ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ»

Κυβερνο-επιθέσεις κατά επιχειρήσεων και η αντιμετώπισή τους

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΜΠΑΣΔΑΝΗ Αναστασία του Δημητρίου

Αθήνα, 2023

Τριμελής Επιτροπή

Χρήστος Τσουραμάνης, Ομότιμος Καθηγητής Πανεπιστημίου Πατρών (Επιβλέπων)

Γρηγόριος Λάζος, Καθηγητής Παντείου Πανεπιστημίου

Ευσταθία Λαμπροπούλου, Καθηγήτρια Παντείου Πανεπιστημίου

Αφιερώνεται στην κόρη μου

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΤΜ : αυτόματη ταμειολογιστική μηχανή

βλ. : βλέπε

Γ.Κ.Π.Δ. : Γενικός Κανονισμός για την Προστασία των Δεδομένων

Ε.Ε. : Ευρωπαϊκή Ένωση

Ε.Ο.Χ. : Ευρωπαϊκός Οικονομικός Χώρος

Επιμ. : επιμέλεια

Η.Π.Α. : Ηνωμένες Πολιτείες Αμερικής

κ.ά. : και άλλα

κ.λπ. : και λοιπά

Μετ. : Μετάφραση

ό.π. : όπως παραπάνω

π.χ. : παραδείγματος χάρη

σελ. : σελίδα

σσ. : σελίδες

σύν. : συνεργάτες

Τ.Π.Ε. : Τεχνολογία Πληροφοριών και Επικοινωνίας

AIDS : Acquired Immune Deficiency Syndrome

AOL : America Online

CDs : Compact Discs

CIA : Confidentiality - Integrity - Availability

CIAAA : Confidentiality - Integrity - Availability - Accountability - Authenticity

CVV : Card Verification Value

DDOS : Distributed denial of service

Ed. : Editor

GDPR : General Data Protection Regulation

HTTP : Hyper Text Transfer Protocol

IDS : Intrusion Detection Systems

IP : Internet Protocol

M.F.A. : Multi - Factor Authentication

p. : page

POS : Point Of Sale

pp. : pages

PSN : PlayStation Network

SIM : Subscriber Identity Module

SMS : Short Message Service

USB : Universal Serial Bus

vol : volume

& : και

% : τοις εκατό

Ε Υ Χ Α Ρ Ι Σ Τ Ι Ε Σ

Ολοκληρώνοντας τις μεταπτυχιακές μου σπουδές και στο πλαίσιο εκπόνησης της διπλωματικής μου εργασίας, θα ήθελα να ευχαριστήσω όλους όσοι με ενθάρρυναν και με στήριξαν.

Πιο συγκεκριμένα, θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου κ. Τσουραμάνη Χρήστο για την επιστημονική του καθοδήγηση, τις παραγωγικές υποδείξεις του, καθώς επίσης και για την εμπιστοσύνη που επέδειξε στο πρόσωπό μου με την ανάθεση της συγκεκριμένης διπλωματικής εργασίας.

Παράλληλα, θα ήθελα να εκφράσω την ευγνωμοσύνη μου στους γονείς μου, οι οποίοι πάντα πίστευαν σε εμένα και μου συμπαραστέκονταν με κάθε τρόπο.

Τέλος, ευχαριστώ ιδιαίτερα τον σύζυγό μου που ήταν δίπλα μου και με στήριζε καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ ..... - 4 -
ΠΡΟΛΟΓΟΣ ..... - 11 -
ΜΕΡΟΣ Α΄ ..... - 13 -
Εισαγωγικές παρατηρήσεις ..... - 13 -
1. Εισαγωγή στην κοινωνία της πληροφορίας ..... - 13 -
2. Η έννοια της επιχείρησης ..... - 15 -
3. Η έννοια του κυβερνοχώρου ..... - 17 -
4. Η είσοδος των επιχειρήσεων στον κυβερνοχώρο ..... - 18 -
5. Η σκοτεινή πλευρά του κυβερνοχώρου και οι κίνδυνοι που διατρέχουν οι επιχειρήσεις σε αυτόν ..... - 20 -
ΜΕΡΟΣ Β΄ ..... - 26 -
Το φαινόμενο των κυβερνοεπιθέσεων κατά των επιχειρήσεων ..... - 26 -
1. Εννοιολογική προσέγγιση ..... - 26 -
2. Γενικό προφίλ κυβερνοεπιθέσεων ..... - 30 -
3. Χαρακτηριστικά γνωρίσματα και σκοτεινός αριθμός ..... - 33 -
4. Κίνητρα ..... - 35 -
5. Επιπτώσεις ..... - 38 -
6. Κατηγοριοποίηση και τύποι κυβερνοεπιθέσεων κατά επιχειρήσεων ..... - 40 -
7. Περιγραφική ανάλυση δημοφιλών κυβερνοεπιθέσεων ..... - 48 -
7.1 Επίθεση phishing ..... - 49 -
7.2 Επίθεση Salami Slicing ..... - 51 -
7.3 Επίθεση Ransomware ..... - 52 -
7.4 Επίθεση Cryptojacking ..... - 53 -
8. Γενικά στατιστικά δεδομένα ..... - 54 -
ΜΕΡΟΣ Γ΄ ..... - 57 -
Οργάνωση ομάδων & περιπτώσεις μελέτης κυβερνοεπιθέσεων ..... - 57 -
1. Οργάνωση ομάδων και κυβερνοεπιθέσεις ..... - 57 -
2. Παραδείγματα κυβερνοεπιθέσεων σε επιχειρήσεις ..... - 60 -
ΜΕΡΟΣ Δ΄ ..... - 65 -
Ζητήματα κυβερνοασφάλειας: ..... - 65 -
προληπτικά μέτρα & αντιμετώπιση περιστατικών ..... - 65 -
1. Η ασφάλεια του πληροφοριακού συστήματος μιας επιχείρησης ..... - 65 -
2. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων στις επιχειρήσεις ... - 72 -

3. Εταιρικός σχεδιασμός για την πρόληψη κυβερνοεπιθέσεων ..... - 75 -
4. Σχέδιο αντιμετώπισης κυβερνοεπιθέσεων σε βάρος επιχειρήσεων ..... - 85 -
5. Δυσχέρειες στον εντοπισμό και τη δίωξη των κυβερνοεπιθέσεων ..... - 89 -
ΕΠΙΛΟΓΟΣ ..... - 93 -
ΒΙΒΛΙΟΓΡΑΦΙΑ ..... - 97 -
Ελληνόγλωσση ..... - 97 -
Ξενόγλωσση ..... - 98 -
Διαδικτυακές πηγές..... - 106 -
ΠΑΡΑΡΤΗΜΑΤΑ..... - 107 -
Παράρτημα Ι..... - 107 -

Περίληψη

Σε μια εποχή όπου οι επιχειρήσεις προβαίνουν σε αρκετές συναλλαγές μέσω του κυβερνοχώρου, οι επιθέσεις που αυτές δέχονται εντός αυτού, είναι πλέον πολύ συνηθισμένες. Οι κυβερνοεπιθέσεις λοιπόν σε βάρος των επιχειρήσεων αυξάνονται με ραγδαίο ρυθμό, και την ίδια αυξητική πορεία ακολουθούν και οι δυσμενείς συνέπειες. Ως απόρροια αυτού, κρίνεται σκόπιμη η αναφορά στον τομέα της κυβερνοασφάλειας, με σκοπό τη γενικότερη αντιμετώπιση των κυβερνοεπιθέσεων και την ασφάλεια του πληροφοριακού συστήματος της εκάστοτε επιχείρησης.

Εξαιτίας της πολυπλοκότητας του φαινομένου των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, έχουνε γίνει αρκετές προσπάθειες προκειμένου να διερευνηθούν οι μηχανισμοί μέσω των οποίων διάφοροι παράγοντες δρουν στη διαμόρφωση, συντήρηση και εξάπλωση του φαινομένου αυτού. Ο σκοπός της συγκεκριμένης εργασίας είναι να παρουσιάσει στους αναγνώστες μια πλήρη εικόνα του αντίκτυπου που έχουν οι κυβερνοεπιθέσεις στις επιχειρήσεις και να προτείνει πιθανούς τρόπους πρόληψης και αντιμετώπισης των επιθέσεων αυτών, λαμβάνοντας παράλληλα υπόψη τα ελληνικά και διεθνή δεδομένα και στοχεύοντας στη χάραξη και υλοποίηση αποτελεσματικής αντεγκληματικής πολιτικής.

Λέξεις - Κλειδιά:

κυβερνοεπίθεσεις, επιχειρήσεις, κίνδυνοι, ασφάλεια, τρόποι αντιμετώπισης

Abstract

In a time where companies conduct many transactions through cyberspace, attacks on these companies within cyberspace, have become commonplace. Cyber attacks on companies are therefore increasing rapidly, and with them come negative consequences. As a result, it is considered strategic to focus on the field of cybersecurity, in order to generally address cyber attacks and ensure the security of the information system of each company.

Due to the complexity of the phenomenon of cyber attacks on companies, there have been several efforts to examine the mechanisms through which various factors contribute to the formation, maintenance and expansion of this phenomenon. The aim of this study is to present to the readers a comprehensive picture of the impact of cyber attacks on companies and to suggest possible methods of preventing and addressing these attacks, taking into account Greek and international data and aiming at the design and implementation of an effective counter-cyber policy.

Keywords

cyber attacks, companies, risks, security, coping strategies

ΠΡΟΛΟΓΟΣ

Τις τελευταίες δεκαετίες, μαζί με τη ραγδαία ανάπτυξη της τεχνολογίας γενικότερα και ειδικότερα των Τεχνολογιών της Πληροφορικής και της Επικοινωνίας, γεννήθηκε και ωρίμασε η χρήση του κυβερνοχώρου ως εργαλείο στην καθημερινή ζωή όλων των ανθρώπων, με σκοπό την πληροφόρηση, την επικοινωνία, την ψυχαγωγία, την ικανοποίηση αναγκών, την εκπαίδευση, το εμπόριο.

Ταυτόχρονα, οι επιχειρήσεις στράφηκαν και αυτές προς τον κυβερνοχώρο, με αποτέλεσμα να εξαρτώνται πλέον σε μεγάλο βαθμό από τα ψηφιακά συστήματα. Ωστόσο, πέραν των ευχερειών (π.χ. δυνατότητα για επικοινωνία, αποθήκευση δεδομένων, άμεσες συναλλαγές, κ.λπ.), η εξάρτηση αυτή δημιούργησε και αρκετές απειλές. Το γεγονός αυτό ήταν αναμενόμενο, αφού ταυτόχρονα με την τεχνολογία, αναπτύσσεται και η εγκληματική δραστηριότητα. Έτσι λοιπόν οι κυβερνοεγκληματίες, εκμεταλλευόμενοι τις δυνατότητες και τις υπηρεσίες του κυβερνοχώρου, διαπράττουν κυβερνοεπιθέσεις σε βάρος των επιχειρήσεων, μέσα από ευκαιρίες που τους δίδονται για υποκλοπή εταιρικών δεδομένων, κωδικών πρόσβασης, τραπεζικών λογαριασμών και αριθμών πιστωτικών καρτών, κ.λπ.. Το γεγονός αυτό δύναται να βλάψει τη φήμη των επιχειρήσεων επηρεάζοντας αρνητικά τρίτους όπως τους πελάτες τους, τυχόν προμηθευτές, τους συνεργάτες και το προσωπικό τους, αλλά και να προκαλέσει τεράστια οικονομική και υλική ζημία.

Παράλληλα όμως, ενώ τα πρόσωπα που εγκληματούν ανακαλύπτουν διαρκώς εναλλακτικούς τρόπους διάπραξης κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, ταυτόχρονα και οι ιθύνοντες σε ζητήματα ασφαλείας καθώς και οι διωκτικές αρχές, για να συμβαδίζουν με την τεχνολογία, ανακαλύπτουν νέα προγράμματα, τεχνικές και μέσα εξιχνίασης με σκοπό την αντιμετώπιση των κυβερνοεπιθέσεων και τη γενικότερη προστασία των εννόμων αγαθών της περιουσίας, της προσωπικής ελευθερίας, της τιμής.

Μέχρι σήμερα οι κυβερνοεπιθέσεις σε βάρος των επιχειρήσεων, έχουν συζητηθεί αρκετά από τα Μέσα Μαζικής Ενημέρωσης, τις κυβερνήσεις και τους νομικούς. Έτσι και η εργασία αυτή, αποτελεί μια προσέγγιση γύρω από το ζήτημα των κυβερνοεπιθέσεων εις βάρος των επιχειρήσεων και την αντιμετώπισή τους.

Πιο συγκεκριμένα, στο πρώτο μέρος δίνονται ορισμένες εισαγωγικές παρατηρήσεις αναφορικά με τις βασικές έννοιες που θα μας απασχολήσουν, ήτοι την έννοια της «επιχείρησης» και την έννοια του «κυβερνοχώρου», προκειμένου να

προσεγγίσουμε το φαινόμενο με τον καλύτερο δυνατό τρόπο. Ταυτόχρονα γίνεται μία σύνδεση αυτών μέσα από την είσοδο των επιχειρήσεων στον ψηφιακό κόσμο του κυβερνοχώρου, η οποία οδηγεί είτε σε οφέλη που αποκομίζουν οι επιχειρήσεις, είτε σε κινδύνους με τους οποίους έρχονται αντιμέτωποι εντός αυτού.

Το δεύτερο μέρος εστιάζει στο φαινόμενο των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων. Πιο συγκεκριμένα προσεγγίζεται το φαινόμενο εννοιολογικά και παρατίθενται το γενικό προφίλ, τα κίνητρα, οι επιπτώσεις αυτού και τα χαρακτηριστικά γνωρίσματα, με έμφαση στον σκοτεινό αριθμό που παρουσιάζει το φαινόμενο ένεκα του συνδυασμού πολλών παραγόντων, όπως η αποσιώπηση περιστατικών για την προστασία της φήμης της εκάστοτε επιχείρησης. Επιπρόσθετα, παρουσιάζονται οι κατηγοριοποιήσεις, από τις πολλές που έχουν επιχειρηθεί έως σήμερα, μαζί με τους τύπους κυβερνοεπιθέσεων που εμπίπτουν σε αυτές. Η κατηγοριοποίηση αφορά το πεδίο εφαρμογής τους, τον σκοπό, τη σοβαρότητα, τη νομική υπόσταση, και τη διάκριση τους σε γνήσιες και μη γνήσιες κυβερνοεπιθέσεις. Ακόμη, αναλύονται ορισμένες δημοφιλείς κυβερνοεπιθέσεις (phishing, salami slicing, ransomware, cryptojacking) και παρουσιάζονται ορισμένα στατιστικά δεδομένα, από τα ελάχιστα που είναι διαθέσιμα σε επίπεδο επιχειρήσεων.

Εν συνεχεία, στο τρίτο μέρος παρουσιάζεται η τυπολογία ομάδων που προβαίνουν σε κυβερνοεπιθέσεις γενικά, σύμφωνα με την πρόταση που έκανε ο McGuire (2012), καθώς και οι ρόλοι που λαμβάνουν τα μέλη κάθε ομάδας. Επίσης, ακολουθούν παραδείγματα κυβερνοεπιθέσεων που έλαβαν χώρα σε βάρος διάφορων επιχειρήσεων, μέσα από τα οποία εμφανίζεται η κυρίαρχη επίπτωση που είναι η οικονομική ζημία.

Το τέταρτο μέρος εστιάζει σε ζητήματα κυβερνοασφάλειας, μέσα από επισημάνσεις που γίνονται για να τονιστεί η σπουδαιότητά της. Παράλληλα, ενώ από τη μία γίνεται αναφορά στον Γενικό Κανονισμό Προστασίας Δεδομένων (Γ.Κ.Π.Δ.), παρουσιάζονται ενδεικτικά διάφορα μέτρα για την πρόληψη και παρατίθεται ένα σχέδιο αντιμετώπισης, από την άλλη επισημαίνονται οι δυσχέρειες που εμποδίζουν την εξιχνίαση των περιστατικών αυτών (π.χ. νομοθεσία, απουσία αποδείξεων, κ.λπ.).

Τέλος, στον επίλογο παρατίθενται εν συντομία οι προβληματισμοί που αναδύονται από τη βιβλιογραφική ανασκόπηση, προτείνοντας παράλληλα μέτρα που θα μπορούσαν να εφαρμοστούν, τόσο διεθνώς όσο και στον ελλαδικό χώρο.

ΜΕΡΟΣ Α΄

Εισαγωγικές παρατηρήσεις

1. Εισαγωγή στην κοινωνία της πληροφορίας

Η ραγδαία ανάπτυξη της τεχνολογίας γενικότερα, και ειδικότερα των τεχνολογιών της πληροφορικής και της επικοινωνίας, συνιστούν αναμφισβήτητα μία αλήθεια στις ημέρες μας, η οποία συνοδευόμενη από το φαινόμενο της παγκοσμιοποίησης, θέτουν στο επίκεντρο των επιστημονικών μελετών την κοινωνία της πληροφορίας.

Σύμφωνα με τις κατευθυντήριες οδηγίες της 2054^{ης} Συνόδου της Ευρωπαϊκής Ένωσης την 1^{η} Δεκεμβρίου 1997 με θέμα «Τηλεπικοινωνίες», προσδιορίστηκε ένα ολοκληρωμένο εννοιολογικό πλαίσιο για την κοινωνία της πληροφορίας, όπου τεκμηριώθηκαν τα ακόλουθα: «*Η σύγχρονη κοινωνία βρίσκεται σε μια νέα κατάσταση όπου χαμηλού κόστους πληροφορίες, αποθηκευμένες σε σειρές δεδομένων και τεχνολογίες μετάδοσης πληροφοριών, βρίσκονται σε γενική χρήση. Η κατάσταση αυτή οδηγεί σε μια γενίκευση της πληροφορίας και χρήσης των δεδομένων που συνοδεύεται από οργανωτικές, εμπορικές και νομικές καινοτομίες, οι οποίες μεταλλάσσουν τη ζωή του κόσμου της παραγωγής αλλά και της κοινωνίας ως σύνολο*» (European Communities, 1997, p.15).

Σήμερα, η κοινωνία της πληροφορίας συνιστά τον κόσμο στον οποίο ζούμε και αναπτύσσουμε τις καθημερινές μας δραστηριότητες. Αν ανατρέξουμε στο παρελθόν, θα δούμε ότι για πολλούς αιώνες, η κοινωνία αυτή χαρακτηρίζονταν ως αγροτική κοινωνία, η οποία στηριζόταν στην καλλιέργεια της γης και την κτηνοτροφία. Με την πάροδο των χρόνων και συγκεκριμένα μεταξύ των ετών 1750 έως 1850, η αγροτική κοινωνία μεταλλάχθηκε σε μία βιομηχανικά κατευθυνόμενη κοινωνία, όπου η αγροτική οικονομία ναι μεν δεν είχε εξαφανιστεί, όμως είχε παραδώσει την πρωταρχική θέση της στη βιομηχανία και την επεξεργασία των φυσικών αγαθών (Furnell, 2006, pp.1-2). Ωστόσο, τη δεκαετία 1940-1950, την βιομηχανικά κατευθυνόμενη κοινωνία ακολούθησε η κοινωνία της πληροφορίας [1]. Πλέον, η διείσδυση και η μεταμόρφωση της τεχνολογίας των ηλεκτρονικών

[1] Αξίζει να σημειωθεί ότι ο όρος «κοινωνία της πληροφορίας» έκανε την εμφάνισή του το έτος 1968 όπου χρησιμοποιήθηκε για πρώτη φορά από τον Ιάπωνα Koyama και ακολούθως το έτος 1971 από τον Masuda κατά τον επιχειρησιακό σχεδιασμό της κοινωνίας της πληροφορίας στην Ιαπωνία.

υπολογιστών, οδήγησε την πληροφορία στο επίκεντρο, με το χειρισμό και την ανταλλαγή αυτής να φέρνουν στην επιφάνεια μια νέα πραγματικότητα (Furnell, 2006, p.2).

Στην πραγματικότητα, η κοινωνία της πληροφορίας συνιστά μια κοινωνία εντός της οποίας παράγονται, χρησιμοποιούνται, διανέμονται, διαχειρίζονται και ενσωματώνονται με δημιουργικό και παραγωγικό τρόπο οι πληροφορίες, με απώτερο στόχο το κέρδος ενός ανταγωνιστικού πλεονεκτήματος κατά την άσκηση πολιτικής, πολιτιστικής και οικονομικής δραστηριότητας. Πρόκειται δηλαδή για ένα νέο οργανωτικό και κοινωνικό μοντέλο, με κύριο συστατικό στοιχείο την ψηφιοποιημένη πληροφορία, η οποία είναι προσπελάσιμη από όλους τους πολίτες της, ανεξαρτήτως γεωγραφικών και χρονικών περιορισμών, αντανακλώντας διάφορες πτυχές της καθημερινότητάς μας, όπως την επικοινωνία, την ψυχαγωγία, την εκπαίδευση, το εμπόριο, τις συναλλαγές, τη στρατηγική μεγάλων εταιριών, τις πολιτικές διακηρύξεις κ.ά.. Η αποτελεσματική λειτουργία του εν λόγω μοντέλου, βασίζεται στις τεχνολογίες της πληροφορικής και της επικοινωνίας γενικότερα, και στο διαδίκτυο ειδικότερα. Οι δε ευρύτερες πληθυσμιακές ομάδες που κατέχουν τα απαιτούμενα μέσα και συμμετέχουν σε αυτή τη μορφή της κοινωνίας, μπορούν να χαρακτηρισθούν ως ομάδες με «ψηφιακούς πολίτες» που εισέρχονται σε μία σύγχρονη μορφή κοινωνίας. Τα χαρακτηριστικά αυτού του μοντέλου, περιλαμβάνουν την πρόσβαση των «ψηφιακών πολιτών» σε μεγάλο όγκο πληροφοριών, τη μείωση του κόστους και του χρόνου πρόσβασης στην πληροφορία και την εκμηδένιση των αποστάσεων πρόσβασης (Παρασκευάς και σύν., 2015, σελ.40).

Η πρόσβαση κάθε πολίτη στην κοινωνία της πληροφορίας, αποτελεί ένα εξέχον ζήτημα. Για τον λόγο αυτό, το νομοθετικό πλαίσιο της χώρας μας μερίμνησε για την εξασφάλιση και ρύθμιση αυτής μέσα από το Ελληνικό Σύνταγμα. Έτσι λοιπόν, στην παράγραφο 2 του άρθρου 5^{A} του Συντάγματος [2], θεσπίζεται η υποχρέωση του κράτους να προσδίδει σε κάθε πολίτη το δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας, διευκολύνοντας ταυτόχρονα την πρόσβαση των πληροφοριών που διακινούνται ηλεκτρονικά. Η κοινωνία των πληροφοριών με τη σειρά της, οφείλει:

[2] *Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρούμενων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19.*

α) να εξασφαλίζει την πρόσβαση των πολιτών στις ευκαιρίες, τη γνώση και τις αγορές που παρέχουν οι νέες τεχνολογίες,

β) να διευκολύνει τη δημιουργία ενός περιβάλλοντος στο οποίο θα αναπτυχθούν καινοτομίες και θα ανθίσουν επιχειρηματικές πρωτοβουλίες, στηριζόμενη πάντοτε στο ισχύον θεσμικό πλαίσιο και τους μηχανισμούς της αγοράς,

γ) να διασφαλίζει τι ατομικές ελευθερίες και τα δικαιώματα των πολιτών,

δ) να προασπίζει τη λειτουργία των δημοκρατικών θεσμών και

ε) να παρέχει υποστήριξη σε όσους δεν επιτύχουν την ένταξή τους. Με τον τρόπο αυτό, ενισχύεται η κοινωνική και οικονομική ένταξη έκαστου πολίτη στο νέο αυτό μοντέλο οικονομίας, και συνάμα αποκλείεται κάθε πιθανότητα κοινωνικού αποκλεισμού (Παρασκευάς και σύν., 2015, σελ.40).

Τέλος, σύμφωνα με τον Furnell (2006) κρίνεται απαραίτητη η διάκριση ανάμεσα στις εννοιολογικές αποσαφηνίσεις και στους λειτουργικούς ορισμούς των όρων τεχνολογία και κοινωνία της πληροφορίας. Η τεχνολογία συνδέεται με την πρόκληση σημαντικών κοινωνικών αλλαγών που πιθανόν να μην είχαν επιτευχθεί, ενώ η κοινωνία της πληροφορίας, συνδέεται με την αξιοποίηση αυτών των αλλαγών, με βασική προϋπόθεση τη σωστή χρήση των τεχνολογιών της πληροφορίας. Στην εποχή μας, η τεχνολογία αποτελεί ένα πολύ σημαντικό εργαλείο για τον εκσυγχρονισμό του κράτους. Ακόμη και αν κάποιος επιλέξει να αποφύγει τη χρήση αυτής επιστρέφοντας σε πρακτικές του παρελθόντος (π.χ. ανάληψη χρημάτων από υποκατάστημα τράπεζας έναντι αναλήψεως από αυτόματη ταμειολογιστική μηχανή ΑΤΜ), το μόνο που θα επιτύχει θα είναι απλά το να πηγαίνει ένα βήμα πίσω χωρίς να εξελίσσεται και χωρίς να επιτρέπει την προσαρμογή και ένταξή του στην κοινωνία της πληροφορίας (Furnell, 2006, p.2).

2. Η έννοια της επιχείρησης

Για τις ανάγκες της παρούσας εργασίας, θα πραγματοποιηθεί μία σύντομη αναφορά στην έννοια των επιχειρήσεων. Σε ένα γενικό πλαίσιο, η επιχείρηση αντικατοπτρίζει μια κοινωνική κατασκευή ως απόρροια της σύνθεσής της από ανθρώπους. Ειδικότερα, πρόκειται για μια νομική οντότητα που σχηματίζεται από μία ομάδα ιδιωτών με σκοπό να δραστηριοποιηθεί (Teece, 2010). Η νομική αυτή οντότητα, στην ουσία αναφέρεται σε μία παραγωγική-οικονομική μονάδα η οποία

αξιοποιεί και συνδυάζει τους συντελεστές παραγωγής [3], με σκοπό αφενός την παραγωγή προϊόντων ή υπηρεσιών, αφετέρου τη διάθεσή τους στην αγορά έναντι ανταλλακτικής αξίας. Με τον τρόπο αυτό παράγει πλούτο, συμμετέχοντας σε όλα τα στάδια της οικονομικής δραστηριότητας (Κοντάκος και σύν., 2009, σελ.11).

Η οργάνωση των επιχειρήσεων βασίζεται στην αποκομιδή κερδών μέσω επιχειρηματικών δραστηριοτήτων και μη κερδοσκοπικών φιλανθρωπικών οργανώσεων. Εκτός από κερδοσκοπικές και μη κερδοσκοπικές, οι επιχειρήσεις μπορούν να διακριθούν ανάλογα με τον τομέα παραγωγής σε:

α) επιχειρήσεις πρωτογενούς παραγωγής, π.χ. γεωργικές, δασικές, αλιευτικές,

β) επιχειρήσεις δευτερογενούς παραγωγής, π.χ. βιομηχανίες, οικοτεχνίες, βιοτεχνίες,

γ) επιχειρήσεις τριτογενούς παραγωγής, π.χ. υπηρεσιών, μεταφοράς, εμπορικές, και

δ) επιχειρήσεις μικτής απασχόλησης.

Επιπλέον, ανάλογα με το μέγεθός τους [4] ταξινομούνται σε μικρές, μεσαίες και μεγάλες επιχειρήσεις, ενώ ανάλογα με το φορέα μπορεί να επρόκειτο για δημόσια, ιδιωτική, δημοτική-κοινοτική ή ακόμη και μικτή επιχείρηση. Τέλος, μια άλλη διάκριση των επιχειρήσεων πραγματώνεται με βάση τη νομική μορφή τους, όπου έχουμε τις ατομικές επιχειρήσεις, δηλαδή αυτές που απαρτίζονται μονάχα από ένα πρόσωπο που είναι ο ιδιοκτήτης ή ο ιδρυτής, απασχολούμενος ή βοηθούμενος από κάποιον αριθμό ατόμων, τις εταιρικές επιχειρήσεις, δηλαδή αυτές στις οποίες συνεργάζονται δύο ή περισσότερα άτομα και τις συλλογικές επιχειρήσεις όπου μπορεί να είναι τα σωματεία, οι σύλλογοι, οι συνεταιρισμοί κ.λπ. (Κοντάκος και σύν., 2009, σσ.11-12).

Μια επιχείρηση μοιράζεται αρκετά από τα νομικά δικαιώματα και τις ευθύνες των ατόμων, όπως για παράδειγμα τη δυνατότητα σύναψης συμβάσεων, το δικαίωμα να προσφύγει στη δικαιοσύνη, να δανειστεί χρήματα, να πληρώσει φόρους, να προσλάβει υπαλλήλους, να διαθέτει περιουσιακά στοιχεία ακόμα και να εισέρχεται στην κοινωνία της πληροφορίας και στον κυβερνοχώρο, τον οποίο θα ορίσουμε παρακάτω (Κοντάκος και σύν., 2009, σελ.12). Αξίζει να σημειωθεί ότι στην εποχή μας οι περισσότερες επιχειρήσεις, πέραν του φυσικού χώρου τους, έχουν εισέλθει και στον κυβερνοχώρο, ερχόμενες αντιμέτωπες και με τους κινδύνους που αυτός

[3] Με τον όρο συντελεστές παραγωγής νοούνται τόσο οι έμψυχοι συντελεστές, δηλαδή το ανθρώπινο δυναμικό μιας επιχείρησης, τόσο και οι άψυχοι συντελεστές, δηλαδή ο εξοπλισμός, οι εγκαταστάσεις και κάθε άλλο στοιχείο που υποβοηθά τη λειτουργία της εκάστοτε επιχείρησης, π.χ. η τεχνογνωσία.

[4] Το μέγεθος των επιχειρήσεων προσδιορίζεται βάσει είτε του αριθμού εργαζομένων, είτε του αριθμού πωλήσεων, είτε τέλος, του ισολογισμού τους.

ελλοχεύει, πέραν των ευχερειών που μπορεί να προσδίδει (De Marco et al., 2019). Με άλλα λόγια, υλοποιούν το ηλεκτρονικό επιχειρείν, στρατηγικές δηλαδή, βάσει των οποίων μπορούν και αναπτύσσουν την επιχειρηματική τους δραστηριότητα χρησιμοποιώντας τις νέες τεχνολογίες, διεκπεραιώνοντας τις συναλλαγές τους μέσα από τη χρήση ηλεκτρονικών μέσων και στοχεύοντας στην άμεση ανταπόκριση του καταναλωτή-πελάτη (Δουληγέρης & Μητρόπουλος, 2016).

Η συγκεκριμένη εργασία θα εστιάσει στη μελέτη όλων των επιχειρήσεων γενικότερα, χωρίς να γίνει κάποια διάκριση των κατηγοριών αυτών. Συνεπώς όπου χρησιμοποιείται ο όρος επιχείρηση χωρίς να γίνεται κάποια ειδικότερη επισήμανση, θα αναφερόμαστε σε κάθε είδος επιχείρησης, χωρίς να εξαιρέσουμε κάποια κατηγορία εξ αυτών.

3. Η έννοια του κυβερνοχώρου

Στη σημερινή εποχή, ο κυβερνοχώρος αποτελεί έναν τομέα που έχει δημιουργηθεί εξ ολοκλήρου από τον ανθρώπινο παράγοντα. Στην ουσία πρόκειται για μια έκρηξη πληροφοριών, η οποία μέσα σε ένα σύντομο χρονικό διάστημα, λόγω της ανάπτυξης των τεχνολογιών συλλογής, αποθήκευσης, επεξεργασίας, προβολής και μετάδοσης, οδήγησε σε μία ραγδαία αύξηση των πληροφοριών αυτών, διαθέσιμων σε ένα μεγάλο ποσοστό του παγκόσμιου πληθυσμού (45% κατά το έτος 2016; Φρυδάς, 2018, σελ.25).

Ο κυβερνοχώρος εκτός της ποσοτικής αλλαγής που επέφερε, προκάλεσε συνάμα και μια ποιοτική αλλαγή. Πιο συγκεκριμένα οδήγησε στη δημιουργία μιας νέας οικονομίας και κοινωνίας. Η ποιοτική αυτή αλλαγή, οδήγησε με τη σειρά της σε μια νέα κατάσταση με κύριο χαρακτηριστικό την απώλεια της ιδιωτικότητας και την εμφάνιση της απειλής του κυβερνοεγκλήματος (Φρυδάς, 2018, σσ.25-26). Σε μια προσπάθεια προσδιορισμού του όρου του κυβερνοχώρου, γίνεται αντιληπτό ότι ο ίδιος λειτουργεί ως μια παγκόσμια εικονική πραγματικότητα που ξεπερνά τα εθνικά σύνορα και δημιουργεί νέα δεδομένα αναφορικά με το μέγεθος του τόπου τέλεσης της κάθε πράξης (Κιούπης, 1999, σελ.76).

Ως έννοια, χρησιμοποιήθηκε για πρώτη φορά από το συγγραφέα επιστημονικής φαντασίας William Gibson το 1984 (όπως αναφέρθηκε στο Benedikt, 1991), και μέχρι σήμερα, έχουν γίνει αρκετές προσπάθειες προκειμένου να αποδοθεί με ορθό τρόπο και να εξασφαλισθεί ένας κοινά αποδεκτός ορισμός του. Σε γενικές γραμμές, χρησιμοποιείται για να περιγράψει ένα πλασματικό περιβάλλον (π.χ.

διαδίκτυο) εντός του οποίου λαμβάνουν χώρα επικοινωνίες μέσω ηλεκτρονικών συστημάτων. Πιο συγκεκριμένα, ο Benedikt όρισε τον κυβερνοχώρο ως «*ένα νέο παράλληλο σύμπαν που δημιουργήθηκε και συντηρείται από ένα σύνολο υπολογιστών του κόσμου και από τις γραμμές επικοινωνίας τους*» (Benedikt, 1991, p.1). Πρόκειται δηλαδή για έναν κόσμο, μέσα στον οποίο μορφοποιείται η διακίνηση γνώσης, μυστικών, δεικτών, εικόνων, ήχων, ψυχαγωγίας και αλληλοεπιδράσεων μεταξύ διαφορετικών κόσμων. Κύριο χαρακτηριστικό του κυβερνοχώρου αποτελεί αφενός η συνεχή αλλαγή στην οποία υπόκειται, αφετέρου η κυριαρχία του, δεδομένου ότι καμία κεντρική οντότητα δεν επεμβαίνει ασκώντας έλεγχο στα δίκτυα που τον αποτελούν.

Εν ολίγοις, ο κυβερνοχώρος συνιστά έναν πολυδιάστατο, κοντινό αλλά και συνάμα απρόσωπο χώρο χωρίς αρχή και τέλος, που εξασφαλίζει την απόλυτη διεπαφή υπολογιστή και ανθρώπου (Mbanaso & Dandaura, 2015). Τέλος, θα πρέπει να επισημανθεί η διάκριση ανάμεσα στους όρους «κυβερνοχώρος» και «διαδίκτυο». Ο κυβερνοχώρος αποτελεί μία πιο ευρεία έννοια, δεδομένου ότι επιτρέπει στους χρήστες να πλοηγηθούν, να εξερευνήσουν και κυρίως να επικοινωνήσουν μεταξύ τους, σε αντίθεση με το διαδίκτυο, όπου η επιρροή των ανωτέρω μεταβλητών είναι πιο περιορισμένη (Kalay & Marx, 2005).

4. Η είσοδος των επιχειρήσεων στον κυβερνοχώρο

Η εξέλιξη της τεχνολογίας σήμερα, φέρνει τεράστιες αλλαγές στον τρόπο με τον οποίο λειτουργεί ο επιχειρηματικός κόσμος. Παρατηρούμε διαρκώς, επιχειρήσεις ανεξαρτήτως μεγέθους από ολόκληρο τον κόσμο, να εισέρχονται στον κυβερνοχώρο προκειμένου να εκμεταλλευτούν τις δυνατότητες που αυτός προσδίδει (Λάζος, 2001,σελ.25). Η είσοδός τους αυτή αποσκοπεί στη διευκόλυνση των καθημερινών δραστηριοτήτων και λειτουργιών τους, στην επέκταση των επιχειρηματικών τους στόχων τόσο σε εθνικό όσο και σε διεθνές επίπεδο και στη γενικότερη βελτίωση των δυνατοτήτων και της ανταγωνιστικότητάς τους στη νέα ψηφιακή, ευρωπαϊκή και παγκόσμια οικονομία (Wiggins, 2002).

Πιο συγκεκριμένα, ένας από τους βασικότερους λόγους για τον οποίο επιλέγει μια επιχείρηση να εισέλθει στο εικονικό αυτό περιβάλλον του κυβερνοχώρου, είναι η δυνατότητα που της παρέχεται για την προώθηση υπηρεσιών χωρίς να δεσμεύεται από χρονικούς και λοιπούς περιορισμούς (Ching & Ellis, 2004). Για παράδειγμα, μια επιχείρηση μπορεί να προβαίνει στις παραπάνω ενέργειες όλες τις ημέρες της

εβδομάδας ανεξαρτήτως αργιών, εορτών και καθ' όλη τη διάρκεια του εικοσιτετραώρου. Παράλληλα, παρέχεται η δυνατότητα εξυπηρέτησης των πελατών ανεξαρτήτως χωρικών περιορισμών, δηλαδή σε ολόκληρο τον κόσμο, χωρίς να απαιτείται η φυσική παρουσία κάποιου προσώπου ή της ίδιας της επιχείρησης.

Ένας ακόμη λόγος που συνέβαλε σε μεγάλο ποσοστό στο να εισέλθουν περισσότερες επιχειρήσεις στον κυβερνοχώρο, αποτελεί το γεγονός ότι μπορούν να διαφημίσουν τα προϊόντα ή τις υπηρεσίες τους με μικρότερο κόστος σε περισσότερους πελάτες, και να τους προσδίδουν τη δυνατότητα άμεσης επαφής με τις παροχές τους και αγοράς αυτών ενώ βρίσκονται στον προσωπικό τους χώρο. Με τον τρόπο αυτό αποφεύγεται η σπατάλη χρόνου από την πλευρά ορισμένων πελατών, ενώ παράλληλα οι επιχειρήσεις προσελκύουν περισσότερους πελάτες, οι οποίοι εξακολουθούν να επιλέγουν τη συγκεκριμένη επιχείρηση και ενδεχομένως να τη διαφημίζουν και σε τρίτους.

Ταυτόχρονα, θα πρέπει να τονίσουμε ότι η είσοδος των επιχειρήσεων στον κυβερνοχώρο, αποδείχθηκε εξαιρετικά κερδοφόρα, κατά τα τελευταία έτη. Αυτό αποδεικνύεται ιδιαίτερα εν μέσω πανδημίας Covid-19, η οποία οδήγησε σε διακοπή δραστηριοτήτων στις περισσότερες επιχειρήσεις όπου λειτουργούσαν με «φυσικό τρόπο» (Sharma et al., 2020). Έτσι λοιπόν, επιχειρήσεις οι οποίες είχαν προηγουμένως διευρύνει τους ορίζοντές τους στον κυβερνοχώρο, ή ακόμη και αυτές που ένεκα της πανδημίας αποφάσισαν να επεκταθούν σε αυτόν, κατάφεραν να λειτουργήσουν εν μέσω καραντίνας και ενδεχομένως να αυξήσουν και τα κέρδη τους, με αποτέλεσμα να μην προκύψει ουδεμία, ή έστω μηδαμινή, ζημία, όπως συνέβη με επιχειρήσεις όπου δεν το έκαναν.

