ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
UNIVERSITY OF PATRAS
Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων
Τμήμα Διοικητικής Επιστήμης & Τεχνολογίας

D.I.MA
ΠΜΣ "Ψηφιακή Καινοτομία και Διοίκηση"
MSc in Digital Innovation

Πτυχιακή Εργασία

Κοινωνικές & Οικονομικές Προεκτάσεις του Ηλεκτρονικού Εγκλήματος

ΣΥΨΑ ΜΑΡΙΑ

Εποπτεύων Καθηγητής, **Γιάννης Σταματίου**

Πάτρα, Φεβρουάριος 2022

ΠΕΡΙΛΗΨΗ

Η συγκεκριμένη μεταπτυχιακή εργασία αναφέρεται στις οικονομικές και κοινωνικές προεκτάσεις του ηλεκτρονικού εγκλήματος. Η τεχνολογία είναι συνεχώς σε άνθιση και οπωσδήποτε αναγκαία αφού με τις εντυπωσιακές ανακαλύψεις έχει επιτρέψει στον άνθρωπο να έχει πρόσβαση σε πληροφορίες και εφαρμογές που στο παρελθόν ήταν ανύπαρκτες.

Υπάρχει όμως και άνθιση στο έγκλημα δίνοντας την ευκαιρία στου εγκληματίες του κυβερνοχώρου να επωφεληθούν και να μπορούν να επιτεθούν και να έχουν πρόσβαση σε πολλές πληροφορίες των οργανισμών ή επιχειρήσεων.

Στη συγκεκριμένη εργασία δίνονται πληροφορίες για τις πιο γνωστές απειλές βάσει του οργανισμού ENISA. Αναλύονται περιπτώσεις επιθέσεων σε οργανισμούς και μη για να γίνει αντιληπτό τι μπορεί να επιφέρει μια επίθεση γενικότερα.

Επιπλέον, μέσα από διάφορες μελέτες γίνεται προσπάθεια επεξήγησης των οικονομικών προεκτάσεων του ηλεκτρονικού εγκλήματος. Είναι μελέτες από διάφορα ινστιτούτα που δημοσιεύουν ετήσιες εκθέσεις για περιστατικά στον κυβερνοχώρο. Εξετάζονται επίσης οι κοινωνικές και ψυχολογικές επιπτώσεις που προκαλούν οι επιθέσεις αυτές στην καθημερινή ζωή των ανθρώπων. Αναλύεται το προφίλ των επιτιθέμενων αλλά και των δραστών.

Ωστόσο στη συγκεκριμένη μελέτη, αποτυπώνεται ταξινόμηση των διαφόρων τύπων βλαβών στον οργανισμό ή στην επιχείρηση και αναλύονται στενά ο αντίκτυπος της βλάβης αλλά και ο κίνδυνος. Ως συνέπεια αυτής της ταξινόμησης θα είναι η καλύτερη κατανόηση του ευρύτερου κινδύνου που αντιμετωπίζει ένας οργανισμός και μια επιχείρηση.

Σκοπός της εργασίας ήταν η πλήρης κατανόηση κυρίως κοινωνικών, ψυχολογικών και οικονομικών επιπτώσεων των διαδικτυακών επιθέσεων. Όταν το άτομο επαγρυπνά και έχει πλήρως αντιληφθεί τις συνέπειες δέχεται πιο εύκολα τους κανόνες ασφαλείας που του υποδεικνύουν οι ειδικοί.

ABSTRACT

This thesis refers to the economic and social implications of cybercrime. Technology is constantly flourishing and certainly necessary since with the impressive discoveries it has allowed man to have access to information and applications that were previously non-existent.

But there is also a flourishing in crime, giving cybercriminals the opportunity to benefit and to be able to attack and have access to a lot of information from organizations or businesses.

This work provides information on the most well-known threats under ENISA. Cases of attacks on organizations are analyzed to understand what an attack can bring about in general.

In addition, through various studies an attempt is made to explain the economic implications of cybercrime. They are studies by various institutes that publish annual reports on cyber incidents. It also examines the social and psychological impact of these attacks on people's daily lives. The profile of the attackers and perpetrators is analyzed.

However, in this study, a classification of the different types of damages in the organization or business is depicted and the impact of the damage and the risk are closely analyzed. Because of this classification will be a better understanding of the wider risk faced by an organization and a business.

There was no approach to the security measures that the person should take to protect himself from cyberattacks because the purpose of the work was to fully understand mainly the consequences of online attacks. When the person is vigilant and has fully realized the consequences, he accepts the safety rules more easily.

ΛΕΞΕΙΣ - ΚΛΕΙΔΙΑ

Κυβερνοασφάλεια, κίνδυνος, αντίκτυπος, επιθέσεις, κυβερνοσυμβάντα, κοινωνικός αντίκτυπος, ψυχολογική επιστήμη, ηλεκτρονικό έγκλημα, ψυχολογία του κυβερνοχώρου, ασφάλεια οργανισμού

Cybersecurity, risk; cyber-attack impacts, harm, organisational security, Cyber-attacks, social impacts, psychological impacts, cyberpsychology, behavioral science, risk perception, online safety, cybercrime, cybersecurity

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

ΠΡΟΛΟΓΟΣ

Η συγκεκριμένη μεταπτυχιακή διπλωματική εργασία αναφέρεται σε ένα πολύ νέο και συγχρόνως ενδιαφέρον αντικείμενο που έχει αναδυθεί τα τελευταία χρόνια, το ηλεκτρονικό έγκλημα. Η ανάπτυξη του διαδικτύου σε συνδυασμό με την ταχύτητα ανάπτυξης της τεχνολογίας, έφερε στο προσκήνιο ένα νέο τρόπο εγκλήματος. Δεν θα πρέπει όμως να εστιάζουμε μόνο στο έγκλημα αλλά και τις επιπτώσεις που αυτό επιφέρει στους οργανισμούς και εν γένει στην κοινωνία.

Οι περιπτωσιολογικές μελέτες που αναφέρονται στη συγκεκριμένη μελέτη επιλέχθηκαν με βάση τον αντίκτυπο των κυβερνοεπιθέσεων στους εν λόγω οργανισμούς / επιχειρήσεις εξαιτίας των μακροχρόνιων επιπτώσεων αυτών των επιθέσεων. Γίνεται προσπάθεια να κατανοήσουμε πως οι επιθέσεις μπορεί να διαταράξουν κρίσιμες υπηρεσίες παγκοσμίως. Ο κίνδυνος των επιθέσεων στον κυβερνοχώρο έχει αλματώδη αύξηση παράλληλα με την ανάπτυξη της τεχνολογίας.

Επιπλέον, μελετήθηκαν και αναφέρονται οικονομικές μελέτες παρέχοντας οικονομικά στοιχεία δίνοντας πληροφορίες για το ποιοι είναι αυτοί οι τομείς που βάλλονται τις περισσότερες φορές.

Αρωγός σε αυτή την προσπάθεια είναι **ο εξαίρετος επιβλέποντας καθηγητής κ. Ι. Σταματίου** που με ενέπνευσε από τις διαλέξεις του στο μάθημα του μεταπτυχιακού προγράμματος ώστε να ασχοληθώ με το συγκεκριμένο θέμα. Η βοήθεια του στη συγγραφή της συγκεκριμένης εργασίας είναι μεγάλη και θα ήθελα να τον ευχαριστήσω θερμά.

Θα πρέπει επίσης, να ευχαριστήσω την οικογένεια μου και ειδικότερα, **τον σύζυγο μου Ανδρέα και τα παιδιά μου Ηλία και Άννα-Μαρία** που έπαιξαν καταλυτικό ρόλο σε αυτή μου την προσπάθεια. Ήταν αυτοί που πάντα μου έδιναν κουράγιο, δύναμη και ενθάρρυνση για να συνεχίσω.

ΚΕΦΑΛΑΙΟ 1

1.1. Τι είναι το Διαδίκτυο

Ένα παγκόσμιο δίκτυο συνδεδεμένων υπολογιστών και άλλων ηλεκτρονικών συσκευών αποτελεί το γνωστό σε όλους Διαδίκτυο. Με τη χρήση λοιπόν του διαδικτύου είναι δυνατή η πρόσβαση σε κάθε πληροφορία, η επικοινωνία με οποιονδήποτε στον κόσμο και τόσα άλλα πράγματα.

Η προέλευση του διαδικτύου έχει τις ρίζες της στις ΗΠΑ της δεκαετία του 1950. Ο Ψυχρός Πόλεμος βρισκόταν στο αποκορύφωμά του και υπήρχαν τεράστιες εντάσεις μεταξύ της Βόρειας Αμερικής και της Σοβιετικής Ένωσης. Και οι δύο υπερδυνάμεις είχαν στην κατοχή τους θανατηφόρα πυρηνικά όπλα, και οι άνθρωποι ζούσαν με το φόβο επιθέσεων έκπληξη μεγάλου βεληνεκούς. Οι ΗΠΑ συνειδητοποίησαν ότι χρειάζονταν ένα σύστημα επικοινωνιών που δεν θα μπορούσε να επηρεαστεί από μια σοβιετική πυρηνική επίθεση.

Αυτό οδήγησε τελικά στη δημιουργία του ARPANET (Advanced Research Projects Agency Network), του δικτύου που τελικά εξελίχθηκε σε αυτό που γνωρίζουμε τώρα ως Διαδίκτυο. Το ARPANET ήταν μια μεγάλη επιτυχία, αλλά η πρόσβαση περιορίστηκε σε ορισμένους ακαδημαϊκούς και ερευνητικούς οργανισμούς που είχαν συμβόλαια με το Υπουργείο Άμυνας. Σε απάντηση σε αυτό, δημιουργήθηκαν άλλα δίκτυα για την παροχή κοινής χρήσης πληροφοριών.

Οι υπολογιστές εκείνη την εποχή ήταν μεγάλοι και ακίνητοι και για να χρησιμοποιηθούν οι πληροφορίες που ήταν αποθηκευμένες σε οποιονδήποτε υπολογιστή, κάποιος έπρεπε είτε να ταξιδέψει στο χώρο του υπολογιστή είτε να στείλει μαγνητικές ταινίες υπολογιστών μέσω του συμβατικού ταχυδρομικού συστήματος.

Η 1η Ιανουαρίου 1983 θεωρείται τα επίσημα γενέθλια του Διαδικτύου. Πριν από αυτό, τα διάφορα δίκτυα υπολογιστών δεν είχαν έναν τυπικό τρόπο επικοινωνίας μεταξύ τους. Ένα νέο πρωτόκολλο επικοινωνιών δημιουργήθηκε με την ονομασία Πρωτόκολλο ελέγχου μεταφοράς/Πρωτόκολλο εργασίας Internet (TCP/IP). Αυτό επέτρεψε σε διαφορετικά είδη υπολογιστών σε διαφορετικά δίκτυα να "μιλούν" μεταξύ τους. Το ARPANET και το Δίκτυο Αμυντικών Δεδομένων άλλαξαν επίσημα στο πρότυπο TCP/IP την 1η Ιανουαρίου 1983, εξ ου και η γέννηση του Διαδικτύου. Όλα τα δίκτυα θα μπορούσαν τώρα να συνδεθούν με μια καθολική γλώσσα.[1], [2]

1.2. Τεχνολογία του Διαδικτύου

Η τεχνολογία διαδικτύου είναι η ικανότητα του Διαδικτύου να μεταδίδει πληροφορίες και δεδομένα μέσω διαφορετικών διακομιστών και συστημάτων. Η τεχνολογία του Διαδικτύου είναι σημαντική σε πολλούς διαφορετικούς κλάδους, επειδή επιτρέπει στους ανθρώπους να επικοινωνούν μεταξύ τους με μέσα που δεν ήταν απαραίτητα διαθέσιμα. Το Διαδίκτυο είναι

[1] A Brief History of the Internet (usg.edu)
[2] Internet History of 1970s | Internet History

ουσιαστικά μια μεγάλη βάση δεδομένων όπου μπορούν να διαβιβαστούν και να μεταδοθούν όλοι οι διαφορετικοί τύποι πληροφοριών. Μπορεί να μεταδοθεί παθητικά με τη μορφή μη διαδραστικών ιστότοπων και ιστολογίων. Μπορεί επίσης να μεταβιβαστεί ενεργά με τη μορφή κοινής χρήσης αρχείων και φόρτωσης εγγράφων. Η τεχνολογία του Διαδικτύου έχει οδηγήσει σε πληθώρα πληροφοριών που είναι διαθέσιμες σε οποιονδήποτε είναι σε θέση να έχει πρόσβαση στο Διαδίκτυο. Επέτρεψε στους ανθρώπους που ήταν εξοικειωμένοι με τα εγχειρίδια και τις βιβλιοθήκες να μάθουν οτιδήποτε θα μπορούσαν να θέλουν από την άνεση ενός υπολογιστή.

