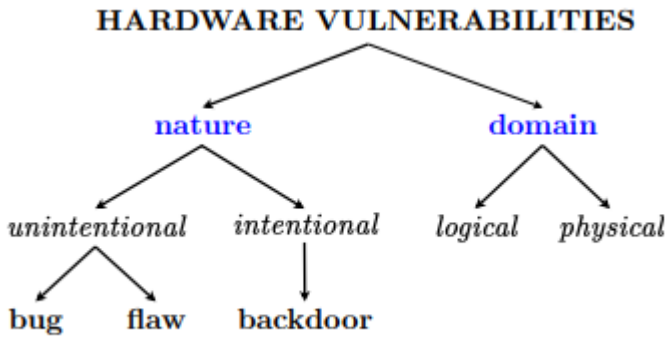
Λειτουργικό σύστημα είναι το λογισμικό που ελέγχει τη συνολική λειτουργία ενός υπολογιστικού συστήματος. Πιο συγκεκριμένα, επιτρέπει σε πολλά προγράμματα και διεργασίες να μοιράζονται ταυτόχρονα τους ίδιους πόρους και παρέχει τα μέσα για την δημιουργία, την αποθήκευση και την ανάκτηση εγγράφων. Το λειτουργικό σύστημα αποτελεί μια διεπαφή λογισμικού, μια διασύνδεση δηλαδή, του υπολογιστικού συστήματος με τον χρήστη. Ωστόσο, οι σύγχρονες πλατφόρμες λογισμικών εκτελούν μεγάλο αριθμό εφαρμογών πολλές από τις οποίες δεν εξασφαλίζουν καμία εγγύηση για την ασφάλεια της μνήμης σε περίπτωση λάθους. Αυτό έχει ως αποτέλεσμα το λειτουργικό σύστημα να είναι ευάλωτο σε επιθέσεις που αφορούν κυρίως στην αλλοίωση της μνήμης , στην αναπροσαρμογή των δικαιωμάτων του χρήστη, και στη μόλυνση του κώδικα προγραμμάτων (αν δεν ληφθούν υπόψην ασφαλείς τεχνικές προγραμματισμού). Οι ευπάθειες αυτές, δίνουν την δυνατότητα στον επιτιθέμενο να αλλάξει την συμπεριφορά και την ροή εκτέλεσης ενός προγράμματος χρησιμοποιώντας κακόβουλες καταχωρήσεις που μεταβάλλουν ή αλλοιώνουν τον χώρο μνήμης του. Παραδείγματα τέτοιων επιθέσεων έχουν ως εξής [19] [20]:

- Buffer Overflow
- Integer Overflow
- Heap Overflow
- Stack Overflow
- SQL injection
- Scripting

Αδυναμίες στον εξοπλισμό

Ο εξοπλισμός (hardware) αποτελεί αδιαμφισβήτητα το βασικό δομικό στοιχείο των υπολογιστικών συστημάτων, καθώς χάρις αυτόν σήμερα παράγεται αλλά και ανταλλάσσεται μεγάλος όγκος δεδομένων. Δρομολογητές (routers), διακόπτες (switches), τείχη προστασίας (firewalls), αφαιρούμενα μέσα και διακομιστές (servers), είναι μόνο μερικά από τα στοιχεία που συγκαταλέγονται στον εξοπλισμό ενός υπολογιστικού συστήματος. Ελαττώματα του εξοπλισμού ωστόσο, μπορεί να αποτελέσουν πηγή ευπαθειών και κατά συνέπεια να θέσουν σε κίνδυνο ολόκληρο το δίκτυο καθιστώντας το ευάλωτο σε διάφορες μορφές επιθέσεων. Οι ευπάθειες του υλικού ταξινομούνται αρχικά με βάση τη φύση και το πεδίο ορισμού τους. Αναφορικά με την φύση τους, μπορεί να είναι απρόθυμες ή επιτηδευμένες. Μπορεί δηλαδή, η

ευπάθεια να εισαχθεί στην εκάστοτε συσκευή με πρόθεση ή όχι, κατά τη διάρκεια της φάσης του σχεδιασμού ή της παραγωγής του υλικού. Στις απρόθυμες αδυναμίες συγκαταλέγονται τα σφάλματα (**bugs**) και οι τεχνολογικές ατέλειες (**flaws**). Στις επιτηδευμένες αδυναμίες από την άλλη, ανήκει η παράνομη πρόσβαση που επιτυγχάνεται με επιθέσεις πίσω πόρτας (**backdoors**).



Εικόνα 6 Ευπάθειες Υλικού

Bug : Πρόκειται για ασυνέπεια μεταξύ μιας προδιαγραφής και της υλοποίησής της, η οποία εισάγεται από λάθος κατά τη διάρκεια της φάσης του σχεδιασμού. Η ασυνέπεια αυτή ωστόσο δεν είναι ανιχνεύσιμη κατά τη διάρκεια της επακόλουθης φάσης της επαλήθευσης και εξακρίβωσης.

Flaw : Οι ατέλειες, από την άλλη αποτελούν χαρακτηριστικό. Δεν είναι ασυνέπειες αλλά το αποτέλεσμα της εσφαλμένης αντίληψης του σχεδιαστή ο οποίος δεν έλαβε υπόψη του την ενδεχόμενη επικινδυνότητα του.

Backdoor : Πρόκειται για ευπάθεια που εισάγεται με πρόθεση σε συσκευές και αναφέρεται ως «ευπάθεια πίσω πόρτας» καθώς το άτομο που τις εισάγει έχει ως στόχο να αποκτήσει τη βεβαιότητα μιας μακροπρόθεσμης πρόσβασης στο σύστημα ή ακόμη και την κατάχρησή του. Παράδειγμα τέτοιας ευπάθειας είναι ο Δούρειος Ίππος του υλικού (Hardware Trojan) ο οποίος τίθεται σε λειτουργία κατόπιν ενεργοποίησης.

Εν αντιθέσει με τη φύση τους, οι ευπάθειες του υλικού ανήκουν σε ένα πεδίο ορισμού το οποίο μπορεί να είναι λογικό ή φυσικό. Στο λογικό πεδίο ορισμού, οι ευπάθειες εισάγονται κατά τα πρώιμα στάδια σχεδίασης της συσκευής. Από την άλλη, μια ευπάθεια ανήκει στο φυσικό πεδίο ορισμού όταν εισάγεται στα τελευταία στάδια χαρτογράφησης της τεχνολογίας, κατά τη διαδικασία σχεδίασής της. Ένα τέτοιο παράδειγμα είναι οι συνεχόμενες εγγραφές σε κελιά μνήμης DRAM (row hammering). Αυτό μπορεί να οδηγήσει σε παράκαμψη του περιεχομένου των γειτονικών κελιών και οφείλεται στο φαινόμενο της διαρροής ηλεκτρικού φορτίου. [21]

ΕΥΠΑΘΕΙΕΣ ΣΤΗΝ ΔΙΑΜΟΡΦΩΣΗ

Οι ευπάθειες στη διαμόρφωση του συστήματος, αποτελούν τρωτά σημεία του υπολογιστικού συστήματος για τα οποία οι διαχειριστές και οι μηχανικοί των δικτύων πρέπει να είναι συνεχώς

ενήμεροι ώστε να τα εντοπίζουν και να τα επανορθώνουν. Οι μη ασφαλισμένοι λογαριασμοί χρηστών , οι κωδικοί που μαντεύονται εύκολα, η κακή διαμόρφωση των διαδικτυακών υπηρεσιών αλλά και του δικτυακού εξοπλισμού καθώς και οι λανθασμένες εργοστασιακές ρυθμίσεις προϊόντων αποτελούν αδυναμίες που αν δεν γίνουν άμεσα αντιληπτές μπορούν να κάνουν το έργο των επιτιθέμενων πιο εύκολο και γρήγορο και να επιφέρουν μη αναστρέψιμα και καταστροφικά για τον χρήστη αποτελέσματα.

ΜΗ ΑΣΦΑΛΙΣΜΕΝΟΙ ΛΟΓΑΡΙΑΣΜΟΙ ΧΡΗΣΤΩΝ

Οι λογαριασμοί χρηστών που αποθηκεύονται σε συσκευές πρέπει να είναι επαρκώς ασφαλισμένοι. Σε διαφορετική περίπτωση τα δεδομένα που μεταδίδονται σε ένα δίκτυο χωρίς να ληφθούν υπόψιν παράμετροι ασφαλείας, είναι δυνατό να εκθέσουν πληροφορίες όπως ονόματα χρηστών και κωδικούς πρόσβασης, κάτι που μπορεί να αποτελέσει απειλή για την ασφάλεια ενός ολόκληρου υπολογιστικού συστήματος. Χαρακτηριστικό παράδειγμα είναι η παρακολούθηση και ανάλυση της κίνησης των πακέτων μέσα σε ένα δίκτυο από επιτιθέμενους που έχουν ως σκοπό τους να αντλήσουν ευαίσθητα δεδομένα των χρηστών.

ΛΟΓΑΡΙΑΣΜΟΙ ΧΡΗΣΤΩΝ ΜΕ ΕΥΚΟΛΟΥΣ ΚΩΔΙΚΟΥΣ ΠΡΟΣΒΑΣΗΣ

Πρόκειται για το σύνηθες πρόβλημα των αδύναμων κωδικών πρόσβασης που είναι εύκολο για κάποιον να τους μαντέψει. Ωστόσο θα πρέπει να εφαρμόζονται μέτρα που να ασφαλίζουν το επίπεδο χρήστη. Σε οργανισμούς και επιχειρήσεις υπάρχει συγκεκριμένη πολιτική που τίθεται από τον διαχειριστή του δικτύου και είναι απαραίτητο να ακολουθείται για τη δημιουργία κωδικών κυρίως σε συσκευές μείζονος σημασίας όπως servers, routers αλλά και σε βάσεις δεδομένων. Οι χρήστες θα πρέπει να μεταβάλλουν τους εργοστασιακούς κωδικούς, να αλλάζουν τακτικά όσους υπάρχουν ήδη, αλλά και να διατηρούν τη μυστικότητά τους προς αποφυγήν διαρροής των ευαίσθητων δεδομένων.

ΔΙΑΜΟΡΦΩΣΗ ΘΥΡΩΝ TCP ΚΑΙ ΤΩΝ ΔΙΑΔΙΚΤΥΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Σε ένα υπολογιστικό σύστημα είναι απαραίτητο να υπάρχει έλεγχος για το ποιές εφαρμογές θα επιτρέπεται να έχουν πρόσβαση σε αυτό και για ποιό σκοπό. Η έλλειψη του ορθού διαχωρισμού τους αποτελεί συχνό πρόβλημα καθώς η λανθασμένη ενεργοποίηση απομακρυσμένων υπηρεσιών και η σάρωση θυρών μπορεί να αποβεί εξίσου μεγάλο ρίσκο.

Ανοιχτές θύρες που δεν φιλτράρονται, μπορεί να επιτρέψουν σε θύτες τη διείσδυση στο σύστημα. Η σάρωση θυρών, πιο συγκεκριμένα, είναι μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, ώστε να ληφθούν πληροφορίες και να αναγνωριστούν οι υπηρεσίες που προσφέρει το εκάστοτε σύστημα. Κάθε φορά που ολοκληρώνεται μια σάρωση, αυτή καταγράφεται αυτόματα σε ένα φάκελο που ονομάζεται log file. Αν μια σάρωση δεν έρθει εις πέρας ολοκληρωμένα, το σύστημα θεωρεί πως δεν συνέβη ποτέ και έτσι δεν καταγράφεται. Ένας τρόπος, για παράδειγμα, που έχουν αναπτύξει οι crackers για να σαρώνουν θύρες χωρίς να γίνονται αντιληπτοί, είναι η half open SYN scan. Με αυτό τον τρόπο σταματάνε τη σάρωση

πριν ολοκληρωθεί ενώ στο μεταξύ το πρόγραμμα βρίσκει την διαθέσιμη ανοιχτή θύρα και εισέρχεται παράνομα στο σύστημα. [22]

Οι σύγχρονες διαδικτυακές υπηρεσίες και τα προγράμματα πλοήγησης επιτελούν ένα πλήθος λειτουργιών που στηρίζονται σε τεχνολογίες όπως της Java Script, της Active-X, των plug-ins και άλλων. Οι λειτουργίες αυτές, επιτρέπουν μια πιο δυναμική διαμόρφωση των περιεχομένων που παρουσιάζονται στον χρήστη. Αυτό γίνεται ουσιαστικά με την εκτέλεση κώδικα, του οποίου η προέλευση σε πολλές περιπτώσεις δεν είναι εγγυημένη και αν επιλέξει ο χρήστης να το εγκαταστήσει, του παραχωρεί στην ουσία κάθε δικαίωμα πρόσβασης στο σύστημά του.

Η **JavaScript** για παράδειγμα, είναι μια γλώσσα προγραμματισμού που έχει ως στόχο να προσδίδει συμπεριφορά στα προγράμματα πλοήγησης. Για να είναι αυτό εφικτό, θα πρέπει ο χρήστης να παραχωρήσει το δικαίωμα πρόσβασης στα αποθηκευμένα δεδομένα που φυλάσσονται στο πρόγραμμα πλοήγησης ή και στο ίδιο το σύστημα. Αυτό όμως μπορεί να οδηγήσει και σε πιθανές ανεπιθύμητες πράξεις. Ένα πρόγραμμα JavaScript είναι δυνατό να υποκλέψει τα στοιχεία από ένα σύστημα και να τα στείλει σε άλλους ή να τα τροποποιήσει. Χωρίς κατάλληλη προστασία, είναι επίσης δυνατό να έχει πρόσβαση σε όλα τα αρχεία του συστήματος ,όπως ακριβώς και ο ίδιος ο χρήστης και μπορεί να τα στείλει οπουδήποτε στο διαδίκτυο. Είναι εξίσου δυνατό, να στείλει μηνύματα ηλεκτρονικού ταχυδρομείου σε λίστα αποδεκτών αλλά και να καθιστά ένα πρόγραμμα που εκτελείται σε ένα παράθυρο, να διαβάζει ή να τροποποιεί στοιχεία ενός προγράμματος που τρέχει παράλληλα σε ένα άλλο παράθυρο με αποτέλεσμα τη διαρροή πληροφοριών. [22]

Τα **cookies** από την άλλη, είναι μικρά αρχεία που υπάρχουν στο πρόγραμμα περιήγησης και στα οποία αποθηκεύονται διάφορες πληροφορίες και προτιμήσεις του χρήστη από την επίσκεψή του σε διάφορες ιστοσελίδες έτσι ώστε η πλοήγησή του στο διαδίκτυο να γίνεται πιο εύχρηστη και άμεση . Υπάρχουν διαφόρων ειδών cookies και αν και είναι ένα καλό εργαλείο μάρκετινγκ, πολλές φορές ωστόσο είναι και επικίνδυνο εφόσον διαχειρίζονται πληθώρα προσωπικών δεδομένων. Πιο συγκεκριμένα, υπάρχουν τα cookies που είναι μόνιμα και περιέχουν ονόματα χρηστών και κωδικούς ώστε να γίνεται αυτόματη η ανάκτησή του σε επόμενες επισκέψεις. Υπάρχουν τα third-party cookies όπου η καταγραφή των προτιμήσεων και των κινήσεων του χρήστη, γίνεται από τρίτους και τέλος, υπάρχουν τα session cookies που παραμένουν όσο διαρκεί η περιήγηση του χρήστη στον ιστότοπο και μετά διαγράφονται. [22]

Η **ActiveX** , είναι μια εφαρμογή κινητού κώδικα που γνωστοποιήθηκε από τη Microsoft. Πρόκειται για εφαρμογή μικρού, κινητού κώδικα τοποθετημένου σε πολλούς, διαφορετικούς ιστοτόπους που στόχο έχει να εμπλουτίζει την περιήγηση των χρηστών με εφέ, κινούμενα σχέδια και βίντεο. Η επικινδυνότητα της βρίσκεται στο ότι έχει πλήρη πρόσβαση στο λειτουργικό σύστημα και γι αυτό τον λόγο απαιτείται προσοχή όταν ζητείται η άδεια του χρήστη για την εγκατάσταση κάποιας σχετικής επέκτασης ακόμη και αν είναι επικυροποιημένη με ψηφιακές υπογραφές. [22]

ΜΗ ΑΣΦΑΛΕΙΣ ΕΡΓΟΣΤΑΣΙΑΚΕΣ ΡΥΘΜΙΣΕΙΣ ΣΕ ΠΡΟΪΟΝΤΑ – ΑΝΕΠΑΡΚΗΣ ΔΙΑΜΟΡΦΩΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΞΟΠΛΙΣΜΟΥ

Οι προκαθορισμένες ρυθμίσεις που εμπεριέχονται σε αρκετά προϊόντα, πολλές φορές δημιουργούν από μόνες τους κενά στην ασφάλεια. Η αλλαγή των εργοστασιακών κωδικών σε δρομολογητές και λογαριασμούς χρηστών, η ενεργοποίηση φιλτραρίσματος των MAC διευθύνσεων, η τροποποίηση και η ενημέρωση του λειτουργικού συστήματος είναι μερικά από τα βήματα που θα πρέπει να ακολουθώνται για την ασφαλή διασύνδεση του χρήστη στο περιβάλλον του κυβερνοχώρου. Η διαμόρφωση του δικτυακού εξοπλισμού είναι ένα ακόμη κομμάτι που εγείρει ανησυχίες όσον αφορά στην ασφάλεια που παρέχει. Υπολογιστικά συστήματα τα οποία πρέπει οπωσδήποτε να είναι σε θέση να προστατέψουν συγκεκριμένες πληροφορίες και υπηρεσίες ή να επιτρέπουν την είσοδο σε συγκεκριμένα άτομα, απαιτείται να υποστηρίζουν ικανότητα ελέγχου πρόσβασης που θα διαμορφώνεται σύμφωνα με την αρχή των ελάχιστων δικαιωμάτων. Με άλλα λόγια, οι διαχειριστές του δικτύου θα πρέπει να αποκλείουν τις ανεπιθύμητες συνδέσεις επιτρέποντας ταυτόχρονα την πρόσβαση όπου χρειάζεται. Σε περιπτώσεις που είναι απαραίτητο να γίνει πρόσβαση σε προστατευόμενους πόρους ενός συστήματος από εξωτερικά δίκτυα, όπως είναι για παράδειγμα η τηλεεργασία, επιχειρήσεις και εργαζόμενοι χρησιμοποιούν τεχνολογίες απομακρυσμένου ελέγχου πρόσβασης. Ωστόσο όσο και αν διευκολύνει αυτή η πρακτική, αυξάνει κατακόρυφα το ρίσκο κυρίως λόγω έλλειψης ελέγχου φυσικής ασφάλειας, τη χρήση μη ασφαλισμένων δικτύων, τη σύνδεση μολυσμένων συσκευών με εσωτερικά δίκτυα και τη διαθεσιμότητα των πόρων τους σε εξωτερικούς κόμβους. [23]Προκειμένου να εξασφαλίσει την είσοδό του σε ένα σύστημα, ο επιτιθέμενος, πρέπει να εντοπίσει κενά ασφαλείας που πιθανόν να υπάρχουν στην άμυνά του και να εκμεταλλευτεί τρωτά σημεία στις υπηρεσίες που επιτρέπονται από τα τείχη προστασ*ίας του. Για τον λόγο αυτό, όλες οι συνδέσεις που επιτρέπονται στο σύστημα θα πρέπει να διαμορφώνονται με ασφάλεια και προσοχή και να παρακολουθούνται, διαφορετικά ο εισβολέας θα είναι σε θέση* να εκμαιεύσει πληροφορίες που αφορούν τη σύνδεση, ακόμη και να την χρησιμοποιήσει για δικούς του σκοπούς .

Οι λίστες πρόσβασης για παράδειγμα είναι ένα ισχυρό εργαλείο διαχείρισης ενός δικτύου. Σε αυτές υπόκειται το φιλτράρισμα της ροής και ο έλεγχος των πακέτων προς και από τις διασυνδέσεις των δρομολογητών. Οι λίστες πρόσβασης, είναι ένας μηχανισμός που μπορεί να περιορίσει την κυκλοφορία του δικτύου επιτρέποντας την πρόσβαση σε συγκεκριμένους χρήστες ή συσκευές. Η πρόσβαση γίνεται με εκχώρηση δικαιωμάτων ανάγνωσης, εγγραφής και τροποποίησης, έτσι, οι διαχειριστές του δικτύου οφείλουν να είναι προσεκτικοί σε ποιούς την επιτρέπουν. Λάθος δικαιώματα σε λάθος χρήστες μπορεί να καταλήξουν σε μεγάλες απώλειες δεδομένων. [24] Η κρυπτογράφηση των δεδομένων, όπως θα δούμε και στη συνέχεια, είναι από τις βασικότερες απαιτήσεις της ασφάλειας και αναπόσπαστο μέρος της. Είναι στην ουσία τεχνική απόκρυψης μηνυμάτων μέσω υλοποίησης κατάλληλων αλγορίθμων και αποτελεί μια μέθοδο διασφάλισης των διακινούμενων δεδομένων και των οντοτήτων που συναλλάσσονται. Όσο όμως οι απαιτήσεις για την ασφάλεια μεγαλώνουν με την ανάδυση νέων τεχνολογιών, αναλογικά μεγαλώνει και η ανάγκη για ισχυρότερα εργαλεία προστασίας της πληροφορίας που μεταδίδεται. Η χρήση ελεύθερων προγραμμάτων κρυπτολογίας από το διαδίκτυο, η ελλιπής διαχείριση των κλειδιών που χρησιμοποιούνται, η χρήση πρωτοκόλλων που αδυνατούν να καλύψουν τις σύγχρονες απαιτήσεις ασφαλείας (MD4 ,MD5) είναι πιθανό να δώσουν στον επιτιθέμενο το προβάδισμα για μη εξουσιοδοτημένη πρόσβαση σε αρχεία, κωδικούς ή και ολόκληρο το σύστημα. [24]

ΕΥΠΑΘΕΙΕΣ ΣΤΗΝ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η πολιτική ασφαλείας είναι το έγγραφο που συντάσσεται από τον διαχειριστή ή τους διαχειριστές του δικτύου μιας επιχείρησης ή ενός οργανισμού. Περιγράφει τις διαδικασίες που πρέπει να λαμβάνουν χώρα στο σύστημα ώστε να το καταστίσουν ασφαλές, εγκαθιστά τους συμπεριφορικούς κανόνες των χρηστών και ορίζει τις επιπτώσεις τυχόν παραβιάσεων. Κάθε οργανισμός θα πρέπει να έχει εγγράφως διαμορφωμένη την πολιτική ασφαλείας του και να γνωστοποιεί τους κανονισμούς και το νομοθετικό πλαίσιο μέσα στο οποίο θα λειτουργεί. Θα πρέπει τακτικά να επαναπροσδιορίζεται ώστε και οι χρήστες να είναι με τη σειρά τους να είναι ενήμεροι για νέες απειλές και προκλήσεις για την ασφάλεια των πόρων που χειρίζονται καθημερινά. Η ελλιπής πολιτική ασφαλείας που αφορά στις εγκαταστάσεις και στις ενημερώσεις του υλικού και του λογισμικού, η απουσία ανάκαμψης έπειτα από καταστροφές, η έλλειψη συνοχής του επιχειρησιακού πλάνου, αθέμιτες τροποποιήσεις στο σύστημα αλλά και μη εξουσιοδοτημένες εγκαταστάσεις εφαρμογών μπορεί να κάνουν το δίκτυο ευάλωτο σε επιθέσεις. Σε περίπτωση που τα παραπάνω δεν ληφθούν υπόψιν κατά τη σύνταξη της πολιτικής ασφαλείας, η εκάστοτε επιχείρηση ή οργανισμός δύναται να αντιμετωπίσει προβλήματα απώλειας σημαντικών πόρων, δυσφήμισης ακόμη και αποχώρηση πελατών που χάνουν την εμπιστοσύνη τους στη φερεγγυότητά της.

Η πολιτική ασφαλείας λειτουργεί ως κατευθυντήρια οδηγός για τους υπαλλήλους καθώς υποδεικνύει ασφαλείς τρόπους μεταχείρισης των ευαίσθητων δεδομένων. [25]

ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ

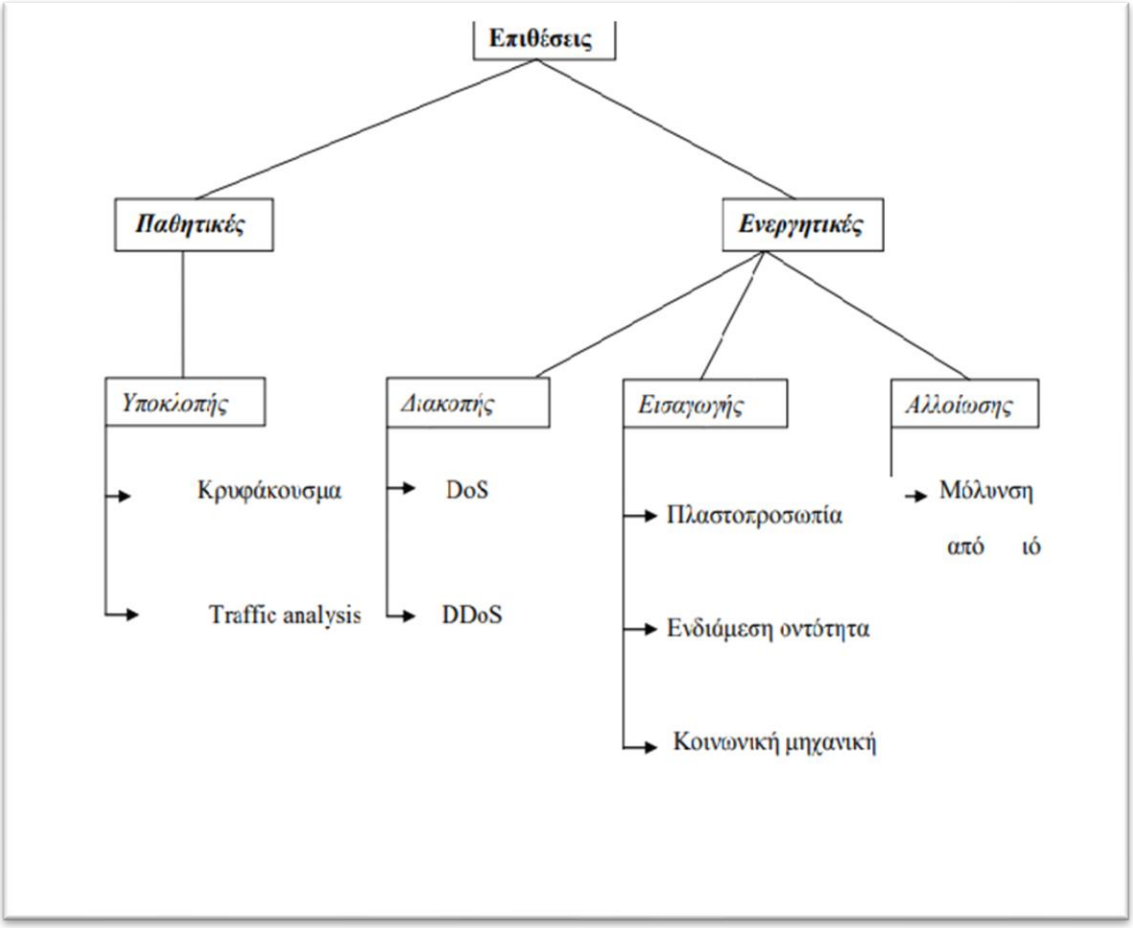
Η σημερινή εποχή χαρακτηρίζεται από δύο όψεις του ίδιου νομίσματος. Η μια όψη περιλαμβάνει την εύρεση νέων ευπαθειών και την εκμετάλλευσή τους από τους θύτες με σκοπό να διεισδύσουν σε δίκτυα και υπολογιστικά συστήματα. Η άλλη όψη περιγράφει τον αγώνα για την διόρθωσή αυτών των ευπαθειών καθώς και την προστασία τους από προγράμματα που τις εκμεταλλεύονται (exploits).

Η επίθεση είναι ένας όρος που απασχολεί σε σημαντικό και ολοένα αυξανόμενο βαθμό οργανισμούς, επιχειρήσεις αλλά και απλούς πολίτες.

Έγινε ήδη αναφορά στο προηγούμενο κεφάλαιο, για τις βασικές αρχές που διέπουν την κυβερνοασφάλεια. Αυτές είναι η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα. Η παραβίαση αυτών των αρχών είναι η πράξη που ονομάζεται επίθεση σε ένα δίκτυο ή σε ένα υπολογιστικό σύστημα και αποσκοπεί στο να εμποδίσει να παρακάμψει τους μηχανισμούς ασφαλείας και ελέγχου του ή και να το αχρηστεύσει τελείως.

Επιθέσεις πραγματοποιούνται καθημερινά ανά τον κόσμο για διάφορους λόγους. Πολλοί είναι οι επιτιθέμενοι που εισβάλουν σε κάποιο σύστημα με σκοπό την κλοπή αριθμών λογαριασμού, ταυτοτήτων και πιστωτικών καρτών για οικονομικό τους όφελος. Οργανισμοί και εταιρίες διαπράττουν επιθέσεις με σκοπό να κατασκοπεύσουν και να υποκλέψουν στοιχεία από ανταγωνιστές τους, ώστε να αποκτήσουν στρατηγικό πλεονέκτημα. Κακόβουλοι χρήστες που θέλουν να κάνουν ζημιά επειδή ένιωσαν ότι αδικήθηκαν στο παρελθόν όπως είναι για παράδειγμα δυσαρεστημένοι πρώην υπάλληλοι εταιριών αλλά και όσοι επιτίθενται από περιέργεια και για διασκέδαση μπορούν να προκαλέσουν ζημιά εν αγνοία τους. Τέλος, μεγάλο

κομμάτι των κυβερνοεπιθέσεων είναι εκείνες που τελούνται για πολιτικούς λόγους, με σκοπό την δημόσια αποκάλυψη τεκμηρίων που έχουν να κάνουν με δολιοφθορές.
Λαμβάνοντας υπόψιν παράγοντες όπως την θέση των συστημάτων που παίρνουν μέρος σε μια επίθεση, τον τρόπο τέλεσής της, τον βαθμό αλληλεπίδρασης του θύτη με τον ή τους στόχους του αλλά και τα αποτελέσματα που θα επιφέρει, οι επιθέσεις μπορούν να ταξινομηθούν σε κατηγορίες όπως φαίνεται στην παρακάτω εικόνα. Οι επιθέσεις που περιλαμβάνονται σε κάθε μια από αυτές τις κατηγορίες, είναι δυνατόν να επηρεάσουν μια ή παραπάνω από μια αρχές της κυβερνοασφάλειας οι οποίες είναι η Ακεραιότητα, η Εμπιστευτικότητα, και η Διαθεσιμότητα. Οι δύο βασικές κατηγορίες είναι οι παθητικές και οι ενεργητικές επιθέσεις.



