ΠΑΝΕΠΙΣΤΗΜΙΟ
ΙΩΑΝΝΙΝΩΝ

ΣΧΟΛΗ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΣ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Μάριος Καλαμπαλίκης

Επιβλέπων: Ευριπίδης Γλαβάς

Καθηγητής

Άρτα, Σεπτέμριος, 2024

Περιεχόμενα

Περίληψη

Η παρούσα εργασία έχει ως κεντρικό θέμα την κυβερνοασφάλεια, ένα θέμα ιδιαίτερα επίκαιρο αυτή την εποχή. Αρχικά, δίνονται ορισμένες βασικές πληροφορίες για την κατανόηση της έννοιας της κυβερνοασφάλειας, της ιστορικής της εξέλιξης, της σημασίας και των βασικών αρχών της. Έπειτα παρουσιάζονται οι κυριότερες απειλές εναντίον της ασφαλούς πλοήγησης στον κυβερνοχώρο και η μεθοδολογία που χρησιμοποιείται προκειμένου να αντιμετωπιστούν αποτελεσματικά, αλλά και να προληφθούν οι κυβερνοεπιθέσεις. Στη συνέχεια αναλύεται το νομοθετικό πλαίσιο που ισχύει στην Ευρωπαϊκή Ένωση και στην Ελλάδα και αφορά το ζήτημα της κυβερνοασφάλειας. Ακολουθεί μια αναφορά στην διαχείριση των κρίσεων στον κυβερνοχώρο και στα στάδια που αυτή ακολουθεί. Η εργασία ολοκληρώνεται με ένα κεφαλαίο αναφορικά με τις σύγχρονες τάσεις αλλά και προκλήσεις στον τομέα της κυβερνοασφάλειας.

Λέξεις/φράσεις κλειδιά: κυβερνοασφάλεια, κυβερνοχώρος, κακόκουβουλο λογισμικό, κυβερνοεπιθέσεις, εισβολή, παραβιάσεις δεδομένων, ENISA, τεχνητή νοημοσύνη

Εισαγωγή

Οι τεχνολογίες δικτύων και πληροφοριών, και ιδιαίτερα το διαδίκτυο, έχουν διεισδύσει σχεδόν σε κάθε τομέα της κοινωνικής, προσωπικής και επαγγελματικής ζωής. Η επίδρασή τους είναι τόσο καθοριστική που σε πολλές περιπτώσεις μπορούμε να μιλήσουμε για πραγματική εξάρτηση από αυτές και αντικειμενική αδυναμία λειτουργίας χωρίς την ύπαρξή τους. Συγκεκριμένα, όσον αφορά το διαδίκτυο, η ραγδαία ανάπτυξή του και η ποικιλία των εφαρμογών και λειτουργιών του το έχουν καταστήσει αναπόσπαστο εργαλείο σε ένα ευρύ φάσμα δραστηριοτήτων που συνδέονται με την οικονομία, το εμπόριο, τις επιχειρήσεις και τους δημόσιους και ιδιωτικούς οργανισμούς. Το διαδίκτυο, ωστόσο, χρησιμοποιείται ευρέως και καθημερινά από τους πολίτες για διάφορους λόγους, όπως η ψυχαγωγία, η ενημέρωση και η εκπαίδευση, οι τραπεζικές συναλλαγές, καθώς και για αλληλεπίδραση και επικοινωνία με άλλους χρήστες.

Ωστόσο, αυτή η εξάρτηση συνοδεύεται από αυξημένους κινδύνους παραβίασης της ασφάλειας, που μπορούν να έχουν σοβαρές συνέπειες για την οικονομία, την κοινωνία και την εθνική ασφάλεια. Ταυτόχρονα οι πολίτες που χρησιμοποιούν πολλές φορές χωρίς προσοχή όλα αυτά τα μέσα βρίσκονται σε κίνδυνο της ιδιωτικότητάς τους και υποκλοπής προσωπικών πληροφοριών.

Σήμερα περισσότερο από ποτέ η προστασία από κυβερνοεπιθέσεις, όπως παραβιάσεις δεδομένων, επιθέσεις DDoS και διεισδύσεις μέσω κακόβουλου λογισμικού, είναι ζωτικής σημασίας. Οι επιθέσεις αυτές δεν απειλούν μόνο την ιδιωτικότητα των δεδομένων, αλλά και τη λειτουργικότητα των συστημάτων που εξυπηρετούν βασικές υπηρεσίες. Η ψηφιακή εποχή απαιτεί από όλους μας να είμαστε πιο ενημερωμένοι και προετοιμασμένοι για την αντιμετώπιση αυτών των απειλών.

Η συνεχής εξέλιξη της τεχνολογίας, όπως το Διαδίκτυο των Πραγμάτων (IoT) και η Τεχνητή Νοημοσύνη (AI), προσφέρει νέες ευκαιρίες αλλά και προκλήσεις για

την κυβερνοασφάλεια. Η αυξανόμενη διασύνδεση και η ευκολία πρόσβασης δημιουργούν νέους δρόμους για επιθέσεις, καθιστώντας την ανάπτυξη ισχυρών και καινοτόμων μέτρων ασφαλείας απαραίτητη.

Στο πλαίσιο αυτό, η Ευρωπαϊκή Ένωση και άλλοι διεθνείς οργανισμοί έχουν λάβει σημαντικές πρωτοβουλίες για την ενίσχυση της κυβερνοασφάλειας, προωθώντας νομοθετικές ρυθμίσεις και συνεργατικά μέτρα που στοχεύουν στη δημιουργία ενός ασφαλέστερου ψηφιακού περιβάλλοντος. Η προστασία των δεδομένων και των συστημάτων μας είναι κρίσιμη για τη διατήρηση της εμπιστοσύνης στις ψηφιακές τεχνολογίες και τη διασφάλιση της συνεχούς και ασφαλούς λειτουργίας των κοινωνιών μας.

Κεφάλαιο 1. Γενικά για την κυβερνοασφάλεια

1.1 Ορισμός της κυβερνοασφάλειας

Για να κατανοήσουμε τον όρο Κυβερνοασφάλεια είναι απαραίτητο να εξετάσουμε τα δύο συνθετικά της λέξης. Το πρώτο συνθετικό «κυβερνό» είναι ένα πρόθεμα που υποδηλώνει τον κυβερνοχώρο και αναφέρεται σε δίκτυα ηλεκτρονικής επικοινωνίας και στην εικονική πραγματικότητα (Oxford, 2014). Ο όρος "κυβερνοχώρος" έγινε δημοφιλής από το μυθιστόρημα του William Gibson το 1984, Neuromancer, στο οποίο περιγράφει το όραμά του για έναν τρισδιάστατο χώρο καθαρής πληροφορίας, που κινείται μεταξύ υπολογιστών και συμπλεγμάτων υπολογιστών, όπου οι άνθρωποι είναι δημιουργοί και χρήστες της πληροφορίας. Αυτό που σήμερα γνωρίζουμε ως κυβερνοχώρο είχε σχεδιαστεί και προοριζόταν ως περιβάλλον πληροφορίας (Singer & Friedman, 2013), και σήμερα υπάρχει μια διευρυμένη εκτίμηση του κυβερνοχώρου. Για παράδειγμα, το Public Safety Canada (2010) ορίζει τον κυβερνοχώρο ως «τον ηλεκτρονικό κόσμο που δημιουργείται από διασυνδεδεμένα δίκτυα τεχνολογίας πληροφορικής και την πληροφορία που υπάρχει σε αυτά τα δίκτυα».

Όσον αφορά τον όρο "ασφάλεια", η βιβλιογραφία δείχνει ότι δεν υπάρχει ένας ευρέως αποδεκτός ορισμός και είναι δύσκολο να οριστεί γενικά. Σύμφωνα με τους Buzan, Wæver και Wilde (1998), όταν μιλάμε για ασφάλεια, πρέπει να κατανοήσουμε ποιος προσπαθεί να εξασφαλίσει τι, ενάντια σε ποιες απειλές, για ποιον, γιατί, με ποια αποτελέσματα και υπό ποιες συνθήκες. Ο ορισμός της ασφάλειας εξαρτάται από την οπτική γωνία του καθενός και από το τι θεωρεί σημαντικό.

Η Κυβερνοασφάλεια, λοιπόν, μπορεί να οριστεί ως η οργάνωση και η συλλογή πόρων, διαδικασιών και δομών που χρησιμοποιούνται για την προστασία του κυβερνοχώρου και των συστημάτων που βασίζονται στον κυβερνοχώρο από περιστατικά που αποκλίνουν νομικά από τα πραγματικά δικαιώματα ιδιοκτησίας (Craigen et al., 2014). Ο όρος αυτός αναφέρεται σε όλα τα μέτρα και τις διασφαλίσεις που εφαρμόζονται για την προστασία των πληροφοριακών συστημάτων και των χρηστών τους από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και ζημιές, προκειμένου να εξασφαλιστεί η «εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα» των δεδομένων (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019).

Η Κυβερνοασφάλεια περιλαμβάνει την πρόληψη και ανίχνευση περιστατικών ασφαλείας, καθώς και την αντίδραση και ανάκαμψη από αυτά. Αυτά τα περιστατικά μπορεί να είναι εσκεμμένα ή τυχαία και περιλαμβάνουν τη διαρροή πληροφοριών, επιθέσεις σε επιχειρήσεις και οργανισμούς, την κλοπή προσωπικών δεδομένων και παρεμβάσεις σε δημοκρατικές διαδικασίες. Οι συνέπειες αυτών των περιστατικών μπορεί να προκαλέσουν βλάβες σε άτομα, οργανισμούς και κοινότητες (Ευρωπαϊκό Ελεγκτικό Συνέδριο, 2019).

1.2 Ιστορική εξέλιξη της κυβερνοασφάλειας

Η ανάγκη για κυβερνοασφάλεια δεν ήταν πάντα τόσο επιτακτική όσο είναι σήμερα. Στην πραγματικότητα, αυτή η ανάγκη ξεκίνησε να διαμορφώνεται, καθώς η τεχνολογία άρχισε να εξελίσσεται ραγδαία, ειδικά από τη δεκαετία του 1940 και μετά. Τότε, η απειλή από τους υπολογιστές ήταν σχεδόν ανύπαρκτη, καθώς οι υπολογιστές ήταν πολύ λίγοι και λίγα άτομα είχαν πρόσβαση σε αυτούς. Επιπλέον, οι υπολογιστές δεν ήταν διασυνδεδεμένοι μεταξύ τους, κάτι που περιόριζε σημαντικά τις δυνατότητες επιθέσεων.

Παρά το γεγονός ότι οι απειλές ήταν ελάχιστες, ο πρώτος υπολογιστικός ιός έκανε την εμφάνισή του το 1949. Αυτός ο ιός δημιουργήθηκε από την αναπαραγωγή προγραμμάτων στον υπολογιστή, δηλαδή προγράμματα που μπορούσαν να αντιγράφουν τον εαυτό τους και να μολύνουν άλλους υπολογιστές. Αυτό το γεγονός φανέρωσε πως είναι δυνατή μια επίθεση και υπάρχει ανάγκη για προστασία των υπολογιστικών συστημάτων.

Η παραβίαση συστημάτων δεν περιοριζόταν μόνο στους υπολογιστές. Στα τέλη της δεκαετίας του 1950, εμφανίστηκε η "παραβίαση τηλεφώνων". Άτομα που ως επί το πλείστον εργάζονταν ως μηχανικοί σε τηλεπικοινωνίες, παραβίαζαν τα συστήματα των εταιρειών τηλεφωνίας για να αποφεύγουν τις χρεώσεις στις κλήσεις τους. Οι μεγάλες εταιρείες τηλεφωνίας της εποχής αντιμετώπισαν σοβαρά προβλήματα με αυτό το φαινόμενο και δεν μπορούσαν να το ελέγξουν. Τελικά, χρειάστηκαν περίπου 30 χρόνια για να βρουν αποτελεσματικούς τρόπους να το καταπολεμήσουν.

Η έννοια της ασφάλειας των υπολογιστών ξεκίνησε τη δεκαετία του 1960, όταν οι πρώτοι υπολογιστές έγιναν ευάλωτοι σε απειλές. Το 1972, το Ινστιτούτο Ερευνών των Πολεμικών Αεροποριών των ΗΠΑ δημοσίευσε το πρώτο εκτενές άρθρο για την ασφάλεια των υπολογιστών, γνωστό ως "The Anderson Report" (Anderson, 1972)

Ωστόσο, το πρώτο κακόβουλο περιστατικό hacking θεωρείται ευρέως ότι ήταν το Morris Worm, το οποίο δημιουργήθηκε από τον Robert Tappan Morris το 1988. Ο Morris, τότε φοιτητής στο Cornell University, δημιούργησε τον ιό ως ένα πείραμα για να δει πόσο μεγάλη είναι η ασφάλεια των δικτύων εκείνης της εποχής. Ο ιός εξαπλώθηκε γρήγορα, επηρεάζοντας περίπου 6.000 συστήματα UNIX και

προκάλεσε σοβαρά προβλήματα σε πολλά δίκτυα, δημιουργώντας σημαντικές οικονομικές ζημιές και διακοπές υπηρεσιών. Ο ιός εκμεταλλεύτηκε αδυναμίες σε διάφορα προγράμματα και τις αδύναμες κωδικούς πρόσβασης για να εξαπλωθεί. Παρά τις αρχικές προθέσεις του Morris να μην προκαλέσει καταστροφή, ο ιός προκάλεσε σημαντική ζημιά λόγω του τρόπου με τον οποίο ήταν προγραμματισμένος να αντιγράφεται πολλές φορές ακόμα και σε ήδη μολυσμένα συστήματα. Το περιστατικό αυτό είχε ως αποτέλεσμα τη δημιουργία του πρώτου Computer Emergency Response Team (CERT) από το DARPA, για να διαχειρίζεται και να αντιμετωπίζει τέτοιου είδους κρίσεις στο μέλλον . Ο ρόλος του CERT ήταν να παρακολουθεί τις κυβερνοαπειλές, να ανταποκρίνεται σε περιστατικά ασφαλείας και να αναπτύσσει πρότυπα και πρακτικές για την προστασία των συστημάτων, βελτιώνοντας έτσι τη συνολική ανθεκτικότητα των δικτύων (Orman, 2023).

Παράλληλα προωθήθηκε η ανάπτυξη λογισμικού ασφαλείας. Εταιρείες όπως η Symantec και η McAfee ξεκίνησαν να προσφέρουν προϊόντα antivirus και firewall για την προστασία των υπολογιστών από κακόβουλο λογισμικό. Τα προϊόντα αυτά έγιναν γρήγορα απαραίτητα για επιχειρήσεις και ιδιώτες, προσφέροντας προστασία από ιούς, σκουλήκια και άλλες μορφές κακόβουλου λογισμικού. Η βιομηχανία λογισμικού ασφαλείας αναπτύχθηκε και επεκτάθηκε ραγδαία κατά τη διάρκεια των επόμενων δεκαετιών . Επίσης δόθηκε μεγαλύτερη έμφαση στην εκπαίδευση και την ενημέρωση των χρηστών και των διαχειριστών συστημάτων σχετικά με τις απειλές και τις πρακτικές ασφαλείας. Τα συνέδρια, οι εκπαιδευτικές εκδηλώσεις και οι δημοσιεύσεις σε θέματα κυβερνοασφάλειας έγιναν πιο συχνά και λεπτομερή. Η ενημέρωση αυτή συνέβαλε στην αύξηση της επίγνωσης των κινδύνων και της ανάγκης για μέτρα προστασίας, κάτι που συνέβαλε σημαντικά στην πρόληψη των επιθέσεων (Kelty, 2011).

Η νομοθεσία ακόμη προσαρμόστηκε προκειμένου να αντιμετωπίσει το κυβερνοέγκλημα. Νέοι νόμοι και κανονισμοί θεσπίστηκαν για την προστασία των

δεδομένων και την επιβολή κυρώσεων στους παραβάτες. Ο Robert Morris ήταν ο πρώτος, ο οποίος καταδικάστηκε βάσει του Computer Fraud and Abuse Act, φανερώνοντας τη σοβαρότητα με την οποία αντιμετωπιζόταν πλέον το κυβερνοέγκλημα. Η αυστηρότερη νομοθεσία αποτέλεσε ένα ισχυρό αποτρεπτικό μέσο κατά των επιθέσεων (Kelty, 2011).