Η τεχνολογία του Διαδικτύου βελτιώνεται συνεχώς και είναι σε θέση να επιταχύνει τον αυτοκινητόδρομο πληροφοριών που έχει δημιουργήσει. Με τις τεχνολογίες να τροφοδοτούν το Διαδίκτυο, οι ταχύτητες είναι ταχύτερες, περισσότερες πληροφορίες είναι διαθέσιμες και γίνονται διαφορετικές διαδικασίες που δεν ήταν δυνατές στο παρελθόν. Η τεχνολογία του Διαδικτύου έχει αλλάξει και θα συνεχίσει να αλλάζει τον τρόπο με τον οποίο ο κόσμος λειτουργεί και τον τρόπο με τον οποίο οι άνθρωποι αλληλεπιδρούν στην καθημερινή ζωή.

Το διαδίκτυο συχνά περιγράφεται ως αποτελούμενο από τρία μέρη: τον επιφανειακό ιστό (surface web), τον βαθύ ιστό (deep web) και τον σκοτεινό ιστό (dark web).

Οι όροι "βαθύς ιστός" και "σκοτεινός ιστός" χρησιμοποιούνται τακτικά, γεγονός που μπορεί να προκαλέσει μεγάλη σύγχυση. Καθώς μιλάμε για τον σκοτεινό ιστό, ακολουθούν μερικά σημεία που πρέπει να έχουμε κάνει κατανοητά.

Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο. Το web είναι ένα εργαλείο επικοινωνίας που χρησιμοποιεί το δίκτυο διαδικτύου. Ο ιστός αποτελείται από τον ιστό επιφάνειας, τον βαθύ ιστό και τον σκοτεινό ιστό.

1.3. Ο επιφανειακός Ιστός (surface web)

Ο επιφανειακός ιστός - μαζί με τον βαθύ ιστό - είναι το μέρος του διαδικτύου που οι περισσότεροι από εμάς χρησιμοποιούμε καθημερινά. Είναι προσβάσιμο μέσω τακτικών προγραμμάτων περιήγησης, όπως το Google Chrome, το Safari ή ο Firefox.

Άλλοι ιστότοποι, συμπεριλαμβανομένων εκείνων των διαδικτυακών καταστημάτων και των επιχειρήσεων, αποτελούν επίσης μέρος του "κανονικού ιστού". Ωστόσο, όταν ανοίγετε έναν ιστότοπο ως επισκέπτης, δεν μπορείτε να δείτε κάθε μέρος αυτού του ιστότοπου. Θα δεις μόνο την επιφάνεια.

Όταν σερφάρετε στο Amazon χωρίς να συνδεθείτε, για παράδειγμα, θα δείτε τις καταχωρήσεις προϊόντων τους. Αλλά θα μπορείτε να δείτε τον ιστότοπο μόνο ως πελάτη, όχι ως πωλητή ή διαχειριστή.

Για να μπορέσετε να κοιτάξετε "πίσω από τα παρασκήνια", θα χρειαστείτε ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Μόλις τα έχετε αυτά, θα είστε σε θέση να περάσετε από την επιφάνεια και να μπείτε στον βαθύ ιστό.

1.4. Ο βαθύς ιστός (deep web)

Ο όρος "βαθύς ιστός" αναφέρεται στο μέρος του διαδικτύου που βρίσκεται πίσω από κλειστές πόρτες. Το μεγαλύτερο μέρος του βαθύ ιστού αποτελείται από σελίδες και βάσεις δεδομένων που προορίζονται μόνο για μια συγκεκριμένη ομάδα ατόμων μέσα σε έναν οργανισμό.

Η βάση δεδομένων εργασίας σας μπορεί να βρίσκεται σε αυτό το τμήμα του ιστού. Για να αποκτήσετε πρόσβαση, θα πρέπει να γνωρίζετε την ακριβή διεύθυνση web (αλλιώς γνωστή ως διεύθυνση URL). Σε ορισμένες περιπτώσεις, θα χρειαστείτε επίσης έναν κωδικό πρόσβασης.

Οι περισσότεροι από εμάς δεν θα έχουν πρόσβαση σε αυτήν τη διεύθυνση URL και τα απαιτούμενα διαπιστευτήρια σύνδεσης — και αυτές οι πληροφορίες δεν μπορούν να βρεθούν ούτε στις μηχανές αναζήτησης. Με άλλα λόγια: μια συμβατική αναζήτηση Google δεν θα δείξει βαθύ περιεχόμενο ιστού ή σελίδες.

Ο βαθύς ιστός είναι το μεγαλύτερο μέρος του διαδικτύου, εκτιμάται ότι αποτελεί μεταξύ 90 και 95% του πλήρους παγκόσμιου ιστού. Παραδείγματα σελίδων στο βαθύ διαδίκτυο είναι: τα προσωπικά δεδομένα και οι σελίδες εταιρειών, πανεπιστημίων, βιβλιοθηκών, νοσοκομείων, κυβερνήσεων, διεθνών οργανισμών κ.ο.κ.

1.5. Ο σκοτεινός ιστός (dark web)

Ο σκοτεινός ιστός είναι το μέρος του βαθύ ιστού που είναι προσβάσιμο μόνο μέσω ενός ειδικού προγράμματος περιήγησης: του προγράμματος περιήγησης Tor.

Ονομάζεται επίσης "darknet", αυτή η συλλογή ιστότοπων αναφέρεται στο ανεξέλεγκτο τμήμα του διαδικτύου. Κανένας οργανισμός, επιχείρηση ή κυβέρνηση δεν είναι υπεύθυνος για τον σκοτεινό ιστό ή είναι σε θέση να επιβάλει κανόνες. Αυτός είναι ακριβώς ο λόγος για τον οποίο ο σκοτεινός ιστός συνδέεται συνήθως με παράνομες δραστηριότητες.

Μερικοί άνθρωποι αναφέρονται σε αυτό το μέρος του διαδικτύου ως "βαθύ ιστό", αλλά αυτός δεν είναι ο σωστός όρος. Είναι αλήθεια ότι ο σκοτεινός ιστός είναι μέρος του βαθύ ιστού, αλλά είναι ένα διαφορετικό τμήμα του διαδικτύου συνολικά.

Όπως αναφέρθηκε, ο βαθύς ιστός είναι προσβάσιμος μέσω τακτικών προγραμμάτων περιήγησης - αρκεί να έχετε την ακριβή διεύθυνση URL. Αυτό δεν ισχύει για τον σκοτεινό ιστό. Είναι αδύνατο να φτάσετε στον σκοτεινό ιστό μέσω ενός κανονικού προγράμματος περιήγησης όπως το Google Chrome ή το Edge.

Ο σκοτεινός ιστός λειτουργεί διαφορετικά από τον κανονικό ιστό. Ακόμα και όταν χρησιμοποιείτε το Tor, οι ιστότοποι σκοτεινού ιστού δεν καταλήγουν σε .com ή .org.

Ο σκοτεινός ιστός λειτουργεί διαφορετικά από τον κανονικό ιστό. Ακόμα και όταν χρησιμοποιείτε το Tor, οι ιστότοποι σκοτεινού ιστού δεν καταλήγουν σε .com ή .org. Αντίθετα, οι διευθύνσεις URL αποτελούνται συνήθως από έναν τυχαίο συνδυασμό γραμμάτων και αριθμών. Καταλήγουν επίσης σε .onion.

Επιπλέον, οι διευθύνσεις URL των σκοτεινών ιστότοπων αλλάζουν τακτικά, οπότε δεν είναι τόσο εύκολο να βρεθούν όσο οι περισσότερες πλατφόρμες σε άλλα μέρη του διαδικτύου.

1.6. Το διαδίκτυο στην Ελλάδα

Στην Ελλάδα το διαδίκτυο έκανε την εμφάνιση του την δεκαετία του 1990 και στην αρχή τα άτομα που είχαν πρόσβαση ήταν κυρίως ερευνητές. Οι πρώτοι πάροχοι έκαναν την εμφάνιση τους αργότερα και μόνο το 1% των κατοίκων το 1995 μπορούσε να έχει πρόσβαση ενώ το αντίστοιχο ποσοστό για το έτος 2000 ήταν 21%, κι αυτό επειδή ήταν εκτενής η χρήση των προσωπικών υπολογιστών. Ήταν η εποχή που και το κινητό τηλέφωνο είχε μεγάλη επέκταση στη χώρα αλλά και στην Ευρωπαϊκή Ένωση.

ΚΕΦΑΛΑΙΟ 2

2.1. Ηλεκτρονικό Έγκλημα (Ορισμός)

Σύμφωνα με τους Forester & Morrison, 1994 , μια εγκληματική πράξη για την οποία χρησιμοποιείται ως μέσο ένας ηλεκτρονικός υπολογιστής θα μπορούσε να είναι ο ορισμός για το Ηλεκτρονικό Έγκλημα.

Κάποιοι από τους όρους που χρησιμοποιούνται στην αγγλική γλώσσα για να ορίσουν το ηλεκτρονικό έγκλημα είναι: cybercrime, computer crime, e-crime και hitech crime. Αντίστοιχα στη γλώσσα μας οι όροι ποικίλουν όπως δικτυακό έγκλημα ή κυβερνοέγκλημα.[3]

Ο πολλαπλασιασμός του εγκλήματος στον κυβερνοχώρο προσθέτει αμέτρητα κόστη αποζημίωσης κάθε χρόνο, επηρεάζοντας άτομα, επιχειρήσεις, ακόμη και κυβερνήσεις.

Καθώς το Διαδίκτυο των Πραγμάτων (IoT) εξελίσσεται και οι έξυπνες συσκευές γίνονται πιο δημοφιλείς, οι εγκληματίες του κυβερνοχώρου επωφελούνται από μια πολύ ευρύτερη επιφάνεια επίθεσης - αυξημένες ευκαιρίες διείσδυσης σε μέτρα ασφαλείας, απόκτηση μη εξουσιοδοτημένης πρόσβασης και διάπραξης εγκλημάτων.

2.2. ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερονασφάλεια)

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ENISA, είναι ο οργανισμός της Ένωσης που είναι αφιερωμένος στην επίτευξη υψηλού κοινού επιπέδου κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ιδρύθηκε το 2004 και ενισχύθηκε από τον νόμο της ΕΕ για την κυβερνοασφάλεια. Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια συμβάλλει στην πολιτική της ΕΕ στον κυβερνοχώρο, ενισχύει την αξιοπιστία των προϊόντων, των υπηρεσιών και των διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με τα κράτη μέλη και τους οργανισμούς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές κυβερνοασφάλειες. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της ευαισθητοποίησης, ο Οργανισμός συνεργάζεται με όλους τους εμπλεκόμενους για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την ενίσχυση της ανθεκτικότητας των υποδομών της Ένωσης και, εν τέλει, τη διατήρηση της ψηφιακής ασφάλειας της κοινωνίας και των πολιτών της Ευρώπης.

[3] Τι είναι ηλεκτρονικό έγκλημα – Ηλεκτρονικό έγκλημα (google.com)

Σε έκθεση του λοιπόν, οι πρωταρχικές απειλές που εντοπίστηκαν περιλαμβάνουν τις πιο κάτω 15 όπως φαίνεται και στο Σχήμα 1.