Εικόνα 7 Κατηγοριοποίηση των επιθέσεων

ΠΑΘΗΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Στις παθητικές επιθέσεις, ο επιτιθέμενος επιδιώκει να έχει την ελάχιστη κατά το δυνατό αλληλεπίδραση με τον στόχο του. Οι ενέργειες που εκτελεί δεν φέρουν κάποια αλλαγή στην κατάσταση του θύματος καθώς ο στόχος δεν είναι να το βλάψουν άμεσα. Ο επιτιθέμενος

περιορίζεται στην απλή παρακολούθηση της διακινούμενης πληροφορίας με απώτερο σκοπό την υποκλοπή δεδομένων. Οι τεχνικές που χρησιμοποιούνται στις παθητικές επιθέσεις αφορούν κυρίως στην ανίχνευση και αποκάλυψη του περιεχομένου των διακινούμενων πακέτων σε ένα δίκτυο, δίχως όμως να το μεταβάλλουν καθώς και την ανάλυση της κίνησης του δικτύου-στόχου όπου υπάρχει η δυνατότητα εύρεσης του τύπου της επικοινωνίας από τη συχνότητα των πακέτων αλλά και από το μέγεθός τους. Οι παθητικές επιθέσεις είναι δύσκολα ανιχνεύσιμες καθώς το θύμα δεν αντιλαμβάνεται την επίθεση εγκαίρως. Στην κατηγορία των παθητικών επιθέσεων ανήκουν οι επιθέσεις της ***υποκλοπής (interception)*** και αποτελούν επιθέσεις έναντι στην αρχή της εμπιστευτικότητας. [26][27][28]

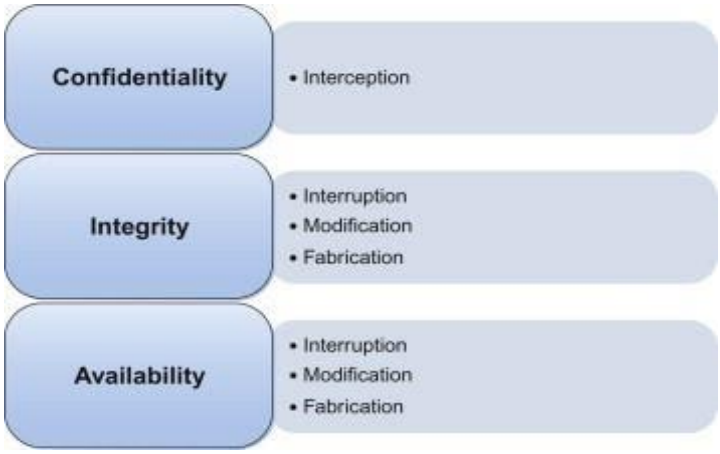
ΕΝΕΡΓΗΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Εν αντιθέσει με τις παθητικές επιθέσεις, στις ενεργητικές ο επιτιθέμενος επιδιώκει να διεισδύσει παράνομα σε ένα σύστημα με σκοπό να κάνει μη εξουσιοδοτημένες αλλαγές σε αυτό και να μεταβάλλει τους πόρους του ή να επηρεάσει την λειτουργία τους. Τέτοιες ενέργειες είναι, για παράδειγμα, η τροποποίηση των διακινούμενων ή αποθηκευμένων δεδομένων και η δημιουργία νέων ροών δεδομένων και είναι επιθέσεις ενάντια στην ακεραιότητα και την διαθεσιμότητα του συστήματος. Οι ενεργητικές επιθέσεις είναι εύκολα ανιχνεύσιμες καθώς το θύμα αντιλαμβάνεται άμεσα τις επιπτώσεις. Η αντιμετώπισή τους ωστόσο αποτελεί πρόβλημα εφόσον όσο μεγαλύτερη η προσπάθεια που απαιτείται για να τελεστεί μια επίθεση, τόσο πιο καταστροφικά θα είναι και τα αποτελέσματα που αυτή θα επιφέρει. Στις ενεργητικές επιθέσεις συγκαταλέγονται οι επιθέσεις **διακοπής (interruption)**, οι επιθέσεις **εισαγωγής (fabrication)** και οι επιθέσεις **αλλοίωσης (modification)** τις οποίες και θα αναλύσουμε στο αμέσως επόμενο υποκεφάλαιο . [26][27][28]

ΑΝΑΛΥΣΗ ΤΩΝ ΕΠΙΘΕΣΕΩΝ

ΕΠΙΘΕΣΕΙΣ ΥΠΟΚΛΟΠΗΣ (INTERCEPTION ATTACKS)

Καθημερινά διακινείται στον κυβερνοχώρο τεράστιος όγκος προσωπικών δεδομένων από χρηματοπιστωτικά ιδρύματα, ιδιωτικές εταιρείες και δημόσιες υπηρεσίες τα οποία σε συνδυασμό με την ικανότητα των υπολογιστών να παρακολουθούν και να καταγράφουν στοιχεία και κινήσεις φυσικών προσώπων οδηγούν στην πρόκληση επιθέσεων που προσβάλλουν τις τρεις βασικότερες αρχές της κυβερνοασφάλειας. Στον όρο προσωπικά δεδομένα περιλαμβάνεται κάθε πληροφορία που περιγράφει ένα πρόσωπο όπως είναι το όνομά του, το επώνυμο, το επάγγελμα και η οικογενειακή του κατάσταση. Εδώ, αξίζει να σημειωθεί, ότι η αποκάλυψη προσωπικών δεδομένων που είναι καταχωρημένα σε ένα πληροφοριακό σύστημα αποτελεί παράβαση του θεσμικού πλαισίου περί Προστασίας Προσωπικών Ατομικών Δεδομένων και διώκεται ποινικά.



Εικόνα 8 Είδη επιθέσεων που αντιστοιχούν στις θεμελιώδεις αρχές Κυβερνοασφάλειας

Συγκεκριμένα, η υποκλοπή συνιστά μορφή παθητικής επίθεσης κατά της εμπιστευτικότητας των πληροφοριακών συστημάτων από κάποιο πρόσωπο, από κάποιο πρόγραμμα ή σύστημα υπολογιστή. Οι επιθέσεις υποκλοπής κατά βάση περιλαμβάνουν τη μη εξουσιοδοτημένη είσοδο των χρηστών σε δεδομένα, εφαρμογές και περιβάλλοντα εργασίας. Ο εκάστοτε επιτιθέμενος δύναται να εγκαθιδρύσει δικές του ροές δεδομένων ή να παρακολουθεί τις ροές δεδομένων που εξελίσσονται ήδη από και προς τον στόχο με σκοπό να συλλέξει πληροφορίες είτε για δικό του όφελος, είτε με σκοπό να τις αποκαλύψουν σε τρίτους έναντι κάποιου οικονομικού ανταλλάγματος, ή ακόμη και να τις χρησιμοποιήσει για κάποια μεταγενέστερη επίθεση. Στις επιθέσεις υποκλοπής γενικότερα γίνεται απόπειρα εξαπάτησης του χρήστη από επιτήδειους με διάφορες τεχνικές έχοντας ως απώτερο στόχο ο πρώτος να αποκαλύψει πληροφορίες που θα κάνουν εύκολη την πρόσβαση του στο σύστημα. Οι δύο βασικές κατηγορίες επιθέσεων υποκλοπής είναι το **κρυφάκουσμα** (packet sniffers) και η **ανάλυση κίνησης** (traffic analysis) και περιγράφονται παρακάτω.

- **ΚΡΥΦΑΚΟΥΣΜΑ (PACKET SNIFFERS):**

Πρόκειται για μέθοδο υποκλοπής των πακέτων που διασχίζουν ένα δίκτυο. Ο κακόβουλος χρήστης εντοπίζει τα πακέτα που μπορεί να περιέχουν χρήσιμα δεδομένα τα οποία ανήκουν σε άλλους χρήστες μέσα στο τοπικό δίκτυο, χωρίς όμως να τα τροποποιήσει. Η τεχνική αυτή είναι αποτελεσματική είτε το δίκτυο είναι μεταγωγής είτε όχι, με τη διαφορά ότι στα δίκτυα μεταγωγής τα πακέτα αποστέλλονται μόνο στον κόμβο προορισμού και όχι σε όλο το δίκτυο, κάτι που δυσκολεύει την ανίχνευση της κίνησης. Οι ωτοακουστές είναι ουσιαστικά προγράμματα που εγκαθίστανται σε ένα υπολογιστικό σύστημα και μπορούν να αποτελέσουν ισχυρό όπλο για τέλεση κακόβουλων πράξεων όπως για παγίδευση(wiretapping) και για ηλεκτρονική παρείσφρηση (hacking), αυτό εξαρτάται από τις προθέσεις του εκάστοτε χρήστη. Από την άλλη, οι packet sniffers χρησιμοποιούνται σε συστήματα ανίχνευσης εισβολών και στη διαχείριση δικτύων και μπορούν να αποτελέσουν χρήσιμα εργαλεία για τους διαχειριστές, ώστε να είναι σε θέση να παρακολουθούν και να επιβεβαιώνουν την ορθή κίνηση των πακέτων εντός ενός δικτύου

καθώς και να συλλέγουν και να καταγράφουν πληροφορίες που αφορούν σε όλα ή επιλεγμένα πακέτα που μεταδίδονται μέσα σε αυτό, άσχετα με την διευθυνσιοδότησή τους. Οι ωτοακουστές, παρέχουν σημαντικές πληροφορίες του συστήματος που σχετίζονται με την κίνηση και τα πρωτόκολλα που χρησιμοποιούνται στις εφαρμογές ηλεκτρονικού ταχυδρομείου (SMTP, POP, IMAP) και στο διαδίκτυο (HTTP), αλλά και στο πρωτόκολλο μεταφοράς αρχείων FTP (Telnet authentication, FTP passwords, SMB, NFS). Στα δίκτυα οι ωτοακουστές «πιάνουν» μόνο τα πακέτα που αντιστοιχούν σε έναν συγκεκριμένο παραλήπτη, ωστόσο, αν τεθεί σε συγκεκριμένη λειτουργία (*promiscuous mode),* είναι δυνατό να ανιχνεύει πακέτα κατευθυνόμενα προς όλους τους προορισμούς**.** Υπάρχει πληθώρα προγραμμάτων που εκτελούν λειτουργίες ανιχνευτών με διάφορες μεθόδους άλλα αυτό είναι κάτι που θα αναλυθεί σε επόμενο κεφάλαιο. [29] [30]

- **ΑΝΑΛΥΣΗ ΚΙΝΗΣΗΣ (TRAFFIC ANALYSIS):**

Η ανάλυση κίνησης μπορεί να χαρακτηριστεί και ως η διαδικασία που ακολουθεί την παρατήρηση της συμφόρησης των ροών δεδομένων σε ένα δίκτυο. Περιλαμβάνει την ανίχνευση, την καταγραφή και την ανάλυση μοτίβων επικοινωνίας έτσι ώστε να υπάρχει έγκαιρος εντοπισμός και αντιμετώπιση σε απειλές κατά της ασφάλειας που πιθανόν να προκύψουν, ακόμη και αν τα μηνύματα που ανταλλάσσονται, είναι κρυπτογραφημένα. Για να γίνει αυτό εφικτό, γίνεται χρήση ωτοακουστών και αναλυτών πρωτοκόλλων οι οποίοι αναλαμβάνουν να συλλέξουν τη διακινούμενη πληροφορία, να αποκωδικοποιήσουν τα πακέτα δεδομένων που ανταλλάσσονται μεταξύ των πρωτοκόλλων και τέλος, να αποδώσουν την κίνηση του δικτύου σε αναγνώσιμη μορφή. Η ανάλυση κίνησης χρησιμοποιείται από επιτιθέμενους που επιδιώκουν να βρουν τρόπους διείσδυσης σε ένα σύστημα και να παραβιάσουν δεδομένα. Ωστόσο, ανάλυση κίνησης χρησιμοποιούν και οι διαχειριστές των σύγχρονων δικτύων με σκοπό να επιλύουν γρήγορα πιθανά προβλήματα εντός των δικτύων και να διαχειρίζονται την ασφάλειά τους. Η ανάλυση κίνησης αποτελεί σημαντικό κομμάτι στην λειτουργικότητα και την διαχείριση των δικτύων καθώς καθιστά πιο άμεση την ανίχνευση απειλών και κακόβουλων λογισμικών. Αυτό επιτυγχάνεται παρακολουθώντας την αυξημένη κίνηση μεταξύ των κόμβων του δικτύου και δίνει το έναυσμα για περεταίρω ανάλυση. [31][32]

ΕΠΙΘΕΣΕΙΣ ΔΙΑΚΟΠΗΣ (INTERRUPTION ATTACKS)

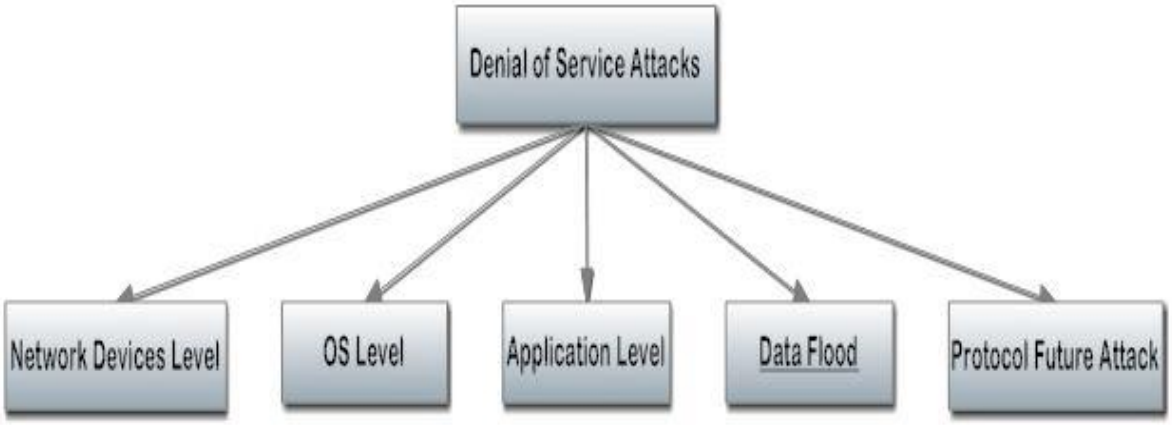
Οι επιθέσεις διακοπής είναι ενεργητικές επιθέσεις που δρουν κατά της αρχής της διαθεσιμότητας. Στόχος των επιθέσεων διακοπής είναι να καταστίσουν τους πόρους ενός συστήματος μη διαθέσιμούς (unavailable) ή ακατάλληλους για χρήση (unusable) για ένα συγκεκριμένο χρονικό διάστημα ή και μόνιμα. Στις επιθέσεις διακοπής συγκαταλέγονται ενέργειες όπως η κακόβουλη καταστροφή ενός δικτύου, η διαγραφή ενός προγράμματος και των δεδομένων που περιέχονται σε αυτό αλλά και η ολοκληρωτική αποκοπή της σύνδεσης. Στην κατηγορία αυτών των επιθέσεων ανήκουν οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service, DoS), οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (Distributed Denial of Service, DDoS) . [33]

- **DOS ΕΠΙΘΕΣΕΙΣ**

Οι επιθέσεις άρνησης εξυπηρέτησης είναι από τις επικινδυνότερες επιθέσεις που μπορούν να λάβουν δράση σε ένα δίκτυο υπολογιστών. Ο επιτιθέμενος που εξαπολύει μια τέτοια επίθεση, έχει ως στόχο του να κατακλύσει τον εξυπηρετητή του δικτύου με πληθώρα πακέτων (συνήθως με ερωτήματα, queries, ή πακέτα τύπου ICMP) έτσι ώστε το δίκτυο να υπερφορτωθεί με αιτήματα συνδέσεων και να μην είναι πλέον σε θέση να προσφέρει τις υπηρεσίες του, ή ακόμη και να καταρρεύσει τελείως. Στις επιθέσεις άρνησης εξυπηρέτησης, με άλλα λόγια, γίνεται προσπάθεια εξάντλησης των πόρων του δικτύου έτσι ώστε οι θύτες να έχουν τη δυνατότητα να παρεμποδίσουν την επικοινωνία μεταξύ δύο κόμβων του, τη μετάδοση δεδομένων εντός αυτού, ή ακόμη και την αλλοίωση των υπηρεσιών που αυτό παρέχει. Υπάρχουν τρείς κυρίαρχες μέθοδοι εκτέλεσης μιας επίθεσης άρνησης εξυπηρέτησης οι οποίοι είναι οι εξής [34] :

1. Η κατανάλωση όλων των διαθέσιμων υπολογιστικών πόρων του δικτύου, όπως είναι το εύρος ζώνης, ο διαθέσιμος χώρος στον δίσκο και οι χρόνοι του επεξεργαστή.
2. Η παρεμπόδιση της ομαλής διαμόρφωσης των πληροφοριών, όπως για παράδειγμα είναι οι πληροφορίες δρομολόγησης.
3. Η παρεμπόδιση της ορθής λειτουργίας των δομικών στοιχείων του δικτύου. Η ασυνήθιστα αργή λειτουργία του δικτύου, η μη διαθεσιμότητα συγκεκριμένων ιστοσελίδων ή η ανικανότητα εισόδου σε οποιαδήποτε ιστοσελίδα, καθώς και η δραματική αύξηση της ανεπιθύμητης αλληλογραφίας που αποστέλλεται, είναι κάποια από τα παραδείγματα που συναντώνται συχνά.

Οι επιθέσεις άρνησης εξυπηρέτησης είναι πλέον πολυάριθμες με πολλές από αυτές να έχουν μεγάλη πιθανότητα να αποβούν εξαιρετικά καταστροφικές με την ικανότητα τους να διακόπτουν τη λειτουργία μεταξύ των δικτύων. Ο βασικός στόχος του ατόμου που εξαπολύει μια τέτοια επίθεση είναι να αποκλείσει την είσοδο των εξουσιοδοτημένων χρηστών από διάφορες υπηρεσίες, ιστοσελίδες ή και ολόκληρο το δίκτυο. Για να γίνει αυτό εφικτό, ο επιτιθέμενος εντοπίζει και εκμεταλλεύεται σφάλματα και αδυναμίες στο λογισμικό των δρομολογητών και των άλλων συσκευών του δικτύου. Ακόμη μπορούν να χρησιμοποιήσουν υπέρ τους ευπάθειες στον τρόπο που το λειτουργικό σύστημα εφαρμόζει τα πρωτόκολλα ή που μπορεί να υπάρχουν στις εφαρμογές που «τρέχουν» στον υπολογιστή του θύματος. Όπως είναι ευδιάκριτο, οι επιθέσεις άρνησης εξυπηρέτησης δύναται να λάβουν χώρα σε διάφορα επίπεδα ενός υπολογιστικού συστήματος και με ποικίλους τρόπους και τεχνικές. Στην εικόνα που παρατίθεται φαίνεται η κατηγοριοποίησή τους ανάλογα με το επίπεδο δράσης τους και εν συνεχεία ακολουθεί μια σύντομη ανάλυσή τους. [35]



Εικόνα 9 Κατηγοριοποίηση επιθέσεων DoS

ΕΠΙΠΕΔΟ ΣΥΣΚΕΥΗΣ ΔΙΚΤΥΟΥ (NETWORK DEVICE LEVEL): Στην υποκατηγορία αυτή ανήκουν οι επιθέσεις που μπορούν να προκληθούν , όπως αναφέρθηκε στην προηγούμενη παράγραφο, αν ο θύτης εκμεταλλευτεί ελαττώματα και αδυναμίες του λογισμικού ή αν προσπαθήσει να εξαντλήσει τους πόρους των δικτυακών συσκευών. Οι επιθέσεις αυτές έχουν ως κύριο στόχο τους συσκευές όπως είναι οι δρομολογητές ,οι εξυπηρετητές, τα κινητά οι προσωπικοί υπολογιστές και τα τείχη προστασίας.

ΕΠΙΠΕΔΟ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ (OS LEVEL) : Εδώ, ο επιτιθέμενος στοχεύει σε αδυναμίες στον τρόπο που ένα λειτουργικό σύστημα υλοποιεί και διαχειρίζεται τα πρωτόκολλα που το απαρτίζουν. Χαρακτηριστικό παράδειγμα είναι η αδυναμία του να δεσμεύσει αρκετή μνήμη για τα υπερμεγέθη πακέτα ήχους που του αποστέλλονται και οδηγείται σε υπερχείλιση της προσωρινής μνήμης (πχ Ping of Death).

ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ (APPLICATION LEVEL) : Οι επιθέσεις στο επίπεδο εφαρμογής προσπαθούν να θέσουν ένα σύστημα ή μια μηχανή εκτός λειτουργίας. Αυτό μπορούν να το πετύχουν είτε εκμεταλλευόμενοι σφάλματα σε εφαρμογές που εκτελούνται στον υπολογιστή του θύματος, είτε προσπαθώντας να εξαντλήσουν τους πόρους του συστήματός του με εφαρμογές όπως για παράδειγμα με επαναλαμβανόμενες εκτελέσεις ρουτινών (πχ finger bomb).

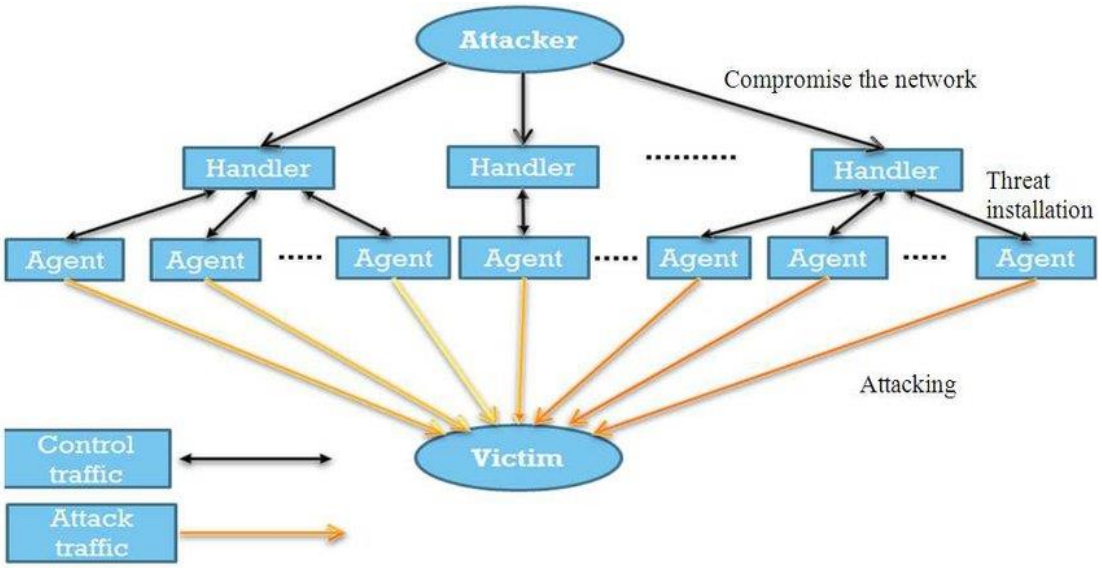
ΕΠΙΠΕΔΟ ΥΠΕΡΧΕΙΛΙΣΗΣ ΔΕΔΟΜΕΝΩΝ (DATA FLOOD): Στις επιθέσεις υπερχείλισης δεδομένων γίνεται εκμετάλλευση του διαθέσιμου εύρους ζώνης του δικτύου του θύματος κατά το μέγιστο δυνατό. Ο κακόβουλος χρήστης εκμεταλλεύεται το εύρος των συνδέσεων που μπορούν να πραγματοποιηθούν ταυτόχρονα στο δίκτυο στέλνοντας μεγάλο αριθμό άσκοπων συνδέσεων, προκαλώντας έτσι την επεξεργασία τεράστιου όγκου δεδομένων. Το δίκτυο υπερχειλίζει και στη συνέχεια τίθεται εκτός λειτουργίας (πχ DDoS).

ΕΠΙΠΕΔΟ ΛΕΙΤΟΥΡΓΙΑΣ ΠΡΩΤΟΚΟΛΛΩΝ (PROTOCOL BASED): Οι επιθέσεις στο επίπεδο λειτουργίας πρωτοκόλλων, εκμεταλλεύονται ελαττώματα που μπορεί να υπάρχουν στα πρωτόκολλα που χρησιμοποιούντα. Πολλοί κακόβουλοι χρήστες επωφελούνται από το γεγονός

ότι οι διευθύνσεις IP μπορούν να παραποιηθούν καθώς και από το γεγονός ότι ο DNS εξυπηρετητής δεν ελέγχει την ορθότητα των στοιχείων στη βάση δεδομένων του. Αυτό έχει ως αποτέλεσμα ο επιτιθέμενος να αποκτά τη δυνατότητα να τροποποιήσει την διεύθυνση μιας ιστοσελίδας ώστε να παραπέμπει σε κάποια άλλη.

- **DDOS ΕΠΙΘΕΣΕΙΣ**

Η βασική διαφορά με τις κλασσικές επιθέσεις άρνησης εξυπηρέτησης, είναι στην πηγή της επίθεσης. Οι DoS επιθέσεις αφορούν άμεσα τον επιτιθέμενο και το θύμα. Αντίθετα, οι κατανεμημένες επιθέσεις μπορεί να έχουν πολλαπλές πηγές (SANS 2005). Εδώ, ο θύτης επιστρατεύει έναν αριθμό μηχανών που ονομάζονται bots ή **zombies**. Ο ίδιος, επιλέγει ευάλωτα μηχανήματα ώστε να μπορέσει να τα παραβιάσει και να εγκαταστήσει σε αυτά κακόβουλο λογισμικό, με σκοπό να τα έχει κάτω από τον πλήρη έλεγχό του και την κατάλληλη στιγμή, με εντολή του, όλοι μαζί να ξεκινήσουν να επιτίθενται στον υπολογιστή-στόχο. Η διαδικασία εισαγωγής του κακόβουλου προγράμματος δεν γίνεται άμεσα αντιληπτή από τον χρήστη, ούτε σκοπεύει να προκαλέσει απαραίτητα κάποια ζημία στο σύστημά του. Στην ουσία ο επιτιθέμενος επιδιώκει να διατηρήσει το πρόγραμμα που εισήγαγε σε αδράνεια και να το προστατεύσει από τον εντοπισμό και την απενεργοποίησή του, ώστε ο μολυσμένος υπολογιστής να συμμετάσχει ενεργά και αποτελεσματικά την ώρα της επίθεσης, ενάντια στον πραγματικό στόχο. Πραγματοποιείται έτσι μια συντονισμένη επίθεση στο θύμα καθώς λαμβάνει τεράστιο όγκο δεδομένων από πολλές πηγές ταυτόχρονα, με αποτέλεσμα να μην μπορεί να διαχειριστεί την συμφόρηση και να καταρρεύσει. Μια επίθεση DDoS μπορεί να πραγματοποιηθεί κάνοντας χρήση πολλών επιπέδων επικοινωνίας. Στο μοντέλο δύο επιπέδων, για παράδειγμα, υπάρχει μια σειρά από bots ανάμεσα στο θύτη και το θύμα. Στο μοντέλο των τριών επιπέδων, ανάμεσα στον θύτη και το θύμα, παρεμβάλλονται οι χειριστές (**handlers**) οι οποίοι παραβιάζονται από τον επιτιθέμενο με ειδικό πρόγραμμα (malware, θα αναλυθεί σε επόμενο κεφάλαιο) ώστε να μπορούν με την σειρά τους να ελέγχουν το αμέσως επόμενο επίπεδο, εκείνο των πρακτόρων (**agents**) και να προσδιορίζουν ποιοι από τους πράκτορες είναι διαθέσιμοι για να συμμετέχουν στην επίθεση. Οι πράκτορες είναι υπολογιστές στους οποίους εκτελούνται ειδικά προγράμματα ώστε να λαμβάνουν πληροφορίες σχετικά με την ώρα της επίθεσης ή τυχόν αναβαθμίσεις που μπορεί να χρειάζεται ο εισαγόμενος κώδικας και είναι οι τελικοί κόμβοι και υπεύθυνοι για την μεγάλη ποσότητα δεδομένων που αποστέλλονται στο τελικό θύμα-στόχο. Κατά την διάρκεια της επίθεσης όλα τα μηχανήματα που συμμετέχουν, είναι και αυτά δευτερεύοντα θύματα της επίθεσης χωρίς να το αντιλαμβάνονται, αυτός είναι και ο βασικός λόγος που οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης είναι δύσκολο να ανιχνευτούν έγκαιρα, αλλά και να βρεθεί ο πραγματικός υπαίτιος. Η επικοινωνία επιτιθέμενου-handler και handler-agent, πραγματοποιείται μέσω των πρωτοκόλλων TCP, UDP και ICMP. Τέλος, ανάλογα με την παραμετροποίηση των ρυθμίσεων του δικτύου της επίθεσης, ένας handler μπορεί να επικοινωνεί με έναν ή περισσότερους agents. Στην παρακάτω εικόνα, φαίνεται η δομή μιας κατανεμημένης επίθεσης και η σχέση μεταξύ των κόμβων που την απαρτίζουν. [36]



Εικόνα 10 Δομή μιας επίθεσης DDoS

ΕΠΙΘΕΣΕΙΣ ΕΙΣΑΓΩΓΗΣ (FABRICATION ATTACKS)

Οι επιθέσεις εισαγωγής πραγματεύονται την δημιουργία παράτυπων πληροφοριών, διαδικασιών, επικοινωνιών ή δεδομένων μέσα σε ένα υπολογιστικό σύστημα, που σε προηγούμενη κατάστασή του, δεν υπήρχαν. Η παράνομη πρόσβαση σε ένα δίκτυο, η εισαγωγή ψευδών στοιχείων ή η πρόσθεση εγγραφών σε μια βάση δεδομένων είναι μερικά παραδείγματα τέτοιων επιθέσεων. Οι επιθέσεις εισαγωγής, κατά κύριο λόγο, προσβάλλουν την αρχή της ακεραιότητας. Υπάρχουν ωστόσο περιπτώσεις που φαίνεται να καταρρίπτουν και την αρχή της διαθεσιμότητας. Αν για παράδειγμα ο επιτιθέμενος δημιουργήσει επιπρόσθετες διαδικασίες ή ροές δεδομένων σε ένα δίκτυο, η κίνηση του θα αυξηθεί καταναλώνοντας όλο και περισσότερο τους διαθέσιμους πόρους του, έως ότου τους εξαντλήσει, κάνοντας αδύνατη την είσοδο των νόμιμων χρηστών στο σύστημα. [11]

- **ΠΛΑΣΤΟΠΡΟΣΩΠΙΑ (MASQUERADING/SPOOFING)**

MASQUERADING

Μια επίθεση αντιποίησης, λαμβάνει χώρα όταν ένας μη εξουσιοδοτημένος χρήστης στο δίκτυο, προσποιείται ότι είναι κάποιος άλλος. Η επίθεση αυτή, σκοπό έχει να επιτρέψει στον επιτιθέμενο την προσπέλαση υπηρεσιών στις οποίες έχουν πρόσβαση συγκεκριμένοι χρήστες στο δίκτυο ή με στόχο να αποκτήσει περισσότερα δικαιώματα μέσα στο δίκτυο από αυτά που του επιτρέπονται. Στις επιθέσεις πλαστοπροσωπίας συνήθως εμπεριέχονται και άλλες μορφές ενεργητικών επιθέσεων. [11]

SPOOFING

Οι μέθοδοι ηλεκτρονικών εξαπατήσεων μπορούν να πάρουν πολλές μορφές και διαστάσεις, αρκετές από τις οποίες περιλαμβάνουν την ψευδή αναπαράσταση της μεταδιδόμενης πληροφορίας. Πρόκειται για επιθέσεις που μπορούν να διαδραματιστούν σε διάφορα μέρη ενός υπολογιστικού συστήματος. [37]

1. IP SPOOFING
2. ARP SPOOFING
3. EMAIL SPOOFING
4. WEB SPOOFING
5. DNS SPOOFING

Παρακάτω θα δούμε πιο αναλυτικά τις μορφές spoofing που αναφέρθηκαν.