Τέλος, μπορεί η είσοδος των επιχειρήσεων στον κυβερνοχώρο να γίνεται με σκοπό τη δημιουργία επιχειρηματικών ευκαιριών, ωστόσο επισημαίνεται ότι η εμφάνιση των κινδύνων (π.χ. από παράνομη πρόσβαση, αλλοίωση, κλοπή και ζημία γενικότερα των πληροφοριακών συστημάτων από μη εξουσιοδοτημένους χρήστες) υπερισχύει, προκαλώντας στο τέλος περισσότερη «ζημία» στην κάθε επιχείρηση, έναντι του «κέρδους» που έχει να αποκομίσει από την είσοδο αυτή (De Marco et al., 2019).

5. Η σκοτεινή πλευρά του κυβερνοχώρου και οι κίνδυνοι που διατρέχουν οι επιχειρήσεις σε αυτόν

Όπως στην επιστήμη της φαινομενολογίας όπου ένα φαινόμενο δύναται να είναι είτε φανερό είτε κρυφό, το ίδιο συμβαίνει και στην περίπτωση του κυβερνοχώρου. Από τη μία λοιπόν υπάρχει η φανερή του πλευρά με όλα τα προνόμια τα οποία παρέχει στον κάθε έναν οργανισμό, όπως αυτά που αναφέρθηκαν για τις επιχειρήσεις που εισέρχονται σε αυτόν στην προηγούμενη ενότητα, από την άλλη όμως, διαφαίνεται μια σκοτεινή πλευρά η οποία περιλαμβάνει τους κινδύνους που ελλοχεύουν και αυξάνονται με ραγδαίο ρυθμό (Ηλιοπούλου, 2018, σελ.425).

Κατά καιρούς έχουν γίνει αρκετές προσπάθειες προκειμένου να καταλήξουμε σε έναν ευρέως αποδεκτό ορισμό για τον κίνδυνο στον κυβερνοχώρο. Ωστόσο, από τη βιβλιογραφία δεν προκύπτει μία γενική ομοφωνία για την επίτευξη αυτών των προσπαθειών, ενώ συνάμα, αρκετοί από τους ορισμούς που έχουν δοθεί, αντανακλούν πιο περιορισμένα εννοιολογικά πλαίσια ενώ άλλοι παρουσιάζουν μια ευρύτερη προοπτική. Για παράδειγμα, ένας ορισμός υπό τη στενή έννοια δόθηκε από τον Mukhopadhyay και τους συνεργάτες του (2005), οι οποίοι συσχετίζουν τον κίνδυνο στον κυβερνοχώρο με την ύπαρξη κακόβουλων ηλεκτρονικών συμβάντων που προκαλούν διακοπή της επιχειρηματικής δραστηριότητας και χρηματική ζημία. Αντίθετα, οι Böhme και Kataria (2006) συνέδεσαν τον κίνδυνο στον κυβερνοχώρο με την αποτυχία των συστημάτων πληροφοριών, ενώ άλλοι ερευνητές με τον κίνδυνο ασφάλειας πληροφοριών, προσδίδοντας με αυτόν τον τρόπο μια πιο ευρεία περιγραφή του όρου «κίνδυνος στον κυβερνοχώρο» (Ögüt et al., 2011). Σε ένα γενικότερο πλαίσιο, θεωρείται ότι ο όρος «κίνδυνος στον κυβερνοχώρο» περιλαμβάνει ένα πλήθος πηγών κινδύνου που επηρεάζουν τα οικονομικά της εκάστοτε επιχείρησης, τα στοιχεία και τις πληροφορίες αναφορικά με τις εσωτερικές λειτουργίες και την οργάνωσή της, καθώς επίσης και λοιπά δεδομένα που εμπίπτουν στο απόρρητο κυβερνήσεων ή ατόμων (Eling & Wirfs, 2016, pp.5-6).

Οι κίνδυνοι που μπορεί να προκύψουν εντός του κυβερνοχώρου είναι πολλοί λόγω των διαρκών επιθέσεων και μπορεί να οδηγήσουν σε σημαντικές δυσλειτουργίες και αξιοσημείωτες απώλειες των επιχειρήσεων-στόχων. Συγκεκριμένα, αναφέρονται στη ζημία που μπορεί να προκληθεί σε έναν οργανισμό από μη εξουσιοδοτημένη πρόσβαση, χρήση, τροποποίηση, καταστροφή κ.λπ. δεδομένων, πληροφοριών και επικοινωνιών.

Σε γενικές γραμμές, τα δεδομένα αναφορικά με τους κινδύνους στον κυβερνοχώρο είναι περιορισμένα, αφενός διότι δεν υπάρχει κοινό πρότυπο για την καταγραφή των επιθέσεων σε αυτόν, αφετέρου γιατί οι ίδιες οι επιχειρήσεις αποσιωπούν προκειμένου να μη πλήττεται η φήμη τους (Wiggins, 2002). Το γεγονός αυτό μεταφράζεται σε όρους εγκληματολογίας με την εμφάνιση ενός μεγάλου σκοτεινού αριθμού των επιθέσεων στον κυβερνοχώρο, συμβάλλοντας σημαντικά στον περιορισμό της γνώσης όλων των πιθανών κινδύνων που ελλοχεύουν εντός αυτού. Ωστόσο, η Ευρωπαϊκή Ένωση, τον Μάιο του 2018 έθεσε σε ισχύ τον Γ.Κ.Π.Δ. (GDPR), βάσει του οποίου υποχρεώνονται οι επιχειρήσεις να αναφέρουν κάθε παραβίαση-κίνδυνο σε βάρος τους, εντός 72 ωρών, στην εκάστοτε αρμόδια εποπτική αρχή, με τη μη συμμόρφωσή τους, να επιφέρει την επιβολή ενός εξαιρετικά υψηλού προστίμου (άρθρο 33 GDPR).

Το ζήτημα των κινδύνων που αντιμετωπίζουν οι επιχειρήσεις στον κυβερνοχώρο αποτέλεσε αντικείμενο διερεύνησης των Garg και των συνεργατών του (Garg et al., 2003). Συγκεκριμένα, οι εν λόγω ερευνητές εξέτασαν τα διαθέσιμα δεδομένα, με σκοπό την καταμέτρηση του αντίκτυπου στην απόδοση των επιχειρήσεων, από τις πιθανές παραβιάσεις εντός του κυβερνοχώρου. Κατέληξαν στο συμπέρασμα ότι η παραβίαση της ασφάλειας των δεδομένων μιας επιχείρησης, μπορεί να θέσει σε κίνδυνο την εμπιστοσύνη των πελατών απέναντι της και κατ' επέκταση να οδηγήσει στην απομάκρυνσή τους, γεγονός το οποίο οδηγεί στην πτώση των μετοχών της και στη σταδιακή μείωση του κέρδους.

Ο Hallam-Baker, καταπιάστηκε και αυτός το 2008 με το ζήτημα των κινδύνων που ελλοχεύουν για τις επιχειρήσεις που εισέρχονται στον κυβερνοχώρο. Σύμφωνα με αυτόν, βασικός στόχος και κίνητρο των περισσότερων επιθέσεων στον κυβερνοχώρο ήταν η προσωπική διασκέδαση αυτού που έκανε την κυβερνοεπίθεση. Κάποιες άλλες φορές, τα εσωτερικά κίνητρα του δράστη τον ωθούσαν σε ενέργειες επίδειξης της ανωτερότητάς του και συγκεκριμένα απόδειξης της ικανότητάς του να προσπερνάει εύκολα το σύστημα μιας μεγάλης επιχείρησης και να βρίσκει απόρρητα στοιχεία τόσο δικά της όσο και των πελατών της. Μέσα από όλα αυτά, κατέληξε στο ότι με την πάροδο των ετών οι κίνδυνοι αυξάνονται, δεδομένου ότι οι επιθέσεις στον κυβερνοχώρο γενικότερα, και ειδικότερα στις επιχειρήσεις που αναπτύσσουν τη δραστηριότητά τους εντός αυτού, γίνονται ολοένα και πιο πολύπλοκες, με αποτελέσματα ακόμη πιο ολέθρια (Hallam-Baker, 2008).

Ακολούθως το 2010, οι Maillart και Sornette μελετώντας και αυτοί το ίδιο ζήτημα, ανέφεραν ότι η παράνομη δράση του ανθρώπινου παράγοντα στον κυβερνοχώρο, έχει ως απώτερο στόχο το προσωπικό κέρδος μέσω της εκμετάλλευσης των δεδομένων. Επιπλέον πρόσθεσαν ότι ορισμένες φορές ο δράστης ζητά από τις επιχειρήσεις που έπεσαν θύματα της κυβερνοεπίθεσης κάποιο χρηματικό ποσό, προκειμένου να μην προβεί στη γνωστοποίηση και έκθεση των στοιχείων που βρήκε (Maillart & Sornette, 2010).

Παρομοίως, ο Brockett και οι συνεργάτες του το 2012, ανέφεραν ότι οι κίνδυνοι που αντιμετωπίζουν οι επιχειρήσεις που αναπτύσσουν τις δραστηριότητές τους εντός του κυβερνοχώρου, αντιπροσωπεύουν μια διαρκώς αυξανόμενη απειλή τόσο για τους δημόσιους οργανισμούς όσο και για τις ιδιωτικές επιχειρήσεις. Βασική επίπτωση των κινδύνων αυτών αποτελεί η αλλοίωση φήμης της εκάστοτε επιχείρησης. Ταυτόχρονα, τόνισαν ότι ενδέχεται να προκαλέσουν βλάβη στο οργανωτικό σύστημα με αποτέλεσμα την πιθανή απώλεια εμπιστοσύνης είτε των ήδη υπαρχόντων πελατών, είτε ακόμη και των μελλοντικών. Σύμφωνα με τους ίδιους, το γεγονός ότι η τεχνολογία εξελίσσεται με τόσο ραγδαίους ρυθμούς και το ότι ο κυβερνοχώρος έχει διεισδύσει σε τόσο μεγάλο βαθμό στις ζωές όλων, άφησε απροετοίμαστες τις επιχειρήσεις με αποτέλεσμα να αδυνατούν να εξασφαλίσουν την προάσπισή τους έναντι των κινδύνων που δημιουργήθηκαν εξαιτίας αυτής της τεχνολογικής εξέλιξης. Πλέον, η εμφάνιση των απειλών και κινδύνων είναι πιο συχνή, με τη φύση τους να έχει τροποποιηθεί πλήρως και τη σοβαρότητά τους να έχει ενισχυθεί (Brockett et al., 2012).

Εν συνεχεία, ο Hall (2016) αναφέρθηκε και αυτός με τη σειρά του στους κινδύνους που διατρέχουν οι επιχειρήσεις στον κυβερνοχώρο. Συγκεκριμένα εστίασε στη στάση πολλών επιχειρήσεων, αναφορικά με τις πρακτικές που έχουν υιοθετήσει για την αντιμετώπιση των κυβερνοεπιθέσεων, και κατέληξε στο συμπέρασμα ότι οι επιχειρήσεις εφαρμόζουν ελλιπείς πρακτικές διαχείρισης κινδύνων και ότι δεν λαμβάνουν προληπτικά μέτρα αντιμετώπισης αυτών. Παράλληλα, υποστήριξε ότι η επιτυχία μιας επιχείρησης εξασφαλίζεται με βασική προϋπόθεση την ασφάλεια έναντι των κινδύνων στον κυβερνοχώρο. Κάτι τέτοιο επιτυγχάνεται με την ορθή επικοινωνία ανάμεσα στους ιθύνοντες της επιχείρησης και στο τμήμα ασφάλειας που διαχειρίζεται αυτούς τους κινδύνους, είτε πρόκειται για εσωτερικό τμήμα ασφάλειας είτε για εξωτερικούς συνεργάτες οι οποίοι έχουν αναλάβει την προστασία της επιχείρησης από κυβερνοεπιθέσεις (Hall, 2016).

Όλες οι προαναφερόμενες έρευνες αναφορικά με τους κινδύνους που απειλούν τις επιχειρήσεις που δραστηριοποιούνται στον κυβερνοχώρο, μας δίνουν μια βασική εικόνα ως προς τους γενεσιουργούς λόγους εμφάνισης των κινδύνων αυτών και κατ' επέκταση των επιθέσεων, με κυριότερο από αυτούς την επιθυμία για οικονομικό κέρδος και την ανάγκη για το αίσθημα ανωτερότητας. Ταυτόχρονα, μας γνωστοποιούν τις επερχόμενες συνέπειες αυτών, όπως τη ζημία, τόσο από άποψη οικονομική όσο και από οργανωτική του συστήματος, με δεδομένα να καταστρέφονται ολοσχερώς και να οδηγούν σε αρρυθμίες της ομαλής λειτουργίας της εκάστοτε επιχείρησης. Τέλος, καταλήγουν ότι η βασικότερη προϋπόθεση αντιμετώπισής τους είναι η εξασφάλιση ενός ασφαλούς συστήματος που θα μεριμνήσει για την πλήρη ετοιμότητα σε περιπτώσεις επιθέσεων και την ανάλογη αντιμετώπιση αυτών με αντίστοιχες τεχνικές (Garg et al., 2003; Hallam-Baker, 2008; Maillart & Sornette, 2010; Brockett et al., 2012; Hall, 2016).

Οι κίνδυνοι σήμερα αυξάνονται ολοένα και περισσότερο, αφού ο τρόπος δράσης των εγκληματιών γίνεται ακόμη πιο περίπλοκος, καθιστώντας δύσκολο τον εντοπισμό τους. Παράλληλα, οι εγκληματίες αλλάζουν τους στόχους τους, τον τρόπο επίδρασής τους στις επιχειρήσεις καθώς και τις μεθόδους επίθεσής τους σε διαφορετικά συστήματα ασφαλείας. Άλλοι παράγοντες που ενισχύουν τους κινδύνους είναι η εν γένει κατανεμημένη φύση του διαδικτύου, η εκτός της δικαιοδοσίας τους επίθεση των κυβερνοεγκληματιών που καθιστά την αστυνόμευση εξαιρετικά δύσκολη, η αυξανόμενη κερδοφορία και η εύκολη πρόσβαση του εμπορίου γενικότερα στο dark web (Wiggins, 2002).

Σε γενικές γραμμές μπορούμε να πούμε ότι οι κίνδυνοι στον κυβερνοχώρο μπορεί να πηγάζουν είτε από εξωτερικές απειλές, δηλαδή από ανθρώπους και μέσα που βρίσκονται εξωτερικά του δικτύου, είτε από εσωτερικές απειλές, από άτομα δηλαδή εντός του δικτύου που επιδιώκουν να αποπροσανατολίσουν τους διαχειριστές του ή από προσπάθειες σταδιακής ενσωμάτωσης ενός λανθασμένου κώδικα στο εκάστοτε δίκτυο, προκειμένου να προκληθεί σταδιακή αλλοίωση (Wiggins, 2002). Υπάρχουν συνεπώς από τη μία πλευρά οι εσωτερικοί κίνδυνοι που διακρίνονται στους εσωτερικούς κακόβουλους (Internal Malicious) και τους εσωτερικούς ακούσιους (Internal Unintentional) και από την άλλη οι εξωτερικοί κίνδυνοι, διακρινόμενοι με τη σειρά τους σε εξωτερικούς κακόβουλους (External Malicious) και εξωτερικούς ακούσιους (External Unintentional) (Πίνακας 1).

Εσωτερικοί Κίνδυνοι	Εσωτερικοί Κακόβουλοι (Internal Malicious)	Όταν κάποιο άτομο μέσα από την επιχείρηση εσκεμμένα διαγράφει ή κλέβει στοιχεία και δεδομένα.
	Εσωτερικοί Ακούσιοι (Internal Unintentional)	Όταν κάποιο άτομο μέσα από την επιχείρηση σβήσει δεδομένα του πληροφοριακού συστήματος μιας επιχείρησης, από αμέλεια.
Εξωτερικοί Κίνδυνοι	Εξωτερικοί Κακόβουλοι (External Malicious)	Οργανωμένες και ανεξέλεγκτες εγκληματικές επιθέσεις από πρόσωπα που βρίσκονται εκτός της επιχείρησης, αποκτώντας πρόσβαση σε δεδομένα που δεν τους ανήκουν, με σκοπό την υποκλοπή στοιχείων.
	Εξωτερικοί Ακούσιοι (External Unintentional)	Όταν κάποιο άτομο που βρίσκεται εκτός της επιχείρησης προκαλεί ζημία από αμέλειά του.

Πίνακας 1
Περιγραφή κατηγοριών εσωτερικών και εξωτερικών κινδύνων

Από τους ανωτέρω κινδύνους, ενώ οι εξωτερικοί κίνδυνοι είναι αυτοί που δημιουργούν μεγάλο όλεθρο για τις επιχειρήσεις, οι εσωτερικοί κίνδυνοι ενδέχεται να είναι ακόμη πιο καταστροφικοί, αφού οι δυσαρεστημένοι υπάλληλοι ή τα άπληστα στελέχη τους, μπορούν να προκαλέσουν υψηλότερες χρηματικές απώλειες (Wiggins, 2002).

Οι κίνδυνοι στον κυβερνοχώρο μπορούν επίσης να ταξινομηθούν ανάλογα με τη δραστηριότητα, το είδος και την πηγή της επίθεσης (Eling & Schnell, 2016). Έτσι λοιπόν, οι κίνδυνοι ανάλογα με τη δραστηριότητα μπορεί να είναι εγκληματικοί ή μη εγκληματικοί. Ως κίνδυνοι εγκληματικοί, μπορεί να θεωρηθούν οι επιθέσεις όπως κλοπή δεδομένων από hacker, ή ακόμη και ο εκβιασμός προκειμένου να εξασφαλίσουν κάποιο χρηματικό ποσό ώστε να μη δημοσιεύσουν τις πληροφορίες που βρήκαν. Αντίθετα, ως κίνδυνοι μη εγκληματικοί θεωρούνται για παράδειγμα οι φυσικές καταστροφές. Έτσι λοιπόν, η πυρκαγιά σε μια επιχείρηση ή σε τμήμα της επιχείρησης μπορεί να προκαλέσει απώλεια δεδομένων από τις πληροφοριακές βάσεις της εταιρείας. Παράλληλα, μη εγκληματικός κίνδυνος θεωρείται και η μη αποτελεσματική χρήση του τεχνολογικού εξοπλισμού μιας επιχείρησης, όπως για παράδειγμα η διαγραφή στοιχείων από το σκληρό δίσκο ύστερα από επανεκκίνηση του συστήματος. Οι κίνδυνοι επιπλέον, ανάλογα με το είδος της επίθεσης μπορεί να είναι κάποιο κακόβουλο λογισμικό, ανεπιθύμητη αλληλογραφία, επίθεση εμπιστευτικών πληροφοριών κ.ά., ενώ τέλος ανάλογα με την πηγή μπορεί να επρόκειτο για τρομοκράτες, εγκληματίες, την κυβέρνηση, κ.λπ. (Eling & Wirfs, 2016, pp.7-8).

Καταλήγοντας, θα πρέπει να σημειωθεί ότι όσο η τεχνολογία εξελίσσεται, τόσο εξελίσσονται και οι κίνδυνοι στον κυβερνοχώρο. Πλέον, αποτελούν μεγάλη πρόκληση και συνεχή απειλή, αφού μπορούν να θέσουν σε κίνδυνο επιχειρήσεις σε βαθμό ανεξέλεγκτο. Ταυτόχρονα, είναι δύσκολο να προσδιοριστούν σε σύγκριση με τους υπόλοιπους κινδύνους που διατρέχει μια επιχείρηση όπως είναι οι πιστωτικοί ή οι επενδυτικοί κίνδυνοι (Thornton, 2018). Θα πρέπει λοιπόν η κάθε επιχείρηση να εστιάζει στην προστασία των δικτύων και των συστημάτων της, και όχι μόνο στην ασφάλεια των φυσικών περιουσιακών στοιχείων και τις αστικές ευθύνες, όπως γινόταν στο παρελθόν, προκειμένου να προλάβει και να αντιμετωπίσει επιτυχώς τους ενδεχόμενους κινδύνους στον κυβερνοχώρο.

ΜΕΡΟΣ Β΄

Το φαινόμενο των κυβερνοεπιθέσεων κατά των επιχειρήσεων

1. Εννοιολογική προσέγγιση

Η ραγδαία τεχνολογική εξέλιξη έχει προκαλέσει αξιοσημείωτες αλλαγές στην καθημερινή ζωή των ανθρώπων, όπως αναφέρθηκε και παραπάνω. Μαζί με αυτές τις αλλαγές, οδήγησε και στην εμφάνιση νέων μορφών εγκληματικότητας, αλλά και στην εξέλιξη των ήδη υπαρχόντων. Έτσι λοιπόν, εκδηλώθηκε και εξέλιξη της εγκληματικότητας στον κυβερνοχώρο, με αποτέλεσμα να αναπτυχθούν νέοι τύποι επίθεσης, τεχνικές και μέσα που οδηγούν στην εύκολη πρόσβαση των εισβολέων ακόμη και στα πολύ καλά ελεγχόμενα περιβάλλοντα, προκαλώντας ζημίες σε πολλά επίπεδα. Ας δούμε όμως τη σημασία του όρου κυβερνοεπίθεση.

Όπως και στις μεταβλητές που αναφέρθηκαν προηγουμένως, έτσι και στην προκειμένη περίπτωση, δεν έχει γίνει κοινά αποδεκτή μία πλήρη και αντιπροσωπευτική εννοιολογική αποσαφήνιση της έννοιας των κυβερνοεπιθέσεων. Οι ορισμοί είναι αρκετοί με αντίστοιχες αναλύσεις και προεκτάσεις. Ταυτόχρονα, οι διχογνωμίες είναι εξίσου αρκετές, δεδομένου ότι χρησιμοποιούνται όροι όπως ηλεκτρονικό έγκλημα, κυβερνοέγκλημα, έγκλημα υψηλής τεχνολογίας κ.ά., ενώ η Ευρωπαϊκή Σύμβαση του Συμβουλίου της Ευρώπης δεν περιλαμβάνει κάποιον ακριβή ορισμό (Φαρσεδάκης, 2009). Παρόλα αυτά ως κυβερνοεπίθεση ορίζεται κάθε επίθεση ενός ή περισσότερων υπολογιστών εναντίον άλλων υπολογιστών ή δικτύων, με σκοπό είτε την απενεργοποίηση αυτών, είτε την απόκτηση πρόσβασης και τη διαχείριση δεδομένων. Στην ουσία πρόκειται για επίθεση που στοχεύει είτε να ασκήσει τον απόλυτο έλεγχο των συστημάτων υπολογιστών μέσω της διατάραξης, απενεργοποίησης ή καταστροφής αυτών, είτε να τροποποιήσει, να διαγράψει, να χειριστεί ή να κλέψει τις πληροφορίες που διατηρούνται εντός των συστημάτων αυτών (Waxman, 2011). Σε γενικές γραμμές, μία κυβερνοεπίθεση θέτει σε κίνδυνο την ασφάλεια πληροφοριών, επηρεάζοντας ταυτόχρονα την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους, που θα αναλυθούν παρακάτω.

Για την αποτελεσματικότερη καταγραφή των κυβερνοεπιθέσεων, μπορούμε να διακρίνουμε δύο βασικές κατηγορίες:

α) τις γνήσιες κυβερνοεπιθέσεις που συνιστούν γνήσια εγκλήματα τα οποία δεν προϋπήρχαν της εμφάνισης των ηλεκτρονικών υπολογιστών και του διαδικτύου, και ταυτόχρονα τελούνται και εξιχνιάζονται αποκλειστικά και μόνο με τη χρήση ψηφιακής τεχνολογίας, και

β) τις παραδοσιακές επιθέσεις-εγκλήματα, των οποίων η νομοτυπική μορφή υπήρχε πριν από την εμφάνιση των ηλεκτρονικών υπολογιστών, ωστόσο μπορούν να τελεσθούν και να εξιχνιασθούν και με τη χρήση/βοήθεια του ηλεκτρονικού υπολογιστή αλλά και χωρίς αυτή (Βλαχόπουλος, 2007, σελ.38).

Προκειμένου να πραγματοποιηθεί μία κυβερνοεπίθεση, ακολουθούνται κάποια βασικά στάδια τα οποία διαμορφώνουν και την ανατομία της. Τα στάδια αυτά είναι τα κάτωθι:

α) η προετοιμασία του δράστη μέσω συλλογής των απαιτούμενων πληροφοριών,

β) η εκμετάλλευση κάποιου τρωτού σημείου του λογισμικού και η πρόσβαση στα δικαιώματα και τις πληροφορίες,

γ) η εναπόθεση κωδικοποιημένων στοιχείων από το δράστη εφόσον καταλήξει στο επιθυμητό επίπεδο πρόσβασης με σκοπό μελλοντική πρόσβαση, και

δ) η εξαφάνιση και ο καθαρισμός των ιχνών (Lyle Artz, 2002, pp.16-17). Η δε διάρκεια των σταδίων αυτών, ποικίλλει ανάλογα με το πλήθος των συλλεγόντων πληροφοριών προ της επιθέσεως, το βαθμό τρωτότητας του εκάστοτε λογισμικού, την αρχική θέση του δράστη και κυρίως ανάλογα με το επίπεδο ικανοτήτων και δυνατοτήτων αυτού (Lyle Artz, 2002, pp.17-18).

Μία κυβερνοεπίθεση μπορεί να έχει διάφορα «θύματα», ή καλύτερα διάφορους στόχους. Στόχος της λοιπόν μπορεί να είναι δημόσιοι ή ιδιωτικοί οργανισμοί, υπάλληλοι ή στελέχη των οργανισμών αυτών ή ακόμη και σημαντικές εθνικές υποδομές όπως για παράδειγμα οι αερολιμένες, οι οργανισμοί παροχής ενέργειας κ.λπ.. Στην εργασία αυτή ωστόσο, θα μας απασχολήσουν οι δημόσιοι ή ιδιωτικοί οργανισμοί, δηλαδή οι επιχειρήσεις γενικότερα, ανεξαρτήτως μεγέθους, είδους και γεωγραφικής περιοχής.

Οι κυβερνοεπιθέσεις λοιπόν, δύναται να προσβάλλουν όχι μόνο επιχειρήσεις μεγάλου και μεσαίου μεγέθους, αλλά συνάμα και εκείνες που είναι μικρότερου μεγέθους. Πιο συγκεκριμένα, τα ευρήματα ερευνών φανέρωσαν ότι οι μικρές επιχειρήσεις βρίσκονται στο στόχαστρο των επιτιθέμενων στον κυβερνοχώρο σε ένα ποσοστό της τάξεως του 43%, με μόνο το 14% να θεωρούνται κατάλληλα προετοιμασμένες από άποψη κυβερνοασφάλειας (Alghamdi, 2021). Αυτός είναι και ο

βασικότερος λόγος για τον οποίο οι μικρές επιχειρήσεις συνήθως αδυνατούν να αντιμετωπίσουν επιτυχώς τις κυβερνοεπιθέσεις. Παράλληλα, σε κυβερνοεπίθεση μπορεί να υπόκειται οποιοσδήποτε κλάδος, ωστόσο εκείνοι που κινδυνεύουν περισσότερο είναι αυτοί που εμπλέκονται στενά με την καθημερινή ζωή των ανθρώπων. Τέτοια παραδείγματα αποτελούν οι χρηματοοικονομικοί τύποι επιχειρήσεων ή οργανισμών, τα ιδρύματα υγειονομικής περίθαλψης κ.ά. (Mclean, 2022). Πιο αναλυτικά, σύμφωνα με μελέτη της IBM Security, κατά το έτος 2021, οι κατασκευαστικές επιχειρήσεις μαζί με τις χρηματοοικονομικές/πιστωτικές βρισκόταν στις πρώτες θέσεις των επιχειρήσεων-στόχων κυβερνοεπιθέσεων, αντίθετα οι επιχειρήσεις των Μέσων Μαζικής Ενημέρωσης και εκπαίδευσης, είχαν πληγεί σε πολύ μικρό βαθμό, σε ποσοστά που εμφανίζονται στον πίνακα 2 που ακολουθεί (IBM Security, 2022b).

Τύποι Επιχειρήσεων	**Ποσοστό στο σύνολο των επιθέσεων (2021)**
Κατασκευαστικές	23.2
Χρηματοοικονομικές/Ασφαλιστικές	22.4
Επαγγελματικών Υπηρεσιών	12.7
Ενέργειας	8.2
Πωλήσεων	7.3
Υγείας	5.1
Μέσων Μαζικής Μεταφοράς	4.0
Κυβερνητικές	2.8
Εκπαίδευσης	2.8
Μέσων Μαζικής Ενημέρωσης	2.5

Πίνακας 2

Ποσοστό επιθέσεων ανά τύπο επιχείρησης κατά το έτος 2021

Πηγή: X - Force Threat Intelligence Index 2022 (IBM Security, 2022b)

Επιπρόσθετα, οι κυβερνοεπιθέσεις πραγματώνονται ανεξαρτήτως γεωγραφικής περιοχής με αποτέλεσμα η ύπαρξή τους να είναι γνωστή σε όλες τις ηπείρους. Ειδικότερα, σύμφωνα με μελέτη της IBM Security, κατά την καταγραφή

των γεωγραφικών τάσεων για το έτος 2021, η Ασία βρέθηκε στην πρώτη θέση με ποσοστό άνω του 26%, λόγω των αυξημένων επιθέσεων που δέχθηκε η Ιαπωνία κατά την τέλεση των Θερινών Ολυμπιακών Αγώνων, ενώ αντίθετα στην τελευταία θέση βρέθηκε η Λατινική Αμερική με ποσοστό 13%, (Πίνακας 3) (IBM Security, 2022b).

Γεωγραφικές Περιοχές	**Ποσοστό στο σύνολο των επιθέσεων (2021)**
Ασία	26.0
Ευρώπη	24.0
Βόρεια Αμερική	23.0
Μέση Ανατολή & Αφρική	14.0
Λατινική Αμερική	13.0

Πίνακας 3
Ποσοστό επιθέσεων ανά γεωγραφική περιοχή κατά το έτος 2021
Πηγή: X - Force Threat Intelligence Index 2022 (IBM Security, 2022b)

Γενικότερα, οι κυβερνοεπιθέσεις που πραγματώνονται σε βάρος των επιχειρήσεων, συνιστούν σήμερα ένα από τα πιο σημαντικά είδη κυβερνοεπιθέσεων. Στη βιβλιογραφία συναντώνται ως εταιρικά εγκλήματα στον κυβερνοχώρο (corporate computer crimes) και μας απασχολούν αρκετά λόγω των δισεκατομμυρίων δολαρίων που κοστίζουν κάθε χρόνο. Το εταιρικό έγκλημα στον κυβερνοχώρο στρέφεται όπως προαναφέρθηκε σε επιχειρήσεις και μέσω αυτού επιδιώκεται:

α) η τροποποίηση δεδομένων με κακόβουλο σκοπό,

β) η πρόσβαση σε επιχειρηματικά σχέδια και εταιρικές στρατηγικές,

γ) η πρόσβαση σε ιδιόκτητα δεδομένα, π.χ. πρόσβαση στη φόρμουλα ενός προϊόντος όπως τα φάρμακα,

δ) η απόκτηση προσωπικών πληροφοριών για τους εργαζόμενους της επιχείρησης, κ.ά. (Wiggins, 2002).

Ταυτόχρονα, αξίζει να σημειωθεί ότι τα εταιρικά εγκλήματα στον κυβερνοχώρο, δεν διαφέρουν πολύ από τα συμβατικά εγκλήματα του λευκού περιλαιμίου (white-collar crime) (Wiggins, 2002), τα οποία εισήγαγε στην εγκληματολογία ο Αμερικανός E. Sutherland (1949). Μπορούμε να πούμε δηλαδή ότι

πρόκειται για εγκλήματα επιχειρηματικών και οικονομικών κύκλων, όπως οικονομικές απάτες, κατάχρηση εξουσίας, αθέμιτος ανταγωνισμός μεταξύ επιχειρήσεων κ.λπ. (Ζαραφωνίτου, 2004, σσ.109-110).

Εκ των ανωτέρω τεκμαίρεται ότι οι κυβερνοεπιθέσεις αποτελούν έναν από τους κορυφαίους κινδύνους τόσο για τον ιδιωτικό όσο και για το δημόσιο τομέα. Συγκεκριμένα το 2020, είχαν καταταχθεί στην πέμπτη θέση των κινδύνων (Mclean, 2022), το 2021 αυξήθηκαν κατά μέσο όρο 50% παγκοσμίως σε σύγκριση με το 2020 [5] και το 2022, ο αριθμός τους συνέχισε να πολλαπλασιάζεται με γεωμετρική πρόοδο, με αποτέλεσμα να διεκδικούν θέση πρωτιάς μεταξύ των κινδύνων. Μικρές και μεσαίες επιχειρήσεις γίνονται ολοένα και περισσότερο στόχος κυβερνοεπιθέσεων, ενώ ταυτόχρονα αναμένεται αύξηση των τελευταίων κατά 200% μέχρι το 2025 (Alghambi, 2021). Οι κυβερνοεπιθέσεις λοιπόν έχουν ενταχθεί στην καθημερινότητά μας και είναι πραγματικά δύσκολο να προβλέψουμε το μέλλον τους, καθώς η εμπιστοσύνη των εγκληματιών στον κυβερνοχώρο έχει αυξηθεί λόγω της δυνατότητας αποφυγής του εντοπισμού τους. Για το λόγο αυτό είναι αναγκαία η βαθύτερη γνώση του φαινομένου αυτού, με σκοπό τη χάραξη και υλοποίηση αποτελεσματικής αντεγκληματικής πολιτικής.

2. Γενικό προφίλ κυβερνοεπιθέσεων

Όπως αναφέραμε και στο προηγούμενο υποκεφάλαιο, διάφοροι λειτουργικοί ορισμοί έχουν προταθεί, επιχειρώντας να απεικονίσουν με σαφήνεια τη φύση και την πολυπλοκότητα που χαρακτηρίζουν τις κυβερνοεπιθέσεις, χωρίς όμως να έχει υπάρξει μέχρι στιγμής ένας ορισμός που να είναι κοινά αποδεκτός από όλους (Hathaway et al., 2012 ; Owens et al., 2009). Παρόλα αυτά, ορισμένοι ερευνητές βασιζόμενοι στους ορισμούς που θα εκθέσουμε παρακάτω, κατέληξαν στο συμπέρασμα ότι οι κυβερνοεπιθέσεις παρουσιάζουν ένα κοινό προφίλ το οποίο αντανακλά πέντε γνωρίσματα που είναι τα εμπλεκόμενα μέρη, ο στόχος, τα κίνητρα, οι επιπτώσεις στον στόχο και η διάρκεια.

Η βιβλιογραφική ανασκόπηση διαφόρων άρθρων, με σκοπό την εννοιολογική αποσαφήνιση του όρου «κυβερνοεπίθεση», οδήγησε στον εντοπισμό των ακόλουθων έξι ορισμών:

[5] Μέσα στους τομείς που είχαν πληγεί περισσότερο, ανήκε η εκπαίδευση και η έρευνα, όπου δεχόταν πάνω από 1605 επιθέσεις κατά μέσο όρο, την εβδομάδα.

α) Η οποιαδήποτε ενέργεια που εκτελείται αποσκοπώντας στην υπονόμευση των λειτουργιών ενός δικτύου υπολογιστών για λόγους πολιτικής ή εθνικής ασφάλειας (Hathaway et al., 2012).

β) Η εκτέλεση σκόπιμων ενεργειών για μια εκτεταμένη χρονική περίοδο, που στοχεύουν στην τροποποίηση, υποβάθμιση, διατάραξη, ή και στην καταστροφή αντίπαλων συστημάτων υπολογιστών, δικτύων, προγραμμάτων και πληροφοριών (Owens et al., 2009).

γ) Οι επιχειρήσεις επίθεσης είτε άμυνας που στοχεύουν στην τροποποίηση, διαγραφή, καταστροφή των δεδομένων ή του λογισμικού, στην άρνηση πρόσβασης στον υπολογιστή για σκοπούς προπαγάνδας ή εξαπάτησης, μερικής ή ολικής δυσλειτουργίας του στοχευόμενου υπολογιστή/δικτύου και των συναφή στοιχείων που σχετίζονται με τον υπολογιστή/δίκτυο, και πρόκλησης φυσικής βλάβης και ζημίας σε εξωγενή από τον υπολογιστή, το δίκτυο ή το σύστημα, στοιχεία και αντικείμενα (Roscini, 2014, pp.1-42).

δ) Η αξιοποίηση του κυβερνοχώρου με σκοπό την επίτευξη πρόσβασης σε απόρρητες και μη εξουσιοδοτημένες πληροφορίες, την κατασκοπεία, την κλοπή δεδομένων και περιουσιακών στοιχείων/χρημάτων και την απενεργοποίηση δικτύων (Uma & Padmavathi, 2013).

ε) Οι πράξεις εχθρικού χαρακτήρα που διενεργούνται μέσω της χρήσης υπολογιστών, συναφών δικτύων ή συστημάτων και που στοχεύουν στη διατάραξη της λειτουργίας ή και στην καταστροφή περιουσιακών στοιχείων και συστημάτων των αντιπάλων (Staff, 2010).

στ) Οι ενέργειες που αποσκοπούν στην αλλαγή, διακοπή ή καταστροφή των συστημάτων υπολογιστών ή των συναφή δικτύων, των προγραμμάτων τους ή και των πληροφοριών τους (Waxman, 2011).

Κάθε ένας από τους ορισμούς που παρουσιάστηκε παραπάνω, επιχειρεί να απαντήσει σε μία, ή και περισσότερες, από τις ακόλουθες ερωτήσεις:

- ✓ Σε ποια είδη περιουσιακών στοιχείων στοχεύουν οι επιθέσεις στον κυβερνοχώρο;
- ✓ Ποιες είναι οι επιπτώσεις των κυβερνοεπιθέσεων στα στοχευμένα περιουσιακά στοιχεία;
- ✓ Τι παρακινεί τις επιθέσεις στον κυβερνοχώρο;
- ✓ Ποιοι παράγοντες εμπλέκονται στις κυβερνοεπιθέσεις;
- ✓ Ποια είναι η διάρκεια των κυβερνοεπιθέσεων;

Ως απάντηση στις προαναφερόμενες ερωτήσεις, οι ερευνητές σκιαγράφησαν ένα γενικό προφίλ που χαρακτηρίζει το μεγαλύτερο ποσοστό των κυβερνοεπιθέσεων και το οποίο αντανακλά πέντε βασικά γνωρίσματα:

α) *εμπλεκόμενα μέρη*

Τουλάχιστον δύο συμμετέχοντες εμπλέκονται σε κάθε κυβερνοεπίθεση, ο ιδιοκτήτης του περιουσιακού στοιχείου που αποτελεί και τον τελικό στόχο της επίθεσης και ένας αντίπαλος (Staff, 2010). Συνήθως, οι λειτουργικοί ορισμοί των κυβερνοεπιθέσεων δεν εξετάζουν τη φύση των αντιπάλων. Οι επιχειρήσεις αμυντικού ή επιθετικού χαρακτήρα μπορούν να εκτελεστούν είτε από κράτη, επιχειρήσεις, ομάδες, συλλόγους ή και μεμονωμένα σε ατομικό επίπεδο.