ΕΙΚΟΝΑ 1 ΟΙ 15 ΠΙΟ ΠΡΩΤΑΡΧΙΚΕΣ ΑΠΕΙΛΕΣ ΒΑΣΙΣΜΕΝΕΣ ΣΤΟΝ ENISA

Πηγή: *Κύριες κυβερνοαπειλές στην ΕΕ - Consilium (europa.eu)*

ΕΙΚΟΝΑ 2: ΓΡΑΦΗΜΑ ΠΟΥ ΠΑΡΟΥΣΙΑΖΕΙ ΣΤΟΙΧΕΙΑ ΚΑΙ ΑΡΙΘΜΟΥΣ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΚΥΡΙΕΣ ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ

2.3. Οι 15 πιο γνωστές Απειλές βασισμένες στην αναφορά του ENISA[4]

#1 Malware

Το κακόβουλο λογισμικό είναι ένας συνηθισμένος τύπος κυβερνοεπίθεσης με τη μορφή κακόβουλου λογισμικού. Οι οικογένειες κακόβουλου λογισμικού περιλαμβάνουν κρυπτομερή, ιούς, ransomware, worms και spyware. Οι πιο κοινοί στόχοι τους είναι κλοπή πληροφοριών ή ταυτότητας, κατασκοπεία και διακοπή υπηρεσιών Κατά τη διάρκεια του 2019, οι κρυπτογραφητές ήταν ένα από τα πιο διαδεδομένα κακόβουλα προγράμματα με αποτέλεσμα υψηλό κόστος πληροφορικής, αυξημένη κατανάλωση ηλεκτρικής ενέργειας και μειωμένη παραγωγικότητα των εργαζομένων. Το Ransomware παρουσίασε μια μικρή αύξηση το 2019 σε σύγκριση με το 2018, αν και εξακολουθεί να βρίσκεται στο κάτω μέρος της λίστας των τύπων κακόβουλου λογισμικού Τα πρωτόκολλα ιστού και e-mail ήταν οι πιο συνηθισμένοι τρόποι που χρησιμοποιούνται για τη διάδοση κακόβουλου λογισμικού. Ωστόσο, χρησιμοποιώντας τεχνικές ωμής βίας ή εκμεταλλευόμενοι τις ευπάθειες του συστήματος, ορισμένες οικογένειες κακόβουλου λογισμικού μπόρεσαν να εξαπλωθούν ακόμη περισσότερο μέσα σε ένα δίκτυο. Αν και οι παγκόσμιες ανιχνεύσεις παρέμειναν στα επίπεδα του προηγούμενου έτους, υπήρξε μια αισθητή στροφή από καταναλωτικούς σε επιχειρηματικούς στόχους.

#2 Επιθέσεις ιστού (Web-based attacks)

Οι επιθέσεις που βασίζονται στον ιστό είναι μια ελκυστική μέθοδος με την οποία μπορούν να εξαπατούν τα θύματα χρησιμοποιώντας διαδικτυακά συστήματα και υπηρεσίες. Αυτό καλύπτει μια τεράστια επιφάνεια επίθεσης, για παράδειγμα διευκολύνοντας κακόβουλες διευθύνσεις URL ή κακόβουλα σενάρια για να κατευθύνουν τον χρήστη ή το θύμα στον ιστότοπο που επιθυμούν ή λήψη κακόβουλου περιεχομένου και την εισαγωγή κακόβουλου κώδικα σε έναν νόμιμο αλλά παραβιασμένο ιστότοπο για κλοπή πληροφοριών (δηλ. formjacking) για οικονομικό όφελος, πληροφορίες κλοπή ή ακόμη και εκβιασμός μέσω ransomware. Εκτός από αυτά παραδείγματα, εκμεταλλεύσεις του προγράμματος περιήγησης στο Διαδίκτυο και του συστήματος διαχείρισης περιεχομένου (CSM) είναι σημαντικοί φορείς που παρατηρούνται από διαφορετικές ερευνητικές ομάδες να χρησιμοποιούνται ως κακόβουλοι παράγοντες. Οι επιθέσεις ωμής βίας, για παράδειγμα, στοχεύουν σε μια λειτουργία με συντριπτική διαδικτυακή εφαρμογή με απόπειρες σύνδεσης με όνομα χρήστη και κωδικό πρόσβασης. Οι επιθέσεις που βασίζονται στον ιστό μπορούν να επηρεάσουν τη διαθεσιμότητα ιστότοπων, εφαρμογών και διεπαφές προγραμματισμού εφαρμογών (API), παραβιάζοντας το απόρρητο και την ακεραιότητα των δεδομένων.

[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

#3 Ηλεκτρονικό ψάρεμα (phishing)

Το ηλεκτρονικό ψάρεμα (phishing) είναι η δόλια απόπειρα κλοπής δεδομένων χρηστών, όπως η σύνδεση με διαπιστευτήρια, στοιχεία πιστωτικής κάρτας ή ακόμη και χρήματα που χρησιμοποιούν κοινωνικές τεχνικές μηχανικής. Αυτός ο τύπος επίθεσης ξεκινά συνήθως μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, που φαίνεται να έχουν σταλεί από αξιόπιστη πηγή, με σκοπό να πείσει τον χρήστη να ανοίξει ένα κακόβουλο συνημμένο ή να ακολουθήσει μια δόλια διεύθυνση URL. Μια στοχευμένη μορφή του phishing που ονομάζεται «spear phishing» βασίζεται στην εκ των προτέρων έρευνα για τα θύματα έτσι ώστε η απάτη να φαίνεται πιο αυθεντική, καθιστώντας την έτσι μια από τους πιο επιτυχημένους τύπους επιθέσεων σε δίκτυα επιχειρήσεων. Μια συναισθηματική απάντηση δικαιολογεί τις ενέργειες πολλών ανθρώπων όταν είναι phished και είναι ακριβώς αυτό που ψάχνουν οι χάκερ. Στο πλαίσιο εκπαίδευσης, αυτό πρέπει να προσπαθήσει να επιτύχει μια προσομοίωση ηλεκτρονικού ψαρέματος.

Εκπαιδευτικό e-mail : Οι χρήστες είναι ένα από τα μέτρα που χρησιμοποιούνται συχνά για την πρόληψη του ηλεκτρονικού ψαρέματος, αλλά τα αποτελέσματα δεν είναι πειστικά αφού οι φορείς απειλής αλλάζουν συνεχώς τον τρόπο λειτουργίας τους. Έλεγχος ταυτότητας μηνύματος βάσει τομέα, το πρότυπο αναφοράς και συμμόρφωσης (DMARC) διασφαλίζει ότι το e-mail από αναξιόπιστες πηγές αποκλείονται, μειώνοντας το ποσοστό επιτυχίας των phishing, πλαστογραφία και spam επιθέσεις. Στο μέλλον, το e-mail θα εξακολουθήσει να είναι ο νούμερο ένα μηχανισμός για phishing αλλά όχι για πολύ. Βλέπουμε ήδη αύξηση της χρήσης του στα μηνύματα κοινωνικής δικτύωσης, WhatsApp και άλλα για τη διενέργεια επιθέσεων. Η πιο σχετική αλλαγή θα γίνει στις μεθόδους που χρησιμοποιούνται για την αποστολή των μηνυμάτων, η οποία θα γίνει πιο εξελιγμένη με την υιοθέτηση της Τεχνητής Νοημοσύνης (AI) για την προετοιμασία και την αποστολή των μηνυμάτων.

#4 Επιθέσεις εφαρμογών Διαδικτύου (Web application attacks)

Οι εφαρμογές και οι τεχνολογίες Ιστού έχουν γίνει βασικό μέρος του Διαδίκτυο υιοθετώντας διαφορετικές χρήσεις και λειτουργίες. Η αύξηση των διαδικτυακών εφαρμογών και των διαδεδομένων υπηρεσιών τους δημιουργούν προκλήσεις για την προστασία τους από απειλές με ποικίλα κίνητρα από οικονομική ή φήμη φθοράς έως κλοπή κρίσιμων ή προσωπικών πληροφοριών. Οι υπηρεσίες και οι εφαρμογές Ιστού εξαρτώνται κυρίως από βάσεις δεδομένων για αποθήκευση ή παράδοση των απαιτούμενων πληροφοριών. Ένα πολύ γνωστό παράδειγμα επίθεσης είναι ο τύπος SQL Injection (SQLi) και μια από τις πιο συνηθισμένες απειλές εναντίον τους σε τέτοιες υπηρεσίες. Ένα άλλο παράδειγμα είναι οι επιθέσεις σεναρίων μεταξύ ιστότοπων (XSS). Σε αυτόν τον τύπο επίθεσης, γίνεται κατάχρηση αδυναμιών σε μορφές ή άλλες λειτουργίες εισόδου εφαρμογών Ιστού που οδηγούν σε άλλες κακόβουλες λειτουργίες όπως η ανακατεύθυνση σε κακόβουλο ιστότοπο. Καθώς λοιπόν οι οργανισμοί εξειδικεύονται και αναπτύσσουν μεγαλύτερη αυτοματοποίηση στις διαδικτυακές εφαρμογές και τον κύκλο ζωής τους, απαιτούν ασφάλεια και είναι από τα καίρια θέματα και προτεραιότητά τους. Αυτή η εισαγωγή σύνθετων περιβαλλόντων οδηγεί την υιοθέτηση νέων υπηρεσιών, όπως διεπαφές προγραμματισμού εφαρμογών (API) , τα οποία δημιουργούν νέες προκλήσεις για την ασφάλεια των εφαρμογών Ιστού. Οι οργανισμοί που

εμπλέκονται πρέπει να εξετάσουν περισσότερη πρόληψη και ανίχνευση ως μέτρα ασφαλείας. Για παράδειγμα, περίπου το 80% των οργανισμών που υιοθετούν API αναπτύσσουν ελέγχους στην κυκλοφορία εισόδου τους.

#5 Ανεπιθύμητο μήνυμα (Spam)

Το πρώτο ανεπιθύμητο μήνυμα στάλθηκε το 1978 από έναν υπεύθυνο μάρκετινγκ σε 393 άτομα μέσω ARPANET. Αφορούσε μια διαφημιστική καμπάνια για ένα νέο προϊόν από την εταιρεία στην οποία εργαζόταν, την Digital Equipment Corporation. Για αυτούς τους πρώτους 393 ανεπιθύμητοι χρήστες ήταν τόσο ενοχλητικό όσο θα ήταν σήμερα, ανεξάρτητα από την καινοτομία της ιδέας. Η λήψη ανεπιθύμητων μηνυμάτων είναι ενοχλητικό, αλλά μπορεί επίσης να δημιουργήσει μια ευκαιρία για ένα κακόβουλο λογισμικό να κλέψει προσωπικές πληροφορίες ή να εγκαταστήσει κακόβουλο λογισμικό Το spam αποτελείται από: μαζική αποστολή ανεπιθύμητων μηνυμάτων. Θεωρείται ως απειλή στον κυβερνοχώρο αφού χρησιμοποιείται ως επίθεσης για διανομή ή ενεργοποίηση άλλων απειλών. Μια άλλη αξιοσημείωτη πτυχή είναι το πώς μερικές φορές μπορεί να συγχέεται το spam ή παρερμηνεύεται ως εκστρατεία ηλεκτρονικού ψαρέματος. Η κύρια διαφορά μεταξύ των δύο είναι το γεγονός ότι το phishing είναι μια στοχευμένη δράση με χρήση κοινωνικής μηχανικής τακτικές, με στόχο ενεργά την κλοπή δεδομένων των χρηστών. Αντίθετα, το spam είναι μια τακτική για αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε μαζική λίστα. Οι καμπάνιες ηλεκτρονικού ψαρέματος μπορούν να χρησιμοποιούν τακτικές ανεπιθύμητης αλληλογραφίας για τη διανομή μηνυμάτων ενώ τα ανεπιθύμητα μηνύματα μπορούν να συνδέσουν τον χρήστη με παραβίαση ιστότοπου για εγκατάσταση κακόβουλου λογισμικού και κλοπή προσωπικών δεδομένων. Εκστρατείες ανεπιθύμητης αλληλογραφίας, κατά τη διάρκεια αυτών των τελευταίων 41 ετών εκμεταλλεύτηκαν πολλά δημοφιλή παγκόσμια κοινωνικά και αθλητικά γεγονότα όπως η UEFA Europa Τελικός League, US Open, μεταξύ άλλων. Ακόμα κι έτσι, δεν μπορεί να συγκριθεί με την ανεπιθύμητη δραστηριότητα που παρατηρήθηκε φέτος εξαιτίας της πανδημίας του COVID-19.