1. IP SPOOFING

Πρόκειται για την τεχνική χρήσης πλαστών διευθύνσεων IP έτσι ώστε ένας κόμβος να ξεγελαστεί και να αποδέχεται μη έγκυρα δεδομένα. Ο επιτιθέμενος προωθεί πακέτα δεδομένων σε έναν υπολογιστή-στόχο χρησιμοποιώντας ως διεύθυνση αποστολής, μια διεύθυνση που να υποδεικνύει μια αξιόπιστη πηγή. Έτσι, το θύμα εξαπατάται ,πείθεται για την εγκυρότητα του αποστολέα και αποδέχεται τα πακέτα ως έγκυρα.

2. ARP SPOOFING

Βασίζεται στη λειτουργία του πρωτοκόλλου ARP (Address Resolution Protocol) του οποίου η βασική λειτουργία είναι να αντιστοιχίζει IP διευθύνσεις με φυσικές MAC διευθύνσεις προκειμένου να διενεργηθεί μια επικοινωνία TCP σε ένα δίκτυο. Οι αντιστοιχήσεις αυτές καταγράφονται σε ζευγάρια στον πίνακα που έχει ο κάθε υπολογιστής στην μνήμη του (arp cache) και κάθε φορά που γίνεται μια καινούρια σύνδεση, τα στοιχεία του ανανεώνονται. Κατά την εδραίωση μιας φυσιολογικής σύνδεσης μεταξύ δύο κόμβων έστω Α και Β, ο Α στέλνει request με την IP του και την IP του Β με τον οποίο θέλει να επικοινωνήσει. Ο Β τότε, απαντάει με reply το οποίο περιέχει την IP και την MAC διεύθυνσή του. Τέλος , ο Α διαβάζει το reply και ανανεώνει τον πίνακά του προσθέτοντας και το καινούριο ζευγάρι. Ωστόσο, στο ARP δεν υπάρχουν μηχανισμοί αυθεντικοποίησης για τα αιτήματα (**requests**) και τις απαντήσεις (**replies**) που αποστέλλονται μεταξύ των κόμβων. Αυτό σημαίνει ότι ένας κακόβουλος χρήστης μπορεί να στείλει πλαστά απαντητικά πακέτα χρησιμοποιώντας την IP του κόμβου-στόχου και την δική του MAC διεύθυνση, χωρίς να γίνει αντιληπτός.

3. EMAIL SPOOFING

Ένα μήνυμα ηλεκτρονικής αλληλογραφίας αποτελείται από τρία μέρη :

1. Το τμήμα εσωτερικών διεργασιών μέσα από το οποίο δρομολογείται το μήνυμα.
2. Το κύριο σώμα στο οποίο βρίσκεται το περιεχόμενο του μηνύματος.

3. Την επικεφαλίδα (Header) στην οποία περιέχονται όλες οι πληροφορίες για το μήνυμα (προέλευση, προορισμό, θέμα, ημερομηνία κτλ).

Κατά την τεχνική αυτή, αποστέλλονται στο θύμα μηνύματα τα οποία φαινομενικά προέρχονται από έγκυρο χρήστη, ενώ στην ουσία προέρχονται από τον επιτιθέμενο. Ο τελευταίος, με κατάλληλες τροποποιήσεις στην επικεφαλίδα του μηνύματος καταφέρνει να κρύψει την ταυτότητά του και να εξαπατήσει τον εκάστοτε στόχο, με σκοπό είτε να προσβάλλει το σύστημά του επιμολύνοντας το με κακόβουλο λογισμικό, είτε για να εκμαιεύσει προσωπικές πληροφορίες και δεδομένα, ή πολλές φορές απλώς για να προκαλέσουν πρόβλημα. Πρόκειται ωστόσο για μια από τις ευκολότερες πρακτικά επιθέσεις που όμως παρά την απλότητά της, μπορεί να επιφέρει καταστροφικές συνέπειες. Αυτό οφείλεται κυρίως στο γεγονός ότι τα πρωτόκολλα που χρησιμοποιούνται δεν περιλαμβάνουν κανένα μηχανισμό αυθεντικοποίησης με αποτέλεσμα οποιοσδήποτε να μπορεί να παρέμβει στα στο μήνυμα και να αλλάξει τα στοιχεία της επικεφαλίδας του, προς όφελός του.

4. WEB SPOOFING

Πρόκειται για ακόμη μια κατηγορία επιθέσεων κατά την οποία ο χρήστης λαμβάνει λανθασμένες πληροφορίες. Το WEB spoofing είναι ένα είδος επίθεσης που επιτρέπει στον θύτη να παρακολουθεί παθητικά τους ιστότοπους που επισκέπτεται ένας χρήστης στο διαδίκτυο, καθώς και το περιεχόμενο αυτών. Επίσης έχει την δυνατότητα να καταγράφει τα δεδομένα που εισάγει ο χρήστης σε πλατφόρμες, να τα τροποποιεί καθώς και να δημιουργεί ακριβή αντίγραφα σελίδων τα οποία και ελέγχει με τέτοιο τρόπο ώστε όλη η δικτυακή κίνηση ανάμεσα στον χρήστη και το διαδίκτυο, να περνάει από τον ίδιο.

5. DNS SPOOFING

Μια επίθεση στην υπηρεσία ονοματοδοσίας (DNS), μπορεί να οριστεί και ως η επιτυχημένη εισαγωγή ψευδών πληροφοριών επίλυσης ονομάτων απ έναν μη εξουσιοδοτημένο χρήστη. Με την εισαγωγή νέων αλλά και την τροποποίηση των ήδη καταχωρημένων πληροφοριών, ο επιτιθέμενος αποκτά τη δυνατότητα να ανακατευθύνει μτον χρήστη από έναν έγκυρο ιστότοπο, σε έναν της επιλογής του.

- **ΕΝΔΙΑΜΕΣΗ ΟΝΤΟΤΗΤΑ (Man-in-the-Middle)**

Πρόκειται για μια από τις πιο διαδεδομένες επιθέσεις στην ασφάλεια των δικτύων και των υπολογιστικών συστημάτων με αδυναμίες στα πρωτόκολλα αυθεντικοποίησης. Στην προκειμένη περίπτωση, ο θύτης παρεμβάλλεται στην επικοινωνία μεταξύ δυο έμπιστων οντοτήτων και τους πείθει ότι η σύνδεσή τους είναι ασφαλής. Με τον τρόπο αυτό, όλα τα μηνύματα των συμμετεχόντων περνάνε από τον έλεγχο του κακόβουλου χρήστη ο οποίος έχει την δυνατότητα να τα διαγράψει, να δημιουργήσει νέα, ή να τροποποιήσει αυτά που ήδη υπάρχουν και έπειτα αν θέλει να τα επαναπροωθήσει, χωρίς οι χρήστες να αντιληφθούν ότι παρακολουθούνται. Οι επιθέσεις στις οποίες γίνεται μεμονωμένη καταγραφή των μηνυμάτων και έπειτα η αποστολή τους χωρίς να αλλάξει κάτι στην δομή τους, ονομάζονται ***επιθέσεις επανάληψης (replay attacks)***. [38]

- **ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ (SOCIAL ENGINEERING)**

Ως κοινωνική μηχανική ορίζεται η τεχνική της ψυχολογικής χειραγώγησης του ατόμου με σκοπό να δράσει με συγκεκριμένους τρόπους ή να φανερώσει εμπιστευτικές πληροφορίες που θα βοηθήσουν έναν κακόβουλο χρήστη να διαπράξει απάτη ή να παραβιάσει ένα σύστημα. Οι επιθέσεις αυτής της κατηγορίας δεν προϋποθέτουν ιδιαίτερες γνώσεις για να διεξαχθούν επιτυχώς καθώς το επίκεντρο δεν είναι τα μέσα που θα χρησιμοποιηθούν αλλά η ίδια η ψυχολογία του θύματος. Ιδιαίτερη εφαρμογή έχουν στα μέσα κοινωνικής δικτύωσης εκμεταλλευόμενοι την άγνοια του απλού χρήστη. Ιδιαίτερο παράδειγμα αποτελεί το Phishing. [39]

- **ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΩΝ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ**

Η εισαγωγή κωδικών έχει γίνει ο πλέον συνηθέστερος τρόπος αυθεντικοποίησης των χρηστών στα σύγχρονα υπολογιστικά συστήματα. Η λάθος επιλογή τους μπορεί να τους καταστήσει ευάλωτους σε τέτοιες μορφές επιθέσεων. Σε αυτή την κατηγορία επιθέσεων, το επίκεντρο είναι η υποκλοπή των κωδικών πρόσβασης των χρηστών, με τέτοιο τρόπο ώστε ο θύτης να εξασφαλίσει την είσοδό του σε ένα σύστημα ως εξουσιοδοτημένος χρήστης. [40]

ΕΠΙΘΕΣΕΙΣ ΩΜΗΣ ΒΙΑΣ (BRUTE FORCE ATTACK)

Οι επιθέσεις ωμής βίας χρησιμοποιούνται ως μέθοδοι υποκλοπής κωδικών πρόσβασης. Κατά τη μέθοδο αυτή, δοκιμάζονται όλοι οι πιθανοί συνδυασμοί ανάλογα με το πλήθος των χαρακτήρων του κωδικού, έως ότου να βρεθεί ο σωστός. Αυτό σημαίνει πως αν για παράδειγμα ένας κωδικός αποτελείται από 8 χαρακτήρες, με βάση το αγγλικό αλφάβητο που αποτελείται από 26, θα είχαμε 26^8 = 208.827.064.576 συνδυασμούς! Είναι φανερό πως υπάρχει μεγάλη κατανάλωση χρόνου μέχρι να έρθει σε πέρας. Όσο μεγαλύτερος είναι ο συνδυασμός χαρακτήρων αναλογικά πολύπλοκη είναι και η διαδικασία εύρεσής του. [40]

ΕΠΙΘΕΣΕΙΣ ΛΕΞΙΚΟΥ (DICTIONARY ATTACK)

Στην επίθεση αυτή, ο θύτης έχει στην διάθεσή του (μέσω κατάλληλου προγράμματος) ένα λεξικό. Το λεξικό αυτό περιέχει ένα σύνολο λέξεων οι οποίες εισάγονται διαδοχικά από τον κακόβουλο χρήστη στο πεδίο συμπλήρωσης του κωδικού πρόσβασης, μέχρι να βρεθεί η κατάλληλη, που θα του επιτρέψει την πρόσβαση. [40]

ΚΑΤΑΣΚΟΠΕΙΑ (*SHOULDER SURFING*)

Είναι η επίθεση που προκύπτει από την αφέλεια του χρήστη να αποκρύπτει κατάλληλα τους κωδικούς πρόσβασής του, ή να τους αφήνει σε εμφανές μέρος. Έτσι, κάποιος που θα παρατηρήσει τις κινήσεις του θα μπορεί εύκολα να τους διακρίνει. [40]

ΕΠΙΘΕΣΕΙΣ ΑΛΛΟΙΩΣΗΣ (MODIFICATION ATTACKS)

Οι επιθέσεις αλλοίωσης είναι επιθέσεις ενάντια στην αρχή της Ακεραιότητας. Πρόκειται για την αθέμιτη εισαγωγή διαγραφή ή τροποποίηση των πληροφοριών που υπάρχουν σε ένα

υπολογιστικό σύστημα. Ο επιτιθέμενος είναι δυνατό να προσθέσει δεδομένα που προηγουμένως δεν υπήρχαν , να μεταβάλλει το περιεχόμενο των μεταδιδόμενων μηνυμάτων ή ακόμη και να αλλάξει ρυθμίσεις στα εκτελούμενα προγράμματα. Τα προαναφερθέντα, μπορούν να επιτευχθούν με ποικίλους τρόπους, μερικοί από τους οποίους παρατίθενται στη συνέχεια. [11]

- **ΜΟΛΥΝΣΗ ΑΠΟ ΙΟΥΣ**

Ο ιός είναι ένα κακόβουλο λογισμικό το οποίο επί της ουσίας είναι ένα κομμάτι κώδικα που προσκολλάται σε άλλα προγράμματα ή αρχεία τα οποία ονομάζονται **ξενιστές,** δημιουργώντας αντίγραφα του εαυτού του**.** Οι ξενιστές με τη σειρά τους μολύνουν και άλλους υπολογιστές διαμοιράζοντας αντίγραφα του ιού μόλις βρίσκουν μη μολυσμένο τμήμα λογισμικού. Όταν ένας ξενιστής εκτελείται, ταυτόχρονα, εκτελείται και ο ιός χωρίς όμως αυτό να γίνεται άμεσα αντιληπτό από τον χρήστη. Κατά την εκτέλεσή του, ο ιός μπορεί να διαγράψει αρχεία και προγράμματα. Κατά τη διάρκεια της ζωής του ένας ιός ακολουθεί τις εξής φάσεις οι οποίες μπορεί να διαφέρουν από έναν υπολογιστή ή ένα λειτουργικό σύστημα σε ένα άλλο. [41]

ΛΑΝΘΑΝΟΥΣΑ ΦΑΣΗ Ή ΦΑΣΗ ΥΠΝΟΥ (DORMANT PHASE)

Σε αυτή τη φάση ο ιός είναι ανενεργός. Παραμένει σε αυτή την κατάσταση έως ότου να υπάρξει κάποιο συμβάν που να τον θέσει σε λειτουργία όπως για παράδειγμα κάποιο άλλο πρόγραμμα ή ημερομηνία εκκίνησης. Δεν περνάνε όλοι οι ιοί υποχρεωτικά από αυτή τη φάση.

ΦΑΣΗ ΔΙΑΔΟΣΗΣ (PROPAGATION PHASE)

Σε αυτό το στάδιο ο ιός δημιουργεί αντίγραφα του εαυτού του και τα τοποθετεί σε άλλα προγράμματα, αρχεία, ή σε περιοχές συστήματος του δίσκου. Κάθε μολυσμένο πρόγραμμα αποκτά τώρα ένα αντίγραφο του ιού το οποίο και εισάγει σε άλλα προγράμματα σε επόμενη φάση διάδοσης.

ΦΑΣΗ ΠΥΡΟΔΟΤΗΣΗΣ (TRIGGERING PHASE)

Εδώ, ο ιός ενεργοποιείται και είναι έτοιμος να εκτελέσει τις ενέργειες για τις οποίες προορίζεται. Όπως και στη λανθάνουσα φάση, έτσι και εδώ, η ενεργοποίηση προκαλείται από κάποιο άλλο συμβάν.

ΦΑΣΗ ΕΚΤΕΛΕΣΗΣ (EXECUTION PHASE)

Ο ιός τίθεται σε λειτουργία και αρχίζει να εκτελείται. Κάποιοι ιοί επιτελούν αβλαβείς λειτουργίες όπως είναι η απενεργοποίηση ενός υπολογιστή ή η εμφάνιση ενός μηνύματος στην οθόνη ενώ άλλοι έχουν την δυνατότητα να καταστρέφουν προγράμματα και να διαγράφουν αρχεία. Τα αποτελέσματα μπορεί να διαφέρουν ανάλογα με τους σκοπούς του κακόβουλου χρήστη.

- **ΣΚΟΥΛΗΚΙΑ (WORMS)**

Τα σκουλήκια είναι τμήματα κακόβουλου λογισμικού τα οποία λειτουργούν ανεξαρτήτως άλλων προγραμμάτων. Δημιουργούν και αυτά πιστά αντίγραφα του εαυτού τους τα οποία και

αποστέλλουν στους υπολογιστές εντός ενός δικτύου επιμολύνοντάς τους. Τα σκουλήκια εντοπίζουν και εκμεταλλεύονται αδυναμίες συστημάτων και υπολογιστών ώστε να τους μολύνουν με τα αντίγραφά τους. Έχουν πολλά κοινά με τους ιούς όπως το γεγονός ότι και οι δύο είναι επικίνδυνες και δύσκολα αντιμετωπίσιμες κατηγορίες κακόβουλου λογισμικού. Ωστόσο η βασική τους διαφορά έγκειται στο γεγονός ότι τα σκουλήκια αντιγράφονται και μεταδίδονται αυτόνομα χωρίς κάποια ανθρώπινη παρέμβαση. [42]

- **ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ (TROJAN HORSES)**

Είναι και αυτά προγράμματα τα οποία φαινομενικά έχουν καλοήθη σκοπό αλλά στην πραγματικότητα επιτελούν επιβλαβείς λειτουργίες. Μπορούν να τοποθετηθούν κρυφά σε συστήματα από επιτήδειους και να αντιγράψουν παράνομα πληροφορίες χρηστών, να διαγράψουν αρχεία ή ακόμη και να αλλάξουν τα δικαιώματα των χρηστών. Οι Δούρειοι Ίπποι συχνά «καμουφλάρονται» ανάμεσα σε άλλα, νόμιμα προγράμματα με αποτέλεσμα ο χρήστης να συνεχίζει τις ενέργειές του χωρίς να αντιλαμβάνεται την παρουσία του κακόβουλου λογισμικού στο σύστημά του. [42]

- **RANSOMWARE**

Πρόκειται επίσης για κακόβουλο λογισμικό που ως στόχο έχει να περιορίσει την πρόσβαση του νόμιμου χρήστη στο ίδιο του το σύστημα. Την στιγμή που ένας υπολογιστής μολυνθεί, τα δεδομένα που περιέχει, κρυπτογραφούνται ενώ το κλειδί για την αποκρυπτογράφησή τους, βρίσκεται στην κατοχή του κακόβουλου χρήστη. Το θύμα ενημερώνεται συνήθως για την επίθεση με σχετικό μήνυμα στην οθόνη του, κατόπιν του ζητείται χρηματική αμοιβή προκειμένου να του επιστραφούν πίσω τα δεδομένα. Όταν ένα ransomware εγκατασταθεί σε έναν υπολογιστή, τυπικά στοχεύει ευαίσθητα δεδομένα και αρχεία μεγάλης αξίας για το θύμα όπως βάσεις δεδομένων, φωτογραφίες, οικονομικές πληροφορίες και άλλα. [42]

ΑΝΑΤΟΜΙΑ ΜΙΑΣ ΕΠΙΘΕΣΗΣ

Είδαμε έως τώρα το πλήθος των διαφορετικών κυβερνοεπιθέσεων που είναι δυνατό να τελεστούν στα πλαίσια του κυβερνοχώρου καθώς και την επικινδυνότητα κάθε κατηγορίας ξεχωριστά. Κάθε μέρα κάνουν την εμφάνισή τους νέες μέθοδοι και τεχνικές επιθέσεων ανάλογα με τους απώτερους σκοπούς του κακόβουλου χρήστη. Σε αυτό το μέρος του κεφαλαίου θα αναλυθεί η ανατομία των κυβερνοεπιθέσεων καθώς και τα βήματα που ακολουθεί ο θύτης στην προσπάθειά του να αποκτήσει πρόσβαση σε ένα υπολογιστικό σύστημα. Η παρούσα ανάλυση θα ωφελήσει τον μέσο χρήστη ώστε να κατανοήσει καλύτερα το πως διενεργείται μια κυβερνοεπίθεση και κατ'επέκταση να είναι σε θέση να προστατεύσει το υπολογιστικό του σύστημα με επαρκείς αμυντικούς μηχανισμούς, αποφεύγοντας έγκαιρα μελλοντικές επιθέσεις. Σε ευρύτερα πλαίσια, τα βήματα που εκτελούνται κατά τη διάρκεια μιας επίθεσης είναι η έρευνα, η εκμετάλλευση, η παραβίαση και η επίδραση. [43] Πιο συγκεκριμένα:

ΕΡΕΥΝΑ (SURVEY): Κατά τη διαδικασία της έρευνας, ο επιτιθέμενος αναζητάει τον πιθανό στόχο. Εφόσον τον εντοπίσει, εκτελεί ενέργειες ώστε να συλλέξει και να αναλύσει όλες τις πληροφορίες που αφορούν το θύμα με σκοπό να διακρίνει κάποια ευπάθεια προς εκμετάλλευση. Με τη χρήση εργαλείων σάρωσης δικτύου και άλλων τεχνικών, συλλέγει

πληροφορίες σχετικές με το δίκτυο του στόχου, το σύστημα ασφαλείας του ή ακόμη και τον ίδιο.

ΠΑΡΑΔΟΣΗ (DELIVERY): Στο σημείο αυτό και εφόσον ο επιτιθέμενος έχει εντοπίσει κάποια τρωτότητα στο σύστημα του θύματος, επιλέγει τον τρόπο με τον οποίο θα διενεργήσει προσπάθειες για την εκμετάλλευσή της. Για να το καταφέρει αυτό, συνήθως αποστέλλει στον στόχο κάποιο κακόβουλο πρόγραμμα το οποίο θα μολύνει τον υπολογιστή του στόχου μόλις το παραλάβει.

ΠΑΡΑΒΙΑΣΗ (BREACH): Το μέγεθος της ζημιάς, ως αποτέλεσμα του προηγούμενου βήματος, εξαρτάται από την φύση της ευπάθειας και τον τρόπο που ο θύτης επέλεξε να την προσποριστεί. Σε αυτό το σημείο ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση στο σύστημα με τρόπο τέτοιο που θα του εξασφαλίσει τα περισσότερα δικαιώματα ώστε να επιτύχει τον αρχικό του στόχο.

ΕΠΙΔΡΑΣΗ (AFFECT): Το στάδιο αυτό περιλαμβάνει την εφαρμογή ενεργειών μέσω των οποίων ο επιτιθέμενος εισβάλλει σε ένα σύστημα. Οι ενέργειες που ακολουθεί μετά την είσοδό του, μπορεί να ποικίλλουν ανάλογα με τα κίνητρα που έχει. Ο ίδιος, μπορεί να θέλει να εξερευνήσει το σύστημα του θύματος, να τροποποιήσει ρυθμίσεις που μπορεί να επηρεάσουν την λειτουργία του, να αποκτήσει πρόσβαση σε διαδικτυακούς λογαριασμούς του ή ακόμη και να επεκτείνει τον έλεγχό του και σε άλλα συστήματα πέρα από αυτό.

Μόλις ο θύτης αποκτήσει το επιθυμητό επίπεδο πρόσβασης στο υπολογιστικό σύστημα και επιτύχει τον στόχο του, διαγράφει τα ίχνη που πιθανόν να άφησε με την εισβολή του ώστε να μην γίνει αντιληπτός. Πριν ολοκληρωθεί η επίθεση ο θύτης είναι δυνατό να τοποθετήσει στο σύστημα του στόχου κάποιο πρόσθετο πρόγραμμα ή κακόβουλο λογισμικό που σε επόμενη επίθεση, θα διευκολύνουν την είσοδό του στο ίδιο σύστημα.

ΑΛΥΣΙΔΑ ΘΑΝΑΤΟΥ (CYBER KILL CHAIN)

Για να υπάρχει η δυνατότητα απόκρισης και ανάλυσης των περιστατικών που λαμβάνουν χώρα στον κυβερνοχώρο, δημιουργήθηκε το μοντέλο της αλυσίδας θανάτου (Cyber Kill Chain, CKC). Το μοντέλο αυτό, αναπτύχθηκε από τους ερευνητές της εταιρίας Lockheed Martin, αρχικά με σκοπό την κατανόηση της στρατηγικής των φυσικών επιθέσεων και έχει βρει εφαρμογή στον σχεδιασμό της άμυνας έναντι τρομοκρατικών επιθέσεων, καθώς υπογραμμίζει τις αρχές που θα βοηθήσουν τον αμυνόμενο να σχεδιάσει την καλύτερη πρακτική προστασίας του. Η αλυσίδα θανάτου είναι ουσιαστικά η προσομοίωση και η ανάλυση των βημάτων που ακολουθώνται από έναν κακόβουλο χρήστη ώστε να φέρει σε πέρας μια αξιόποινη πράξη σε ένα υπολογιστικό σύστημα και αποτελείται από επτά στάδια-φάσεις. Ακολουθεί η αναφορά τους και μια σύντομη ανάλυση για κάθε ένα από αυτά. [44]

1. Αναγνώριση-RECONNAISSANCE

Είναι το πρώτο στάδιο κατά το οποίο ο επιτιθέμενος εντοπίζει και επιλέγει το ενδεχόμενο θύμα. Στη συνέχεια, μαζεύει όσες περισσότερες πληροφορίες μπορεί ώστε να δημιουργήσει ένα προφίλ για τον στόχο και με βάση αυτό να αποφασίσει ποιά μέσα θα χρησιμοποιήσει για την επίθεσή του. Η συλλογή των πληροφοριών γίνεται με διάφορους τρόπους μεταξύ των

οποίων είναι η ηλεκτρονική αλληλογραφία του θύματος, οι ιστόχωροι που επισκέπτεται, τα μέσα κοινωνικής δικτύωσης και επιτυγχάνεται με τη χρήση εργαλείων ανίχνευσης δικτύου. Η αναγνώριση μπορεί να είναι δύο ειδών, ενεργητική ή παθητική. Στην περίπτωση της ενεργητικής αναγνώρισης, απαιτείται εκτενέστερη έρευνα των πληροφοριών που θα εκμαιευτούν ώστε να χτιστεί ένα προφίλ για τον στόχο, όσο γίνεται πιο αντιπροσωπευτικό. Η μέθοδος αυτή, είναι ριψοκίνδυνη καθώς υπάρχει μεγαλύτερη πιθανότητα να γίνει αντιληπτός από τον στόχο. Στην παθητική αναγνώριση, από την άλλη, ο θύτης απλώς συλλέγει όσες πληροφορίες μπορεί διατηρώντας την μυστικότητά του.

2. Επιλογή του όπλου - WEAPONIZATION

Είναι το στάδιο στο οποίο ο επιτιθέμενος πραγματεύεται τον σχεδιασμό της παράνομης διείσδυσής του σε ένα σύστημα κάνοντας χρήση των πληροφοριών που συλλέχθηκαν κατά το προηγούμενο στάδιο. Επί της ουσίας δημιουργεί ένα φορτίο προς παράδοση στο θύμα το οποίο αποτελείται από ένα πρόγραμμα εκμετάλλευσης ευπαθειών (exploit) σε συνδυασμό με έναν Δούρειο Ίππο απομακρυσμένης διαχείρισης (Remote Access Trojan, RAT).

3. Παράδοση-DELIVERY

Σε αυτό το βήμα αποστέλλεται στον στόχο το πρόγραμμα που δημιουργήθηκε στο προηγούμενο στάδιο και είναι υψίστης σημασίας αφού από αυτό καθορίζεται η επιτυχία της επίθεσης. Είναι εξίσου υψίστης επικινδυνότητας, καθώς σε κάθε ενέργεια του θύτη υπάρχει πάντα η πιθανότητα να γίνει αντιληπτός. Υπάρχουν διάφορες μέθοδοι που μπορούν να χρησιμοποιηθούν για την παράδοση του κακόβουλου φορτίου στον στόχο. Η αποστολή συνδέσμων που απαιτούν από τον χρήστη λήψη εκτελέσιμων αρχείων και τα μολυσμένα αρχεία σε αφαιρούμενα μέσα αποθήκευσης (Injected USB Flash), είναι μερικά από τα παραδείγματα.

4. Εκμετάλλευση-EXLOITATION

Έπειτα από την επιτυχή παράδοση του κακόβουλου λογισμικού στον στόχο και εφόσον υπάρξει η επιθυμητή αλληλεπίδραση από πλευράς του. Ο θύτης αξιοποιεί διάφορες τεχνικές ώστε να γίνει η εκκίνηση του προγράμματος εκμετάλλευσης ευπαθειών που θα πυροδοτήσει τη λειτουργία του κακόβουλου κώδικα. Για να γίνει αυτό θα πρέπει να πληρούνται ορισμένες προϋποθέσεις.

Το θύμα θα πρέπει να χρησιμοποιεί ένα λειτουργικό σύστημα που να είναι συμβατό με το πρόγραμμα που θα χρησιμοποιηθεί για την επίθεση. Επίσης θα πρέπει να μην έχει πραγματοποιήσει αναβαθμίσεις ή ενημερώσεις ώστε να διατηρηθεί η συμβατικότητά του. Τέλος, το πρόγραμμα του επιτιθέμενου δεν πρέπει να γίνει αντιληπτό από αντιικά λογισμικά ή άλλους μηχανισμούς ασφαλείας.