Η τεχνολογία εξελίχθηκε επίσης σημαντικά με την ανάπτυξη νέων μεθόδων κρυπτογράφησης, ελέγχου ταυτότητας και διαχείρισης πρόσβασης, βελτιώνοντας την ασφάλεια των συστημάτων. Νέα εργαλεία και τεχνικές αναπτύχθηκαν για την ανίχνευση και την αντιμετώπιση των απειλών σε πραγματικό χρόνο, συμβάλλοντας στην ενίσχυση της προστασίας των πληροφοριακών συστημάτων και της δικτυακής υποδομής (Kelty, 2011).

Κατά τη δεκαετία του 1990, οι τεχνολογίες ασφάλειας εξελίχθηκαν ραγδαία. Η δημιουργία των πρώτων firewalls και των συστημάτων ανίχνευσης εισβολών (IDS) ήταν καθοριστική. Το 1993, η Netscape Communications δημιούργησε το πρωτόκολλο SSL (Secure Sockets Layer) για την ασφαλή επικοινωνία μέσω του διαδικτύου (Γεωργιάδης, 2015).

Η δεκαετία του 2000 χαρακτηρίστηκε από την εξάπλωση των απειλών και την ανάπτυξη κανονιστικών πλαισίων. Το 2001, ο ιός "Code Red" μόλυνε εκατοντάδες χιλιάδες συστήματα μέσα σε λίγες ώρες (Moore, D., et al., 2002). Επιπλέον, η ψήφιση του νόμου Sarbanes-Oxley (SOX) στις ΗΠΑ το 2002 επέβαλε αυστηρές απαιτήσεις για την ασφάλεια των πληροφοριακών συστημάτων στις εταιρείες (Romano, S., 2003).

Σήμερα, οι κυβερνοεπιθέσεις γίνονται όλο και πιο εξελιγμένες, με τη χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης να αυξάνει τις δυνατότητες ανίχνευσης και αντιμετώπισης απειλών. Η πανδημία COVID-19 αύξησε την εξάρτηση από τις διαδικτυακές υπηρεσίες, ενισχύοντας την ανάγκη για ισχυρές πολιτικές και τεχνολογίες ασφάλειας (Hejase, 2021).

1.3 Σημασία κυβερνοασφάλειας

Η κυβερνοασφάλεια έχει καταστεί κρίσιμη για την προστασία των δεδομένων και την ασφάλεια των πληροφοριακών συστημάτων σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο. Η προστασία της οικονομικής ευημερίας αποτελεί έναν από τους κύριους λόγους που υπογραμμίζουν τη σημασία της κυβερνοασφάλειας. Οι κυβερνοεπιθέσεις μπορούν να οδηγήσουν σε σημαντικές οικονομικές απώλειες μέσω κλοπής δεδομένων, εκβιασμού και διακοπών λειτουργίας των επιχειρήσεων (Goutam, 2015).

Η διασφάλιση της επιχειρησιακής συνέχειας είναι εξίσου σημαντική. Οι διακοπές στις επιχειρησιακές δραστηριότητες λόγω κυβερνοεπιθέσεων μπορούν να επιφέρουν καταστροφικές συνέπειες. Μία επίθεση είναι δυνατόν να αναγκάσει μία επιχείρηση να σταματήσει τη λειτουργία της, να χάσει πελάτες, και να αντιμετωπίσει νομικά προβλήματα (Goutam, 2015).

Η κυβερνοασφάλεια δεν αφορά μόνο τις επιχειρήσεις. Ο κάθε πολίτης είναι ευάλωτος σε επιθέσεις οι οποίες καταλήγουν σε κλοπή ταυτότητας, απάτες και απώλεια προσωπικών δεδομένων. Η κλοπή ταυτότητας συμβαίνει όταν οι εγκληματίες αποκτούν πρόσβαση σε προσωπικές πληροφορίες, όπως αριθμούς κοινωνικής ασφάλισης, στοιχεία πιστωτικών καρτών ή άλλες ευαίσθητες

πληροφορίες, και τις χρησιμοποιούν για να διαπράξουν απάτες. Αυτές οι πληροφορίες μπορούν να κλαπούν μέσω επιθέσεων phishing, όπου οι χρήστες παραπλανούνται να αποκαλύψουν τα δεδομένα τους μέσω πλαστών emails ή ιστοσελίδων που μοιάζουν αξιόπιστα (Goutam, 2015).

Η ταχεία ανάπτυξη των τεχνολογιών καθιστά την κυβερνοασφάλεια μια συνεχώς αυξανόμενη πρόκληση. Παρά το γεγονός ότι αναπτύσσουμε διάφορα πλαίσια και τεχνολογίες για την προστασία των δικτύων και των πληροφοριών μας, αυτές οι λύσεις είναι συχνά προσωρινές και δεν παρέχουν μακροπρόθεσμη ασφάλεια. Παρόλα αυτά, η καλύτερη κατανόηση των θεμάτων ασφάλειας και η εφαρμογή κατάλληλων στρατηγικών μπορούν να μας βοηθήσουν να προστατεύσουμε την πνευματική ιδιοκτησία και τα εμπορικά μας μυστικά, καθώς και να μειώσουμε τις οικονομικές απώλειες και τις ζημιές στη φήμη μας (Goutam, 2015).

Οι κυβερνητικές αρχές, τόσο σε κεντρικό όσο και σε τοπικό επίπεδο, διαχειρίζονται μεγάλες ποσότητες δεδομένων και εμπιστευτικών αρχείων σε ψηφιακή μορφή. Αυτά τα δεδομένα αποτελούν κύριο στόχο για κυβερνοεπιθέσεις. Συχνά, οι κυβερνήσεις αντιμετωπίζουν δυσκολίες στην προστασία αυτών των πληροφοριών λόγω ανεπαρκών υποδομών, έλλειψης ευαισθητοποίησης σχετικά με τις απειλές και περιορισμένων χρηματοδοτικών πόρων. Για να διασφαλιστεί η παροχή αξιόπιστων υπηρεσιών στην κοινωνία, η διατήρηση υγιούς επικοινωνίας μεταξύ πολιτών και κυβέρνησης, καθώς και η προστασία των εμπιστευτικών πληροφοριών, είναι κρίσιμο οι κυβερνητικοί φορείς να επενδύσουν στις κατάλληλες τεχνολογίες και στρατηγικές κυβερνοασφάλειας (Goutam, 2015).

1.4 Βασικές αρχές της Κυβερνοασφάλειας

Η κυβερνοασφάλεια στηρίζεται σε τρεις θεμελιώδεις αρχές γνωστές ως "CIA Triad":

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα

Αυτές οι αρχές είναι κρίσιμες για τη διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων (Jang-Jaccard, 2014).

1.4.1 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα αφορά τη διασφάλιση ότι οι πληροφορίες είναι προσβάσιμες μόνο σε εξουσιοδοτημένα άτομα και συστήματα. Ο σκοπός είναι να προστατεύονται τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή. Μέτρα για την επίτευξη της εμπιστευτικότητας περιλαμβάνουν την κρυπτογράφηση δεδομένων, την εφαρμογή ισχυρών κωδικών πρόσβασης, την πολιτική ελέγχου πρόσβασης και την εκπαίδευση των χρηστών στην αναγνώριση και αποτροπή επιθέσεων phishing (Jang-Jaccard, 2014).

1.4.2 Ακεραιότητα (Integrity)

Η ακεραιότητα συνδέεται με τη διασφάλιση πως τα δεδομένα είναι ακριβή και αξιόπιστα και δεν έχουν υποστεί μη εξουσιοδοτημένη ή ακούσια τροποποίηση. Κάτι τέτοιο σημαίνει ότι τα δεδομένα χρειάζεται να παραμένουν αμετάβλητα από κακόβουλες επιθέσεις ή από σφάλματα συστημάτων. Μέτρα για την προστασία της ακεραιότητας περιλαμβάνουν τον έλεγχο πρόσβασης, την καταγραφή αλλαγών (logging), τη χρήση κρυπτογραφικών τεχνικών για την επαλήθευση της ακεραιότητας των δεδομένων και την εφαρμογή δικλείδων ασφαλείας, όπως η διπλή έγκριση αλλαγών στα κρίσιμα δεδομένα (Jang-Jaccard, 2014).

1.4.3 Διαθεσιμότητα (Availability)

Η διαθεσιμότητα διασφαλίζει ότι οι πληροφορίες και οι πόροι του συστήματος είναι προσβάσιμα όταν χρειάζονται από εξουσιοδοτημένους χρήστες. Αυτό σημαίνει ότι τα συστήματα πρέπει να λειτουργούν συνεχώς και να είναι ανθεκτικά σε διακοπές λειτουργίας. Μέτρα για την επίτευξη της διαθεσιμότητας περιλαμβάνουν τη χρήση εφεδρικών συστημάτων, τακτικά backup, την προστασία από επιθέσεις Denial of Service (DoS) και την εφαρμογή ανθεκτικών αρχιτεκτονικών συστημάτων που είναι σε θέση να αντιμετωπίσουν αποτυχίες και να συνεχίσουν να λειτουργούν (Jang-Jaccard, 2014).

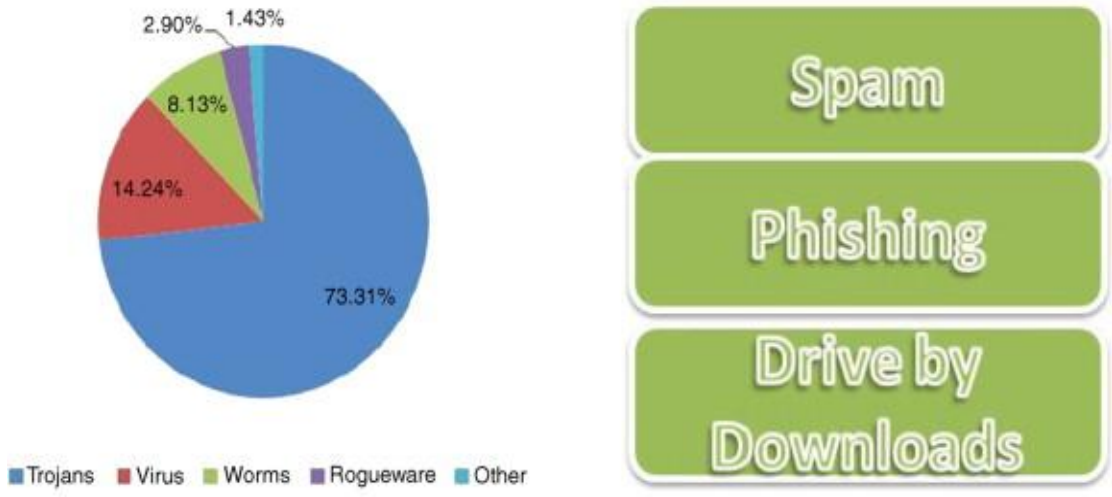
Κεφάλαιο 2. Κύριες Απειλές κατά της Κυβερνοασφάλειας

2.1 Κακόβουλο λογισμικό (malware)

Το κακόβουλο λογισμικό, ή malware, αποτελεί μία από τις κύριες απειλές για την κυβερνοασφάλεια. Περιλαμβάνει διάφορους τύπους λογισμικού που σχεδιάστηκαν για να προκαλέσουν βλάβη ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα. Οι κύριοι τύποι κακόβουλου λογισμικού περιλαμβάνουν τους εξής:

- Ιοί (Viruses): Οι ιοί είναι προγράμματα τα οποία επισυνάπτονται σε άλλα νόμιμα προγράμματα ή αρχεία και εκτελούνται όταν το μολυσμένο πρόγραμμα εκτελείται. Οι ιοί μπορούν να προκαλέσουν βλάβη στα αρχεία και τα προγράμματα ενός συστήματος, να διαγράψουν δεδομένα, ή να προκαλέσουν δυσλειτουργία του συστήματος.
- Δούρειοι Ίπποι (Trojans): Οι δούρειοι ίπποι είναι προγράμματα που φαίνονται αβλαβή ή χρήσιμα, αλλά στην πραγματικότητα περιέχουν κακόβουλο κώδικα, ο οποίος εκτελείται μόλις το πρόγραμμα εγκατασταθεί και εκτελεστεί. Αυτά τα προγράμματα συχνά χρησιμοποιούνται για να δημιουργήσουν "πίσω πόρτες" (backdoors) που επιτρέπουν την απομακρυσμένη πρόσβαση στον υπολογιστή του θύματος.
- Rogueware: Το rogueware, γνωστό επίσης ως rogue security software ή scareware, είναι μια μορφή κακόβουλου λογισμικού που παρουσιάζεται ως νόμιμο λογισμικό ασφαλείας ή υπηρεσία antivirus, με σκοπό να εξαπατήσει τους χρήστες ώστε να το κατεβάσουν και να το εγκαταστήσουν στον υπολογιστή τους. Αφού εγκατασταθεί, αυτό το λογισμικό συνήθως εμφανίζει ψευδείς προειδοποιήσεις ασφαλείας και ειδοποιήσεις για ιούς, προσπαθώντας να πείσει τους χρήστες να αγοράσουν την "πλήρη" έκδοση του λογισμικού για να επιλύσουν τα υποτιθέμενα προβλήματα.

- Σκουλήκια (Worms): Τα σκουλήκια είναι αυτόνομα προγράμματα τα οποία έχουν τη δυνατότητα να πολλαπλασιάζονται και να διαδίδονται από υπολογιστή σε υπολογιστή μέσω δικτύων. Σε αντίθεση με τους ιούς, δεν χρειάζεται να επισυνάπτονται σε άλλα προγράμματα ή αρχεία για να διαδοθούν. Συχνά εκμεταλλεύονται ευπάθειες στο λογισμικό προκειμένου να διαδοθούν και να προκαλέσουν καταστροφές.
- Ransomware: Το ransomware κρυπτογραφεί τα αρχεία του θύματος και απαιτεί την πληρωμή λύτρων για την αποκρυπτογράφηση και επαναφορά των αρχείων. Αυτή η μορφή επίθεσης έχει αυξηθεί σημαντικά τα τελευταία χρόνια, με πολλές επιθέσεις να στοχεύουν επιχειρήσεις, νοσοκομεία και κυβερνητικούς οργανισμούς.
- Spyware: Το spyware παρακολουθεί τη δραστηριότητα του χρήστη στον υπολογιστή και συλλέγει πληροφορίες χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Μπορεί να καταγράφει πληκτρολογήσεις, να συλλέγει ευαίσθητα δεδομένα όπως κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών, και να παρακολουθεί τη διαδικτυακή δραστηριότητα.
- Adware: Το adware εμφανίζει ανεπιθύμητες διαφημίσεις στον υπολογιστή του χρήστη και συχνά συνοδεύεται από άλλα είδη κακόβουλου λογισμικού. Παρόλο που το adware δεν είναι πάντα καταστροφικό, είναι δυνατόν να επιβραδύνει το σύστημα και να παρακολουθεί τη διαδικτυακή δραστηριότητα του χρήστη (Jang-Jaccard, 2014).



Εικόνα 1. Οι μορφές malware πηγή: Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993

Το κακόβουλο λογισμικό (malware) είναι σε θέση να μολύνει συστήματα με πολλούς τρόπους, οι οποίοι περιλαμβάνουν τη διάδοση από μολυσμένα μηχανήματα, την εξαπάτηση του χρήστη ώστε να ανοίξει μολυσμένα αρχεία, ή την επίσκεψη των χρηστών σε κακόβουλους ιστότοπους. Το κακόβουλο λογισμικό μπορεί ακόμη και να φορτωθεί σε μια μονάδα USB που έχει τοποθετηθεί σε μολυσμένη συσκευή και στη συνέχεια να μολύνει κάθε άλλο σύστημα στο οποίο θα εισαχθεί αυτή η μονάδα USB. Αυτός ο τρόπος διάδοσης είναι ιδιαίτερα επικίνδυνος, καθώς οι χρήστες συχνά δεν υποψιάζονται ότι μια φυσική συσκευή αποθήκευσης θα μπορούσε να είναι φορέας κακόβουλου λογισμικού (Jang-Jaccard, 2014).

Το κακόβουλο λογισμικό διαδίδεται επίσης μέσω συσκευών και εξοπλισμού που περιέχουν ενσωματωμένα συστήματα. Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται τις ευπάθειες σε τέτοιες συσκευές, ώστε να εισάγουν κακόβουλο κώδικα με επιβλαβείς συνέπειες ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δίκτυα και δεδομένα (Jang-Jaccard, 2014).