#6 DDoS (Distributed Denial of Service)

Είναι γνωστές οι επιθέσεις Distributed Denial of Service (DDoS) όταν οι χρήστες ενός συστήματος ή μιας υπηρεσίας δεν είναι σε θέση να έχουν πρόσβαση σε πληροφορίες, υπηρεσίες ή άλλους πόρους. Αυτό το στάδιο μπορεί να επιτευχθεί με εξάντληση της υπηρεσίας ή υπερφόρτωση των στοιχείων στο δίκτυο υποδομής. Οι κακόβουλοι φορείς αύξησαν τον αριθμό των επιθέσεων με στόχευση σε περισσότερους τομείς και διαφορετικά κίνητρα. Ενώ οι αμυντικοί μηχανισμοί και οι στρατηγικές γίνονται πιο ισχυρές, οι κακόβουλοι φορείς επίσης προωθούν τις τεχνικές τους δεξιότητες. Συγκεκριμένες αναφορές δείχνουν ότι οι κακόβουλοι χρησιμοποιούν ολοένα και πιο νέες τεχνικές. Βελτιώνουν επίσης τις εμπορικές τους τακτικές ξεκινώντας να διαφημίζουν τις υπηρεσίες τους στο διαδίκτυο. Ιστορικά, οι υπηρεσίες DDoS διαφημίζονταν στα σκοτεινά φόρουμ ιστού, αλλά τώρα χρησιμοποιούν και κοινά κοινωνικά κανάλια πολυμέσων όπως το YouTube και το Redit για την προώθηση των υπηρεσιών τους. Το 2019, είδαμε νέες καταχωρήσεις στην κορυφαία λίστα 10 χωρών προέλευσης DDoS (Χονγκ Κονγκ, Νότια Αφρική, κ.λπ.). Επιπλέον ήταν η χρονιά που αυξήθηκε η δραστηριότητα DDoS από τα botnets. Οι συσκευές IoT είναι

«Εστία» για τα botnets DDoS, και η Κίνα (24%), η Βραζιλία (9%) και το Ιράν (6%) , θεωρούνται ως οι χώρες που έχουν μολυνθεί περισσότερο από παράγοντες botnet. Ένας ερευνητής προέβλεψε ότι, με την εφαρμογή και τη διανομή του 5G θα αυξηθεί εκθετικά ο αριθμός των συνδεδεμένων συσκευών, εξ ου και η επέκταση των δικτύων botnet. Αν και οι επιθέσεις DoS δεν είναι καινούριες, το επίπεδο πολυπλοκότητάς τους αυξάνεται και παρατηρείται ότι κακόβουλοι παράγοντες εκτελούν ενεργά περισσότερες αναγνωριστικές δραστηριότητες από πριν.

#7 Κλοπή ταυτότητας (Identity theaft)

Η κλοπή ταυτότητας ή η ταυτοποίηση απάτης είναι η παράνομη χρήση προσωπικών δεδομένων και πληροφοριών ενός θύματος από έναν απατεώνα για να υποδυθεί το πρόσωπο αυτό και να αποκτήσει οικονομικό πλεονέκτημα και άλλα οφέλη. Σύμφωνα με μια ετήσια έκθεση ασφαλείας, τουλάχιστον 900 διεθνείς περιπτώσεις εντοπίστηκαν ως κλοπές ταυτότητας ή εγκλήματα που σχετίζονται με κλοπή ταυτότητας. Τα πιο σημαντικά περιστατικά που αναφέρθηκαν ήταν:

- σχεδόν 106 εκατομμυρίων αμερικανικών και καναδικών τραπεζών προσωπικές πληροφορίες πελατών από παραβίαση δεδομένων Capital One περιστατικό τον Μάρτιο του 2019
- 170 εκατομμυρίων ονομάτων χρήστη και κωδικών πρόσβασης που χρησιμοποιούνται από τον ψηφιακό προγραμματιστή παιχνιδιών Zynga τον Σεπτέμβριο του 2019.
- η κλοπή 20 εκατομμυρίων λογαριασμών από τη βρετανική υπηρεσία ήχου Mixcloud
- ο συμβιβασμός 600.000 οδηγών και 57 εκατομμυρίων χρηστών για προσωπικές πληροφορίες από το περιστατικό παραβίασης δεδομένων της Uber τον Νοέμβριο του 2019 .
- και η κλοπή 9 εκατομμυρίων προσωπικών αρχείων από πελάτες της EasyJet συμπεριλαμβανομένων των δελτίων ταυτότητας και των πιστωτικών καρτών. Η τάση κλοπής ταυτότητας αντικατοπτρίζεται σε μεγάλο βαθμό στις παραβιάσεις δεδομένων, η οποία, σε σύγκριση με το 2018, σημείωσε αριθμό ρεκόρ. 3.800 περιπτώσεις αποκαλύφθηκαν, 4,1 δισεκατομμύρια εκτεθειμένα αρχεία και αύξηση 54% στον αριθμό των αναφερόμενων παραβιάσεων.

#8 Data breach

Η παραβίαση δεδομένων είναι ένας τύπος περιστατικού ασφάλειας στον κυβερνοχώρο στον οποίο πληροφορίες (ή μέρος ενός πληροφοριακού συστήματος) έχουν πρόσβαση χωρίς δικαίωμα εξουσιοδότησης, συνήθως με κακόβουλη πρόθεση, και οδηγεί σε πιθανή απώλεια ή κατάχρηση αυτών των πληροφοριών. Περιλαμβάνει επίσης «ανθρώπινο λάθος» , συχνά συμβαίνει κατά τη διαμόρφωση και την ανάπτυξη ορισμένων υπηρεσιών και συστημάτων και μπορεί να οδηγήσει σε ακούσια έκθεση δεδομένων. Σε πολλές περιπτώσεις, εταιρείες ή οργανισμοί δεν γνωρίζουν ότι έχει γίνει παραβίαση δεδομένων στο περιβάλλον τους λόγω της πολυπλοκότητας της επίθεσης και μερικές φορές λόγω της έλλειψης ελέγχου και ταξινόμησης σε αυτά τα πληροφοριακά συστήματα.

Με βάση την έρευνα, χρειάζονται περίπου 206 ημέρες για τον εντοπισμό παραβίασης δεδομένων σε έναν οργανισμό. Έτσι, ο χρόνος συγκράτησης, η αποκατάσταση και η ανάκτηση των δεδομένων σημαίνει ότι χρειάζεται περισσότερος χρόνος για την επιστροφή στην κανονικότητα. Παρά τους κινδύνους που εμπλέκονται, οι οργανισμοί διατηρούν ακόμη περισσότερα δεδομένα χρησιμοποιώντας υποδομές αποθήκευσης cloud και περίπλοκα εσωτερικά περιβάλλοντα. Αυτά τα περιβάλλοντα σταδιακά εκτίθενται όλο και περισσότερο σε νέους και διαφορετικούς κινδύνους, ανάλογους της ευαισθησίας των αποθηκευμένων πληροφοριών. Δεν αποτελεί έκπληξη το γεγονός ότι ο αριθμός των παραβιάσεων δεδομένων αυξήθηκε το 2019 και 2020. Νέα ευρήματα υποδηλώνουν επίσης ότι ο αντίκτυπος δεν είναι αισθητός όταν διαπιστώνεται παραβίαση δεδομένων - ο οικονομικός αντίκτυπος όμως παραμένει για περισσότερα από 2 χρόνια μετά το αρχικό περιστατικό.

#9 Insider threat (Εσωτερική απειλή)

Μια εσωτερική απειλή είναι μια ενέργεια που μπορεί να οδηγήσει σε ένα περιστατικό, που εκτελείται από κάποιον ή μια ομάδα ανθρώπων που συνδέονται ή εργάζονται για το δυνητικό θύμα. Υπάρχουν διάφορα μοτίβα που σχετίζονται με απειλές από μέσα. Ένα πασίγνωστο μοτίβο απειλών εσωτερικού (γνωστό και ως «κατάχρηση προνομίων») συμβαίνει όταν οι ξένοι συνεργάζονται με εσωτερικούς παράγοντες για να κερδίσουν μη εγκεκριμένη πρόσβαση σε περιουσιακά στοιχεία. Οι εσωτερικοί άνθρωποι μπορεί να προκαλέσουν βλάβη ακούσια μέσω απροσεξίας ή λόγω έλλειψης γνώσης. Αφού οι εσωτερικοί απολαμβάνουν συχνά εμπιστοσύνη και προνόμια, καθώς και γνώση σε οργανωτικές πολιτικές, και διαδικασίες του οργανισμού, είναι δύσκολο να γίνει διάκριση μεταξύ νόμιμου, κακόβουλου και εσφαλμένου όσον αφορά την πρόσβαση σε εφαρμογές, δεδομένα και συστήματα.

Οι πέντε τύποι εσωτερικής απειλής ανάλογα με τους στόχους καθορίζονται ως:

α) οι απρόσεκτοι εργαζόμενοι που χειρίζονται λάθος δεδομένα, παραβιάζουν τις πολιτικές χρήσης και κάνουν εγκατάσταση μη εξουσιοδοτημένων εφαρμογών ·

β) οι εσωτερικοί πράκτορες που κλέβουν πληροφορίες για λογαριασμό ξένων ·

γ) οι δυσαρεστημένοι υπάλληλοι που επιδιώκουν να βλάψουν τον οργανισμό τους ·

δ) οι κακόβουλοι εσωτερικοί χρήστες που χρησιμοποιούν τα υπάρχοντα δικαιώματα για να κλέψουν πληροφορίες για προσωπικό όφελος

ε) τα άτεχνα τρίτα μέρη που διακυβεύουν την ασφάλεια μέσω ευφυΐας, κακής χρήσης ή κακόβουλης πρόσβασης ή χρήσης ενός περιουσιακού στοιχείου.

Και οι πέντε τύποι εσωτερικών απειλών πρέπει να μελετώνται συνεχώς, ώστε αναγνωρίζοντας την ύπαρξή τους και τον τρόπο λειτουργίας τους να καθορίζεται η στρατηγική του οργανισμού που αφορά την ασφάλεια και την προστασία δεδομένων.

#10 Botnets

Το botnet είναι ένα δίκτυο συνδεδεμένων συσκευών που έχουν μολυνθεί από κακόβουλο λογισμικό bot. Αυτές οι συσκευές χρησιμοποιούνται συνήθως από κακόβουλους παράγοντες για τη διεξαγωγή επιθέσεων Distributed Denial of Service (DDoS)

Το δίκτυο υπολογιστών που έχουν μολυνθεί από το κακόβουλο λογισμικό ρίσκονται υπό τον έλεγχο ενός μόνο επιθετικού μέρους, γνωστού ως "bot-herder". Κάθε μεμονωμένο μηχάνημα υπό τον έλεγχο του bot-herder είναι γνωστό ως bot. Από ένα κεντρικό σημείο, το επιτιθέμενο μέρος μπορεί να διατάξει κάθε υπολογιστή στο botnet του για να πραγματοποιήσει ταυτόχρονα μια συντονισμένη εγκληματική ενέργεια. Η κλίμακα ενός botnet (πολλά από τα οποία αποτελούνται από εκατομμύρια bots) επιτρέπουν στον εισβολέα να εκτελέσει ενέργειες μεγάλης κλίμακας που προηγουμένως ήταν αδύνατες με κακόβουλο λογισμικό. Δεδομένου ότι τα botnets παραμένουν υπό τον έλεγχο ενός απομακρυσμένου εισβολέα, τα μολυσμένα μηχανήματα μπορούν να λαμβάνουν ενημερώσεις και να αλλάζουν τη συμπεριφορά τους εν κινήσει. Ως αποτέλεσμα, οι bot-herders είναι συχνά σε θέση να νοικιάσουν πρόσβαση σε τμήματα του botnet τους στη μαύρη αγορά για σημαντικό οικονομικό όφελος.

Τα κακόβουλα bots, που αναφέρονται ως «κακά bots», όχι μόνο εξελίσσονται συνεχώς, αλλά και οι δεξιότητες των ανθρώπων και το επίπεδο ανάπτυξης των bots γίνονται υψηλά εξειδικευμένες σε ορισμένες εφαρμογές, όπως οι πάροχοι άμυνας. Από διαφορετική οπτική γωνία, τα botnets παρέχουν ένα εργαλείο θα μπορούσαμε να πούμε, για εγκληματίες στον κυβερνοχώρο για την έναρξη διαφόρων λειτουργιών από το e-banking απάτη σε ransomware , εξόρυξη κρυπτονομισμάτων και επιθέσεις DDoS.

#11 Physical manipulation, damage, theft and loss

Η φυσική παραβίαση, η ζημιά, η κλοπή και η απώλεια έχουν αλλάξει δραστικά τα τελευταία χρόνια. Η ακεραιότητα των συσκευών είναι ζωτικής σημασίας για να εξελιχθεί η τεχνολογία και για περισσότερες υλοποιήσεις του Διαδικτύου των Πραγμάτων (IoT). Το διαδίκτυο των πραγμάτων (IoT) μπορεί να ενισχύσει τη φυσική ασφάλεια με πιο προηγμένες και πολύπλοκες λύσεις.