5. Εγκατάσταση-INSTALLATION

Στο σημείο αυτό γίνεται η εγκατάσταση του κακόβουλου λογισμικού στον υπολογιστή του θύματος. Η εγκατάσταση επιτυγχάνεται είτε με κάποια ενέργεια του θύτη είτε γίνεται αυτόματα. Σε οποιαδήποτε από τις δύο περιπτώσεις, ο θύτης δημιουργεί ένα σημείο πρόσβασης που του επιτρέπει την παρουσία στο περιβάλλον του θύματος. Πρόκειται για ένα καίριο κομμάτι της αλυσίδας καθώς αν υπάρξει κάποια επιπλοκή ο κώδικας που

εγκαταστάθηκε δεν θα εκτελεστεί και η επίθεση θα σταματήσει. Τα σύγχρονα προγράμματα κακόβουλου λογισμικού χρησιμοποιούν **droppers** και **downloaders**.

Πιο συγκεκριμένα, droppers είναι προγράμματα που εγκαθίστανται και τρέχουν στον υπολογιστή του στόχου. Πριν την εκτέλεσή τους όμως, απενεργοποιούν τους μηχανισμούς ασφαλείας του συστήματος και κρύβουν την εγκατάσταση του κακόβουλου λογισμικού. Από την άλλη, downloaders είναι προγράμματα που επιτελούν τις ίδιες ακριβώς λειτουργίες με τους droppers, με τη διαφορά ότι δεν περιέχουν τον κακόβουλο κώδικα, αλλά συνδέονται σε απομακρυσμένο αποθετήριο αρχείων για να κάνουν τη λήψη του.

6. Εκτέλεση εντολών και ελέγχου-COMMAND AND CONTROL

   Μέσω του κακόβουλου λογισμικού που εγκαθίσταται στο προηγούμενο βήμα, ο θύτης δημιουργεί ένα κανάλι στο σύστημα του στόχου. ώστε να μπορεί απομακρυσμένα να υποβάλλει με εντολές τις ενέργειες που επιθυμεί να συμβούν, ποιές πληροφορίες επιθυμεί να αποσπαστούν και να έχει τον πλήρη έλεγχό του συστήματος. Το σύστημα του στόχου μπορεί να έχει κεντρικοποιημένη αρχιτεκτονική ή αποκεντρωμένη αρχιτεκτονική.

   Στην περίπτωση της κεντρικοποιημένης αρχιτεκτονικής, δηλαδή του κλασσικού μοντέλου πελάτη-εξυπηρετητή (client-server), ο κεντρικός server χρησιμοποιείται για να στέλνει εντολές και να ελέγχει τους μολυσμένους υπολογιστές. Ο αριθμός των μολυσμένων μηχανημάτων, εξαρτάται από τη διαθεσιμότητα του συστήματος του στόχου, σε πόρους υλικού και λογισμικού. Σε αυτή την αρχιτεκτονική αν υπάρξει κάποια αποτυχία στον server, σταματάει η λειτουργία ολόκληρου του δικτύου.

   Από την άλλη, στη αποκεντρωμένη αρχιτεκτονική ή αλλιώς Peer to Peer, οι μολυσμένοι υπολογιστές χρησιμοποιούνται ως κόμβοι που κάθε ένας από αυτούς είναι υπεύθυνος μόνο για ένα υποσύνολο μολυσμένων μηχανημάτων και όχι για όλα. Ο κάθε κόμβος με τη σειρά του ελέγχει ένα άλλο υποσύνολο.

7. Επίτευξη του αρχικού στόχου-ACTION ON OBJECTIVE

   Σε αυτό το στάδιο και μόνον εφόσον έχουν προηγηθεί τα προηγούμενα έξι βήματα, ο θύτης αποκτά τη δυνατότητα να εκτελέσει τις ενέργειες που θα φέρουν εις πέρας τον αρχικό του στόχο. Στις περισσότερες των περιπτώσεων οι στόχοι των επιτιθέμενων αφορούν την εξόρυξη δεδομένων. Σε αυτό μεταξύ άλλων περιλαμβάνεται η συλλογή, η κρυπτογράφηση, και η απόσπαση πληροφοριών αλλά και γενικότερα επιθέσεις που καταπατούν τις βασικές αρχές της κυβερνοασφάλειας (ακεραιότητα, διαθεσιμότητα, εμπιστευτικότητα). Εναλλακτικά μπορεί να αποτελέσει ένα πρώτο βήμα για παραβίαση περαιτέρω συστημάτων.

<u>ΚΕΦΑΛΑΙΟ 3</u> ΕΡΓΑΛΕΙΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΑΣΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

Σύμφωνα με τον William Stallings, «*Στο πλαίσιο της ασφάλειας δικτύων, ο έλεγχος πρόσβασης έχει να κάνει με τον έλεγχο και περιορισμό της πρόσβασης σε δικτυακούς κόμβους και εφαρμογές, μέσω τηλεπικοινωνιακών ζεύξεων. Για την επίτευξη αυτού, για κάθε οντότητα που αποπειράται να αποκτήσει πρόσβαση πρέπει πρώτα να προσδιορίζεται ή να αυθεντικοποιείται, έτσι ώστε να της αποδοθούν τα σωστά δικαιώματα πρόσβασης*.» [8]

Με βάση το παραπάνω μπορούμε να πούμε πως σημαντική απαίτηση όλων των σύγχρονων υπολογιστικών συστημάτων πλέον, είναι η εφαρμογή μηχανισμών ασφαλείας που θα προστατεύουν τις πληροφορίες των χρηστών από τα είδη των επιθέσεων που αναλύσαμε έως τώρα. Σκοπός αυτής της απαίτησης είναι το κάθε σύστημα να μπορεί να περιορίζει την είσοδο και τις ενέργειες που μπορούν να εκτελεστούν μέσα σε αυτό, όπως για παράδειγμα το ποιά αρχεία μπορεί να διαβάσει ο κάθε χρήστης, τα κριτήρια με τα οποία αυτά θα διαμοιράζονται και ποιά προγράμματα έχει δυνατότητα ο καθένας να εκτελέσει.

Οι μηχανισμοί ασφαλείας είναι ένα σύνολο ενεργειών που απαρτίζονται από τρεις βασικές έννοιες, την αυθεντικοποίηση, τον έλεγχο εισόδου και τον εσωτερικό έλεγχο του δικτύου και εφαρμόζονται στα σύγχρονα υπολογιστικά συστήματα ώστε να είναι σε θέση να λειτουργούν με σεβασμό έναντι των βασικών αρχών της κυβερνοασφάλειας και να προστατεύουν τους πόρους τους. Παρακάτω, παρουσιάζονται επιγραμματικά οι αναφερθείσες έννοιες, ενώ στη συνέχεια του κεφαλαίου θα γίνει εκτενέστερη ανάλυσή τους, με σκοπό ο αναγνώστης να έχει μια ολοκληρωμένη εικόνα των βημάτων που πρέπει να ακολουθηθούν, ώστε να μπορεί να προστατεύσει επαρκώς το σύστημά του, να αντιλαμβάνεται και να αντιμετωπίζει έγκαιρα επερχόμενες απειλές.

ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ (AUTHENTICATION) : Σε ευρύτερα πλαίσια, είναι το σύνολο των ενεργειών που ακολουθώνται για να επιβεβαιωθεί η ταυτότητα ενός χρήστη μέσα σε ένα δίκτυο που τον χαρακτηρίζει ως μια εξουσιοδοτημένη οντότητα. Υπάρχουν διάφορες μέθοδοι αυθεντικοποίησης όπως θα δούμε και παρακάτω, η πιο συνήθης, είναι η χρήση κωδικού πρόσβασης. Η διαδικασία της αυθεντικοποίησης μπορεί να λάβει χώρα μεταξύ δύο υπολογιστών ή δύο διεργασιών και πραγματοποιείται και αμφίδρομα. [45]

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ (ACCESS CONTROL) : Οι διαδικασίες ελέγχου πρόσβασης πραγματοποιούνται με την προϋπόθεση ότι ένας χρήστης έχει ταυτοποιηθεί και λαμβάνουν χώρα μετά την αυθεντικοποίηση. Ο έλεγχος πρόσβασης προσδιορίζει ποιές θα είναι οι ενέργειες που θα επιτρέπονται σε κάθε οντότητα βάσει δικαιωμάτων. [45]

ΕΛΕΓΧΟΣ ΡΟΗΣ (AUDIT) : Στον έλεγχο ροής συλλέγονται πληροφορίες όσον αφορά τις ενέργειες που εκτελούνται σε ένα υπολογιστικό σύστημα. Οι πληροφορίες αυτές αναλύονται με σκοπό να εντοπιστούν πιθανά προβλήματα ή εισβολές στο σύστημα και να διαγνωστούν τα αίτιά τους. Ο έλεγχος ροής μπορεί να συμβεί σε πραγματικό χρόνο (κατά την διάρκεια την σύνδεσης) ή σε δεύτερο χρόνο. [45]

ΔΙΑΔΙΚΑΣΙΕΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Όπως αναφέρθηκε και προηγουμένως, ως αυθεντικοποίηση ορίζεται το μέτρο ασφαλείας κατά το οποίο εξετάζονται τα δικαιώματα ενός χρήστη πριν την είσοδό του σε ένα υπολογιστικό σύστημα. Πρόκειται για την διαδικασία επιβεβαίωσης της εγκυρότητας της ταυτότητας ενός ατόμου, προκειμένου να του επιτραπεί η πρόσβαση σε ένα σύστημα. Υπάρχουν τρεις βασικοί παράγοντες (factors) που καθορίζουν την διαδικασία της αυθεντικοποίησης. [11]

1. Κάτι που ο χρήστης γνωρίζει (Something You Know, SYK)

Ο παράγοντας αυτός υποδεικνύει ότι η αυθεντικοποίηση γίνεται με βάση κάποια πληροφορία για την οποία έχει γνώση μόνο ο εκάστοτε χρήστης. Στις περισσότερες περιπτώσεις η πληροφορία αυτή είναι κάποιο PIN (Personal Identification Number), ή κάποιος κωδικός πρόσβασης που είτε έχει επιλέξει ο ίδιος ο χρήστης, είτε έχει παραχθεί μέσω κάποιου προγράμματος γεννήτριας κωδικών.

Η χρήση κωδικών πρόσβασης είναι από τις πιο συνήθεις τεχνικές αυθεντικοποίησης που όμως ενέχει αρκετούς κινδύνους αν εφαρμοστεί από τον χρήστη λανθασμένη διαχείριση. Οι χρήστες θα πρέπει να αλλάζουν συχνά τους κωδικούς που χρησιμοποιούν, να θέτουν πιο πολύπλοκους συνδυασμούς στους χαρακτήρες τους και να αποφεύγουν να τους γνωστοποιούν σε άλλους. Για συστήματα που δεν έχουν υψηλές απαιτήσεις ασφαλείας, είναι μια αποτελεσματική και οικονομική λύση. Από την άλλη, τα συστήματα που απαιτούν υψηλά ποσοστά ασφαλείας (π.χ. εταιρείες, τράπεζες, κυβερνητικοί οργανισμοί) , έχουν συγκεκριμένα κριτήρια επιλογής των συνθηματικών τους τα οποία καθορίζονται από το πλαίσιο της πολιτικής ασφαλείας τους. Στη συνέχεια, οι κωδικοί αυτοί, φιλτράρονται (με λογισμικό password filter) για να ελεγχθεί και να διαπιστωθεί ότι πληρούν τις προϋποθέσεις. Σε πολλές περιπτώσεις μάλιστα, χρησιμοποιούνται τεχνικές που εφαρμόζουν και οι εισβολείς συστημάτων (π.χ. cracking), προκειμένου να διαπιστωθεί η ισχύς τους. [11]

2. Κάτι που ο χρήστης έχει στην κατοχή του (Something You Have, SYH)

Σύμφωνα με αυτόν τον παράγοντα, η διαδικασία της αυθεντικοποίησης στηρίζεται στην κατοχή ενός φυσικού αντικειμένου. Παραδείγματα τέτοιων αντικειμένων είναι η μαγνητική κάρτα, η έξυπνη κάρτα, η ταυτότητα ή τα USB tokens (μικρές συσκευές που επιβεβαιώνουν ηλεκτρονικά την αυθεντικότητα του ατόμου). Τα φυσικά αντικείμενα ωστόσο, δεν αποτελούν ασφαλείς και αξιόπιστες μεθόδους αυθεντικοποίησης από την στιγμή που υπάρχει η πιθανότητα να κλαπούν ή να χαθούν, γι αυτό τον λόγο πολλές φορές ο παράγοντας αυτός εφαρμόζεται σε συνδυασμό με κάποιον από τους άλλους δυο τύπους. [11]

3. Κάτι που τον χαρακτηρίζει (Something You Are, SYA)

ΒΙΟΜΕΤΡΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Στην συγκεκριμένη περίπτωση, η ταυτοποίηση γίνεται με την σάρωση και την στατιστική ανάλυση των βιομετρικών χαρακτηριστικών ενός χρήστη. Στα βιομετρικά του χαρακτηριστικά ανήκουν, πληροφορίες για ένα άτομο, όπως για παράδειγμα τα δακτυλικά αποτυπώματα, η αναγνώριση φωνής, η αναγνώριση προσώπου, η αναγνώριση της ίριδα του ματιού αλλά και του αμφιβληστροειδή του (retina). Στόχος αυτής της μεθόδου είναι η επαλήθευση της ταυτότητας του χρήστη (Identity Verification), αλλά και η ταυτοποίησή του (Identification),

για αυτό τον λόγο εκτελείται σε δύο βήματα. Στο πρώτο βήμα γίνεται η διαδικασία της εγγραφής (registration phase) κατά την οποία συλλέγεται το δείγμα μέσω κάποιας συσκευής σάρωσης όπως οπτικούς αναγνώστες ή ψηφιακή κάμερα. Στη συνέχεια ακολουθεί η επεξεργασία του συλλεγμένου δείγματος το οποίο ψηφιοποιείται και αποθηκεύεται στην βάση δεδομένων ως πρότυπο (template) για αυθεντικοποίηση σε δεύτερο χρόνο. Στο δεύτερο βήμα, γίνεται η επαλήθευση. Το βιομετρικό χαρακτηριστικό του χρήστη, συγκρίνεται με το πρότυπο που αποθηκεύτηκε κατά την εγγραφή στη βάση δεδομένων. Έπειτα, εξάγεται το αποτέλεσμα αναγνώρισης που προσδιορίζει αν το δείγμα έχει ταυτοποιηθεί με το πρότυπο στη βάση, ή όχι. [11]

ΣΥΜΠΕΡΙΦΟΡΙΣΤΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Κατά τη διάρκεια των καθημερινών τους δραστηριοτήτων, οι άνθρωποι τείνουν να αναπτύσσουν μοναδικές δεξιότητες, να χρησιμοποιούν τις δικές τους στρατηγικές και να διαμορφώνουν τους δικούς τους τρόπους συμπεριφοράς. Οι ερευνητές αυτής της κατηγορίας, επιδιώκουν να ποσοτικοποιήσουν τα συμπεριφοριστικά χαρακτηριστικά που παρουσιάζει ο κάθε άνθρωπος έτσι ώστε να δημιουργηθεί ένα προφίλ με βάση το οποίο θα γίνεται η επιτυχής εξακρίβωση της ταυτότητάς του. Ανάλογα με την πληροφορία που συλλέγεται κάθε φορά, τα συμπεριφοριστικά χαρακτηριστικά μπορούν να καταταχθούν σε κατηγορίες. Πιο συγκεκριμένα, συμπεριφοριστικά στοιχεία μπορούν να εξαχθούν έπειτα από την ανάλυση της συγγραφικής ιδιότητας ενός χρήστη, όπως είναι για παράδειγμα ένα χειρόγραφο απόσπασμα πάνω στο οποίο εξετάζονται το λεξικό, τα σημεία στίξης και η πίεση που ασκείται κατά την συγγραφή. Η δεύτερη κατηγορία, προκύπτει από την παρατήρηση της αλληλεπίδρασης ανθρώπου-μηχανής, όπου αναλύεται ο τρόπος χρήσης συσκευών εισόδου (π.χ. δυναμική στο πληκτρολόγιο, στο ποντίκι, στις τεχνολογίες αφής) αλλά και η εφαρμογή στρατηγικών και δεξιοτήτων που μπορεί να έχει ο χρήστης κατά τη διάρκεια αυτής της αλληλεπίδρασης (ταχύτητα, συντομεύσεις πληκτρολογίου). Η τρίτη κατηγορία είναι συναφής με την προηγούμενη, καθώς αναλύονται τα γεγονότα που προκύπτουν από την αλληλεπίδραση του χρήστη με τον υπολογιστή. Πρόκειται για ενέργειες χαμηλού επιπέδου, όπως είναι για παράδειγμα τα ίχνη που αφήνουν οι εκτελέσεις προγραμμάτων, οι κλήσεις συστήματος (system calls), ή οι εγγραφές πρόσβασης (registry access), και λαμβάνουν χώρα χωρίς να το αντιλαμβάνεται άμεσα ο χρήστης. Στην τέταρτη κατηγορία, ανήκουν οι κινητικές δεξιότητες ενός ατόμου, οι οποίες περιλαμβάνουν τη λειτουργία του εγκεφάλου, του σκελετού, των αρθρώσεων και του νευρικού συστήματος. Παράδειγμα κινητικής δεξιότητας αποτελεί ο βηματισμός. [46]

ΠΟΛΙΤΙΚΕΣ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ

Η διαδικασία που ακολουθείται της ταυτοποίησης των χρηστών, είναι εκείνη του ελέγχου πρόσβασης. Πρόκειται για την ενέργεια που προσδιορίζει ποιος χρήστης έχει πρόσβαση στο σύστημα και για ποιες λειτουργίες αυτός είναι εξουσιοδοτημένος. Επίσης καθορίζει αν το εκάστοτε αίτημά του θα πρέπει να απορριφθεί ή όχι. Πιο συγκεκριμένα, σύμφωνα με τον Dieter Gollman, ο όρος «πρόσβαση» υποδηλώνει την ύπαρξη μιας ενεργής οντότητας (ενός υποκειμένου) που προσπελαύνει ένα αντικείμενο ακολουθώντας κάποιες συγκεκριμένες

διαδικασίες, ενώ υπάρχει μηχανισμός εξουσιοδότησης (reference monitor) που αποδέχεται ή απορρίπτει την πρόσβαση. Ανάλογα με τις απαιτήσεις ασφαλείας των πληροφοριακών συστημάτων αλλά και τον βαθμό ευαισθησίας της πληροφορίας, γίνεται χρήση των κατάλληλων μηχανισμών ελέγχου πρόσβασης. Η πολιτική ελέγχου πρόσβασης αποτελεί μέρος της πολιτικής ασφαλείας ενός οργανισμού και προσδιορίζει τους κανόνες ελέγχου αλλά και τα δικαιώματα των χρηστών που τον απαρτίζουν. Παρακάτω παρατίθενται κάποιες βασικές έννοιες που θα βοηθήσουν στην καλύτερη κατανόηση των μηχανισμών ελέγχου πρόσβασης που ακολουθούν. [12][47]

ΥΠΟΚΕΙΜΕΝΟ (Subject): Ως υποκείμενα ορίζονται οι χρήστες, οι διεργασίες καθώς και τα προγράμματα που προσπαθούν να ανταλλάσουν δεδομένα μέσω δικτύου.

ΑΝΤΙΚΕΙΜΕΝΟ (Object): Ως αντικείμενα ορίζονται οι πόροι που προστατεύονται από το σύστημα. Μπορεί να είναι υπηρεσίες, αρχεία ή φάκελοι.

ΛΕΙΤΟΥΡΓΙΑ (Operation): Ως λειτουργία ορίζεται η ενεργή διαδικασία που επικαλείται ένα αντικείμενο.

ΔΙΚΑΙΩΜΑ (Privilege): Είναι η εξουσιοδότηση για την διεκπεραίωση μιας πράξης στο υπολογιστικό σύστημα. Συγκεκριμένα, για την παραχώρηση πρόσβασης σε έναν πληροφοριακό πόρο, δηλαδή σε ένα αντικείμενο.

ΛΙΣΤΑ ΕΛΓΧΟΥ ΠΡΟΣΒΑΣΗΣ (ACL): Μια λίστα που σχετίζεται με ένα αντικείμενο και καθορίζει όλα τα θέματα που μπορούν να έχουν πρόσβαση στο αντικείμενο, μαζί με τα δικαιώματά τους στο αντικείμενο. Κάθε εγγραφή στη λίστα είναι ένα ζεύγος (υποκείμενο, σύνολο δικαιωμάτων).

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ Matrix: Ένας πίνακας στον οποίο κάθε γραμμή αντιπροσωπεύει ένα θέμα, κάθε στήλη αντιπροσωπεύει ένα αντικείμενο και κάθε εγγραφή είναι το σύνολο των δικαιωμάτων πρόσβασης του υποκειμένου στο συγκεκριμένο αντικείμενο. Γενικά, ο πίνακας ελέγχου πρόσβασης είναι αραιός: τα περισσότερα υποκείμενα δεν έχουν δικαιώματα πρόσβασης σε στα περισσότερα αντικείμενα. Ως εκ τούτου, έχουν προταθεί διάφορες αναπαραστάσεις. Ο πίνακας ελέγχου πρόσβασης μπορεί να αναπαρασταθεί ως μια λίστα από τριπλέτες, με τη μορφή <υποκείμενο, δικαιώματα, αντικείμενο>.

ΔΙΑΧΩΡΙΣΜΟΣ ΑΡΜΟΔΙΟΤΗΤΩΝ (Separation of Duty, SOD): Η αρχή ότι κανένας χρήστης δεν πρέπει να έχει αρκετά προνόμια έτσι ώστε να αποτρέπεται η κατάχρηση του συστήματος. Ο διαχωρισμός των καθηκόντων μπορεί να επιβληθεί είτε στατικά με τον ορισμό αντικρουόμενων ρόλων (δηλαδή ρόλων που δεν μπορούν να εκτελεστούν από τον ίδιο χρήστη) είτε δυναμικά με εφαρμογή του ελέγχου κατά τη στιγμή της πρόσβασης.

ΑΣΦΑΛΕΙΑ (Safety): Η διαμόρφωση του ελέγχου πρόσβασης (π.χ. μηχανισμός ελέγχου πρόσβασης ή μοντέλο) με τρόπο τέτοιο ώστε να μην έχει ως αποτέλεσμα τη διαρροή δικαιωμάτων σε μη εξουσιοδοτημένους χρήστες.

ΕΦΑΡΜΟΞΗ ΤΟΜΕΩΝ ΚΑΙ ΤΥΠΟΥ (Domain and Type Enforcement): Κάθε διεργασία εκτελείται εντός ενός τομέα και στα αντικείμενα αποδίδεται ένας τύπος. Ένας ορισμός τομέα καθορίζει τα δικαιώματα που έχει κάθε τομέας σε αντικείμενα ενός συγκεκριμένου τύπου. Όλες οι διεργασίες που εκτελούνται εντός του ίδιου τομέα έχουν το ίδιο σύνολο δικαιωμάτων

πρόσβασης. Η ανάθεση διεργασιών σε τομείς παρέχει έναν ευέλικτο μηχανισμό για την εφαρμογή μιας πολιτικής ασφαλείας.

ΚΑΤΑ ΔΙΑΚΡΙΣΗ ΜΟΝΤΕΛΟ DAC (DESCRETIONARY ACCESS CONTROL)

Ο προαιρετικός έλεγχος πρόσβασης όπως αλλιώς ονομάζεται, λειτουργεί ως μέσο περιορισμού της πρόσβασης σε πόρους και αντικείμενα του συστήματος με βάση την ταυτότητα ενός μεμονωμένου χρήστη ή μιας ομάδας χρηστών στην οποία ανήκει. Στο μοντέλο αυτό εντάσσεται η πολιτική του μηχανισμού της ιδιοκτησίας των αντικειμένων του συστήματος, κατά το οποίο η πρόσβαση στο αντικείμενο από τρίτους επαφίεται στην κρίση του ιδιοκτήτη. Εκείνος δύναται να εγκρίνει ή να απορρίψει την άδεια εισόδου σε άλλα υποκείμενα. Πρόκειται για ένα χρηστοκεντρικό και αρκετά ευέλικτο μοντέλο ελέγχου προσπέλασης που βρίσκει ευρεία χρήση σε εμπορικούς και κρατικούς φορείς. Ωστόσο κρίνεται ακατάλληλο για συστήματα με υψηλές απαιτήσεις σε ασφάλεια καθώς τα δικαιώματα που εκχωρεί ο ιδιοκτήτης σε κάποιο υποκείμενο έχουν κληρονομικό χαρακτήρα και μπορούν να μεταβιβαστούν σχετικά εύκολα σε κάποιο τρίτο εν αγνοία του, γεγονός που το κάνει ευάλωτο σε επιθέσεις Δούρειου Ίππου. [47][48]

ΚΑΤ'ΑΠΑΙΤΗΣΗ ΜΟΝΤΕΛΟ MAC (MANDATORY ACCESS CONTROL)

Κατά το μοντέλο αυτό, οι αποφάσεις για τον έλεγχο πρόσβασης υπόκεινται σε κάποια κεντρική αρχή και όχι μεμονωμένα στον ιδιοκτήτη των αντικειμένων του συστήματος. Σε αυτή την περίπτωση, το υποκείμενο (χρήστης) και το αντικείμενο, συσχετίζονται με έναν μηχανισμό επιπέδων ευαισθησίας ο οποίος συνήθως υλοποιείται με την χρήση ετικετών τόσο στους χρήστες όσο και στα αντικείμενα. Οι ετικέτες αυτές καθορίζουν την εξουσιοδότηση των υποκειμένων (clearance), καθώς και την σημαντικότητα των αντικειμένων (classification). Τα επίπεδα ευαισθησίας της πληροφορίας διακρίνονται ως Αδιαβάθμητη (infinitely), Εμπιστευτική (confidential), Απόρρητη (confidential), Άκρως απόρρητη(top secret). Κατά τη χρήση αυτού του μοντέλου, το υποκείμενο δεν έχει την ικανότητα να τροποποιήσει τα δικαιώματα πρόσβασης που του έχουν αποδοθεί αλλά ούτε και να έχει πρόσβαση σε δεδομένα άλλης βαθμίδας (για παράδειγμα αν ένας χρήστης είναι εξουσιοδοτημένος στη βαθμίδα secret, δεν μπορεί να διαβάσει δεδομένα που ανήκουν στη βαθμίδα top secret). Το τελευταίο αποτελεί κανόνα και ονομάζεται απλός κανόνας ασφαλείας. Το κατ'απαίτηση μοντέλο βρίσκει εφαρμογή κυρίως σε στρατιωτικά περιβάλλοντα όπου γίνεται χρήση διαβάθμισης της πληροφορίας. [47][48]

ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΒΑΣΙΣΜΕΝΗ ΣΕ ΡΟΛΟΥΣ (ROLE BASED ACCESS CONTROL)

Πρόκειται για ένα καινοτόμο μοντέλο όσον αφορά στη διαχείριση των δικαιωμάτων πρόσβασης, καθώς για πρώτη φορά εισάγεται η έννοια του ρόλου. Στο μοντέλο αυτό, οι χρήστες δεν αποκτούν άμεσα άδειες για εκτέλεση εργασιών, αλλά ο διαχωρισμός των καθηκόντων πραγματοποιείται δυναμικά. Κατά τον συγκεκριμένο μηχανισμό, οι διαχειριστές του εκάστοτε πληροφοριακού συστήματος δημιουργούν ρόλους σύμφωνα με τις ανάγκες του

κάθε οργανισμού, οι οποίοι περιλαμβάνουν ένα σύνολο δικαιωμάτων και αντιπροσωπεύουν καθορισμένες δραστηριότητες. Στη συνέχεια, οι ρόλοι αυτοί ανατίθενται στους χρήστες ανάλογα με τις αρμοδιότητες που έχουν αναλάβει. Οι βασικές σχέσεις αυτού του μοντέλου, είναι η ανάθεση ρόλων στους χρήστες (user-role assignment) και η ανάθεση δικαιωμάτων στους ρόλους (permission-role assignment), που αν και αλληλένδετες, προσφέρουν στα συστήματα που κάνουν χρήση αυτού του μοντέλου ευελιξία και διαχειριστική ευκολία. [47][48]

Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗΝ ΥΠΗΡΕΣΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η αδιάκοπη εξέλιξη των τεχνολογιών και των υπολογιστικών συστημάτων, θέτει πλέον επιτακτική την ανάγκη προστασίας των δεδομένων που διακινούνται καθημερινά στον κυβερνοχώρο. Η εξασφάλιση του απορρήτου στις ψηφιακές επικοινωνίες επιτυγχάνεται με την απόκρυψη του περιεχομένου της διακινούμενης πληροφορίας. Το ευρύτερο διεπιστημονικό πεδίο που ασχολείται με την μελέτη της ασφαλούς επικοινωνίας, ονομάζεται ***κρυπτολογία***. Η κρυπτολογία αποτελείται από δύο επιμέρους πεδία, την *κρυπτογραφία* και την *κρυπτανάλυση*. Η κρυπτογραφία είναι το πεδίο εκείνο που ασχολείται με την μελέτη, την ανάπτυξη και τη χρήση τεχνικών που κωδικοποιούν την πληροφορία με τρόπο τέτοιο ώστε να μην είναι προσπελάσιμη και αναγνώσιμη από χρήστες που δεν διαθέτουν δικαιώματα εξουσιοδότησης. Η διαδικασία της κωδικοποίησης της πληροφορίας ονομάζεται κρυπτογράφηση, ενώ η ανάκτηση του αρχικού (κωδικοποιημένου) μηνύματος από τον εξουσιοδοτημένο παραλήπτη, ονομάζεται αποκρυπτογράφηση και είναι η αντίστροφη ακριβώς διαδικασία. Η κρυπτανάλυση από την άλλη, είναι ο κλάδος της κρυπτολογίας που ασχολείται με την προσπάθεια ανεύρεσης αδύναμων σημείων στους κρυπτογραφικούς αλγόριθμους έχοντας ως στόχο είτε την υποκλοπή του κρυπτογραφημένου μηνύματος, είτε την κατασκευή ασφαλέστερων δομών κρυπτογραφικών αλγορίθμων. Για να γίνει μια επίθεση κρυπτανάλυσης εφικτή, υπάρχουν δύο προσεγγίσεις. Κατά την πρώτη προσέγγιση, ο επιτιθέμενος θα πρέπει να είναι σε θέση να γνωρίζει κάποια γενικά χαρακτηριστικά του αρχικού μηνύματος ή ολόκληρο το αρχικό μήνυμα και το κρυπτοκείμενο έτσι ώστε να είναι εφικτό να ανακτηθεί είτε το αρχικό μήνυμα, είτε το κλειδί που χρησιμοποιείται. Η δεύτερη προσέγγιση, είναι με επιθέσεις εξαντλητικής αναζήτησης όπου ο επιτιθέμενος εξετάζει ένα προς ένα τα πιθανά κλειδιά μέχρι να αποκρυπτογραφηθεί το κρυπτοκείμενο και να ανακτηθεί το αρχικό μήνυμα. Τα είδη επιθέσεων που λαμβάνουν χώρα σε κρυπτογραφικά συστήματα με βάση τη ποσότητα πληροφορίας που γνωρίζει ο κρυπταναλυτής είναι η επίθεση γνωστού κρυπτοκειμένου, γνωστού μηνύματος, επιλεγμένου μηνύματος και επιλεγμένου κειμένου. [8][49]

ΣΥΜΜΕΤΡΙΚΗ ΚΑΙ ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Πριν εμβαθύνουμε, είναι απαραίτητο να γίνει μια παρουσίαση των βασικών όρων που απαρτίζουν την λειτουργία ενός κρυπτογραφικού συστήματος. Ένα κρυπτογραφικό σύστημα λοιπόν, αποτελείται από τα εξής χαρακτηριστικά: [8]

- Αρχικό μήνυμα : Είναι το μήνυμα που μπαίνει ως είσοδος στον αλγόριθμο με σκοπό να κρυπτογραφηθεί.