Η μόλυνση από κακόβουλο λογισμικό είναι δυνατόν να συμβεί σε οποιοδήποτε σημείο του κύκλου ζωής ενός συστήματος. Τα θύματα ενδέχεται να είναι συστήματα τελικού χρήστη, διακομιστές, συσκευές δικτύου (όπως δρομολογητές και μεταγωγείς), καθώς και συστήματα ελέγχου διεργασιών όπως ο Εποπτικός Έλεγχος και η Απόκτηση Δεδομένων (SCADA). Τα συγκεκριμένα συστήματα είναι συχνά στόχος, καθώς η λειτουργία τους είναι κρίσιμη για πολλές βιομηχανίες και υποδομές (Jang-Jaccard, 2014).

Η ταχεία αύξηση και η πολυπλοκότητα του κακόβουλου λογισμικού αποτελεί σημαντική ανησυχία στο διαδίκτυο σήμερα. Οι επιθέσεις κακόβουλου λογισμικού συνεχώς εξελίσσονται, καθιστώντας την προστασία των συστημάτων και των

δεδομένων όλο και πιο δύσκολη. Οι επιθέσεις αυτές επιφέρουν σοβαρές συνέπειες, όπως η απώλεια δεδομένων, η παραβίαση της ιδιωτικότητας και η διακοπή των επιχειρησιακών διαδικασιών. Ως εκ τούτου, η ανάγκη για αποτελεσματικά μέτρα προστασίας και πρόληψης είναι πιο επιτακτική από ποτέ (Jang-Jaccard, 2014).

2.2 Επιθέσεις Phishing

Οι επιθέσεις phishing είναι ένας από τους πιο διαδεδομένους και επικίνδυνους τύπους κυβερνοεπιθέσεων με κύριο στόχο την εξαπάτηση των χρηστών για να αποκαλύψουν ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης, στοιχεία πιστωτικών καρτών, και προσωπικά δεδομένα. Η λέξη "phishing" προέρχεται από το "fishing" (ψάρεμα), υποδηλώνοντας ότι οι επιτιθέμενοι "ψαρεύουν" για πληροφορίες μέσω απατηλών μηνυμάτων (Alkhalil et al., 2021).

Στις περισσότερες επιθέσεις phishing, η διαδικασία ξεκινά με τη συλλογή πληροφοριών σχετικά με τον στόχο. Αυτή είναι η αρχική φάση της προετοιμασίας, όπου ο επιτιθέμενος (phisher) ερευνά για να βρει λεπτομέρειες που μπορεί να χρησιμοποιήσει για να παραπλανήσει το θύμα του. Αυτές οι πληροφορίες μπορεί να προέρχονται από τα μέσα κοινωνικής δικτύωσης, δημόσια αρχεία ή άλλα ανοιχτά δεδομένα. Έπειτα ο phisher αποφασίζει ποια μέθοδος επίθεσης θα χρησιμοποιηθεί, όπως η αποστολή ενός δόλιου email που φαίνεται να προέρχεται από μια νόμιμη πηγή, όπως μια τράπεζα ή μια γνωστή εταιρεία, ή την κατασκευή μιας ψεύτικης ιστοσελίδας που μιμείται μια αυθεντική (Alkhalil et al., 2021).

Ακολουθεί η φάση προετοιμασίας. Κατά τη διάρκεια της φάσης προετοιμασίας, ο phisher αρχίζει να ψάχνει για τρωτά σημεία μέσω των οποίων θα μπορούσε να παγιδεύσει το θύμα. Ενδέχεται για παράδειγμα να επιλέξει τη

δημιουργία ενός δόλιου email που περιέχει έναν σύνδεσμο σε μια ψεύτικη ιστοσελίδα ή τη χρήση κακόβουλου λογισμικού το οποίο εγκαθίσταται στον υπολογιστή του θύματος όταν ανοίξει ένα συνημμένο αρχείο (Alkhalil et al., 2021).

Στη φάση της επίθεσης, ο phisher στέλνει το email ή μήνυμα και περιμένει απάντηση από το θύμα. Για παράδειγμα, ένας εισβολέας είναι πιθανόν να στείλει ένα email στο οποίο προσποιείται ότι είναι από την τράπεζα του θύματος, ζητώντας από τον χρήστη να επιβεβαιώσει τα στοιχεία του τραπεζικού λογαριασμού, διαφορετικά ο λογαριασμός μπορεί να ανασταλεί. Το email αυτό θα χρησιμοποιεί τα ίδια γραφικά στοιχεία, εμπορικά σήματα και χρώματα της νόμιμης τράπεζας προκειμένου να φαίνεται πιστευτό (Alkhalil et al., 2021).

Εάν το θύμα πέσει στην παγίδα και υποβάλει τα στοιχεία του, αυτά θα μεταδοθούν απευθείας στον phisher. Ο εισβολέας είναι σε θέση να χρησιμοποιήσει τις πληροφορίες για διάφορους κακόβουλους σκοπούς, όπως η ανάληψη χρημάτων από τον τραπεζικό λογαριασμό του θύματος, η χρήση των δεδομένων για εκβιασμό ή η διάπραξη περαιτέρω απάτης (Alkhalil et al., 2021).

Με τη συνεχή εκπαίδευση και την ενίσχυση της ευαισθητοποίησης σχετικά με τις επιθέσεις phishing, οι χρήστες μπορούν να αναγνωρίσουν τα σημάδια αυτών των επιθέσεων και να προστατεύσουν καλύτερα τις πληροφορίες τους από τους κακόβουλους επιτιθέμενους (Alkhalil et al., 2021).

Εικόνα 2. Η διαδικασία του phising, πηγή: Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060

2.3 Επιθέσεις DOS/DDoS

Οι επιθέσεις Άρνησης Υπηρεσίας (Denial-of-Service ή DoS) εκμεταλλεύονται το διαδίκτυο για να στοχεύσουν κρίσιμες υπηρεσίες διαδικτύου. Αυτός ο τύπος επίθεσης έχει ως σκοπό να αποτρέψει τους νόμιμους χρήστες από την πρόσβαση σε συγκεκριμένους δικτυακούς πόρους ή να υποβαθμίσει τις κανονικές υπηρεσίες για τους νόμιμους χρήστες, στέλνοντας τεράστια ανεπιθύμητη κυκλοφορία στο θύμα (υπολογιστές ή δίκτυα) ώστε να εξαντληθούν οι υπηρεσίες και η χωρητικότητα των συνδέσεων ή το εύρος ζώνης (Eliyan & Di Pietro, 2021).

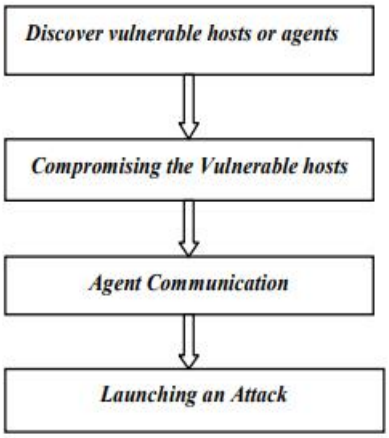
Οι επιθέσεις DoS επιδιώκουν να κατακλύσουν το δίκτυο ή τον διακομιστή του στόχου με υπερβολική κυκλοφορία, προκαλώντας την εξάντληση των πόρων του

συστήματος, όπως το εύρος ζώνης και η επεξεργαστική ισχύς. Αυτό έχει ως αποτέλεσμα τη μείωση της ταχύτητας ή ακόμη και τη διακοπή της λειτουργίας των υπηρεσιών. Οι επιτιθέμενοι μπορεί να εκμεταλλευτούν ευπάθειες λογισμικού για να προκαλέσουν δυσλειτουργίες στο σύστημα του στόχου, επιτυγχάνοντας με αυτόν τον τρόπο άρνηση υπηρεσίας. Η επίθεση πραγματοποιείται μέσω της αποστολής ειδικά διαμορφωμένων αιτήσεων, οι οποίες προκαλούν σφάλματα στο λογισμικό του στόχου (Prasad et al., 2014).

Στην περίπτωση των κατανεμημένων επιθέσεων άρνησης υπηρεσίας (Distributed Denial-of-Service ή DDoS), η επίθεση πραγματοποιείται από πολλαπλά συστήματα που είναι διασκορπισμένα στο διαδίκτυο. Αυτά τα συστήματα, γνωστά ως "bots" ή "zombies," είναι συνήθως μολυσμένα με κακόβουλο λογισμικό και ελέγχονται από τον επιτιθέμενο. Οι επιθέσεις αυτές στο διαδίκτυο μπορούν να εκτελεστούν χρησιμοποιώντας δύο κύριες μεθόδους. Στην πρώτη μέθοδο, ο επιτιθέμενος στέλνει κακόβουλα πακέτα στο θύμα για να μπερδέψει ένα πρωτόκολλο ή μια εφαρμογή που εκτελείται σε αυτό (δηλαδή, επίθεση εκμετάλλευσης ευπαθειών). Η δεύτερη μέθοδος περιλαμβάνει ουσιαστικά τις επιθέσεις κατακλυσμού σε επίπεδο δικτύου/μεταφοράς/εφαρμογών, στις οποίες ο επιτιθέμενος μπορεί να κάνει ένα ή και τα δύο από τα ακόλουθα: (i) να διακόψει τη συνδεσιμότητα ενός νόμιμου χρήστη εξαντλώντας το εύρος ζώνης, τους πόρους δικτύου ή την ικανότητα επεξεργασίας δρομολογητών ή (ii) να διακόψει τις υπηρεσίες ενός νόμιμου χρήστη εξαντλώντας τους πόρους του διακομιστή όπως η CPU, η μνήμη, το εύρος ζώνης του δίσκου/βάσης δεδομένων και το εύρος ζώνης εισόδου/εξόδου (Prasad et al., 2014).

Μια επίθεση Κατανεμημένης Άρνησης Υπηρεσίας (DDoS) αποτελείται από διάφορα στοιχεία. Μπορεί να πραγματοποιηθεί μέσω διαφόρων πρωτοκόλλων όπως TCP, UDP ή ICMP και βασίζεται στη διαμόρφωση του δικτύου με έναν ή

περισσότερους διαχειριστές. Ο επιτιθέμενος ξεκινά την επίθεση επιλέγοντας το σύστημα-στόχο, τη διάρκεια της επίθεσης και προσαρμόζοντας τα χαρακτηριστικά της επίθεσης όπως ο τύπος, η διάρκεια, το Time to Live (TTL) και οι αριθμοί θυρών (Prasad et al., 2014).

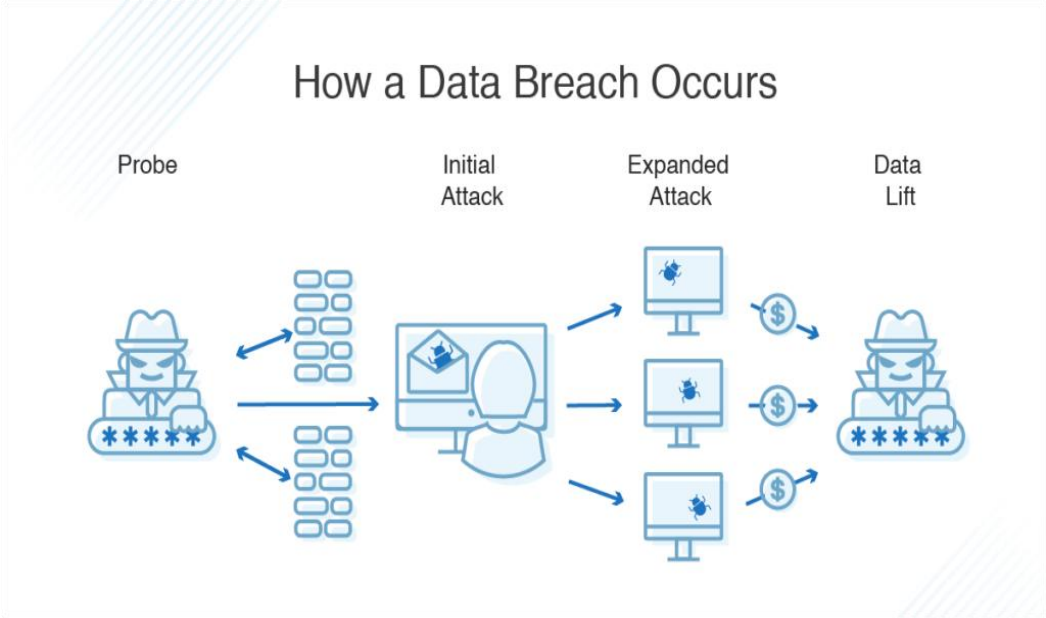


Εικόνα 3, Οι φάσεις των επιθέσεων DDOS, πηγή: Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. Global Journal of Computer Science and Technology, 14(7), 15-32.

2.4 Παραβιάσεις Δεδομένων (Data Breaches)

Οι παραβιάσεις δεδομένων αποτελούν μία από τις πιο σοβαρές απειλές στην κυβερνοασφάλεια, καθώς μπορούν να έχουν καταστροφικές συνέπειες για άτομα, επιχειρήσεις και οργανισμούς. Μία παραβίαση δεδομένων συμβαίνει όταν ευαίσθητες, προστατευμένες ή εμπιστευτικές πληροφορίες εκτίθενται σε ένα μη εξουσιοδοτημένο άτομο. Τέτοιες πληροφορίες είναι τα προσωπικά δεδομένα, οικονομικές πληροφορίες, ιατρικά αρχεία, πνευματική ιδιοκτησία και άλλες ευαίσθητες πληροφορίες (Zhang et al., 2022).

Συχνά, οι παραβιάσεις δεδομένων οφείλονται σε ανθρώπινα λάθη, όπως η αποστολή ευαίσθητων πληροφοριών σε λάθος παραλήπτη ή η χρήση αδύναμων κωδικών πρόσβασης. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν κακόβουλο λογισμικό, όπως είδαμε προηγουμένως, για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Το κακόβουλο λογισμικό μπορεί να εγκατασταθεί σε ένα σύστημα μέσω επιθέσεων phishing ή άλλων μορφών εξαπάτησης. Εργαζόμενοι ή πρώην εργαζόμενοι ενδέχεται επίσης να αποτελέσουν απειλή, εάν έχουν κακές προθέσεις και πρόσβαση σε ευαίσθητες πληροφορίες (Zhang et al., 2022).



Εικόνα 4, Πώς πραγματοποιείται η παραβίαση δεδομένων, πηγή: https://www.dnsstuff.com/data-breach-101

Οι συνέπειες των παραβιάσεων δεδομένων μπορεί να είναι καταστροφικές, περιλαμβάνοντας οικονομικές απώλειες, βλάβη στη φήμη και νομικές επιπτώσεις για τους οργανισμούς. Οι επιχειρήσεις ίσως καταλήξουν να χάσουν την εμπιστοσύνη των πελατών τους και να αντιμετωπίσουν σημαντικά πρόστιμα και κυρώσεις λόγω της μη συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων. Για να προστατευτούν από τις παραβιάσεις δεδομένων, οι οργανισμοί είναι απαραίτητο να εφαρμόζουν αυστηρές πολιτικές ασφάλειας, να εκπαιδεύουν τους εργαζομένους τους και να

χρησιμοποιούν προηγμένα τεχνολογικά μέσα για την ανίχνευση και αποτροπή των επιθέσεων (Zhang et al., 2022).

2.5 Κοινωνική Μηχανική (Social Engineering)

Οι επιθέσεις κοινωνικής μηχανικής αυξάνονται ραγδαία στα σημερινά δίκτυα και αποδυναμώνουν την αλυσίδα της κυβερνοασφάλειας. Σκοπός τους είναι να χειραγωγήσουν άτομα και επιχειρήσεις ώστε να αποκαλύψουν πολύτιμα και ευαίσθητα δεδομένα προς όφελος των κυβερνοεγκληματιών. Η κοινωνική μηχανική αποτελεί πρόκληση για την ασφάλεια όλων των δικτύων, ανεξάρτητα από την ανθεκτικότητα των firewalls, των μεθόδων κρυπτογράφησης, των συστημάτων ανίχνευσης εισβολών και των προγραμμάτων προστασίας από ιούς. Οι άνθρωποι είναι πιο πιθανό να εμπιστευτούν άλλους ανθρώπους σε σύγκριση με τους υπολογιστές ή τις τεχνολογίες. Επομένως, αποτελούν τον αδύναμο κρίκο στην αλυσίδα της ασφάλειας. Οι κακόβουλες δραστηριότητες που πραγματοποιούνται μέσω ανθρώπινων αλληλεπιδράσεων επηρεάζουν ένα άτομο ψυχολογικά ώστε να αποκαλύψει εμπιστευτικές πληροφορίες ή να παραβιάσει τις διαδικασίες ασφάλειας (Salahdine & Kaabouch, 2019).