Με αυτόν τον τρόπο, συστήματα που βασίζονται στην ασφάλεια IP με έξυπνους αισθητήρες, Wi-Fi κάμερες, έξυπνος φωτισμός ασφαλείας, drones και ηλεκτρονικές κλειδαριές μπορούν να παρέχουν δεδομένα επιτήρησης που αξιολογούνται από την Τεχνητή Νοημοσύνη (AI) και Μηχανισμοί μηχανικής μάθησης (ML) για τον εντοπισμό απειλών και την αντιμετώπισή τους με ελάχιστη καθυστέρηση και μέγιστη ακρίβεια. Ωστόσο, έξυπνα κτίρια, φορητές συσκευές και έξυπνα φορητά μπορούν να χρησιμοποιηθούν για να παρακάμψουν τα μέτρα ασφαλείας.

Το 2019, οι φυσικές επιθέσεις που σχετίζονται με ATM και POS συνεχίστηκαν στην Ευρώπη και παγκοσμίως, αλλά οι προκύπτουσες απώλειες ήταν χαμηλότερες από το μέσο όρο σε σχέση με το προηγούμενο έτος και την περασμένη δεκαετία. Τα καλά νέα είναι ότι οι εταιρείες, οι διαχειριστές πληροφορικής και οι υπεύθυνοι λήψης αποφάσεων στρέφονται προς την υβριδική

κυβερνοασφάλεια και τη φυσική ασφάλεια αν και στο παρελθόν η φυσική ασφάλεια δεν ήταν προτεραιότητα.

#12 Information leakage

Παραβίαση δεδομένων συμβαίνει όταν δεδομένα, για τα οποία ένα οργανισμός είναι υπεύθυνος, υπόκεινται σε συμβάν ασφαλείας που έχει ως αποτέλεσμα παραβίαση εμπιστευτικότητα, διαθεσιμότητα ή ακεραιότητα. Μια παραβίαση δεδομένων προκαλεί συχνά μια διαρροή πληροφοριών, η οποία αποτελεί μία από τις σημαντικότερες απειλές στον κυβερνοχώρο. Όταν αναφερόμαστε σε παραβιασμένες πληροφορίες αναφερόμαστε σε προσωπικές πληροφορίες, προσωπικά οικονομικά δεδομένα που αποθηκεύονται σε υποδομές πληροφορικής πληροφορίες υγείας (PHI) και φυλάσσονται στα αποθετήρια των παρόχων υγειονομικής περίθαλψης.

Όταν παρατηρούνται παραβιάσεις ασφαλείας στους τίτλους των δελτίων, ιστολόγια, εφημερίδες και τεχνικές αναφορές, η στόχευση είναι κυρίως είτε από αντιπάλους ή από την καταστροφική αποτυχία των διαδικασιών της κυβερνοάμυνας και των τεχνικών. Παρ' όλα αυτά, η αδιαμφισβήτητη αλήθεια είναι ότι, παρά τις επιπτώσεις ή το πεδίο εφαρμογής ενός τέτοιου γεγονότος, η παραβίαση προκαλείται συνήθως από τη δράση ενός ή πολλών ατόμων ή από αποτυχία της οργανωτικής διαδικασίας.

#13 Ransomware

Το Ransomware έχει γίνει ένα δημοφιλές όπλο στα χέρια κακόβουλων φορείς που προσπαθούν να βλάψουν κυβερνήσεις, επιχειρήσεις και ιδιώτες σε καθημερινή βάση. Σε τέτοιες περιπτώσεις, το θύμα ransomware μπορεί να υποφέρει από οικονομικές απώλειες είτε με την καταβολή των απαιτούμενων λύτρων είτε με την καταβολή του κόστους που ανέρχεται από την απώλεια, εάν δεν συμμορφώνονται με τα αιτήματα των επιτιθέμενων.

Σε ένα περιστατικό το 2019, στη Βαλτιμόρη, το Μέριλαντ υπέστη λουκέτο και αναμένεται να πληρώσει 18,2 εκατομμύρια δολάρια ΗΠΑ (περίπου 15,4 εκατομμύρια ευρώ) (αν και η πόλη αρνήθηκε να πληρώσει τα λύτρα.)

Με τον αυξανόμενο αριθμό των περιστατικών, είναι προφανές ότι το να γίνεις θύμα δεν είναι ένα «αν» αλλά μάλλον το «πότε». Ωστόσο, στην πλειοψηφία των αγώνων των χωρών ενάντια στο ransomware, πρέπει να αντιμετωπιστούν διάφορες προκλήσεις, όπως π.χ. η έλλειψη συντονισμού και συνεργασίας μεταξύ φορέων και αρχών, η έλλειψη νομοθεσίας, που σαφώς ποινικοποιεί επιθέσεις ransomware. Αν και υπάρχουν ασφαλιστήρια συμβόλαια στον κυβερνοχώρο από τις αρχές του 2002 , ransomware οι επιθέσεις είναι ένας από τους κύριους λόγους για το αυξημένο ενδιαφέρον για αυτόν τον τύπο ασφάλισης τα τελευταία 5 χρόνια. Σε μερικά από τα περιστατικά του 2019, τα λύτρα ή το κόστος ανάκτησης καλύφθηκε από τέτοιες συμβάσεις. Δυστυχώς, εάν είναι γνωστό ότι είναι ασφαλισμένοι οι πιθανοί στόχοι ransomware, οι επιτιθέμενοι υποθέτουν ότι πιθανότατα θα πληρωθούν. Άλλο μειονέκτημα για το θύμα είναι ότι οι ασφαλιστικοί φορείς πληρώνουν λύτρα εκ των προτέρων για τον μετριασμό της ζημιάς και να διατηρήσουν τη φήμη

του θύματος ανέπαφη. Ωστόσο, μια τέτοια συμμόρφωση με την καταβολή λύτρων ενθαρρύνει την κοινότητα των χάκερ και δεν εξασφαλίζει ούτε το θύμα ούτε και την ανάκαμψη στη φήμη του.

#14 Cyberespionage

Η κατασκοπεία στον κυβερνοχώρο θεωρείται ταυτόχρονα απειλή και κίνητρο εγχειριδίου για την κυβερνοασφάλεια. Ορίζεται ως «η χρήση δικτύων υπολογιστών να αποκτήσουν παράνομη πρόσβαση σε εμπιστευτικές πληροφορίες, συνήθως αυτές που διατηρούνται από την κυβέρνηση ή άλλη οργάνωση. Το 2019, πολλές αναφορές αποκάλυψαν ότι οι παγκόσμιοι οργανισμοί σκέφτονται στον κυβερνοχώρο την κατασκοπεία (ή κατασκοπεία που υποστηρίζεται από το έθνος-κράτος) ως μια αυξανόμενη απειλή η οποία επηρεάζει τους βιομηχανικούς τομείς, καθώς και τις κρίσιμες και στρατηγικές υποδομές σε όλο τον κόσμο, συμπεριλαμβανομένων των κυβερνητικών υπουργείων, των σιδηροδρόμων, τους τηλεπικοινωνιακούς παρόχους, τις εταιρείες ενέργειας, τα νοσοκομεία και τράπεζες. Η κατασκοπεία στον κυβερνοχώρο επικεντρώνεται στην οδήγηση της γεωπολιτικής και στην κλοπή από την πολιτεία εμπορικών μυστικών, δικαιώματα πνευματικής ιδιοκτησίας και πληροφορίες για στρατηγικούς τομείς. Κινητοποιεί επίσης παράγοντες από την οικονομία, τη βιομηχανία και ξένες υπηρεσίες πληροφοριών καθώς και παράγοντες που εργάζονται για λογαριασμό τους. Σε μια πρόσφατη έκθεση, οι αναλυτές της απειλής πληροφοριών δεν έμειναν έκπληκτοι όταν έμαθαν ότι το 71% των οργανώσεων αντιμετωπίζει την κατασκοπεία στον κυβερνοχώρο και άλλες απειλές ως «μαύρο κουτί» και εξακολουθούν να μαθαίνουν γι ’αυτά.

Το 2019, ο αριθμός των κυβερνοεπιθέσεων που χρηματοδοτούνται από τα έθνη-κράτη αυξήθηκαν και είναι πιθανό να συνεχιστούν. Αναλυτικά, επιθέσεις που υποστηρίζονται από τα έθνη-κράτη και άλλες επιθέσεις εναντίον των εχθρών στο Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) αυξάνονται στα βοηθητικά προγράμματα, στο πετρέλαιο και στο φυσικό αέριο (ONG) και στους τομείς της μεταποίησης. Επιπλέον, κυβερνοεπιθέσεις που διενεργήθηκαν από ομάδες προηγμένων επίμονων απειλών (APT) το δείχνουν αυτό. Οι οικονομικές επιθέσεις συχνά υποκινούνται από κατασκοπεία. Χρησιμοποιώντας τακτικές, τεχνικές και διαδικασίες (TTP) παρόμοιες με αυτές της κατασκοπείας, αντίστοιχες ομάδες, όπως ο όμιλος Cobalt, το Carbanak και το FIN7 φέρεται να έχουν στοχοποιήσει με επιτυχία μεγάλα χρηματοπιστωτικά ιδρύματα και αλυσίδες εστιατορίων.

Η Επιτροπή Εξωτερικών Υποθέσεων του Ευρωπαϊκού Κοινοβουλίου πρότεινε στα κράτη μέλη να συστήσουν μονάδα κυβερνοάμυνας και να συνεργαστούν για την κοινή τους άμυνα. Δήλωσε ότι *«το στρατηγικό περιβάλλον της Ένωσης έχει επιδεινωθεί ... προκειμένου να αντιμετωπίσει τις πολλαπλές προκλήσεις που επηρεάζουν άμεσα ή έμμεσα την ασφάλεια των κρατών μελών της, τα κράτη μέλη και τους πολίτες τους· λαμβάνοντας υπόψη ότι τα ζητήματα που επηρεάζουν την ασφάλεια των πολιτών της Ε.Ε. περιλαμβάνουν: ένοπλες συγκρούσεις στα ανατολικά και νότια της ευρωπαϊκής ήπειρου και στα εύθραυστα κράτη· τρομοκρατία – και ιδίως Τζιχάντ –, κυβερνοεπιθέσεις και εκστρατείες παραπληροφόρησης·και ξένη παρέμβαση στις ευρωπαϊκές πολιτικές και εκλογικές διαδικασίες»*.

Παράγοντες που υποκινούνται από οικονομικό, πολιτικό ή ιδεολογικό κέρδος θα εστιάζουν όλο και περισσότερο στις επιθέσεις σε δίκτυα προμηθευτών με αδύναμη ασφάλεια στον κυβερνοχώρο.

#15 Cryptojacking

Το Cryptojacking (γνωστό και ως cryptomining) είναι η μη εξουσιοδοτημένη χρήση των πόρων της συσκευής για εξόρυξη κρυπτονομισμάτων. Οι στόχοι περιλαμβάνουν οποιοδήποτε συνδεδεμένη συσκευή, όπως υπολογιστές και κινητά τηλέφωνα ·ωστόσο, οι εγκληματίες στον κυβερνοχώρο στοχεύουν όλο και περισσότερο τις υποδομές cloud Αυτός ο τύπος επίθεσης δεν έχει προκαλέσει την προσοχή του νόμου αφού σπάνια αναφέρονται , εξαιτίας των σχετικά λίγων αρνητικών συνεπειών τους. Παρ 'όλα αυτά, οι οργανισμοί μπορεί να παρατηρήσουν υψηλότερο κόστος πληροφορικής, υποβαθμισμένα εξαρτήματα υπολογιστών, αυξημένη κατανάλωση ηλεκτρικής ενέργειας και μειωμένη παραγωγικότητα των εργαζομένων που προκαλείται από πιο αργούς σταθμούς εργασίας.