- Αλγόριθμος κρυπτογράφησης: Είναι η μέθοδος μέσω της οποίας μετασχηματίζεται το αρχικό μήνυμα σε κρυπτογράφημα.
- Κλειδί κρυπτογράφησης: Μια ποσότητα πληροφορίας σε μορφή bit που μπαίνει ως είσοδος μαζί με το αρχικό μήνυμα στη συνάρτηση κρυπτογράφησης. Κάθε κλειδί που χρησιμοποιείται στο ίδιο μήνυμα, παράγει διαφορετική έξοδο.
- Κρυπτοκείμενο: Φαινομενικά πρόκειται για μια τυχαία ροή από σύμβολα και αριθμούς. Στην ουσία είναι το πλέον κρυπτογραφημένο μήνυμα σε μορφή ακατάληπτη για τους ανθρώπους αλλά και τις εφαρμογές.
- Αλγόριθμος αποκρυπτογράφησης: Είναι η αντίστροφη διαδικασία από την κρυπτογράφηση. Με τον ίδιο τρόπο, δέχεται ως είσοδο το κρυπτοκείμενο και το κλειδί αποκρυπτογράφησης.

Αξίζει να αναφερθεί ότι τα σύγχρονα κρυπτογραφικά συστήματα ανάλογα με τον αριθμό των κλειδιών που χρησιμοποιούνται διακρίνονται σε συμμετρικά και ασύμμετρα.

Συμμετρική κρυπτογραφία

Στη συμμετρική κρυπτογραφία ο αποστολέας και ο παραλήπτης χρησιμοποιούν το ίδιο μυστικό κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Το κλειδί αυτό, μεταδίδεται μέσω ενός ασφαλούς καναλιού επικοινωνίας και είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη του μηνύματος. Κατά την συμμετρική κρυπτογράφηση δύναται να χρησιμοποιούνται τεχνικές αντιμετάθεσης, τεχνικές αντικατάστασης ή συνδυασμός τους. Στις τεχνικές αντικατάστασης, κάθε σύμβολο του αρχικού μηνύματος αντικαθίσταται από κάποιο σύμβολο του κρυπτογράμματος ενώ στις τεχνικές αντιμετάθεσης, τα σύμβολα του αρχικού μηνύματος αντιμετατίθενται με κάποιο συστηματικό τρόπο. Η συμμετρική κρυπτογράφηση ονομάζεται και συμβατική ή μυστικού κλειδιού. Παραδείγματα συμμετρικής κρυπτογράφησης αποτελούν οι αλγόριθμοι DES (Data Encryption Standard) , Triple-DES (Triple- Data Encryption Standard), AES (Advanced Encryption Standard) . [8]

Ασύμμετρη κρυπτογραφία

Η λειτουργία της ασύμμετρης κρυπτογράφησης ή αλλιώς της κρυπτογραφίας δημοσίου κλειδιού, στηρίζεται στην ύπαρξη δύο διαφορετικών κλειδιών που σχετίζονται μεταξύ τους, όπου το ένα χρησιμοποιείται για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση. Το κλειδί της κρυπτογράφησης είναι δημόσιο, μπορεί δηλαδή να είναι γνωστό σε όλους. Το κλειδί της αποκρυπτογράφησης είναι ιδιωτικό και είναι γνωστό μόνο στον αποστολέα και στον παραλήπτη, έτσι ώστε η εισερχόμενη επικοινωνία να είναι ασφαλής. Ωστόσο, η γνώση του ενός κλειδιού δεν οδηγεί στην αποκάλυψη του άλλου. Η ασύμμετρη κρυπτογράφηση στηρίζεται σε μαθηματικές συναρτήσεις και όχι σε αντιμεταθέσεις και αντικαταστάσεις όπως η συμμετρική. Παραδείγματα ασύμμετρων κρυπταλγορίθμων αποτελεί ο αλγόριθμος Diffie-Hellman και ο RSA. [8]

ΒΑΣΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

Με την χρήση των σύγχρονων κρυπτογραφικών συστημάτων διασφαλίζεται το απόρρητο στις ψηφιακές επικοινωνίες και είναι δυνατό να αντιμετωπιστούν έγκαιρα συγκεκριμένες απειλές. Οι στόχοι που μπορούν να επιτευχθούν με την χρήση της κρυπτογραφίας, είναι η **εμπιστευτικότητα** (confidentiality), η **ακεραιότητα** (integrity), η **μη απάρνηση** (no repudiation) και η **αυθεντικοποίηση** (authentication). Αναλυτικότερα, με την εμπιστευτικότητα, διασφαλίζεται ότι τα προς μετάδοση δεδομένα δεν θα γνωστοποιηθούν καθώς επίσης και το ότι δεν θα είναι προσπελάσιμα από χρήστες που δεν έχουν δικαιώματα εξουσιοδότησης. Ο στόχος αυτός, υλοποιείται με την βοήθεια μηχανισμών ελέγχου πρόσβασης. Με την ακεραιότητα εξασφαλίζεται ότι τα μεταδιδόμενα δεδομένα δεν θα υποβληθούν σε κανενός είδους τροποποίηση ή αντικατάσταση από μη εξουσιοδοτημένες οντότητες. Αυτό επιτυγχάνεται με την χρήση των ψηφιακών υπογραφών. Ακόμη με τη συμβολή των ψηφιακών υπογραφών επιτυγχάνεται και η μη απάρνηση, κατά την οποία και ο αποστολέας και ο παραλήπτης ενός μηνύματος δεν είναι σε θέση να αποποιηθούν την γνησιότητα της προέλευσης και του προορισμού αυτού του μηνύματος. Με την αυθεντικοποίηση πραγματοποιείται η αναγνώριση της ταυτότητας των οντοτήτων που επικοινωνούν ή της πηγής προέλευσης και αποστολής των δεδομένων. [50]

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Η πλέον ασφαλής τεχνολογική μέθοδος που χρησιμοποιείται ως μέσο επικύρωσης της γνησιότητας ενός συνόλου δεδομένων, είναι εκείνη της ψηφιακής υπογραφής. Η ψηφιακή υπογραφή είναι ένας μηχανισμός αυθεντικοποίησης για τους χρήστες που συναλλάσσονται, αλλά και ένας τρόπος προστασίας των πληροφοριών που εμπεριέχονται στα αρχεία και τα μηνύματα που διακινούνται. Όπως στη καθημερινότητα, μια οντότητα κατοχυρώνεται νομικά με την χειρόγραφη υπογραφή, ομοίως και στην ψηφιακή πραγματικότητα η ηλεκτρονική υπογραφή έχει νομική ισχύ και δεσμεύει τον υπογράφοντα με το μήνυμα που αποστέλλεται. Η σημασία των ψηφιακών υπογραφών έγκειται στην εγκυρότητα και την επαληθευσιμότητα που προσφέρουν. Η ψηφιακή υπογραφή είναι μια τεχνολογία που βασίζεται στην ασύμμετρη κρυπτογραφία και είναι δύο τα στάδια που την απαρτίζουν, η δημιουργία της και η επαλήθευσή της.

Για την δημιουργία της ψηφιακής υπογραφής χρησιμοποιείται το ιδιωτικό κλειδί, ενώ η επαλήθευσή της από τον παραλήπτη, πραγματοποιείται με την χρήση του δημοσίου κλειδιού. Η πιο διαδεδομένη μέθοδος δημιουργίας μιας ηλεκτρονικής υπογραφής ονομάζεται «μέθοδος του δακτυλικού αποτυπώματος» ή και αλλιώς γνωστή ως «σύνοψη μηνύματος» (message digest). Σύμφωνα με την συγκεκριμένη μέθοδο, ο αποστολέας χρησιμοποιεί έναν αλγόριθμο κατακερματισμού έτσι ώστε να παράγει μια σύντμηση του μηνύματος που θέλει να μεταβιβάσει. Ανεξάρτητα με το μέγεθος του μηνύματος, μετά την σύντμηση, παράγεται μια ακολουθία ψηφίων σταθερού μήκους, που ονομάζεται κώδικας κατακερματισμού (hash code). Στη συνέχεια, ο αποστολέας κρυπτογραφεί τον κώδικα κατακερματισμού κάνοντας χρήση του ιδιωτικού κλειδιού , όπου το αποτέλεσμα είναι η δημιουργία της ψηφιακής υπογραφής. Η ψηφιακή υπογραφή, τελικά προσαρτάται στο αρχικό, μη κρυπτογραφημένο μήνυμα και το σύνολο αποστέλλεται στον τελικό παραλήπτη. [51]

Η διαδικασία επαλήθευσης της ψηφιακής υπογραφής πραγματοποιείται στην πλευρά του παραλήπτη. Αρχικά, ο ίδιος διαχωρίζει το μήνυμα από την ψηφιακή υπογραφή και το αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα. Στη συνέχεια δημιουργεί και εκείνος μια σύνοψη του μηνύματος που παρέλαβε, χρησιμοποιώντας τον ίδιο αλγόριθμο κατακερματισμού. Με τον τρόπο αυτό παράγεται μια νέα σύντμηση. Χαρακτηριστικό της μεθόδου δακτυλικού αποτυπώματος, είναι το γεγονός ότι για συγκεκριμένη τιμή εισόδου, παράγεται πάντα η ίδια έξοδος, το αντίστροφο όμως δεν ισχύει! Ο παραλήπτης συγκρίνει τη δική του σύντμηση, με εκείνη του αποστολέα. Εφόσον οι δύο συντμήσεις είναι ίδιες, πιστοποιείται ότι το μήνυμα παραδόθηκε στον παραλήπτη χωρίς αλλοιώσεις ή τροποποιήσεις. Στην περίπτωση που υπάρχει κάποια διαφορά στις δυο τιμές, αυτό σημαίνει ότι το προς αποστολή μήνυμα έχει υποστεί μεταβολές. [1][8][51]

Όπως στην πραγματική ζωή ένας χρήστης ή μια υπηρεσία δεν αρκείται μόνο στην ύπαρξη της χειρόγραφης υπογραφής, αλλά απαιτείται, με κάποιο τρόπο, να έχει θεωρηθεί η γνησιότητά της από μια έμπιστη αρχή, με παρόμοιο τρόπο και στα πληροφοριακά συστήματα, το δημόσιο κλειδί θα πρέπει να επαληθεύεται από μια τρίτη έμπιστη οντότητα (Third Trusted Party), εκτός των συναλλασσόμενων. Η έμπιστη οντότητα ,παράγει το ψηφιακό πιστοποιητικό, ένα ηλεκτρονικό έγγραφο που πιστοποιεί το δημόσιο κλειδί και το συσχετίζει με την ταυτότητα του ιδιοκτήτη του, αλλά και παρέχει έναν ασφαλή τρόπο με τον οποίο θα μεταδίδονται οι τιμές των δημοσίων κλειδιών καθώς και οι πληροφορίες των κατόχων τους. Η έμπιστη Τρίτη οντότητα που δημιουργεί και διαχειρίζεται τα πιστοποιητικά, ονομάζεται Αρχή Πιστοποίησης (Certificate Authority, CA) και αποτελεί μέρος του μοντέλου της αρχιτεκτονικής υποδομής δημοσίου κλειδιού στο πλαίσιο του προτύπου X.509. [1] Η δυνατότητα απόκτησης ψηφιακού πιστοποιητικού, πραγματοποιείται κατόπιν αιτήσεως στην Αρχή Πιστοποίησης. Με βάση λοιπόν το πρότυπο X.509, η δομή ενός ψηφιακού πιστοποιητικού θα πρέπει να καθορίζεται ως εξής:

- Έκδοση (Version)
- Σειριακός αριθμός πιστοποιητικού (Serial Number)
- Προσδιοριστικό αλγορίθμου υπογραφής (Signature Algorithm identifier)
- Όνομα εκδότη (Issuer name)
- Όνομα ιδιοκτήτη (Subject name)
- Περίοδος ισχύος (Validity date)
- Πληροφορίες δημοσίου κλειδιού ιδιοκτήτη (Subject's public key information)
- Μοναδικό αναγνωριστικό εκδότη (Issuer unique identifier)
- Μοναδικό αναγνωριστικό ιδιοκτήτη (Subject unique identifier)
- Επεκτάσεις (extentions)

ΤΟ ΣΥΣΤΗΜΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ KERBEROS

Το Kerberos είναι ένα σύστημα αυθεντικοποίησης που αναπτύχθηκε στο MIT στα πλαίσια του project Athena. Σκοπός του είναι να παρέχει ισχυρή αυθεντικοποίηση σε εφαρμογές πελάτη-εξυπηρετητή (client-server) και να επιτρέπει στους χρήστες να μπορούν να προσπελαύνουν τους πόρους του δικτύου με ασφάλεια. Το Kerberos χρησιμοποιεί συμμετρική κρυπτογράφηση και είναι δυο οι διαθέσιμες εκδόσεις του, η έκδοση 4 και η έκδοση 5 στην οποία προστέθηκαν κάποιες αλλαγές σε θέματα ασφαλείας. Το εν λόγω σύστημα αυθεντικοποίησης περιλαμβάνει ένα κεντρικοποιημένο εξυπηρετητή με βάση τον οποίο λειτουργεί ως Τρίτη έμπιστη οντότητα. Ο

εξυπηρετητής αυτός είναι αρμόδιος για την αμοιβαία αυθεντικοποίηση μεταξύ χρηστών και διακομιστών. Το σύστημα Kerberos προσφέρει κατά βάση δύο υπηρεσίες: [8]

- Την υπηρεσία εξυπηρετητή αυθεντικοποίησης (Authentication Server, AS) που επαληθεύει την ταυτότητα των χρηστών κατά την σύνδεσή τους.
- Την υπηρεσία εξυπηρετητή εκχώρησης εισιτηρίων (Ticket Granting Server, TGS) που πιστοποιεί την ταυτότητα των χρηστών και έπειτα εκδίδει εισιτήρια για πρόσβαση σε συγκεκριμένες υπηρεσίες [52]

Το εισιτήριο του συστήματος Kerberos είναι μια δομή στην οποία εφαρμόζεται συμμετρική κρυπτογράφηση με χρήση του κλειδιού υπηρεσίας, στην οποία περιέχονται τα ακόλουθα στοιχεία:

α) Η ταυτότητα του πελάτη

β) Η διεύθυνση του πελάτη

γ) Το κλειδί της συνόδου (session key)

δ) Η χρονική σήμανση που καθορίζει μέχρι πότε θα είναι έγκυρο το κλειδί (timestamp)

ε) Σημαίες (flags) που δηλώνουν αν το εισιτήριο είναι έγκυρο, ανανεώσιμο, μεταχρονολογημένο, προωθούμενο κ.α

Το περιβάλλον του Kerberos αποτελείται από τον βασικό εξυπηρετητή του Kerberos, έναν αριθμό πελατών-χρηστών και τους εξυπηρετητές εφαρμογών. Ο βασικός εξυπηρετητής έχει στη βάση δεδομένων του τα ID και τα συνθηματικά όλων των χρηστών και μοιράζεται ένα μυστικό κλειδί με κάθε διακομιστή. Το περιβάλλον αυτό, ονομάζεται βασιλεία του Kerberos (Kerberos realm) και είναι ένα σύνολο διαχειριζόμενων κόμβων που μοιράζονται την ίδια βάση δεδομένων. [8]

Κατά την λειτουργία του Kerberos, ο χρήστης κάνει αίτηση στον AS για πρόσβαση στον διακομιστή TGS δηλώνοντας την ταυτότητα του. Εφόσον ο AS ταυτοποιήσει τον χρήστη, δημιουργεί ένα εισιτήριο το οποίο περιέχει την ταυτότητα του χρήστη και την ταυτότητα του διακομιστή και τα αποστέλλει πίσω στον χρήστη κρυπτογραφημένα με το μυστικό κλειδί που μοιράζεται ο AS με τον διακομιστή. Στη συνέχεια, ο χρήστης κάνει αίτηση εκχώρησης υπηρεσίας στον TGS, στην οποία του δηλώνει την ταυτότητά του, την ταυτότητα της υπηρεσίας που επιθυμεί και το εισιτήριο που του αποδόθηκε από τον AS. Ο TGS αποκρυπτογραφεί το εισιτήριο με το μυστικό κλειδί που μοιράζεται με τον AS και ταυτοποιεί τις πληροφορίες του εισερχόμενου αιτήματος με το ID του χρήστη και τη διεύθυνση δικτύου. Εφόσον οι πληροφορίες είναι έγκυρες, τότε ο χρήστης παραλαμβάνει το εισιτήριο εκχώρησης υπηρεσίας το οποίο και παρουσιάζει μαζί με την ταυτότητά του. Τέλος, ο διακομιστής αποκρυπτογραφεί το εισιτήριο (του TGS) έτσι ώστε να ανακτήσει το κλειδί συνόδου και με βάση τις πληροφορίες που εμπεριέχονται στο εισιτήριο, να αυθεντικοποιήσει τον χρήστη. Μετά την ολοκλήρωση των παραπάνω βημάτων, ο χρήστης και η υπηρεσία έχουν ταυτοποιηθεί αμοιβαία και μοιράζονται ένα μυστικό κλειδί μέσω ενός ασφαλούς καναλιού επικοινωνίας.[8]

ΣΥΓΧΡΟΝΑ ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

Από όσα έχουν αναφερθεί έως τώρα, είναι αντιληπτό ότι η χρήση της κρυπτογραφίας είναι υψίστης σημασίας για τα σύγχρονα ψηφιακά περιβάλλοντα έτσι ώστε να εξασφαλίζεται η ιδιωτικότητα των χρηστών και η κατά το δυνατό, ασφαλέστερη διακίνηση των δεδομένων τους στον κυβερνοχώρο. Με την πάροδο του χρόνου έχουν αναπτυχθεί αρκετά κρυπτογραφικά συστήματα και πρωτόκολλα που εξυπηρετούν τον σκοπό αυτό. Κάποια από αυτά αφορούν στην ασφάλεια του ηλεκτρονικού ταχυδρομείου όπως είναι για παράδειγμα το Pretty Good Privacy (PGP) και το S/MIME (Secure/ Multipurpose Internet Mail Extension), κάποια στην ασφάλεια πρόσβασης και πλοήγησης στον Παγκόσμιο Ιστό (π.χ. SSL-TLS) και κάποια στην ασφάλεια των ηλεκτρονικών συναλλαγών (π.χ. SET). Ακολουθεί μια σύντομη περιγραφή των προαναφερθέντων κρυπτογραφικών πρωτοκόλλων PGP, S/MIME, SSL-TLS και SET.

PGP (Pretty Good Privacy)

Αποτελεί ένα κρυπτογραφικό σύστημα που σχεδιάστηκε το 1991 από τον Phil Zimmerman με κύριο σκοπό την προστασία του απορρήτου. Σύμφωνα με τον Andrew S. Tanenbaum, ο Zimmerman βασίστηκε στην εξής αρχή «*Αν η προστασία του απορρήτου γίνει παράνομη, τότε μόνο οι παράνομοι θα έχουν προστασία απορρήτου*». [51] Το PGP είναι στην ουσία ένα λογισμικό ανοιχτού κώδικα, ελεύθερα διαθέσιμο σε παγκόσμιο επίπεδο που παρέχει υπηρεσίες εμπιστευτικότητας και αυθεντικοποίησης σε εφαρμογές ηλεκτρονικού ταχυδρομείου και αποθήκευσης αρχείων. Η λειτουργία του λαμβάνει χώρα στο επίπεδο εφαρμογής του TCP/IP και θεωρείται εξαιρετικά ασφαλές λόγω των αλγορίθμων κρυπτογράφησης που χρησιμοποιούνται. Συγκεκριμένα, χρησιμοποιεί RSA, DSS, Diffie-Hellman για κρυπτογράφηση δημοσίου κλειδιού και CAST-128, IDEA και Triple DES για συμμετρική κρυπτογράφηση, ενώ για τη συνάρτηση κατακερματισμού χρησιμοποιείται ο SHA-1. Η λειτουργία του PGP στηρίζεται στην παροχή πέντε υπηρεσιών, στην **αυθεντικοποίηση** μέσω της ψηφιακής υπογραφής, στην **εμπιστευτικότητα** μέσω της συμμετρικής κρυπτογράφησης, στην **συμπίεση** με τη χρήση του αλγορίθμου ZIP, στη **συμβατότητα ηλεκτρονικού ταχυδρομείου** με σχήμα κωδικοποίησης radix-64, και τέλος, στην **κατάτμηση και επανένωση** των μηνυμάτων μεγάλου μεγέθους. [8]

S/MIME (Secure/ Multipurpose Internet Mail Extension)

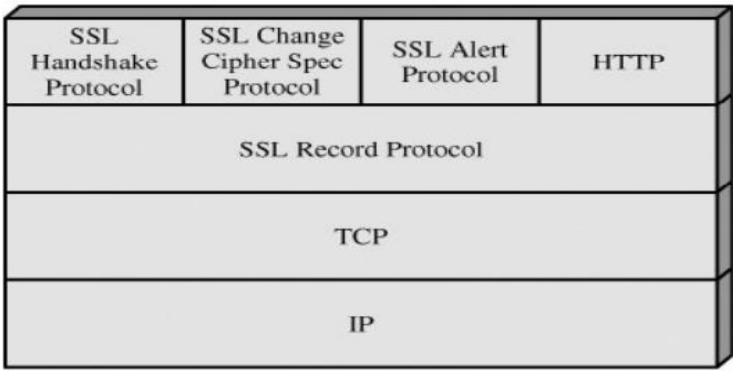
Το πρότυπο MIME αποτελεί επέκταση του προτύπου RFC 822, του πρωτοκόλλου μέσω του οποίου παραδοσιακά μορφοποιούνται και αποστέλλονται τα μηνύματα ηλεκτρονικού ταχυδρομείου. Το MIME αναπτύχθηκε με σκοπό να αντιμετωπίσει περιορισμούς των πρωτοκόλλων μεταφοράς ηλεκτρονικού ταχυδρομείου. [8] Το MIME είναι, επί της ουσίας, μια τεχνική προδιαγραφή πρωτοκόλλων επικοινωνίας που περιγράφει την μεταφορά αρχείων πολυμέσων όπως είναι το βίντεο, ο ήχος και η εικόνα και αναλύονται εκτενέστερα στο RFC 1521. Το S/MIME είναι εξέλιξη του απλού MIME και δημιουργήθηκε για την ενίσχυση της ασφάλειας του ηλεκτρονικού ταχυδρομείου. Αναπτύχθηκε αρχικά από την RSA Data Security και βρίσκεται, όπως και το PGP, στην στοίβα προτύπων του Internet Engineering Task Force

(IETF), με πληθώρα εγγράφων που να προσδιορίζουν την λειτουργία του. Τα σπουδαιότερα από αυτά τα πρότυπα είναι τα RFC 3369, 3370, 3850 και 3851. Στο S/MIME προστέθηκαν δυο επιπλέον στοιχεία, η κρυπτογράφηση και οι ψηφιακές υπογραφές. Στόχος του είναι οι χρήστες να έχουν τη δυνατότητα να αποστέλλουν ψηφιακά υπογεγραμμένα, κρυπτογραφημένα, ή ταυτόχρονα ψηφιακά υπογεγραμμένα και κρυπτογραφημένα μηνύματα μεταξύ τους. Το S/MIME χρησιμοποιεί για κρυπτογράφηση τους αλγορίθμους Diffie-Hellman, RSA και Triple DES, ενώ για τη δημιουργία ψηφιακής υπογραφής χρησιμοποιείται ο SHA-1 και ο MD5 (για συμβατότητα με παλαιότερες εκδόσεις). Ακόμη, χρησιμοποιεί πιστοποιητικά δημοσίου κλειδιού βασισμένα στο πρότυπο X.509. Η λειτουργία του S/MIME είναι παρόμοια με εκείνη του PGP με τη βασική διαφορά ότι το πρώτο δεν λειτουργεί αυτόνομα ως εφαρμογή αλλά παρέχει τις κρυπτογραφικές υπηρεσίες του σε άλλα προγράμματα. Οι νεότερες εκδόσεις του S/MIME επιτρέπουν τη δράση του σε συνδυασμό με άλλα πρωτόκολλα όπως είναι το HTTP, FTP και το SET. [8][53]

SSL-TLS (Secure Socket Layer – Transport Layer Security)

Το SSL, που στα ελληνικά μεταφράζεται ως Ασφαλές Επίπεδο Υποδοχών, αλλά και η νεότερη έκδοσή του TLS , αποτελεί ένα σύνολο από πρωτόκολλα ασφαλείας που αναπτύχθηκε από την Netscape το 1995 για την ασφάλεια των WEB επικοινωνιών. Το SSL χρησιμοποιεί το TCP με σκοπό την δημιουργία ασφαλών συνδέσεων επικοινωνίας μεταξύ δύο οντοτήτων από άκρο σε άκρο. Πιο συγκεκριμένα, το SSL είναι ένα νέο επίπεδο στην στοίβα πρωτοκόλλων του TCP/IP, βρίσκεται ανάμεσα στο επίπεδο εφαρμογών και στο επίπεδο μεταφοράς. Βασική του λειτουργία είναι να δέχεται αιτήσεις απ τους φυλλομετρητές και να τις μεταβιβάζει στο TCP για μετάδοση στον διακομιστή. Όπως φαίνεται και στην παρακάτω εικόνα, αποτελείται από δύο υποεπίπεδα πρωτοκόλλων, το πρωτόκολλο καταγραφής (SSL Record Protocol) που παρέχει βασικές υπηρεσίες σε πρωτόκολλα υψηλότερου επιπέδου όπως είναι για παράδειγμα το HTTP και άλλο ένα επίπεδο ως τμήμα του SSL το οποίο περιλαμβάνει τρία πρωτόκολλα που χρησιμοποιούνται για την διαχείριση ανταλλαγής μηνυμάτων . Τα πρωτόκολλα αυτά του SSL, είναι το πρωτόκολλο Χειραψίας (SSL Handshake Protocol), το πρωτόκολλο Αλλαγής Παραμέτρων Κρυπτογράφησης (SSL Change Cipher Spec Protocol) και τέλος, το πρωτόκολλο Συναγερμού (SSL Alert Protocol). Έπειτα από την εγκαθίδρυση της ασφαλούς σύνδεσης, αναλαμβάνει την διαχείριση της συμπίεσης και της κρυπτογράφησης. Οι υπηρεσίες που προσφέρει το SSL κατά τη δημιουργία ασφαλών συνδέσεων μεταξύ υποδοχών, περιλαμβάνουν: [8][52]

1. Διαπραγμάτευση παραμέτρων μεταξύ πελάτη και διακομιστή
2. Αμοιβαία πιστοποίηση ταυτότητας
3. Μυστικότητα στην επικοινωνία
4. Προστασία της ακεραιότητας των δεδομένων



Εικόνα 11 Επίπεδα του Πρωτοκόλλου SSL

SET (Secure Transactions Protocol)

Το SET είναι ένα πρωτόκολλο ασφαλείας, μια ανοιχτή προδιαγραφή του οποίου η σχεδίαση έχει ως στόχο την ασφαλή περάτωση κρυπτογραφημένων ηλεκτρονικών συναλλαγών με χρήση πιστωτικών καρτών. Η προδιαγραφή αυτή αναπτύχθηκε για πρώτη φορά τον Φεβρουάριο του 1996 από ένα σύνολο εταιρειών μεταξύ των οποίων ήταν η Visa, η Mastercard, η Verisign,η IBM, η Microsoft και η Netscape. *Το SET δεν είναι ένα σύστημα πληρωμής, αλλά μια μορφοποίηση (specification), ένα σύνολο πρωτοκόλλων που επιτρέπει την ασφαλή διεξαγωγή των ηλεκτρονικών συναλλαγών με πιστωτικές κάρτες σε ένα ανοιχτό δίκτυο όπως είναι το Internet*. Οι υπηρεσίες που προσφέρει η συγκεκριμένη προδιαγραφή είναι οι εξής:

1. Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ των μελών που συναλλάσσονται.
2. Παρέχει εμπιστευτικότητα με τη χρήση ψηφιακών πιστοποιητικών βάσει του προτύπου X.509v3
3. Παρέχει ιδιωτικότητα περιορίζοντας την κοινοποίηση των πληροφοριών μόνο στους συναλλασσόμενους όταν αυτό είναι απαραίτητο.