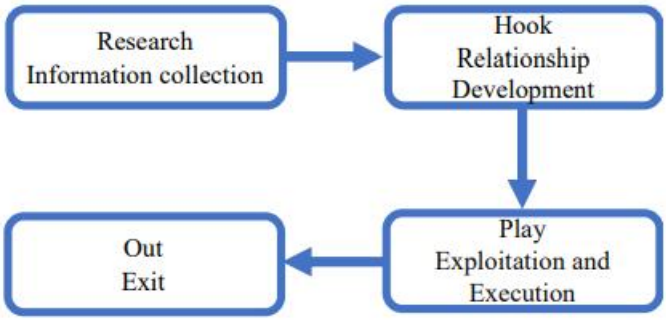
Αν και οι επιθέσεις κοινωνικής μηχανικής διαφέρουν μεταξύ τους, έχουν ένα κοινό μοτίβο με παρόμοιες φάσεις. Το κοινό μοτίβο περιλαμβάνει τέσσερις φάσεις:

(1) συλλογή πληροφοριών για τον στόχο

(2) ανάπτυξη σχέσης με τον στόχο

(3) εκμετάλλευση των διαθέσιμων πληροφοριών και εκτέλεση της επίθεσης

(4) έξοδος χωρίς να αφήνουν ίχνη.



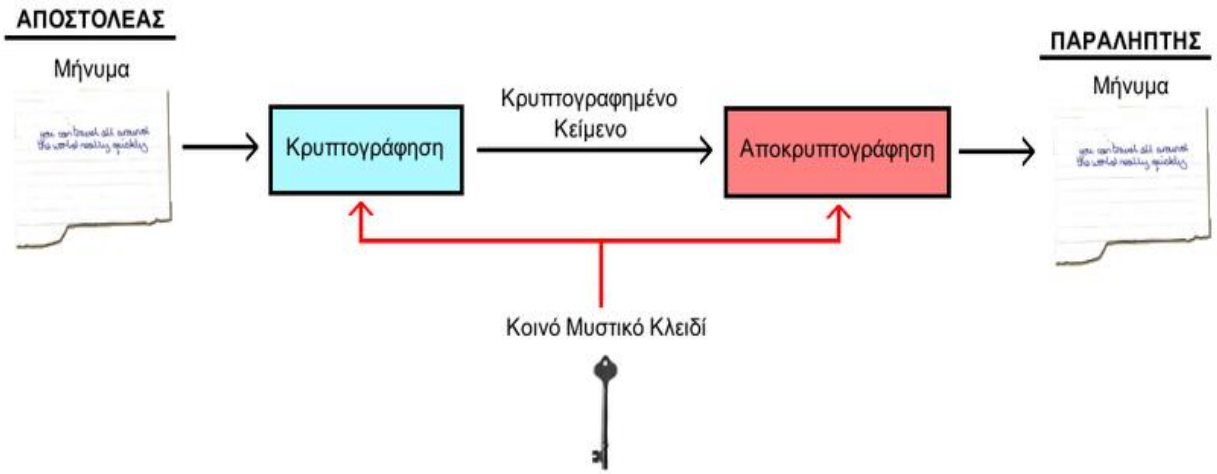
Εικόνα 5, Οι φάσεις των επιθέσεων κοινωνικής μηχανικής, πηγή: Segovia, L., Torres, F., Rosillo, M., Tapia, E., Albarado, F., & Saltos, D. (2017). Social engineering as an attack vector for ransomware. In Proceedings of the Conference on Electrical Engineering and Information Communication Technology (pp. 1-6). Pucon, Chile.

Οι επιθέσεις κοινωνικής μηχανικής μπορούν να χωριστούν σε κατηγορίες ανάλογα με την εμπλεκόμενη οντότητα (άνθρωπος ή λογισμικό) και τον τρόπο διεξαγωγής (κοινωνικές, τεχνικές, φυσικές επιθέσεις). Μπορούν επίσης να ταξινομηθούν ως άμεσες ή έμμεσες. Άμεσες επιθέσεις περιλαμβάνουν φυσική επαφή, παρακολούθηση, και τηλεφωνική εξαπάτηση. Έμμεσες επιθέσεις πραγματοποιούνται εξ αποστάσεως μέσω κακόβουλου λογισμικού σε email ή SMS (Salahdine & Kaabouch, 2019).

Κεφάλαιο 3. Τεχνολογίες και Μέθοδοι Κυβερνοασφάλειας

3.1 Κρυπτογράφηση (Encryption)

Η κρυπτογράφηση είναι μια θεμελιώδης τεχνολογία της κυβερνοασφάλειας που προστατεύει την εμπιστευτικότητα των δεδομένων. Αποτελεί τη διαδικασία μετατροπής των δεδομένων σε κώδικα, ώστε μόνο τα εξουσιοδοτημένα μέρη να μπορούν να τα αποκρυπτογραφήσουν και να τα κατανοήσουν. Η κρυπτογράφηση χρησιμοποιεί αλγόριθμους και κρυπτογραφικά κλειδιά για να διασφαλίσει ότι τα δεδομένα παραμένουν ασφαλή από μη εξουσιοδοτημένη πρόσβαση, ακόμη και αν αυτά τα δεδομένα υποκλαπούν (Diffie & Hellman, 2022).



Εικόνα 6, Η διαδικασία της κρυπτογράφησης, πηγή: https://el.wikipedia.org

Υπάρχουν δύο κύριοι τύποι κρυπτογράφησης: η συμμετρική και η ασύμμετρη κρυπτογράφηση. Η συμμετρική κρυπτογράφηση χρησιμοποιεί το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Αυτό σημαίνει ότι τα εμπλεκόμενα μέρη πρέπει να διατηρούν το κλειδί ασφαλές και να το μοιράζονται με ασφάλεια. Η ασύμμετρη κρυπτογράφηση, από την άλλη πλευρά, χρησιμοποιεί δύο διαφορετικά κλειδιά: ένα δημόσιο κλειδί για την κρυπτογράφηση

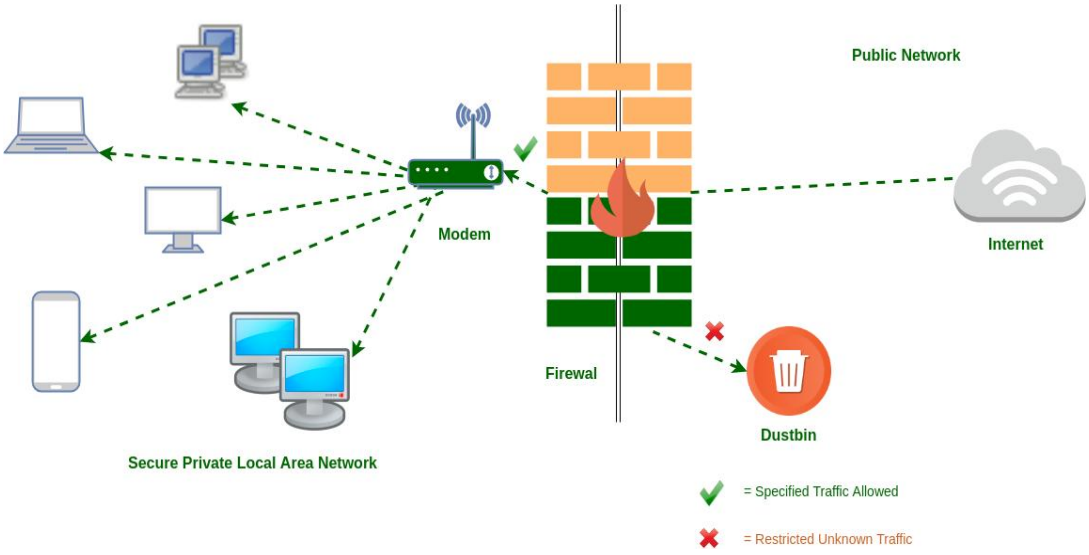
και ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση. Αυτό επιτρέπει την ασφαλή επικοινωνία χωρίς την ανάγκη ανταλλαγής του ιδιωτικού κλειδιού (Diffie & Hellman, 2022).

Η κρυπτογράφηση διαδραματίζει κρίσιμο ρόλο στην προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων σε πολλούς τομείς, όπως οι χρηματοοικονομικές συναλλαγές, η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, και οι διαδικτυακές αγορές. Επιπλέον, είναι απαραίτητη για τη συμμόρφωση με κανονισμούς και νομοθεσίες περί προστασίας δεδομένων, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση (Diffie & Hellman, 2022).

Στη σύγχρονη εποχή, η κρυπτογράφηση έχει εξελιχθεί σημαντικά για να ανταποκριθεί στις αυξημένες απαιτήσεις ασφάλειας και τις νέες προκλήσεις που προκύπτουν από την ψηφιακή μεταμόρφωση. Η κρυπτογράφηση με καμπύλες ελλείψεως (Elliptic Curve Cryptography, ECC) είναι μία από τις πιο προηγμένες μορφές κρυπτογράφησης που χρησιμοποιούνται σήμερα. Η ECC προσφέρει ισχυρή ασφάλεια με μικρότερα κλειδιά σε σύγκριση με άλλες μεθόδους, όπως η RSA, καθιστώντας την ιδανική για εφαρμογές όπου η αποδοτικότητα και η ταχύτητα είναι κρίσιμες. Η ανάπτυξη κβαντικών υπολογιστών έχει οδηγήσει σε έρευνες για κρυπτογράφηση ανθεκτική σε κβαντικούς υπολογιστές (post-quantum cryptography). Αυτή η νέα μορφή κρυπτογράφησης στοχεύει να προστατεύσει τα δεδομένα από την υπολογιστική δύναμη των μελλοντικών κβαντικών υπολογιστών οι οποίοι είναι ευκολότερο να σπάσουν τις παραδοσιακές κρυπτογραφικές μεθόδους (Bernstein et al., 2008).

3.2 Τείχη προστασίας (firewalls)

Ένα τείχος προστασίας (firewall) είναι μια ηλεκτρονική συσκευή ή ένα λογισμικό που ελέγχει τη ροή δεδομένων και πληροφοριών που μπαίνουν ή βγαίνουν από ένα δίκτυο. Ο σκοπός του είναι να αποτρέπει την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο από κακόβουλους χρήστες, αποτρέποντας έτσι την απώλεια δεδομένων και την εκμετάλλευση των υπηρεσιών του δικτύου (Hayajne et al., 2013).



Εικόνα 7, Τείχος προστασίας, πηγή: https://novelcomm.gr/firewall-security/

Σε ένα υπολογιστικό δίκτυο, τα τείχη προστασίας λειτουργούν ως φύλακες, εξετάζοντας όλα τα δεδομένα που εισέρχονται και εξέρχονται για να αποφασίσουν αν πρέπει να επιτραπούν ή όχι, σύμφωνα με ένα σύνολο προκαθορισμένων κανόνων. Η βασική ιδέα πίσω από τα τείχη προστασίας είναι να δημιουργήσουν ένα φράγμα ανάμεσα σε ένα εσωτερικό, ιδιωτικό και ασφαλές δίκτυο, και στον εξωτερικό κόσμο, δηλαδή το διαδίκτυο, το οποίο θεωρείται δημόσιο, μη αξιόπιστο και γεμάτο κινδύνους (Hayajne et al., 2013).

Τα τείχη προστασίας διακρίνονται γενικά σε προσωπικά και δικτυακά τείχη προστασίας. Τα προσωπικά, ή αλλιώς "host-based", τείχη προστασίας είναι συνήθως εφαρμογές λογισμικού που εγκαθίστανται για να τρέχουν στο λειτουργικό σύστημα. Στις μέρες μας, τα περισσότερα λειτουργικά συστήματα διαθέτουν ενσωματωμένα τείχη προστασίας. Τα προσωπικά τείχη προστασίας γίνονται όλο και πιο δημοφιλή και στοχεύουν στην προστασία μεμονωμένων συσκευών από κακόβουλα πακέτα δεδομένων, εκτελώντας φιλτράρισμα πακέτων σε επίπεδο συσκευής (Hayajne et al., 2013).

Συναντώνται οι ακόλουθες κατηγορίες Τειχών Προστασίας:

- Packet Filtering Firewalls: Αυτά τα τείχη προστασίας λειτουργούν στο επίπεδο του δικτυακού πρωτοκόλλου και επιτρέπουν ή απορρίπτουν την κίνηση δεδομένων με βάση προκαθορισμένους κανόνες. Εξετάζουν τα πακέτα δεδομένων και αποφασίζουν εάν θα επιτρέψουν ή θα απορρίψουν την κίνησή τους με βάση την IP διεύθυνση, το πρωτόκολλο, και τον αριθμό θύρας.

- Stateful Inspection Firewalls: Τα συγκεκριμένα firewalls παρακολουθούν τη ροή δεδομένων σε όλη τη διάρκεια της σύνδεσης, λαμβάνοντας υπόψη την κατάσταση κάθε σύνδεσης. Έτσι, μπορούν να αναγνωρίσουν και να αποτρέψουν πιο εξελιγμένες επιθέσεις που δεν μπορούν να αντιμετωπιστούν μόνο με την ανάλυση των μεμονωμένων πακέτων δεδομένων.

- Proxy Firewalls: Αυτό το είδος τειχών προστασίας λειτουργεί ως μεσάζοντας μεταξύ του εσωτερικού δικτύου και του εξωτερικού δικτύου. Όλες οι συνδέσεις και οι αιτήσεις δεδομένων περνούν πρώτα από το proxy firewall, το οποίο αξιολογεί και καθαρίζει την κίνηση πριν την προωθήσει στο εσωτερικό δίκτυο. Τα proxy firewalls είναι γνωστά για την ικανότητά τους να προσφέρουν καλύτερη ανωνυμία και προστασία από ορισμένες μορφές επιθέσεων.

- Next-Generation Firewalls (NGFW): Τα σύγχρονα τείχη προστασίας επόμενης γενιάς συνδυάζουν την παραδοσιακή λειτουργικότητα με προηγμένες δυνατότητες, όπως η επιθεώρηση εφαρμογών, η ενσωμάτωση με συστήματα πρόληψης εισβολών (IPS), και η ανάλυση των απειλών σε πραγματικό χρόνο. Αυτά τα τείχη προστασίας είναι σχεδιασμένα για να αντιμετωπίζουν τις σύγχρονες, πολυδιάστατες απειλές που εμφανίζονται στο διαδίκτυο.

3.3 Ανίχνευση και Πρόληψη Εισβολών (IDS/IPS)

Η ανίχνευση και πρόληψη εισβολών (IDS/IPS) αποτελεί μια ιδιαιτέρως σημαντική πτυχή της κυβερνοασφάλειας, με σκοπό την προστασία των συστημάτων και δικτύων από κακόβουλες επιθέσεις. Τα συστήματα IDS και IPS λειτουργούν ως φράγματα ασφαλείας τα οποία ανιχνεύουν και αποτρέπουν επιθέσεις σε πραγματικό χρόνο, προσφέροντας ένα επιπλέον επίπεδο προστασίας πέρα από τα τείχη προστασίας (Ashoor & Gore, 2012).

Ανίχνευση Εισβολών (IDS)

Τα συστήματα Ανίχνευσης Εισβολών (IDS) είναι σχεδιασμένα για να παρακολουθούν την κίνηση του δικτύου και να εντοπίζουν ύποπτες δραστηριότητες που μπορεί να υποδηλώνουν μια επίθεση. Ένα IDS μπορεί να είναι είτε δικτυακό (NIDS), το οποίο παρακολουθεί την κίνηση του δικτύου, είτε κεντρικό (HIDS), το οποίο παρακολουθεί τις δραστηριότητες ενός συγκεκριμένου συστήματος ή διακομιστή.