Στην ένατη έκθεση του ο ENISA επισημαίνει ότι όσον αφορά τις τάσεις, κατά την περίοδο αναφοράς (Απρίλιο 2020-Απρίλιο 2021) αναφέρονται τα εξής:

- Το Ransomware έχει αξιολογηθεί ως η πρωταρχική απειλή για την περίοδο 2020-2021.
- Οι κυβερνητικές οργανώσεις έχουν εντείνει το παιχνίδι τους τόσο σε εθνικό όσο και σε διεθνές επίπεδο.
- Οι εγκληματίες του κυβερνοχώρου παρακινούνται όλο και περισσότερο από τη δημιουργία εσόδων από τις δραστηριότητές τους, π.χ. ransomware.
- Το κρυπτονόμισμα παραμένει η πιο κοινή μέθοδος πληρωμής για τους παράγοντες απειλής.
- Η μείωση του κακόβουλου λογισμικού που παρατηρήθηκε το 2020 συνεχίζεται και κατά τη διάρκεια του 2021. Το 2021, είδαμε αύξηση των απειλών που καταφεύγουν σε σχετικά νέες ή ασυνήθιστες γλώσσες προγραμματισμού για να μεταδώσουν στον κώδικά τους.
- Ο όγκος των μολύνσεων από cryptojacking έφθασε σε πρωτοφανή υψηλά επίπεδα το πρώτο τρίμηνο του 2021, σε σύγκριση με τα τελευταία χρόνια. Το οικονομικό κέρδος που συνδέεται με την κρυπτογράφηση παρακινεί τους παράγοντες για επιθέσεις.
- Ο COVID-19 εξακολουθεί να είναι το κυρίαρχο δέλεαρ στις καμπάνιες για επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου.
- Σημειώθηκε αύξηση των παραβιάσεων δεδομένων που σχετίζονται με τον τομέα της υγειονομικής περίθαλψης.
- Οι παραδοσιακές καμπάνιες DDoS (Κατανεμημένη Άρνηση Υπηρεσίας) το 2021 είναι πιο στοχευμένες, πιο επίμονες και όλο και περισσότερο πολυτομεακές. Το IoT (Διαδίκτυο των Πραγμάτων) σε συνδυασμό με τα δίκτυα κινητής τηλεφωνίας σε ένα νέο κύμα επιθέσεων DDoS.
- Το 2020 και το 2021, παρατηρούμε αύξηση των μη κακόβουλων περιστατικών, καθώς η πανδημία COVID-19 πολλαπλασίασε τα ανθρώπινα σφάλματα και τις εσφαλμένες ρυθμίσεις του συστήματος, μέχρι το σημείο που οι περισσότερες το 2020 προκλήθηκαν από σφάλματα.

Κατά την επόμενη δεκαετία, η ασφάλεια στον κυβερνοχώρο θα γίνει όλο και πιο δύσκολο να εκτιμηθεί και ερμηνευτεί λόγω της αυξανόμενης πολυπλοκότητας του απειλητικού τοπίου.

ΚΕΦΑΛΑΙΟ 3

3.1 Κοινωνικές και Ψυχολογικές Επιπτώσεις

Οι επιθέσεις στον κυβερνοχώρο έχουν γίνει πλέον πολύ συνηθισμένες. Οι αναφορές σε αυτές τις επιθέσεις γίνονται ολοένα και πιο πολλές, στα μέσα ενημέρωσης αλλά και σε ακαδημαϊκά άρθρα που επισημαίνουν την ποικιλία και διαφορετικότητα των επιθέσεων και των εγκλημάτων στον κυβερνοχώρο. Συγκεκριμένα θα πρέπει να αντιληφθούμε και να κατανοήσουμε πως επηρεάζονται τα άτομα μετά από μια επίθεση στον κυβερνοχώρο. Η έρευνα που επικαλούμαστε επικεντρώνεται σε βασικά ζητήματα που σχετίζονται με την κατανόηση των συμβάντων αλλά και της αντίληψης του κινδύνου, τα κίνητρα, τα χαρακτηριστικά του εισβολέα (π.χ. ταυτότητα επιτιθέμενου, ταυτότητα στόχου και κλίμακα επίθεσης).

Είναι αδιαμφισβήτητος ο αντίκτυπος του κυβερνοχώρου στο κοινωνικό σύνολο. Παρέχει στιγμιαία επικοινωνία μέσω πλατφορμών, ηλεκτρονικό εμπόριο και μεγάλη αλληλεπίδραση μεταξύ ατόμων αλλά και διαφόρων οργανώσεων. Όμως καθώς ο κυβερνοχώρος έχει αυξηθεί, το ίδιο ισχύει και για τον αριθμό και την ποικιλία των κυβερνοεπιθέσεων.

Τις κυβερνοεπιθέσεις τις ορίζουμε ως γεγονότα που θέτουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα ή τη διαθεσιμότητα ενός οργανισμού. Αυτές οι επιθέσεις αφορούν hacking και άρνηση παροχής υπηρεσιών (DoS), ransomware και μολύνσεις spyware και μπορούν να επηρεάσουν όλους μέχρι και τις κρίσιμες εθνικές υποδομές μιας χώρας.

Έρευνες έχουν δείξει ότι το κοινό είναι πιο πιθανό να ανταποκριθεί στις επιπτώσεις μια κυβερνοεπίθεσης παρά στην ίδια την επίθεση. Ως παράδειγμα αυτού είναι η επίθεση κακόβουλου λογισμικού που μολύνει έναν εθνικό σταθμό παραγωγής ενέργειας και προκαλεί προβλήματα σε χιλιάδες πολίτες. Εδώ λοιπόν η επίθεση του κακόβουλου λογισμικού μπορεί να μην εστιάζεται στο κοινό, δηλαδή να μην έχει ως παραλήπτες το κοινό, έμμεσα όμως δεν υπάρχει θέρμανση, δεν μπορείς να προετοιμάσεις φαγητό και όλα όσα επακολουθούν από την έλλειψη ενέργειας.

Οι βασικοί τομείς που θα εξεταστούν για να μπορέσουμε να έχουμε μια πλήρη αποτύπωση είναι οι κοινωνικές και ψυχολογικές επιπτώσεις (συναισθηματικές και συμπεριφορικές). Ο κοινωνικός αντίκτυπος μιας επίθεσης στον κυβερνοχώρο αναφέρεται σε πτυχές όπως η κοινωνική διαταραχή που προκαλείται στην καθημερινή ζωή των ανθρώπων και σε ζητήματα όπως το άγχος, η απώλεια εμπιστοσύνης στο κυβερνοχώρο και κατ επέκταση στην τεχνολογία. Οι ψυχολογικές επιπτώσεις περιλαμβάνουν προσωπικές πτυχές όπως θυμό, οργή, κατάθλιψη.

Κάποια θέματα που θα εξεταστούν είναι η αντίληψη κινδύνου, κουλτούρα του φόβου, κίνητρο προστασίας. Επίσης θα εξεταστεί η ταυτότητα του δράστη και η κλίμακα της ηλεκτρονικής επίθεσης.

Ένα σημαντικό στοιχείο της έρευνας είναι οι πεποιθήσεις δηλαδή η αντίδραση του χρήστη γενικά με την ασφάλεια αλλά και εάν θα εφαρμόσει μηχανισμούς ασφάλειας εάν του δοθεί η ευκαιρία.

Εξαρτάται λοιπόν από τις πεποιθήσεις του, σχετικά με την σοβαρότητα ενός γεγονότος, την ευαισθησία στην απειλή, η αντιληπτή αυτό-αποτελεσματικότητα, το κόστος και η αποτελεσματικότητα των προληπτικών ή ελαφρυντικών συμπεριφορών. Αυτοί λοιπόν οι παράγοντες καθιστούν δύσκολο το κίνητρο προστατευτικών πρακτικών (συμπεριφορών) ασφάλειας στον κυβερνοχώρο καθώς και την πρόβλεψη κοινωνικών και ψυχολογικών αντιδράσεων του κοινού σε μια κυβερνοεπίθεση. Αυτό μπορεί να αφορά οποιαδήποτε μορφή επίθεσης όπως οι κίνδυνοι στον κυβερνοχώρο του Internet of Things ή την Τεχνητή Νοημοσύνη.

Ένα άλλο στοιχείο που αποτελεί σημαντικό παράγοντα και που σχετίζεται με το έγκλημα και τις εκδηλώσεις του είναι η γενική κουλτούρα του φόβου. Ο φόβος του εγκλήματος μπορεί να ωθήσει τους ανθρώπους να αλλάξουν την συμπεριφορά τους. Σε ατομικό επίπεδο, οι άνθρωποι ανταποκρίνονται γενικά στον φόβο του εγκλήματος υιοθετώντας προστατευτική συμπεριφορά ή συμπεριφορά αποφυγής. Ο ψυχολογικός φόβος μπορεί να οδηγήσει σε έντονο άγχος και φόβο για το έγκλημα που δεν είναι ρεαλιστικό. Αυτό το φαινόμενο μπορεί να έχει σχέση με το έγκλημα και κατ' επέκταση σε κυβερνοεπιθέσεις και εγκλήματα στον κυβερνοχώρο.

Όσον αφορά τις αντιδράσεις του κοινού σε επιθέσεις και σε διαδικτυακά εγκλήματα σε ξεχωριστό κεφάλαιο, θα αναφερθούμε σε δύο σενάρια πραγματικής επίθεσης στον κυβερνοχώρο που έλαβαν χώρο το 2017: η παγκόσμια επίθεση WannaCry και η επίθεση στη Lloyds Banking Group. Επιδίωξη μέσα από την αναφορά σε αυτές τις επιθέσεις είναι να γίνουν αντιληπτές οι ψυχολογικές επιπτώσεις σε ατομικό επίπεδο αλλά και στην ευρύτερη κοινωνία. Ουσιαστικά αυτή η ανάλυση έχει ως σκοπό να αντιληφθούμε τις απειλές στον κυβερνοχώρο από την οπτική γωνία της κυβερνοψυχολογίας.

3.2. Παράγοντες που επηρεάζουν τις αντιλήψεις του κινδύνου και τις αντιδράσεις στον κίνδυνο

Το κίνητρο ενός χρήστη για να αντιδράσει στον αντιληπτό κίνδυνο αλλά και να εφαρμόσει μέτρα ασφαλείας εξαρτάται από τις πεποιθήσεις του όσον αφορά την σοβαρότητα ενός γεγονότος, την ευαισθησία στην απειλή, την αντιληπτή αυτό-αποτελεσματικότητα , το κόστος και την αποτελεσματικότητα των προληπτικών ή ελαφρυντικών συμπεριφορών. Επίσης, η γενική κουλτούρα του φόβου μπορεί να οδηγήσει τους ανθρώπους να αλλάξουν την συμπεριφορά τους.

Έρευνα στην δημόσια αντίληψη του κινδύνου καταδεικνύει ότι υπάρχουν πιθανοί παράγοντες που μπορούν να επηρεάσουν τα δημόσια επίπεδα του αντιληπτού κινδύνου όπως το εάν η έκθεση στον κίνδυνο αντιλαμβάνεται ως : (i) εθελοντική (αποδοχή αυξημένου κινδύνου μέσω επικίνδυνων διαδικτυακών δραστηριοτήτων), (ii) οικεία (λόγω την συχνότητας στα μέσα ενημέρωσης) ή άγνωστη (έλλειψη κατανόησης των αιτιών και συνέπειες), (iii) ελεγχόμενη ή ανεξέλεγκτη (iv) δίκαιη (τυχαία) ή άδικη (στοχευμένη) και (v) εάν ο κίνδυνος προκαλεί φόβο ή όχι.

Επιπρόσθετα, προτείνεται η στάση, η ευαισθησία στον κίνδυνο και ο συγκεκριμένος φόβος και πως θα μπορούσαν να χρησιμοποιηθούν ως επεξηγηματικές μεταβλητές για την αντίληψη του κινδύνου Στο άρθρο των Nurse et al. (2011) αποτυπώνεται περαιτέρω ότι τα πρόσωπα χρησιμοποιούν τέσσερις κύριες διαστάσεις για να κρίνουν τους διαδικτυακούς κινδύνους, δηλαδή

1. την ικανότητα ελέγχου ή αποφυγής του κινδύνου,
2. τον φόβο των συνεπειών,
3. την έλλειψη εξοικειώσεων των κινδύνων και
4. την αμεσότητα των συνεπειών/επιπτώσεων.

Οι πολίτες αναγνωρίζουν την απειλή των κυβερνοεπιθέσεων, αλλά τα μέτρα που λαμβάνουν για την αντιμετώπιση αυτής της απειλής ποικίλλουν. Οι άνθρωποι αντιδρούν στον κίνδυνο με διαφορετικούς τρόπους με βάση τη διπλή επεξεργασία πληροφοριών. Μερικοί αντιδρούν με βάση τη λογική, αναλύοντας τον κίνδυνο και άλλοι μπορεί να αντιδράσουν ενστικτωδώς με βάση τα συναισθήματα για τον κίνδυνο . Τα συναισθήματα μπορούν επίσης να χρησιμεύσουν ως προβολέας για την καθοδήγηση της προσοχής μας αλλά και για την παροχή κινήτρων στα άτομα να δράσουν. Για παράδειγμα, οι άνθρωποι μπορούν να αποφασίσουν να δράσουν σχετικά με τους κινδύνους που σχετίζονται με τις τεχνολογίες με βάση τα συναισθήματά τους.