Οι φορείς που εμπλέκονται σε ένα σύστημα SET είναι ο κάτοχος της κάρτας (card holder), ο έμπορος (merchant), ο διανομέας (issuer), η τράπεζα υποδοχής (acquirer), η πύλη πληρωμής (payment gateway) και τέλος, η Αρχή Πιστοποίησης (CA). Σύμφωνα με το συγκεκριμένο πρωτόκολλο, τα μέλη που αλληλεπιδρούν έχουν στην κατοχή τους από ένα ζεύγος δημόσιου-ιδιωτικού κλειδιού και ένα πιστοποιητικό δημοσίου κλειδιού αντίστοιχα. [8]

ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ (INTRUSION DETECTION SYSTEMS)

Η ανάπτυξη της τεχνολογίας και η ολοένα αυξανόμενη χρήση των δικτυωμένων υπολογιστικών συστημάτων, έχει ως αποτέλεσμα την αναλογική αύξηση των παράνομων δραστηριοτήτων και εισβολών που λαμβάνουν χώρα καθημερινά. Καθώς η τεχνολογία εξελίσσεται, το ίδιο αλλάζουν και οι κίνδυνοι που ελλοχεύουν. Οι ενέργειες που απαιτούνται για ασφάλεια είναι μια διαδικασία με δυναμικό χαρακτήρα που χρήζει διαρκούς αναθεώρησης. Απαραίτητη προϋπόθεση για την ασφαλέστερη και πιο ομαλή λειτουργία των δικτύων και των

υπολογιστικών συστημάτων είναι η υλοποίηση ενός συστήματος παρακολούθησης και διαχείρισης που θα το εποπτεύει διαρκώς και θα ενημερώνει τους διαχειριστές για τυχόν ύποπτες δραστηριότητες. Η υλοποίηση αυτή, ως μια καλή λύση για την εξασφάλιση της ασφάλειας, ονομάζεται **Σύστημα Ανίχνευσης Εισβολών** (Intrusion Detection Systems, IDS). Πρόκειται για ένα λογισμικό που ελέγχει την κίνηση στο υπολογιστικό σύστημα και παρακολουθεί τις λειτουργίες που επιτελούνται με συγκεκριμένα εργαλεία και μηχανισμούς. Σε περίπτωση που το IDS ανιχνεύσει κάποια μη φυσιολογική (ανώμαλη) δραστηριότητα, τότε παρέχει έγκαιρη προειδοποίηση έτσι ώστε να ληφθούν τα κατάλληλα μέτρα για την αποτροπή της. Σε αντίθετη περίπτωση ωστόσο, η επικείμενη επίθεση θα πρέπει να αντιμετωπιστεί από τους διαχειριστές ασφαλείας το συντομότερο δυνατό. Συνοψίζοντας, ένα σύστημα ανίχνευσης εισβολών εξυπηρετεί τρεις βασικές λειτουργίες, την *παρακολούθηση* και την *ανίχνευση* του συστήματος που εποπτεύει (στην πιο απλή του μορφή, αυτό γίνεται αναλύοντας τα αρχεία καταγραφής και ελέγχου του συστήματος, δηλαδή τα log files και τα audit files) και την *ανταπόκριση* σε ύποπτες, μη εξουσιοδοτημένες δραστηριότητες.

Σε ευρύτερα πλαίσια, υπάρχουν τρεις *μηχανισμοί* λειτουργίας των συστημάτων ανίχνευσης εισβολών. Ο πρώτος είναι ο μηχανισμός με ανίχνευση ανωμαλιών ή κακής συμπεριφοράς (anomaly or behavior based detection), ο μηχανισμός αυτός στηρίζεται στην ύπαρξη ενός μοτίβου συμπεριφοράς που αποκλίνει από το φυσιολογικό. Αν δηλαδή παρατηρηθεί στο σύστημα κάποια συμπεριφορά που δεν συνάδει με την φυσιολογική, τότε αυτή εκλαμβάνεται ως επίθεση. Για την ακρίβεια, κατά τον μηχανισμό αυτόν, οποιαδήποτε μη φυσιολογική συμπεριφορά ανιχνεύεται από το σύστημα ως επίθεση. Ο δεύτερος μηχανισμός είναι με ανίχνευση λανθασμένης χρήσης ή ανίχνευσης υπογραφής (misuse or signature detection). Στην περίπτωση αυτή, υπάρχουν κάποιες προκαθορισμένες, μη αποδεκτές ενέργειες, που ονομάζονται πρότυπα ή υπογραφές οι οποίες όταν γίνουν αντιληπτές από το σύστημα αναγνωρίζονται και αντιμετωπίζονται όπως μια επίθεση. Οι δύο προαναφερθέντες μηχανισμοί βασίζουν την λειτουργία τους στην δημιουργία μιας λίστας που θα προκαθορίζει ποιές συμπεριφορές θα πρέπει να θεωρούνται φυσιολογικές και ποιές ενέργειες θα πρέπει να αποκλείονται. Φυσικά στην πράξη είναι δύσκολο να προσδιοριστεί επαρκώς μια τέτοια λίστα, για τον λόγο αυτό αναπτύχθηκε ένα πιο εύχρηστο μοντέλο του οποίου η λειτουργία στηρίζεται στον τρόπο με τον οποίο γίνεται η συλλογή της πληροφορίας. Αυτός είναι και ο πιο κοινός τρόπος κατηγοριοποίησης των συστημάτων ανίχνευσης εισβολών Με βάση λοιπόν την πηγή συλλογής των πληροφοριών, τα IDS μπορούν να ταξινομηθούν ως ακολούθως: [54]

1. Host-Based IDS
2. Network-Based IDS
3. Application-Based IDS

<u>Host-Based IDS (HIDS)</u>

Λειτουργούν με βάσει τις πληροφορίες που συλλέγονται από ένα μεμονωμένο υπολογιστικό σύστημα. Συγκεκριμένα, παρακολουθεί και αναλύει με ακρίβεια και αξιοπιστία την κίνηση που διέρχεται απο ένα συγκεκριμένο κόμβο (host) και μπορεί να προσδιορίσει ποιες διεργασίες και ποιοι χρήστες εμπλέκονται σε μια επίθεση του λειτουργικού συστήματος. Τα host-based συστήματα έχουν τη δυνατότητα να αντιληφθούν έγκαιρα μια απόπειρα επίθεσης καθώς έχουν άμεση πρόσβαση και δυνατότητα παρακολούθησης των αρχείων δεδομένων (data files) και των διεργασιών του συστήματος που συνήθως αποτελούν κύριο στόχο των επιτήδειων. Για την ακρίβεια, δύο είναι οι πηγές άντλησης πληροφοριών των συστημάτων ανίχνευσης επιθέσεων

αυτής της κατηγορίας, τα ίχνη ελέγχου του λειτουργικού συστήματος (audit trails) και τα αρχεία καταγραφής (system logs) [53]. Τα host-based IDS είναι εξαιρετικά αποτελεσματικά στην ανάλυση δικτυακών επιθέσεων καθώς μπορούν να προσδιορίσουν τις ενέργειες που πραγματοποίησε ο εισβολέας, ποιες εντολές εκτέλεσε και ποια αρχεία έχει προσπελάσει [55]. Επιπλέον, κάποια HIDS αντιδρούν μόνο όταν λαμβάνει χώρα κάποιο συμβάν, ενώ κάποια άλλα αντιλαμβάνονται την αύξηση της κίνησης σε ένα συγκεκριμένο κόμβο του δικτύου όπου το HIDS είναι εγκατεστημένο και παρέχουν συναγερμό σε πραγματικό χρόνο. Βασικό πλεονέκτημα των συστημάτων ανίχνευσης αυτού του τύπου είναι το γεγονός ότι υπάρχει δυνατότητα λειτουργίας ακόμη και σε περίπτωση που η δικτυακή κίνηση είναι κρυπτογραφημένη. Με την παρακολούθηση που πραγματοποιούν στους τοπικούς κόμβους έχουν επίσης την δυνατότητα να εντοπίσουν επιθέσεις που τα δικτυακά IDS, δεν μπορούν. [56]

Network-Based IDS (NIDS)

Η πλειοψηφία των εμπορικών συστημάτων ανίχνευσης εισβολών ανήκουν σε αυτή την κατηγορία. Τα συστήματα ανίχνευσης εισβολών δικτύου ανιχνεύουν επιθέσεις αναλύοντας τα πακέτα που διακινούνται σε όλο το δίκτυο και όχι μεμονωμένα σε έναν κόμβο όπως οι HIDS. Εγκαθίστανται σε διάφορα σημεία στο δίκτυο και μόλις ανιχνεύσουν κάποια ύποπτη ή ασυνήθιστη κίνηση την αναφέρουν στον κεντρικό σταθμό διαχείρισης. Οι NIDS έχουν την δυνατότητα να λειτουργούν χωρίς να γίνονται αντιληπτοί έτσι ώστε οι εισβολείς να δυσκολεύονται να εντοπίσουν την παρουσία αλλά και την τοποθεσία τους. [53] Τα NIDS έχουν μια βάση δεδομένων στην οποία βρίσκονται αποθηκευμένες υπογραφές , δηλαδή μοτίβα από επιθέσεις που έχουν λάβει χώρα στο παρελθόν. Έτσι, αν κάποιο NIDS ανιχνεύσει κάποια ύποπτη κίνηση πακέτου στο δίκτυο, συγκρίνει το περιεχόμενό του με το περιεχόμενο της βάσης και αν υπάρχει ταυτοποίηση σημαίνει ότι μια νέα επίθεση βρίσκεται σε εξέλιξη και θα πρέπει να αποτραπεί [57] . Στη συνέχεια δημιουργείται προειδοποίηση (alert) η οποία μεταβιβάζεται στον διαχειριστή του δικτύου ώστε να προβεί στις απαραίτητες ενέργειες.

Application-Based IDS (AIDS)

Τα συστήματα ανίχνευσης επιθέσεων αυτής της κατηγορίας, θεωρούνται ως υποσύνολο των συστημάτων ανίχνευσης επιθέσεων κόμβων HIDS που αναλύσαμε προηγουμένως και η λειτουργία τους στηρίζεται στην ανάλυση των συμβάντων που πραγματοποιούνται εντός μιας εφαρμογής λογισμικού. Σε αυτή την κατηγορία, οι πληροφορίες αντλούνται αναλύοντας τα αρχεία καταγραφής (log files) των εφαρμογών. Χαρακτηριστικό των AIDS είναι ότι η ύποπτη συμπεριφορά προέρχεται από εξουσιοδοτημένους χρήστες που υπερβαίνουν τα δικαιώματά τους [54].

ΣΥΣΤΗΜΑΤΑ ΠΡΟΛΗΨΗΣ ΕΙΣΒΟΛΩΝ (INTRUSION PREVENTION SYSTEMS)

Όπως έγινε αντιληπτό, τα συστήματα ανίχνευσης εισβολών αποτελούν τον ακρογωνιαίο λίθο για την ασφάλεια των σύγχρονων δικτύων και υπολογιστικών συστημάτων. Η λειτουργία τους, ωστόσο, περιορίζεται στην ανίχνευση των πιθανών εισβολών και στην ενημέρωση του διαχειριστή του δικτύου, ο οποίος στη συνέχεια θα κρίνει ποιες ενέργειες θα πρέπει να ακολουθηθούν ανάλογα με την κρισιμότητα του συμβάντος. Η διαδικασία αυτή όμως απαιτεί χρόνο κατά τη διάρκεια του οποίου υπάρχει η πιθανότητα πρόκλησης σοβαρής βλάβης στο

σύστημα από επικείμενη εισβολή. Το πρόβλημα αυτό αντιμετωπίζει ένα νέο μοντέλο συστήματος ανίχνευσης εισβολής και ονομάζεται Σύστημα Πρόληψης Εισβολής (Intrusion Prevention Systems). Το μοντέλο αυτό, φέρει τις ίδιες λειτουργίες με τα κλασσικά IDS (δηλαδή την ανίχνευση και την αναφορά συμβάντος) και επιπλέον παρέχει την δυνατότητα πρόληψης των πιθανών επιθέσεων. Η πρόληψη μπορεί να συμβεί με δύο τρόπους, είτε με άμεση αντίδραση όπου γίνεται αναδρομολόγηση των πακέτων που ανήκουν στην δικτυακή κίνηση της επίθεσης, είτε έμμεση, όπου το IPS δίνει εντολή σε άλλα συστήματα (πχ firewalls) να προβούν στις απαραίτητες ενέργειες. [1]

HONEYPOTS

Ένα honeypot αποτελεί ένα πόρο πληροφοριακού συστήματος του οποίου η αξία έγκειται στο γεγονός της μη εξουσιοδοτημένης, έκνομης ή διακινδυνευμένης χρήσης του. Πρόκειται για ένα ειδικά διαμορφωμένο σύστημα που λειτουργεί παθητικά ,του οποίου σκοπός είναι να δελεάζει και να προσελκύει πιθανούς εισβολείς και να τους προτρέπει να επιτεθούν σε αυτό κρατώντας τους μακριά από κρίσιμα συστήματα. Τα honeypots είναι κατασκευασμένα με τέτοιο τρόπο ώστε να μοιάζουν με πραγματικά πληροφοριακά συστήματα τα οποία φαίνεται ότι περιέχουν πολύτιμες πληροφορίες που όμως δεν θα προσπέλαζε κάποιος εξουσιοδοτημένος χρήστης . Για αυτόν τον λόγο, κάθε είσοδος σε ένα τέτοιο σύστημα δείχνει ύποπτη. Τα honeypots είναι εξοπλισμένα με συστήματα παρακολούθησης και αρχεία καταγραφής συμβάντων και κάθε επίθεση σε αυτό φαινομενικά είναι επιτυχής. Με αυτόν τον τρόπο, συλλέγονται χρήσιμες πληροφορίες για τις ενέργειες που πραγματοποιεί και τις τεχνικές που χρησιμοποιεί κάποιος εισβολέας για να διεισδύσει, εξάγονται χρήσιμα συμπεράσματα που αφορούν νέους τύπους επιθέσεων (πχ zero day exploits) και καθίσταται ευκολότερος ο εντοπισμός του. Αξίζει να σημειωθεί, ότι τα honeypots δεν λειτουργούν ως ασπίδα προστασίας έναντι των πραγματικών υπολογιστικών συστημάτων αλλά χρησιμοποιούνται ως ένα μέσο παροχής γνώσεων σε ότι αφορά τους εισβολείς, τις επιθέσεις και την αντιμετώπισή τους. Επίσης συντελούν στην γνωστοποίηση και διόρθωση ευπαθειών σε πραγματικά συστήματα. Τα honeypots μπορούν να ταξινομηθούν είτε ανάλογα με τον βαθμό αλληλεπίδρασής τους με τον επιτιθέμενο ή το κακόβουλο λογισμικό είτε ανάλογα με τον σκοπό τους. Ανάλογα με τον βαθμό αλληλεπίδρασης, χωρίζονται στις εξής τρεις κατηγορίες ως ακολούθως : [12][58][59]

1. Honeypots χαμηλής αλληλεπίδρασης
2. Honeypots υψηλής αλληλεπίδρασης
3. Honeypots μεσαίας αλληλεπίδρασης

Σύμφωνα με τον Lance Spitzner, ανάλογα με τον σκοπό τους κατατάσσονται ως εξής : [59]

1. Στα honeypots που χρησιμεύουν στην έρευνα
2. Στα honeypots που χρησιμεύουν στην παραγωγή

<u>Honeypots χαμηλής αλληλεπίδρασης</u>

Τα honeypots χαμηλής αλληλεπίδρασης δεν αποτελούν λειτουργικό σύστημα αλλά προσομοιώνουν ένα τμήμα λειτουργικού συστήματος ή κάποιας δικτυακής υπηρεσίας με σκοπό να προσελκύσουν το ενδιαφέρον των επιτήδειων, ενώ την ίδια στιγμή καταγράφει τις ενέργειες που πραγματοποιούνται. Ο εισβολέας δεν έχει πρόσβαση σε ολόκληρο το σύστημα και κατά συνέπεια δεν μπορεί να το χρησιμοποιήσει για περαιτέρω δικτυακές επιθέσεις. Τα honeypots χαμηλής αλληλεπίδρασης έχουν περιορισμένες δυνατότητες, μπορούν ωστόσο να χρησιμοποιηθούν για συλλογή πληροφοριών σχετικά με τις δραστηριότητες των αποστολέων ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (spammers), των worms αλλά και για την λήψη αντίμετρων ενάντια σε αυτά. Τα συγκεκριμένα honeypots είναι απλά στην εφαρμογή και στην συντήρησή τους και διατρέχουν χαμηλό επίπεδο ρίσκου εφόσον οι εισβολείς δεν έχουν πλήρη πρόσβαση στους υπολογιστικούς πόρους. Χαρακτηριστικό παράδειγμα των honeypots αυτής της κατηγορίας είναι τα *honeyd*. [58][60]

Honeypots υψηλής αλληλεπίδρασης

Τα honeypots υψηλής αλληλεπίδρασης, αποτελούν την πιο προηγμένη κατηγορία honeypot. Παρέχουν μια αρκετά πιο ρεαλιστική εικόνα ενός λειτουργικού συστήματος και συλλέγεται μεγαλύτερη ποσότητα πληροφοριών από τις επιθέσεις που πραγματοποιούνται, καθώς όλες οι ενέργειες των επιτιθέμενων καταγράφονται και αναλύονται ενδελεχώς. Αυτό το είδος των honeypot είναι αρκετά περίπλοκο και χρονοβόρο στην υλοποίησή του. Επίσης, το ρίσκο που ενέχει η χρήση τους είναι αρκετά μεγαλύτερο εφόσον ο εισβολέας έχει πλήρη πρόσβαση στους πόρους του συστήματος, επομένως έχει και την δυνατότητα να επεκτείνει την επίθεσή του και σε άλλα πληροφοριακά συστήματα. Ακριβώς επειδή οι εισβολείς έχουν στη διάθεσή τους αφθονία πόρων, οι διαχειριστές του δικτύου θα πρέπει συνεχώς να επιτηρούν τις δραστηριότητες που εκτελούνται για να βεβαιώνονται ότι δεν θα δημιουργηθεί κάποιος σοβαρός κίνδυνος ή κενό στην ασφάλεια του συστήματος. Χαρακτηριστικό παράδειγμα αυτού του τύπου των honeypot είναι τα honeynets τα οποία χρησιμοποιούνται κυρίως για ερευνητικούς σκοπούς. [58][60]

Honeypots μεσαίας αλληλεπίδρασης

Τα συγκεκριμένα honeypots μπορούν διαφορετικά να ονομαστούν και μεικτής αλληλεπίδρασης καθώς συνδυάζουν στοιχεία από τα δύο προηγούμενα είδη. Ομοίως με τα χαμηλής αλληλεπίδρασης honeypot, δεν αποτελούν λειτουργικό σύστημα, αλλά οι υπηρεσίες που προσομοιώνουν είναι τεχνικά πιο περίπλοκες και αληθοφανείς. Έτσι ο επιτιθέμενος έχει μεγαλύτερο βαθμό αλληλεπίδρασης με το σύστημα, θεωρώντας πως το πεδίο δράσης του είναι ένα πραγματικό λειτουργικό σύστημα. Κατά συνέπεια υπάρχει η πιθανότητα να λάβουν χώρα πιο σύνθετες επιθέσεις οι οποίες καταγράφονται και αναλύονται και στη συνέχεια εξάγονται συμπεράσματα από τους διαχειριστές για την καλύτερη και αποδοτικότερη προστασία του δικτύου. Χαρακτηριστικό παράδειγμα αυτού του τύπου των honeypot είναι τα *honeytraps*. [58][60]

Honeypots για ερευνητικούς σκοπούς

Ένα honeypot που χρησιμοποιείται για έρευνα είναι σχεδιασμένο με τρόπο τέτοιο ώστε να συλλέγει πληροφορίες που αφορούν σε νέες απειλές, κίνητρα και τεχνικές της blackhat κοινότητας. Οι επιτιθέμενοι παρακολουθούνται την ώρα της δράσης τους και κάθε ενέργειά τους καταγράφεται έτσι ώστε οι διαχειριστές του δικτύου να είναι αργότερα σε θέση να αναλύσουν την συμπεριφορά και τις μεθόδους που έχουν χρησιμοποιηθεί. Τα honeypots αυτού του είδους, βρίσκουν εφαρμογή κυρίως σε πανεπιστημιακές και στρατιωτικές δομές και κυβερνητικούς οργανισμούς. Βασικό τους μειονέκτημα αποτελεί το γεγονός ότι είναι δύσκολα στην χρήση και στη συντήρησή τους και δεσμεύουν μεγάλο όγκο δεδομένων. Ωστόσο είναι ένα ισχυρό εργαλείο που συνεισφέρει στην ανάπτυξη εγκληματολογικών γνώσεων και δεξιοτήτων αλλά και στην μελέτη των κυβερνοαπειλών. [60]

Honeypots παραγωγής

Σκοπός της συγκεκριμένης κατηγορίας honeypot είναι να προστατεύσουν το δίκτυο στο οποίο είναι εγκατεστημένα. Οι απαιτήσεις σε λειτουργικότητα είναι χαμηλότερες σε σύγκριση με τα ερευνητικά, γι αυτό και η κατασκευή αλλά και η εφαρμογή τους είναι πιο εύκολη. Τα honeypots παραγωγής είναι σε θέση να αναγνωρίζουν τις τεχνικές των επιθέσεων που εξαπολύονται, παρέχουν όμως λιγότερες πληροφορίες για τους εισβολείς. Οι πληροφορίες αυτές περιορίζονται στο σύστημα από το οποίο προέρχεται μια επίθεση και τις ευπάθειες που εκμεταλλεύτηκαν μέχρι να την ολοκληρώσουν. Δεν αποκαλύπτονται όμως πληροφορίες όσον αφορά στην ταυτότητα του εισβολέα ή τα εργαλεία που χρησιμοποιήθηκαν για να την επιτύχουν. Τα honeypots παραγωγής αντικατοπτρίζουν ένα δίκτυο παραγωγής μιας εταιρείας με σκοπό να δελεάσουν τον επιτιθέμενο και να αλληλεπιδράσει με αυτό. Από αυτή την αλληλεπίδραση γνωστοποιούνται ευπάθειες που πιθανόν να υπάρχουν στο δίκτυο. Εφόσον οι διαχειριστές ενημερωθούν σχετικά με τις ευπάθειες μπορούν με κατάλληλες ενέργειες να παρέχουν έγκαιρη προειδοποίηση για επερχόμενη επίθεση, να μειώσουν το ρίσκο μελλοντικών εισβολών και να χτίσουν καλύτερες γραμμές άμυνας για μεταγενέστερες απειλές. Αξίζει να σημειωθεί ότι τα honeypots παραγωγής δεν λειτουργούν ως μηχανισμοί πρόληψης. Η αποδοτικότερη εφαρμογή τους προβλέπει τον συνδυασμό των honeypots με κάποιο IDS ή firewall. [60]

ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ (FIREWALLS)

Τα τείχη προστασίας αποτελούν έναν μηχανισμό προστασίας που μπορεί να είναι υλικό, λογισμικό ή συνδυασμός και των δύο. Σκοπός του είναι να παρακολουθεί και να φιλτράρει πακέτα από την δικτυακή κίνηση που επιχειρούν να εισέλθουν στο προστατευόμενο ιδιωτικό δίκτυο, ή να αποχωρήσουν από αυτό. Αποτελεί ένα εργαλείο που διαχωρίζει το προστατευμένο

δίκτυο, μέρος αυτού, ή τον υπολογιστή του χρήστη από το «μη προστατευμένο» δίκτυο, όπως είναι για παράδειγμα το internet. Τα firewalls στηρίζουν την λειτουργία τους σε τρείς βασικές αρχές: [1][8][15]

1. Όλη η δικτυακή κίνηση, από το προστατευμένο ιδιωτικό δίκτυο προς το Internet αλλά και αντίστροφα, θα πρέπει να διέρχεται από το firewall
2. Μόνο η δικτυακή κίνηση που είναι εξουσιοδοτημένη από την πολιτική ασφαλείας του firewall επιτρέπεται να διέλθει από αυτό.
3. Το ίδιο το τείχος προστασίας θα πρέπει να είναι αδύνατο να διαπεραστεί.

Τα firewall ταξινομούνται στις εξής τρείς κατηγορίες, ακολουθεί σύντομη περιγραφή τους: [8]

1. Packet Filters (Φιλτράρισμα πακέτων)
2. Circuit-level Gateways (Πύλες επιπέδου κυκλώματος)
3. Application-level Gateways (Πύλες επιπέδου εφαρμογής)

Packet Filter (Φιλτράρισμα πακέτων)

Αυτό το είδος firewall εξετάζει τα εισερχόμενα και εξερχόμενα πακέτα και με βάση ένα σύνολο κανόνων που εφαρμόζονται και καθορίζει αν τα εν λόγω πακέτα θα προωθηθούν ή θα απορρίφθούν. Οι κανόνες φιλτραρίσματος που εφαρμόζονται, στηρίζονται στις πληροφορίες που περιέχονται στις κεφαλίδες (headers) των πακέτων που διακινούνται (IP, TCP, UDP). Οι πληροφορίες αυτές μπορεί να είναι:

- Η IP διεύθυνση της πηγής
- Η IP διεύθυνση του προορισμού
- Ο TCP ή UDP αριθμός θύρας πηγής και προορισμού
- Το πεδίο πρωτοκόλλου (το πρωτόκολλο που χρησιμοποιείται)

Για να αποφασιστεί από το firewall αν ένα πακέτο θα προωθηθεί, αν θα αναβληθεί η μετάδοση του για αργότερα ή αν θα απορριφθεί, συγκρίνεται το περιεχόμενο της κεφαλίδας του με την λίστα κανόνων του firewall ώσπου να βρεθεί κάποιος κανόνας να ταιριάζει. Ανάλογα με τον κανόνα εκτελείται και η αντίστοιχη ενέργεια.

Circuit-level Gateways (Πύλες επιπέδου κυκλώματος)

Τα firewalls αυτής της κατηγορίας δεν επιτρέπουν την δημιουργία απευθείας συνδέσεων ανάμεσα σε έναν κόμβο εντός του προστατευμένου δικτύου και ενός εξωτερικού κόμβου. Στην περίπτωση αυτή δημιουργούνται δύο ξεχωριστές συνδέσεις. Η μια σύνδεση είναι μεταξύ της πύλης (δηλαδή του firewall) και του εσωτερικού κόμβου και η δεύτερη σύνδεση είναι μεταξύ της πύλης και του εξωτερικού κόμβου. Εφόσον οι δύο συνδέσεις έχουν εδραιωθεί επιτυχώς, η πύλη αναλαμβάνει τον ρόλο του αναμεταδότη προωθώντας τα τμήματα των πακέτων που λαμβάνει, από τη μια σύνδεση στην άλλη χωρίς να εξετάζει το περιεχόμενό τους.

Application-level Gateways (Πύλες επιπέδου εφαρμογής)

Οι πύλες επιπέδου εφαρμογής, γνωστές και ως proxy servers (διακομιστές μεσολάβησης), είναι προϊόν λογισμικού που λειτουργεί ως αναμεταδότης της κίνησης στο επίπεδο εφαρμογής. Η λειτουργία του θυμίζει αρκετά τις πύλες επιπέδου κυκλώματος, ωστόσο υπάρχουν αρκετές διαφορές. Ο διακομιστής μεσολάβησης είναι μια υπηρεσία που παρεμβάλλεται μεταξύ πελάτη και εξυπηρετητή και σκοπός του είναι ο έλεγχος της επικοινωνίας, η οποία περιορίζεται σε ανταλλαγή πακέτων μεταξύ έμπιστων υπηρεσιών του δικτύου. Ένας proxy server μπορεί να έχει δυο λειτουργίες, να είναι δηλαδή πελάτης και εξυπηρετητής ταυτόχρονα. Όταν λοιπόν ο πελάτης (για παράδειγμα χρήστης εντός του προστατευμένου δικτύου) ζητήσει πρόσβαση σε κάποια υπηρεσία εκτός δικτύου, αποστέλλεται αίτηση στον proxy server. Ο proxy server με την σειρά του, ζητάει τα απαραίτητα στοιχεία ώστε να αυθεντικοποιήσει τον πελάτη. Μόλις ολοκληρωθεί η διαδικασία της αυθεντικοποίησης ο proxy server ξεκινάει να αναμεταδίδει τα τμήματα TCP στα οποία περιέχονται τα δεδομένα των δύο άκρων (πελάτη-διακομιστή).

Αξίζει να επισημανθεί ότι ο proxy server πριν ξεκινήσει την μετάδοση των τμημάτων αντικαθιστά την IP διεύθυνση του πελάτη με την δική του (Host IP address hiding). Με τον τρόπο αυτόν η ταυτότητα του πελάτη δεν γνωστοποιείται στον μη ασφαλή χώρο και αποφεύγονται επιθέσεις spoofing. Αλλαγή γίνεται και στον αριθμό των θυρών (port address translation, PAT) πριν την έξοδο των δεδομένων των δεδομένων από τον ασφαλή χώρο. Ωστόσο οι πραγματικοί αριθμοί θυρών είναι αποθηκευμένοι σε πίνακα αντιστοίχισης, έτσι κατά την είσοδο δεδομένων στον ασφαλή χώρο, επανατοποθετούνται οι πραγματικές τιμές στην κεφαλίδα των πακέτων. [15]

ΚΕΦΑΛΑΙΟ 4 ΠΡΟΣΟΜΟΙΩΣΗ ΕΠΙΘΕΣΗΣ SQL INJECTION

ΕΙΣΑΓΩΓΗ

Με την ταχεία εξάπλωση του διαδικτύου, υπάρχει σήμερα πληθώρα διαδικτυακών εφαρμογών και ιστοσελίδων που εξυπηρετούν άμεσα τις καθημερινές ανάγκες του χρήστη. Οι εφαρμογές αυτές, μπορεί να αφορούν σε τραπεζικές συναλλαγές, ηλεκτρονικό εμπόριο, μέσα κοινωνικής δικτύωσης , ηλεκτρονικές ψηφοφορίες και πολλές ακόμη κατηγορίες. Οι διαδικτυακές εφαρμογές που παρέχουν δυναμικές ιστοσελίδες (οι σελίδες δηλαδή που παρέχουν αλληλεπίδραση με τον χρήστη), στηρίζονται στην αρχιτεκτονική πελάτη-εξυπηρετητή και η μεταξύ τους αλληλεπίδραση πραγματοποιείται με την χρήση του πρωτοκόλλου HTTP. Όταν ένας χρήστης επιθυμεί πρόσβαση σε μια διαδικτυακή εφαρμογή, αποστέλλει αίτηση σύνδεσης μέσω του φυλλομετράτε του (web browser) στον εκάστοτε διακομιστή. Ο διακομιστής στη συνέχεια, εφόσον εγκαθιδρύσει την σύνδεση, επιστρέφει στον πελάτη τα επιθυμητά δεδομένα, συνήθως σε μορφή HTML έτσι ώστε να είναι κατανοητά από τον χρήστη. Σε πολλές περιπτώσεις, οι διαδικτυακές εφαρμογές χρειάζεται να επικοινωνούν με βάσεις δεδομένων μέσω του διακομιστή ούτως ώστε να αντλήσουν τις ζητούμενες πληροφορίες για λογαριασμό του χρήστη. Για λόγους μεγαλύτερης ευελιξίας συνήθως μαζί με την HTML χρησιμοποιούνται και άλλες γλώσσες προγραμματισμού κατάλληλες για την δημιουργία δυναμικών σελίδων αλλά και για την συλλογή πληροφοριών από τις βάσεις δεδομένων με την χρήση ερωτημάτων. Μια τέτοια γλώσσα είναι για παράδειγμα η PHP, είναι scripting γλώσσα και εκτελείται από πλευράς διακομιστή.