Το IDS λειτουργεί αναλύοντας την κίνηση του δικτύου ή τις καταγραφές του συστήματος για μοτίβα που ταιριάζουν με γνωστές επιθέσεις. Χρησιμοποιεί υπογραφές (signatures) ή ανωμαλίες (anomalies) για να εντοπίσει τις ύποπτες δραστηριότητες. Όταν εντοπιστεί μια πιθανή εισβολή, το IDS στέλνει ειδοποιήσεις

στους διαχειριστές συστήματος ώστε να ληφθούν τα απαραίτητα μέτρα. Ωστόσο, το IDS δεν λαμβάνει ενεργά μέτρα για να σταματήσει την επίθεση.

- Πρόληψη Εισβολών (IPS)

Τα συστήματα Πρόληψης Εισβολών (IPS) λειτουργούν παρόμοια με τα IDS, με τη διαφορά ότι τα IPS μπορούν να λάβουν ενεργά μέτρα για να σταματήσουν την επίθεση.

Συγκεκριμένα, Το IPS παρακολουθεί την κίνηση του δικτύου σε πραγματικό χρόνο και μπορεί να μπλοκάρει ή να απορρίψει κακόβουλες πακέτες δεδομένων, σταματώντας τις επιθέσεις πριν φτάσουν στους στόχους τους. Εκτός από την ανίχνευση, το IPS είναι σε θέση να προσαρμόζει δυναμικά τους κανόνες του για να αποκλείσει επιθέσεις, αποτρέποντας την εξάπλωσή τους στο δίκτυο.

Συχνά, τα συστήματα IDS και IPS χρησιμοποιούνται σε συνδυασμό για να παρέχουν μια ολοκληρωμένη λύση ασφάλειας. Ο συνδυασμός αυτός επιτρέπει τόσο την ανίχνευση όσο και την πρόληψη επιθέσεων, εξασφαλίζοντας την καλύτερη δυνατή προστασία.

3.4 Έλεγχος Πρόσβασης (Access Control)

Ο έλεγχος πρόσβασης είναι μια βασική τεχνική ασφάλειας, η οποία καθορίζει ποιος ή τι μπορεί να δει ή να χρησιμοποιήσει πόρους σε ένα υπολογιστικό περιβάλλον. Είναι ένας θεμελιώδης μηχανισμός στην ασφάλεια των πληροφοριών που διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε συγκεκριμένους πόρους. Οι κύριες έννοιες του ελέγχου πρόσβασης περιλαμβάνουν την ταυτοποίηση και την εξουσιοδότηση. Η ταυτοποίηση είναι η διαδικασία επιβεβαίωσης της ταυτότητας ενός

χρήστη, ενώ η εξουσιοδότηση καθορίζει τα δικαιώματα που έχει ένας ταυτοποιημένος χρήστης (Mahalle et al., 2013).

Υπάρχουν διάφορα μοντέλα ελέγχου πρόσβασης. Το Εκλεκτικό Μοντέλο (Discretionary Access Control, DAC) βασίζεται στην ταυτότητα των χρηστών και στις λίστες ελέγχου πρόσβασης (ACL). Στο Υποχρεωτικό Μοντέλο (Mandatory Access Control, MAC), η πρόσβαση βασίζεται σε προκαθορισμένες πολιτικές που επιβάλλονται από μια κεντρική αρχή. Το Μοντέλο βάσει Ρόλων (Role-Based Access Control, RBAC) αναθέτει στους χρήστες ρόλους και τα δικαιώματα συνδέονται με αυτούς τους ρόλους. Το Μοντέλο βάσει Χαρακτηριστικών (Attribute-Based Access Control, ABAC) βασίζεται σε χαρακτηριστικά όπως χαρακτηριστικά χρηστών, πόρων και περιβαλλοντικά χαρακτηριστικά, παρέχοντας πιο λεπτομερή έλεγχο (Mahalle et al., 2013).

Οι πολιτικές ελέγχου πρόσβασης περιλαμβάνουν το ελάχιστο δικαίωμα, το οποίο υποδεικνύει ότι οι χρήστες πρέπει να έχουν το ελάχιστο επίπεδο πρόσβασης που είναι απαραίτητο για την εκτέλεση των καθηκόντων τους, και τον διαχωρισμό καθηκόντων, ο οποίος διαιρεί τα καθήκοντα και τα δικαιώματα μεταξύ πολλαπλών χρηστών για την αποτροπή της απάτης και των λαθών (Mahalle et al., 2013).

3.5 Διαχείριση Ταυτότητας και Πρόσβασης (Identity and Access Management - IAM)

Η Διαχείριση Ταυτότητας και Πρόσβασης (Identity and Access Management - IAM) είναι μια θεμελιώδης πτυχή της κυβερνοασφάλειας που διασφαλίζει ότι τα κατάλληλα άτομα έχουν πρόσβαση στους κατάλληλους πόρους τη σωστή στιγμή και για τους σωστούς λόγους. Η IAM περιλαμβάνει διαδικασίες, τεχνολογίες και

πολιτικές, οι οποίες χρησιμοποιούνται με στόχο τη διαχείριση των ψηφιακών ταυτοτήτων και των δικαιωμάτων πρόσβασης (Singh et al., 2023).

Η IAM αρχίζει με την ταυτότητα, που αφορά τη δημιουργία και τον χειρισμό μοναδικών ψηφιακών ταυτοτήτων για χρήστες, συσκευές ή εφαρμογές. Κάθε ταυτότητα έχει ένα σύνολο διαπιστευτηρίων, όπως ονόματα χρήστη και κωδικούς πρόσβασης, που χρησιμοποιούνται για την επαλήθευση της ταυτότητας του χρήστη ή της συσκευής. Μετά την επαλήθευση, η IAM προχωρά στον έλεγχο της πρόσβασης, ο οποίος καθορίζει ποιοι πόροι και υπηρεσίες είναι προσβάσιμοι για την ταυτοποιημένη οντότητα. Αυτό επιτυγχάνεται μέσω κανόνων και πολιτικών που καθορίζουν τα δικαιώματα πρόσβασης βάσει των ρόλων και των ευθυνών του χρήστη εντός του οργανισμού (Singh et al., 2023).

Σημαντικός ρόλος της IAM είναι η διαχείριση του κύκλου ζωής της ταυτότητας, η οποία αφορά τη δημιουργία, τη συντήρηση και την απόσυρση των ταυτοτήτων. Οι διαδικασίες αυτές διασφαλίζουν ότι οι ταυτότητες είναι ενημερωμένες και ότι οι χρήστες έχουν πρόσβαση μόνο στους πόρους που χρειάζονται για την εκτέλεση των καθηκόντων τους. Επιπλέον η IAM ελέγχει την ταυτότητα πολλαπλών παραγόντων (MFA), προσθέτοντας ένα επιπλέον επίπεδο ασφάλειας απαιτώντας περισσότερες από μία μορφές επαλήθευσης πριν επιτραπεί η πρόσβαση (Singh et al., 2023).

Η IAM επιτρέπει την ανίχνευση και την απόκριση σε περιστατικά που κλονίζουν την ασφάλεια, όπως προσπάθειες μη εξουσιοδοτημένης πρόσβασης, μέσω καταγραφής και παρακολούθησης δραστηριοτήτων χρηστών. Οι πληροφορίες αυτές χρησιμοποιούνται για τη διερεύνηση και την αντιμετώπιση παραβιάσεων ασφαλείας. Επιπλέον, η IAM συμβάλλει στη συμμόρφωση με κανονιστικές απαιτήσεις, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), επιβεβαιώνοντας ότι οι

οργανισμοί ακολουθούν τις απαιτούμενες διαδικασίες για την προστασία των προσωπικών δεδομένων (Singh et al., 2023).

Η τεχνολογία IAM έχει λογισμικό και συστήματα όπως καταλόγους υπηρεσιών (LDAP), συστήματα ελέγχου πρόσβασης βάσει ρόλων (RBAC), και πλατφόρμες ταυτοποίησης ως υπηρεσία (IDaaS). Οι λύσεις αυτές είναι δυνατόν να ενσωματωθούν σε διάφορες υποδομές πληροφορικής, όπως τοπικά δίκτυα, εφαρμογές cloud και κινητές συσκευές, παρέχοντας μια συνεκτική και ασφαλή προσέγγιση στη διαχείριση ταυτότητας και πρόσβασης (Singh et al., 2023).

Η Διαχείριση Ταυτότητας και Πρόσβασης είναι ουσιαστική για την προστασία των πληροφοριακών πόρων και την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Με τη σωστή εφαρμογή της IAM, οι οργανισμοί μπορούν να περιορίσουν τους κινδύνους ασφαλείας, να ενισχύσουν την προστασία των δεδομένων και να βελτιώσουν τη λειτουργική αποδοτικότητα (Singh et al., 2023).

Κεφάλαιο 4. Νομοθετικό πλαίσιο για τη διαχείριση της κυβερνοασφάλειας

4.1 Ευρωπαϊκή Ένωση

Από τις αρχές του 2000, η ασφάλεια έναντι κυβερνοεπιθέσεων είχε γίνει σημαντικό θέμα για την Ευρωπαϊκή Ένωση (ΕΕ). Ωστόσο, η ΕΕ άρχισε να ενεργοποιείται πιο έντονα σε αυτόν τον τομέα μετά το 2004. Το έτος αυτό, με τον Κανονισμό 460/2004, ιδρύθηκε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, γνωστός ως ENISA. Το 2006 η ΕΕ εξέδωσε την πρώτη πρωτοβουλία σχετικά με την ασφάλεια των δικτύων, η οποία αντικαταστάθηκε το 2013 από τη "Στρατηγική για την Κυβερνοασφάλεια". Η στρατηγική αυτή ήταν το αποτέλεσμα μιας μακροχρόνιας διαδικασίας διαβουλεύσεων και βασίστηκε στην "Ψηφιακή Ατζέντα για την Ευρώπη" του 2010 και επικεντρώθηκε στην πρόληψη και διαχείριση των αδυναμιών και ελλείψεων των ευρωπαϊκών συστημάτων τηλεπικοινωνιών (Γερονικολού, 2021).

Η ψήφιση της Οδηγίας 2016/1148 αποτέλεσε καθοριστικό βήμα για την ΕΕ στον τομέα της κυβερνοασφάλειας. Η Οδηγία αυτή θέσπισε μέτρα για την προστασία συστημάτων δικτύου και πληροφοριών σε όλη την Ευρωπαϊκή Ένωση. Επιπλέον, υπογράμμισε την ανάγκη για την ανάπτυξη ειδικών ομάδων στα κράτη-μέλη, γνωστών ως Computer Security Incident Response Teams (CSIRTs). Ο στόχος αυτών των ομάδων είναι η ενίσχυση της εμπιστοσύνης και η προώθηση της συνεργατικότητας σε επιχειρησιακό επίπεδο εντός της ΕΕ (Γερονικολού, 2021).

Το 2016 ψηφίστηκε ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (GDPR), ο οποίος, αν και δεν επικεντρώνεται άμεσα στην κυβερνοασφάλεια, την επηρεάζει σημαντικά. Ο κανονισμός επέφερε μεγάλη πρόοδο στην κυβερνοασφάλεια, ιδιαίτερα για οικονομικές και κοινωνικές δραστηριότητες που χρησιμοποιούν ψηφιακή τεχνολογία, και καθορίζει αυστηρές κυρώσεις για παραβιάσεις. Το 2019, αναθεωρήθηκε η στρατηγική του 2013 με τον Κανονισμό 2019/881, ο οποίος εστιάζει στην ανάπτυξη ενός ευρωπαϊκού μηχανισμού πιστοποίησης για την ασφαλή χρήση ψηφιακών προϊόντων και υπηρεσιών και την ενίσχυση του ρόλου του ENISA (Γερονικολού, 2021).

Τον Φεβρουάριο του 2020, η ΕΕ αναθεώρησε την Οδηγία NIS με την Οδηγία NIS2, στο πλαίσιο της προετοιμασίας της Ευρώπης για τον ψηφιακό κόσμο. Παράλληλα αναθεωρήθηκε η Στρατηγική για την Κυβερνοασφάλεια, με κύριους στόχους την προστασία των κρίσιμων υποδομών και των πολιτών από κυβερνοαπειλές, και την ενίσχυση της ψηφιακής ασφάλειας απέναντι σε τρίτες χώρες. Στα πλαίσια αυτής της στρατηγικής, συζητήθηκε η ανάπτυξη ενός δικτύου κέντρων επιχειρήσεων ασφαλείας με υποστήριξη τεχνητής νοημοσύνης και η δημιουργία μιας Κοινής Κυβερνομονάδας για την ενίσχυση της συνεργασίας μεταξύ των θεσμών της ΕΕ και των εθνικών αρχών (Γερονικολού, 2021).

4.2 Ελλάδα

Στη χώρα μας η αρχή που είναι αρμόδια για την αντιμετώπιση και την πρόληψη του ηλεκτρονικού εγκλήματος είναι το τμήμα της Ελληνικής Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΔΗΕ). Δύο απο τα πιο σημαντικά τμήματα απο τα οποία αποτελείται η ΔΔΗΕ είναι το τμήμα προστασίας ανηλίκων μέσω του διαδικτύου το οποίο ερευνά και αναζητά εγκλήματα σε βάρος παιδιών, σε υποθέσεις όπως αυτοκτονίες, εξαφάνισης και παρενόχληση με τη χρήση διαδικτύου ή άλλων ηλετκρονικών μέσων

το γνωστό σε όλους (cyber bulling). Το 2ο τμήμα είναι η Δίωξη Οικονομικών Εγκλημάτων η οποία αναζητά καθημερινά στο διαδίκτυο και σε πολλά άλλα ηλεκτρονικά μέσα για οικονομικά εγκλήματα που προκαλουν βλάβες στη δημόσια οικονομία όπως και στην εθνική οικονομία με σκοπό να προκαλούν χρυματικές απώλειες.

Επίσης στη χώρα μας ο νόμος 4070/2012 ορίζει τις υποχρεώσεις των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών για την προστασία και την ασφαλή λειτουργία των δικτύων. Συγκεκριμένα το άρθρο 37 υπογραμμίζει την υποχρέωση για λήψη όλων των απαραίτητων τεχνικών και οργανωτικών μέτρων για τη διαχείριση των κινδύνων, ώστε να εξασφαλίζεται η ασφάλεια των δικτύων και των υπηρεσιών. Τα μέτρα αυτά πρέπει να είναι ανάλογα με τον υφιστάμενο κίνδυνο και να φροντίζουν τόσο για την αποτροπή των κινδύνων όσο και την ελαχιστοποίηση των συνεπειών από συμβάντα ασφαλείας. Οι πάροχοι οφείλουν επίσης να διασφαλίζουν την ακεραιότητα των δικτύων για συνεχή και αδιάλειπτη παροχή υπηρεσιών. Κάθε παραβίαση της ασφάλειας ή της ακεραιότητας των δικτύων που επηρεάζει σημαντικά τη λειτουργία τους πρέπει να αναφέρεται στην ΕΕΤΤ (Εθνική Επιτροπή Τηλεποικινωνιών και Ταχυδρομείων) , η οποία ειναι η εθνική ρυθμιστική αρχή σε ζητήματα που έχουν σχέση με την παροχή υπηρεσιών και δικτύων ηλετρονικών επικοινωνιών η οποία με τη σειρά της ενημερώνει την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Μπαλτά, 2022).

Ακόμη, η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία ιδρύθηκε σύμφωνα με το άρθρο 1 του νόμου 3115/2003 διαδραματίζει σημαντικό ρόλο στην κυβερνοασφάλεια. Οι αρμοδιότητές της περιλαμβάνουν τον τακτικό και έκτακτο έλεγχο των επιχειρήσεων, την παρακολούθηση της συμμόρφωσης με τη νομοθεσία για την άρση του απορρήτου και την επιβολή διοικητικών κυρώσεων όταν παραβιάζεται η σχετική νομοθεσία. Η ΑΔΑΕ επίσης διερευνά καταγγελίες για παραβίαση του απορρήτου των επικοινωνιών, εκδίδει κανονιστικές διοικητικές πράξεις για την προστασία του απορρήτου και εκδίδει γνωμοδοτήσεις και συστάσεις που εμπίπτουν στις αρμοδιότητές της (Μπαλτά, 2022).