β) *στοχευμένα περιουσιακά στοιχεία*

Πέντε από τους έξι ορισμούς που παρατίθενται παραπάνω προσδιορίζουν τα περιουσιακά στοιχεία που στοχεύουν οι κυβερνοεπιθέσεις και τα οποία περιλαμβάνουν κυρίως συστήματα υπολογιστών και δίκτυα (Hathaway et al., 2012 ; Owens et al., 2009 ; Staff, 2010 ; Waxman, 2011), πληροφορίες, προγράμματα και λειτουργίες συστημάτων ή συναφή δικτύων (Hathaway et al., 2012 ; Owens et al., 2009 ; Roscini, 2014 ; Waxman, 2011) και αντικείμενα εξωγενή από τον υπολογιστή, το δίκτυο ή το σύστημα (Roscini, 2014).

γ) *κίνητρα*

Τα κίνητρα των κυβερνοεπιθέσεων αντανακλούν την πρόσβαση σε μη εξουσιοδοτημένες ή ασφαλείς πληροφορίες, την κατασκοπεία, την κλοπή δεδομένων και περιουσιακών στοιχείων (κυρίως χρημάτων) (Uma & Padmavathi, 2013). Επιπλέον, οι κυβερνοεπιθέσεις πραγματοποιούνται για λόγους εθνικής ασφάλειας και πολιτικών αιτιών (Hathaway et al., 2012), καθώς επίσης και για λόγους προπαγάνδας ή εξαπάτησης (Roscini, 2014).

δ) *επιπτώσεις στα στοχευμένα περιουσιακά στοιχεία*

Η τροποποίηση, η φθορά, η διαγραφή, η εξαπάτηση, η υποβάθμιση, η απενεργοποίηση ή/και η καταστροφή των περιουσιακών στοιχείων (Owens, et al., 2009 ; Roscini, 2014 ; Uma & Padmavathi, 2013 ; Waxman, 2011) σε συνδυασμό με την άρνηση πρόσβασης στα περιουσιακά στοιχεία (Roscini, 2014), αποτελούν σημαντικές απόρροιες των κυβερνοεπιθέσεων. Συνήθως, οι εν λόγω απόρροιες των κυβερνοεπιθέσεων αντανακλούν τρεις βασικές διαστάσεις, τη λογική διάσταση (όπως είναι η άρνηση πρόσβασης σε περιουσιακά στοιχεία), τη γνωστική διάσταση (όπως είναι η εξαπάτηση κατά την οποία γίνεται χρήση ψευδών πληροφοριών προκειμένου

να πειστεί ο αντίπαλος) και τη φυσική διάσταση (όπως είναι η καταστροφή του στοχευμένου περιουσιακού κεφαλαίου).

ε) *διάρκεια*

Μόνο ο ορισμός του Owens και των συνεργατών του (2009), αναφέρεται στην προβλεπόμενη διάρκεια των κυβερνοεπιθέσεων, τονίζοντας ότι μία κυβερνοεπίθεση είναι δυνατόν να διαρκέσει ένα παρατεταμένο χρονικό διάστημα.

Το ανωτέρω γενικό προφίλ, χαρακτηρίζει κάθε είδους κυβερνοεπίθεση. Συνεπώς αντικατοπτρίζει και τις κυβερνοεπιθέσεις σε βάρος επιχειρήσεων που μας απασχολούν στη συγκεκριμένη εργασία.

3. Χαρακτηριστικά γνωρίσματα και σκοτεινός αριθμός

Οι κυβερνοεπιθέσεις κατά επιχειρήσεων, όπως και γενικότερα όλες οι επιθέσεις που λαμβάνουν χώρα στον κυβερνοχώρο, φέρουν διάφορα χαρακτηριστικά, τα οποία καθιστούν δυσχερή τον εντοπισμό τους και κατ' επέκταση την εξιχνίασή τους ως εγκλήματα και την ποινική δίωξη των εισβολέων-δραστών. Τέτοια χαρακτηριστικά είναι:

- η *ανωνυμία*, αφού μέσω ορισμένων τεχνολογικών υποδομών του διαδικτύου και ιδίως του σκοτεινού διαδικτύου (Dark Web), παρέχεται η δυνατότητα στους δράστες να μη χρησιμοποιούν καθόλου τα προσωπικά τους στοιχεία ή ακόμη να κάνουν χρήση ψευδών για να προσελκύονται οι υποψήφιες επιχειρήσεις-θύματα,
- η *ταχύτητα*, αφού πρόκειται για μια στιγμιαία και άμεση επικοινωνία χωρίς μετακίνηση, με αποτέλεσμα την εύκολη και ανέξοδη επίθεση, πολλές φορές χωρίς να την αντιλαμβάνεται η ίδια η επιχείρηση-θύμα,
- η *ευκολία*, σε ότι έχει να κάνει με την επίθεση και κατ' επέκταση τη διάπραξη εγκλήματος αλλά και η δυσκολία στην εξιχνίαση καθώς δεν αφήνονται ίχνη, και
- ο *διασυνοριακός χαρακτήρας*, όπου τα αποτελέσματα μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς στόχους ανεξαρτήτως εδαφικού περιορισμού (Σφακιανάκης, 2016, σσ. 21-23).

Παράλληλα, πέραν των ανωτέρω χαρακτηριστικών γνωρισμάτων, προκύπτουν και ορισμένα άλλα χαρακτηριστικά στοιχεία των κυβερνοεπιθέσεων που τις καθιστούν στους δράστες, περισσότερο αποτελεσματικές. Τα χαρακτηριστικά αυτά είναι (Goderdzishvili, 2010):

- η *εναρμόνιση*

Ο επιτιθέμενος θα αναμένει να εναρμονιστεί η διαδικασία, προκειμένου να εισβάλει και να μολύνει το σύστημα. Ο συγχρονισμός των βημάτων που εμπλέκονται στην παράνομη απόκτηση των πληροφοριών, τους οδηγεί στην έγκαιρη και επιτυχή ολοκλήρωση των αποτελεσμάτων που περιμένουν.

- η *οργάνωση*

Οι επιτιθέμενοι χρησιμοποιούν οργανωμένες μεθόδους, για να εισβάλουν και να μολύνουν το σύστημα με περισσότερη ευκολία. Η χρήση οργανωμένων μεθόδων, θα τους οδηγήσει στην ολοκλήρωση περισσότερων επιτυχημένων αποτελεσμάτων.

- ο *αντίκτυπος*

Οι κυβερνοεπιθέσεις είναι συνήθως μεγάλης κλίμακας και ουσιαστικά μολύνουν δισεκατομμύρια υπολογιστές σε ολόκληρο τον κόσμο, επιφέροντας τεράστιες απώλειες δεδομένων και προκαλώντας σημαντικές οικονομικές ζημίες.

- η *αυστηρή οριοθέτηση*

Οι κυβερνοεπιθέσεις εκτελούνται με τέλεια ακολουθία και με τέτοιο τρόπο ώστε η προκύπτουσα ζημία να είναι αρκετά σοβαρή προκειμένου να θέσει σε κίνδυνο την ομαλή λειτουργία ολόκληρης της επιχείρησης.

- η *έλλειψη αυθορμητισμού* (*ad hoc*)

Οι κυβερνοεπιθέσεις εκτελούνται σκόπιμα, με σχολαστικό και πολύ προσεκτικό σχεδιασμό, στοχεύοντας στην πρόκληση της μέγιστης ζημίας.

- η *διαθεσιμότητα χρόνου και πόρων*

Οι κυβερνοεπιθέσεις προγραμματίζονται εκ των προτέρων, οπότε βασική προϋπόθεση για την οργάνωση μιας επίθεσης, αποτελεί η διαθεσιμότητα χρόνου και χρημάτων.

Τα ανωτέρω χαρακτηριστικά, δεν καλύπτουν όλο το φάσμα χαρακτηριστικών γνωρισμάτων που μπορεί να αναλυθεί. Παράλληλα, κατά την διερεύνηση των χαρακτηριστικών, έχουν αναδειχθεί διάφορα μεθοδολογικά προβλήματα, όπως το γεγονός ότι ορισμένες κυβερνοεπιθέσεις καταγράφονται με ακρίβεια, άλλες υπερεκτιμούνται, άλλες υποτιμούνται ενώ άλλες απουσιάζουν. Αυτό έχει ως συνέπεια, η εικόνα που παρουσιάζεται αναφορικά με τις κυβερνοεπιθέσεις σε βάρος επιχειρήσεων, να μην είναι αντιπροσωπευτική του συνόλου. Επιπρόσθετα, τα θύματα-επιχειρήσεις, για λόγους όπως η αποφυγή δικαστικής ταλαιπωρίας, η πιθανή χρηματική τους ικανοποίηση από τους δράστες, η ύπαρξη παράλληλα προς τη δημόσια και μιας «ιδιωτικής» δικαιοσύνης, η πεποίθηση πως κινδυνεύει η φήμη τους,

αλλά και λόγω της αμφιβολίας τους ως προς την αποτελεσματικότητα της ποινικής δικαιοσύνης, εκδηλώνουν έντονη απροθυμία στο να καταγγείλουν τις τελούμενες σε βάρος τους επιθέσεις, γεγονός το οποίο μεγεθύνει και αυτό από την πλευρά του το σκοτεινό αριθμό (Φαρσεδάκης, 2005, σελ.153) και κατ' επέκταση τον ακριβή αριθμό καθ' είδος και αριθμό των κυβερνοεπιθέσεων κατά των επιχειρήσεων.

Παράλληλα, ο εντοπισμός της προέλευσης των κυβερνοεπιθέσεων και κατ' επέκταση η διαλεύκανση αυτών των εγκλημάτων, καθίσταται ακόμη πιο δυσχερής λόγω των πολλαπλών τόπων τέλεσης και από το γεγονός ότι η εξωτερίκευση της επιθετικής συμπεριφοράς μπορεί να εντοπίζεται σε χώρα διαφορετική από εκείνη όπου βρίσκονται τα αποδεικτικά στοιχεία. Έτσι, λαμβάνοντας υπόψη και ότι οι αρμόδιες Αρχές σε πολλές χώρες δεν συνεργάζονται ή ακόμη απαιτούν εισαγγελική παρέμβαση για παροχή στοιχείων, δυσχεραίνει η ανακάλυψη και σύλληψη δραστών, αφήνοντας ένα μεγάλο αριθμό κυβερνοεπιθέσεων σε βάρος επιχειρήσεων, ανεξιχνίαστες. Η ύπαρξη αυτή του σκοτεινού αριθμού, δημιουργεί αρνητικές συνέπειες στις διάφορες επίσημες εγκληματολογικές στατιστικές, οι οποίες προέρχονται από αστυνομικές, δικαστικές και εισαγγελικές Αρχές, αφού καταλήγουν να απεικονίζουν την εμφανή εγκληματικότητα αναφορικά με τις κυβερνοεπιθέσεις στις επιχειρήσεις, χωρίς να καταλαμβάνουν και τις περιπτώσεις αθέατης εγκληματικότητας, καθώς μεταξύ του εμφανούς και του πραγματικού δείκτη των κυβερνοεπιθέσεων αυτών, μεσολαβεί ο λεγόμενος σκοτεινός αριθμός. Τέλος, τεκμαίρεται ότι η άγνοια των πραγματικών ποσοτικών και ποιοτικών διαστάσεων, έχει ως αποτέλεσμα τη δυσκολία στη χάραξη ορθολογικής και συνάμα αποτελεσματικής αντεγκληματικής ή εγκληματοπροληπτικής πολιτικής (Wiggins, 2002).

4. Κίνητρα

Προκειμένου να κατανοήσουμε καλύτερα τη φύση των κυβερνοεπιθέσεων κατά των επιχειρήσεων, θα πρέπει να μελετήσουμε τα κίνητρα που κρύβονται πίσω από αυτές. Με άλλα λόγια, θα πρέπει να αναζητήσουμε τους γενεσιουργούς παράγοντες που ωθούν σε μια τέτοια επίθεση. Οι επιθέσεις αυτές λοιπόν, πέραν του βασικότερου κινήτρου που είναι το οικονομικό, μπορεί να οφείλονται και σε πολιτικές συγκρούσεις, σε θρησκευτικές πεποιθήσεις, είτε ακόμη να προκαλούνται ένεκα της επικρατούσας κοινωνικής έντασης και πολιτιστικής διάστασης (Gandhi et al., 2011 ; Das & Nayak, 2013).

Βασικό λοιπόν κίνητρο της διενέργειας περιστατικών κυβερνοεπίθεσης σε βάρος επιχειρήσεων είναι η επιδίωξη χρηματοοικονομικού οφέλους. Η ανάγκη για εύκολη απόκτηση πλούτου και η απληστία που διακατέχει τους εισβολείς (επιχειρηματίες, στελέχη ή ιδιώτες), τους οδηγεί στο να εισβάλλουν παρανόμως στα δεδομένα επιχειρήσεων και με διάφορους τρόπους, όπως η κλοπή κωδικών πιστωτικών καρτών και τραπεζικών λογαριασμών, να τις ζημιώνουν οικονομικά (Balan, et al., 2017).

Ακόμη, μια τέτοια επίθεση μπορεί να οφείλεται σε πολιτικούς παράγοντες. Συνήθως, πρόκειται για επιθέσεις σε επιχειρήσεις πολιτικών εχθρών που εξαπολύονται από μέλη διαφορετικών πολιτικών παρατάξεων, με απώτερο στόχο την πρόκληση ζημίας στη φήμη τους ή ακόμη την κλοπή χρημάτων που αποσκοπεί στη χρηματοδότηση των δραστηριοτήτων τους (Gandhi et al., 2011). Τα πολιτικά κίνητρα δύναται να αφορούν και επιθέσεις με σκοπό την κατασκοπεία ή τη διαμαρτυρία σε βάρος κρατών ή κυβερνήσεων, για τις πολιτικές τους ενέργειες και τις γενικότερες κυβερνητικές τους δράσεις.

Παράλληλα, οι κυβερνοεπιθέσεις αυτές μπορεί να οφείλονται και σε κοινωνικούς ή πολιτιστικούς παράγοντες, όπως προαναφέρθηκε. Τέτοιοι παράγοντες μπορεί να είναι είτε οι γεωγραφικές και πολιτιστικές διαφορές, είτε συγκεκριμένοι επέτειοι ή ιστορικά γεγονότα, είτε ακόμη και ο ανταγωνισμός που αναπτύσσεται μεταξύ επιχειρήσεων που απαρτίζονται από διαφορετικές κοινωνικές ομάδες. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στους παράγοντες αυτούς, καθώς πολλές φορές, μια διαπολιτισμική σύγκρουση μπορεί να οδηγήσει σε εθνική σύγκρουση (Das & Nayak, 2013).

Πέραν της βασικής αυτής κατηγοριοποίησης των κινήτρων, ο Goderdzishvili (2010) κατέγραψε μία λίστα με πρόσθετα κίνητρα, όπως:

- η παρεμπόδιση πληροφοριών

Ο κύριος στόχος του επιτιθέμενου είναι να εμποδίσει την πρόσβαση σε σημαντικές πληροφορίες οποιασδήποτε εξουσιοδοτημένης επιχείρησης ή κυβερνητικών υπηρεσιών, για την απόκτηση συγκεκριμένων δεδομένων και πληροφοριών σε περίπτωση ανάγκης. Η πράξη αυτή θα έχει ως αποτέλεσμα να θέσει σε κίνδυνο την ικανότητα της εκάστοτε επιχείρησης ή της εκάστοτε κυβέρνησης να σχεδιάσει και να εκτελέσει μελλοντικά πλάνα δράσης.

- η αντιμετώπιση διεθνών μέτρων ασφαλείας στον κυβερνοχώρο

Απώτερος σκοπός είναι να αμφισβητήσουν και να σπάσουν ή να ξεπεράσουν τους κανόνες και τα μέτρα που έθεσε η διεθνής κοινότητα ασφάλειας στον κυβερνοχώρο. Ο επιτιθέμενος προσπαθεί να επιτύχει τον εν λόγω σκοπό μέσω της αύξησης της πολυπλοκότητας της επίθεσής του ή μέσω της απόκρυψης του προγράμματός του σε κάποια κανονική διαδικασία, η οποία στη συνέχεια παρακάμπτει τα μέτρα ασφαλείας.

- η επιβράδυνση της διαδικασίας λήψης αποφάσεων

Οι κυβερνοεπιθέσεις σε επιχειρήσεις συμβάλλουν σημαντικά στη διατάραξη της ισορροπίας και της ομαλής λειτουργίας κρίσιμων τομέων όπως του στρατού ή των υπηρεσιών έκτακτης ανάγκης, γεγονός που δύναται να επιφέρει καθυστέρηση στη διαδικασία λήψης αποφάσεων που αφορούν ζητήματα ζωής/θανάτου ή ζητήματα στρατιωτικού περιεχομένου.

- η άρνηση παροχής δημόσιων υπηρεσιών

Μέσω του αποκλεισμού πρόσβασης των εξουσιοδοτημένων χρηστών στις πληροφορίες οποιασδήποτε επιχείρησης ή κυβέρνησης που σχετίζεται με τη λειτουργία διαφόρων δημόσιων υπηρεσιών, οι επιτιθέμενοι μπορούν να προκαλέσουν σύγχυση σε διάφορους τομείς, όπως σε τράπεζες, στα μέσα μαζικής μεταφοράς, στα χρηματιστήρια, κ.ά..

- η μείωση της εμπιστοσύνης

Ένεκα της κλοπής των πληροφοριών και δεδομένων, παρατηρείται σημαντική μείωση της εμπιστοσύνης του κοινού σχετικά με την αξιοπιστία ή την ασφάλεια μιας επιχείρησης.

- η υποβάθμιση της φήμης της χώρας

Η υποβάθμιση της φήμης μιας χώρας αποτελεί πρωταρχικό κίνητρο μιας κυβερνοεπίθεσης. Ωστόσο, κάθε χώρα έχει αναπτύξει κατάλληλες τεχνικές και πρακτικές προκειμένου να ενισχύσει το κύρος της μεταξύ των διαφόρων αναπτυσσόμενων χωρών, σε περίπτωση υπονόμευσης από μεγάλης κλίμακας κυβερνοεπίθεση σε επιχείρηση.

Ταυτόχρονα, άλλοι παράγοντες που ωθούν στη διάπραξη κυβερνοεπιθέσεων σε βάρος επιχειρήσεων έχουν βρεθεί να είναι οι εξής:

- η ραγδαία αύξηση της τεχνολογίας και η ψηφιοποίηση κάθε πτυχής της καθημερινής και οικονομικής ζωής,
- η εκρηκτική αύξηση των χρηστών διαδικτύου που οδηγεί και στην αντίστοιχη αύξηση των δραστών σε συνδυασμό με το δείκτη χαμηλού κινδύνου που διατρέχουν ενόψει των τεράστιων κερδών,

- το γεγονός ότι οι επιχειρήσεις δεν μοιράζονται συνεχώς επίσημες πληροφορίες σχετικά με την εξάπλωση του φαινομένου, με αποτέλεσμα η κυβερνοεπίθεση να ανακαλύπτεται μετά από μήνες ή χρόνια,
- η ανάγκη των δραστών για ηθική ικανοποίηση και επιβεβαίωση των δυνατοτήτων τους, και
- η ελλιπής εκπαίδευση του προσωπικού που διαπραγματεύεται ζητήματα ασφαλείας της εκάστοτε επιχείρησης, η οποία δεν επιτρέπει τον έγκαιρο εντοπισμό τυχόν απειλών και εισβολών στα συστήματα δεδομένων, σε συνδυασμό με τις ανεπαρκείς επενδύσεις των επιχειρήσεων για ζητήματα κυβερνοασφάλειας. Από έρευνες έχει παρατηρηθεί ότι μόνο το 9% των επιχειρήσεων αυξάνει τον προϋπολογισμό του για την ασφάλειά τους στον κυβερνοχώρο, κατά 25% (De Marco et al., 2019).

Τα ανωτέρω κίνητρα, αποτελούν και τη βάση προκειμένου να προσδιοριστούν οι επιπτώσεις/κόστη που προκύπτουν στις επιχειρήσεις όπου προσβάλλονται από κυβερνοεπιθέσεις.

5. Επιπτώσεις

Τα κίνητρα που παρατίθενται στο προηγούμενο κεφάλαιο, οδηγούν ένα άτομο ή μια ομάδα ατόμων στην κυβερνοεπίθεση. Από τη στιγμή που θα καταλήξει η επίθεση αυτή να είναι επιτυχής, τότε οι επιπτώσεις είναι άμεσα εμφανείς στην επιχείρηση, προκαλώντας μεγάλη ζημία. Οι επιπτώσεις αυτές, αποτελούν τον αντίκτυπο του εγκλήματος στην επιχείρηση και στην πραγματικότητα είναι το άθροισμα των υλικών ζημιών/κόστους και των μη υλικών βλαβών στην επιχείρηση. Σήμερα, διανύοντας το έτος 2022, παρατηρείται αύξηση του συνολικού κόστους που προκαλείται στις επιχειρήσεις από την παραβίαση δεδομένων, σε σχέση με το 2020, η οποία αγγίζει το 13% (IBM Security, 2022a).

Αναλυτικότερα, οι επιπτώσεις ταξινομούνται σε οικονομικές, νομικές και λειτουργικές, συμπεριλαμβανόμενης σε αυτές και της ζημίας της φήμης (Kaspersky, 2015). Αναλυτικότερα, ως αντίκτυπος μιας κυβερνοεπίθεσης σε βάρος μιας επιχείρησης μπορεί να είναι (Livanis, 2016):

α) η οικονομική ζημία, η οποία ενδεχομένως να προκύπτει από κλοπή εταιρικών πληροφοριών, οικονομικών δεδομένων (π.χ. τραπεζικά στοιχεία, στοιχεία κάρτας αναλήψεως) και χρημάτων, είτε από απώλεια επιχείρησης ή σύμβασης, είτε ακόμη και από διακοπή των συναλλαγών (π.χ. αδυναμία πραγματοποίησης συναλλαγών

μέσω Διαδικτύου). Επιπλέον, εδώ μπορεί να συμπεριληφθεί και το κόστος με το οποίο επιβαρύνεται η εκάστοτε επιχείρηση για την επισκευή συστημάτων, δικτύων και συσκευών που προσβάλλονται κατά την παραβίαση όπου δέχεται. Ακόμη, άμεση οικονομική ζημία μπορεί να υποστούν και οι μέτοχοι της επιχείρησης, δεδομένου ότι η κυβερνοεπίθεση μπορεί να οδηγήσει σε πτώση της τιμής της μετοχής της επιχείρησης.

β) η προσφυγή στη νομική οδό με αγωγές από μετόχους, υπαλλήλους, πελάτες και τρίτα πρόσωπα των οποίων τα ψηφιακά δεδομένα προσβάλλονται. Ταυτόχρονα, εάν αυτά τα δεδομένα παραβιαστούν είτε με δόλο είτε από αμέλεια και δεν έχουν προηγουμένως εφαρμοστεί τα κατάλληλα μέτρα ασφαλείας που ορίζονται στους νόμους περί προστασίας δεδομένων και απορρήτου, ενδέχεται να επιβληθούν πρόστιμα και ρυθμιστικές κυρώσεις.

γ) η προσβολή της εταιρικής φήμης, η οποία διαβρώνει ένα βασικό στοιχείο της σχέσης ανάμεσα στην επιχείρηση και τον πελάτη, την εμπιστοσύνη. Αν και είναι δύσκολο να προσδιοριστεί πλήρως, οι επιχειρήσεις που πέφτουν θύματα επιθέσεων στον κυβερνοχώρο, είναι δυνατό να δουν την επωνυμία τους να αμαυρώνεται σημαντικά. Επακόλουθο αυτού ενδεχομένως να είναι η απώλεια πελατών και η μείωση πωλήσεων, με άμεση συνέπεια τη μείωση κερδών. Η επίδραση αυτή στη φήμη, μπορεί να επηρεάσει ακόμη και τις σχέσεις με συνεργάτες, προμηθευτές ή επενδυτές και άλλα τρίτα μέλη που ανήκουν στην επιχείρηση, τα οποία μπορεί να αισθάνονται ανασφάλεια αφήνοντας τις ευαίσθητες πληροφορίες και τα προσωπικά δεδομένα τους στα χέρια μιας επιχείρησης της οποίας το σύστημα είχε παραβιαστεί τουλάχιστον μία φορά. Εδώ, σημαντικός είναι και ο ρόλος των Μέσων Μαζικής Ενημέρωσης, τα οποία συνδράμουν στη διαμόρφωση της κοινής γνώμης, ανάλογα με τη συχνότητα προβολής και τον τρόπο σχολιασμού αυτών (Furnell, 2006, p.253).

δ) η δυσλειτουργία του συστήματος, δηλαδή η διακοπή των συστημάτων πληροφορικής που μπορεί να προκαλέσει αρνητικές συνέπειες στη συνολική λειτουργία της επιχείρησης, όπως για παράδειγμα τη μείωση εσόδων. Για παράδειγμα, κατά το έτος 2019, μία στις οκτώ επιχειρήσεις, δηλαδή ένα ποσοστό της τάξεως των 12%, αντιμετώπισε προβλήματα λόγω συμβάντων που σχετίζονταν με την Τεχνολογία Πληροφοριών και Επικοινωνίας και κατ’ επέκταση με τη λειτουργία του συστήματος (Business Continuity & Disaster Recovery, 2020) .

ε) η μείωση παραγωγικότητας και αποδοτικότητας, ένεκα της δυσλειτουργίας των συστημάτων πληροφορικής ή της αρνητικής ανταπόκρισης και ψυχολογίας των

εργαζόμενων. Αξίζει να σημειωθεί ότι πολλές φορές, η μείωση αυτή, ενδέχεται να οδηγήσει ακόμη και σε διακοπή λειτουργίας της επιχείρησης.

στ) ο εκβιασμός με απώτερο στόχο οικονομικά, λειτουργικά ή πολιτικά οφέλη.

Πιο περιληπτικά, οι κυβερνοεπιθέσεις σε βάρος των επιχειρήσεων, μπορούν να επηρεάσουν την παραγωγικότητα/αποδοτικότητα της επιχείρησης και τη θέση της στην αγορά, ενώ συνάμα μπορούν να κλονίσουν την εμπιστοσύνη των πελατών/καταναλωτών. Παράλληλα, η επιχείρηση χάνει πολλά από τα δεδομένα της και ενδεχομένως να κλαπούν εμπορικά μυστικά της, με επακόλουθο αποτέλεσμα όχι μόνο τον κλονισμό των σχέσεων με τους πελάτες της, λόγω έλλειψης εμπιστοσύνης, όπως προαναφέρθηκε, αλλά και την αποζημίωση που πρέπει να καταβληθεί, τις τυχόν συμβατικές κυρώσεις, το κόστος ανάκτησης ζημιών εικόνας και σχεδίων αποκατάστασης από καταστροφές, και τέλος τον ανταγωνισμό (De Marco et al., 2019; Livanis, 2016).

Όλες οι προαναφερόμενες επιπτώσεις είναι αρκετά σημαντικές και μπορούν να αποβούν μοιραίες αφού λειτουργούν ως φρένο στην ανάπτυξη των επιχειρήσεων και της χώρας συνολικά, εμποδίζοντας την ανάπτυξη εθνικών και παγκόσμιων οικονομιών. Τέλος, οι επιπτώσεις αυτές μπορεί να επηρεάζουν την επιχείρηση για αρκετά χρόνια, και για τον λόγο αυτό απαιτείται η έγκαιρη αναγνώριση των κυβερνοεπιθέσεων, προκειμένου να αντιμετωπιστούν και να προκληθεί το μικρότερο δυνατό κόστος.

6. Κατηγοριοποίηση και τύποι κυβερνοεπιθέσεων κατά επιχειρήσεων

Επί του παρόντος, υπάρχει ένας περιορισμένος αριθμός μελετών στη διεθνή βιβλιογραφία που να εξετάζει ενδελεχώς τους διάφορους τύπους των κυβερνοεπιθέσεων, τον τρόπο εξάπλωσής τους και τη σχετική σοβαρότητά τους, γεγονός που έχει καταστήσει πολλές επιχειρήσεις παγκοσμίως, ευάλωτες σε τέτοιου είδους επιθέσεις. Ωστόσο, ως προαπαιτούμενο στοιχείο για την ανάπτυξη και υιοθέτηση κατάλληλων μέτρων ασφαλείας θεωρείται η ακριβής κατανόηση τέτοιων επιθέσεων και η κατηγοριοποίησή τους. Επομένως, μία ολοκληρωμένη λίστα των κυβερνοεπιθέσεων σε συνδυασμό με την κατηγοριοποίησή τους, είναι πιθανόν να συμβάλλουν σημαντικά στη διαμόρφωση αποτελεσματικότερων πρακτικών πρόληψης και ασφάλειας στον κυβερνοχώρο (Uma & Padmavathi, 2013).

Μία κατηγοριοποίηση των κυβερνοεπιθέσεων, μπορεί να γίνει με βάση το πεδίο εφαρμογής τους, το σκοπό, τη σοβαρότητα και τη νομική υπόσταση. Με βάση λοιπόν το πεδίο εφαρμογής τους, διακρίνονται σε κακόβουλες επιθέσεις μεγάλης κλίμακας και σε μη κακόβουλες επιθέσεις μικρής κλίμακας (Howard, 2008). Ο όρος κακόβουλος σημαίνει «με σκοπό να προκληθεί βλάβη». Μια κακόβουλη επίθεση μεγάλης κλίμακας πραγματοποιείται συνήθως από ένα άτομο ή μια ομάδα με σκοπό την αποκόμιση προσωπικών οφελών ή την πρόκληση σύγχυσης, δυσλειτουργιών και χάους. Τέτοιες επιθέσεις λαμβάνουν τεράστιες διαστάσεις, αφορούν χιλιάδες συστήματα υπολογιστών και δικτύων και προκαλούν παγκόσμια κατάρρευση συστημάτων με σημαντικές απώλειες δεδομένων και ζημίες. Οι μη κακόβουλες επιθέσεις μικρής κλίμακας αφορούν κυρίως επιθέσεις που οφείλονται σε λανθασμένους χειρισμούς ή λειτουργικά λάθη ανεκπαίδευτου προσωπικού και μπορούν να προκαλέσουν μικρή απώλεια δεδομένων ή ελάχιστη δυσλειτουργία του συστήματος. Σε τέτοιες περιπτώσεις, τα δεδομένα είναι συνήθως ανακτήσιμα και ο αντίκτυπος του κόστους και της ζημίας δεν είναι σημαντικός (Howard, 2008).

Εν συνεχεία και σχετικά με την κατηγοριοποίηση των κυβερνοεπιθέσεων βάσει του σκοπού, προτάθηκαν τρία είδη επιθέσεων, ονόματι, οι αναγνωριστικές επιθέσεις (Goderdzishvili, 2010), οι επιθέσεις πρόσβασης (Ranum, 1997) και οι επιθέσεις άρνησης υπηρεσίας (Cashell et al., 2004 ; Jovičić & Simić, 2006). Οι αναγνωριστικές επιθέσεις αφορούν τη μη εξουσιοδοτημένη ανίχνευση και χαρτογράφηση του συστήματος και των υπηρεσιών του, και εσωκλείουν ορισμένες διαδικασίες και χαρακτηριστικά, όπως:

α) τη χρήση Packet Sniffers, όπου ο εισβολέας κάνει χρήση μιας ειδικής συσκευής προκειμένου να παρακολουθεί τις κινήσεις μεταξύ δικτυωμένων υπολογιστών και να προχωρήσει στην καταγραφή και αποθήκευση δεδομένων, τα οποία θα χρησιμοποιήσει σε μεταγενέστερες αναλύσεις,

β) τη μέθοδο Port Scanning (σάρωση της θύρας), όπου ο επιτιθέμενος επιχειρεί να εισβάλει σε έναν υπολογιστή μέσω της αποστολής μηνυμάτων, προκειμένου να μάθει ποιες από τις υπηρεσίες του υπολογιστή συσχετίζονται με έναν πολύ γνωστό αριθμό θύρας,

γ) τη μέθοδο σάρωσης Ping Sweep, όπου χρησιμοποιείται από τον εισβολέα προκειμένου να προσδιορίσει το εύρος των διευθύνσεων IP που αντιστοιχούν σε κεντρικούς υπολογιστές, και

δ) τη χρήση ερωτημάτων σχετικά με πληροφορίες στο διαδίκτυο, όπου ο εισβολέας μπορεί να απευθύνει ερωτήματα προκειμένου να μάθει σε ποιον ανήκει κάποιος τομέας και τις διευθύνσεις που έχουν εκχωρηθεί σε αυτόν τον τομέα (Goderdzishvili, 2010).

Παρομοίως, στις επιθέσεις πρόσβασης ο εισβολέας δημιουργεί τη δυνατότητα να αποκτήσει πρόσβαση σε μια συσκευή όπου δεν έχει εξουσιοδότηση ή τον κωδικό της, χακάροντας τα δεδομένα ή κατασκευάζοντας εργαλεία τα οποία είναι σε θέση να εκμεταλλευτούν τα τρωτά σημεία και τις ευπάθειες των εφαρμογών που δέχονται επίθεση (Ranum, 1997). Οι επιθέσεις πρόσβασης διακρίνονται με τη σειρά τους σε:

α) επιθέσεις στο μυστικό κωδικό (on secret code), όπου ο μη εξουσιοδοτημένος χρήστης προσπαθεί να χακάρει το λογαριασμό ενός μικρού τομέα χρησιμοποιώντας όλους τους πιθανούς συνδυασμούς κωδικών πρόσβασης,

β) επιθέσεις αξιοποίησης θύρας εμπιστοσύνης (utilization of trust port), όπου ο εισβολέας θέτει σε κίνδυνο έναν αξιόπιστο κεντρικό υπολογιστή προκειμένου να τον χρησιμοποιήσει για να οργανώσει σταδιακές επιθέσεις,

γ) επιθέσεις ανακατεύθυνσης θύρας (port redirection), όπου ένας εισβολέας χρησιμοποιεί έναν αξιόπιστο κεντρικό υπολογιστή προκειμένου να αποκτήσει πρόσβαση σε άλλους κεντρικούς υπολογιστές που προστατεύονται από ένα τείχος προστασίας δικτύου,

δ) επιθέσεις Man-in-the-middle, όπου αποτελούν ενεργές μορφές υποκλοπής, μέσω των οποίων ο εισβολέας συνδέεται με τα θύματα και αναμεταδίδει μηνύματα μεταξύ τους πείθοντάς τα ότι επικοινωνούν ιδιωτικά, και

ε) επιθέσεις ηλεκτρονικού ψαρέματος (phishing), όπου μέσω της αποστολής ψευδών ηλεκτρονικών μηνυμάτων, ο εισβολέας επιχειρεί να εξαπατήσει το θύμα προκειμένου να εκθέσει προσωπικά του δεδομένα και πληροφορίες (Ranum, 1997).

Τέλος, οι επιθέσεις άρνησης υπηρεσίας προκαλούν τόσο τη διατάραξη της ισορροπίας του συστήματος, επηρεάζοντας την ομαλή λειτουργία του και επιφέροντας καθυστερήσεις, διαγραφές και αλλοιώσεις πληροφοριών, όσο και την κατάρρευσή του (Cashell et al., 2004 ; Jovičić & Simić, 2006). Ο εισβολέας θα απενεργοποιήσει το δίκτυο ή θα καταστρέψει το σύστημα δικτύου, προκειμένου να αρνηθεί σκοπίμως τις υπηρεσίες του στους χρήστες (Mishra & Saini, 2009).

Μία περαιτέρω μεταβλητή που χρησιμοποιήθηκε από τους ερευνητές προκειμένου να κατηγοριοποιήσουν τα διάφορα είδη των κυβερνοεπιθέσεων, σχετίζεται με τη σοβαρότητά τους. Στο σημείο αυτό, οι κυβερνοεπιθέσεις

ταξινομούνται σε ενεργητικές και παθητικές (Uma & Padmavathi, 2013). Το κύριο συστατικό των ενεργητικών επιθέσεων είναι η ελευθερία του εισβολέα να μεταδώσει δεδομένα σε όλα τα μέρη ή να μπλοκάρει την μετάδοση των δεδομένων, επιλέγοντας μονές ή πολλαπλές κατευθύνσεις. Ο εισβολέας είναι σε θέση να τερματίσει τη μετάδοση των δεδομένων που αποστέλλονται από τα μέρη του δικτύου, καθώς βρίσκεται μεταξύ των διακομιστών. Αντιθέτως, οι παθητικές επιθέσεις αφορούν επιθέσεις κατά τις οποίες ένας μη εξουσιοδοτημένος εισβολέας παρακολουθεί την επικοινωνία μεταξύ δύο μερών για να αποσπάσει πληροφορίες μέσω υποκλοπών ή μέσω παρόμοιων μεθόδων, χωρίς όμως να παρεμβαίνει στη βάση δεδομένων (Uma & Padmavathi, 2013).

Ακολουθώντας παρόμοιο σκεπτικό, οι επιθέσεις στον κυβερνοχώρο κατηγοριοποιούνται και με βάση τη νομική τους υπόσταση. Έτσι, διακρίνονται σε ηλεκτρονικά εγκλήματα, σε κυβερνοκατασκοπεία, σε κυβερνοτρομοκρατία και σε κυβερνοπόλεμο (Goderdzishvili, 2010). Αναφορικά με τα ηλεκτρονικά εγκλήματα, ένας λειτουργικός ορισμός ο οποίος είναι κοινά αποδεκτός στη διεθνή εγκληματολογική βιβλιογραφία ορίζει το ηλεκτρονικό έγκλημα ως ένα ποινικό αδίκημα που περιλαμβάνει έναν υπολογιστή ως αντικείμενο του εγκλήματος ή ως το εργαλείο που χρησιμοποιείται για τη διάπραξη βασικών στοιχείων του αδικήματος. Οι παράγοντες που συμβάλλουν στη διαμόρφωση των ηλεκτρονικών εγκλημάτων είναι η ανωνυμία, οι ευπάθειες που χαρακτηρίζουν τη λειτουργικότητα του συστήματος, ο αποθηκευτικός χώρος του υπολογιστή και η έλλειψη γνώσεων του χρήστη (Singh, 2014). Από την άλλη πλευρά, η κυβερνοκατασκοπεία αντανακλά τη διαδικασία απόκτησης μυστικών πληροφοριών που αφορούν ομάδες, κυβερνήσεις και άτομα, με σκοπό την απόκτηση οφελών, χρησιμοποιώντας μεθόδους παράνομης κατάχρησης και τεχνικές κακόβουλων λογισμικών, συμπεριλαμβανομένων των δούρειων ίππων και του κατασκοπευτικού λογισμικού. Η δε κυβερνοτρομοκρατία, αφορά επιθέσεις που βασίζονται αποκλειστικά στο διαδίκτυο, αντικατοπτρίζοντας τρομοκρατικές δραστηριότητες, όπως τη σκόπιμη διακοπή της λειτουργίας ενός μεγάλου αριθμού δικτύου υπολογιστών, μέσω της εισαγωγής ιών (Janczewski & Colarik, 2007, pp.1-5). Τέλος, ο κυβερνοπόλεμος με τη σειρά του αφορά τις ενέργειες ενός κράτους να διεισδύσει σε υπολογιστή ή στο δίκτυο ενός άλλου έθνους, προκειμένου να προκαλέσει όσο το δυνατόν μεγαλύτερη ζημία (Goderdzishvili, 2010).