Οι περισσότερες διαδικτυακές εφαρμογές που αλληλεπιδρούν με βάσεις δεδομένων, χρησιμοποιούν φόρμες που διαθέτουν πεδία εισόδου. Σε αυτά τα πεδία, ο χρήστης εισάγει δεδομένα όπως για παράδειγμα τα διαπιστευτήριά του για την είσοδό του σε μια εφαρμογή, ή κάποιο προϊόν για αναζήτηση. Τα δεδομένα που εισάγονται αποστέλλονται στην βάση δεδομένων σε μορφή δυναμικών ερωτημάτων (queries) της γλώσσας SQL (Structured Query Language). Στη συνέχεια, η βάση δεδομένων επεξεργάζεται τα στοιχεία εισόδου και επιστρέφει τις ανάλογες πληροφορίες.

Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν την διαδικασία που περιγράφηκε παραπάνω μεταβάλλοντας τα γνήσια SQL ερωτήματα και εγχέοντας κακόβουλο κώδικα στα πεδία εισόδου. Το γεγονός αυτό, έχει ως αποτέλεσμα οι επιτήδειοι να αποκτούν πρόσβαση στις βάσεις δεδομένων και να έχουν την δυνατότητα να μεταβάλλουν, να διαγράψουν πληροφορίες, ακόμη και να προκαλέσουν διακοπή της λειτουργίας της. Η επίθεση αυτή ονομάζεται SQL injection (επίθεση έγχυσης κώδικα). Στο παρόν κεφάλαιο, πραγματοποιείται προσομοίωση αυτής της επίθεσης σε ιστοσελίδα που δημιουργήθηκε τοπικά για τον σκοπό αυτό. Η ιστοσελίδα θα περιλαμβάνει μια φόρμα εισόδου στην οποία οι χρήστες θα έχουν πρόσβαση

εισάγοντας τα διαπιστευτήριά τους (όνομα χρήστη και κωδικό). Η επίθεση που θα πραγματοποιηθεί αφορά στην απόπειρα εισόδου στην πλατφόρμα χωρίς διαπιστευτήρια.

Θα αναλυθούν τόσο τα βήματα που ακολουθήθηκαν για την κατασκευή της σελίδας, όσο για την διεξαγωγή της επίθεσης. Στη συνέχεια, παρατίθενται πρακτικές βελτιστοποίησης της ασφάλειας του κώδικα της ιστοσελίδας αλλά και θέματα που αφορούν στην ασφάλεια του χρήστη. Ωστόσο, πριν την περιγραφή της υλοποίησης θα παρουσιαστούν τα εργαλεία και οι τεχνολογίες που χρησιμοποιήθηκαν τα οποία είναι τα εξής:

1. Notepad++
2. Xampp
3. Apache HTTP εξυπηρετητής
4. MySql
5. PHP
6. HTML-CSS
7. PhpMyAdmin

Notepad++

Είναι ένα δωρεάν πρόγραμμα επεξεργασίας πηγαίου κώδικα για το λειτουργικό σύστημα των Microsoft Windows. Το Notepad++ παρέχει την δυνατότητα παράλληλης επεξεργασίας πολλών αρχείων, ανοιγμένων σε καρτέλες σε ένα ενιαίο παράθυρο. [1]

XAMPP

Το όνομά του προέρχεται από το παρακάτω ακρωνύμιο:

X (Cross- Platform)

Apache

MySQL

PHP

Perl

Το XAMPP είναι ένα δωρεάν λογισμικό ανοιχτού κώδικα που επιτρέπει την ρύθμιση ενός τοπικού περιβάλλοντος διακομιστή ιστού, στον υπολογιστή του χρήστη. Επί της ουσίας, δίνει την δυνατότητα σε έναν οικιακό υπολογιστή να λειτουργήσει ως web server υποστηρίζοντας την ανάπτυξη τοπικών ιστοσελίδων. Το XAMPP είναι λογισμικό ανεξάρτητο πλατφόρμας (Cross- Platform) και υπάρχουν διανομές για περιβάλλοντα όπως Microsoft, Linux και OS X. Το συγκεκριμένο εργαλείο αποτελείται από τις τελευταίες εκδόσεις του Apache HTTP server,

της βάσης δεδομένων SQL (συγκεκριμένα MariaDB) και διερμηνευτές των γλωσσών PHP και Perl. [2]

APACHE SERVER

Ο Apache HTTP είναι εξυπηρετητής που διαδραμάτισε καίριο ρόλο για την ανάπτυξη του παγκόσμιου ιστού. Αναπτύσσεται και συντηρείται από μια ανοιχτή κοινότητα προγραμματιστών και υπάρχει πληθώρα διανομών για διαφορετικά λειτουργικά συστήματα. Περιλαμβάνει αρκετά χαρακτηριστικά κάποια από τα οποία ενσωματώνονται ως μονάδες (modules) στον πυρήνα επεκτείνοντας την λειτουργικότητά του. Τέτοια είναι για παράδειγμα τα modules αυθεντικοποίησης (mod_access, mod_auth,) και τα modules για την υποστήριξη των πρωτοκόλλων SSL και TLS (mod_ssl). Είναι από τους δημοφιλέστερους εξυπηρετητές και μπορεί να χρησιμοποιηθεί και σε τοπικά δίκτυα συνεργαζόμενος με συστήματα διαχείρισης βάσεων δεδομένων. [3]

MySql

Είναι ένα, ανοιχτού κώδικα, σύστημα διαχείρισης βάσεων δεδομένων που διανέμεται δωρεάν. Είναι ένα πρόγραμμα, το οποίο μέσω του MySQL εξυπηρετητή παρέχει σε πολλούς χρήστες πρόσβαση σε ένα σύνολο βάσεων δεδομένων. Ο εξυπηρετητής εξασφαλίζει ότι πολλοί χρήστες θα μπορούν να εισέλθουν ταυτόχρονα στο σύστημα και ότι θα τους παρέχεται γρήγορη πρόσβαση. Επίσης, διασφαλίζει το γεγονός ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν δικαίωμα πρόσβασης στο σύστημα. [4]

PHP

Η PHP (Hypertext Preprocessor) είναι , όπως αναφέρθηκε και προηγουμένως, μια γλώσσα προγραμματισμού που εκτελείται από πλευράς διακομιστή. Η PHP χρησιμοποιείται για τον καθορισμό των λειτουργιών που θα εκτελεί η δυναμική ιστοσελίδα, πλαισιωμένη απο την HTML η οποία χρησιμοποιείται για την μορφοποίηση της. Σε αντίθεση με μια απλή HTML σελίδα της οποίας το περιεχόμενο αποστέλλεται απευθείας στον πελάτη, ο κώδικας της PHP σελίδας πρώτα ερμηνεύεται και μετά αποστέλλεται το παραγόμενο αποτέλεσμα. [5]

HTML-CSS

Η HTML (HyperText Markup Language) είναι μια γλώσσα υπερκειμένου που περιγράφει τα αντικείμενα που περιέχονται σε μια ιστοσελίδα, ενώ προσφέρει χαρακτηριστικά που επιτρέπει στους προγραμματιστές να εμπλουτίσουν τις εφαρμογές τους με διαδραστική λειτουργικότητα. Η HTML ορίζει μια κοινή μορφοποίηση για τις ιστοσελίδες η οποία περιλαμβάνει τίτλους

(title), επικεφαλίδες (headings), παραγράφους (paragraphs), λίστες (lists) και πίνακες (tables). Το όνομα του καθενός από αυτά τα στοιχεία περικλείεται μέσα σε σύμβολα (“<” , “>”) που ονομάζονται ετικέτες (tags). Κάθε αρχείο HTML περιέχει το κείμενο της σελίδας και τις ετικέτες που καθορίζουν την δομή, την μορφοποίηση και τους συνδέσμους υπερκειμένων για άλλες σελίδες ή πολυμεσικά αρχεία.

Παρά το γεγονός ότι ο στοιχειώδης καθορισμός της εμφάνισης μιας σελίδας πραγματοποιείται από την HTML, η εφαρμογή, η επεξεργασία και η ενημέρωση της μορφοποίησης γίνεται από τα “αλλεπάλληλα φύλλα στυλ” CSS (Cascading Style Sheets). Το εν λόγω εργαλείο χρησιμοποιείται συνδυαστικά με την HTML για να καθορίσει χαρακτηριστικά όπως χρώματα, στοίχιση, εμφάνιση, διάταξη, γραμματοσειρά κ.α. [6]

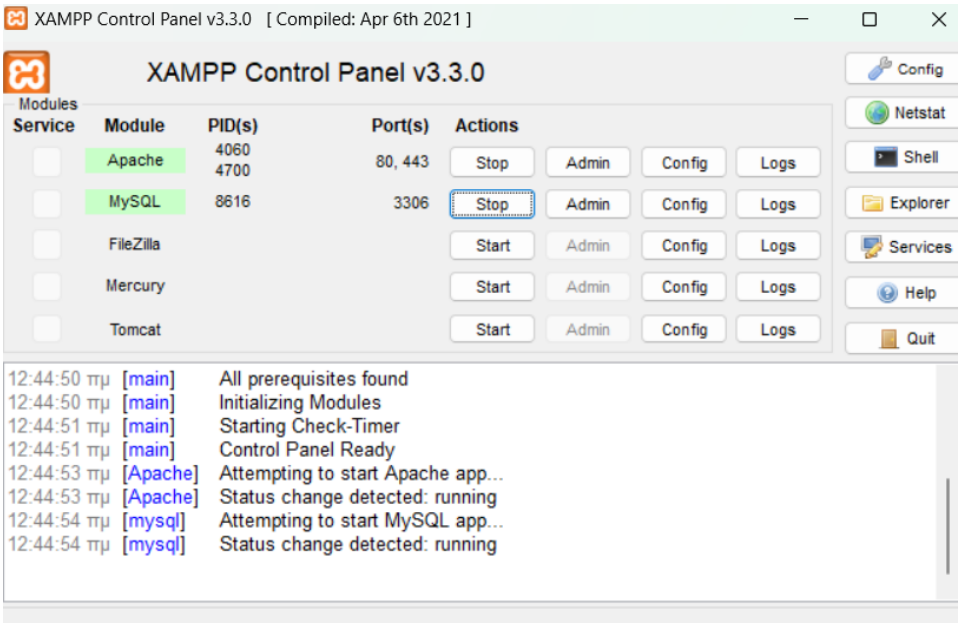
PhpMyAdmin

Είναι ένα δωρεάν και ανοιχτού κώδικα λογισμικό γραμμένο σε γλώσσα PHP που στοχεύει στην διαχείριση βάσεων δεδομένων μέσω ενός προγράμματος περιήγησης. Το εργαλείο PhpMyAdmin παρέχει την δυνατότητα εκτέλεσης διαχειριστικών εργασιών, συμπεριλαμβανομένων της δημιουργίας μιας βάσης δεδομένων, της εκτέλεσης ερωτημάτων (queries) και της προσθήκης λογαριασμών χρηστών. Πιο συγκεκριμένα, μέσω του PhpMyAdmin μπορεί να πραγματοποιηθεί η δημιουργία, η επεξεργασία και η διαγραφή πινάκων, πεδίων, ευρετηρίων, γραμμών και στηλών, καθώς επίσης η εκτέλεση ερωτημάτων SQL, η προσθήκη, επεξεργασία και αφαίρεση λογαριασμών χρηστών και των δικαιωμάτων τους. [7]

ΥΛΟΠΟΙΗΣΗ ΠΡΟΣΟΜΟΙΩΣΗΣ

Η ΒΑΣΗ ΔΕΔΟΜΕΝΩΝ

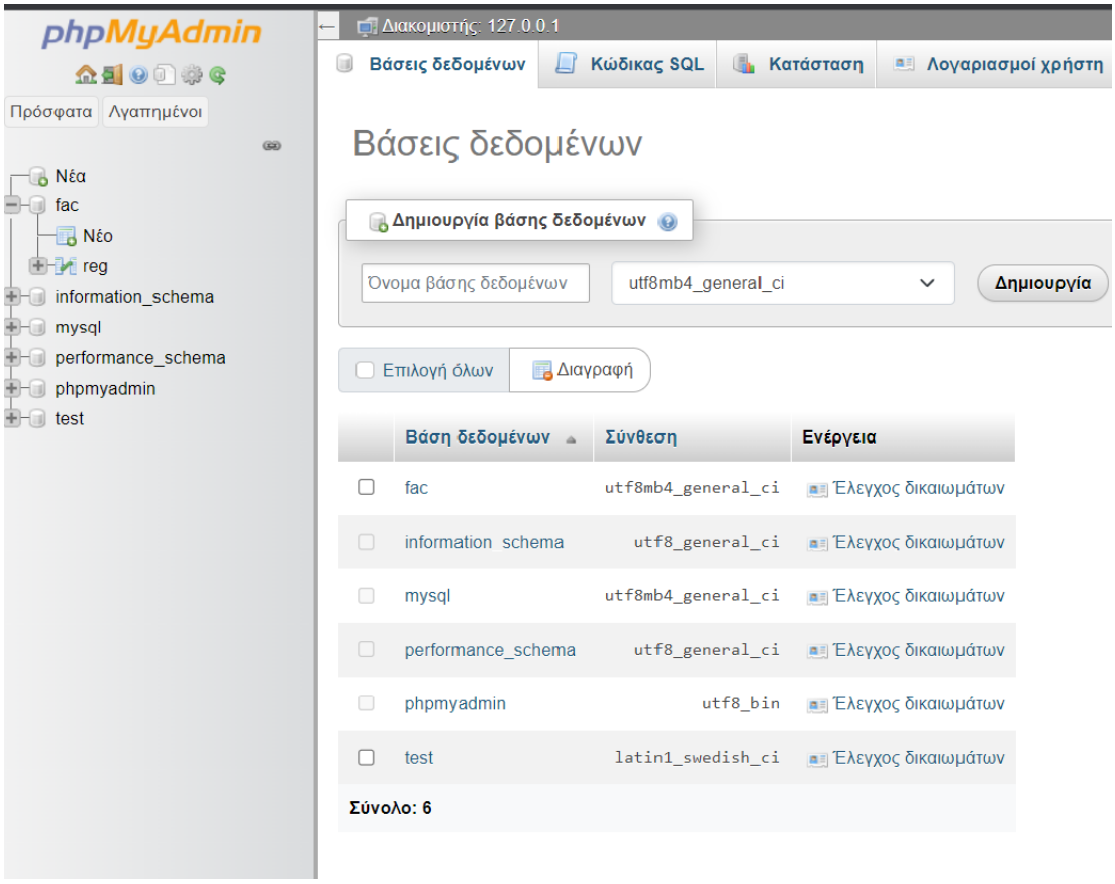
Για να γίνει εφικτή η υλοποίηση της προσομοίωσης και να υπάρχει σύνδεση ανάμεσα στην ιστοσελίδα και στην βάση δεδομένων, θα πρέπει να ενεργοποιήσουμε τους διακομιστές Apache και MySQL πατώντας το start στο πρόγραμμα xampp, όπως φαίνεται και στην παρακάτω εικόνα.



Εικόνα 12 Το περιβάλλον του προγράμματος XAMPP

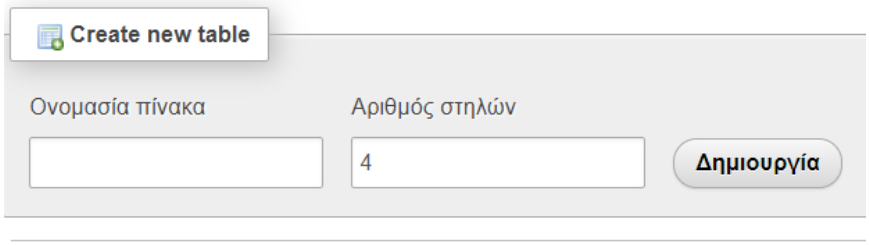
Από τη στιγμή που θα ολοκληρωθεί η εγκατάσταση του xampp στον υπολογιστή, δημιουργείται αυτόματα στον τοπικό δίσκο και ο αντίστοιχος φάκελός του, μέσα στον οποίο περιέχεται ο φάκελος htdocs (C:\xampp\htdocs) . Μέσα στον htdocs δημιουργούμε έναν άλλο φάκελο, στην προκειμένη περίπτωση με όνομα «isi» ο οποίος θα περιέχει τα αρχεία με τον κώδικα της εργασίας με επέκταση .php . Για την συγγραφή του κώδικα χρησιμοποιήθηκε το εργαλείο Notepad++ .

Εφόσον έχει γίνει η εκκίνηση του apache server και του MySql server στο xampp, ανοίγουμε τον περιηγητή και πληκτρολογώντας την διεύθυνση http://localhost/phpmyadmin/index.php?route=/server/databases . Έτσι, γίνεται είσοδος στην εφαρμογή Phpmyadmin όπου μπορούμε πλέον να φτιάξουμε την επιθυμητή βάση δεδομένων με χαρακτηριστικά της επιλογής μας (πίνακες, γραμμές, στήλες κ.α) . Στην εικόνα που ακολουθεί, φαίνεται μια προεπισκόπηση της εφαρμογής Phpmyadmin καθώς και η δυνατότητα δημιουργίας μιας νέας βάσης δεδομένων πληκτρολογώντας το όνομα και πατώντας το κουμπί «Δημιουργία». Ακόμη, στην στήλη αριστερά, βλέπουμε την βάση δεδομένων με όνομα «fac», που έχουμε δημιουργήσει για τις ανάγκες της εργασίας, η οποία περιλαμβάνει τον πίνακα με όνομα « reg» με τα στοιχεία όλων των χρηστών.

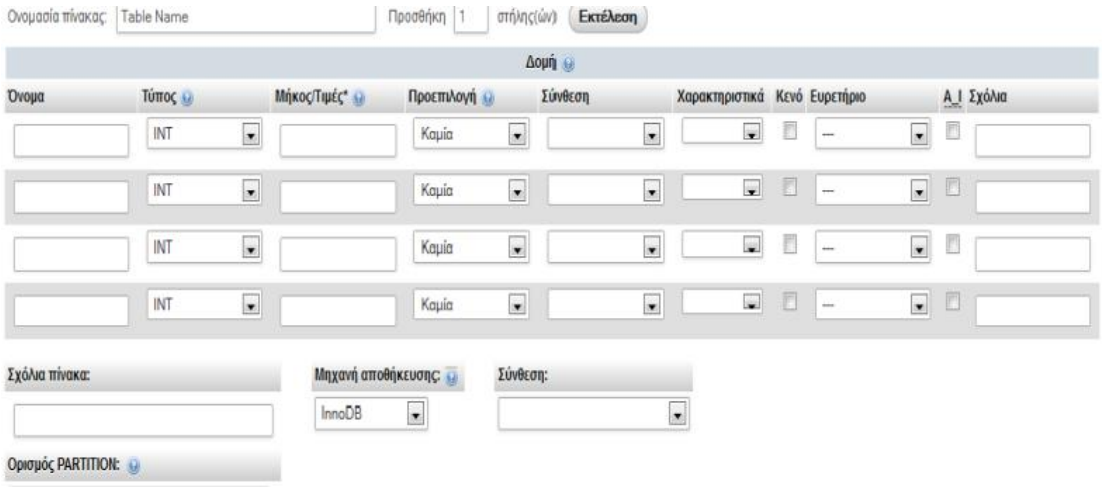


Εικόνα 13 Το περιβάλλον της εφαρμογής phpMyAdmin

Για να δημιουργήσουμε τον πίνακα, πατάμε στο όνομα της βάσης δεδομένων και έπειτα συμπληρώνουμε το όνομα και τον αριθμό στηλών που επιθυμούμε να έχει. Επιλέγουμε για κάθε πεδίο τον τύπο, το μήκος, τη σύνθεση, διαλέγουμε αν το πεδίο θα έχει κενή τιμή (null) ή όχι, αν η τιμή του πεδίου θα αυξάνεται αυτόματα (A_I), αν θα έχει πρωτεύοντα ή μοναδικά κλειδιά ή άλλα ειδικά χαρακτηριστικά. Εφόσον ολοκληρώσουμε αυτή τη διαδικασία, πατάμε το κουμπί «Εκτέλεση» και από την επιλογή «Δομή» μπορούμε να δούμε τον πίνακα που δημιουργήσαμε και να πραγματοποιήσουμε αλλαγές σύμφωνα με τις απαιτήσεις που προκύπτουν. Τα βήματα που περιγράψαμε φαίνονται στις παρακάτω εικόνες.



Εικόνα 14 Δημιουργία Πίνακα στη Βάση Δεδομένων



Εικόνα 15 Πεδία του Πίνακα της Βάσης Δεδομένων

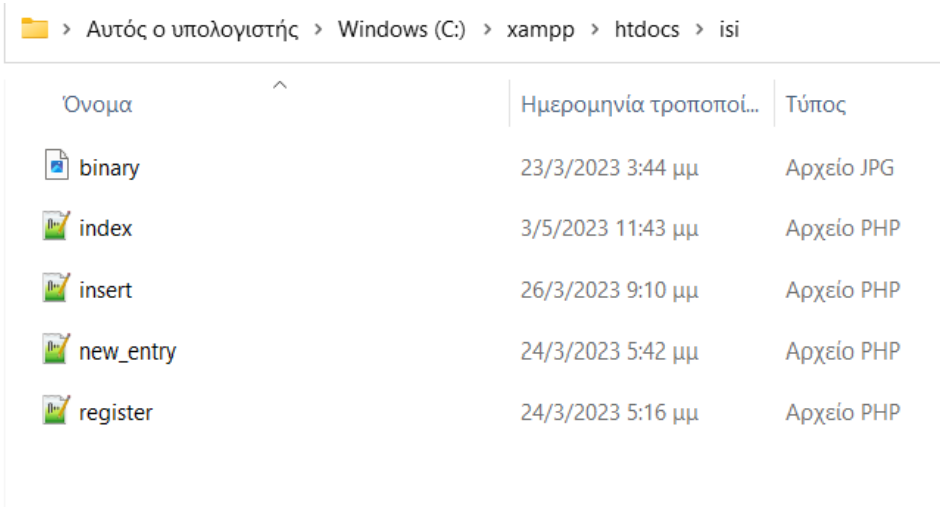
Στην εικόνα που ακολουθεί, φαίνονται τα περιεχόμενα του πίνακα reg. Όταν ένας χρήστης κάνει την εγγραφή του στην πλατφόρμα, συμπληρώνει το όνομα χρήστη (username), τον κωδικό που επιθυμεί (pass), την ημερομηνία γέννησης (dob) και το τηλέφωνό του (tel). Το εργαλείο phpmyadmin μας δίνει την δυνατότητα να τροποποιήσουμε τα στοιχεία ενός πίνακα ή μιας ολόκληρης βάσης δεδομένων (όπως φαίνεται και παρακάτω με τις επιλογές επεξεργασία, αντιγραφή, διαγραφή). Ωστόσο τις ίδιες ενέργειες μπορούμε να τις πραγματοποιήσουμε γράφοντας τις κατάλληλες εντολές σε κώδικα SQL με την επιλογή «Κώδικας SQL» στο επάνω μέρος της σελίδας του phpmyadmin .

		username	pass	dob	tel
☐	Επεξεργασία Αντιγραφή Διαγραφή	lola	123	1999-02-20	1234124
☐	Επεξεργασία Αντιγραφή Διαγραφή	leny	466	1992-08-03	28375
☐	Επεξεργασία Αντιγραφή Διαγραφή	dimitris	729o	1995-02-13	89866
☐	Επεξεργασία Αντιγραφή Διαγραφή	mpam	987	1997-01-12	77576
☐	Επεξεργασία Αντιγραφή Διαγραφή	dan	kjh9f0wr8f	2000-07-09	41160
☐	Επεξεργασία Αντιγραφή Διαγραφή	anna	myr	1996-04-06	87987
☐	Επεξεργασία Αντιγραφή Διαγραφή	candis	test123	1992-01-01	46098

Εικόνα 16 Περιεχόμενα του Πίνακα της Βάσης Δεδομένων

Η ΙΣΤΟΣΕΛΙΔΑ

Πριν ξεκινήσουμε την περιγραφή της σελίδας και την προσομοίωση της επίθεσης, παρακάτω παρατίθενται όλα τα αρχεία που χρησιμοποιήθηκαν για την δημιουργία και την μορφοποίηση της.

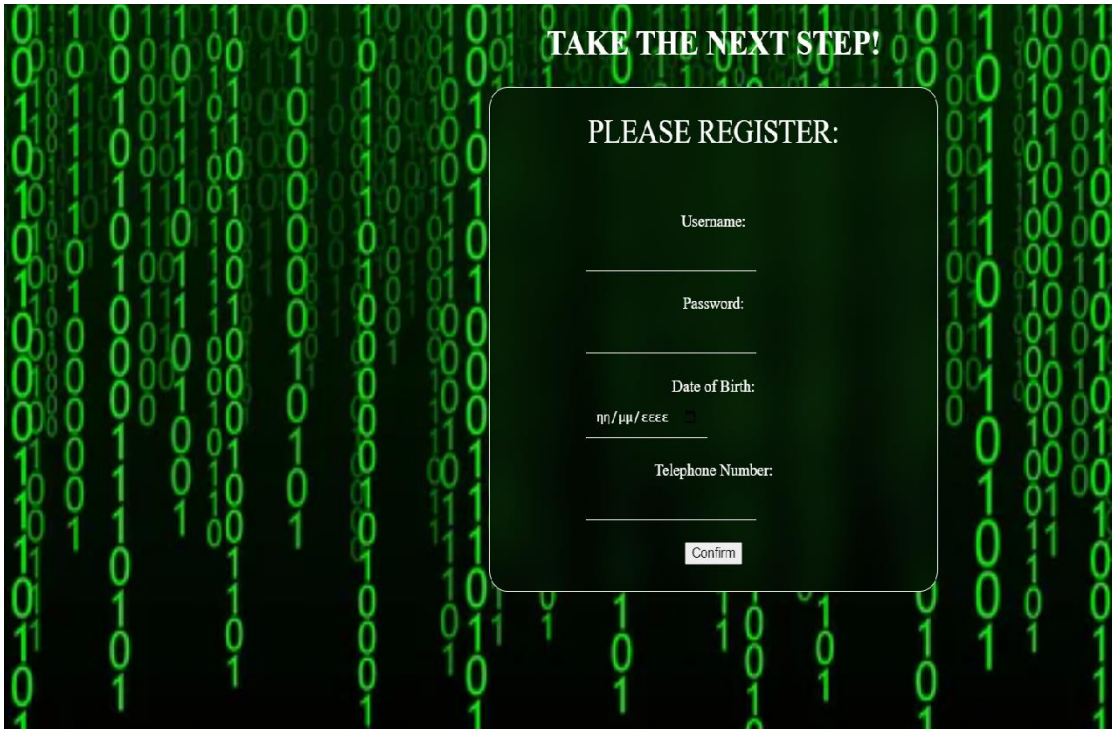


Εικόνα 17 Αρχεία για τη δημιουργήθηκαν και την μορφοποίηση της ιστοσελίδας

Στις δύο επόμενες εικόνες φαίνεται το τελικό αποτέλεσμα . Η πρώτη είναι η πλατφόρμα εισόδου όπου ο χρήστης συμπληρώνει τα διαπιστευτήριά του για την είσοδό του στη βάση δεδομένων της ομάδας κυβερνοασφάλειας. Στην περίπτωση που ο χρήστης δεν έχει λογαριασμό του δίνεται η δυνατότητα πατώντας το κουμπί *join* να μεταφερθεί στην φόρμα εγγραφής και συμπληρώνοντας τα στοιχεία του, να δημιουργήσει έναν νέο.

Εικόνα 18 Η πλατφόρμα εισόδου της ιστοσελίδας

Στην εικόνα που ακολουθεί φαίνεται η φόρμα εγγραφής στην οποία ο χρήστης συμπληρώνει τα πεδία όνομα χρήστη, κωδικό, ημερομηνία γέννησης και αριθμό τηλεφώνου για να δημιουργήσει έναν νέο λογαριασμό.