Πιο πρόσφατα, με το Προεδρικό Διάταγμα 82/2017, συστάθηκε η Εθνική Αρχή Κυβερνοασφάλειας στην Ελλάδα με κύριο στόχο την προστασία των συστημάτων πληροφορικής και των επικοινωνιών σε εθνικό επίπεδο από κυβερνοεπιθέσεις και άλλες απειλές. Οι αρμοδιότητές της περιλαμβάνουν τον καθορισμό και την εφαρμογή πολιτικών και στρατηγικών κυβερνοασφάλειας, τη θέσπιση κανονισμών και την παροχή οδηγιών για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων. Επίσης, η αρχή επιβλέπει και ελέγχει την τήρηση των κανόνων και των πολιτικών ασφάλειας από τους φορείς που παρέχουν κρίσιμες υπηρεσίες και υποδομές, διασφαλίζοντας ότι οι οργανισμοί συμμορφώνονται με τις απαιτήσεις ασφάλειας. Διαδραματίζει κεντρικό ρόλο στον συντονισμό των δράσεων αντιμετώπισης κυβερνοεπιθέσεων και περιστατικών ασφάλειας, συνεργαζόμενη με άλλες εθνικές και διεθνείς αρχές για την αποτελεσματική διαχείριση και ανάκαμψη από τέτοια περιστατικά. Εργάζεται για την αύξηση της ευαισθητοποίησης και την παροχή εκπαίδευσης σχετικά με θέματα κυβερνοασφάλειας τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα, προωθώντας την κατανόηση των κινδύνων και των καλών πρακτικών για την προστασία των πληροφοριακών συστημάτων. Επιπλέον, συνεργάζεται με διεθνείς οργανισμούς και άλλες χώρες για την ανταλλαγή πληροφοριών, την υιοθέτηση βέλτιστων πρακτικών και την ενίσχυση της συλλογικής ασφάλειας στον κυβερνοχώρο. Η ίδρυση της Εθνικής Αρχής Κυβερνοασφάλειας ήταν ένα σημαντικό βήμα για την ενίσχυση της εθνικής ασφάλειας στον κυβερνοχώρο και την προστασία των κρίσιμων υποδομών και υπηρεσιών από τις απειλές και τις επιθέσεις που αναδύονται συνεχώς στον ψηφιακό κόσμο (Μπαλτά, 2022).

Κεφάλαιο 5. Διαχείριση Κρίσεων και Αποκατάσταση μετά από Κυβερνοεπιθέσεις

Η διαχείριση κρίσεων και η αποκατάσταση μετά από κυβερνοεπιθέσεις είναι κρίσιμα στοιχεία για τη διατήρηση της επιχειρησιακής συνέχειας και την ελαχιστοποίηση των επιπτώσεων από τέτοιου είδους περιστατικά. Η διαδικασία περιλαμβάνει τέσσερα βασικά στάδια: προετοιμασία, άμεση αντίδραση, αποκατάσταση και εκμάθηση από τα συμβάντα. Αυτά τα στάδια συνεισφέρουν στη βελτίωση των αμυντικών μηχανισμών και στην ενίσχυση της ανθεκτικότητας του οργανισμού απέναντι σε μελλοντικές επιθέσεις.

5.1 Προετοιμασία

Η προετοιμασία είναι το πρώτο και πιο σημαντικό βήμα στη διαχείριση κρίσεων στην αποκατάσταση μετά από κυβερνοεπιθέσεις. Χωρίς ένα καλά σχεδιασμένο και εκτελεσμένο σχέδιο προετοιμασίας, οι οργανισμοί είναι ευάλωτοι σε σοβαρές διαταραχές και απώλειες που μπορούν να προκύψουν από τέτοιες επιθέσεις. Αυτό περιλαμβάνει την ανάπτυξη και την επικαιροποίηση ενός σχεδίου αντιμετώπισης περιστατικών (Incident Response Plan - IRP). Το σχέδιο αυτό πρέπει να περιλαμβάνει σαφείς οδηγίες για το πώς να αναγνωριστούν, να καταγραφούν και να αναφερθούν τα περιστατικά ασφάλειας.

Στο πλαίσιο της προετοιμασίας περιλαμβάνονται:

- Εκπαίδευση και Ευαισθητοποίηση: Τακτική εκπαίδευση των υπαλλήλων σε θέματα κυβερνοασφάλειας και την αναγνώριση απειλών. Η εκπαίδευση χρειάζεται να είναι διαρκής και να καλύπτει τις νέες και αναδυόμενες απειλές καθώς και τις καλύτερες πρακτικές ασφάλειας. Η εκπαίδευση και η

ευαισθητοποίηση του προσωπικού είναι κρίσιμα στοιχεία για τη δημιουργία μιας κουλτούρας ασφάλειας στον οργανισμό (Cyber Protections Hub, 2023).

- Σενάρια και Ασκήσεις: Διενέργεια ασκήσεων προσομοίωσης περιστατικών για να αξιολογηθεί η ετοιμότητα της ομάδας. Αυτές οι ασκήσεις βοηθούν στον εντοπισμό αδυναμιών στα σχέδια αντιμετώπισης και στη βελτίωση της συνεργασίας μεταξύ των ομάδων. Οι ασκήσεις θα πρέπει να είναι ρεαλιστικές και να καλύπτουν διάφορα σενάρια επιθέσεων που τονίζουν τη σημασία της προσομοίωσης για τη βελτίωση της αντίδρασης σε πραγματικές επιθέσεις (Cyber Protections Hub, 2023).
- Διατήρηση Εφεδρικών Αντιγράφων: Τακτική δημιουργία και διατήρηση εφεδρικών αντιγράφων των δεδομένων για την αποκατάσταση μετά από μια επίθεση. Αυτό περιλαμβάνει τη διατήρηση ασφαλών και ενημερωμένων αντιγράφων ασφαλείας των κρίσιμων δεδομένων και συστημάτων, καθώς και την τακτική δοκιμή των διαδικασιών αποκατάστασης για να διασφαλιστεί η αποτελεσματικότητα τους (Cyber Protections Hub, 2023).
- Σύσταση Ομάδας Αντιμετώπισης Περιστατικών (CSIRT): Η ομάδα CSIRT πρέπει να αποτελείται από ειδικούς σε διάφορους τομείς, συμπεριλαμβανομένων της διαχείρισης, της τεχνολογίας, της νομικής υποστήριξης και της επικοινωνίας. Οι ρόλοι και οι αρμοδιότητες κάθε μέλους πρέπει να είναι σαφείς και προκαθορισμένοι για να εξασφαλίζεται η αποτελεσματική αντίδραση κατά τη διάρκεια ενός περιστατικού (CrowdStrike, 2021).
- Απόκτηση και Διατήρηση Κατάλληλων Υποδομών και Εργαλείων: Οι οργανισμοί πρέπει να διαθέτουν τα κατάλληλα εργαλεία για την ανίχνευση και διερεύνηση περιστατικών, καθώς και για τη συλλογή και διατήρηση αποδεικτικών στοιχείων. Η τεχνολογία ασφαλείας πρέπει να προσφέρει ορατότητα σε όλα τα τελικά σημεία και να συλλέγει δεδομένα για τα περιστατικά (Thompson, 2018).

5.2 Άμεση Αντίδραση

Η άμεση αντίδραση σε μια κυβερνοεπίθεση είναι ζωτικής σημασίας για τον περιορισμό των επιπτώσεων και τη διαχείριση της κρίσης. Ένα από τα πρώτα βήματα είναι η απομόνωση των επηρεαζόμενων συστημάτων, που περιλαμβάνει την αποσύνδεσή τους από το δίκτυο για να αποτραπεί η εξάπλωση της επίθεσης και η προστασία των υπόλοιπων συστημάτων. Αφορά την φυσική αποσύνδεση καλωδίων δικτύου ή τη διακοπή της λειτουργίας του δικτυακού προσαρμογέα και τη ρύθμιση των κανόνων του τείχους προστασίας για τον περιορισμό της κυκλοφορίας δεδομένων (Cyber Protections Hub, 2023).

Μετά την απομόνωση, ακολουθεί η επιβεβαίωση και ανάλυση της επίθεσης, όπου οι ομάδες ασφαλείας αναλύουν τα καταγεγραμμένα δεδομένα και τα ίχνη της επίθεσης για να καθορίσουν τη φύση και την έκταση της ζημιάς. Αυτή η διαδικασία είναι εξαιρετικά σημαντική για τον εντοπισμό της πηγής της επίθεσης και την αξιολόγηση των συνεπειών της (Cyber Protections Hub, 2023).

Η επικοινωνία είναι επίσης βασικό στοιχείο, καθώς είναι σημαντικό να ενημερωθούν όλοι οι ενδιαφερόμενοι, όπως οι εσωτερικοί συνεργάτες, οι πελάτες και οι ρυθμιστικές αρχές, σύμφωνα με τις εσωτερικές πολιτικές και τις νομικές απαιτήσεις. Στο πλαίσιο αυτό παρέχονται σαφείς πληροφορίες σχετικά με το περιστατικό και τα μέτρα που λαμβάνονται για την αντιμετώπισή του (Cyber Protections Hub, 2023).

5.3 Αποκατάσταση

Η αποκατάσταση είναι μια δύσκολη και απαραίτητη διαδικασία μετά από μια κυβερνοεπίθεση, καθώς περιλαμβάνει την επαναφορά των συστημάτων και των

δεδομένων στην κανονική τους κατάσταση και τη βελτίωση των διαδικασιών ασφαλείας. Η διαδικασία αποκατάστασης περιλαμβάνει διάφορα σημαντικά βήματα:

- Αποκατάσταση Δεδομένων: Μετά από μια επίθεση, είναι πολύ σημαντικό να επαναφέρουμε τα δεδομένα χρησιμοποιώντας εφεδρικά αντίγραφα. Κάτι τέτοιο εξασφαλίζει την αποκατάσταση της επιχειρησιακής συνέχειας και ελαχιστοποιεί την απώλεια δεδομένων. Η ποιότητα και η επικαιρότητα των εφεδρικών αντιγράφων είναι καθοριστικοί παράγοντες για την επιτυχία αυτής της διαδικασίας.
- Αναβάθμιση Ασφαλείας: Μετά την ανάλυση της επίθεσης, είναι αναγκαίο να διορθωθούν οι ευπάθειες που εκμεταλλεύτηκαν οι επιτιθέμενοι. Αυτό μπορεί να περιλαμβάνει την ενημέρωση του λογισμικού, την ενίσχυση των συστημάτων ασφάλειας και την εισαγωγή νέων μέτρων για την αποτροπή μελλοντικών επιθέσεων.
- Επανεξέταση των Πολιτικών: Η επίθεση παρέχει σημαντικά διδάγματα που είναι χρήσιμο να ενσωματωθούν στις πολιτικές και διαδικασίες ασφαλείας της οργάνωσης. Η αναθεώρηση των πολιτικών αυτών με βάση τα ευρήματα της επίθεσης βοηθά στην ενίσχυση της ασφάλειας και στην αποτροπή παρόμοιων περιστατικών στο μέλλον.

Αυτές οι ενέργειες είναι απαραίτητες για την πλήρη αποκατάσταση της λειτουργικότητας και την ενίσχυση της ασφάλειας των συστημάτων. Είναι σημαντικό να πραγματοποιούνται μεθοδικά και σε συνεργασία με όλες τις εμπλεκόμενες πλευρές, προκειμένου να διασφαλιστεί η πλήρης αποκατάσταση και η βελτίωση της ασφάλειας (Choi et al., 2023).

5.4 Μαθαίνοντας από τις κυβερνοεπιθέσεις

Μια κυβερνοεπίθεση είναι πιθανόν να αποβεί διδακτική για τις μελλοντικές ενέργειες ενός οργανισμού. Παρέχει την κατάλληλη ανατροφοδότηση για τις μέχρι

τώρα λειτουργίες και αντιδράσεις στους κινδύνους που εμφανίζονται. Προκειμένου μια κυβερνοεπίθεση να αποφευχθεί στο μέλλον είναι απαραίτητη η λεπτομερής ανασκόπηση του περιστατικού και η εξαγωγή συμπερασμάτων για την πρόληψη παρόμοιων συμβάντων στο μέλλον. Η διαδικασία έχει τα ακόλουθα στάδια:

- Ανάλυση μετά την Κρίση: Η διαδικασία ξεκινά με μια διεξοδική ανάλυση του συμβάντος, γνωστή και ως post-mortem analysis. Αυτή περιλαμβάνει την αξιολόγηση των αιτίων της επίθεσης, την εκτίμηση της ζημίας που προκλήθηκε, και την εξέταση των αντιδράσεων και μέτρων που ελήφθησαν. Ο στόχος είναι να κατανοηθεί πλήρως το συμβάν και να εντοπιστούν τυχόν αδυναμίες στα συστήματα ασφαλείας και τις διαδικασίες του οργανισμού.
- Ενημέρωση του Σχεδίου Αντιμετώπισης: Τα ευρήματα από την ανάλυση χρησιμοποιούνται για την ενημέρωση και τη βελτίωση του Σχεδίου Αντιμετώπισης Περιστατικών (IRP). Πραγματοποιείται αναθεώρηση των διαδικασιών, ενημέρωση των εργαλείων ασφαλείας και ενίσχυση των πολιτικών πρόσβασης. Η συνεχής αναπροσαρμογή του IRP είναι απαραίτητη για την προσαρμογή στις νέες απειλές και τεχνολογικές εξελίξεις.
- Εκπαίδευση και Ανανέωση Γνώσεων: Το ανθρώπινο δυναμικό παραμένει η πρώτη γραμμή άμυνας σε θέματα κυβερνοασφάλειας. Συνεπώς, είναι σημαντικό οι εργαζόμενοι να ενημερώνονται συνεχώς για τις νέες πρακτικές και τεχνολογίες ασφαλείας. Προωθείται η παρακολούθηση σεμιναρίων, η εκπαίδευση σε νέες τεχνολογίες και η διενέργεια ασκήσεων για την αντιμετώπιση περιστατικών.

Η διαδικασία της εκμάθησης και της βελτίωσης βοηθά τους οργανισμούς να ελαχιστοποιήσουν τις επιπτώσεις μελλοντικών επιθέσεων και να βελτιώσουν την ανθεκτικότητά τους. Με την προσαρμογή στις νέες απειλές και την ενίσχυση των διαδικασιών ασφαλείας, οι οργανισμοί είναι σε θέση να ανταποκρίνονται πιο αποτελεσματικά και άμεσα στις προκλήσεις της κυβερνοασφάλειας.

Κεφάλαιο 6. Προκλήσεις και Τάσεις στην Κυβερνοασφάλεια

6.1 Ασφάλεια στο Διαδίκτυο των Πραγμάτων (IoT Security)

Η ραγδαία εξάπλωση του Διαδικτύου των Πραγμάτων (IoT) σε διάφορους τομείς, όπως αυτοματισμός κτιρίων, έξυπνες μεταφορές, υγειονομική περίθαλψη και βιομηχανικός έλεγχος, αλλάζει τον τρόπο με τον οποίο αντιλαμβανόμαστε και διαχειριζόμαστε τον φυσικό κόσμο. Καθώς τα συστήματα IoT αναλαμβάνουν την παρακολούθηση και διαχείριση σύνθετων οικοσυστημάτων, η ασφάλεια και η αξιοπιστία των δεδομένων που μεταδίδονται από και προς αυτές τις συσκευές αποτελούν κύρια πηγή ανησυχίας (Jurcut et al., 2020).

Έχει αναφερθεί σε αρκετές μελέτες ότι τα δίκτυα IoT αντιμετωπίζουν πολλές προκλήσεις ασφάλειας, όπως η αυθεντικοποίηση, η εξουσιοδότηση, η διαρροή πληροφοριών, η ιδιωτικότητα, η επαλήθευση, η παραποίηση, η παρεμβολή και η υποκλοπή. Το IoT παρέχει μια υποδομή δικτύου με διαλειτουργικά πρωτόκολλα επικοινωνίας και εργαλεία λογισμικού για τη σύνδεση στο διαδίκτυο για έξυπνες φορητές συσκευές (smartphones, προσωπικούς ψηφιακούς βοηθούς (PDA) και τάμπλετ), έξυπνες οικιακές συσκευές (έξυπνη τηλεόραση, κλιματιστικά, συστήματα φωτισμού, έξυπνα ψυγεία κ.λπ.), αυτοκίνητα και συστήματα απόκτησης αισθητηριακών δεδομένων (Jurcut et al., 2020).