Πέραν της κατηγοριοποίησής τους με βάση το πεδίο εφαρμογής, τον σκοπό, τη σοβαρότητα και τη νομική υπόσταση, μία άλλη βασική κατηγοριοποίηση, όπως αναφέρθηκε και παραπάνω, είναι αυτή των γνήσιων κυβερνοεπιθέσεων, δηλαδή των εξελιγμένων νέων εγκλημάτων που στοχεύουν άμεσα στην ακεραιότητα της τεχνολογίας της πληροφορίας που δημιουργήθηκε με την έλευση των υπολογιστών και του διαδικτύου, και αυτή των παραδοσιακών επιθέσεων-εγκλημάτων που ενεργοποιούνται στον κυβερνοχώρο με τη χρήση ηλεκτρονικών υπολογιστών, δικτύων υπολογιστών ή άλλων μορφών επικοινωνίας, πληροφοριών και τεχνολογίας, δηλαδή εγκλήματα στα οποία η τεχνολογία της πληροφορίας λειτουργεί κυρίως ως εργαλείο (Βλαχόπουλος, 2007, σελ.38). Στις κατηγορίες αυτές υπάγονται διάφοροι τύποι κυβερνοεπιθέσεων που στοχεύουν επιχειρήσεις.

Έτσι λοιπόν, στην πρώτη κατηγορία κυβερνοεπιθέσεων εντάσσονται οι τύποι που εξαρτώνται αποκλειστικά από τον κυβερνοχώρο. Συνεπώς, η αντικειμενική υπόστασή τους πληρείται με την ύπαρξη τόσο του ηλεκτρονικού περιβάλλοντος όσο και της σύνδεσης στο διαδίκτυο. Τέτοιοι τύποι είναι:

α) η παράνομη παρεμβολή συστήματος ή δεδομένων

Σύμφωνα με το άρθρο 4 της υπ' αριθμόν 2013/40/ΕΕ οδηγίας του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, η παράνομη παρεμβολή σε σύστημα μπορεί να οφείλεται στην απλή εισαγωγή ηλεκτρονικών δεδομένων, στη διαβίβαση, ζημία, φθορά, αλλοίωση, διαγραφή ή εξάλειψη αυτών, είτε ακόμη και στον αποκλεισμό της πρόσβασης στα δεδομένα αυτά και δύναται να οδηγήσει σε σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών. Ομοίως, σύμφωνα με το άρθρο 5 της ανωτέρω οδηγίας, η παράνομη παρεμβολή σε δεδομένα μπορεί να οφείλεται στη φθορά, ζημία, αλλοίωση, εξάλειψη και διαγραφή ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών, είτε στον αποκλεισμό πρόσβασης στα δεδομένα αυτά (Ευρωπαϊκή Επιτροπή, 2017, σελ.8). Γενικότερα, οι παρεμβολές τόσο των δεδομένων, όσο και του συστήματος, τις περισσότερες φορές προέρχονται από μολύνσεις από κακόβουλο λογισμικό (malware), είτε ακόμη και από κακόβουλες ενέργειες ατόμων ή ομάδων που έχουν προηγουμένως αποκτήσει παράνομη πρόσβαση σε αυτά (Paoli et al., 2018). Ως κακόβουλο λογισμικό μπορεί να περιγραφεί ένα λογισμικό το οποίο έχει εγκατασταθεί σε ένα σύστημα χωρίς τη συγκατάθεση του χρήστη, με σκοπό να διακυβεύσει την εμπιστευτικότητα, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων. Οι πιο συνηθισμένοι τύποι αυτού

είναι ο ιός (virus) ο οποίος μολύνει τα εκτελέσιμα αρχεία και προκαλεί βλάβη μετά τη μόλυνση, το σκουλήκι (worm) το οποίο αναπαράγει τον εαυτό του και καταναλώνει χώρο και χρόνο για να ολοκληρώσει έναν παράνομο σκοπό παραδίδοντας ένα ωφέλιμο φορτίο κακόβουλου ιού ή προκαλώντας υπερφόρτωση δικτύου, η λογική βόμβα (logic bomb) η οποία προσαρτάται σε μια εφαρμογή και ακολούθως ενεργοποιείται από ένα συγκεκριμένο περιστατικό (π.χ. συγκεκριμένη ώρα και ημερομηνία, λογική συνθήκη κ.ά.) απελευθερώνοντας έναν ιό ή προκαλώντας άλλη ζημία, ο Δούρειος ίππος (Trojan horse) ο οποίος μέσω της μεταμφίεσης ή παραπλάνησης αποκρύπτει την πραγματική του λειτουργία, εισέρχεται στο σύστημα και αφού φτάσει στο στόχο του, απελευθερώνει έναν ιό ή σκουλήκι, κ.λπ. (Wiggins, 2002). Ταυτόχρονα, η παράνομη παρεμβολή συστήματος δύναται να προκληθεί και από επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDOS) ή από ανεπιθύμητη αλληλογραφία (spam), με αποτέλεσμα το ίδιο το σύστημα πληροφορικής να υπερφορτώνεται από την τεράστια ποσότητα δεδομένων και αιτημάτων που αποστέλλονται σε αυτό (Clough, 2010). Οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDOS) διακυβεύουν τη διαθεσιμότητα των δεδομένων, εκμεταλλευόμενες τα συγκεκριμένα όρια χωρητικότητας που ισχύουν για τους πόρους ενός συστήματος. Πιο συγκεκριμένα, στέλνονται πολλαπλά αιτήματα στο διακομιστή που δέχεται επίθεση, με σκοπό να υπερβεί την ικανότητα διαχείρισής τους επηρεάζοντας κατά αυτόν τον τρόπο τη λειτουργία τους (Douligeris & Mitrokosta, 2004). Από την άλλη πλευρά, η ανεπιθύμητη αλληλογραφία (spam), αφορά ηλεκτρονικά μηνύματα (email) με διαφημιστικό ή εμπορικό περιεχόμενο για αμφίβολα προϊόντα, προγράμματα γρήγορου πλουτισμού, νομικές υπηρεσίες κ.ά., τα οποία αποστέλλονται μαζικά σε παραλήπτες που δεν έχουν ζητήσει την αποστολή τους και οι οποίοι διαφορετικά δεν θα επέλεγαν να τα είχαν λάβει (Cranor & LaMacchia, 1998).

β) η παράνομη πρόσβαση σε συστήματα πληροφορικής

Η παράνομη πρόσβαση σε συστήματα πληροφορικής, όπως ρητά μνημονεύεται στο άρθρο 3 της υπ' αριθμόν 2013/10/ΕΕ οδηγίας του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, αναφέρεται όχι μόνο στην παράνομη απόκτηση πρόσβασης στο σύνολο ενός συστήματος πληροφοριών, αλλά συνάμα και στην παράνομη πρόσβαση σε μέρος αυτού (Ευρωπαϊκή Επιτροπή, 2017, σελ.7). Η παράνομη αυτή πρόσβαση, επιτυγχάνεται από τους hackers και τους crackers, οι

οποίοι αποκτούν πρόσβαση σε συστήματα και δεδομένα χωρίς εξουσιοδότηση, μέσω της χρήσης εργαλείων, όπως για παράδειγμα ανιχνευτές κωδικών πρόσβασης, Δούρειοι ίπποι κ.λπ., και μέσω τεχνικών οι οποίες αποσκοπούν στην κοινωνική κατασκευή πληροφοριών σύνδεσης από ανυποψίαστους χρήστες. Οι hackers διακρίνονται σε αυτούς με το «μαύρο καπέλο» ή αλλιώς hackers της «σκοτεινής πλευράς», δηλαδή αυτούς που αποκτούν πρόσβαση χωρίς άδεια και συχνά με επιβλαβή τρόπο, σε αυτούς με το «άσπρο καπέλο» που είναι οι ηθικοί που εργάζονται για το καλό των συστημάτων ασφαλείας (π.χ. υπάλληλοι και μισθωμένοι σύμβουλοι) και σε αυτούς με το «γκρίζο καπέλο», δηλαδή σε αυτούς που βρίσκονται ανάμεσα στις δύο προαναφερόμενες κατηγορίες και τα κίνητρά τους είναι αδιευκρίνιστα ή εναλλάσσονται διαρκώς. Αντίθετα οι crackers, λειτουργούν τις περισσότερες φορές ως hackers με «μαύρο καπέλο» και εισέρχονται στα συστήματα ασφαλείας αποκλειστικά για παράνομους και εγκληματικούς λόγους ή για προσωπικά κέρδη. Συνεπώς όλοι οι crackers είναι ταυτόχρονα και hackers, χωρίς να ισχύει και το αντίστροφο, γεγονός το οποίο διαφοροποιεί τις δύο αυτές κατηγορίες, δεδομένου ότι οι hackers δύναται να μην αποσκοπούν σε κακόβουλες δραστηριότητες και να μη παραβιάζουν τους νόμους με τις πράξεις τους (Furnell, 2006, pp.52-54). Ο συγκεκριμένος τύπος κυβερνοεπίθεσης σε βάρος επιχειρήσεων αποτελεί συχνά ένα προκαταρκτικό βήμα για τη διάπραξη πιο σοβαρών αδικημάτων στον κυβερνοχώρο, όπως η κυβερνοκατασκοπεία, η οποία παρατίθεται ακολούθως (Paoli et al., 2018).

γ) η κυβερνοκατασκοπεία

Η κυβερνοκατασκοπεία, η οποία αναφέρθηκε και στην κατηγοριοποίηση με βάση τη νομική υπόσταση, έχει ως στόχο, όπως προαναφέρθηκε, την απόκτηση με παράνομο τρόπο επιχειρηματικών και εμπορικών δεδομένων. Πιο συγκεκριμένα, τα δεδομένα αυτά δύναται να αφορούν τακτικές εταιρικές πληροφορίες (π.χ. έγγραφα που περιγράφουν επιχειρηματικές διαδικασίες ή στρατηγικές, τιμές προσφοράς συμβολαίων, κ.ά.), υψηλής αξίας πνευματική ιδιοκτησία (π.χ. πρωτότυπα προϊόντα) και μαζικά επιχειρηματικά δεδομένα (π.χ. στοιχεία πελατών ή υπαλλήλων και οικονομικά στοιχεία της επιχείρησης) (Paoli et al., 2018). Η μεθοδολογία αυτών των επιθέσεων περιλαμβάνει γενικά μια άμεση επίθεση μέσω δραστηριοτήτων κοινωνικής μηχανικής ή μέσω της εγκατάστασης κακόβουλου λογισμικού στα συστήματα της επιχείρησης-θύμα, επιτρέποντας στον εισβολέα να έχει τον απόλυτο έλεγχο. Αυτό το είδος επίθεσης, προέρχεται συνήθως από μια ανταγωνιστική επιχείρηση που έχει τις

περισσότερες φορές ως στόχο την ανάκτηση ενός κενού παραγωγής ή αγοράς. Προκειμένου αυτή η επίθεση να είναι προσοδοφόρα, απαραίτητη προϋπόθεση συνιστά η εμπλοκή ενός ειδικού σε υπολογιστές ή ενός άπιστου υπαλλήλου (De Marco et al., 2019).

Στη δεύτερη κατηγορία κυβερνοεπιθέσεων υπάγονται τύποι εγκλημάτων που προϋπήρχαν και τελούνται με την αρωγή της ψηφιακής τεχνολογίας, συνεπώς η αντικειμενική υπόσταση παραμένει ίδια, διαφοροποιείται όμως ο τρόπος τέλεσης και πιο συγκεκριμένα το μέσο τέλεσης. Τέτοιοι τύποι είναι:

α) ο κυβερνοεκβιασμός

Ο εκβιασμός στον κυβερνοχώρο είναι μια εγκληματική ενέργεια που διαπράττεται μέσω της παράνομης εγκατάστασης ενός κακόβουλου λογισμικού τύπου ransomware. Το ransomware, εγκαθίσταται σε υπολογιστές της επιχείρησης που είναι το θύμα χωρίς την άδειά της και διαδίδεται είτε μέσω μολυσμένων συνημμένων ηλεκτρονικών μηνυμάτων, είτε μέσω άλλων τύπων κακόβουλου λογισμικού. Πιο συγκεκριμένα, μέσω του λογισμικού αυτού ο εγκληματίας μπλοκάρει, εξ αποστάσεως, κάποιον υπολογιστή της επιχείρησης ή κρυπτογραφεί δεδομένα που είναι αποθηκευμένα στο σύστημα πληροφορικής, καθιστώντας τα απροσπέλαστα ή μη χρησιμοποιήσιμα για εξουσιοδοτημένους χρήστες. Πολλές φορές καθίσταται αδύνατη ακόμη και η λειτουργία ολόκληρου του συστήματος. Ακολούθως, η επιχείρηση, προκειμένου να ανακτήσει τα δεδομένα αυτά, θα πρέπει να εισάγει ένα κρυπτογραφικό κλειδί, το οποίο βρίσκεται στη διάθεση των κυβερνοεγκληματιών που ευθύνονται για την επίθεση αυτή (Europol, 2016, p.17). Ως εκ τούτου, καλείται να πληρώσει ένα χρηματικό ποσό, προκειμένου να καταφέρει να αποκρυπτογραφήσει τα δεδομένα ή να λειτουργήσει και πάλι το σύστημα (Oz et al., 2022). Σήμερα, στις επιχειρήσεις παρατηρείται όχι μόνο η κρυπτογράφηση των δεδομένων μέσω του ransomware, αλλά ταυτόχρονα και η «απορρόφηση» των ευαίσθητων ή ιδιωτικών αρχείων και πληροφοριών, με αποτέλεσμα οι δράστες να αποσπούν χρηματικά ποσά (λύτρα), προκειμένου να μην εκθέσουν την εκάστοτε επιχείρηση σε ότι αφορά τον κανόνα προστασίας προσωπικών δεδομένων (GDPR), με μία ενδεχόμενη διαρροή πληροφοριών (Ransomware New Generation, 2021). Αξίζει δηλαδή να σημειωθεί, ότι πέραν του κακόβουλου αυτού λογισμικού, ο εκβιασμός στον κυβερνοχώρο πραγματώνεται και με άλλες τεχνικές. Μία τεχνική μπορεί να αφορά την απόσπαση χρηματικού ποσού προκειμένου να μη δημοσιοποιηθούν τα κλεμμένα δεδομένα, όπως

προαναφέρθηκε, μπορεί επιπλέον όμως να αφορά την απόσπαση χρηματικού ποσού, κυρίως από επιχειρήσεις των οποίων η καθημερινή λειτουργία εξαρτάται σε μεγάλο βαθμό από τα συστήματα πληροφορικής, προκειμένου να προστατευθούν και να αποτρέψουν καταστροφικές σε βάρος τους επιθέσεις (Paoli et al., 2018).

β) η διαδικτυακή απάτη

Η διαδικτυακή απάτη, είναι η παραδοσιακή απάτη που πραγματοποιείται με τη βοήθεια του υπολογιστή και της τεχνολογίας γενικότερα. Στην ουσία πρόκειται για την εκμετάλλευση μέσω υπολογιστή, με σκοπό το κέρδος ενός οφέλους π.χ. οικονομικό ή την πρόσβαση σε προσωπικά στοιχεία. Η πρόσβαση αυτή, μπορεί να έχει ως σκοπό την παράνομη απόκτηση, των υπηρεσιών που παρέχει η επιχείρηση-θύμα, και πραγματώνεται είτε με την απόκτηση των διαπιστευτηρίων ενός διαχειριστή ή υπαλλήλου της επιχείρησης μέσω τεχνικών (π.χ. phishing, κοινωνική μηχανική, κ.ά.), είτε με την απόκτηση των διαπιστευτηρίων ενός νόμιμου χρήστη (De Marco et al., 2019). Άλλοι τύποι διαδικτυακής απάτης σε βάρος επιχειρήσεων είναι η απάτη σε διαδικτυακές τραπεζικές υπηρεσίες, η απάτη με προκαταβολές η οποία περιλαμβάνει την υπόσχεση στην επιχείρηση ενός μεγάλου χρηματικού ποσού με αντάλλαγμα μια μικρή προκαταβολή την οποία και δίνει η επιχείρηση χωρίς να λάβει κάποιο χρηματικό ποσό αφού ο δράστης συνήθως εξαφανίζεται, και η απάτη σε δημοπρασία η οποία συμβαίνει όταν η επιχείρηση αγοράζει και πληρώνει ηλεκτρονικά ορισμένες υπηρεσίες ή προϊόντα τα οποία είτε είναι χαμηλότερης ποιότητας από την προβλεπόμενη διαφήμιση, είτε δεν παραδίδονται ποτέ (Paoli et al., 2018).

Οι ανωτέρω κατηγοριοποιήσεις είναι δύο από τις πολλές που έχουν επιχειρηθεί έως σήμερα, αφού υπάρχουν και άλλες με διαφορετικά κριτήρια και στόχους, που ενδεχομένως να είναι περισσότερο συγκεντρωτικές και αναλυτικές.

7. Περιγραφική ανάλυση δημοφιλών κυβερνοεπιθέσεων

Στο συγκεκριμένο υποκεφάλαιο επιχειρείται η περιγραφική ανάλυση τεσσάρων πιο δημοφιλών κυβερνοεπιθέσεων που είναι το phishing (ηλεκτρονικό ψάρεμα), το salami slicing (τεμαχισμός σαλαμιού), το ransomware και το cryptojacking. Η ανάλυση αυτή αφορά την προέλευσή τους, τις παραλλαγές στις διάφορες μεθόδους που χρησιμοποίησαν εξαιτίας της ραγδαίας αύξησης της τεχνολογίας και τον τρόπο λειτουργίας τους (modus operandi).

7.1 Επίθεση phishing

Το ηλεκτρονικό ψάρεμα, γνωστό ως phishing, πρωτοεμφανίστηκε στα συστήματα δικτύου της America Online (AOL) [6], στις αρχές της δεκαετίας του 1990. Ορισμένοι hackers κατάφεραν να δημιουργήσουν ψεύτικους λογαριασμούς, χρησιμοποιώντας πλαστές ταυτότητες και πιστωτικές κάρτες. Παρά την ασυμβατότητα με τις πραγματικές κάρτες και τις ταυτότητες των κατόχων, οι λογαριασμοί συνέχιζαν να περνούν από απλές δοκιμασίες εξακρίβωσης που πραγματοποιούνταν από την AOL, εξαιτίας τεχνικών αδυναμιών του συστήματος. Ως επακόλουθο, η AOL πίστευε ότι οι λογαριασμοί ήταν νόμιμοι και για αυτό παρέμεναν ενεργοί μέχρι να χρεωθούν και να διαπιστωθεί η μη εγκυρότητά τους. Η δημιουργία πλαστών λογαριασμών δεν αποτέλεσε από μόνη της μια διαδικασία ηλεκτρονικού ψαρέματος, αλλά έθεσε τις βάσεις για την ανάπτυξη και διαμόρφωση της εν λόγω κυβερνοεπίθεσης (Jakobsson & Myers, 2006, pp.1-29).

Η ραγδαία εξέλιξη της τεχνολογίας οδήγησε στη δημιουργία διαφόρων μεθόδων που στοχεύουν σε μία πιο αποτελεσματική και επιτυχή έκβαση αυτών των επιθέσεων στον κυβερνοχώρο. Επομένως, μερικές από τις μεθόδους του ηλεκτρονικού ψαρέματος που εξελίχθηκαν μέσα στο χρόνο, είναι οι ακόλουθες:

- Spear phishing

Αποτελεί μία από τις πιο δημοφιλείς στρατηγικές που αντιπροσωπεύουν το 91% των επιθέσεων. Συνήθως πραγματοποιείται με τη χρήση των προσωπικών στοιχείων του θύματος προκειμένου να κερδίσει την εμπιστοσύνη του, αυξάνοντας έτσι τις πιθανότητες επιτυχίας (Shashidhar, 2017).

- Whaling

Ο στόχος είναι κυρίως τα ανώτερα και υψηλόβαθμα στελέχη μιας επιχείρησης. Συνήθως, υλικό ηλεκτρονικού ταχυδρομείου δημοσιεύεται είτε με τη μορφή κλήτευσης, είτε ως παράπονο πελατών ή ως ζήτημα που αφορά τη λειτουργία και οργάνωση της επιχείρησης (Vaishnaw & Tandan, 2015).

- Clone phishing

Αποτελεί μια περαιτέρω μορφή παραδοσιακής επίθεσης ηλεκτρονικού ψαρέματος κατά την οποία ένα γνήσιο μήνυμα ηλεκτρονικού ταχυδρομείου κλωνοποιείται, αντικαθιστώντας τα συνημμένα αρχεία που είναι ψευδή ή κατευθύνοντας το χρήστη σε μια εντελώς ψεύτικη φόρμα ή διεύθυνση (Vaishnaw & Tandan, 2015).

[6] Η America Online (AOL), είναι ένας πάροχος διαδικτυακών υπηρεσιών με έδρα τη Νέα Υόρκη.

Οι παραπάνω τύποι ηλεκτρονικού ψαρέματος θεωρούνται παραδοσιακοί, επειδή βασίζονται αποκλειστικά σε μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται μέσω διαδικτύου. Παρομοίως, άλλες μορφές ηλεκτρονικού ψαρέματος περιλαμβάνουν τη χρήση σύντομων μηνυμάτων SMS μέσω κινητών τηλεφώνων ή smartphone (Smishing, ακρώνυμο των λέξεων Short Message Service και Phishing) ή τη χρήση φωνητικών μηνυμάτων (Vishing, ακρώνυμο των λέξεων Voice και Phishing), όπου ο εισβολέας επικοινωνεί με το θύμα προκειμένου να αποκτήσει πρόσβαση σε προσωπικά στοιχεία και πληροφορίες (Yeboah-Boateng & Amanor, 2014).

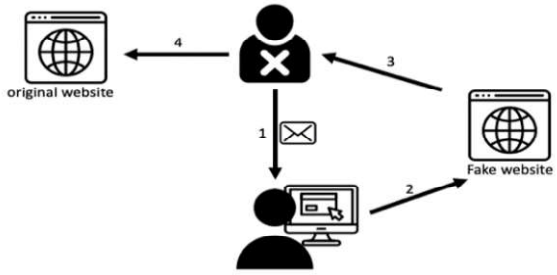
Ως προς τον τρόπο λειτουργίας μιας επίθεσης ηλεκτρονικού ψαρέματος, έχουν παρατηρηθεί τρία βασικά στάδια (Jakobsson & Myers, 2006):

α) το δέλεαρ (lure), όπου ο εισβολέας προσπαθεί να πείσει το θύμα να ακολουθήσει ένα σύνδεσμο για να κατεβάσει ένα κακόβουλο πρόγραμμα ή να εισχωρήσει σε έναν ψεύτικο ιστότοπο,

β) ο γάντζος (hook), όπου το θύμα παγιδεύεται ανοίγοντας για παράδειγμα το σύνδεσμο που έστειλε η τράπεζα εισάγοντας πληροφορίες, και

γ) η παγίδα (catch), όπου επιτυγχάνεται η κλοπή και η πρόσβαση σε προσωπικά στοιχεία.

Συνοψίζοντας, ο εισβολέας στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στο θύμα, το οποίο περιέχει ένα σύνδεσμο προς έναν ψεύτικο ιστότοπο παρόμοιο με τον αρχικό (Βήμα 1). Όταν το θύμα μπαίνει στον ψεύτικο ιστότοπο και εισάγει τις απαιτούμενες πληροφορίες, όπως κωδικό πρόσβασης και όνομα χρήστη, οι πληροφορίες αποστέλλονται στον εισβολέα (Βήμα 2 & Βήμα 3). Στη συνέχεια, ο εισβολέας θα χρησιμοποιήσει τον κωδικό πρόσβασης και το όνομα χρήστη στον αρχικό ιστότοπο (Βήμα 4).



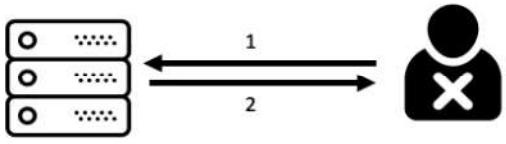
Εικόνα 1
Επίθεση Phishing
Πηγή: Four Most Famous Cyber Attacks for Financial (Altwairqi et al., 2019)

7.2 Επίθεση Salami Slicing

Στη συγκεκριμένη επίθεση, ο εισβολέας χρησιμοποιεί μαθηματικές μεθόδους και συλλογισμούς προκειμένου να επιτύχει τους στόχους του. Οι υπολογισμοί γίνονται βάσει δεκαδικών ψηφίων, συνήθως 2 ή 3 θέσεων. Πιο συγκεκριμένα, ο εισβολέας στρογγυλοποιεί τις τιμές, και τα δεκαδικά ψηφία τα μεταφέρει στο λογαριασμό του χωρίς να ενημερώνει το χρηματοπιστωτικό ίδρυμα (Kabay, 2002).

Οι επιθέσεις salami slicing διακρίνονται σε δύο τύπους, στις εσωτερικές και εξωτερικές επιθέσεις (Allhassan et al., 2018). Οι εσωτερικές επιθέσεις αποτελούν και τον πιο συχνό τύπο επίθεσης salami slicing. Κατά τη διάρκεια αυτών των επιθέσεων, ο εισβολέας εμφανίζεται να είναι πολύ εξοικειωμένος με το σύστημα ασφαλείας της επιχείρησης. Για παράδειγμα, ένας τραπεζικός υπάλληλος εισάγει κακόβουλο λογισμικό στο διακομιστή της τράπεζας με σκοπό να αποκομίσει χρήματα στο λογαριασμό του, μέσω των συναλλαγών που κάνουν οι πελάτες της συγκεκριμένης τράπεζας. Αντιθέτως, οι εξωτερικές επιθέσεις συμβαίνουν εκτός της επιχείρησης. Στην προκειμένη περίπτωση, ο εισβολέας εγκαταλείπει την επιχείρηση έχοντας γνώση του συστήματος ασφαλείας και επιχειρεί να αποκτήσει παράνομη πρόσβαση σε πληροφορίες και δεδομένα της, προκειμένου να προκαλέσει σοβαρή ζημία σε αυτή.

Στην τεχνική του salami slicing, οι επιτιθέμενοι κλέβουν πόρους ή χρήματα λίγο-λίγο κάθε φορά, έτσι ώστε να μη γίνονται αντιληπτοί. Όπως προαναφέραμε για παράδειγμα, ένας τραπεζικός υπάλληλος εγκαθιστά ένα λογισμικό στους διακομιστές της τράπεζας, μέσω του οποίου αποσύρει κάθε φορά ένα μικρό χρηματικό ποσό από το λογαριασμό κάθε πελάτη. Κάθε κάτοχος λογαριασμού δε δύναται να παρατηρήσει αυτή τη μικρή απώλεια στο λογαριασμό του, παρόλο που κάθε μήνα ο εισβολέας θα κερδίζει ένα σημαντικό χρηματικό ποσό. Η εγκατάσταση δηλαδή του κακόβουλου λογισμικού στο διακομιστή της τράπεζας, αποσκοπεί στην αφαίρεση μικρών σε αξία χρηματικών ποσών, τα οποία αποστέλλονται στον εισβολέα χωρίς να ενημερώνει την τράπεζα.



Εικόνα 2
Επίθεση Salami Slicing
Πηγή: Four Most Famous Cyber Attacks for Financial (Altwairqi et al., 2019)

7.3 Επίθεση Ransomware

Ο πρώτος ιός ransomware δημιουργήθηκε το 1989 από τον Joseph L. Poppt, ο οποίος και διένειμε τον ιό μέσω δισκέτας, στο Διεθνές Συνέδριο του Παγκόσμιου Οργανισμού Υγείας για το AIDS. Το κακόβουλο λογισμικό μέτρησε τον αριθμό επανεκκινήσεων του υπολογιστή και μόλις ο υπολογιστής έφτασε τις 90 φορές επανεκκίνησης, ξεκίνησε η κρυπτογράφηση ή το κλείδωμα των αρχείων (Faragallah et al., 2018 ; Sodhi et al., 2018). Για την αποκατάσταση της πρόσβασης, οι χρήστες έπρεπε να στείλουν 189 δολάρια στον υπολογιστή της Cyborg Corporation [7].

Υπάρχουν δύο κύριοι τύποι ransomware, το crypto ransomware το οποίο είναι το πιο δημοφιλές και κρυπτογραφεί τα δεδομένα και τα αρχεία του υπολογιστή, και το locker ransomware το οποίο κλειδώνει τον υπολογιστή, το λογισμικό ή άλλα εξαρτήματα του υπολογιστή, όπως το ποντίκι και το πληκτρολόγιο. Πιο συγκεκριμένα:

- Crypto Ransomware

Πρόκειται για ένα κακόβουλο λογισμικό αρχείου και δεδομένων που εκτελεί σιωπηλή αναζήτηση έπειτα από την εισαγωγή του στο σύστημα του χρήστη. Ωστόσο, τα συστήματα που έχουν μολυνθεί συνεχίζουν να λειτουργούν κανονικά, επειδή τα σημαντικά αρχεία του λειτουργικού συστήματος και των εφαρμογών δεν έχουν επηρεαστεί. Στη συνέχεια, το κακόβουλο λογισμικό κρυπτογραφεί δεδομένα και αρχεία του θύματος, καθιστώντας τα άχρηστα και ζητώντας από το θύμα ένα χρηματικό ποσό (λύτρα) προκειμένου να του δώσει το κλειδί αποκρυπτογράφησης (Bhardwaj et al., 2016).

- Locker Ransomware

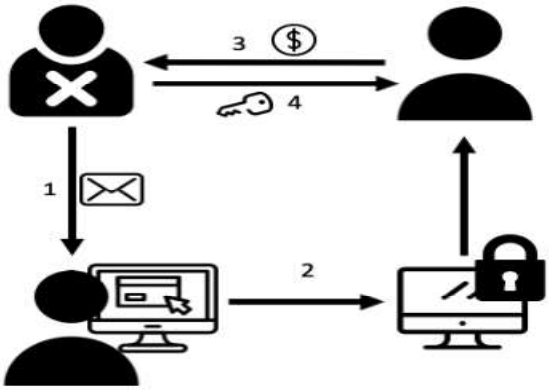
Επηρεάζει συνήθως τα εξαρτήματα και τον εξοπλισμό των ηλεκτρονικών υπολογιστών, όπως το ποντίκι, το πληκτρολόγιο, κλειδώνοντάς τα ή απαγορεύοντας την πρόσβαση στους χρήστες τους. Το ransomware εμφανίζεται δηλαδή στην οθόνη του υπολογιστή παρέχοντας περιορισμένη πρόσβαση σε ορισμένες απαιτούμενες λειτουργίες, όπως στην κίνηση του ποντικιού, που επιτρέπουν στο θύμα να εισέλθει. Έπειτα το θύμα, αναγκάζεται να πληρώσει τα απαιτούμενα λύτρα προκειμένου να του παραχωρηθεί η πλήρη πρόσβαση στον υπολογιστή του (Bhardwaj et al., 2016).

Ο τρόπος λειτουργίας της επίθεσης ransomware είναι παρόμοιος με τον τρόπο που λειτουργεί η επίθεση phishing. Ο εισβολέας αρχικά πείθει το θύμα να

[7] Εταιρεία λογισμικού στη Ν. Υόρκη.

ακολουθήσει ένα σύνδεσμο ή να κατεβάσει ένα πρόγραμμα. Μόλις το θύμα πέσει στην παγίδα, ο εισβολέας κλειδώνει τον υπολογιστή ή εμποδίζει την πρόσβαση στα δεδομένα. Έπειτα, ο εισβολέας ζητά ένα χρηματικό ποσό (λύτρα), προκειμένου να απενεργοποιήσει το κακόβουλο πρόγραμμα (Richardson & North, 2017).

Αναλυτικότερα, ο εισβολέας στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που περιέχει κακόβουλα αρχεία, και αυτά με τη σειρά τους είτε κλειδώνουν ορισμένες υπηρεσίες του υπολογιστή ή ολόκληρο τον υπολογιστή, είτε κρυπτογραφούν δεδομένα (Βήμα 1 & Βήμα 2). Ακολούθως, το θύμα θα πρέπει να πληρώσει λύτρα στον εισβολέα, έτσι ώστε να λάβει σε αντάλλαγμα το κλειδί για την αποκρυπτογράφηση ή την επαναφορά των υπηρεσιών του υπολογιστή (Βήμα 3 & Βήμα 4) (Sodhi et al., 2018).



Εικόνα 3
Επίθεση Ransomware
Πηγή: Four Most Famous Cyber Attacks for Financial (Altwairqi et al., 2019)

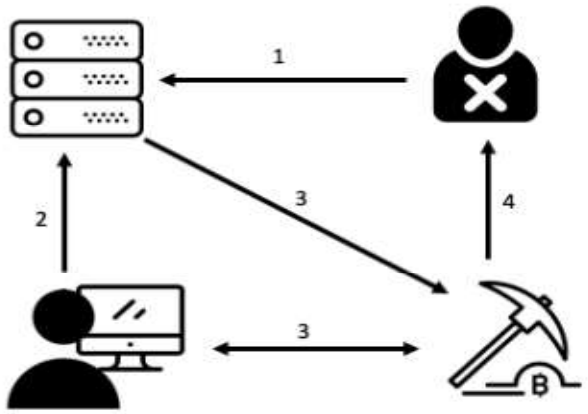
7.4 Επίθεση Cryptojacking

Η επίθεση cryptojacking διενεργήθηκε για πρώτη φορά το 2017, όταν ο ιστότοπος Coinhive δημοσίευσε έναν κωδικό που επέτρεπε στους κρυπτογράφους να εξάγουν κρυπτονομίσματα. Ακολουθώντας την ίδια λογική του συγκεκριμένου ιστότοπου, εμφανίστηκε στο διαδίκτυο ένας μεγάλος αριθμός πλαστών ιστοσελίδων που επέτρεπαν στους κρυπτογράφους να εκμεταλλεύονται παράνομα τους προσωπικούς υπολογιστές, τον εξοπλισμό και τους διακομιστές διαφόρων χρηστών (Sigler, 2018).

Υπάρχουν δύο τρόποι για την έναρξη μιας επίθεσης cryptojacking, τα σενάρια κακόβουλου λογισμικού (malware scripts) και ο κώδικας JavaScript στο πρόγραμμα

περιήγησης (Sigler, 2018). Τα σενάρια κακόβουλου λογισμικού αναφέρονται στην εγκατάσταση ενός κακόβουλου λογισμικού στον υπολογιστή του χρήστη, όπου με τη βοήθεια του κωδικού που παρέχεται μέσω της εν λόγω εγκατάστασης, ξεκινάει η διαδικασία εξόρυξης κρυπτονομισμάτων. Σε αντίθεση με τα παραδοσιακά κακόβουλα λογισμικά, αυτός ο τύπος των επιθέσεων δεν προκαλεί βλάβες στον υπολογιστή. Από την άλλη πλευρά, στην επίθεση cryptojacking που εισάγει έναν κακόβουλο κώδικα JavaScript σε μια ιστοσελίδα, ο hacker επιτίθεται μαζικά σε διάφορες συσκευές. Οποιαδήποτε συσκευή μπορεί να υποστεί κρυπτογράφηση, όταν το θύμα περιηγηθεί σε μια σελίδα στην οποία έχει εισαχθεί ένας κακόβουλος κωδικός JavaScript. Παρόλα αυτά, δεν είναι όλες οι προσεγγίσεις εξόρυξης κρυπτονομισμάτων κακόβουλες.

Γενικότερα, στην επίθεση cryptojacking, και ο εισβολέας και το θύμα είναι συνδεδεμένοι στο διακομιστή, και ακολούθως ο εισβολέας χρησιμοποιεί μία από τις προηγούμενες τεχνικές για τον έλεγχο της συσκευής του χρήστη (Βήμα 1 & Βήμα 2). Η διαδικασία αυτή επιτρέπει στον εισβολέα να εξερευνήσει το σύστημα και να στείλει νομίσματα στον εαυτό του (Βήμα 3 & Βήμα 4).



Εικόνα 4
Επίθεση Cryptojacking
Πηγή: Four Most Famous Cyber Attacks for Financial (Altwairqi et al., 2019)

8. Γενικά στατιστικά δεδομένα

Στη βιβλιογραφία υπάρχει ένας περιορισμένος αριθμός στατιστικών δεδομένων, που είναι διαθέσιμος, αναφορικά με τα διάφορα είδη των κυβερνοεπιθέσεων και των επιχειρήσεων που αυτές προσβάλλουν. Γενικότερα, οι επιχειρήσεις τείνουν να αποκρύπτουν τον αριθμό και τον αντίκτυπο των επιθέσεων,

προκειμένου να διαφυλάξουν το κύρος τους και να διατηρήσουν την εμπιστοσύνη του πελάτη. Ωστόσο υπάρχουν ορισμένα δεδομένα τα οποία εκτίθενται ακολούθως.

Με βάση τις εκθέσεις ορισμένων ερευνητών, η επίθεση phishing βρέθηκε να κατέχει την πρώτη θέση, ως την πιο διαδεδομένη επίθεση στον κυβερνοχώρο γενικά, ακολουθώντας με τη σειρά τους οι επιθέσεις ransomware και cryptojacking (O'Gorman, 2019 ; Pournouri et al., 2019). Αναλυτικότερα, ο αριθμός των επιθέσεων phishing κατά το έτος 2019 έφτασε τα 240 εκατομμύρια, ενώ οι επιθέσεις ransomware και cryptojacking δεν ξεπέρασαν τα 14 εκατομμύρια, με τον αριθμό των επιθέσεων ransomware να υπερτερεί του αριθμού των επιθέσεων cryptojacking. Επίσης, κατά το ίδιο έτος, βρέθηκε ότι ένα ποσοστό της τάξεως του 84% των επιθέσεων στον κυβερνοχώρο, αντανακλούσε κίνητρα κυρίως εγκληματικού χαρακτήρα και οι στόχοι των επιθέσεων ήταν περισσότερο οι μεμονωμένοι χρήστες του διαδικτύου, παρά οι επιχειρήσεις (Pournouri et al., 2019).