Εικόνα 19 Η πλατφόρμα εγγραφής στην ιστοσελίδα

Στη συνέχεια δοκιμάζουμε την είσοδο στην πλατφόρμα με τα όνομα (username) και τον κωδικό (password) ενός εκ των χρηστών που ήδη υπάρχουν στον πίνακα της βάσης δεδομένων. Όταν συμπληρώνει ο χρήστης τα στοιχεία του στα πεδία username και password, ο κώδικας που εκτελείται είναι ο εξής:

```
$username = $_REQUEST['username'];

$pass = $_REQUEST['pass'];

$sql = "select * from reg where username = '$username ' and pass = '$pass
' ";

$result = mysqli_query($conn,"$sql");

if(mysqli_num_rows($result)>0)

{

echo "$username Welcome to cybersecurity team!" ;
```

```
                }

                 else{

                        echo "ERROR:Sorry, something went wrong with your credentials.
Please try again or make a register.  "

                                . mysqli_error($conn);

}
```

Ας αναλύσουμε λίγο τον κώδικα. Με την μέθοδο REQUEST συλλέγονται τα στοιχεία που εισάγει ο χρήστης στα πεδία εισόδου. Έπειτα, με τα στοιχεία που δόθηκαν, εκτελείται το παρακάτω sql ερώτημα :

“select * from reg where username= '$username' and pass ='$pass'”

Όπου οι μεταβλητές του ερωτήματος αντικαθίστανται με τα στοιχεία που δίνει ο χρήστης, ως εξής:

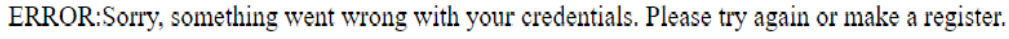
“select * from reg where username='lola' and pass ='123'”

Τα στοιχεία που δόθηκαν στα πεδία, συγκρίνονται με αυτά που υπάρχουν στον πίνακα της βάσης δεδομένων και το αποτέλεσμα αποθηκεύεται στην μεταβλητή result. Στη συνέχεια, το αποτέλεσμα αυτό, χρησιμοποιείται από την συνάρτηση mysqli_num_rows η οποία ελέγχει γραμμή προς γραμμή τα στοιχεία του πίνακα reg για να ταυτοποιήσει τα στοιχεία που εισήχθησαν στα πεδία εισόδου. Εάν υπάρχει έστω και μια γραμμή στον πίνακα με τα ίδια στοιχεία, η σύνδεση είναι επιτυχής και εμφανίζεται το μήνυμα « ‘όνομα χρήστη’ Welcome to cybersecurity team!», σε διαφορετική περίπτωση εμφανίζει μήνυμα σφάλματός. Παίρνοντας ενδεικτικά το όνομα χρήστη lola με κωδικό 123, το μήνυμα που θα μας εμφανίσει μόλις πατήσουμε το κουμπί submit, θα είναι μήνυμα επιτυχημένης σύνδεσης στην πλατφόρμα ως ακολούθως.

lola Welcome to cybersecurity team!

Εικόνα 20 Μήνυμα επιτυχημένης εισόδου

Αν δεν υπάρχει ταυτοποίηση των στοιχείων στην βάση δεδομένων, δηλαδή αν ο χρήστης δεν έχει κάποιο ενεργό λογαριασμό ή πληκτρολογήσει λάθος στοιχεία σύνδεσης, θα εμφανιστεί μήνυμα λάθους όπως προκύπτει στην παρακάτω εικόνα.



Εικόνα 21 Μήνυμα αποτυχημένης εισόδου

Η ΕΠΙΘΕΣΗ

Αναφέρθηκε ήδη, ότι για την εκτέλεση της επίθεσης έγχυσης κώδικα χρησιμοποιούνται δημόσια πεδία εισαγωγής δεδομένων, όπως είναι οι φόρμες διαδικτυακών εφαρμογών, στις οποίες οι χρήστες καλούνται να συμπληρώσουν τα στοιχεία τους για την επιτυχημένη είσοδό τους σε αυτές. Σε μια sql injection επίθεση, γίνεται, επί της ουσίας, εισαγωγή εντολών sql στα πεδία της φόρμας, αντί για τα αναμενόμενα δεδομένα. Σε περίπτωση που δεν ληφθούν σωστές προγραμματιστικές τεχνικές και δεν πραγματοποιείται έλεγχος των δεδομένων εισόδου, αυτό μπορεί να παραχωρήσει σε κακόβουλους χρήστες, επιτυχημένη είσοδο στην βάση δεδομένων της εφαρμογής, καθώς επίσης και την δυνατότητα να πραγματοποιήσουν μη εξουσιοδοτημένες ενέργειες σε αυτή (όπως για παράδειγμα υποκλοπή ευαίσθητων δεδομένων). Για την επίθεση λοιπόν, θα γίνει εισαγωγή κώδικα sql στο πεδίο του ονόματος χρήστη, που σκοπό έχει την είσοδο μη εξουσιοδοτημένων χρηστών στην εφαρμογή. Έτσι, στο πεδίο του ονόματος χρήστη γράφουμε την εντολή **‘ OR 1=1—** , ‘όπως φαίνεται και στην εικόνα που ακολουθεί και πατάμε το πληκτρο submit.

Εικόνα 22 Εισαγωγή εντολής sql στο πεδίο του ονόματος χρήστη

Όπως έχουμε ήδη δει στην αρχή του κεφαλαίου, ο κώδικας που εκτελείται όταν ένας χρήστης εισάγει τα διαπιστευτήριά του στα πεδία, είναι:

"select * from reg where username = '$username ' and pass = '$pass ' ";

Ωστόσο, όταν πληκτρολογείται η παραπάνω εντολή στο πεδίο του ονόματος χρήστη, το ερώτημα sql μετατρέπεται ως εξής:

“select * from reg where username= ‘ ‘ OR 1=1— “ ;

Αυτό που συμβαίνει στην ουσία, είναι ότι το ερώτημα θα είναι αληθές για κενό πεδίο ονόματος χρήστη ή για 1=1 , το οποίο θα ισχύει πάντοτε. Οι δύο παύλες αποτελούν χαρακτήρες σχολίων στην sql, πράγμα που σημαίνει ότι το υπόλοιπο ερώτημα παρακάμπτεται με αποτέλεσμα να επιτρέπεται η είσοδος στον επιτιθέμενο και να εμφανίζεται το μήνυμα επιτυχημένης σύνδεσης όπως φαίνεται παρακάτω.

'OR 1=1-- Welcome to cybersecurity team!

Εικόνα 23 Επιτυχημένη είσοδος κακόβουλου χρήστη

Το παραπάνω αποτελεί ένα ενδεικτικό παράδειγμα της επίθεσης έγχυσης κώδικα στην πιο απλή μορφή της. Υπάρχουν αρκετοί τρόποι με τους οποίους ένας κακόβουλος χρήστης θα

μπορούσε να φέρει σε πέρας μια τέτοια επίθεση. Τέτοιοι είναι για παράδειγμα με εξαγωγή συμπερασμάτων από τα μηνύματα λάθους. Σε μια τέτοια περίπτωση, ο επιτιθέμενος εγχέει κώδικα sql προσπαθώντας να προκαλέσει κάποιο λάθος στα ερωτήματα προς τη βάση δεδομένων. Τέτοια λάθη μπορεί να είναι λογικά, συντακτικά ή μετατροπής τύπου. Μέσα από τα μηνύματα λάθους ο κακόβουλος χρήστης είναι σε θέση να εξάγει συμπεράσματα που αφορούν στα χαρακτηριστικά και την δομή της βάσης δεδομένων και μπορεί να τα χρησιμοποιήσει για την διεξαγωγή μεταγενέστερων επιθέσεων.

ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΜΥΝΤΙΚΕΣ ΠΡΑΚΤΙΚΕΣ

Για την αποτελεσματικότερη προστασία μιας βάσης δεδομένων από επιθέσεις έγχυσης κώδικα, ενδείκνυται η εφαρμογή ασφαλών προγραμματιστικών τεχνικών στον κώδικα της εφαρμογής, η προσεκτική ανάθεση διαχειριστικών δικαιωμάτων στους χρήστες και η εγκατάσταση τειχών προστασίας στο πληροφοριακό σύστημα. Πιο συγκεκριμένα:

ΠΑΡΑΜΕΤΡΟΠΟΙΗΜΕΝΑ ΕΡΩΤΗΜΑΤΑ (Parameterized statements ή Prepared Statements)

Είναι μια τεχνική που χρησιμοποιείται για την εκτέλεση των ίδιων ή παρόμοιων δηλώσεων, επαναλαμβανόμενα, με υψηλή αποδοτικότητα και αποτελείται από δύο στάδια, την προετοιμασία και την εκτέλεση . Στο στάδιο της προετοιμασίας η δήλωση με την μορφή προτύπου αποστέλλεται στον εξυπηρετητή της βάσης δεδομένων για έλεγχο. Έπειτα, ακολουθεί η εκτέλεση του ερωτήματος, όπου οι παράμετροι αποθηκεύονται σε μεταβλητές οι οποίες είναι συνδεδεμένες με τον τύπο δεδομένων και αποστέλλονται στον server. https://www.php.net/manual/en/mysqli.quickstart.prepared-statements.php

ΕΛΕΓΧΟΣ ΕΙΣΟΔΟΥ (Validating Input)

Το φιλτράρισμα της εισόδου, των πεδίων, δηλαδή, που συμπληρώνει ο χρήστης, είναι μια τεχνική που χρησιμοποιείται για να καθορίσει ποιες εισακτέες τιμές είναι αποδεκτές όπως είναι για παράδειγμα ο τύπος, το μήκος , το περιεχόμενο και το μέγεθος των μεταβλητών. Για παράδειγμα, για αριθμητικές παραμέτρους να απορρίπτονται οι χαρακτήρες που δεν είναι ψηφία.

ΑΠΟΘΗΚΕΥΜΕΝΕΣ ΔΙΑΔΙΚΑΣΙΕΣ (Stored Procedures)

Δεν αποτελούν πάντα την ασφαλέστερη επιλογή άμυνας από επιθέσεις sql injection, ούτε είναι τόσο ασφαλή όσο τα παραμετροποιημένα ερωτήματα που αναφέρθηκαν προηγουμένως.

Ωστόσο με την κατάλληλη χρήση μπορούν να επιφέρουν το ίδιο αποτέλεσμα. Η διαφορά μεταξύ αυτών των δύο, έγκειται στο γεγονός ότι οι αποθηκευμένες διαδικασίες καθορίζονται και αποθηκεύονται στη βάση δεδομένων και έπειτα καλούνται από την εφαρμογή. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

ΔΙΑΧΕΙΡΙΣΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ (Administrative Privileges)

Για να ελαχιστοποιηθούν οι πιθανότητες μιας επιτυχημένης επίθεση έγχυσης κώδικα, θα πρέπει να ελαχιστοποιούνται και τα δικαιώματα που ανατίθενται στον κάθε χρήστη της βάσης δεδομένων ακολουθώντας την αρχή του λιγότερο προνομιούχου. Ο προγραμματιστής θα πρέπει να ξεκινάει από τον λιγότερο προνομιούχο χρήστη, αναθέτοντας του μόνο τα δικαιώματα που χρειάζεται (π.χ. μόνο το δικαίωμα ανάγνωσης) και αφαιρώντας τα υπόλοιπα. Για πολλούς σχεδιαστές μιας webεφαρμογής θα πρέπει να αποφεύγεται η χρήση του ίδιου λογαριασμού διαχειριστή ώστε να υπάρχει καλύτερος έλεγχος της βάσης δεδομένων.

ΧΡΗΣΗ ΤΕΙΧΩΝ ΠΡΟΣΤΑΣΙΑΣ (FIREWALLS)

Μια ακόμη αμυντική πρακτική έναντι των επιθέσεων αυτών, αποτελεί η χρήση τειχών προστασίας. Η χρήση ενός τείχους προστασίας εφαρμογής (web application firewall) είναι ένας μηχανισμός αντιμετώπισης sql injection ο οποίος παρέχει ένα σύνολο κανόνων που φιλτράρει δυνητικά αιτήματα ιστού.

ΕΦΑΡΜΟΓΗ ΠΑΡΑΜΕΤΡΟΠΟΙΗΜΕΝΟΥ ΕΡΩΤΗΜΑΤΟΣ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΤΗΝ ΕΠΙΘΕΣΗ

Στην περίπτωση της παρούσας εργασίας, θα γίνει εφαρμογή των παραμετροποιημένων ερωτημάτων με χρήση της συνάρτησης bind_param(). Εδώ, σε σύγκριση με την εκτέλεση του κώδικα στην προηγούμενη εκδοχή της, η δήλωση $stmt προετοιμάζεται με την χρήση της συνάρτησης prepare() και αποστέλλεται στον εξυπηρετητή της βάσης $conn για έλεγχο. Παρατηρείται ότι οι μεταβλητές ‘$username’ και ‘$pass’ αντικαθίστανται με τα ερωτηματικά. Στη συνέχεια, χρησιμοποιείται η συνάρτηση bind_param(). Η συνάρτηση αυτή συνδέει τις παραμέτρους του ερωτήματος sql και δηλώνει στην βάση δεδομένων τον τύπο τους (εδώ είναι και τα δύο string, οπότε χρησιμοποιείται το όρισμα ss), περιορίζοντας έτσι τις πιθανότητες μιας επίθεσης sql injection. Ο κώδικας διαμορφώνεται όπως φαίνεται παρακάτω.

```
$stmt = $conn->prepare("SELECT * FROM reg WHERE username = ? AND pass = ?");
$stmt->bind_param("ss", $username, $pass);
$stmt->execute();
$stmt->store_result();
```

Μετά την αλλαγή στον κώδικα, αν στο πεδίο username της σελίδας εισάγουμε **‘ OR 1=1--** το μήνυμα που θα εμφανιστεί θα είναι το παρακάτω:

ERROR:Sorry, something went wrong with your credentials. Please try again or make a register.

Εικόνα 24 Μήνυμα λάθους με χρήση PDO

Ο ΚΩΔΙΚΑΣ

Στη συνέχεια ακολουθεί ο κώδικας που γράφτηκε τόσο για την κατασκευή και την λειτουργία της ιστοσελίδας, όσο για την σύνδεσή της με την βάση δεδομένων.

Το αρχείο index.php

```
<!DOCTYPE html>
<html lang="en">
<head>
        <title>Log in form</title>
        <style>
        h1{
color:white;}
```

```
body{
        margin:0;
        padding:0;
background-image:url('binary.jpg');
        background-repeat:no-repeat;
        background-attachment:fixed;
background-size:100% 100% ; }
legend{
color:white;
                align:left;
                font-size:30px;
        }
        p{
        color: white;
        position:fixed;
        left:0px;
        bottom:50px
}
        #username{
                border:none;
                background:transparent;
                border-bottom:1px solid white;
        padding:10px;
        margin-bottom:20px;
        display:flex;
        color:white;}
```

```
        #pass{
                border:none;
                background:transparent;
                border-bottom:1px solid white;
        padding:10px;
        margin-bottom:20px;
        display:flex;
        color:white;
        }
.container{
  width:400px;
  height:380px;
  padding:40px;
  text-align:center;
  border:1px solid white;
  border-radius:20px;
  backdrop-filter:blur(20px) brightness(50%);
  display:flex;
  flex-direction:column;
  justify-content:center;
  align-items:center;
  color:white;
}
</style>
</head>
<body>
```

```
<center>
<h1> Cybersecurity Team </h1>
<div class="container">
<form action="insert.php" method="post" autocomplete="off">
<legend> LOG IN :</legend><br><br><br>
<label for="username"> Username:</label>
        <input type="text" name="username" id="username">
        <label for="pass">Password:</label>
        <input type="password" name="pass" id="pass">
         <input type="submit" value="Submit">
        </div>
        </form>
        </center>
        <p> You don't have an account yet? Make your register now in one step!
 <a href="http://localhost/try/register.php" target="_blank"> join</a>      </p>
</body>
</html>
```

Το αρχείο Insert.php

```
<!DOCTYPE html>
<html>
<head>
  <title>Insert Page page</title>
</head>
      <body>
  <center>
```

```
<?php
$servername ="localhost";
$username ="root";
$pass =" ";
$database_name = "fac";
$conn = mysqli_connect("localhost", "root", "", "fac")
or die("cannot connect");
// Check connection
if($conn === false){
die("ERROR: Could not connect. "
. mysqli_connect_error());
}

$mysqli = mysqli_select_db($conn, "$database_name")or
die("cannot select DB");
// Taking all 2 values from the form data(input)
$username = $_REQUEST['username'];
$pass = $_REQUEST['pass'];
$stmt = $conn->prepare("SELECT * FROM reg WHERE username = ? AND pass = ?");
$stmt->bind_param("ss", $username, $pass);
$stmt->execute();
$stmt->store_result();
if($stmt->num_rows>0)
{
echo "$username Welcome to cybersecurity team!" ;
}
```

```
        else{
                echo "ERROR:Sorry, something went wrong with your credentials. Please try again
  or make a register.  "
                        . //mysqli_error($conn);
                        $stmt->close();
}
        // Close connection
        mysqli_close($conn);
        ?>
  </center>
</body>
        </html>
```

<u>Το αρχείο new_entry.php</u>

```
        <!DOCTYPE html>
        <html>
        <head>
        <title>Insert Page page</title>
        </head>
        <body>
        <center>
        <?php
         $servername ="localhost";
         $username ="root";
         $pass ="";
        $dob="";
```

```
 $tel="";
$db_name = "fac";
 $isValid=true;
 $conn = mysqli_connect("localhost", "root", "", "fac")
                    or die("cannot connect");
$mysqli = mysqli_select_db($conn, "fac")or
 die("cannot select DB");
// Taking all 4 values from the form data(input)
$username = $_POST['username'];
$pass = $_POST['pass'];
$dob=$_POST['dob'];
$tel=$_POST['tel'];
// Performing insert query execution// here our table name is reg

$data = $_POST;if (empty ($data['username'])||
   empty($data['pass']) ||
          empty ($data ['dob'])||
          empty ($data ['tel'])) {
          die('please fill the fields');}
if ($stm=$conn->prepare ('select username from reg where username=?'))
{
$stm->bind_param("s",$username);
$stm->execute();
$stm-> store_result();
if ($stm->num_rows > 0){
                    $isValid=false;
```

```
                echo'username taken';
}
        else if($isValid) {
                $insertSql="insert into reg (username,pass,dob,tel) values (?,?,?,?)";
                $stm=$conn->prepare($insertSql);
                $stm-> bind_param("sssd",$username,$pass,$dob,$tel);
                $stm->execute();
                $stm->close();
                echo'success';
                }
        }
```

<u>To αρχείο register.php</u>

```
<!DOCTYPE html>
<html lang="en">
<head>
<title>Log in form</title>
<style>
h1{
color:white;
}
body{
margin:0;
padding:0;
background-image:url('binary.jpg');
```

```
background-repeat:no-repeat;
background-attachment:fixed;
background-size:100% 100% ;
}
  legend{
color:white;
align:left;
font-size:30px;
}
#username{
border:none;
background:transparent;
border-bottom:1px solid white;
padding:10px;
margin-bottom:20px;
display:flex;
color:white;}
#pass{
border:none;
background:transparent;
border-bottom:1px solid white;
padding:10px;
margin-bottom:20px;
display:flex;
color:white;}
#dob{
```

```
border:none;
background:transparent;
border-bottom:1px solid white;
padding:10px;
margin-bottom:20px;
display:flex;
color:white;}
#tel{
border:none;
background:transparent;
border-bottom:1px solid white;
padding:10px;
margin-bottom:20px;
display:flex;
color:white;}
.container{
 width:400px;
  height:380px;
  padding:40px;
  text-align:center;
  border:1px solid white;
  border-radius:20px;
  backdrop-filter:blur(20px) brightness(50%);
   display:flex;
  flex-direction:column;
  justify-content:center;
```

```
 align-items:center;
 color:white;
}
</style>
</head>
<body>
<center>
<h1> TAKE THE NEXT STEP! </h1>
<div class="container">
<form action="new_entry.php" method="post" autocomplete="off">
<legend> PLEASE REGISTER: </legend><br><br><br>
<label for="username"> Username:</label>
<input type="text" name="username" id="username">
<label for="pass">Password:</label>
<input type="password" name="pass" id="pass">
 <label for="dob">Date of Birth:</label>
<input type="date" name="dob" id="dob">
 <label for="tel">Telephone Number:</label>
<input type="tel" name="tel" id="tel">
 <input type="submit" value="Confirm">
/div>
</form>
</center>
</body>
$conn->close();
?>
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Παγκαλος Γ. , Μαυρίδης Ι., Ασφάλεια πληροφοριακών συστημάτων και δικτύων (2002) https://static.eudoxus.gr/books/25/chapter-5425.pdf

[2] Solms R. , Niekerk J. (2013) From information security to cyber security https://profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

[3] Whitman M. , Mattord H. Principles of information security (2016) https://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

[4] Καμπαρίδου Ε. , (2015) Η στρατηγική κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση

[5] Authenticated U.S Government Information, 109th Congress 1st session (2005), To amend the Homeland Security Act of 2002 to enhance cybersecurity, and for other purposes https://www.govinfo.gov/content/pkg/BILLS-109hr285ih/pdf/BILLS-109hr285ih.pdf

[6] International Telecommunication Union, Series X: Data networks, open system communications and security (2008) https://www.itu.int/rec/T-REC-X.1205-200804-I

[7] Stallings W. Επικοινωνίες υπολογιστών και δεδομένων (2014)

[8] Stallings W. Κρυπτογραφία και ασφάλεια δικτύων: Αρχές & Εφαρμογές (2006)

[9] Garfinkel S. De-Identification of personal information (2015) https://nvlpubs.nist.gov/nistpubs/ir/2015/nist.ir.8053.pdf

[10] Μαυρίδης Ι. Ασφάλεια πληροφοριών στο διαδίκτυο (2015)

[11] Pfleeger C. & Pfleeger S. L. & Margulies J. Security in computing (2015)

[12] Στρουγγάρης Ζ. Η αξιολόγηση κινδύνου στην ασφάλεια πληροφοριών (2020)

[13] Ghazouani M. Medromi H. Sayouti A. Information Security Risk Assessment-A Practical Approach with a Mathematical Formulation of Risk (2014) https://research.ijcaonline.org/volume103/number8/pxc3899155.pdf

[14] Goswami R. , Sharma S. , Chawla C. , Pande J. Cyber Attacks and Counter Measures: User Perspective (2016) https://uou.ac.in/sites/default/files/slm/MIT(CS)-103.pdf

[15] Kizza J. M. Guide to computer network security (2017)

[16] Alotaibi A. M. , Alrashidi B. D. , Naz S. , Parveen Z. Security issues in protocols of TCP/IP model at Layers level (2017) https://www.researchgate.net/publication/330132778_Security_issues_in_Protocols_of_TCPIP_Model_at_Layers_Level

[17] Casad J. Μάθετε το TCP/IP σε 24 ώρες (2010)

[18] Mugala M. Security vulnerabilities and countermeasures in TCP/IP layers (2014) https://www.academia.edu/7527310/Security_Vulnerabilities_and_Countermeasures_In_TCP_IP_Layers

[19] Pal M. , Dokania V. , Dey P. K. Memory corruption-basic attacks and countermeasures (2016) https://www.researchgate.net/publication/311515579_Memory_Corruption-Basic_Attacks_and_Counter_Measures

[20] Gens D. OS-level attacks and defenses: From software to hardware-based exploits (2018) https://tuprints.ulb.tu-darmstadt.de/8482/1/gens_diss.pdf

[21] Prinetto P. , Roascio G. Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy (2020) https://ceur-ws.org/Vol-2597/paper-16.pdf

[22] Δελή Μολά Α. Πτυχιακή εργασία « Έλεγχος τρωσιμότητας προσωπικών υπολογιστών» (2018) https://ikee.lib.auth.gr/record/299952/files/%CE%95%CE%9B%CE%95%CE%93%CE%A7%

CE%9F%CE%A3%20%CE%A4%CE%A1%CE%A9%CE%A3%CE%99%CE%9C%CE%9F%CE%A4%CE%97%CE%A4%CE%91%CE%A3%20%CE%A0%CE%A1%CE%9F%CE%A3%CE%A9%CE%A0%CE%99%CE%9A%CE%A9%CE%9D%20%CE%A5%CE%A0%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%A3%CE%A4%CE%A9%CE%9D.pdf

[23] Souppaya M. , Scarfone K. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (2016) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf

[24] Βασιλάκης Κ. Σημειώσεις μαθήματος «ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ» (2004-2005) https://eclass.uoa.gr/modules/document/file.php/DI273/%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/notes.pdf

[25] Σταματινός Μ. Πτυχιακή εργασία Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων (2015) https://hellanicus.lib.aegean.gr/bitstream/handle/11610/9313/file0.pdf?sequence=1&isAllowed=y

[26] Ahmad H. , Verma S. , Kumar N. , Shekhar J. Classification of Internet Security Attacks (2011) **https://www.researchgate.net/publication/262494946_Classification_of_Internet_Security_Attacks**

[27] Μάγκος Ε. Σημειώσεις μαθήματος Ασφάλεια υπολογιστών και προστασία δεδομένων (2007) http://195.130.124.90/~emagos/security/Simeioseis-Asfaleia%20Part%20A.pdf

[28] Δέμης Π. , Μαρούδη Α. Πτυχιακή εργασία Ανάλυση απαιτήσεων ασφάλειας που σχετίζονται με το ηλεκτρονικό έγκλημα και υλοποίηση μεθόδων επίθεσης με στόχο το ηλεκτρονικό έγκλημα καθώς και υλοποίηση αντίμετρων που να αποτρέπουν την επίθεση (2016)

[29] Saroha S. , Restraining packet sniffing & security : A brief overview (2020) https://ijisrt.com/assets/upload/files/IJISRT20DEC678.pdf

[30] Patel N. Packet sniffing: Network wiretapping (2009) https://www.researchgate.net/publication/267908713_Packet_Sniffing_Network_Wiretapping

[31] Alqudah N. , Yassen Q. Machine learning for traffic analysis: A review (2020) https://www.sciencedirect.com/science/article/pii/S1877050920305494?ref=pdf_download&fr=RR-2&rr=83382067c973eea4

[32] Manish J. , Theyazn H. A review on network traffic analysis and prediction techniques https://arxiv.org/ftp/arxiv/papers/1507/1507.05722.pdf

[33] Andress J. The Basics of Information Security (2014) https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition

[34] Murad M. A. Intrusion Detection, Denial of Service (DOS) (2006) https://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/DoS.pdf

[35] Καραμάνης Ν. Επιθέσεις Distributed Denial of Service (DDoS) και μέτρα προστασίας σε δίκτυα δεδομένων. (2010) https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4091/Karamanis.pdf?sequence=2&isAllowed=y

[36] Ormiston K. Eloff M.M. Denial of Service & Distributed Denial of Service on the Internet (2006) https://www.researchgate.net/publication/220803146_Denial-of-Service_Distributed_Denial-of-Service_on_The_Internet

[37] Babu R.P., Bhaskari L.D. , Satyanayana CH. A Comprehensive Analysis of Spoofing (2010) https://www.researchgate.net/publication/49597043_A_Comprehensive_Analysis_of_Spoofing

[38] Ylli E. , Fejzaj J. Man in the Middle: Attack and Protection (2021) https://ceur-ws.org/Vol-2872/short08.pdf

[39] Nohlberg M. Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks (2008) https://www.diva-portal.org/smash/get/diva2:200190/FULLTEXT01.pdf

[40] Raza M. , Iqbal M. , Sharif M. , Haider W. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication (2012) https://www.researchgate.net/publication/236898951_A_Survey_of_Password_Attacks_and_Comparative_Analysis_on_Methods_for_Secure_Authentication

[41] Stallings W. Λειτουργικά Συστήματα : Αρχές Σχεδίασης (2009)

[42] Saeed Hama M. Malware in Computer Systems: Problems and Solutions (2020) https://www.researchgate.net/publication/340770783_Malware_in_Computer_Systems_Problems_and_Solutions

[43] National Cyber Security Centre, Common cyber attacks: reducing the impact (2016) https://www.ncsc.gov.uk/static-assets/documents/common_cyber_attacks_ncsc.pdf

[44] Garba A. F. The Anatomy of a Cyber Attack: Dissecting the Cyber Kill Chain (2019) https://www.researchgate.net/publication/330658097_The_Anatomy_of_a_Cyber_Attack_Dissecting_the_Cyber_Kill_Chain

[45] Ravi S. , Samarati R. Authentication, Access Control, and Audit (1996) https://spdp.di.unimi.it/papers/survey96.pdf

[46] Yampolskiy R. , Govindaraju V. Behavioural biometrics: a survey and classification (2008) https://www.researchgate.net/publication/247836093_Behavioural_biometrics_A_survey_and_classification]

[47] Hu V. , Ferraiolo D. , Kuhn R. Assessment of Access Control Systems (2006) https://nvlpubs.nist.gov/nistpubs/legacy/ir/nistir7316.pdf

[48] Αντωνακοπούλου Α. Έλεγχος Πρόσβασης Πληροφοριακών Συστημάτων με «Επίγνωση Πλαισίου» Βασισμένος σε Οντολογίες (2014) http://artemis.cslab.ece.ntua.gr:8080/jspui/bitstream/123456789/8970/1/PD2014-0042.pdf

[49] Γερμανός Γ., Γεωργίου Ν. Κυβερνοέγκλημα Πρόληψη- Διερεύνηση- Αντιμετώπιση (2021)

[50] Κάτος Β. , Στεφανίδης Γ. Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης (2003)

[51] Καραδημητρίου Κ. Η ηλεκτρονική Υπογραφή ως μέσο ασφάλειας στο ηλεκτρονικό εμπόριο (2007) https://phdtheses.ekt.gr/eadd/handle/10442/19145

[52] Tanenbaum A. Δίκτυα Υπολογιστών (2003)

[53] Kizza J. Guide to Computer Network Security (2017)

[54] Bace R. , Mell P. Intrusion Detection Systems (NIST Special Publication) https://csrc.nist.rip/library/NIST%20SP%20800-031%20Intrusion%20Detection%20Systems%20(IDS),%202001-11.pdf

[55] Vijayarani S. , Phil M. Intrusion Detection System – A study (2015) https://airccse.org/journal/ijsptm/papers/4115ijsptm04.pdf

[56] Rehman R. Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID (2003) https://ptgmedia.pearsoncmg.com/imprint_downloads/informit/perens/0131407333.pdf

[57] Ρούσσος Β. Συστήματα Διαχείρισης & Ανίχνευσης Εισβολών Διαχείριση Logs (2012) https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/5824/Roussos.pdf?sequence=2&isAllowed=y

[58] Shukla M. , Verma P. Honeypot: Concepts, Types and Working (2015) https://www.ijedr.org/papers/IJEDR1504100.pdf

[59] Spitzner L. Honeypots: Tracking Hackers (2002) http://www.it-docs.net/ddata/792.pdf

[60] Πατρώνη Μ. Honeypots και ασφάλεια πληροφοριακών συστημάτων (2013) https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/5655/Patroni.pdf?sequence=2&isAllowed=y

URLs

[1] https://notepad-plus-plus.org/

[2] https://www.apachefriends.org/index.html

[3] https://httpd.apache.org/

[4] https://www.mysql.com/

[5] https://www.php.net/manual/en/intro-whatis.php

[6] https://html.com/

[7] https://www.phpmyadmin.net/