Η αυξημένη συνδεσιμότητα και προσβασιμότητα των συσκευών εγείρει σημαντικές ανησυχίες για την ασφάλεια όλων των χρηστών του δικτύου, είτε

πρόκειται για ανθρώπους είτε για μηχανές. Μια χαρακτηριστική περίπτωση είναι η επίθεση από το κακόβουλο λογισμικό Mirai το 2016, που παραβίασε τον πάροχο υπηρεσιών DNS Dyn μέσω μιας επίθεσης DDoS με botnet, εκμεταλλευόμενη IoT συσκευές όπως εκτυπωτές, κάμερες IP, οικιακές πύλες και παιδικά μόνιτορ. Η συγκεκριμένη επίθεση αναδεικνύει τις ευπάθειες των IoT συσκευών σε κυβερνοεπιθέσεις (Williams et al., 2017).

Οι βασικές αιτίες των προκλήσεων ασφάλειας στα σύγχρονα αυτοματοποιημένα συστήματα που βασίζονται στην πληροφορία είναι η ανασφαλής και ανεξέλεγκτη σύνδεσή τους στο διαδίκτυο και η έλλειψη μηχανισμών ελέγχου πρόσβασης για ασφαλή και αξιόπιστη επικοινωνία. Επιπλέον, οι ευπάθειες στα συστήματα IoT προκύπτουν λόγω των φυσικών περιορισμών των συσκευών IoT, όπως η χαμηλή υπολογιστική ισχύς, η περιορισμένη χωρητικότητα αποθήκευσης και η μικρή διάρκεια ζωής της μπαταρίας. Η έλλειψη προτύπων ασφάλειας για το IoT και η ευρεία χρήση υλικού και λογισμικού από τρίτους επιδεινώνουν την κατάσταση. Αυτά τα συστήματα συχνά δεν είναι επαρκώς ασφαλή, ειδικά όταν εγκαθίστανται σε περιβάλλοντα που δεν μπορούν να προστατευτούν ή να απομονωθούν με άλλους τρόπους. Οι περιορισμοί των πόρων στις συσκευές IoT καθιστούν δύσκολη τη χρήση σύνθετων και χρονοβόρων αλγορίθμων κρυπτογράφησης για ασφαλή επικοινωνία, γεγονός που τις καθιστά ευάλωτες σε διάφορους τύπους επιθέσεων (Jurcut et al., 2020).

Οι πιο διαδεδομένες συσκευές που συνδέονται για να εξυπηρετήσουν εφαρμογές IoT για σκοπούς ενημέρωσης και ψυχαγωγίας είναι οι έξυπνες τηλεοράσεις, οι διαδικτυακές κάμερες και οι εκτυπωτές. Οι συγκεκριμένες συσκευές εμφανίζουν υψηλό κίνδυνο για επιθέσεις τρίτων. Επίσης, οι φορητές συσκευές, όπως τα έξυπνα τηλέφωνα, τα PDAs και τα mini-PCs, είναι οι κύριες πλατφόρμες μέσω των οποίων οι άνθρωποι αλληλεπιδρούν με την τεχνολογία IoT. Αυτές οι συσκευές διαθέτουν προηγμένες δυνατότητες, όπως υπηρεσίες εντοπισμού θέσης, βιομετρικούς

αισθητήρες, επιταχυνσιόμετρα/γυροσκόπια και μεγάλη χωρητικότητα μνήμης. Οι σύγχρονες κινητές συσκευές είναι ευάλωτες σε διάφορες επιθέσεις και απειλές, όπως επιθέσεις DoS (Denial of Service), [1]Sinkhole Attacks, [2]Bluesnarfing, [3]Bluejacking, αλλοίωση, διαφθορά και διαγραφή δεδομένων. Ακόμη μπορούν να πραγματοποιηθούν αναλύσεις κίνησης (Traffic Analysis), με παρακολούθηση της κίνησης δεδομένων για να αποκαλυφθούν ευαίσθητες πληροφορίες. Οι τεχνολογίες όπως το LR-WPAN (Low-Rate Wireless Personal Area Network), το Bluetooth και το Wi-Fi είναι επίσης ευάλωτες σε επιθέσεις κατά τη διάρκεια της μεταφοράς δεδομένων (Jurcut et al., 2020).

6.2 Ασφάλεια στο Υπολογιστικό Νέφος (Cloud Security)

Οι γρήγορες εξελίξεις στην τεχνολογία πληροφορικής και επικοινωνιών (ICT) έχουν επιτρέψει τη δημιουργία του "υπολογιστικού νέφους" ως μια επιτυχημένη λύση για την εύκολη αποθήκευση, πρόσβαση, επεξεργασία και διαμοιρασμό πληροφοριών. Με τα σημαντικά πλεονεκτήματα της επεκτασιμότητας και της ευελιξίας, το υπολογιστικό νέφος έχει προσελκύσει εταιρείες και άτομα, τα οποία όλο και περισσότερο χρησιμοποιούν τους πολλούς διαθέσιμους παρόχους για την αποθήκευση και επεξεργασία δεδομένων (Samarati, & De Capitani di Vimercati, 2016).

Ωστόσο, αυτή η ευκολία συνοδεύεται από την απώλεια ελέγχου των ιδιοκτητών των δεδομένων και από διάφορες απειλές για την ασφάλεια, οι οποίες μπορεί να περιορίσουν την ευρεία αποδοχή και χρήση του υπολογιστικού νέφους. Οι πάροχοι νέφους συνήθως εφαρμόζουν βασικά μέτρα ασφαλείας για την προστασία

[1] Sinkhole Attacks: Σε αυτές τις επιθέσεις, τα δεδομένα ανακατευθύνονται σε μια κακόβουλη συσκευή, η οποία μπορεί να τα κλέψει ή να τα τροποποιήσει.
[2] Bluesnarfing: Αφορά την κλοπή δεδομένων από κινητές συσκευές μέσω Bluetooth χωρίς τη γνώση του χρήστη
[3] Bluejacking: Αποστολή ανεπιθύμητων μηνυμάτων μέσω Bluetooth σε άλλες συσκευές.

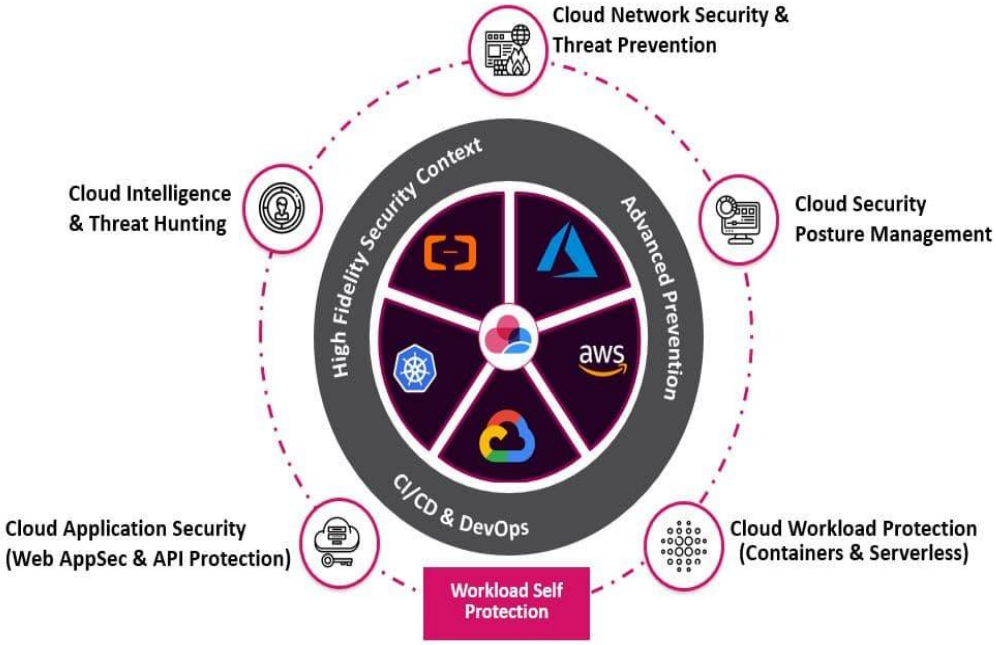
των δεδομένων κατά την αποθήκευση, την επεξεργασία και την επικοινωνία, διαθέτοντας πόρους για την ασφάλεια που πολλοί ιδιώτες και εταιρείες μπορεί να μην μπορούν να αντέξουν οικονομικά (Samarati, & De Capitani di Vimercati, 2016).

Παρά ταύτα, οι ιδιοκτήτες των δεδομένων και οι χρήστες του νέφους χάνουν τον έλεγχο των δεδομένων τους και της επεξεργασίας τους. Σύμφωνα με τον ENISA (2009), η απώλεια ελέγχου και διακυβέρνησης είναι ένας από τους μεγαλύτερους κινδύνους του υπολογιστικού νέφους (Samarati, & De Capitani di Vimercati, 2016).

Ένα βασικό πρόβλημα που πρέπει να αντιμετωπιστεί όταν βασιζόμαστε στο υπολογιστικό νέφος για την αποθήκευση δεδομένων είναι η διασφάλιση της προστασίας (δηλαδή, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας) των αποθηκευμένων δεδομένων. Με τις τρέχουσες λύσεις, οι χρήστες χρειάζεται συνήθως να εμπιστεύονται πλήρως τους παρόχους νέφους. Παρόλο που οι πάροχοι εφαρμόζουν μέτρα ασφαλείας στις υπηρεσίες που προσφέρουν, αυτά τα μέτρα τους επιτρέπουν να έχουν πλήρη πρόσβαση στα δεδομένα. Για παράδειγμα, το Google Docs ή το Salesforce υποστηρίζουν την κρυπτογράφηση των δεδομένων τόσο κατά τη μεταφορά όσο και στην αποθήκευση, αλλά διαχειρίζονται και τα κλειδιά κρυπτογράφησης, με αποτέλεσμα οι χρήστες να μην έχουν άμεσο έλεγχο στο ποιος μπορεί να έχει πρόσβαση στα δεδομένα τους (Samarati, & De Capitani di Vimercati, 2016).

Ένας τρόπος για την ενίσχυση της ασφάλειας είναι η κρυπτογράφηση των δεδομένων πριν την αποθήκευσή τους στο νέφος. Με την κρυπτογράφηση, οι χρήστες είναι σε θέση να διασφαλίσουν ότι μόνο εκείνοι που κατέχουν τα κλειδιά κρυπτογράφησης μπορούν να αποκρυπτογραφήσουν και να έχουν πρόσβαση στα δεδομένα. Αυτό μειώνει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, ακόμα και από τον πάροχο του νέφους. Ωστόσο, η διαχείριση των κλειδιών

κρυπτογράφησης αποτελεί μια κρίσιμη παράμετρο για την ασφάλεια των δεδομένων. Οι χρήστες είναι απαραίτητο να διατηρούν τα κλειδιά τους ασφαλή και να χρησιμοποιούν αξιόπιστες μεθόδους για τη διανομή και την αποθήκευσή τους. Υπάρχουν υπηρεσίες τρίτων που παρέχουν εξειδικευμένες λύσεις για τη διαχείριση κλειδιών (Key Management Services - KMS), οι οποίες προσφέρουν επιπλέον ασφάλεια και ευκολία (Samarati, & De Capitani di Vimercati, 2016).



Εικόνα 8, Οι προϋποθέσεις για ασφάλεια στο cloud, πηγή: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

Παρά τις προόδους αυτές, η απώλεια ελέγχου και διακυβέρνησης παραμένει μια σημαντική πρόκληση. Η απώλεια ελέγχου αναφέρεται στην αδυναμία των χρηστών να έχουν πλήρη εποπτεία και έλεγχο των δεδομένων τους όταν αυτά βρίσκονται στο νέφος. Κάτι τέτοιο είναι πιθανόν να έχει σοβαρές επιπτώσεις, ειδικά για ευαίσθητα ή κρίσιμα δεδομένα. Οι χρήστες χρειάζεται να βασίζονται στους παρόχους για την ασφάλεια και τη συμμόρφωση με τους κανονισμούς, γεγονός το οποίο ενδέχεται να δημιουργήσει ανησυχίες σχετικά με την ιδιωτικότητα και την ασφάλεια των δεδομένων (Samarati, & De Capitani di Vimercati, 2016).

6.3 Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στην Κυβερνοασφάλεια

Η χρήση της Τεχνητής Νοημοσύνης (ΤΝ) και της Μηχανικής Μάθησης (ΜΜ) στην Κυβερνοασφάλεια αποτελεί έναν ταχέως αναπτυσσόμενο τομέα που υπόσχεται να ενισχύσει σημαντικά τις δυνατότητες ανίχνευσης και αντιμετώπισης απειλών. Ωστόσο, η ενσωμάτωση αυτών των τεχνολογιών συνοδεύεται από πολυάριθμες προκλήσεις, οι οποίες χρειάζεται να αντιμετωπιστούν προκειμένου να εξασφαλιστεί η αποτελεσματική τους χρήση.

Σύμφωνα με τον Sarker (2021), η ΤΝ έχει τη δυνατότητα να ανιχνεύει και να αντιμετωπίζει επιθέσεις σε πραγματικό χρόνο, προσφέροντας ταχύτερη απόκριση και πιο αποτελεσματική προστασία. Τα συστήματα ΤΝ μαθαίνουν από τις επιθέσεις και προσαρμόζονται, βελτιώνοντας συνεχώς την ικανότητά τους να αναγνωρίζουν νέες απειλές. Ένα παράδειγμα είναι η χρήση των νευρωνικών δικτύων για την ανίχνευση ανωμαλιών στη δικτυακή κίνηση, που επιτρέπει την ταχύτερη και ακριβέστερη ταυτοποίηση των κυβερνοαπειλών. Επιπλέον, οι Buczak και Guven (2016) αναφέρουν ότι οι τεχνικές ΜΜ, όπως οι αλγόριθμοι ταξινόμησης, ανίχνευσης ανωμαλιών και clustering, μπορούν να χρησιμοποιηθούν για την ανίχνευση και πρόβλεψη απειλών.

Παρά τα σημαντικά πλεονεκτήματα, η εφαρμογή της ΜΜ στην Κυβερνοασφάλεια παρουσιάζει προκλήσεις. Μία από αυτές είναι η ανάγκη για μεγάλες ποσότητες δεδομένων για την εκπαίδευση των μοντέλων. Επιπλέον, ελλοχεύει πάντα ο κίνδυνος οι επιτιθέμενοι να εκμεταλλευτούν κακόβουλα δεδομένα για να παραπλανήσουν τα συστήματα ΜΜ.

Η αποτελεσματική χρήση της ΤΝ και της ΜΜ στην Κυβερνοασφάλεια απαιτεί την ανάπτυξη προηγμένων μεθόδων για την αντιμετώπιση αυτών των προκλήσεων. Η συνεχής έρευνα και η εξέλιξη των τεχνολογιών αυτών είναι απαραίτητες για την ενίσχυση της ανθεκτικότητας των συστημάτων ασφαλείας και την προστασία των δεδομένων από τις σύγχρονες απειλές.

6.4 Διεθνής συνεργασία για την κυβερνοασφάλεια

1992, το Οικονομικό και Κοινωνικό Συμβούλιο των Ηνωμένων Εθνών σημείωσε ότι το οργανωμένο έγκλημα έχει γίνει διεθνές, διασχίζοντας τα εθνικά σύνορα. Αυτό περιλαμβάνει δραστηριότητες όπως η τρομοκρατία, η εμπορία ναρκωτικών και όπλων, η εμπορία ανθρώπων και άλλες παράνομες δραστηριότητες που απειλούν την ασφάλεια και υπονομεύουν το κράτος δικαίου. Για την αντιμετώπιση αυτών των προκλήσεων, τα Ηνωμένα Έθνη υποστηρίζουν τα κράτη μέσω διεθνών συμβάσεων και πρωτοκόλλων, με το Γραφείο των Ηνωμένων Εθνών για τα Ναρκωτικά και το Έγκλημα να επιβλέπει την εφαρμογή αυτών των συμφωνιών (Croasdell & Palustre, 2019).