Συνεχίζοντας στο ίδιο μήκος κύματος, τα ερευνητικά δεδομένα που αφορούν την έκθεση μιας παλαιότερης μελέτης σχετικά με το είδος των κυβερνοεπιθέσεων στις επιχειρήσεις, ανέδειξαν τις επιθέσεις phishing και την ανεπιθύμητη αλληλογραφία (spam) ως τις σημαντικότερες και συχνότερες απειλές των επιχειρήσεων στον κυβερνοχώρο (B2B International, 2014, όπως αναφέρθηκε στους Iovan & Iovan, 2016). Συγκεκριμένα, το 68% των ερωτηθέντων δήλωσε ότι οι επιχειρήσεις τους αποτέλεσαν στόχοι επιθέσεων μέσω της χρήσης ιών, σκουληκιών και κακόβουλων λογισμικών κατά τη χρονική περίοδο 2013-2014, ενώ ο όγκος των επιθέσεων ανεπιθύμητης αλληλογραφίας κατά την ίδια χρονική περίοδο αυξήθηκε σημαντικά, επηρεάζοντας το 61% των επιχειρήσεων συγκριτικά με το ποσοστό της τάξεως του 41%, που είχε σημειωθεί κατά το έτος 2012.

Αναφορικά με τη γεωγραφική θέση των επιχειρήσεων που αποτέλεσαν στόχο των κυβερνοεπιθέσεων, οι επιχειρήσεις στη Νότια Αμερική δέχθηκαν τις περισσότερες επιθέσεις, με το 72% των ερωτηθέντων να αναφέρει τους ιούς και τα λογισμικά υποκλοπής spyware, ως τις σοβαρότερες εξωτερικές απειλές. Οι ρώσικες επιχειρήσεις δέχθηκαν και αυτές ένα μεγάλο αριθμό επιθέσεων, με ένα ποσοστό της τάξεως του 72% να αντιπροσωπεύει τα εν λόγω περιστατικά. Στην Ιαπωνία, ένα ποσοστό της τάξεως του 47% των επιχειρήσεων, αποτέλεσε στόχο κακόβουλων επιθέσεων. Επιπλέον, ο υψηλότερος αριθμός περιστατικών ανεπιθύμητης αλληλογραφίας καταγράφηκε σε επιχειρήσεις στη Βόρεια Αμερική και στη Ρωσία, με ποσοστά της τάξεως των 69% και 67%, αντίστοιχα, ενώ ο χαμηλότερος αριθμός

σημειώθηκε στη Μέση Ανατολή και στην Ιαπωνία, με ποσοστά της τάξεως των 55% και 42%, αντίστοιχα. Τέλος, οι επιχειρήσεις στη Βόρεια Αμερική αντιμετώπισαν επιθέσεις phishing σε μεγαλύτερη κλίμακα (51%), συγκριτικά με άλλες επιχειρήσεις που βρισκόντουσαν στην Ασία (46%), στη Ρωσία, στην Ιαπωνία και σε χώρες της Νότιας Αμερικής, οι οποίες σημείωσαν κατά μέσο όρο ένα ποσοστό της τάξεως του 26% (B2B International, 2014, όπως αναφέρθηκε στους Iovan & Iovan, 2016).

ΜΕΡΟΣ Γ΄

Οργάνωση ομάδων & περιπτώσεις μελέτης κυβερνοεπιθέσεων

1. Οργάνωση ομάδων και κυβερνοεπιθέσεις

Προτού προχωρήσουμε με την παράθεση ορισμένων περιπτώσεων που αφορούν τις κυβερνοεπιθέσεις σε διάφορες επιχειρήσεις και οργανισμούς, θεωρούμε σημαντικό να αναφερθούμε συνοπτικά στην κατηγοριοποίηση των ομάδων που σχεδιάζουν, οργανώνουν και εκτελούν τις επιθέσεις αυτές στον κυβερνοχώρο.

Από τη βιβλιογραφική ανασκόπηση του McGuire (2012), διαπιστώθηκε ότι μέχρι και ένα ποσοστό της τάξεως του 80% του εγκλήματος στον κυβερνοχώρο, θα μπορούσε να είναι αποτέλεσμα κάποιας μορφής οργανωμένης δραστηριότητας. Το γεγονός αυτό δε σημαίνει, ωστόσο, ότι αυτές οι ομάδες παίρνουν τη μορφή παραδοσιακών, ιεραρχικά οργανωμένων, εγκληματικών ομάδων ή ότι αυτές οι ομάδες διαπράττουν αποκλειστικά και μόνο ψηφιακά εγκλήματα. Αντιθέτως, είναι πιθανόν η συγκεκριμένη μελέτη να υποδηλώνει ότι οι παραδοσιακές ομάδες οργανωμένου εγκλήματος επεκτείνουν τις δραστηριότητές τους στον ψηφιακό κόσμο, σε συνδυασμό με νεότερους και πιο ελαστικούς τύπους ψηφιακής εγκληματικότητας. Επιπλέον, ο McGuire (2012) τόνισε ότι στο δείγμα που μελέτησε, οι μισές ομάδες που διέπρατταν ψηφιακά εγκλήματα αποτελούνταν από 6 ή και περισσότερα άτομα, με το ένα τέταρτο των ομάδων που εξετάστηκαν να περιλαμβάνουν στο ενεργητικό τους περισσότερα από 10 άτομα και με εξίσου το ένα τέταρτο αυτών των ομάδων να αναφέρουν τους 6 μήνες ως χρονική διάρκεια δράσης τους.

Ο McGuire (2012) πρότεινε μια τυπολογία ομάδων ψηφιακού εγκλήματος, η οποία περιλαμβάνει τρείς κύριους τύπους ομάδων, με τον κάθε τύπο να χωρίζεται σε δύο υποομάδες, αντανακλώντας κατ' αυτό τον τρόπο τη δύναμη της σχέσης που αναπτύσσεται μεταξύ των μελών και υπογραμμίζει ταυτόχρονα τη δυνατότητα τροποποίησης της τυπολογίας, καθώς εξελίσσεται το ψηφιακό περιβάλλον.

Οι ομάδες τύπου Ι λειτουργούν ουσιαστικά διαδικτυακά και μπορούν να διακριθούν περαιτέρω σε σμήνη (swarms) και σε κόμβους (hubs). Είναι κυρίως «εικονικές» και η αξιοπιστία τους αξιολογείται μέσω της φήμης που αποκτούν από διαδικτυακές παράνομες δραστηριότητες. Πιο συγκεκριμένα, τα σμήνη περιγράφονται ως «αποδιοργανωμένες» ομάδες χωρίς ηγεσία, αλλά με κοινό σκοπό.

Συνήθως λειτουργούν σε ιογενείς μορφές και φαίνεται να είναι πιο ενεργά σε ιδεολογικά καθοδηγούμενες διαδικτυακές δραστηριότητες, όπως στα εγκλήματα μίσους και πολιτικής αντίστασης. Οι κόμβοι από την άλλη πλευρά είναι πιο οργανωμένες ομάδες, με σαφή εικόνα και δομή του σκοπού και των εντολών τους. Εμπεριέχουν ένα εστιακό σημείο (κόμβο), γύρω από το οποίο συγκεντρώνονται περιφερειακοί συνεργάτες. Οι διαδικτυακές τους δραστηριότητες περιλαμβάνουν ένα ευρύ φάσμα ενεργειών, όπως πειρατεία, επιθέσεις phishing, κ.λπ. (McGuire, 2012).

Παρομοίως, οι ομάδες τύπου ΙΙ περιγράφονται ως «υβρίδια» (hybrids), γιατί συνδυάζουν διαδικτυακές και εκτός δικτύου εγκληματικές δραστηριότητες. Διακρίνονται σε ομαδοποιημένα υβρίδια (clustered hybrids) και σε εκτεταμένα υβρίδια (extended hybrids). Σε ένα ομαδοποιημένο υβρίδιο, η εγκληματική δραστηριότητα πραγματώνεται από μία μικρή ομάδα ατόμων και επικεντρώνεται σε συγκεκριμένες ενέργειες ή μεθόδους. Η δομή τους είναι παρεμφερή με τη δομή των κόμβων, αλλά εναλλάσσονται απρόσκοπτα μεταξύ online και offline εγκληματικές δραστηριότητες. Μια κλασική δραστηριότητα των ομαδοποιημένων υβριδίων, αποτελεί η παράνομη πρόσβαση σε πιστωτικές κάρτες όπου θα χρησιμοποιήσουν τα δεδομένα για online αγορές ή θα πωλήσουν τα δεδομένα σε δίκτυα που ασχολούνται με παράνομες δραστηριότητες. Από την άλλη πλευρά, τα εκτεταμένα υβρίδια, ενώ παρουσιάζουν παρόμοιους τρόπους λειτουργίας με τα ομαδοποιημένα υβρίδια, είναι λιγότερο συγκεντρωτικά. Συνήθως, απαρτίζονται από πολλούς συνεργάτες, χωρίζονται σε αρκετές υποομάδες, εκτελούν μια ευρεία γκάμα εγκληματικών δραστηριοτήτων, και παράλληλα διατηρούν ένα επαρκή επίπεδο συντονισμού, το οποίο συμβάλλει σημαντικά στην επιτυχημένη ολοκλήρωση των δραστηριοτήτων τους (McGuire, 2012).

Οι ομάδες τύπου ΙΙΙ λειτουργούν κυρίως εκτός σύνδεσης, συμβάλλουν σημαντικά στην προώθηση του ψηφιακού εγκλήματος και διακρίνονται σε ιεραρχίες (hierarchies) και συγκεντρώσεις (aggregate), ανάλογα με το βαθμό συνοχής και οργάνωσής τους. Οι ιεραρχίες περιγράφονται ως παραδοσιακές εγκληματικές ομάδες (οικογένειες) που μεταφέρουν ορισμένες από τις δραστηριότητές τους στο διαδίκτυο. Παραδείγματα περιλαμβάνουν την επέκταση ορισμένων ομάδων της μαφίας που ασχολούνται με την πορνεία σε ιστότοπους πορνογραφίας, το διαδικτυακό τζόγο, τον εκβιασμό για τερματισμό της λειτουργίας των συστημάτων, την πρόσβαση σε ιδιωτικά αρχεία μέσω επιθέσεων κακόβουλου λογισμικού ή πειρατείας (Broadhurst et al.,2014). Αντιθέτως, οι συγκεντρωτικές ομάδες δεν διαρκούν για μεγάλο χρονικό

διάστημα, είναι πιο ελαστικές στην οργάνωσή τους και συχνά δεν έχουν κάποιο σαφή σκοπό. Χρησιμοποιούν τις ψηφιακές τεχνολογίες με ad hoc τρόπο, γεγονός που μπορεί να προκαλέσει ζημίες σε αρκετά μεγάλο βαθμό. Παραδείγματα αποτελούν η χρήση κινητών τηλεφώνων ή ασύρματου εξοπλισμού τύπου Blackberry, μέσω των οποίων συντόνιζαν τις δραστηριότητες συμμοριών, όπως συνέβη κατά τη διάρκεια των κοινωνικών διαταραχών που διαδραματίστηκαν στο Ηνωμένο Βασίλειο το 2011 ή κατά τη διάρκεια των κοινωνικών διαταραχών που έλαβαν χώρα στο Σύδνεϋ το Σεπτέμβριο του 2012 (Cubby & McNeilage, 2012).

Τέλος, οι πιο εξελιγμένες εγκληματικές οργανώσεις στον κυβερνοχώρο χαρακτηρίζονται από σημαντικές εξειδικεύσεις, οι οποίες αντανακλούν συγκεκριμένους ρόλους που υιοθετούν οι δράστες. Τέτοιοι ρόλοι είναι οι ακόλουθοι (Chabinsky, 2010):

- Οι *κωδικοποιητές* ή οι *προγραμματιστές* (coders), οι οποίοι σχεδιάζουν και διαμορφώνουν το κακόβουλο λογισμικό και τα κατάλληλα εργαλεία που θα χρησιμοποιηθούν για τη διάπραξη της εκάστοτε εγκληματικής δραστηριότητας.
- Οι *διανομείς* ή οι *πωλητές* (distributors), οι οποίοι εμπορεύονται και πωλούν κλεμμένα δεδομένα και εγγυώνται για τα αγαθά που παρέχονται από τις άλλες ειδικότητες.
- Οι *τεχνικοί* (technicians), οι οποίοι συντηρούν την εγκληματική υποδομή και τις τεχνολογίες υποστήριξης, όπως τους διακομιστές, τα κρυπτογραφικά συστήματα, κ.ά..
- Οι *hacker*, οι οποίοι αναζητούν και εκμεταλλεύονται τρωτά σημεία σε εφαρμογές, συστήματα και δίκτυα, για να αποκτήσουν παράνομη πρόσβαση.
- Οι *ειδικοί σε θέματα απάτης* (fraud specialists), οι οποίοι αναπτύσσουν και χρησιμοποιούν προγράμματα κοινωνικής μηχανικής, συμπεριλαμβανομένων του ηλεκτρονικού ψαρέματος (phishing) και της ανεπιθύμητης αλληλογραφίας (spam).
- Οι *οικοδεσπότες* (hosts), οι οποίοι παρέχουν «ασφαλείς» εγκαταστάσεις διακομιστών και τοποθεσιών παράνομου περιεχομένου, συχνά μέσω περίτεχνων δικτύων botnet και proxy.
- Οι *ταμίες* (cashers), οι οποίοι ελέγχουν την απόρριψη λογαριασμών και παρέχουν τα συγκεκριμένα ονόματα και τους λογαριασμούς σε άλλους εγκληματίες έναντι αμοιβής. Επίσης, διαχειρίζονται μεμονωμένους μεταφορείς μετρητών.
- Οι *money mules*, οι οποίοι μεταφέρουν τα έσοδα από απάτες που έχουν διαπράξει σε ένα τρίτο πρόσωπο, για να βρίσκονται σε ασφαλή τοποθεσία.

- Οι *ταμίες* (tellers), οι οποίοι βοηθούν στη μεταφορά και τη νομιμοποίηση παράνομων εσόδων μέσω υπηρεσιών ψηφιακού νομίσματος και μεταξύ διαφορετικών εθνικών νομισμάτων.
- Τα *στελέχη* του οργανισμού (executives), τα οποία επιλέγουν τους στόχους, διαχειρίζονται τη διαμονή των εγκληματικών προϊόντων, προσλαμβάνουν και αναθέτουν στα μέλη τα παραπάνω καθήκοντα.

2. Παραδείγματα κυβερνοεπιθέσεων σε επιχειρήσεις

Παρακάτω παρατίθεται μια σειρά από παραδείγματα κυβερνοεπιθέσεων σε επιχειρήσεις ανά τον κόσμο, που διενεργήθηκαν είτε από μεμονωμένους παραβάτες, είτε από ομάδες εγκληματικών οργανώσεων.

- **Υπόθεση Sam Yin - Gucci Hacker**

Ο Sam Yin, ηλικίας 34 ετών, ήταν ένας πρώην υπάλληλος της εταιρείας Gucci που απολύθηκε αφού κατηγορήθηκε ότι πούλησε κλεμμένα παπούτσια και τσάντες της επωνυμίας «Gucci», στην ασιατική αγορά. Ο Yin, μετά την απόλυσή του, κατάφερε να εισβάλει στο πληροφοριακό σύστημα της εταιρείας, χρησιμοποιώντας ένα μυστικό λογαριασμό που είχε δημιουργήσει κατά τη διάρκεια που εργαζόταν σε αυτή, σε συνδυασμό με ένα ψεύτικο όνομα υπαλλήλου. Με τον τρόπο αυτό, έκλεισε τους υπολογιστές ολόκληρης της επιχείρησης, μπλοκάροντας την πρόσβαση σε αρχεία και σε μηνύματα ηλεκτρονικής αλληλογραφίας για σχεδόν μία ολόκληρη εργάσιμη ημέρα. Επιπλέον, προχώρησε στη διαγραφή διακομιστών, στην εξαφάνιση ηλεκτρονικών γραμματοκιβωτίων και στην απενεργοποίηση των ρυθμίσεων αποθήκευσης. Η εταιρεία «Gucci» υπολόγισε το κόστος της επίθεσης περίπου στα 200.000 δολάρια. Ο Yin καταδικάστηκε σε ποινή φυλάκισης που κυμαινόταν από 2 έως 6 έτη (Italiano, 2012) και το κίνητρο για τη συγκεκριμένη επίθεση φαίνεται να ήταν η εκδίκηση ενός δυσαρεστημένου πρώην υπαλλήλου.

- **Υπόθεση Andrew Auernheimer - Apple iPad Snoop**

Τον Ιούνιο του 2010, ο Andrew Auernheimer, ηλικίας 25 ετών, κατάφερε να αποκτήσει πρόσβαση στις διευθύνσεις ηλεκτρονικού ταχυδρομείου 114.000 χρηστών iPad, συμπεριλαμβανομένων διασημοτήτων και πολιτικών, παραβιάζοντας έτσι τον ιστότοπο της εταιρείας τηλεπικοινωνιών AT&T. Ο Auernheimer ήταν μέλος της ομάδας Goatse Security, η οποία ειδικευόταν στην ανίχνευση και στην αποκάλυψη

ελαττωμάτων ασφαλείας. Η επίθεση έγινε όταν ο Auernheimer μαζί με άλλους hackers, αντιλήφθηκαν ότι θα μπορούσαν να ξεγελάσουν τον ιστότοπο της AT&T, εάν έστελναν αίτημα HTTP που θα περιελάμβανε το σειριακό αριθμό της κάρτας SIM για την αντίστοιχη συσκευή. Με το να μαντεύουν σειριακούς αριθμούς, οι παραβάτες κατάφεραν να αποκτήσουν πρόσβαση σε έναν μεγάλο αριθμό ηλεκτρονικών διευθύνσεων. Ο Auernheimer καταδικάστηκε σε ποινή φυλάκισης 3,5 ετών για την εκμετάλλευση ενός ελαττώματος ασφαλείας της εταιρείας τηλεπικοινωνιών AT&T (Thomas, 2013). Το κίνητρο για την εν λόγω επίθεση φαίνεται να ήταν η επιθυμία του δράστη να επιδείξει τεχνική επάρκεια.

- **Υπόθεση Target**

Το Δεκέμβριο του 2013, η επιχείρηση Target [8] ανακοίνωσε παραβίαση της ασφάλειάς της στον κυβερνοχώρο. Τα δεδομένα 40 εκατομμυρίων πιστωτικών καρτών είχαν κλαπεί, και πάνω από 70 εκατομμύρια προσωπικοί λογαριασμοί επηρεάστηκαν. Τα ονόματα των πιστωτικών και χρεωστικών καρτών των πελατών της Target, οι ημερομηνίες λήξης και οι κωδικοί επαλήθευσης CVV των καρτών, πωλήθηκαν στη μαύρη αγορά έναντι του ποσού των 53,7 εκατομμυρίων δολαρίων (Tobias, 2014). Το κακόβουλο λογισμικό άρχισε να συλλέγει δεδομένα μόλις μόλυνε τα τερματικά POS των λιανοπωλητών, χωρίς να γίνει αντιληπτή η δράση του για ένα διάστημα 6 ημερών. Η επίθεση αυτή κόστισε στην επιχείρηση Target το ποσό των 148 εκατομμυρίων δολαρίων, που μεταξύ άλλων περιελάμβανε πληρωμές για ένα έτος δωρεάν παρακολούθησης πιστώσεων και προστασίας κλοπής δεδομένων. Επίσης, η εταιρεία ξόδεψε 61 εκατομμύρια δολάρια προκειμένου να αναβαθμίσει την τεχνολογία των συστημάτων ασφαλείας της, ενώ τα κέρδη της μειώθηκαν κατά 46% το τέταρτο τρίμηνο του 2013 (Tobias, 2014).

- **Υπόθεση Universal Continental Holdings, Inc**

Η Universal Continental Holdings, Inc [9] στην οποία ανήκει η United Airlines, η δεύτερη μεγαλύτερη αεροπορική εταιρεία στον κόσμο, ανακοίνωσε ότι έπεσε θύμα κυβερνοεπίθεσης τον Ιούλιο του 2014. Πληροφορίες επιβατικών πτήσεων, προορισμών και δεδομένα κοινωνικής ασφάλισης εκλάπησαν από το Γραφείο Διαχείρισης Προσωπικών Δεδομένων. Τα εν λόγω δεδομένα θα μπορούσαν να

[8] Εταιρεία online αγορών.
[9] Εταιρεία συμβουλευτικών υπηρεσιών ανθρώπινου δυναμικού.

διασταυρωθούν με κλεμμένα ιατρικά και οικονομικά αρχεία, αντίστοιχα. Αναφέρθηκαν 21,5 εκατομμύρια χακαρισμένοι λογαριασμοί, ενώ το 80% των θυμάτων προερχόταν από τις ΗΠΑ. Σε αντίθεση με τα αρχεία υγειονομικής περίθαλψης ή τα οικονομικά δεδομένα, η παραβίαση δεδομένων στις αεροπορικές εταιρείες εγείρουν ανησυχίες, αφού οι μετακινήσεις εκατομμυρίων επιβατών μπορούν να μετατραπούν σε αντικείμενα δημόσιας έκθεσης (Riley & Robertson, 2015). Η United Airlines προχώρησε στην αποκατάσταση των μιλίων των πελατών, ως μια ένδειξη συγνώμης για την κυβερνοεπίθεση που υπέστη (Riley & Robertson, 2015).

- **<u>Υπόθεση Home Depot</u>**

Η Home Depot, η μεγαλύτερη εταιρεία λιανικής πώλησης οικιακών ειδών στον κόσμο, ανακοίνωσε παραβίαση των συστημάτων ασφαλείας της από κακόβουλο λογισμικό, το Σεπτέμβριο του 2014. Το κακόβουλο λογισμικό είχε εισαχθεί στα συστήματα υπολογιστών της εταιρείας από τον Απρίλιο του 2014, όπου και παρέμεινε για ένα χρονικό διάστημα 5 περίπου μηνών (Smith, 2014). Η εταιρεία δήλωσε ότι οι δράστες χρησιμοποιούσαν το όνομα χρήστη και τον κωδικό πρόσβασης ενός πωλητή προκειμένου να εισέλθουν στην περίμετρο του δικτύου. Η εταιρεία δεν κατάφερε να εντοπίσει τους hacker, αφού χρησιμοποίησαν ένα εξατομικευμένο κακόβουλο λογισμικό το οποίο δεν είχε χρησιμοποιηθεί άλλη φορά και το οποίο δεν εντοπίστηκε από τα παραδοσιακά λογισμικά προστασίας από ιούς. Περίπου 56 εκατομμύρια λογαριασμών πιστωτικών και χρεωστικών καρτών σε συνδυασμό με ένα μεγάλο αριθμό διευθύνσεων ηλεκτρονικού ταχυδρομείου, παραβιάστηκαν. Η συγκεκριμένη κυβερνοεπίθεση κόστισε στην εταιρεία Home Depot 90 εκατομμύρια δολάρια συνολικά (Smith, 2014).

- **<u>Υπόθεση Staples</u>**

Το Staples, ένα δημοφιλές κατάστημα ειδών γραφείου στις ΗΠΑ, ανακοίνωσε ότι έπεσε θύμα επίθεσης στον κυβερνοχώρο, τον Οκτώβριο του 2014. Το κατάστημα υπέστη επίθεση κακόβουλου λογισμικού, όπου τα προσωπικά δεδομένα των πελατών όπως ονόματα κατόχων κάρτας, λογαριασμοί πιστωτικών και χρεωστικών καρτών των πελατών, ημερομηνίες λήξης και κωδικοί επαλήθευσης των καρτών, παραβιάστηκαν (Smith et al., 2018). Οι εκτιμήσεις αναφέρουν ότι 115 από τα 1400 καταστήματα λιανικής σε όλη την Αμερική, επηρεάστηκαν. Μία ομάδα ειδικών στην κατασκευή κακόβουλων λογισμικών ονόματι «Anunak», γνωστή και για τις επιθέσεις

στη ρωσική χρηματοοικονομική βιομηχανία, θεωρήθηκε υπεύθυνη για την επίθεση. Η Staples ενημέρωσε τους πελάτες της ότι θα προσέφερε δωρεάν υπηρεσίες προστασίας, ασφάλισης και κλοπής των προσωπικών τους δεδομένων (Smith et al., 2018).

- **Υπόθεση Sony**

Η Sony, μια πολυεθνική εταιρεία που ειδικεύεται στη ψυχαγωγία, στα τυχερά παιχνίδια και στα ηλεκτρονικά, τον Απρίλιο του 2011, ανακοίνωσε ότι τα προσωπικά δεδομένα 77 εκατομμυρίων PlayStation Network (PSN) συνδρομητών, καθώς και 24,6 εκατομμύρια Sony Online Entertainment λογαριασμοί, είχαν δεχθεί παραβίαση (Bonner, 2012). Η παραβίαση των δεδομένων αφορούσε πληροφορίες σχετικά με στοιχεία σύνδεσης, ιστορικά αγορών, στοιχεία καρτών και διευθύνσεις χρεώσεων. Η Sony αναγκάστηκε να απενεργοποιήσει τις υπηρεσίες PSN για ένα μήνα, προκειμένου να εκτιμηθεί το μέγεθος της επίθεσης. Μια πρόχειρη εκτίμηση του κόστους ανέφερε ένα ποσό της τάξεως των 171 εκατομμυρίων δολαρίων, χωρίς αυτός ο αριθμός να περιλαμβάνει ωστόσο τις ποινικές αποζημιώσεις από αγωγές, τις απώλειες που σχετίζονται με τη διακοπή των επιχειρηματικών δραστηριοτήτων, την κεφαλαιοποίηση της αγοράς ή την παραβίαση λογαριασμών πιστωτικών και χρεωστικών καρτών (Bonner, 2012).

Τρία χρόνια μετά από αυτά τα περιστατικά, το Νοέμβριο του 2014, τα δεδομένα της Sony Pictures διέρρευσαν για άλλη μια φορά. Τα δεδομένα που παραβιάστηκαν αφορούσαν περισσότερα από 30.000 εσωτερικά έγγραφα, 170.000 μηνύματα ηλεκτρονικής αλληλογραφίας, αριθμούς κοινωνικής ασφάλισης των υπαλλήλων της Sony, ιατρικά ιστορικά και ταινίες που δεν είχαν ακόμα κυκλοφορήσει. Η ίδια η κυβερνοεπίθεση παρέλυσε όλα τα συστήματα της Sony, καθιστώντας τη διαδικτυακή βάση δεδομένων της μη ανιχνεύσιμη, το τηλεφωνικό της σύστημα απενεργοποιημένο και καταστρέφοντας το 75% των διακομιστών της (Barnes & Cieply, 2014). Μετά την επίθεση, οι υπάλληλοι της Sony έλαβαν απειλητικά μηνύματα ηλεκτρονικής αλληλογραφίας συνοδευόμενα από μια εικόνα κομμένου κεφαλιού, τα οποία ανέφεραν ότι εάν δεν προέβαιναν σε καταγγελίες κατά της Sony, τα προσωπικά τους δεδομένα θα δημοσιοποιούνταν και οι πιστωτικές τους κάρτες θα ήταν διαθέσιμες για πώληση στις αγορές Dark Net. Παράλληλα, ορισμένοι υπάλληλοι παρατήρησαν στους τραπεζικούς τους λογαριασμούς υπέρβαση των

πιστωτικών ορίων (Barnes & Cieply, 2014). Υποβλήθηκαν ομαδικές αγωγές εργαζομένων, είτε γιατί η Sony δεν ειδοποίησε τα άτομα των οποίων τα δεδομένα διέρρευσαν, είτε ένεκα του φόβου πως θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν οι προσωπικές πληροφορίες που διέρρευσαν. Επιπλέον, 47.000 υπάλληλοι και ηθοποιοί επλήγησαν από τη συγκεκριμένη κυβερνοεπίθεση, ενώ η κυβέρνηση της Βόρειας Κορέας θεωρήθηκε υπαίτια από πολλούς, επειδή η ταινία «The interview» παρουσίαζε τη φανταστική δολοφονία του Κορεάτη ηγέτη Κιμ Γιονγκ Ουν. Το περιεχόμενο της ταινίας θεωρήθηκε προσβλητικό και ότι συμβάλλει σημαντικά στην προώθηση της τρομοκρατίας. Για το λόγο αυτό, η Sony κλήθηκε να ακυρώσει την προβολή της ταινίας και να διακόψει την παραγωγή ταινιών που σχετίζονται με τρομοκρατικές επιθέσεις (Peterson, 2014).

- **<u>Υπόθεση Ashley Madison</u>**

Τον Ιούλιο του 2015, πληροφορίες για 33 εκατομμύρια λογαριασμούς και προσωπικά δεδομένα ατόμων που ήταν εγγεγραμμένα στον ιστότοπο Ashley Madison, έναν ιστότοπο γνωριμιών που διευκόλυνε τη σύναψη ερωτικών και εξωσυζυγικών σχέσεων, διέρρευσαν (Agrafiotis et al., 2018). Βασικές αρχές του συγκεκριμένου ιστότοπου αποτελούσαν η τήρηση της ιδιωτικότητας και της ασφάλειας μέσω των οποίων θα έχτιζαν μια σχέση εμπιστοσύνης με τους πελάτες τους. Η κυβερνοεπίθεση επομένως, επέφερε δραματικές συνέπειες στη φήμη της εταιρείας, όχι μόνο επειδή εξέθεσε τα τρωτά σημεία των συστημάτων ασφαλείας της, αλλά και επειδή το αίτημα των πελατών να διαγραφούν τα προσωπικά τους δεδομένα, δεν ικανοποιήθηκε (Agrafiotis et al., 2018). Ως αποτέλεσμα, η εταιρεία δέχθηκε ένα μεγάλο αριθμό αγωγών, ενώ πολλοί πελάτες έπεσαν θύματα εκβιασμών που αντανακλούσαν επαγγελματικές, προσωπικές και οικονομικές διακλαδώσεις.

ΜΕΡΟΣ Δ΄

Ζητήματα κυβερνοασφάλειας: προληπτικά μέτρα & αντιμετώπιση περιστατικών

1. Η ασφάλεια του πληροφοριακού συστήματος μιας επιχείρησης

Όπως αναλύθηκε και στα προηγούμενα κεφάλαια, οι επιχειρήσεις έρχονται αντιμέτωπες με πολλούς κινδύνους στον κυβερνοχώρο. Έτσι, προκειμένου να αποφύγουν τις όποιες δυσμενείς συνέπειες, οφείλουν να μεριμνούν για την ασφάλεια των πληροφοριακών συστημάτων τους προκειμένου να προασπίζεται τόσο η πνευματική ιδιοκτησία, όσο και τα τυχόν προσωπικά ή ιδιωτικά και εμπιστευτικά δεδομένα που χειρίζονται. Η ασφάλεια αυτή των πληροφοριακών συστημάτων των επιχειρήσεων (cyber security), αποτελεί τη συλλογή δραστηριοτήτων που προστατεύουν το πληροφοριακό σύστημα και τα δεδομένα που είναι αποθηκευμένα σε αυτό (Kim & Solomon, 2021, pp.10-11), και συνιστά ένα ζήτημα που συγκεντρώνει ολοένα και περισσότερη προσοχή λόγω της ευρείας εξάρτησης της καθημερινότητας του επιχειρηματικού κόσμου από τα συστήματα υπολογιστών (Backhouse & Dhillon, 1996).

Μέσα από την ανασκόπηση της βιβλιογραφίας, διαπιστώνεται ότι ενώ ο όρος της ασφάλειας στον κυβερνοχώρο χρησιμοποιείται ευρέως, οι ορισμοί που του προσδίδονται είναι εξαιρετικά μεταβλητοί, συχνά υποκειμενικοί και μερικές φορές, μη αναλυτικοί. Η απουσία αυτή ενός συνοπτικού και ευρέως αποδεκτού ορισμού που αποτυπώνει την πολυδιάστατη εικόνα της ασφάλειας στον κυβερνοχώρο, παρεμποδίζει τις επιστημονικές και τεχνολογικές προόδους, ενώ συνάμα διαχωρίζει τους κλάδους που θα πρέπει να ενεργούν συντονισμένα για την επίλυση των περίπλοκων προκλήσεων στον κυβερνοχώρο. Ωστόσο, ένας γενικός και περιληπτικός ορισμός που θα μπορούσε να δοθεί είναι αυτός που ορίζει την ασφάλεια στον κυβερνοχώρο ως «*την οργάνωση και συλλογή πόρων, διαδικασιών και δομών που χρησιμοποιούνται για την προστασία του κυβερνοχώρου και των συστημάτων που υποστηρίζουν τον κυβερνοχώρο, από περιστατικά που δεν ευθυγραμμίζονται με τα δικαιώματα ιδιοκτησίας*» (Craigen et al., 2014).

Η ασφάλεια των επιχειρήσεων στον κυβερνοχώρο, συνιστά επιπλέον ένα προϊόν μεταφοράς του κινδύνου, το οποίο μπορούν να εξασφαλίσουν οι επιχειρήσεις για να μετριάσουν τις απώλειες ένεκα προβλημάτων τεχνολογίας πληροφοριών (π.χ.

διακοπή λειτουργίας της επιχείρησης από δυσλειτουργία υπολογιστών, κλοπή ή απώλεια των δεδομένων της από κακόβουλα λογισμικά, κ.ά.) (Fauntleroy et al., 2015). Ειδικότερα, η ασφάλεια αυτή εξασφαλίζεται μέσα από δραστηριότητες που προασπίζουν τις πληροφορίες, τα δεδομένα και τα συστήματα πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, διακοπή, τροποποίηση ή καταστροφή, από εισβολείς στα δίκτυα όπως ιοί/σκουλήκια, από κλοπές ή βανδαλισμούς, από φυσικές καταστροφές, από δυσμενείς περιβαλλοντικές συνθήκες, από διακοπές ρεύματος και γενικότερα από άλλες ανεπιθύμητες καταστάσεις (Andress, 2014, p.3). Στην εργασία αυτή, θα επικεντρωθούμε στην προστασία των δεδομένων και περιουσιακών στοιχείων των συστημάτων των επιχειρήσεων από αυτούς που επιδιώκουν να τα χρησιμοποιήσουν με κατάχρηση, με σκοπό την αντιμετώπιση του κυρίαρχου ζητήματος αυτής, που είναι οι κυβερνοεπιθέσεις σε βάρος επιχειρήσεων.

Με το ζήτημα της ασφάλειας στον κυβερνοχώρο ασχολήθηκαν αρκετοί ερευνητές. Για παράδειγμα ο Gordon και οι συνεργάτες του το 2003 μελέτησαν θέματα σχετικά με την ασφάλεια έναντι των κινδύνων στον κυβερνοχώρο και πιο συγκεκριμένα ζητήματα που σχετίζονται με την τιμολόγηση των πληροφοριών που προσφέρουν ασφάλεια έναντι των κινδύνων (pricing), την πλευρά της δυσμενούς επιλογής (adverse selection) και την πλευρά του ηθικού κινδύνου (moral hazard). Όσον αφορά την τιμολόγηση, ανέφεραν ότι αυτή σε κάθε περίπτωση διαφέρει και καθορίζεται με βάση τα δεδομένα της εκάστοτε επιχείρησης και κατάστασης. Αναφορικά με το ζήτημα της δυσμενούς επιλογής, κατέληξαν στο ότι όσο πιο επίφοβο είναι μια επιχείρηση να πέσει θύμα παραβίασης των δεδομένων της, τόσο περισσότερες πιθανότητες υπάρχουν προκειμένου να αναζητήσει έναν τρόπο που θα της προσφέρει την πολυπόθητη διαδικτυακή της ασφάλεια. Τέλος, ενώ η δυσμενή επιλογή αφορά στην ουσία ιδιωτικές πληροφορίες της επιχείρησης *πριν* από τη σύναψη σύμβασης για την ασφάλειά της, το ζήτημα του ηθικού κινδύνου αφορά την έλλειψη κινήτρων από την πλευρά της επιχείρησης να λάβει μέτρα που μειώνουν τις πιθανότητες ζημίας, *μετά* την αγορά ασφάλισης. Η προσφορά εκπτώσεων για τη λήψη συγκεκριμένων μέτρων ασφαλείας, αποτελεί στην τελευταία περίπτωση ένα βασικό κίνητρο (Gordon et al., 2003).

Το 2005 ο Mukhopadhyay και οι συνεργάτες του, υποστήριξαν ότι τα λογισμικά που χρησιμοποιούνται από επιχειρήσεις για την προστασία από κακόβουλες επιθέσεις, δεν αποδίδουν στο βαθμό που θα έπρεπε. Πρότειναν λοιπόν την απόκτηση ενός ασφαλιστικού προϊόντος ως συμπληρωματικό τρόπο προστασίας,

προκειμένου να μειωθεί η οικονομική ζημία που προκαλείται, με τον ισχυρισμό ότι τα πλεονεκτήματα από την ασφάλιση θα είναι μεγαλύτερα από το κόστος που θα προκύψει για την ασφάλισή τους. Επιπροσθέτως, έκαναν λόγο για τη θεωρία της χρησιμότητας (utility theory). Πρόκειται για μία θετική θεωρία που στηρίζεται στα οικονομικά προκειμένου να εξηγήσει την παρατηρούμενη συμπεριφορά και τις επιλογές των ατόμων, ή στη συγκεκριμένη περίπτωση, των επιχειρήσεων. Η κάθε επιχείρηση σύμφωνα με την προαναφερθείσα θεωρία θα πλήρωνε το ασφάλιστρο με βάση το προφίλ των κινδύνων που έχει να αντιμετωπίσει (Mukhopadhyay et al., 2005).

Ο Shackelford (2012) μελετώντας τον αντίκτυπο των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, κατέληξε στο συμπέρασμα ότι οι επιχειρήσεις οφείλουν να στραφούν σε πρακτικές ασφάλισής τους στον κυβερνοχώρο, προκειμένου να μπορούν να διαχειριστούν καλύτερα τις επιθέσεις που δέχονται καθώς επίσης και τις νομικές ευθύνες που προκύπτουν από τις παραβιάσεις δεδομένων. Επισήμανε λοιπόν την επιτακτική ανάγκη να ληφθούν μέτρα για την ασφάλεια στον κυβερνοχώρο και υποστήριξε ότι οι επιχειρήσεις οφείλουν να εντοπίζουν τρόπους που τις καθιστούν ικανές να προβλέπουν τους κινδύνους, προκειμένου να μειώσουν τον εταιρικό κίνδυνο και να εξασφαλίσουν την ευημερία και τη δομή τους. Αυτό θα επιτευχθεί μέσω της ενίσχυσης της ασφάλειας της επιχείρησης στον κυβερνοχώρο με την συνδρομή λογισμικών και ειδικών προγραμμάτων ασφάλισης, όπως για παράδειγμα με την εγκατάσταση τειχών προστασίας, την επένδυση σε δυνατότητες ανίχνευσης εισβολής, την κρυπτογράφηση κ.λπ.. Ακολούθως, ο ίδιος υποστήριξε ότι οι επιχειρήσεις θα πρέπει να αξιολογήσουν την ασφαλιστική τους κάλυψη και να πραγματοποιήσουν ανάλυση του κόστους και του οφέλους από την έκθεσή τους στον κυβερνοχώρο, και τέλος να αποφασίσουν εάν θα επενδύσουν σε κάποια νέα μορφή ασφάλισης κινδύνου στον κυβερνοχώρο (Shackelford, 2012).