Άλλοι συγγραφείς προτείνουν ότι, τόσο οι εμπειρογνώμονες όσο και τα μέλη του κοινού ενδέχεται να συγχέουν τα γεγονότα με την ατομική ερμηνεία τους, επειδή οι αντιλήψεις για τον κίνδυνο βασίζονται συχνά στην ερμηνεία των γεγονότων, τα οποία τροφοδοτούνται από ατομική κρίση, αξίες, πεποιθήσεις και στάσεις. Οι Blythe & Camp (2012) υποστήριξαν ότι συνολικά, το κίνητρο ενός χρήστη να εφαρμόσει μηχανισμούς ασφαλείας εξαρτάται από τις πεποιθήσεις του σχετικά με την ευαισθησία του σε εξωγενείς απειλές ασφαλείας, τη δυνητική σοβαρότητά τους , το κόστος και την αποτελεσματικότητα προληπτικών ή ελαφρυντικών συμπεριφορών.

Οι αποφάσεις και οι συμπεριφορές ασφαλείας εκτελούνται σε έναν κόσμο κινδύνου και αβεβαιότητας. Ο Adams (2013) εξηγεί την έννοια της αντιστάθμισης κινδύνου παρουσιάζοντας τον θερμοστάτη κινδύνου. Ισχυρίζεται ότι τα άτομα εκτελούν μια συμπεριφορά εξισορρόπησης μεταξύ της τάσης τους να αναλαμβάνουν κινδύνους (διάθεση κινδύνου) και του αντιληπτού κινδύνου (αντίληψη κινδύνου), όπου η τάση κινδύνου καθορίζεται από αντιληπτές ανταμοιβές, ενώ τα ατυχήματα (αρνητικές εμπειρίες) επηρεάζουν τον αντιληπτό κίνδυνο.

Η εμπιστοσύνη έχει αναγνωριστεί ως βασικό ζήτημα που επηρεάζει τις αντιλήψεις του κοινού για τον κίνδυνο. Το επίπεδο εμπιστοσύνης σε ένα οργανωτικό όργανο που είναι υπεύθυνο για την αντιμετώπιση του κινδύνου θα πρέπει να εξεταστεί τόσο κατά τη διάρκεια των διαδικασιών χάραξης πολιτικής όσο και των διαδικασιών επικοινωνίας. Για παράδειγμα, μια έκθεση της Symantec (2010) έδειξε ότι σχεδόν 9 στους 10 ενήλικες εξετάζουν το έγκλημα στον κυβερνοχώρο και πάνω από το ένα τέταρτο αναμένουν πραγματικά να εξαπατηθούν στο διαδίκτυο. Ωστόσο, παρά την καθολική απειλή και τη συχνότητα εμφάνισης εγκλήματος στον κυβερνοχώρο, μόνο οι μισοί ενήλικες στη μελέτη ισχυρίζονται ότι θα άλλαζαν τον τρόπο που συμπεριφέρονται στο διαδίκτυο αν γίνουν θύματα.

Προκειμένου λοιπόν να είναι επιτυχείς οι προσπάθειες ευαισθητοποίησης των ατόμων, οι υπεύθυνοι χάραξης πολιτικής πρέπει να κατανοήσουν τον τρόπο με τον οποίο οι άνθρωποι σκέφτονται και ανταποκρίνονται σε επιθέσεις κινδύνου και υλοποιημένων επιθέσεων.

Η αυτο-αποτελεσματικότητα θεωρείται όχι ως δεξιότητα αλλά ως η αξιολόγηση του τι μπορεί κανείς να κάνει με τις δεξιότητες. Εξετάζει την πίστη ενός ατόμου στον εαυτό του και τις ικανότητές του. Αυτό αφορά ζητήματα όπως οι κυβερνοεπιθέσεις, επειδή είναι σημαντικό τα άτομα να πιστεύουν ότι έχουν πιθανότητες να προστατευτούν και να ανταποκριθούν με επιτυχία σε ένα περιστατικό επίθεσης.

Εισήχθη μια νέα έννοια σχετικά με τη σχέση μεταξύ της αυτο-αποτελεσματικότητας και του αντιληπτού ελέγχου συμπεριφοράς. Υποστηρίχθηκε ότι «η κεντρική έννοια του αντιληπτού ελέγχου συμπεριφοράς αποτελείται από δύο παράγοντες: την αυτο-αποτελεσματικότητα (σχετικά με την ευκολία / δυσκολία εκτέλεσης μιας συμπεριφοράς) και την ικανότητα ελέγχου (ο βαθμός στον οποίο η απόδοση εξαρτάται αποκλειστικά από το άτομο)». Όταν τα άτομα είναι σε θέση να καθορίσουν ή να επηρεάσουν τι τους συμβαίνει ή τι θα τους συμβεί, αυτά τα άτομα θεωρούνται ότι "είναι υπό έλεγχο". Ο έλεγχος είναι μια κεντρική κατασκευή στην ψυχολογία και το να είσαι υπό έλεγχο είναι μια παγκόσμια επιθυμητή κατάσταση ύπαρξης για τους περισσότερους ανθρώπους. Η ίδια πραγματικότητα ισχύει και στον διαδικτυακό κόσμο, γενικά και μπροστά σε ένα κύμα αναδυόμενων κυβερνοεπιθέσεων.

Σύμφωνα με τη Θεωρία Κινήτρων Προστασίας (PMT), οι περιβαλλοντικοί και προσωπικοί παράγοντες συνδυάζονται για να αποτελέσουν πιθανή απειλή.

Η απειλή ξεκινά δύο γνωστικές διαδικασίες: **εκτίμηση απειλής** και **εκτίμηση αντιμετώπισης**.

Η διαδικασία εκτίμησης της απειλής αξιολογεί τους παράγοντες που σχετίζονται με τη συμπεριφορά που ενδεχομένως δημιουργεί κίνδυνο, συμπεριλαμβανομένων των εγγενών και εξωγενών ανταμοιβών που συνοδεύουν τις ενέργειες, τη σοβαρότητα του κινδύνου και την ευπάθεια κάποιου στην απειλή.

Η διαδικασία αξιολόγησης της αντιμετώπισης αξιολογεί την ικανότητα κάποιου να αντιμετωπίσει και να αποτρέψει τον απειλούμενο κίνδυνο (αυτο-αποτελεσματικότητα και αποτελεσματικότητα ανταπόκρισης), ισορροπημένο με το κόστος (ή τις προσπάθειες) που σχετίζονται με την προστατευτική συμπεριφορά (κόστος απόκρισης).

Η εκτίμηση της απειλής αναφέρεται στο πόσο επιρρεπής αισθάνεται κανείς σε μια απειλή.

Για παράδειγμα, πόσο ευάλωτο είναι ένα άτομο από τη δυνατότητα να πέσει θύμα μιας κυβερνοεπίθεσης όπως το phishing. φυσικά, η ευαισθησία σε επιθέσεις ηλεκτρονικού "ψαρέματος" επηρεάζεται από μια σειρά άλλων πτυχών. Η αξιολόγηση της αντιμετώπισης αξιολογεί τους διάφορους παράγοντες που είναι πιθανό να διασφαλίσουν ότι κάποιος συμμετέχει σε μια συνιστώμενη απάντηση που είναι προληπτικής φύσης. Για παράδειγμα, μην ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από άγνωστο αποστολέα ή αναξιόπιστες ή ύποπτες διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Ως εκ τούτου, η θεωρία λέει ότι για να υιοθετήσει ένα άτομο μια ασφαλή συμπεριφορά, πρέπει να πιστέψει ότι υπάρχει σοβαρή απειλή που είναι πιθανό να συμβεί και ότι υιοθετώντας ασφαλείς ενέργειες, μπορεί να μειώσει αποτελεσματικά την απειλή. Το άτομο θα πρέπει επίσης να είναι πεπεισμένο ότι είναι σε θέση να εμπλακεί.

Η μέτρηση της «πρόθεσης» συμμετοχής στη συνιστώμενη προληπτική δραστηριότητα είναι η συνηθέστερη ένδειξη κινήτρων προστασίας.

Μια άλλη βασική πτυχή της κατανόησης της δημόσιας αντίδρασης σε κακόβουλες κυβερνοεπιθέσεις επικεντρώνεται στο γεγονός ότι οι πολίτες δεν φαίνεται να αντιλαμβάνονται τέτοιες επιθέσεις ως απειλή για τον εαυτό τους και, αν το κάνουν, πιστεύουν ότι υπάρχουν πολύ λίγα που μπορούν να κάνουν για να αποτρέψουν μια τέτοια επίθεση. Αντίθετα, το κοινό είναι πιο πιθανό να ανταποκριθεί στο γεγονός (π.χ. απώλεια υπηρεσιών), παρά στην ίδια την κυβερνοεπίθεση. Οι αντιλήψεις για το τι περιμένουν οι άλλοι ή πώς αντιδρούν οι άλλοι σε μια απειλή είναι πτυχές και των δύο τύπων αξιολόγησης.

Αυτοί οι παράγοντες καθιστούν δύσκολο να συναγάγουμε κοινωνικές και ψυχολογικές απαντήσεις σε μια κυβερνοεπίθεση. Εάν ερμηνεύσουμε κακόβουλες κυβερνοεπιθέσεις μέσω του φακού του PMT, η τρέχουσα κατάσταση της κατανόησης από το κοινό του δυνητικού αντίκτυπου ενός τέτοιου γεγονότος θα μπορούσε ενδεχομένως να περιγραφεί σε υψηλά επίπεδα εκτίμησης απειλής, χαμηλά επίπεδα αυτο-αποτελεσματικότητας, σύγχυση σχετικά με την αποτελεσματικότητα απόκρισης και υψηλό κόστος απόκρισης λόγω της αντιληπτής δυσκολίας λήψης μέτρων ασφαλείας.

3.3 Κέντρο Ελέγχου

Μια άλλη θεωρία που μπορεί να χρησιμοποιηθεί για να περιγράψει συναισθηματικές και συμπεριφορικές απαντήσεις σε ένα διαδικτυακό περιστατικό είναι αυτή του Κέντρου ελέγχου. Ο τύπος ελέγχου έχει ως στόχο να χαρακτηρίσει εάν οι άνθρωποι αισθάνονται ότι έχουν ισχυρό έλεγχο της ζωής τους (εσωτερικό έλεγχο) ή αν πρέπει να βασίζονται σε εξωτερικές δυνάμεις (εξωτερικός έλεγχος). Ο έλεγχος φαίνεται να επηρεάζει τη μάθηση, τα κίνητρα και τη συμπεριφορά του ατόμου.

Τα άτομα με εσωτερικό έλεγχο αισθάνονται ότι η επιτυχία ή η αποτυχία οφείλεται στις προσπάθειες ή τις ικανότητές τους. Εναλλακτικά, τα άτομα με εξωτερικό έλεγχο είναι πιθανό να πιστεύουν ότι άλλοι παράγοντες όπως η τύχη ή η δυσκολία του στόχου ή οι ενέργειες άλλων ανθρώπων είναι η αιτία της επιτυχίας ή της αποτυχίας. Για παράδειγμα, οι χρήστες με εξωτερικό χώρο ελέγχου ενδέχεται να μην λαμβάνουν συχνά προστατευτικά μέτρα κατά των επιθέσεων στον κυβερνοχώρο λόγω της πεποίθησής τους ότι οι πάροχοι Διαδικτύου ή η κυβέρνηση είναι υπεύθυνοι για τη διασφάλιση ενός ασφαλέστερου Διαδικτύου. Η έλλειψη ελέγχου σε μια κατάσταση που θεωρείται απειλητική ή επικίνδυνη μπορεί να προκαλέσει συναισθήματα συναισθηματικής δυσφορίας, φόβου και ανασφάλειας. Τέτοια ισχυρά συναισθήματα μπορούν μερικές φορές να οδηγήσουν σε παράλογη συμπεριφορά ή άλλες εξίσου ισχυρές αντιδράσεις. **Όλες αυτές είναι**

πτυχές που μπορούν να επηρεάσουν τον τρόπο με τον οποίο το κοινό (ψυχολογικά) και η κοινωνία γενικά (κοινωνικά) θα ανταποκριθούν σε μια επίθεση.