Το κυβερνοέγκλημα απαιτεί συντονισμένη δράση από κυβερνήσεις και επιχειρήσεις, αλλά δημιουργεί επίσης μεγάλες προκλήσεις για τη διεθνή συνεργασία. Η κυβερνοεπιθέσεις απειλούν πολλές χώρες μέσω του διαδικτύου, όπως με ιούς ή παραβιάσεις πνευματικών δικαιωμάτων. Τέτοιες περιπτώσεις καταλήγουν σε διαφωνίες για ποια χώρα είναι υποχρεωμένη να αναλάβει την υπόθεση και πώς να γίνουν οι διώξεις χωρίς να ταλαιπωρηθούν οι μάρτυρες, να επαναληφθούν οι προσπάθειες ή να υπάρξει ανταγωνισμός μεταξύ των αρχών επιβολής του νόμου (Croasdell & Palustre, 2019).

Το 1990, η Γενική Συνέλευση των Ηνωμένων Εθνών υιοθέτησε μια απόφαση για το έγκλημα στον τομέα των υπολογιστών. Το 2000 και το 2002, υιοθέτησε επιπλέον αποφάσεις για την καταπολέμηση της εγκληματικής κακής χρήσης της πληροφορικής τεχνολογίας. Η Ομάδα των 8 (G8), που περιλαμβάνει τις ΗΠΑ, το Ηνωμένο Βασίλειο, τη Ρωσία, τη Γαλλία, την Ιταλία, την Ιαπωνία, τη Γερμανία και τον Καναδά, υποστήριξε αυτές τις αποφάσεις με δημόσια ανακοίνωση. Η ανακοίνωση προέβλεπε ότι το προσωπικό επιβολής του νόμου θα πρέπει να εκπαιδευτεί και να εξοπλιστεί για την καταπολέμηση του κυβερνοεγκλήματος, να ακολουθήσει ένα σχέδιο δράσης και να προστατεύει τα δεδομένα και τα συστήματα. Επίσης, όρισε ότι οι χώρες μέλη θα πρέπει να έχουν διαθέσιμο σημείο επαφής 24/7 (Croasdell & Palustre, 2019).

Η Συνεργασία Οικονομίας Ασίας-Ειρηνικού (APEC) εξέδωσε εντολή τον Αύγουστο του 2002 για την καταπολέμηση του κυβερνοεγκλήματος σε περιφερειακό επίπεδο και για την υποστήριξη διεθνών συμβάσεων. Η στρατηγική κυβερνοασφάλειας της APEC στοχεύει στην ενίσχυση των νομικών πλαισίων των οικονομιών της περιοχής για την καταπολέμηση του κυβερνοεγκλήματος και στην προώθηση της ανάπτυξης ικανοτήτων έρευνας και επιβολής του νόμου για την αποτελεσματική αντιμετώπισή του (Croasdell & Palustre, 2019).

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (OECD), που αποτελείται από 34 χώρες, δημοσίευσε το 2002 τις "Κατευθυντήριες Γραμμές για την Ασφάλεια των Συστημάτων και Δικτύων Πληροφοριών: Προς μια Κουλτούρα Ασφαλείας". Το 2002, η Κοινοπολιτεία των Εθνών παρουσίασε ένα υπόδειγμα νόμου βασισμένο στη Σύμβαση για το Κυβερνοέγκλημα, το οποίο παρέχει ένα νομικό πλαίσιο που εναρμονίζει τη νομοθεσία εντός της Κοινοπολιτείας και διευκολύνει τη διεθνή συνεργασία (Croasdell & Palustre, 2019).

Η Οικονομική Κοινότητα Δυτικών Αφρικανικών Χωρών (ECOWAS) είναι μια περιφερειακή ομάδα δυτικοαφρικανικών χωρών που ιδρύθηκε το 1975 και περιλαμβάνει δεκαπέντε κράτη μέλη. Το 2009, η ECOWAS υιοθέτησε την Οδηγία για την Καταπολέμηση του Κυβερνοεγκλήματος στην ECOWAS, η οποία παρέχει ένα νομικό πλαίσιο για τα κράτη μέλη, το οποίο περιλαμβάνει τόσο ουσιαστικό ποινικό δίκαιο όσο και διαδικαστικό δίκαιο. Το θεμέλιο για νέους διεθνείς κανόνες έχει πλέον τεθεί (Croasdell & Palustre, 2019).

Τα τελευταία χρόνια έχει σημειωθεί σημαντική πρόοδος στην ανάπτυξη παγκόσμιων κανόνων κυβερνοασφάλειας. Για παράδειγμα, τον Ιούλιο του 2015, κυβερνητικοί εμπειρογνώμονες από 20 χώρες συνιστούσαν κανόνες κυβερνοασφάλειας για τα κράτη, με στόχο την προώθηση ενός ανοικτού, ασφαλούς, σταθερού, προσβάσιμου και ειρηνικού περιβάλλοντος πληροφορικής και επικοινωνιών με βασικές αρχές που απαγορεύουν στις κυβερνήσεις να εμπλέκονται σε κακόβουλες δραστηριότητες χρησιμοποιώντας τεχνολογία πληροφοριών και επικοινωνιών ή να βλάπτουν την κρίσιμη υποδομή άλλων εθνών (Croasdell & Palustre, 2019).

Η διεθνής συνεργασία, ωστόσο, ακόμη και σήμερα αντιμετωπίζει τις ακόλουθες προκλήσεις:

- Νομοθετικές Διαφορές

  Τα κράτη έχουν διαφορετικά νομικά πλαίσια και προσεγγίσεις για την κυβερνοασφάλεια. Αυτό μπορεί να δημιουργήσει εμπόδια στη συνεργασία, ειδικά όσον αφορά τη δικαιοδοσία και την εφαρμογή του νόμου. Για παράδειγμα, οι κανονισμοί περί προστασίας δεδομένων διαφέρουν σημαντικά μεταξύ ΗΠΑ και Ευρώπης, με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) της ΕΕ να θέτει αυστηρότερες απαιτήσεις.

- Πολιτικές και Πολιτιστικές Διαφορές

Η διαφορετική πολιτική κουλτούρα και οι προτεραιότητες των κρατών δύνανται να επηρεάσουν την προθυμία για συνεργασία. Κάποια κράτη είναι πιθανόν να δίνουν μεγαλύτερη έμφαση στην εθνική ασφάλεια, ενώ άλλα στην προστασία της ιδιωτικότητας, γεγονός το οποίο ενδέχεται να φέρει ως συνεπακόλουθο διαφωνίες και συγκρούσεις συμφερόντων.

- Ανισότητα στις Δυνατότητες

  Ορισμένα κράτη διαθέτουν προηγμένα τεχνολογικά μέσα και πόρους για την αντιμετώπιση κυβερνοαπειλών, ενώ άλλα στερούνται τέτοιων δυνατοτήτων. Κάτι τέτοιο δημιουργεί μια ανισότητα στη συνεργασία φυσικά επηρεάζει την αποτελεσματικότητα των κοινών προσπαθειών.

Κεφάλαιο 7. Συμπεράσματα

Η κυβερνοασφάλεια, λοιπόν, συνιστά έναν πολύ σημαντικό τομέα, ο οποίος διαρκώς εξελίσσεται λόγω των ραγδαίων τεχνολογικών εξελίξεων και της αυξανόμενης εξάρτησης από το διαδίκτυο και τις ψηφιακές τεχνολογίες. Από την ανάλυση που προηγήθηκε προκύπτει ότι η πολυπλοκότητα και η σημασία της προστασίας των ψηφιακών υποδομών και των δεδομένων δεν μπορούν να υποτιμηθούν. Τα τεχνολογικά επιτεύγματα, όπως το Διαδίκτυο των Πραγμάτων (IoT), η Τεχνητή Νοημοσύνη (ΤΝ) και η Μηχανική Μάθηση (ΜΜ), αν και προσφέρουν νέες δυνατότητες, φέρνουν επίσης νέες προκλήσεις και απειλές, οι οποίες χρειάζεται να λαμβάνονται υπ'όψιν.

Όπως είδαμε, η χώρα μας έχει ήδη λάβει μέτρα για να προωθήσει την κυβερνοασφάλεια ακολουθώντας τις υπόλοιπες ευρωπαϊκές χώρες. Άλλωστε, η Ευρωπαϊκή Ένωση έχει αναγνωρίσει την ανάγκη για ενισχυμένη κυβερνοασφάλεια ήδη από τις αρχές του 2000, με σημαντικές νομοθετικές πρωτοβουλίες να λαμβάνουν χώρα μετά το 2004. Η δημιουργία του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) και η έκδοση της Οδηγίας 2016/1148 για την ασφάλεια των συστημάτων δικτύου και πληροφοριών αποδεικνύουν τη δέσμευση της ΕΕ στην προστασία των ψηφιακών υποδομών. Οι νομοθετικές αυτές πρωτοβουλίες ενισχύθηκαν περαιτέρω με τον Κανονισμό 2019/881 και την αναθεώρηση της Οδηγίας NIS2 το 2020, οι οποίες εστιάζουν στην ενίσχυση της συνεργασίας μεταξύ των κρατών-μελών και στην ευθυγράμμιση των κυρώσεων.

Ακόμη και μετά από αυτές τις ρυθμίσεις, οι παραβιάσεις δεδομένων και οι επιθέσεις phishing αποτελούν διαρκείς απειλές για την ασφάλεια των πληροφοριών. Η διαχείριση ταυτότητας και πρόσβασης (IAM) και η ανίχνευση και πρόληψη

εισβολών (IDS/IPS) αποτελούν κρίσιμα εργαλεία για την αντιμετώπιση αυτών των απειλών. Οι τεχνολογίες αυτές επιτρέπουν την αναγνώριση και την απόκριση σε ύποπτες δραστηριότητες, διασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων.

Η Τεχνητή Νοημοσύνη και η Μηχανική Μάθηση φέρνουν νέες δυνατότητες για την ανίχνευση απειλών και την πρόληψη επιθέσεων, αλλά επίσης δημιουργούν νέες προκλήσεις. Η πολυπλοκότητα των συστημάτων αυτών και η ανάγκη για μεγάλους όγκους δεδομένων για την εκπαίδευσή τους μπορεί ωστόσο να οδηγήσει σε νέες ευπάθειες.

Συνοψίζοντας, η προστασία της κυβερνοασφάλειας απαιτεί μια πολυεπίπεδη προσέγγιση που περιλαμβάνει νομοθετικά μέτρα, τεχνολογικές λύσεις και συνεργασία μεταξύ των φορέων. Η συνεχής επαγρύπνηση και η προσαρμογή στις νέες τεχνολογικές εξελίξεις είναι απαραίτητες για την αντιμετώπιση των διαρκώς εξελισσόμενων απειλών και την προστασία των ψηφιακών υποδομών και δεδομένων. Η ευαισθητοποίηση και η εκπαίδευση σε θέματα κυβερνοασφάλειας είναι κρίσιμες για την ενίσχυση της ανθεκτικότητας απέναντι στις κυβερνοαπειλές. Όλοι οι χρήστες, από τον απλό πολίτη έως τον επαγγελματία της πληροφορικής, πρέπει να είναι ενήμεροι και προετοιμασμένοι για την αντιμετώπιση των κινδύνων, συμβάλλοντας στη δημιουργία ενός ασφαλέστερου ψηφιακού κόσμου.

Βιβλιογραφία

- Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.
- Anderson, J. P. (1972). Computer Security Technology Planning Study. U.S. Air Force Electronic Systems Division
- Ashoor, A. S., & Gore, S. (2012). Intrusion detection system (IDS) & intrusion prevention system (IPS): case study. International Journal of Scientific & Engineering Research, 2(7).
- Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 Proceedings 2 (pp. 31-46). Springer Berlin Heidelberg.
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
- Buzan, B., Wæver, O., & De Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.
- Choi, S. H., Youn, J., Kim, K., Lee, S., Kwon, O. J., & Shin, D. (2023). Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement. Sustainability, 15(18), 13404.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10).
- Croasdell D. and & Palustre A. (2019). Transnational cooperation in cybersecurity. In Proc. of the 52nd Hawaii International Conference on System Sciences (HICSS-52), Grand Wailea, Hawaii, page 5598. BY-NC-ND 4.0.
- CrowdStrike. (2021). 2021 Global Threat Report. Retrieved from https://www.crowdstrike.com/resources/reports/2021-crowdstrike-global-threat-report/

- Cyber Protections Hub. (2023). Strategies for isolating affected systems during a cybersecurity incident. https://cyberprotections.org/strategies-for-isolating-affected-systems-during-a-cybersecurity-incident/incident-response-and-forensics/
- Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman (pp. 365-390).
- Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems, 122, 149-171.
- European Network and Information Security Agency – ENISA (2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment/at_download/fullReport
- Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).
- Hayajneh, T., Mohd, B. J., Itradat, A., & Quttoum, A. N. (2013). Performance and information security evaluation with firewalls. International Journal of Security and Its Applications, 7(6), 355-372.
- Hejase, H. J., Fayyad-Kazan, H. F., Hejase, A. J., & Moukadem, I. A. (2021). Cyber security amid COVID-19. Computer and Information Science, 14(2), 1-10.
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.
- Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT security. IoT security: advances in authentication, 27-64.
- Kelty, C. (2011). The Morris Worm. Limn, 1. Retrieved from https://escholarship.org/uc/item/8t12q5bj
- Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. Journal of Cyber Security and Mobility, 1(4), 309-348.

- Moore, D., et al. (2002). The Spread of the Code-Red Worm (CRv2). IEEE Security & Privacy.
- Orman, H. (2003). The Morris worm: A fifteen-year perspective. IEEE Security & Privacy, 1(5), 35-43.
- Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. October 1, http://www.oxforddictionaries.com/definition/english/Cybersecurity
- Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. Global Journal of Computer Science and Technology, 14(7), 15-32.
- Romano, S. (2003). Sarbanes-Oxley and Its Impact on IT Security. Information Systems Security.
- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.
- Samarati, P., & De Capitani di Vimercati, S. (2016). Cloud security: Issues and concerns. Encyclopedia of cloud computing, 205-219.
- Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. SN Computer Science, 2(3), 1-21. https://doi.org/10.1007/s42979-021-00592-x
- Segovia, L., Torres, F., Rosillo, M., Tapia, E., Albarado, F., & Saltos, D. (2017). Social engineering as an attack vector for ransomware. In Proceedings of the Conference on Electrical Engineering and Information Communication Technology (pp. 1-6). Pucon, Chile
- Singer, P. W., & Friedman, A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press
- Singh, C., Thakkar, R., & Warraich, J. (2023). IAM identity Access Management—importance in maintaining security systems within organizations. European Journal of Engineering and Technology Research, 8(4), 30-38.
- Thompson, E. C. (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents. Apress Berkeley, CA. https://doi.org/10.1007/978-1-4842-3870-7

- Williams R., McMahon E., Samtani S., Patton M., and Chen H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. IEEE International Conference on Intelligence and Security Informatics (ISI), doi:10.1109/isi.2017.8004904
- Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: analysis, countermeasures and challenges. International Journal of Information and Computer Security, 19(3-4), 402-442.
- Γερονικολού Μ. (2021), 'Η εξέλιξη της κυβερνοασφάλειας στην ΕΕ',ΟΔΕΘ, 15 Ιουλίου. Διαθέσιμο στο: https://odeth.eu/%CE%B7%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7%CF%84%CE%B7%CF%82%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82%CF%83%CF%84%CE%B7%CE%BD-%CE%B5
- Γεωργιάδης, Χ. Ζ. (2015). Σχεδιασμός και ανάπτυξη mobile εφαρμογής του ΤΗΜΜΥ του Πανεπιστημίου Θεσσαλίας σε περιβάλλον Android
- Ευρωπαϊκό Ελεγκτικό Συνέδριο (2019) Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια. Λουξεμβούργο: Ευρωπαϊκό Ελεγκτικό Συνέδριο Διαθέσιμο στο: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECU RITY_EL.pdf
- Μπαλτά, Ι. (2022). Η κυβερνοασφάλεια στη σύγχρονη ψηφιακή εποχή (Master's thesis, Πανεπιστήμιο Πειραιώς).
- Παπαθανασίου Αναστάσιος . Επιθέσεις υποκλοπής ηλεκτρονικού ταχυδρομείου επιχειρήσεων (BEC): Απειλές, τρωτά σημεία και αντίμετρα - Μια προοπτική για το Ελληνικό τοπίο (Τμήμα Πληροφορικής και Τηλεπικοινωνιών Άρτας, Πανεπιστήμιο Ιωαννίνων)