Παρομοίως, οι Eling και Schnell (2016) ασχολήθηκαν και αυτοί με τη σειρά τους με το ζήτημα της ασφάλισης στον κυβερνοχώρο. Κατά την έρευνά τους, διαπίστωσαν ότι η ασφαλιστική κάλυψη των επιχειρήσεων έναντι των κυβερνοεπιθέσεων, είναι αρκετά περιορισμένη. Πιο συγκεκριμένα τόνισαν ότι στις Η.Π.Α. έχουν γίνει κάποια σημαντικά βήματα προόδου ως προς το ζήτημα αυτό, σε αντίθεση με την Ευρωπαϊκή Ένωση που έχει μείνει αρκετά πίσω. Ακόμη, μελετώντας τη βιβλιογραφία, τόνισαν ότι υπάρχουν σημαντικά κενά ως προς το ζήτημα της ασφάλειας στον κυβερνοχώρο και ότι η πρόσφατη βιβλιογραφία δε δύναται να το

υποστηρίξει καθώς πρόκειται για ένα δυναμικό θέμα που χρειάζεται συνεχή μελέτη από τους ερευνητές. Επιπρόσθετα, οι ίδιοι ανέδειξαν από τη μελέτη τους την ύπαρξη τριών ουσιαστικών προβλημάτων τα οποία εμποδίζουν την ανάπτυξη της ασφαλιστικής αγοράς. Το πρώτο πρόβλημα είναι η αδυναμία πρόβλεψης των απωλειών που ακολουθούν μετά από μία κυβερνοεπίθεση. Το δεύτερο πρόβλημα αφορά το γεγονός ότι οι περισσότερες επιχειρήσεις που καταφεύγουν στην ασφάλιση των πληροφοριακών τους συστημάτων είναι εκείνες οι οποίες έχουν ήδη υποστεί μία σοβαρή επίθεση στον κυβερνοχώρο, με αποτέλεσμα ένα μεγάλο ποσοστό επιχειρήσεων που δεν έχουν προσβληθεί να μην μεριμνούν για την ασφάλειά τους και να είναι περισσότερο εκτεθειμένες στους κινδύνους που ελλοχεύουν. Αξίζει να σημειωθεί στο σημείο αυτό ότι εφόσον οι επιχειρήσεις αυτές ασφαλιστούν, παύουν να λαμβάνουν πια από μόνες τους μέτρα αυτοπροστασίας, γεγονός που τις καθιστά περισσότερο ευάλωτες. Τέλος, το τρίτο πρόβλημα έγκειται στο γεγονός ότι τα υπάρχοντα συμβόλαια ασφάλισης καλύπτουν μονάχα μικρές υλικές ζημίες και περιέχουν αρκετές εξαιρέσεις όπως για παράδειγμα την περίπτωση πρόσβασης σε μη ασφαλείς ιστότοπους, τις αυτοπροκαλούμενες απώλειες κ.ά. (Eling & Schnell, 2016).

Εν συνεχεία ο Franke (2017) εξέτασε την ασφαλιστική αγορά στον κυβερνοχώρο της Σουηδίας. Η έρευνά του πραγματοποιήθηκε μέσα από συνεντεύξεις, τις οποίες του παραχώρησαν οι ιθύνοντες των εταιριών που ασχολούνται με την ασφάλεια στον κυβερνοχώρο, συμπεραίνοντας ότι οι ασφαλιστικές εταιρίες ζητούν από τις επιχειρήσεις που ασφαλίζουν να θωρακίζουν τα πληροφοριακά συστήματά τους. Έτσι, οι επιχειρήσεις με υψηλά επίπεδα αυτοπροστασίας των διαδικτυακών τους δομών και με την πρόσθετη ασφάλεια που παρέχεται σε αυτές από ασφαλιστικές εταιρίες, περιορίζουν τους κινδύνους και σε ορισμένες περιπτώσεις τους αποφεύγουν εξ’ ολοκλήρου. Σε κάθε περίπτωση πρέπει να υπάρχει μέριμνα και από την πλευρά των επιχειρήσεων και όχι εφησυχασμός, καθώς πρόκειται για ένα ζήτημα υψίστης σημασίας (Frakne, 2017).

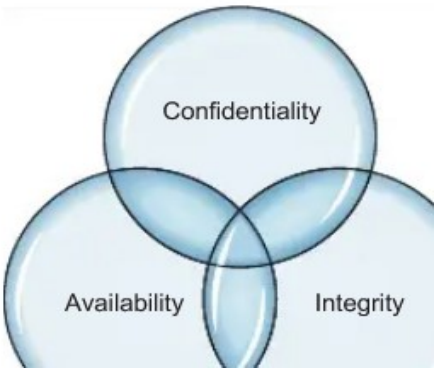
Στην εποχή μας, για να επιτευχθεί η ασφάλεια στον κυβερνοχώρο και να εκμηδενιστούν τα ποσοστά κυβερνοεπιθέσεων σε βάρος τους, οι επιχειρήσεις ακολουθούν τρία βασικά διακριτά στάδια:

α) στάδιο λήψης προληπτικών μέτρων, όπου η επιχείρηση αναπτύσσει έναν εταιρικό σχεδιασμό με μέτρα προστασίας,

β) στάδιο ανίχνευσης, δηλαδή η διαδικασία αναζήτησης και εντοπισμού ιχνών προκειμένου να εξιχνιαστεί οποιοδήποτε περιστατικό κυβερνοεπίθεσης σε βάρος τους και να καταγραφούν οι όποιες συνέπειες, και

γ) στάδιο αντίδρασης, δηλαδή οι ενέργειες που εκδηλώνουν με σκοπό τη διακοπή και αντιμετώπιση των υπό εξέλιξη κυβερνοεπιθέσεων και την αποκατάσταση των πόρων που έχουν υποστεί ζημία (Μαυρίδης, 2015, σσ.16-17).

Παράλληλα, για να μπορούμε να μιλήσουμε για ασφάλεια στον κυβερνοχώρο, θα πρέπει να ικανοποιούνται οι βασικές αρχές της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας (Kim & Solomon, 2021, p.13). Οι βασικές αυτές αρχές αποτελούν το μοντέλο ασφαλείας CIA (Confidentiality - Integrity - Availability), το οποίο καθοδηγεί τις πολιτικές ασφαλείας μίας επιχείρησης.



Εικόνα 5
Μοντέλο ασφαλείας CIA
Πηγή: The basics of information security: understanding the fundamentals of InfoSec in theory and practice (Andress, 2014, p.5)

Αναλύοντας τις αρχές αυτές, θα μπορούσε κανείς να πει ότι η εμπιστευτικότητα (confidentiality) είναι έννοια όμοια με την ιδιωτικότητα και κατοχυρώνεται μέσω της προστασίας των πληροφοριών και δεδομένων, με τέτοιο τρόπο ώστε η χρήση τους να περιορίζεται μόνο σε άτομα με εξουσιοδοτημένη πρόσβαση και για εξουσιοδοτημένους σκοπούς (Andress, 2014, p.6). Οι επιχειρήσεις μπορούν να εξασφαλίσουν την προστασία των ιδιωτικών τους δεδομένων και κατ' επέκταση την εμπιστευτικότητα, είτε με τον καθορισμό κατευθυντήριων γραμμών και πολιτικών με πλήρη καθοδήγηση για τον τρόπο χειρισμού των ιδιωτικών δεδομένων, είτε με τη χρήση τεχνικών κρυπτογραφίας για την απόκρυψη και κωδικοποίηση των

εμπιστευτικών δεδομένων που υπάρχουν σε συσκευές αποθήκευσης και βάσεις δεδομένων, αλλά και αυτών που διακινούνται εντός του κυβερνοχώρου. Από την άλλη πλευρά, η εμπιστευτικότητα τίθεται σε κίνδυνο εντός μιας επιχείρησης με διάφορους τρόπους όπως με την αποστολή ενός συνημμένου μηνύματος ηλεκτρονικής αλληλογραφίας, με την παράνομη εισβολή εντός των συστημάτων της από ανταγωνιστές ή hackers, κ.λπ.. Όσο περισσότερο διασφαλίζεται η εμπιστευτικότητα μιας επιχείρησης με την αποτροπή μη εξουσιοδοτημένης πρόσβασης, τόσο υψηλότερα επίπεδα ελέγχου των προσωπικών τους δεδομένων ενδέχεται να αντιληφθούν οι πελάτες της (Samonas & Coss, 2014). Η αρχή της εμπιστευτικότητας και γενικότερα το απόρρητο των δεδομένων (ιδιωτικότητα), απασχολούν ιδιαίτερα τις πολιτειακές κυβερνήσεις οι οποίες θεσπίζουν νόμους ή ενισχύουν τους ήδη υπάρχοντες σε πολιτειακό και ομοσπονδιακό επίπεδο (Kim & Solomon, 2021, pp.14-16).

Η δεύτερη αρχή, αυτή της ακεραιότητας (integrity), αναφέρεται στην προστασία των πληροφοριών από ανεπιθύμητη ή μη εξουσιοδοτημένη τροποποίηση, αλλοίωση ή καταστροφή (Samonas & Coss, 2014). Πιο συγκεκριμένα, η ακεραιότητα συνδέεται με την εγκυρότητα και την ακρίβεια και συνεπώς η έλλειψη αυτής οδηγεί σε ανακριβείς και μη έγκυρες πληροφορίες και δεδομένα. Για την πλειοψηφία των επιχειρήσεων οι πληροφορίες και τα δεδομένα τους έχουν μεγάλη αξία, δεδομένου ότι αφορούν περιουσιακά στοιχεία πνευματικής ιδιοκτησίας, μυστικούς αλγόριθμους παραγωγής και προώθησης προϊόντων, βάσεις δεδομένων πελατών, κ.ά.. Πρόκειται δηλαδή για δεδομένα που είναι κρίσιμα για τις επιχειρηματικές δραστηριότητες και για το λόγο αυτό το σαμποτάζ και η διαφθορά της ακεραιότητας αυτών ένεκα μη εξουσιοδοτημένων αλλαγών, αποτελούν σοβαρές απειλές για μία επιχείρηση με κίνδυνο να την υπονομεύσουν (Kim & Solomon, 2021, p.16). Προκειμένου λοιπόν να διατηρηθεί η ακεραιότητα, κάθε επιχείρηση θα πρέπει να έχει διαθέσιμα μέσα για την αποτροπή των μη εξουσιοδοτημένων αλλαγών στα δεδομένα και τις πληροφορίες της και προσωπικό με εξειδικευμένη γνώση στο χειρισμό των μέσων αυτών ώστε να αναιρέσουν ή να επαναφέρουν αλλαγές που δεν είναι επιθυμητές (Andress, 2014, pp.6-7).

Τέλος, η τρίτη αρχή της διαθεσιμότητας (availability) αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης στις πληροφορίες και τα δεδομένα, ώστε οι μεν πληροφορίες και τα δεδομένα να είναι προσπελάσιμα και η δε πρόσβαση έγκαιρη και αξιόπιστη (Μαυρίδης, 2015, σελ.18). Ειδικότερα, η διαθεσιμότητα εκφράζεται ως το

χρονικό διάστημα όπου ένα σύστημα και τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους χρήστες του χωρίς διαλείμματα, τα οποία μπορεί να οφείλονται σε μία απλή απώλεια ενέργειας, σε σοβαρότερα προβλήματα του λειτουργικού συστήματος ή εφαρμογής, σε επιθέσεις δικτύου, σε παραβιάσεις ή γενικότερα σε άλλα προβλήματα. Όταν υπάρχει αδικαιολόγητη καθυστέρηση σε υπηρεσίες ενός πληροφοριακού συστήματος που χρειάζεται μια εξουσιοδοτημένη οντότητα, η οποία ενδεχομένως να οφείλεται σε κάποιον εξωτερικό παράγοντα όπως είναι ένας εισβολέας, τότε πρόκειται για επιθέσεις άρνησης υπηρεσίας (Denial of Service). Τέτοιες επιθέσεις είναι αυτές κατά τις οποίες ο επιτιθέμενος κατακλύζει το σύστημα μιας επιχείρησης με έναν εξαιρετικά μεγάλο αριθμό αιτήσεων σύνδεσης (Andress, 2014, p.7). Η διαθεσιμότητα λοιπόν αναδεικνύεται σε ένα σημαντικό χαρακτηριστικό της ασφάλειας, στην εξασφάλιση της οποίας στηρίζεται η εξάλειψη πιθανοτήτων εμφάνισης επιθέσεων άρνησης υπηρεσίας. Ωστόσο, υπάρχουν ελάχιστοι μηχανισμοί που συνδράμουν στην υποστήριξή της.

Στην υπάρχουσα βιβλιογραφία, συναντάται και ένα ισχυρότερο μοντέλο ασφαλείας, γνωστό ως μοντέλο ασφαλείας CIAAA (Confidentiality - Integrity - Availability - Accountability - Authenticity). Η διαφορά του μοντέλου αυτού από το μοντέλο CIA που αναλύθηκε παραπάνω έγκειται στην προσθήκη δύο έτερων αρχών, της υπευθυνότητας (accountability) και της αυθεντικότητας (authenticity). Σύμφωνα με το μοντέλο αυτό, η μεν υπευθυνότητα αναφέρεται στην ανίχνευση των ενεργειών ενός χρήστη και την απόδοσή τους σε αυτόν εφόσον κριθεί αναγκαίο και η δε αυθεντικότητα αναφέρεται στην εμπιστοσύνη που προσδίδεται στην εγκυρότητα ενός μηνύματος ή γενικότερα στην ταυτότητα του αποστολέα (Φρυδάς, 2018, σελ.62).

Εικόνα 6
Μοντέλο ασφαλείας CIAAA
Πηγή: Ο κυβερνοχώρος και η ασφάλειά του (Φρυδάς, 2018, σελ.62)

Σύμφωνα με όσα αναφέρθηκαν παραπάνω, τεκμαίρεται ότι το θέμα της ασφάλειας των επιχειρήσεων στον κυβερνοχώρο είναι εξαιρετικά σημαντικό, καθώς η εξασφάλισή της, αφενός αποτελεί ένα ζήτημα μείζονος σημασίας για τις πολιτικές όλων των κυβερνήσεων παγκοσμίως, αφετέρου συνδέεται άρρηκτα με την ομαλή λειτουργία ολόκληρης της κοινωνίας της πληροφορίας (Παρασκευάς και σύν., 2015, σελ.236). Χωρίς ένα πρόγραμμα ασφάλειας στον κυβερνοχώρο, οι επιχειρήσεις καθίστανται ευάλωτες ως προς την εύρυθμη λειτουργία τους και δεν μπορούν να προασπιστούν από παραβιάσεις δεδομένων, γεγονός που τις καθιστά ακαταμάχητους στόχους για τους εγκληματίες στον κυβερνοχώρο. Ταυτόχρονα τίθεται σε κίνδυνο η ακεραιότητα του συστήματος όχι μόνο για την ίδια την επιχείρηση, αλλά και για όλους τους πελάτες της που έχουν τα προσωπικά τους στοιχεία αποθηκευμένα στο παραβιασμένο σύστημα (Samonas & Coss, 2014).

2. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων [10] στις επιχειρήσεις

Οι επιχειρήσεις σε ολόκληρο τον κόσμο συλλέγουν, επεξεργάζονται και χρησιμοποιούν τα προσωπικά δεδομένα των πελατών τους προκειμένου να μπορέσουν να παρέχουν τις υπηρεσίες τους, είτε δραστηριοποιούνται στον κυβερνοχώρο, είτε εκτός αυτού. Για το λόγο αυτό, οι φορείς και τα νομοθετικά όργανα διαμόρφωσαν ένα ρυθμιστικό πλαίσιο ώστε αυτές οι επιχειρήσεις να συμμορφώνονται σε ένα γενικότερο κανόνα προστασίας δεδομένων και τα ιδιωτικά στοιχεία να προστατεύονται από την αλόγιστη χρήση και παρουσίασή τους. Πρόκειται για το Γενικό Κανονισμό Προστασίας Δεδομένων (Γ.Κ.Π.Δ.), ο οποίος ψηφίστηκε το Μάιο του 2016 από το Ευρωπαϊκό Κοινοβούλιο και τέθηκε σε ισχύ από τις 25 Μαΐου του 2018 (Tikkinen-Piri et al., 2018).

Ο Γ.Κ.Π.Δ. κατηγοριοποιείται σε έντεκα κεφάλαια, εντός των οποίων προσδιορίζονται οι αρχές, τα καθήκοντα του υπεύθυνου και του εκτελών την επεξεργασία, οι ανεξάρτητες εποπτικές αρχές, τα μέσα έννομης προστασίας, η ευθύνη και οι κυρώσεις, καθώς και λοιπές γενικότερες και ειδικότερες διατάξεις. Το πεδίο εφαρμογής του είναι περιορισμένο, και πιο συγκεκριμένα ισχύει για όλες τις επιχειρήσεις που βρίσκονται σε χώρες εντός της Ευρωπαϊκής Ένωσης και του Ευρωπαϊκού Οικονομικού Χώρου, καθώς και για κάθε επιχείρηση εκτός Ευρωπαϊκής

[10] https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

Ένωσης που επιδιώκει συναλλαγές με επιχειρήσεις ή άτομα σε χώρες του Ευρωπαϊκού Οικονομικού Χώρου της Ευρωπαϊκής Ένωσης (Presthus & Sørum, 2018). Κύριος στόχος του είναι:

α) η ενίσχυση του ελέγχου με σκοπό την προστασία των προσωπικών δεδομένων,

β) η διευκόλυνση της ελεύθερης ροής των δεδομένων εντός της ενιαίας αγοράς της Ευρωπαϊκής Ένωσης και

γ) η μείωση του διοικητικού φόρτου, απλοποιώντας το κανονιστικό περιβάλλον για τις διεθνείς επιχειρήσεις (Gobeo et al., 2022, p.5).

Εντός του Γ.Κ.Π.Δ., μεταξύ άλλων, προσδιορίζονται και οι κανόνες τους οποίους οφείλουν να τηρούν οι επιχειρήσεις. Ένας τέτοιος κανόνας προσδιορίζεται για παράδειγμα στο άρθρο 37, το οποίο προσδιορίζει την υποχρέωση διορισμού ενός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer), ο οποίος θα επωμίζεται την ευθύνη παρακολούθησης της συμμόρφωσης της επιχείρησης με τις ορισθείσες διατάξεις του Κανονισμού (Voigt & Von dem Bussche, 2017, pp.53-54). Ένας άλλος κανόνας αναφέρεται στα άρθρα 33 και 34 και αφορά την υποχρέωση άμεσης γνωστοποίησης των περιστατικών παραβίασης προσωπικών δεδομένων (απώλεια ή διαρροή αυτών) στο υποκείμενο των δεδομένων, αλλά και στην εποπτική αρχή. Πιο συγκεκριμένα η γνωστοποίηση αυτή οφείλει να γίνεται εντός 72 ωρών, από τη στιγμή που γίνεται αντιληπτό το περιστατικό παραβίασης (Voigt & Von dem Bussche, 2017, pp.65-66).

Πέραν των ενδεικτικών αυτών κανόνων, οι επιχειρήσεις, σύμφωνα με το άρθρο 5 του Κανονισμού, οφείλουν να ακολουθούν και κάποιες αρχές κατά τη συλλογή, τη χρήση και την επεξεργασία τόσο των δικών τους προσωπικών δεδομένων, όσο και αυτών που βρίσκονται στην κατοχή τους και ανήκουν σε πελάτες της (ιδιώτες, επιχειρήσεις, κυβέρνηση). Σε κάθε επιχείρηση, ο Υπεύθυνος Προστασίας των Προσωπικών Δεδομένων, του οποίου ο ρόλος αναφέρθηκε παραπάνω, οφείλει να είναι σε θέση να αποδείξει τη συμμόρφωση της επιχείρησης με όλες τις αρχές που παρατίθενται ακολούθως (*λογοδοσία*). Οι αρχές αυτές εξασφαλίζουν εν μέρει την πρόληψη από τυχόν κυβερνοεπιθέσεις και είναι οι εξής (Voigt & Von dem Bussche, 2017, pp.87-92):

α) νομιμότητα, αντικειμενικότητα και διαφάνεια

Η χρήση και επεξεργασία των προσωπικών δεδομένων οφείλει να γίνεται με τρόπο σύννομο, θεμιτό και διαφανή ως προς το υποκείμενο των δεδομένων. Επομένως, η

χρήση και επεξεργασία αυτών επιτρέπεται μόνο αν καλύπτεται από τη νομική άδεια ή συγκατάθεση του υποκειμένου τους.

β) περιορισμός σκοπού

Τα προσωπικά δεδομένα που συλλέγει η κάθε επιχείρηση, θα πρέπει να υποβάλλονται σε επεξεργασία μόνο για καθορισμένους, σαφείς και νόμιμους σκοπούς που έχουν καθοριστεί ρητά στο υποκείμενο των δεδομένων, κατά την έναρξη της συνεργασίας τους.

γ) ελαχιστοποίηση δεδομένων

Απαραίτητη η συλλογή, χρήση και επεξεργασία μονάχα των απολύτως απαραίτητων προσωπικών δεδομένων, για συγκεκριμένους και καθορισμένους σκοπούς.

δ) ακρίβεια

Διατήρηση των προσωπικών δεδομένων με τρόπο όπου θα εξασφαλίζεται η έγκαιρη ενημέρωση μέσω επικαιροποίησής τους, προκειμένου να παραμένουν ακριβή.

ε) περιορισμός χρόνου αποθήκευσης

Αποθήκευση των προσωπικών δεδομένων μονάχα για όσο χρονικό διάστημα δεν υπερβαίνει τους καθορισμένους σκοπούς συλλογής, χρήσης και επεξεργασίας τους. Η περίοδος αποθήκευσης θα πρέπει να περιορίζεται σε ένα αυστηρό ελάχιστο.

στ) ακεραιότητα και εμπιστευτικότητα

Τα προσωπικά δεδομένα να χρησιμοποιούνται και να επεξεργάζονται με μέριμνα την προστασία και την ασφάλειά τους, μέσω κατάλληλων τεχνικών ή οργανωτικών μέτρων, όπως π.χ. η κρυπτογράφηση.

Σήμερα, ο Γ.Κ.Π.Δ. αποτελεί έναν από τους αυστηρότερους κανονισμούς προστασίας δεδομένων που υπήρξε ποτέ και η εφαρμογή του είναι πολύ σημαντική αφού επιβάλλει αυστηρές κυρώσεις σε περιπτώσεις μη συμμόρφωσης από επιχειρήσεις που συλλέγουν και επεξεργάζονται δεδομένα πελατών εντός της Ευρωπαϊκής Ένωσης. Οι κυρώσεις που επιβάλλει φέρουν τη μορφή προστίμων, τα οποία είναι ευέλικτα και κλιμακωτά ανάλογα με την εκάστοτε επιχείρηση. Σύμφωνα με το άρθρο 83 αυτού του Κανονισμού, υπάρχουν δύο επίπεδα προστίμων. Το πρώτο επίπεδο προστίμων ανέρχεται στο ύψος των 10 εκατομμυρίων ευρώ ή του 2% των παγκόσμιων ετήσιων εσόδων της επιχείρησης από το προηγούμενο οικονομικό έτος και αφορά τις λιγότερο σοβαρές παραβάσεις, ενώ σε περίπτωση σοβαρότερων παραβάσεων που αντιβαίνουν του δικαιώματος στην ιδιωτική ζωή που συνιστά το επίκεντρο του Κανονισμού, εφαρμόζεται το δεύτερο επίπεδο προστίμων το οποίο ενδέχεται να οδηγήσει σε πρόστιμο ύψους έως και 20 εκατομμύρια ευρώ ή 4% των

παγκόσμιων ετήσιων εσόδων της επιχείρησης από το προηγούμενο οικονομικό έτος. Και στα δύο επίπεδα προστίμων, κάθε φορά επιβάλλεται το υψηλότερο πρόστιμο από τις δύο επιλογές (Gobeo et al., 2022, p.6 ; Voigt & Von dem Bussche, 2017, pp.210-211).

Στο πλαίσιο της εργασίας αυτής και συγκεκριμένα στο στάδιο της αντιμετώπισης, κρίνεται σκόπιμη η αναφορά στον εν θέματι Κανονισμό. Αυτό προκύπτει από το γεγονός ότι ενώ πολλοί δράστες επιδιώκουν την παραβίαση του πληροφοριακού συστήματος μιας επιχείρησης με σκοπό την παράνομη πρόσβαση σε προσωπικά δεδομένα και απόρρητα είτε της ίδιας επιχείρησης, είτε ακόμη και των πελατών της (Ransomware New Generation, 2021), η δράση τους αυτή δεν εκπληρώνεται, ένεκα της ύπαρξης του Κανονισμού αυτού που υποχρεώνει τις επιχειρήσεις να λάβουν δραστικά μέτρα για τη θωράκιση του πληροφοριακού τους συστήματος. Εύλογα λοιπόν τεκμαίρεται ότι ο Γ.Κ.Π.Δ. διαδραματίζει καθοριστικό ρόλο στον τομέα της αντιμετώπισης των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, δεδομένου ότι χωρίς την τήρηση των διατάξεων αυτού, αυξάνονται οι πιθανότητες προσβολής. Οι επιχειρήσεις σήμερα, δεδομένου του μεγάλου αριθμού των προσωπικών δεδομένων που διαχειρίζονται, σε συνδυασμό και με τα υψηλά ποσοστά κυβερνοεπιθέσεων που δέχονται και τις αυστηρές κυρώσεις που επιβάλλει ο Γ.Κ.Π.Δ., επενδύουν πολύ στον τομέα πρόληψης, μέσα από πρακτικές που θα αναλυθούν ακολούθως.

3. Εταιρικός σχεδιασμός για την πρόληψη κυβερνοεπιθέσεων

Όπως αναφέρθηκε και παραπάνω, προκειμένου να κατοχυρωθεί η ασφάλεια των πληροφοριακών συστημάτων και να περιοριστούν τα ποσοστά κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, οι ίδιες οφείλουν να λαμβάνουν προληπτικά μέτρα προστασίας (Μαυρίδης, 2015, σελ.16). Αυτό επιτυγχάνεται μέσω ενός εταιρικού σχεδιασμού όπου περιλαμβάνει όλα αυτά τα προληπτικά μέτρα. Πολλοί πιστεύουν ότι είναι δύσκολο να επιτευχθεί η περιφρούρηση των συστημάτων και των δικτύων μέσα από τον εταιρικό αυτό σχεδιασμό. Ωστόσο υπάρχει πληθώρα ενεργειών που μπορούν να γίνουν, προκειμένου να καταστεί εφικτή η εγκατάσταση κατάλληλων και αποτελεσματικών προγραμμάτων ασφαλείας στα πληροφοριακά συστήματα των επιχειρήσεων, αλλά και να υλοποιηθούν πρακτικές που θα οδηγήσουν σε πλήρως κατοχυρωμένα, από άποψη ασφάλειας, συστήματα και δίκτυα (Furnell, 2006, p.345).

Ο εταιρικός αυτός σχεδιασμός, θα πρέπει να πραγματώνεται όχι μόνο προς όφελος της ίδιας της επιχείρησης, αλλά συνάμα και προς όφελος των πελατών της, διότι σε αντίθετη περίπτωση, η έλλειψη ασφάλειας του πληροφοριακού συστήματος μιας επιχείρησης μπορεί να οδηγήσει σε βλάβη κάποιας άλλης επιχείρησης ή ιδιώτη. Ως απόρροια αυτού, ενδέχεται να εμπλακούν σε δικαστικές διαμάχες που θα ξεκινήσουν μεταξύ τους, είτε ακόμη και να επιβληθούν πρόστιμα στηριζόμενα στις διατάξεις του Γ.Κ.Π.Δ. (Furnell, 2006, p.346 ; Voigt & Von dem Bussche, 2017, pp.210-211).

Την άποψη υπέρ των προγραμμάτων ασφαλείας και των πρακτικών που λειτουργούν με τρόπο προληπτικό, την υιοθετεί ένα μεγάλο ποσοστό επιχειρήσεων, παρόλα αυτά υπάρχουν και εκείνες, οι οποίες έχουν αντίθετη άποψη για τους κάτωθι λόγους:

α) πιστεύουν ότι η ασφάλεια του πληροφοριακού τους συστήματος δεν είναι δική τους ευθύνη, αλλά αντιθέτως θα πρέπει να απασχολήσει κάποιον άλλον εκτός επιχείρησης,

β) έχουν την πεποίθηση ότι η εισαγωγή ενός προγράμματος ασφαλείας θα αναστατώσει την οργάνωση και το πρόγραμμα της επιχείρησης και

γ) ισχυρίζονται ότι το κόστος που θα προκύψει από τη λήψη μέτρων ασφαλείας, θα είναι εξαιρετικά υψηλό, υπερβαίνοντας τον προϋπολογισμό και αποτελώντας ταυτόχρονα ένα αναίτιο έξοδο για την επιχείρηση (Furnell, 2006, p.346 ; Wiggins, 2002).

Οι λόγοι αυτοί, αποτελούν πεποιθήσεις επιχειρήσεων προηγούμενων δεκαετιών. Πλέον, οι σύγχρονες επιχειρήσεις αντιλαμβάνονται ότι μπορεί να πέσουν θύματα κυβερνοεπιθέσεων ανά πάσα ώρα και στιγμή, και συνεπώς πρόκειται για ένα γεγονός που δεν μπορούν να το αγνοήσουν και να το θεωρήσουν ως πρόβλημα κάποιου τρίτου. Επιπρόσθετα, γνωρίζουν ότι τα συστήματα ασφαλείας εγκαθίστανται και ρυθμίζονται από επαγγελματίες και συνεπώς είναι σπάνιο έως και αδύνατο να προκαλέσουν δυσλειτουργία ή να αποτελέσουν εμπόδιο για την ίδια την επιχείρηση. Τέλος, αναγνωρίζουν ότι η ασφάλεια των πληροφοριακών τους συστημάτων αποτελεί ένα εξαιρετικά υψηλό κόστος, όμως αποδέχονται ότι οι επιπτώσεις που ενδέχεται να προκύψουν από την έλλειψη αυτής, θα οδηγήσουν σε κόστη πολύ υψηλότερα από αυτά που χρειάζονται για την ασφάλειά τους (Furnell, 2006, pp.346-347).

Απαιτείται συνεπώς μια ευρύτερη στρατηγική για τα ζητήματα ασφαλείας, η οποία θα περιλαμβάνει προληπτικά μέτρα. Με τον τρόπο αυτό, οι κυβερνοεπιθέσεις

δεν θα αντιμετωπίζονται ad hoc, και δεν θα υπάρχουν αμφιβολίες αναφορικά με το εάν έχει δοθεί η δέουσα προσοχή για την εξασφάλιση ενός σωστού επιπέδου προστασίας, που θα συμβάλλει στη μείωση των κυβερνοεπιθέσεων που λαμβάνουν χώρα σε βάρος των επιχειρήσεων (Furnell, 2006, p.349). Οι επιχειρήσεις λοιπόν, ενδείκνυται να λαμβάνουν τα ακόλουθα προληπτικά μέτρα (Λάζος, 2001, σσ.224-234 ; Sousa, 2019 ; IoT Security, 2022):

α) έλεγχος, καταγραφή και Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems-IDS)

Το ζήτημα του ελέγχου συνδέεται άμεσα με τη μη εξουσιοδοτημένη πρόσβαση, η οποία παρ' όλες τις προσπάθειες που έχουν καταβληθεί σε διάφορα επίπεδα, δεν έχει αντιμετωπιστεί με επάρκεια και εξακολουθεί να αποτελεί ένα βασικό κίνδυνο για την πληροφορική τεχνολογία της εκάστοτε επιχείρησης (Λάζος, 2001, σελ.225). Για την ανίχνευση λοιπόν των εισβολών και την αποτροπή των απειλών, οι μηχανισμοί ελέγχου αποτελούν μία αποτελεσματική λύση. Παράλληλα, σημαντική είναι και η διαδικασία της καταγραφής, δεδομένου ότι η συλλογή των καταγεγραμμένων δεδομένων, δύναται να χρησιμοποιηθεί ως αποδεικτικό στοιχείο μιας παραβίασης ενός πληροφοριακού συστήματος. Ωστόσο η καταγραφή από μόνη της μπορεί να μην είναι και τόσο αποτελεσματική (Furnell, 2006, pp.355-356). Για το λόγο αυτό υπάρχουν αρκετές επιτηδευμένες τεχνικές και Συστήματα Ανίχνευσης Εισβολών που αποτελούν περισσότερο προληπτικούς τρόπους, συμβάλλοντας στον εντοπισμό αφενός ενδείξεων παράνομης δραστηριότητας, μέσω της παρακολούθησης της δικτυακής κίνησης, και αφετέρου παρατυπιών, δηλαδή ενεργειών που αποκλίνουν από τα συνήθη πρότυπα χρήσης, όπως για παράδειγμα ο εντοπισμός σύνδεσης σε ένα σύστημα από άγνωστη στο παρελθόν συσκευή ή μοναδικό ψηφιακό αριθμό ταυτότητας (IP διεύθυνση). Αυτές οι μη φυσιολογικές δραστηριότητες υποδηλώνουν πιθανή παραβίαση και πολλές φορές οδηγούν είτε στην έγκαιρη σύλληψη δραστών, είτε σε λοιπές αυτοματοποιημένες αντιδράσεις για την αντιμετώπιση καταστάσεων. Με τον τρόπο αυτό, επιτυγχάνεται η πρόληψη του χάους που πιθανόν να επικρατούσε στο σύστημα σε περίπτωση μη εντοπισμού τους (Ασφάλεια Υπολογιστικού Νέφους, 2021).

β) απόδειξη αυθεντικότητας του χρήστη

Αν αναλογιστούμε ότι μεγάλο ποσοστό των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων οφείλεται στο γεγονός ότι οι δράστες αποκρύπτουν την πραγματική τους ταυτότητα, χρησιμοποιώντας παρανόμως στοιχεία άλλων χρηστών, αντιλαμβανόμαστε ότι η απόδειξη της αυθεντικότητας είναι ένα σημαντικό μέτρο που τουλάχιστον ελαχιστοποιεί, αν δεν κατορθώσει να εξουδετερώσει, τις πιθανότητες που ενδέχεται να προσβληθεί μια επιχείρηση. Η απόδειξη αυτή της αυθεντικότητας, επιτυγχάνεται με διάφορους τρόπους όπως είναι η χρήση φυσικών σημείων, τα ατομικά βιομετρικά χαρακτηριστικά (π.χ. δακτυλικά αποτυπώματα, αναγνώριση χαρακτηριστικών προσώπου ή φωνής), κ.ά.. Ωστόσο, η πιο κοινή μορφή απόδειξης της αυθεντικότητας ενός χρήστη είναι η χρήση κωδικών πρόσβασης, όπου αποτελούν μία de facto επιλογή, ένεκα της ευκολίας και απλότητας της μορφής τους, καθώς και του χαμηλού κόστους τους (Furnell, 2006, pp.349-350).

Οι κωδικοί πρόσβασης αποτελούν μία ενιαία, αμοιβαία και συμφωνημένη κωδικοποιημένη λέξη, η οποία θεωρείται ότι είναι γνωστή μόνο στο χρήστη και στο λειτουργικό σύστημα (Zviran & Haga, 1999). Δυστυχώς, ενώ αποτελούν σημαντικό μέσο άμυνας, πολλές φορές η ασφάλεια που παρέχουν υποβιβάζεται από τις λάθος επιλογές των χρηστών. Για το λόγο αυτό, υπάρχει μια σειρά καλών πρακτικών που θα πρέπει να ακολουθούνται από τους χρήστες κατά την επιλογή ενός κωδικού πρόσβασης, προκειμένου να βελτιωθεί το επίπεδο ασφάλειας των προσωπικών δεδομένων. Οι πρακτικές αυτές είναι (Furnell, 2006, pp.351-354 ; Zviran & Haga, 1999 ; [11]):

i. Να μη χρησιμοποιούνται κωδικοί οι οποίοι είναι εύκολο να ανακαλυφθούν από hackers, όπως για παράδειγμα χρονολογίες ίδρυσης της επιχείρησης, τίτλοι επωνυμίας τους, στοιχεία διεύθυνσης, ημερομηνία γέννησης του υπαλλήλου που χειρίζεται το σύστημα, κ.λπ. .

ii. Να επιλέγονται κωδικοί πρόσβασης που θα αποτελούνται από τουλάχιστον οκτώ χαρακτήρες, και θα περιλαμβάνουν συνδυασμό πεζών-κεφαλαίων γραμμάτων, αριθμών και συμβόλων. Με τον τρόπο αυτό αυξάνεται ο αριθμός των πιθανών συνδυασμών για ένα πρόγραμμα αυτόματης διάσπασης, προκειμένου να διασπάσει έναν κωδικό.

[11] https://leaf-it.com/10-ways-prevent-cyber-attacks/

iii. Να αλλάζουν ανά τακτά χρονικά διαστήματα οι κωδικοί πρόσβασης, τουλάχιστον μία φορά το μήνα, εκτός και αν πρόκειται για πιο ευαίσθητα προσωπικά δεδομένα της ίδιας της επιχείρησης ή των πελατών της, όπου το χρονικό αυτό διάστημα καλό θα είναι να περιοριστεί σε 7-14 ημέρες. Ένα ορθό σύστημα κωδικών πρόσβασης, εμποδίζει τη χρήση των ίδιων κωδικών για μερικούς μήνες, προκειμένου να αποτρέπει την προσπάθεια επιστροφής σε ήδη χρησιμοποιημένο κωδικό πρόσβασης.

iv. Να μην καταγράφονται οι κωδικοί πρόσβασης σε χαρτί ή σε σημειώματα επικολλημένα στις οθόνες, γιατί είναι εύκολο να εντοπιστούν από τρίτα κακοπροαίρετα πρόσωπα. Μία λύση είναι να χρησιμοποιείται ένα κωδικοποιημένο σχήμα που θα υπενθυμίζει στον κάθε χρήστη τον κωδικό πρόσβασης.

v. Να μη χρησιμοποιείται ο ίδιος κωδικός πρόσβασης σε όλα τα συστήματα.

vi. Να μη γνωστοποιούνται οι κωδικοί πρόσβασης σε κανέναν, συμπεριλαμβανομένων και των συνεργατών.

vii. Να μην επαναπαύεται η ίδια η επιχείρηση με τη χρήση κωδικών πρόσβασης, καθώς η διάσπασή τους είναι εύκολη όχι μόνο από δράστες αλλά και από προγράμματα αυτόματης διάσπασης που κυκλοφορούν ελεύθερα στον κυβερνοχώρο.

Υποθέτοντας ότι η αυθεντικότητα του χρήστη αποδεικνύεται με τη χρήση κωδικών πρόσβασης, ο εκάστοτε χρήστης θα πρέπει να είναι καλά εκπαιδευμένος στη σωστή χρήση αυτών και να λαμβάνει υπόψη όλες τις προαναφερόμενες πρακτικές. Σε περίπτωση απόδειξης αυτής με άλλον τρόπο, όπως για παράδειγμα με τη χρήση βιομετρικών χαρακτηριστικών, κάτι τέτοιο δεν απαιτείται, αφού τα χαρακτηριστικά αυτά είναι μοναδικά και κατά κανόνα αναλλοίωτα για τον κάθε χρήστη (Λάζος, 2001, σελ.225). Συμπερασματικά όμως, με όποιον τρόπο και αν αποδεικνύεται η αυθεντικότητα, θα πρέπει να σημειωθεί ότι αποτελεί ένα υψηλό επίπεδο προστασίας από απειλές, εξωτερικά και εσωτερικά της επιχείρησης.

γ) έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων είναι μία ασφαλής διαδικασία ελέγχου της ταυτότητας του προσώπου, η οποία απαιτεί περισσότερες από μία τεχνικές ελέγχου, όπως για παράδειγμα την εισαγωγή κωδικού που αποστέλλεται στο κινητό τηλέφωνο ή στον προσωπικό λογαριασμό ηλεκτρονικού ταχυδρομείου, τη σάρωση δακτυλικού αποτυπώματος, τη σάρωση προσώπου, κ.ά.. Η πρακτική αυτή συνιστά ένα από τα οικονομικότερα και πιο αποτελεσματικά προληπτικά μέτρα

ενάντια σε κυβερνοεπιθέσεις εις βάρος επιχειρήσεων (Dasgupta et al., 2017, pp.188-189).

δ) τείχη προστασίας (firewalls)

Τα τείχη προστασίας είναι διαρρυθμίσεις που παρακολουθούν και ελέγχουν τη ροή της κυκλοφορίας του δικτύου, με βάση ένα σύνολο προκαθορισμένων κανόνων (Neupane et al., 2018). Με τον τρόπο αυτό προστατεύουν το πληροφοριακό σύστημα ή μέρος αυτού (π.χ. τομέα απορρήτων), από παράνομη πρόσβαση, με βασική προϋπόθεση η πρόσβαση αυτή να προέρχεται από εξωτερική, του πληροφοριακού συστήματος, πηγή, δηλαδή από πηγή που εισέρχεται στο εκάστοτε πληροφοριακό σύστημα μέσω των θυρών. Θα πρέπει να σημειωθεί όμως, ότι ένα τείχος προστασίας δε συνιστά και την καλύτερη δυνατή προστασία, δεδομένου ότι οι απειλές (π.χ. ιοί) μπορεί να εισέρχονται σε ένα σύστημα όχι μόνο απευθείας μέσω των θυρών, αντίθετα μπορεί να προέρχονται και από περιφερειακές συσκευές που εισέρχονται εντός των θυρών, όπως δισκέτες, CDs, USB, κ.λπ. (Λάζος, 2001,σελ.226).

ε) συστήματα αντιμετώπισης κατά των ιών (anti-virus)

Τα συστήματα αντιμετώπισης κατά των ιών συνιστούν λογισμικά προγράμματα που προστατεύουν ένα πληροφοριακό σύστημα από την προσβολή ιών, αναλαμβάνοντας τον έλεγχο της μνήμης, των αρχείων και των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου, για τυχόν σημάδια προσβολής. Τα συστήματα αυτά, προκειμένου να είναι αποτελεσματικά, θα πρέπει να προγραμματίζονται με τέτοιο τρόπο, ώστε να εκτελείται αυτόματα ο έλεγχος για ανίχνευση ιών κατά την έναρξη, χωρίς να δύναται να προσπεράσει τη διαδικασία αυτή ο εκάστοτε χρήστης (Furnell, 2006, p.356). Μειονέκτημά τους συνιστά το γεγονός ότι προστατεύουν ένα σύστημα μονάχα από ιούς που έχουν ήδη εντοπιστεί και έχει ανακαλυφθεί τρόπος «θεραπείας», αφήνοντας το σύστημα εκτεθειμένο απέναντι σε νέους ιούς. Ωστόσο, εκτιμάται από ειδικούς ότι σύντομα θα είναι δυνατός ο εντοπισμός και η κινητοποίηση ενάντια σε κάθε τύπο κυβερνοεπίθεσης, μέσω των Συστημάτων Ηλεκτρονικής Ανοσίας (Electronic Immunity Systems) (Λάζος, 2001, σελ.226).

στ) συστήματα αντιμετώπισης κατά των κακόβουλων λογισμικών (anti-malware)

Παραδοσιακά, οι επιχειρήσεις χρησιμοποιούν συστήματα αντιμετώπισης κατά των ιών, ωστόσο θεωρούνται πια ανεπαρκή (Ransomware New Generation, 2021). Προτείνεται λοιπόν η ύπαρξη πιο εξελιγμένων εργαλείων, όπως είναι τα συστήματα αντιμετώπισης κατά των κακόβουλων λογισμικών. Τα συστήματα αυτά, αποτελούν λογισμικά προγράμματα που στηρίζονται σε τεχνικές παρακολούθησης και αποκλεισμού της κυκλοφορίας του δικτύου. Πιο συγκεκριμένα, σκανάρουν ένα πληροφοριακό σύστημα με σκοπό να εμποδίσουν, να ανιχνεύσουν και να απομακρύνουν ένα κακόβουλο λογισμικό (Morales et al., 2010).

ζ) διατήρηση αντιγράφων ασφαλείας (backups)

Η διατήρηση αντιγράφων ασφαλείας είναι μία πρακτική η οποία πρέπει να ακολουθείται από όλες τις επιχειρήσεις. Η πρακτική αυτή συνδράμει στην ανάκτηση αρχείων και λοιπών κρίσιμων πόρων, οι οποίοι ενδεχομένως να έχουν καταστραφεί είτε από παράνομους εισβολείς, είτε από κακόβουλα λογισμικά. Για παράδειγμα στις περιπτώσεις επιθέσεων ransomware, τα αντίγραφα ασφαλείας δίνουν τη δυνατότητα πρόσβασης σε δεδομένα και αρχεία που ενδεχομένως να έχουν κρυπτογραφηθεί ένεκα της επίθεσης αυτής, και για το λόγο αυτό έχουν εξαιρετική αξία για το πληροφοριακό σύστημα.

Τα αντίγραφα ασφαλείας θα πρέπει να δημιουργούνται σε τακτική βάση και κατά προτίμηση σε συχνότητα ανάλογη της έκτασης και του τύπου της επιχείρησης. Παράλληλα, θα πρέπει να εξασφαλίζεται η ανθεκτικότητα και η καθαρότητά τους από κακόβουλα λογισμικά. Επίσης, θα πρέπει να επανεξετάζεται η διάρκεια διατήρησής τους, και αυτό γιατί οι επιθέσεις ransomware για παράδειγμα, χρησιμοποιούν συχνά καθυστερήσεις χρόνου για να στοχεύσουν φαινομενικά καθαρά συστήματα (Ransomware New Generation, 2021). Οι δε ιθύνοντες της εκάστοτε επιχείρησης, οφείλουν να ενημερώνονται για τη διαδικασία ανάκτησης αρχείων από τα αντίγραφα αυτά.

Πολλές φορές, η πρακτική των αντιγράφων ασφαλείας αποτελεί φύλακα μιας επιχείρησης ενάντια και σε έτερες απειλές όπως είναι για παράδειγμα οι φυσικές καταστροφές (π.χ. φωτιά, πλημμύρα) και λοιποί αστάθμητοι παράγοντες που μπορούν να προκαλέσουν βλάβη των πληροφοριακών συστημάτων. Σήμερα, η πρακτική αυτή

ναι μεν μπορεί να σώσει εν μέρει την επιχείρηση, ωστόσο αυτό δεν σημαίνει ότι τα αρχεία θα επανέλθουν πλήρως στην αρχική τους κατάσταση και ότι οι δραστηριότητες θα συνεχιστούν κατά τον ίδιο τρόπο που λάμβαναν χώρα και πριν. Συνεπώς η πρακτική αυτή δεν βρίσκεται στις πρώτες θέσεις των προληπτικών μέτρων που θα πρέπει να ληφθούν (Furnell, 2006, pp.355-356).

η) κρυπτογράφηση (encryption)

Η κρυπτογράφηση αποτελεί μία από τις πιο σύγχρονες μεθόδους προστασίας των δεδομένων και των προγραμμάτων. Η χρησιμότητά της αυτή προκύπτει λόγω των παρακάτω ιδιοτήτων της:

i. αρτιότητα (integrity), όπου εξασφαλίζει ότι το περιεχόμενο των δεδομένων δεν έχει αλλοιωθεί, μέσω της συμβολής της επισυναπτόμενης ψηφιακής υπογραφής,

ii. εμπιστευτικότητα (confidentiality), αφού επιτυγχάνει την αδυναμία πρόσβασης των πιθανών δραστών στα κρυπτογραφημένα δεδομένα,

iii. εξακρίβωση (authentication), όπου βεβαιώνει την ταυτοπροσωπία του αποστολέα των δεδομένων από το νόμιμο αποδέκτη, μέσω της ψηφιακής υπογραφής του τελευταίου και

iv. μη αποκυρηξιμότητα (non-repudiation), όπου εξασφαλίζει ότι ο συντάκτης των πληροφοριών/δεδομένων, δεν δύναται να αρνηθεί ψευδώς τη σύνταξη αλλά και την αποστολή τους.

Αξίζει να σημειωθεί ότι η κρυπτογράφηση αποτελεί συνάμα ισχυρό όπλο και των εγκληματιών. Χαρακτηριστικό παράδειγμα αποτελεί μία υπόθεση κατασκοπείας στην Ιαπωνία. Στη συγκεκριμένη περίπτωση εξαπολύθηκε ένας ιός ο οποίος υπέκλεψε κωδικούς χρηστών και πρόσβασης από ένα δίκτυο, εν συνεχεία τους κωδικοποίησε και τους τοποθέτησε σε ένα αρχείο. Ακολούθως ο ιός εξουδετερώθηκε με την ανεύρεσή του, το αρχείο όμως με τα κωδικοποιημένα δεδομένα παρέμεινε κρυφό. Τα δεδομένα αυτά όμως, θα παρέμεναν κρυφά ακόμη και σε περίπτωση ανεύρεσης του αρχείου, ένεκα της κρυπτογράφησής τους από τον ιό (Λάζος, 2001, σσ.227-229).

θ) ευταξία του πληροφοριακού συστήματος της επιχείρησης

Η ευταξία του πληροφοριακού συστήματος της επιχείρησης, όσο περίεργο και αν φαίνεται, συνιστά ένα ισχυρό αμυντικό μέσο ενάντια στις παρεισδύσεις. Επιτυγχάνεται μέσω ειδικών προγραμμάτων λογισμικού ή μέσω της ευσυνείδητης

διοίκησης, η οποία κατοχυρώνεται με τη συνεχή εποπτεία και τις παρεμβάσεις όπου αυτό κρίνεται αναγκαίο. Ειδικότερα, η νοικοκυροσύνη (housekeeping) αυτή σημαίνει:

i. οργάνωση ενός προσηλωμένου συστήματος διοίκησης,
ii. ενημερωμένη λίστα με όλους τους ισχύοντες λογαριασμούς,
iii. αποσύνδεση από τους αδρανείς λογαριασμούς και
iv. ελάττωση των χρηστών με προνομιακές δυνατότητες πρόσβασης (Λάζος, 2001, σελ.225).

ι) επιμόρφωση, εκπαίδευση και ενημέρωση

Η επιμόρφωση και η εκπαίδευση του προσωπικού μιας επιχείρησης πάνω σε ζητήματα κυβερνοασφάλειας, σε συνδυασμό με την ηθική χρήση της Τεχνολογίας Πληροφοριών και Επικοινωνίας (Τ.Π.Ε.), αποτελούν από τα πιο σημαντικά μέτρα που μπορούν να συμβάλουν στην πρόληψη κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων (Λάζος, 2001, σσ.229-231). Ζωτικής σημασίας είναι συνάμα και η ενημέρωση αναφορικά με τις εξελίξεις στον τομέα των κυβερνοεπιθέσεων, τις νέες τακτικές των δραστών καθώς επίσης και την κείμενη νομοθεσία, προκειμένου αφενός να βρίσκονται οι υπάλληλοι των επιχειρήσεων ένα βήμα μπροστά από τους κυβερνοεγκληματίες και αφετέρου να μην παραβαίνουν ακούσια τους κανόνες. Πρέπει να σημειωθεί ότι μολονότι τα μαθήματα επαγγελματικής κατάρτισης από την πλευρά της επιχείρησης κοστίζουν αρκετά, είναι προτιμότερο το προβλέψιμο κόστος τους από το απρόβλεπτο κόστος που μπορεί να επιφέρει μία κυβερνοεπίθεση σε βάρος της επιχείρησης (Furnell, 2006, pp.357-358).

ια) λοιπά προληπτικά μέτρα μέσω της διαχείρισης και υποστήριξης του πληροφοριακού συστήματος

Πέραν των προαναφερόμενων ενδεικτικών και όχι εξαντλητικών προληπτικών μέτρων, οι ιθύνοντες για την ασφάλεια μιας επιχείρησης, θα πρέπει να μεριμνούν για τα κάτωθι:

i. εγκατάσταση προγραμμάτων με τις αντίστοιχες τελευταίες ενημερώσεις π.χ. ενημερωμένα αντι-ιικά προγράμματα,
ii. εξακρίβωση ότι οι μέθοδοι ασφαλείας και τα προγράμματα προστασίας είναι ενεργά και διαρκής έλεγχος της αποτελεσματικότητάς αυτών,

iii. διαχωρισμός των συστημάτων που παρέχουν δεδομένα προσβάσιμα σε όλο το ευρύ κοινό μέσω του κυβερνοχώρου, από εκείνα που εμπεριέχουν ευαίσθητα προσωπικά δεδομένα και
iv. απαγορεύσεις στην πρόσβαση στο διαδίκτυο, με σκοπό την αποφυγή της πρόσβασης σε αυτό άνευ αδείας, από οποιονδήποτε εισέρχεται εντός της επιχείρησης (Furnell, 2006, p.359).

Παράλληλα με τις επιχειρήσεις, οι υπάλληλοι αυτών οφείλουν να λαμβάνουν από τη δική τους πλευρά προληπτικά μέτρα. Ενδεικτικά, ορισμένα από τα μέτρα αυτά είναι:

α) η οικειοθελή επιδίωξη για τη συμμετοχή τους σε εκπαιδεύσεις, ώστε να είναι καταρτισμένοι σε ότι αφορά το ζήτημα των κυβερνοεπιθέσεων και πλήρως ενημερωμένοι για την επικαιρότητα και τις εξελίξεις,

β) η απευθείας ενημέρωση των υπευθύνων σε περίπτωση που διαπιστώσουν το παραμικρό το οποίο μπορεί να υποδηλώνει παραβίαση του συστήματος, ή σε περίπτωση που εντοπίσουν κάποιο πρόγραμμα που πιθανόν να μη λειτουργεί ή να μην έχει ενημερωθεί,

γ) η πιστή συμμόρφωση στις οδηγίες που παρατέθηκαν παραπάνω αναφορικά με τους κωδικούς πρόσβασης των προσωπικών λογαριασμών τους στο σύστημα,

δ) η ιδιαίτερη προσοχή απέναντι σε εισερχόμενα μηνύματα ηλεκτρονικής αλληλογραφίας που λαμβάνουν και η αποφυγή ανταπόκρισης σε εκείνα που δεν γνωρίζουν με ασφάλεια τον αποστολέα τους και σε εκείνα που ζητούν προσωπικές πληροφορίες,

ε) η απαγόρευση εισόδου σε δόλιες ιστοσελίδες που χρησιμοποιούνται για την κλοπή προσωπικών δεδομένων και

στ) η υποχρεωτική αποσύνδεση από τους λογαριασμούς τους, ειδικά αν έχουν συνδεθεί από κοινόχρηστο υπολογιστή (Sousa, 2019). Σε όλα τα μέτρα αυτά, καθοριστικό ρόλο παίζει η ακεραιότητα χαρακτήρα του εκάστοτε υπαλλήλου, ώστε να μεριμνήσει για όλα αυτά και να μην εκμεταλλευτεί με δόλιο τρόπο τυχόν τρωτά σημεία προς όφελός του.

Όλα τα παραπάνω μέτρα που προτείνονται, μπορεί να συμβάλουν στην πρόληψη των κυβερνοεπιθέσεων που λαμβάνουν χώρα εις βάρος των επιχειρήσεων, όμως θα πρέπει να μη λησμονούμε ότι η πρόληψη δεν δύναται να επιτευχθεί σε ποσοστό 100%. Το να επιδιώκεις την πρόληψη και κατ' επέκταση την ασφάλεια,

είναι σαν να προσπαθείς να πετύχεις έναν κινούμενο στόχο. Ωστόσο, πάντοτε θα υπάρχει περιθώριο βελτίωσης μέσα από καλές πρακτικές και συνετούς τρόπους συντήρησης.

4. Σχέδιο αντιμετώπισης κυβερνοεπιθέσεων σε βάρος επιχειρήσεων

Η καλή προετοιμασία μέσω των προαναφερθέντων προληπτικών μέτρων κατά το στάδιο της πρόληψης, συνιστά τη βάση για την αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, όποιος και αν είναι ο τύπος της απειλής. Ωστόσο, προτού καταλήξουμε στο στάδιο της αντίδρασης για την αντιμετώπιση των υπό εξέλιξη κυβερνοεπιθέσεων και την αποκατάσταση των πόρων που έχουν υποστεί ζημία, προηγείται η διαδικασία αναζήτησης και εντοπισμού ιχνών προκειμένου να εξιχνιαστεί οποιοδήποτε περιστατικό και να καταγραφούν οι όποιες συνέπειες (Μαυρίδης, 2015, σσ.16-17).

Τα ιδιαίτερα χαρακτηριστικά γνωρίσματα των κυβερνοεπιθέσεων γενικά και τα μέτρα προστασίας που λαμβάνουν οι δράστες, καθιστούν δύσκολη τη διερεύνηση και εξιχνίαση, καθώς οι δράστες αφήνουν πίσω τους μονάχα ψηφιακά ίχνη, των οποίων η ανίχνευση απαιτεί εξειδικευμένη τεχνογνωσία και χρήση εξελιγμένης τεχνολογίας (Σφακιανάκης, 2016,σσ. 21-23). Τα ψηφιακά αυτά ίχνη, τα οποία συμβάλλουν στην εξιχνίαση, είναι δυνατό να εντοπίζονται:

α) στο μέσο πρόσβασης του παραβάτη, αφού με εξειδικευμένες τεχνικές αποκαλύπτονται αρχεία και στοιχεία κρυφά ή αόρατα με γυμνό μάτι, όπως η ημερομηνία, η ώρα και η διάρκεια περιήγησης, οι ιστοσελίδες που επισκέφθηκε, τα άτομα που συνομίλησε κ.λπ.,

β) στις συσκευές που χρησιμοποιούνται βοηθητικά και παράλληλα, όπως κινητά τηλέφωνα, ψηφιακές κάμερες, φωτογραφικές μηχανές, κ.λπ., και τέλος

γ) στους παρόχους διαδικτυακών υπηρεσιών και στις μηχανές διαδικτυακής αναζήτησης, που δίνουν πληροφορίες και με τη βοήθεια των οποίων καθίσταται δυνατός ο εντοπισμός δραστών μέσω του μοναδικού ψηφιακού αριθμού ταυτότητας (IP) (Servida et al., 2019).

Εφόσον λοιπόν εντοπιστούν ίχνη παραβίασης, ξεκινάει το στάδιο της αντίδρασης, δηλαδή της αντιμετώπισης. Η έννοια της αντιμετώπισης, περιλαμβάνει στην ουσία τη μεθοδολογία που χρησιμοποιεί μία επιχείρηση όπως για παράδειγμα τα σχέδια, τις μεθόδους και τα εργαλεία, προκειμένου να αντιμετωπίσει επιτυχώς μία

κυβερνοεπίθεση αξιοποιώντας αποτελεσματικά τους διαθέσιμους πόρους της, να ελαχιστοποιήσει τις πιθανές επιπτώσεις σε βάρος της, να αυξήσει την εμπιστοσύνη των πελατών και των μετόχων της, να ικανοποιήσει τις νομικές υποχρεώσεις που προκύπτουν ένεκα του Γ.Κ.Π.Δ. και να προασπίσει τη φήμη της. Η προαναφερόμενη μεθοδολογία εκδηλώνεται μέσω της ανάπτυξης ενός σχεδίου (Αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας, 2019).

Το σχέδιο αυτό, γνωστό ως σχέδιο αντιμετώπισης κυβερνοεπιθέσεων, αφού ορίσει τι συνιστά απειλή για την εκάστοτε επιχείρηση, παρέχει σαφείς και λεπτομερείς οδηγίες αναφορικά με τη διαδικασία που πρέπει να ακολουθηθεί, προσδιορίζει ομάδες, προσδίδει ρόλους, κ.λπ.. Πιο συγκεκριμένα περιλαμβάνει τα εξής στάδια (Αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας, 2019):

α) **στάδιο προετοιμασίας**

Το στάδιο αυτό συνιστά την κινητήρια δύναμη του σχεδίου αντιμετώπισης κυβερνοεπιθέσεων. Όπως προκύπτει και από την ονομασία του, εδώ τοποθετούνται οι βάσεις και προετοιμάζονται τα θεμέλια για την εξασφάλιση μιας ασφαλούς επιχείρησης. Οι βάσεις αυτές και τα θεμέλια χτίζονται μέσω της ανάπτυξης πολιτικών και διαδικασιών που θα πρέπει να ακολουθούνται σε περίπτωση κυβερνοεπίθεσης. Σημαντική είναι επίσης και η ακριβής σύνθεση μιας ομάδας αντιμετώπισης που θα προβεί στις προαναφερόμενες πολιτικές και διαδικασίες. Ακολούθως, στο στάδιο αυτό αναπτύσσονται σενάρια αντιμετώπισης περιστατικών και σχετικές ασκήσεις προκειμένου να αξιολογηθεί το σχέδιο αντιμετώπισης κυβερνοεπιθέσεων. Τέλος, για να αυξηθούν οι πιθανότητες επιτυχίας του σταδίου αυτού και να επιτευχθούν τα επιθυμητά αποτελέσματα, το κάθε μέλος της επιχείρησης οφείλει να εκπαιδεύεται σε ότι έχει να κάνει με το ρόλο και τις ευθύνες του. Με τον τρόπο αυτό εξασφαλίζεται ότι η αντίδρασή του σε ένα περιστατικό κυβερνοεπίθεσης θα είναι αντίστοιχη με αυτή που εκδήλωνε στο πλαίσιο της εκπαίδευσής του.

β) **στάδιο αναγνώρισης**

Στο δεύτερο στάδιο εμπίπτει η διαδικασία εντοπισμού και αναγνώρισης μιας κυβερνοεπίθεσης, μέσω διαφόρων πρακτικών ή μηχανισμών που αναφέρθηκαν παραπάνω, όπως τα τείχη προστασίας, τα Συστήματα Ανίχνευσης Εισβολών, κ.λπ.. Ειδικότερα, στο στάδιο αυτό θα πρέπει να καταγράφεται ο χρόνος που λαμβάνει χώρα η κυβερνοεπίθεση, ο τρόπος εντοπισμού της και το πρόσωπο που την ανακαλύπτει. Παράλληλα, θα πρέπει να προσδιορίζεται το εύρος της

κυβερνοεπίθεσης και πιο συγκεκριμένα να καταγράφονται τα συστήματα της επιχείρησης που παραβιάστηκαν, σε ποιο βαθμό επηρεάστηκαν και αν τελικά εκδηλώθηκε μεγάλη ζημία στο σύνολο της λειτουργίας της επιχείρησης.

γ) **στάδιο περιορισμού**

Αμέσως μετά την αναγνώριση μιας κυβερνοεπίθεσης, στόχος είναι ο περιορισμός αφενός της περαιτέρω διείσδυσης στην επιχείρηση και αφετέρου της ζημίας που ενδεχομένως να προκληθεί. Αυτό επιτυγχάνεται μέσω στρατηγικών όπως η αποσύνδεση των επηρεαζόμενων συστημάτων από το δίκτυο ή η χρήση εφεδρικών συστημάτων για την επαναφορά των επιχειρησιακών λειτουργιών. Σε καμία περίπτωση δεν ενδείκνυται η άμεση επαναφορά των συστημάτων στην πρότερη κατάσταση, καθώς μια τέτοια κίνηση ενδεχομένως να καταστρέψει τα πολύτιμα ψηφιακά ίχνη που μπορούν είτε να αποκαλύψουν το δράστη, είτε να συμβάλουν στη δημιουργία ενός σχεδίου για την αποφυγή μελλοντικών παρόμοιων περιστατικών (Wiggins, 2002).

δ) **στάδιο εξάλειψης**

Εφόσον έχει προηγηθεί ο περιορισμός όπως προσδιορίστηκε στο προηγούμενο εδάφιο, γίνονται προσπάθειες για την εξουδετέρωση των απειλών και την επαναφορά του πληροφοριακού συστήματος της επιχείρησης, όσο το δυνατόν πλησιέστερα, στην πρότερη κατάστασή του. Στο στάδιο αυτό δηλαδή συμπεριλαμβάνεται η ασφαλής απομάκρυνση κακόβουλων προγραμμάτων, η επιδιόρθωση συστημάτων, η εφαρμογή ενημερώσεων και πολλές φορές η παρακολούθηση προκειμένου να διαπιστωθεί αν το πληροφοριακό σύστημα είναι ευάλωτο σε μελλοντική επίθεση.

ε) **στάδιο ανάκτησης**

Στο στάδιο της ανάκτησης λαμβάνει χώρα η διαδικασία της τελικής αποκατάστασης και επαναφοράς των συστημάτων που έχουν παραβιαστεί. Αυτό γίνεται μόνο εφόσον έχει εξασφαλιστεί το προηγούμενο στάδιο της εξάλειψης, δηλαδή να έχει εξακριβωθεί ότι δεν κινδυνεύουν τα επηρεαζόμενα συστήματα και μπορούν να επιστρέψουν σε λειτουργία και σε περιβάλλον παραγωγής, παρακολουθώντας ταυτόχρονα για τυχόν μη φυσιολογικές δραστηριότητες και δυσλειτουργίες. Επιπρόσθετα, στο στάδιο αυτό εκτιμώνται οι ζημίες και υπολογίζεται το κόστος που έχει προκληθεί από την κυβερνοεπίθεση.

στ) **στάδιο καταγραφής διδαγμάτων**

Το τελευταίο στάδιο είναι αυτό της καταγραφής διδαγμάτων και αποτελεί ένα στάδιο το οποίο παρά το γεγονός ότι είναι εξαιρετικά σημαντικό, συχνά παραλείπεται. Στο στάδιο αυτό εκτιμάται η κατάσταση που επικρατεί στην επιχείρηση μετά από μία επίθεση, αξιολογούνται οι αποφάσεις που ελήφθησαν κατά τη διάρκεια της επίθεσης αυτής, καταγράφονται όσες από αυτές τις αποφάσεις λειτούργησαν επιτυχώς καθώς και όσες παραλείψεις διαπιστώθηκαν. Ακολούθως, συντάσσεται μία έκθεση η οποία περιλαμβάνει όλα τα τρωτά σημεία και στοιχεία που επέτρεψαν την επίθεση, όλα τα μέτρα που πρέπει να ληφθούν για την αποφυγή παρόμοιων περιστατικών στο μέλλον και όλες τις απαιτούμενες τροποποιήσεις που απαιτούνται σε σχετικές διαδικασίες και στην εκπαίδευση των εργαζόμενων. Η έκθεση αυτή χρησιμοποιείται για μελλοντική κατάρτιση και στην πραγματικότητα αποτελεί ένα δίδαγμα.

Για να είναι αποτελεσματικό ένα σχέδιο αντιμετώπισης κυβερνοεπιθέσεων, εκτός των προαναφερόμενων σταδίων, θα πρέπει να λαμβάνονται υπόψη και άλλοι παράμετροι. Αρχικά λοιπόν, θα πρέπει να προσδιορίζονται οι πόροι μιας επιχείρησης που είναι δυνατό να επηρεάσουν τη λειτουργία της ένεκα μιας κυβερνοεπίθεσης, δηλαδή τα συστήματα, τα πρόσωπα, οι διαδικασίες, και να τίθενται σε μία προτεραιότητα με βάση τον κίνδυνο που διατρέχουν και τη σημασία που έχουν για τη γενικότερη λειτουργία της επιχείρησης. Εν συνεχεία επιβάλλεται ένας προσδιορισμός δυνητικών κινδύνων (π.χ. από μηνύματα ηλεκτρονικού ταχυδρομείου) και ενδεδειγμένων διαδικασιών που θα πρέπει να ακολουθούνται ανάλογα με τον κίνδυνο. Οι διαδικασίες αυτές (π.χ. τακτική αμυντικής προσέγγισης), περιορίζουν τις πιθανότητες για έναν υπάλληλο να προβεί σε λανθασμένες ενέργειες πάνω στον πανικό του, οι οποίες ενδεχομένως να αποβούν εξαιρετικά δαπανηρές για την επιχείρηση. Επιπλέον, προκειμένου να συντονιστεί η όλη διαδικασία για την αντιμετώπιση μιας κυβερνοεπίθεσης, απαραίτητος είναι και ο ορισμός μιας ομάδας αντιμετώπισης που θα συμβάλλει στην ελαχιστοποίηση των επιπτώσεων και την άμεση αποκατάσταση αυτών. Παράλληλα, εξίσου σημαντικό για να ευδοκιμήσει το σχέδιο αντιμετώπισης, είναι η υποστήριξη από τη διοίκηση. Η υποστήριξη αυτή, η οποία συνήθως αφορά την εξασφάλιση της αναγκαίας χρηματοδότησης για τη δημιουργία, την άσκηση και την εκτέλεση του σχεδίου, κερδίζεται μέσω της παρουσίασης των στόχων και των πλεονεκτημάτων με τον καλύτερο δυνατό τρόπο (Αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας, 2019).

Το σχέδιο αντιμετώπισης που αναπτύχθηκε παραπάνω μαζί και με τις λοιπές παραμέτρους που αναφέρθηκαν συνιστούν έναν αναγκαίο σχεδιασμό, όμως δεν θα πρέπει να περιοριστούμε μονάχα σε αυτόν. Απαιτείται η προετοιμασία και η εξάσκηση του προσωπικού ως προς τον τρόπο αντίδρασής τους σε ενδεχόμενο περιστατικό κυβερνοεπίθεσης, καθώς επίσης και η διαρκής ενημέρωση και βελτίωση των σχεδίων, χωρίς να παραμένουν στο ράφι μέχρι τη στιγμή που θα χρειαστεί να υλοποιηθούν (Αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας, 2019).

Τέλος, σημειώνεται ότι στο πλαίσιο της αντιμετώπισης, καθοριστικός είναι και ο ρόλος των αρχών. Οι αρχές, θα πρέπει να ενημερώνονται για τις τεχνολογικές εξελίξεις και μέσα από τη χρήση νέων τεχνολογιών, κατάλληλων ανακριτικών και μη διαδικασιών, καθώς και από την ανταλλαγή πληροφοριών με άλλους φορείς και με την ίδια την επιχείρηση, να ανακαλύπτουν αποδεικτικά στοιχεία που συμβάλλουν στη δίωξη των κυβερνοεπιθέσεων. Μόνο μέσα από τη συνεργασία των αρχών, των κυβερνητικών φορέων και των επιχειρήσεων ανοίγει η πόρτα για την αποτελεσματικότερη επίλυση του προβλήματος και τις αποδοτικότερες πιθανές λύσεις (Wiggins, 2002).

5. Δυσχέρειες στον εντοπισμό και τη δίωξη των κυβερνοεπιθέσεων

Μπορεί να έχουν προβλεφθεί τα διάφορα στάδια ενός σχεδίου αντιμετώπισης, ωστόσο ο εντοπισμός και η ποινική δίωξη των περιστατικών κυβερνοεπίθεσης δεν είναι μία εύκολη διαδικασία. Ως εκ τούτου, ο κοινωνικός έλεγχος ως εργαλείο προσαρμογής σε διαφορετικές αξίες και κανόνες που ορίζονται από την κοινωνία, δεν οδηγεί πάντοτε στην πρόληψη του εγκλήματος μέσα από στρατηγικές και μέτρα που λαμβάνονται στο πλαίσιο αντεγκληματικής πολιτικής, αλλά ούτε και στην καταστολή μέσα από την εφαρμογή της κείμενης νομοθεσίας από τους αρμόδιους μηχανισμούς (Χάϊδου, 2003, σελ. 95 ; Φαρσεδάκης, 2016, σελ.169). Με άλλα λόγια οι διωκτικές αρχές, τόσο οι αστυνομικές όσο και οι δικαστικές, αντιμετωπίζουν αρκετές δυσκολίες κατά τη δράση τους, ασκώντας τον τυπικό κοινωνικό έλεγχο. Οι δυσκολίες αυτές και ο επερχόμενος ανεπιτυχής, ορισμένες φορές, κοινωνικός έλεγχος, οφείλονται κατά βάση στο γεγονός ότι οι αποδείξεις ανιχνεύονται δύσκολα και τα ψηφιακά ίχνη εξαφανίζονται εύκολα, όπως έχει αναφερθεί και σε προηγούμενο υποκεφάλαιο (Λάζος, 2001, σελ.211).

Οι δυσκολίες στον εντοπισμό και τη δίωξη των κυβερνοεπιθέσεων, οφείλονται και σε προβλήματα νομοθεσίας. Η γρήγορη εξέλιξη της τεχνολογίας καθιστά πολλές φορές αδύνατο για τη νομοθεσία να την προφτάσει, με αποτέλεσμα να εμφανίζονται δυσχέρειες κατά τη νομική αντιμετώπιση. Για το λόγο αυτό, οι νομοθέτες πρέπει να μεριμνούν για τη γεφύρωση του χάσματος ανάμεσα στην τεχνολογία και το νόμο. Πρέπει να σημειωθεί όμως, ότι ακόμη και να επιτευχθεί αυτό, οι περισσότερες επιχειρήσεις, από τη μία αποφεύγουν να καταγγείλουν τις κυβερνοεπιθέσεις και από την άλλη πολλές φορές καταφεύγουν να προσλαμβάνουν στο προσωπικό τους αυτούς που κατόρθωσαν να παραβιάσουν το σύστημα ασφαλείας τους. Στις πράξεις αυτές προβαίνουν αφενός προς διαφύλαξη της φήμης τους, αφετέρου προς αποφυγή των δυσβάσταχτων δικαστικών εξόδων και της παραπομπής σε δίκη, της οποίας η έκβαση είναι αμφίβολη, ένεκα νομοθεσίας (Λάζος, 2001, σελ.212).

Αναφορικά με το νομοθετικό πλαίσιο, προκύπτουν δυσχέρειες και σε ότι αφορά την εφαρμογή του. Συγκεκριμένα, κατά την προσέγγιση νομικών θεμάτων που αφορούν τον κυβερνοχώρο, απαιτούνται εξειδικευμένες γνώσεις τόσο σε νομικό όσο και σε τεχνικό επίπεδο. Το γεγονός αυτό αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε κράτους καθώς ελάχιστοι νομικοί τις διαθέτουν. Το πρόβλημα βέβαια δεν έγκειται μονάχα σε ότι αφορά τους νομικούς, αλλά επεκτείνεται στο σύνολο των διωκτικών αρχών (αστυνομία, δικαστές, εισαγγελείς, ελεγκτές της δημόσιας διοίκησης), όπου δεν διαθέτουν την απαιτούμενη κατάρτιση και εξοικείωση με την πληροφορική τεχνολογία (Λάζος, 2001, σελ.213). Για παράδειγμα, πολλές φορές λόγω έλλειψης εκπαίδευσης πάνω στο κυβερνοέγκλημα και τη νοοτροπία αυτού, δικαστές ερμηνεύουν ποινικούς νόμους με βάση τις παραδοσιακές νομικές συντεταγμένες, εισαγγελείς καθίστανται αναρμόδιοι στο χειρισμό υποθέσεων που πραγματεύονται τέτοιου είδους εγκλήματα, ενώ αστυνομικοί αδυνατούν να αξιοποιήσουν αποτελεσματικά ένα ένταλμα έρευνας, καθώς δεν γνωρίζουν πως να ανακαλύψουν αποδεικτικά στοιχεία/ψηφιακά ίχνη. Βέβαια, κάτι τέτοιο είναι ως ένα βαθμό αναμενόμενο, καθώς όσοι μεγάλωσαν χωρίς την ανάπτυξη, και πόσο μάλλον την ύπαρξη, του κυβερνοχώρου, δυσκολεύονται στην απόκτηση της απαραίτητης γνώσης. Ευτυχώς όμως πρόκειται για κάτι που βελτιώνεται, δεδομένου ότι οι σύγχρονες διωκτικές αρχές έχουν εξελιχθεί σε αρκετά υψηλό βαθμό. Θα πρέπει ωστόσο να εξελίσσονται διαρκώς για να κατορθώσουν να συμβαδίζουν στο ίδιο επίπεδο με τους δράστες (Λάζος, 2001, σσ.214-217).

Επιπρόσθετα, η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων λόγω του ότι πρόκειται για μια σχετικά νέα μορφή εγκληματικότητας, σε συνδυασμό με το γεγονός ότι τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι κατά κανόνα διατυπωμένη στην αγγλική γλώσσα και η αντίστοιχη μεταφορά αυτών των όρων σε άλλες γλώσσες (π.χ. ελληνικά) δεν είναι ούτε εύκολη αλλά ούτε και δόκιμη, προκαλούν δυσκολία σε αυτόν που ασχολείται με τη νομική πλευρά του θέματος από ποινική άποψη.

Μία άλλη δυσκολία προκύπτει εξαιτίας του διεθνή χαρακτήρα των κυβερνοεπιθέσεων. Οι κυβερνοεπιθέσεις δεν έχουν σύνορα, δεν γνωρίζουν γεωγραφικούς περιορισμούς και τις περισσότερες φορές διαρκούν ελάχιστα μόνο δευτερόλεπτα, όπως για παράδειγμα στις οικονομικές απάτες που συμβαίνουν συχνά σε βάρος των επιχειρήσεων, όπου η μεταβίβαση ενός ποσού από ένα λογαριασμό σε άλλο, γίνεται με μόνο ένα πάτημα που διαρκεί κλάσματα του δευτερολέπτου. Δεν απαιτείται δηλαδή η ύπαρξη κάποιου έμψυχου υλικού, όπως για παράδειγμα ένα όχημα μεταφοράς που απαιτείται στην περίπτωση διακίνησης ναρκωτικών, όπου το προϊόν θα πρέπει να μεταφερθεί φυσικά. Το γεγονός αυτό ενώ διευκολύνει τους δράστες να δρουν με ανεξέλεγκτο τρόπο, δημιουργεί πρόβλημα στις διωκτικές αρχές οι οποίες δύσκολα εντοπίζουν αποδεικτικά στοιχεία που θα οδηγήσουν στη δίωξη και κατ' επέκταση στην αντιμετώπιση των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων. Ακόμη και να εντοπιστούν όμως ψηφιακά ίχνη, δεν μπορούν σε καμία περίπτωση να ταυτιστούν με τα παραδοσιακά αποδεικτικά μέσα, γιατί δεν είναι χειροπιαστά, μπορεί κάποιος από μακριά να αλλάξει τη μορφή και το περιεχόμενό τους ή ακόμη και να τα εξαφανίσει με ένα πάτημα. Αντίθετα, οι αποδείξεις ενός εγκλήματος που λαμβάνει χώρα στο φυσικό κόσμο, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο χώρο και χρόνο. Τέλος, ένεκα του διεθνή χαρακτήρα των κυβερνοεπιθέσεων, προκύπτουν επίσης ζητήματα αναφορικά με το ποια χώρα έχει την αρμοδιότητα εκδίκασης της υπόθεσης (Λάζος, 2001, σσ.217-218).

Παράλληλα, υπάρχουν και κάποιες άλλες ιδιαιτερότητες που συμβάλλουν στην ενίσχυση των δυσχερειών ως προς την προσπάθεια εντοπισμού και επιτυχημένης δίωξης των κυβερνοεπιθέσεων. Μια τέτοια ιδιαιτερότητα είναι ο μη οπτικός χαρακτήρας των αποδείξεων, αφού αυτές δεν υπάρχουν συνήθως σε αναγνώσιμη μορφή. Σε αυτό συνδράμει και το γεγονός ότι τροποποιούνται διαρκώς τα προγράμματα ή τα δεδομένα. Άλλη ιδιαιτερότητα αποτελεί η ευχέρεια εξάλειψης

των αποδείξεων και κωδικοποίησης αυτών, αφού οι δράστες, στην προσπάθεια να αποφύγουν ή να δυσκολέψουν την ποινική δίωξη, εξαφανίζουν ψηφιακά ίχνη, κρυπτογραφούν δεδομένα ή θέτουν κωδικούς ασφαλείας, σε αποδεικτικά στοιχεία (Λάζος, 2001, σσ.218-219).

Μέσα από όλες αυτές τις δυσκολίες που προκύπτουν, εύλογα αναρωτιέται κανείς, «πόσο εύκολη καθίσταται, δικονομικά, η ανακάλυψη ενός δράστη που διαπράττει για παράδειγμα διαδικτυακές απάτες σε βάρος επιχειρήσεων, προσβάλλοντας αόριστο αριθμό θυμάτων ανά τον κόσμο και αποκομίζοντας συγχρόνως τεράστια κέρδη;», «τελικά οι κυβερνοεπιθέσεις σε βάρος επιχειρήσεων μπορούν να ελεγχθούν από άποψη ποινικής συμπεριφοράς, λαμβάνοντας υπόψη όλα όσα αναφέρθηκαν;». Τα ερωτήματα αυτά, δυστυχώς μέχρι και σήμερα, είναι δύσκολο να απαντηθούν.

ΕΠΙΛΟΓΟΣ

Με την ολοκλήρωση της παρούσας εργασίας, συνάγεται το συμπέρασμα ότι η είσοδος των επιχειρήσεων στον κυβερνοχώρο επιφέρει αμφιλεγόμενα αποτελέσματα. Από τη μία, διευκολύνει τις ολοένα και αυξανόμενες ανάγκες που επιτάσσει η εξέλιξη της τεχνολογίας. Από την άλλη όμως, δημιουργεί σημαντικούς κινδύνους, αναδεικνύοντας νέες μορφές κυβερνοεπιθέσεων, είτε επικουρώντας τις ήδη υπάρχουσες.

Είτε εσωτερικά είτε εξωτερικά, αθώα ή όχι, τα εταιρικά εγκλήματα λοιπόν, συμβαίνουν σε καθημερινή βάση. Η πρόοδος της τεχνολογίας άλλωστε, έχει δημιουργήσει ένα περιβάλλον στο οποίο οι εγκληματίες θα ήταν αδιανόητο να μην εκμεταλλευτούν τα υπάρχοντα κενά στην εταιρική υποδομή.

Οι κυβερνοεπιθέσεις αυτές αποτελούν ένα πρόβλημα που θα συνεχίσει να υπάρχει και να αυξάνεται στο μέλλον. Θα πρέπει να έχουμε κατά νου άλλωστε, ότι η πρόσβαση σε μια εταιρική βάση δεδομένων, δίνει εκπληκτική δύναμη στον εισβολέα στο να προκαλέσει απίστευτη ζημία, ακόμη και με τη διαγραφή ενός αρχείου ή την τροποποίηση μερικών αριθμών. Αυτή η δύναμη κινητοποιεί τους δράστες στο να προβαίνουν σε ολοένα και περισσότερες κυβερνοεπιθέσεις, και συνάμα προσελκύει διαρκώς άτομα που επιθυμούν να δράσουν κατά τον ίδιο τρόπο. Οι δε συνέπειες των κυβερνοεπιθέσεων είναι σημαντικές, καθώς προκαλούν ζημία κυρίως στον οικονομικό τομέα, αλλά ταυτόχρονα και στην ακεραιότητα των προσωπικών δεδομένων, τη φήμη και τη λειτουργικότητα της εκάστοτε επιχείρησης, και στο σύνολο της οικονομίας γενικότερα. Ωστόσο, συνέπειες υπάρχουν και σε ψυχολογικό επίπεδο, αν λάβουμε υπόψη το παράδειγμα των υπαλλήλων της εταιρείας Sony που δέχθηκαν εκβιασμό.

Διαπιστώνοντας από την εν θέματι εργασία ότι ο ανθρώπινος παράγοντας είναι καταλυτικός στη γένεση κυβερνοεπιθέσεων, ο ίδιος οφείλει να ανακαλύψει τρόπους πρόληψης και εξάλειψης αυτών. Μέχρι και σήμερα έχουν προταθεί πολλά μέτρα ασφαλείας, με σκοπό την πρόληψη και την ενημέρωση των ιθυνόντων για την ασφαλή λειτουργία των πληροφοριακών συστημάτων των επιχειρήσεων. Ωστόσο, τεκμαίρεται ότι, πολλά ακόμη απομένουν να γίνουν για την καταπολέμηση των κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων, ώστε να εξασφαλισθεί η ομαλή λειτουργία τόσο του επιχειρηματικού κόσμου που αναπτύσσει τις δραστηριότητές του στον κυβερνοχώρο, όσο και της κοινωνίας της πληροφορίας. Παράλληλα, πολλά

αναμένονται να γίνουν και όσον αφορά τον τομέα της δίωξης, ο οποίος αντιμετωπίζει πολλές δυσχέρειες, όπως αναπτύχθηκε παραπάνω. Αυτό θα συνδράμει τόσο ως προς την κατεύθυνση της βελτίωσης των υπαρχουσών ρυθμίσεων, όσο και ως προς την ποιοτικότερη διεξαγωγή της ανακριτικής διαδικασίας, μέσω μιας νόμιμης και ταχείας οδού συγκέντρωσης των αποδεικτικών στοιχείων.

Το βασικό μήνυμα της εργασίας αυτής, είναι ότι οι κυβερνοεπιθέσεις γενικότερα και ειδικότερα σε βάρος των επιχειρήσεων, αποτελούν μία ανεπιθύμητη λειτουργία της κοινωνίας της πληροφορίας, την οποία και θα πρέπει να καταπολεμήσουμε. Θα ήταν ουτοπικό βέβαια, να πιστέψει κανείς ότι είναι εφικτή η ολική εξάλειψη του φαινομένου αυτού, καθώς πάντοτε θα εμφανίζονται στοιχεία ανήθικα και καταστροφικά, τα οποία ανακαλύπτει ο ανθρώπινος παράγοντας και οδηγούν στην αποδιοργάνωση. Πέραν του ότι πρέπει να γίνουν ακόμη πολλά σε επίπεδο αντιμετώπισης, παράλληλα θα πρέπει να αλλάξουμε τη συμπεριφορά μας και να δώσουμε σε αυτόν τον τύπο εγκλήματος τη δέουσα προσοχή που του αρμόζει, όπως και με λοιπές παραδοσιακές μορφές εγκλήματος π.χ. ανθρωποκτονία, κλοπή, κ.ά.. Επιπλέον, η αύξηση των περιστατικών κυβερνοεπιθέσεων σε βάρος επιχειρήσεων πρέπει να αντιμετωπιστεί ως αναπόφευκτη, αν λάβουμε υπόψη ότι ο κυβερνοχώρος θα γίνεται, ολοένα και περισσότερο, ένα φυσικό περιβάλλον προσφοράς ευκαιριών εγκλήματος, καθώς η τεχνολογία εξελίσσεται με γοργούς ρυθμούς.

Αναφορικά με τα μέτρα πρόληψης που υπάρχουν μέχρι σήμερα και αναφέρθηκαν στο κεφάλαιο της αντιμετώπισης, θα πρέπει να πούμε ότι μπορούν ήδη να λύσουν πολλά από τα κοινά προβλήματα που επιτρέπουν αυτές τις κυβερνοεπιθέσεις, και μάλιστα με τρόπο αποτελεσματικό. Επιπρόσθετα όμως, πολλά από αυτά βελτιώνονται διαρκώς και αποκτούν περισσότερες ικανότητες στο να περιορίζουν τις μελλοντικές ευκαιρίες των δραστών. Συνεπώς, με την τεχνολογία να είναι διαθέσιμη, οι τρόποι υπάρχουν και εφόσον είναι ήδη τοποθετημένοι σωστά, το πρόβλημα έγκειται πλέον στη στάση και πληροφόρηση των ατόμων που τους αξιοποιούν. Απαιτείται δηλαδή η εκπαίδευση όχι μόνο από πλευράς υπαλλήλων και ιθύνοντων, αλλά και από πλευράς διωκτικών αρχών. Οι αστυνομικές αρχές θα πρέπει να εξοικειωθούν με την τεχνολογία και με τον τρόπο δράσης των εγκληματιών, ώστε να είναι σε θέση να αναγνωρίζουν αρχικά τα χωλά σημεία ενός συστήματος που οδηγούν στην εκάστοτε κυνερνοεπίθεση, και ακολούθως να μπορούν να εντοπίζουν τα ψηφιακά ίχνη των δραστών. Αυτό βέβαια για να υλοποιηθεί, απαιτεί τη

συνεργασία των αρχών με καταρτισμένα άτομα πάνω στον τομέα της πληροφορικής και τεχνολογίας. Προτείνεται δηλαδή η στελέχωση με περισσότερο προσωπικό ειδικών καθηκόντων που θα έχει τις απαραίτητες εξειδικευμένες γνώσεις, το οποίο σε συνεργασία με τις διωκτικές αρχές θα οδηγήσει στην άμεση εξιχνίαση τέτοιου είδους επιθέσεων. Η δε εκπαίδευση απαιτείται και από την πλευρά των δικαστών και εισαγγελέων, ώστε να είναι σε θέση να εκδικάζουν τις υποθέσεις έχοντας όχι μόνο γνώση των στοιχείων της υπόθεσης, αλλά συγχρόνως κατανοώντας πλήρως τον τρόπο δράσης σε κάθε περιστατικό, προκειμένου να είναι σε θέση να αποδώσουν ποινές που θα στηρίζονται στις αρχές της δίκαιης δίκης και της αναλογικότητας. Βέβαια, επισημαίνεται ότι η εκπαίδευση θα πρέπει να ξεκινήσει και σε ατομικό επίπεδο, δεδομένου ότι το μεγαλύτερο ποσοστό του παγκόσμιου πληθυσμού, είναι εκτεθειμένο στους κινδύνους του κυβερνοχώρου. Γνωρίζοντας ο κάθε ένας πως να προασπιστεί σε ατομικό επίπεδο από τις κυβερνοεπιθέσεις, σίγουρα τα ποσοστά κυβερνοεπιθέσεων σε επακόλουθες έρευνες, θα είναι μικρότερης κλίμακας.

Επιπρόσθετα, η συγκεκριμένη εργασία καλλιεργεί το έδαφος προκειμένου να διεξαχθούν περισσότερες έρευνες σε επιχειρήσεις, ιδιαίτερα τώρα που ο Γ.Κ.Π.Δ. τις υποχρεώνει να αναφέρουν κάθε παραβίαση-κίνδυνο σε βάρος τους. Με τον τρόπο αυτό, μειώνεται ο σκοτεινός αριθμός, ο οποίος εμποδίζει όχι μόνο τη γνώση του τρόπου δράσης ορισμένων δραστών, η οποία ενδεχομένως να συμβάλλει στην αποφυγή παρόμοιου μελλοντικού περιστατικού σε έτερη επιχείρηση, αλλά ταυτόχρονα περιορίζει τα διαθέσιμα δεδομένα προκειμένου να διεξαχθούν έρευνες και να συγκεντρωθούν δεδομένα που θα οδηγήσουν σε ποσοτικές και ποιοτικές έρευνες. Σημειώνεται μάλιστα, ότι οι επιχειρήσεις αποκρύπτουν τα περιστατικά κυβερνοεπιθέσεων σε βάρος τους προκειμένου να μη πλήττεται η φήμη τους, γεγονός που δυσχεραίνει τη συγκέντρωση στοιχείων. Το γεγονός αυτό επιβεβαιώνεται και από τις ελληνικές διωκτικές αρχές, και πιο συγκεκριμένα από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της χώρας μας, από όπου και ζητήθηκαν δεδομένα, πλην όμως, η ίδια γνωστοποίησε ότι δεν είναι εφικτή η διάκριση περιστατικών σε μεμονωμένους χρήστες και σε επιχειρήσεις. Ως εκ τούτου, τεκμαίρεται ότι ο Στρατηγικός Σχεδιασμός της Europol, τηρεί στατιστικά ανά τύπο κυβερνοεπίθεσης και όχι με βάση το θύμα (βλ. Παράρτημα Ι).

Επίσης, σε εθνικό επίπεδο, η χώρα μας, βρίσκεται αρκετά πίσω σε σχέση με άλλες χώρες διεθνώς, σε ότι αφορά την αντιμετώπιση περιστατικών κυβερνοεπιθέσεων. Ας ελπίσουμε ότι στο άμεσο μέλλον θα βελτιωθεί η κατάσταση

αυτή, και θα μπορούμε να μελετήσουμε το φαινόμενο αυτό αντλώντας δεδομένα που μέχρι και σήμερα δεν είναι διαθέσιμα για μελέτη και αξιοποίηση.

Η παρούσα εργασία, δίνει το έναυσμα για την επένδυση στον τομέα της κυβερνοασφάλειας. Αν αναλογιστούν οι υπεύθυνοι κάθε επιχείρησης τις επιπτώσεις (οικονομικές, ψυχολογικές, κ.λπ.) που αναφέρθηκαν στην εργασία αυτή, θα είναι απολύτως σίγουροι ότι αξίζει μία μεγάλη οικονομική επένδυση για τη σωστή ρύθμιση και συντήρηση των πληροφοριακών συστημάτων τους, με γνώμονα πάντα την κυβερνοασφάλεια. Ταυτόχρονα, κάθε άλλος, όπως για παράδειγμα οι υπάλληλοι αυτών, θα πρέπει να αναλάβουν το δικό τους μερίδιο ευθύνης, εξασφαλίζοντας ότι οι ενέργειές τους δεν υποβιβάζουν την προστασία και ασφάλεια των πληροφοριακών συστημάτων. Με τον τρόπο αυτό, μπορούμε να είμαστε αισιόδοξοι και να πιστέψουμε ότι η μείωση των ποσοστών κυβερνοεπιθέσεων σε βάρος των επιχειρήσεων είναι ζήτημα χρόνου, δεδομένου ότι είναι απίθανη η πλήρης εξαφάνιση τόσο των απλώς περιέργων εισβολέων που καταφέρνουν να εισέλθουν σε ένα σύστημα χωρίς άδεια προκειμένου να εντοπίσουν ενδιαφέρουσες πληροφορίες, όσο και των εγκληματιών που διασπείρουν καταστροφικούς ιούς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνόγλωσση

Αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας. (2019). *IT Professional Security*, (60). https://www.itsecuritypro.gr/tefchi/teychos-60-maios-ioynios-2019/

Βλαχόπουλος, Κ. (2007). *Ηλεκτρονικό έγκλημα. Μορφές-Πρόληψη-Αντιμετώπιση*. Νομική Βιβλιοθήκη

Δουληγέρης, Χ. & Μητρόπουλος, Σ. (2016). Ηλεκτρονικό Επιχειρείν και Ηλεκτρονικό Εμπόριο. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις

Ευρωπαϊκή Επιτροπή. (2017). *Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στην οποία αξιολογείται κατά πόσον τα κράτη μέλη έχουν λάβει τα αναγκαία μέτρα προκειμένου να συμμορφωθούν με την οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου.* https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A52017DC0474&qid=1668105503472

Ζαραφωνίτου, Χ. (2004). *Εμπειρική Εγκληματολογία*. Νομική Βιβλιοθήκη

Ηλιοπούλου, Φ. (2018). Η σκοτεινή πλευρά του Διαδικτύου: Στα άδυτα των Deep Web και Darknet. Στο: Μ. Σπυριδάκης, Η. Κουτσούκου & Α. Μαρινοπούλου (Επιμ.), *Κοινωνία του Κυβερνοχώρου* (σσ. 425-442). Εκδόσεις Ι. Σιδέρη

Κιούπης, Δ. (1999). *Ποινικό Δίκαιο και Internet*. Εκδόσεις Αντ. Ν. Σάκκουλα

Κοντάκος, Α., Μαργαρώνης, Κ. & Ζαρίφης, Α. (2009). *Αρχές Λογιστικής*. Οργανισμός Εκδόσεως Διδακτικών Βιβλίων

Λάζος, Γρ. (2001). *Πληροφορική & Έγκλημα*. Νομική Βιβλιοθήκη

Μαυρίδης, Ι. (2015). *Ασφάλεια πληροφοριών στο διαδίκτυο*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις

Παρασκευάς, Μ., Ασημακόπουλος, Γ. & Τριανταφύλλου, Β. (2015). *Κοινωνία της Πληροφορίας. Υποδομές, Υπηρεσίες και Επιπτώσεις.* Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών . https://eclass.uth.gr/modules/document/file.php/PRE_P_112/%CE%94%CE%B9%CE%B1%CE%BB%CE%AD%CE%BE%CE%B5%CE%B9%CF%82%20%CE%9C.%CE%A0%CE%B1%CF%81%CE%B1%CF%83%CE%BA%CE%B5%CF%85%CE%AC/05%20-%20%CE%92%CE%B1%CF%83%CE%B9%CE%BA%CF%8C%20%CE%95%CE%BA%CF%80%CE%B1%CE%B9%CE%B4%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CF%8C%20%CE%A5%CE%BB%CE%B9%CE%BA%CF%8C/%CE%A0%CE%91%CE%A1%CE%91%CE%A3%CE%9A%CE%95%CE%A5%CE%91%CE%A3_%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%

CE%BD%CE%AF%CE%B1_%CF%84%CE%B7%CF%82_%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B1%CF%82.pdf

Σφακιανάκης, Ε. (2016). *Ο κώδικας του Διαδικτύου*. All about Internet

Φαρσεδάκης, Ι. (2005). *Στοιχεία Εγκληματολογίας*. Νομική Βιβλιοθήκη

Φαρσεδάκης, Ι. (2009). *Το έγκλημα στον κυβερνοχώρο και η αντιμετώπισή του.* https://criminology.panteion.gr/files/386/j_farsedakis_kybernoxoros.pdf

Φαρσεδάκης, Ι. (2016). Η πρόληψη του εγκλήματος ως μέσον αντεγκληματικής πολιτικής. Στο: Μ. Γασπαρινάτου (Επιμ.), *Έγκλημα και ποινική καταστολή σε εποχή κρίσης. Τιμητικός Τόμος για το καθηγητή Νέστορα Κουράκη*, Α΄ Τόμος (σσ. 169-181). Εκδόσεις Αντ. Ν. Σάκκουλα

Φρυδάς, Ν. (2018). Ο κυβερνοχώρος και η ασφάλειά του. Στο: Μ. Σπυριδάκης, Η. Κουτσούκου & Α. Μαρινοπούλου (Επιμ.), *Κοινωνία του Κυβερνοχώρου* (σσ. 25-72). Εκδόσεις Ι. Σιδέρη

Χάϊδου, Α. (2003). Σύγχρονη τεχνολογία και κοινωνικός έλεγχος. Στο: Α. Χάϊδου, *Εγκληματολογικά Κείμενα. Ανήλικοι - Ναρκωτικά - Κοινωνικός έλεγχος* (σσ. 35-108). Νομική Βιβλιοθήκη

Ξενόγλωσση

Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber attacks and understanding how the propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Alghamdi, M. (2021). History, Present 2021 and Future of Cyber Attacks. *Journal of Cybersecurity and Information Management*, *8*(2), 71-83. https://doi.org/10.54216/JCIM.080204

Alhassan, N.S., Yusuf, M.O., Karmanje, A.R. & Alam, M. (2018). Salami attacks and their mitigation - An overview. In: *Proceedinds of the 5th International Conference on Computing for Sustainable Global Development*, 4639-4632. https://www.academia.edu/36209397/Salami_Attacks_and_their_Mitigation_An_Overview

Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M. & Al-Amri, J. (2019). Four most famous cyber attacks for financial gains. *International Journal of Engineering and Advanced Technology*, *9*(2), 2131-2139. http://dx.doi.org/10.35940/ijeat.B3601.129219

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress

Backhouse, J. & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European journal of information systems, 5*(1), 2-9. https://doi.org/10.1057/ejis.1996.7

Balan, Sh., Otto, J., Minasian, E. & Aryal, A. (2017). Data Analysis of Cybercrimes in Businesses. *Information Technology and Management Science*, *20*(1), 64-68. http://dx.doi.org/10.1515/itms-2017-0011

Barnes, B. & Cieply, M. (2014). Hacking Reality: When Art Imitates Technology. *The York Tmes*, C1-L**.** https://go.gale.com/ps/i.do?id=GALE%7CA394432818&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=03624331&p=AONE&sw=w&userGroupName=anon%7Efc9d59cf

Benedikt, M. (1991). *Cyberspace: First Steps.* MIT Press. https://monoskop.org/images/c/c1/Benedikt_Michael_ed_Cyberspace_First_Steps_1991.pdf

Bhardwaj, A., Anasthi, V., Sastry, H. & Subrahmanyam, G.V.B. (2016). Ransomware digital extortion: a rising new age threat. *Indian Journal of Science and Technology, 9*(14), 1-5. https://doi.org/10.17485/IJST%2F2016%2FV9I14%2F82936

Böhme, R. & Kataria, G. (2006). *Models and Measures for Correlation in Cyber-Insurance.* Workshop on the Economics of Information Security (WEIS). University of Cambridge

Bonner, L, (2012). Cyber risk: How the 2011 Sony data breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Wash. UJL & Pol'y*, *40*, 257-277. https://openscholarship.wustl.edu/law_journal_law_policy/vol40/iss1/7

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B. & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1), 1-20. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2461983

Brockett, P., Golden, L. & Wolman, W. (2012). Enterprise Cyber Risk Management. In: J. Emblemsvåg (Ed.), *Risk Management for the Future-Theory and Case,* 319-342. http://dx.doi.org/10.5772/33646

Business Continuity & Disaster Recovery (2020). *IT Professional Security*, (63). https://www.itsecuritypro.gr/tefchi/teychos-63-ianoyarios-fevroyarios-2020/

Cashell, B., Jackson, W.D., Jickling, M. & Webel, B. (2004). The economic impact of cyber-attacks. *Congressional research service documents. CRS RL32331 (Washington DC), 2.*

Chabinsky, S.R. (2010). The cyber threat: Who's doing what to whom? In: *Government Security/FOSE Conference*. https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Ching, H. L. & Ellis, P. (2004). Marketing in cyberspace: what factors drive e-commerce adoption? *Journal of marketing management, 20*(3-4), 409-429. https://doi.org/10.1362/026725704323080470

Clough, J. (2010). *Principles of cybercrime*. Cambridge University Press

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-24. 10.22215/timreview/835

Cranor, L.F. & LaMacchia, B.A. (1998). Spam!. *Communications of the ACM, 41*(8), 74-83. https://doi.org/10.1145/280324.280336

Cubby, B. & McNeilage, A. (202). Police investigate rioters' text messages. *Sydney Morning Herald*. https://www.smh.com.au/national/nsw/police-investigate-rioters-text-messages-20120916-260mk.html

Das, S. & Nayak. T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering sciences & Emerging Technologies, 6*(2), 142-153. https://doi.org/10.31142/ijtsrd23456

Dasgupta, D., Roy, A. & Nag, A. (2017). Multi-factor authentication. In: *Advances in User Authentication* (pp. 185-233). Springer, Cham.

De Marco, E., Dibari, P. & Scalera, F. (2019). Cyber Risks and Costs for the Company. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *9*(3), 185-191. http://dx.doi.org/10.6007/IJARAFMS/v9-i3/6357

Douligeris, C. & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer networks*, *44*(5), 643-666. https://doi.org/10.1016/j.comnet.2003.10.003

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance, 17*(5), 474-491. 10.1108/JRF-09-2016-0122

Eling, M. & Wirfs, J. H. (2016). *Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class.* Institute of Insurance Economics. https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf

European Communities. (1997). *Building the European Information Society for us all. Final policy report of the high-level expert group*. http://aei.pitt.edu/8692/1/8692.pdf

Europol. (2016). *Internet organised crime threat assessment (IOCTA) 2016*. Europol

Faragallah, O.S., Alzain, M.A., El-Sayed, H.S., … & Soh, B. (2018). Block-based optical color image encryption based on double random phase encoding. *IEEE Access, 7*, 4184-4194. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8528351

Fauntleroy, C., Wagner, R. & Odell, L. (2015). *Cyber Insurance-Managing Cyber Risk*. *Institute for defence analyses*. https://apps.dtic.mil/sti/pdfs/ADA623798.pdf

Franke, U. (2017) The cyber insurance market in Sweden. *Computers & Security*, *68*, 130-144. https://doi.org/10.1016/j.cose.2017.04.010

Furnell, St. (2006). *Κυβερνοέγκλημα. Καταστρέφοντας την κοινωνία της πληροφορίας* (Χρ. Τσουραμάνης, Επιμ., Φ. Μηλιώνη, Μετ.). Εκδόσεις Παπαζήση

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. (2011). Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political. *IEEE Technology and Society Magazine*, *30*(1), 28-38. 10.1109/MTS.2011.940293

Garg, A., Curtis, J. & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security*, *11*(2), 74-83. 10.1108/09685220310468646

Gobeo, A., Fowler, C. & Buchanan, W.J. (2022). *GDPR and Cyber Security for Business Information Systems*. CRC Press

Goderdzishvili, N. (2010). Legal Assessment of Cyber Attacks on Georgia. *Data Exchange Agency Ministry of Justice of Georgia*

Gordon, L., Loeb, M. & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81-85. https://doi.org/10.1145/636772.636774

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, *2016*(6), 9-10. https://doi.org/10.1016/S1353-4858(16)30057-5

Hallam - Baker, P. (2008). Famous for Fifteen Minutes: A History of Hacking Culture. *CSO Online-Security and Risk*. http://www.csoonline.com/article/217058/famous-for-fifteen-minutes-ahistoryofhacking-culture

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. & Spiegel, J. (2012). The law of cyber-attack. *California law review*, 817-885.

Howart, F. (2008). Modern web attacks. *Network Security, 2008*(4), 13-15. https://doi.org/10.1016/S1353-4858(08)70053-9

IBM Security. (2022a). *Cost of a Data Breach Report 2022.* https://www.ibm.com/downloads/cas/3R8N1DZJ

IBM Security. (2022b). *X - Force Threat Intelligence Index 2022.* https://www.ibm.com/downloads/cas/ADLMYLAZ

IoT Security (2022). *IT Professional Security*, (74). https://www.itsecuritypro.gr/tefchi/teychos-74-martios-aprilios-maios-2022/

Iovan, S. & Iovan, A.A. (2016). From cyber threats to syber-crime. *Journal of Information Systems & Operations Management*, 425-434. http://www.rebe.rau.ro/RePEc/rau/jisomg/WI16/JISOM-WI16-A15.pdf

Italiano, L. (2012). Ex-staffer sentenced to 2-6 years for hacking into Gucci's system. *New York Post*. https://nypost.com/2012/09/10/ex-staffer-sentenced-to-2-6-years-for-hacking-into-guccis-system/

Jakobsson, M. & Myers, S. (2006). *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* John Wiley & Sons

Janczewski, L. & Colarik, A. (2007). *Cyber warface and cyber terrorism*. IGI Global

Jovičić, B. & Simić, D. (2006). Common web application attack types and security using ASP. NET. *Computer Science and Information Systems, 3*(2), 83-96. https://doi.org/10.2298/CSIS0602083J

Kabay, M.E. (2002). Salami fraud. *Network World Security Newsletter, 24.* http://www.minich.com/education/wyo/java/lecture_notes/SalamiFraud.pdf

Kalay, Y. & Marx, J. (2005). Architecture and the Internet: Designing places in cyberspace. *First Monday*. https://doi.org/10.5210/fm.v0i0.1563

Kaspersky Lab. (2015). *Damage control: the cost of security breaches. IT security risks special Report series.* https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Kim, D. & Solomon, M. (2021). *Fundamentals of information systems security*. Jones & Barlett Learning

Livanis, E. (2016). Financial aspects of cyber risks and taxonomy for the efficient handling of these risks. *Economic and Social Development (Book of Proceedings), 14th International Scientific Conference on Economic and Social Development*: May 13-14, 2016, Belgrade, Serbia. SSRN. 80-87. https://ssrn.com/abstract=2790564

Lyle Artz, M. (2002). *NetSPA: A Network Security Planning Architecture*. Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/29899

Maillart, T. & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal B*, *75*(3), 357-364. 10.1140/epjb/e2010-00120-8

Mbanaso, U & Dandaura, E. (2015) The cyberspace: redefining a new world. *IOSR Journal of Computer Engineering, 17*(3), 17-24. http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue3/Version-6/C017361724.pdf

McGuire, M. (2012). Organised crime in the digital age. *John Grieve Centre for Policing and Security*

Mclean, M. (2022). 2022-Must-Know Cyber Attack Statistics and Trends. *Embroker.* https://www.embroker.com/blog/cyber-attack-statistics/

Mishra, B.K. & Saini, H. (2009). Cyber attack classification using game theoretic weighted metrics approach. *World Applied Sciences Journal*, *7*, 206-215. http://www.idosi.org/wasj/wasj7(c&it)/27.pdf

Morales, J.A., Sandhu, R. & Xu, S. (2010). Evaluating detection and treatment effectiveness of commercial anti-malware programs. In: *2010 5th International Conference o Malicious and Malicious and Unwanted Software*, 31-38. https://doi.org/10.1109/MALWARE.2010.5665797

Mukhopadhyay, A., Saha, D., Chakrabarti, B.B., Mahanti, A. & Podder, A. (2005). Insurance for cyber-risk: A Utility Model. *Decision (0304-0941), 32*(1), 152-170. https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model

Neupane, K., Haddad, R. & Chen, L. (2018). Next generation firewall for network security: A survey. In: *SoutheastCon 2018*, 1-6. https://doi.org/10.1109/SECON.2018.8478973

O'Gorman, B. (2019). McAfee labs threats report. *McAfee Labs, Santa Clara.* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

Ögüt, H., Raghunathan, S. & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss and Observability of Self Protection. *Risk Analysis, 31*(3), 497-512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Owens, W., Dam, K. & Lin, H. (2009). *Technology, law and ethics regarding US acquisition of cyber attack capacities*. The National Academies Press. https://doi.org/10.17226/12651

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, *54*(11s), 1-40. https://doi.org/10.1145/3514229

Paoli, L., Kisschers, J. & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*(4), 397-420. https://doi.org/10.1007/s10611-018-9774-y

Peterson, A. (2014). The Sony pictures hack, explained. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

Pournouri, S., Zargari, S. & Akhgar, B. (2019). An investigation of using classification techniques in prediction of type of targets in cyber attacks. In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 202-212. https://doi.org/10.1109/ICGS3.2019.8688266

Presthus, W. & Sørum, H. (2018). Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation. *Procedia Computer Science, 138,* 603-611. http://dx.doi.org/10.1016/j.procs.2018.10.081

Ransomware New Generation (2021). *IT Professional Security*, (68). https://www.itsecuritypro.gr/tefchi/teychos-68-ianoyarios-fevroyarios-2021/

Ranum, M. J. (1997). A taxonomy of Internet attacks. In *proccedings of World Conference on Systems Management and Security.*

Richardson, R. & North, M.M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, 13(1), 10-21. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

Riley, M. & Roberson, J. (2015). China-Tied Hackers That Hit Us Said to Breach United rilines. *Bloomberg*. https://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford University Press

Samonas, S. & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3), 21-45. http://www.proso.com/dl/Samonas.pdf

Servida, F. & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, *28*, S22-S29. https://doi.org/10.1016/j.diin.2019.01.012

Shackelford, S. (2012). Should your firm invest in cyber risk insurance?. *Business Horizons, 55*(4), 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

Sharma, A., Gupta, P. & Noida, I. (2020). Covid 19 Pandemic: Impact on business and cyber security challenges. *Journal of Emerging Technologies and Innovative Research (JETIR), 7*(7), 304-310. https://www.jetir.org/papers/JETIR2007336.pdf

Shashidhar, S. (2017). Spear Phishing - The New Face of Phishing. https://doi.org/10.2139/SSRN.2905041

Sigler, K. (2018). Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), 12-14. http://dx.doi.org/10.1016/S1361-3723(18)30086-1

Singh, D. (2014). Emerging Trends in Cyber-Crimes. *Global Journal of Enterprise Information System, 6*(4), 29-32. https://www.gjeis.com/index.php/GJEIS/article/view/426

Smith, G. (2014). Home Depot Admits 56 million Payment Cards at Risk after Cyber Attack, *The Huffington Post*. https://www.huffpost.com/entry/home-depot-hack_n_5845378

Smith, K.T., Jones, A., Johnson, L. & Smith, L.M. (2018). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethnics in Society*. https://doi.org/10.1108/JICES-02-2018-0010

Sodhi, G.K., Singh Gaba, G., Kansal, L., Babulak, E., AlZain, M., Arora, S. & Masud, M. (2018). Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code. *Indonesian Journal of Electrical*

Engineering and Computer Science, 12(3), 1297-1304. http://doi.org/10.11591/ijeecs.v12.i3.pp1297-1304

Sousa, V. (2019). A Review on Cyber Attacks and Its Preventive Measures. In: *Proceedings of the Digital Privacy and Security Conference, 92*, 92-102. https://privacyandsecurityconference.pt/proceedings/2019/DPSC2019-paper18.pdf

Staff, U.A.F.J. (2010). Joint terminology for cyberspace operations. *Department of defence,* 1-16. https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

Sutherland, E. (1949). *White Collar Crime*. The Dryden Press

Teece, D. (2010). Business models, business strategy and innovation. *Long range planning, 43*(2-3), 172-194. https://doi.org/10.1016/j.lrp.2009.07.003

Thomas, O. (2013). Infamous iPad Hacker Makes No Apologies As He Faces Jail Time. *Business Insider*.

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Tobias, S. (2014). The Year in Cyberattacks. *Newsweek*. https://www.newsweek.com/2014-year-cyber-attacks-295876

Uma, M. & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *International Journal of Network Security, 15*(5), 390-396. http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf

Vaishnaw, N. & Tandan, S. (2015). Development of anti-phishing model for classification of phishing e-mail. *Development*, *4*(6), 39-45.

Voigt, P. & Von dem Bussche, A. (2017). *The EU general data protection regulation (GDPR). A Practical Guide.* Springer International Publishing

Waxman, M. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *The Yale Journal of International Law*, *36*, 421-459. 10.2139/ssrn.1674565

Waxman, M. (2011). Cyber Attacks as "Force" under UN Charter Article 2 (4). *Int'l L. Stud., 87*, 43-57.https://scholarship.law.columbia.edu/faculty_scholarship/847

Wiggins, L. (2002). Corporate Computer Crime: Collaborative Power in Numbers. *Federal Probation Journal, 66*(3), 19-29. https://www.uscourts.gov/sites/default/files/66_3_4_0.pdf

Yeboah-Boateng, E. O. & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-307. https://e-tarjome.com/storage/btn_uploaded/2020-09-12/1599891065_11216-etarjome%20English.pdf

Zviran, M. & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems, 15*(4), 161-185. http://www.jstor.org/stable/40398409

Διαδικτυακές πηγές

https://gdpr.eu/what-is-gdpr/?cn-reloaded=1

https://leaf-it.com/10-ways-prevent-cyber-attacks/

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Ι

MODUS OPERANDI	ΠΛΗΘΟΣ ΥΠΟΘΕΣΕΩΝ			
	2022 (μέχρι 11/2022)	2021	2020	2019
Επιθέσεις σε κρίσιμες υποδομές (Attacks on critical infrastructure) - DDOS Επιθέσεις άρνησης εξυπηρέτησης (Df-service attack, DoS attack)	12	18	10	8
Επιθέσεις σε κρίσιμες υποδομές (Attacks on critical infrastructure) - Man in the middle attacks	47	78	84	76
Επιθέσεις σε κρίσιμες υποδομές (Attacks on critical infrastructure) - Spear phishing (τεχνική ψαρέματος)	117	80	25	10
Παραποίηση Ιστοσελίδας (Defacement of websites) - Malicious website (κακόβουλος ιστότοπος)	37	20	11	4
Κακόβουλο Λογισμικό - Malware - Ransomware (Ψηφιακός εκβιασμός)	97	141	59	92
Κακόβουλη Διαδικτυακή Παρέμβαση - Network intrusions - Insider threat (Εσωτερική απειλή)	4	10	11	4
Απόσπαση πληροφοριών με σκοπό την πρόσβαση σε κάποιο υπολογιστικό σύστημα - Social Engineering - Phishing (via Email)	717	379	75	20
Απόσπαση πληροφοριών με σκοπό την πρόσβαση σε κάποιο υπολογιστικό σύστημα - Social Engineering - Vishing (via telephone)	53	36	7	4
Απόσπαση πληροφοριών με σκοπό την πρόσβαση σε κάποιο υπολογιστικό σύστημα - Social Engineering - Smishing (via SMS)	89	53	6	1
Cryptojacking – Cryptomining	3	1	0	1

Πίνακας 4

Επιθέσεις σε πληροφοριακά συστήματα γενικά, κατά τα έτη 2019 - 2022 (έως και Νοέμβριο 2022)

Πηγή: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (2022)

Στον παραπάνω Πίνακα παρουσιάζονται ορισμένοι τύποι κυβερνοεπιθέσεων που αναπτύχθηκαν στην παρούσα εργασία και εκδηλώθηκαν στον ελλαδικό χώρο,

βάσει του Στρατηγικού Σχεδιασμού της Europol. Όπως αναφέρθηκε και παραπάνω, σύμφωνα και με εκπρόσωπο της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, δεν είναι εφικτός ο διαχωρισμός του Modus Operandi, βάσει της κατηγορίας θυμάτων (π.χ. επιχείρηση, κυβέρνηση, μεμονωμένος χρήστης, κ.ά.). Ωστόσο, μπορούμε απλά να αναφέρουμε ότι τις πρώτες θέσεις για το έτος 2022, κατέχουν οι επιθέσεις phishing (Spear phishing, Smishing, Vishing) και το κακόβουλο λογισμικό ransomware, όπου ακολουθούν μια ανοδική πορεία από το έτος 2019, ενώ στις τελευταίες θέσεις κατά το έτος 2022 βρισκόταν οι κακόβουλες διαδικτυακές παρεμβάσεις από εσωτερικές απειλές και οι επιθέσεις Cryptojacking, δεδομένα τα οποία συμβαδίζουν και με τα στατιστικά λοιπών ερευνών που αναπτύχθηκαν στην υποενότητα με την ανάλυση στατιστικών δεδομένων.