3.4. Μοντέλο εκτεταμένης παράλληλης διαδικασίας

Όπως και το PMT, το μοντέλο εκτεταμένης παράλληλης διαδικασίας υποδηλώνει ότι όταν η αντιληπτή απειλή είναι χαμηλή, ανεξάρτητη από το επίπεδο της αντιληπτής αποτελεσματικότητας απόκρισης, μπορεί να μην υπάρχει περαιτέρω επεξεργασία του μηνύματος. Έτσι, δεν υπάρχει αντίδραση στην επίκληση του φόβου, διότι η απειλή δεν υπόκειται σε περαιτέρω επεξεργασία. Επίσης, το Μοντέλο προτείνει ότι καθώς η αντιληπτή απειλή αυξάνεται ενώ το αντίθετο αποτέλεσμα είναι υψηλό, η αποδοχή μιας προληπτικής συμβουλής θα αυξηθεί επίσης. Σε τέτοιες περιπτώσεις, τα άτομα μπορούν να συνειδητοποιήσουν ότι διατρέχουν κίνδυνο σοβαρής απειλής και έχουν κίνητρο να προστατευθούν. Θεωρούν ότι μπορούν να αποτρέψουν τον κίνδυνο (υψηλή αποτελεσματικότητα)· και μπορεί σκόπιμα και γνωστικά να αναλάβουν δράση για την αντιμετώπιση του κινδύνου. Οι επικλήσεις φόβου με υψηλά επίπεδα απειλής και υψηλά επίπεδα αποτελεσματικότητας παράγουν αποδοχή μιας προτεινόμενης συμπεριφοράς.

Οι γνωστικές διαδικασίες που λαμβάνουν χώρα κατά τη διάρκεια των διαδικασιών ελέγχου κινδύνου ενεργοποιούν ενέργειες προσαρμογής όπως στάσεις, προθέσεις ή αλλαγές συμπεριφοράς που ελέγχουν τον κίνδυνο. Ωστόσο, καθώς η αντιληπτή απειλή αυξάνεται ενώ η αντιληπτή αποτελεσματικότητα είναι χαμηλή, τα άτομα θα κάνουν το αντίθετο από αυτό που προτείνεται. Υπάρχει το επιχείρημα ότι για να ελέγξει τον αφόρητο φόβο μιας κατάστασης χαμηλής αντιληπτής αποτελεσματικότητας, ένα άτομο είτε συνειδητά είτε ασυνείδητα, τείνει να αρνηθεί την απειλή ή να αντιδράσει ενάντια στην προτεινόμενη προληπτική συμπεριφορά και να εκτελέσει ακόμα πιο επικίνδυνη συμπεριφορά για να μειώσει το φόβο ή το άγχος. Αυτό μπορεί να σχετίζεται τόσο με το περιβάλλον εκτός σύνδεσης όσο και με το διαδικτυακό περιβάλλον. Συνολικά, όταν η σοβαρότητα της απειλής είναι υψηλή, σε συνδυασμό με χαμηλή αποτελεσματικότητα, τότε οι άνθρωποι μπορεί να τείνουν να απορρίπτουν τις προτεινόμενες ενέργειες ή οδηγούνται σε αντιδράσεις μπούμερανγκ.

Αυτά δείχνουν περαιτέρω έρευνες σχετικά με την αποτελεσματικότητα των εκστρατειών ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο, η οποία συχνά οδηγεί σε αποτυχία αλλαγής συμπεριφοράς. Επιπλέον, όταν η αντιληπτή αποτελεσματικότητα είναι μέτρια, το κρίσιμο σημείο μπορεί να μην συμβεί άμεσα, αλλά σε μέτριο επίπεδο της απειλής. Για παράδειγμα, όταν η αντιληπτή αποτελεσματικότητα είναι μέτρια, οι άνθρωποι μπορεί αρχικά να πιστεύουν ότι μπορούν να αποτρέψουν μια κυβερνοεπίθεση. Ωστόσο, καθώς η απειλή αυξάνεται σε ένταση και σχετικότητα, τα άτομα μπορεί να αρχίσουν να εγκαταλείπουν κάθε ελπίδα αποτροπής της απειλής ή επαρκούς αντιμετώπισης τυχόν επακόλουθων επιπτώσεων.

Στην ψυχολογία της λογοτεχνίας του φόβου, ο Stekel (1930) επισημαίνει ότι ο φόβος είναι εν μέρει κληρονομικός, μια κληρονομιά αιώνων, που άφησε τα ίχνη του στον εγκέφαλό μας. Αντίστοιχα, η αντιληπτή αποτελεσματικότητα αποτελείται από τις απόψεις του ατόμου σχετικά με τη

σοβαρότητα της απειλής, ενώ η αντιληπτή ευπάθεια αποτελείται από τη στάση του ατόμου σχετικά με τις πιθανότητές του να το αντιμετωπίσει.

Η θεωρία της αυτο-αποτελεσματικότητας προϋποθέτει ότι η αντιληπτή αναποτελεσματικότητα της αντιμετώπισης πιθανών γεγονότων είναι αυτή που δημιουργεί τόσο τις προσδοκίες φόβου όσο και τη συμπεριφορά αποφυγής. Τα άτομα που κρίνονται αποτελεσματικά στη διαχείριση πιθανών απειλών, μπορεί να μην αισθάνονται ούτε φόβο ούτε να αποφεύγουν τις απειλές. Αντίθετα, εάν οι άνθρωποι κρίνουν τον εαυτό τους ως αναποτελεσματικό στην άσκηση ελέγχου των πιθανών απειλών, αντιδρούν με άγχος και δεν θέλουν να έχουν καμία επαφή, αποφεύγοντας έτσι τις απειλές. Για παράδειγμα, σε περίπτωση συμβάντος που σχετίζεται με τον κυβερνοχώρο, όπως απάτη ηλεκτρονικού "ψαρέματος", τα άτομα μπορεί να κρίνουν ότι δεν έχουν τις απαραίτητες δεξιότητες ή γνώσεις προκειμένου να αποφύγουν ένα τέτοιο περιστατικό, αποφεύγοντας έτσι να δράσουν ή να λάβουν προστατευτικά μέτρα. Εάν αυτό πρόκειται να συμβεί σε μεγάλη κλίμακα, θα μπορούσε να έχει αξιοσημείωτο κοινωνικό αντίκτυπο.

Οι προσδοκίες φόβου και οι συμπεριφορές αποφυγής είναι παράγοντες που μπορούν να επηρεάσουν την αντιληπτή αναποτελεσματικότητα της διαχείρισης καταστάσεων.

Αναγνωρίζοντας ότι η ανθρώπινη συμπεριφορά ρυθμίζεται σε μεγάλο βαθμό από προσωπικές πεποιθήσεις αποτελεσματικότητας, οι άνθρωποι μπορούν να ασκήσουν τις δραστηριότητές τους στα χαμηλότερα επίπεδα αυτο-αποτελεσματικότητας παρά την επίκληση υψηλού φόβου και μπορούν να λάβουν προληπτικά μέτρα χωρίς να χρειάζεται να περιμένουν να προκύψουν τα συναισθήματα φόβου και ενθουσιασμού. Διαφορετικές θεωρητικές προσεγγίσεις εξηγούν τις διαδικασίες ελέγχου του φόβου ή τον τρόπο με τον οποίο τα άτομα αναγνωρίζουν γνωστικά το φόβο ή την απειλή, αλλάζοντας τη στάση, τις προθέσεις ή τις συμπεριφορές τους για να αποφύγουν την απειλή (παράγοντες που οδηγούν στην αποδοχή του μηνύματος). Η εξέταση των αιτιών του φόβου αποκαλύπτει μερικές ενδιαφέρουσες πραγματικότητες.

Σύμφωνα με τον Witte (1994) όσο μεγαλύτερη είναι η απειλή, τόσο μεγαλύτερος είναι ο φόβος. Επίσης, η απειλή σχετίζεται με την αίσθηση του φόβου και όχι με την αποτελεσματικότητα.

Ο Witte (1992a) υποστήριξε ότι η αντιληπτή αποτελεσματικότητα καθορίζει μόνο τη φύση της αντίδρασης (έλεγχος του φόβου ή του κινδύνου), ενώ η αντιληπτή απειλή καθορίζει την ένταση της αντίδρασης (πόσος έλεγχος του φόβου ή του κινδύνου προκαλείται). Λαμβάνοντας υπόψη ότι η αντιληπτή απειλή και η πρόκληση φόβου φαίνεται να συνδέονται στενά, είναι πιθανό η απειλή και το συναίσθημα του φόβου να συνεργάζονται για να επηρεάσουν την ένταση μιας αντίδρασης σε ένα κάλεσμα φόβου. Για να το θέσουμε αυτό στο πλαίσιο διαδικτυακών απειλών, όταν τα άτομα φοβούνται μια μεγάλη κυβερνοεπίθεση και συνειδητοποιούν ότι μια αντίδραση θα μπορούσε να αποτρέψει αποτελεσματικά αυτή την απειλή, παρακινούνται να ελέγξουν τον κίνδυνο (κίνητρο προστασίας). Αυτή η διαδικασία ελέγχου θα μπορούσε να ξεκινήσει με τη σκέψη στρατηγικών για την αντιμετώπιση αυτής της απειλής και τη μείωση των επιπτώσεων του αντίστοιχου κινδύνου στη ζωή τους. Όταν κυριαρχούν οι διαδικασίες ελέγχου του κινδύνου, οι άνθρωποι μπορεί αναμφισβήτητα να αντιδράσουν στον κίνδυνο, όχι στο φόβο.

Λαμβάνοντας υπόψη την περίπτωση κυβερνοεπιθέσεων, ένα άλλο παράδειγμα θα ήταν ότι τα θύματα απάτης και κατάχρησης υπολογιστών που έχουν πέσει θύματα στο παρελθόν θα μπορούσαν να λάβουν μέτρα για να αποφύγουν να γίνουν ξανά θύματα στο μέλλον. Η συντριπτική πλειονότητα των θυμάτων απάτης και κατάχρησης ηλεκτρονικών υπολογιστών έχουν πέσει θύματα μόνο μία φορά, με μόνο ένα μικρό ποσοστό να δηλώνει ότι έχει υποστεί επίθεση δύο ή περισσότερες φορές. Τα στατιστικά στοιχεία υποστηρίζουν αυτόν τον ισχυρισμό που δείχνει ότι οι χρήστες μπορούν να μάθουν γρήγορα από τα λάθη τους όταν γίνουν θύματα ηλεκτρονικού εγκλήματος.

Αντίθετα, όταν η αντιληπτή απειλή είναι υψηλή, αλλά η αντιληπτή αποτελεσματικότητα είναι χαμηλή, ξεκινούν οι διαδικασίες ελέγχου του φόβου. Ο φόβος προκαλείται αρχικά και η απειλή γίνεται έντονη όταν τα άτομα αισθάνονται ανίκανα να αποτρέψουν την απειλή. Έτσι, κινητοποιούνται για να χειραγωγήσουν τον φόβο τους (αμυντική χειραγώγηση) υιοθετώντας αντιδράσεις, όπως η άρνηση. Όταν κυριαρχούν οι διαδικασίες ελέγχου του φόβου, τα άτομα αντιδρούν στο φόβο τους, όχι στον κίνδυνο. Τα άτομα μπορεί να αισθάνονται αβοήθητα και θύματα, ενώ η έλλειψη γνώσης τους σχετικά με το έγκλημα στον κυβερνοχώρο θα τους οδηγήσει να αποδεχτούν την πιθανότητα να είναι θύματα ή να αρνηθούν αυτή τη δυνατότητα συνολικά.

Επιπλέον, τα θύματα αισθάνονται τα συνηθισμένα συναισθήματα όταν συνειδητοποιούν ότι έχουν εξαπατηθεί – από ανικανότητα μέχρι οργή.

Σύμφωνα με τον Garland (2001), όταν πρόκειται για το φόβο του εγκλήματος, «οι φόβοι και η δυσαρέσκειά μας, αλλά και οι αφηγήσεις και οι αντιλήψεις μας κοινής λογικής, γίνονται παγιωμένα πολιτιστικά γεγονότα που συντηρούνται και αναπαράγονται από πολιτιστικά σενάρια». Η ιδέα των «πολιτιστικών σεναρίων» μπορεί να βοηθήσει να αποκαλυφθούν πολλά συναισθήματα όπως ο φόβος. αναμφισβήτητα ακόμη και στο πλαίσιο της κυβερνοεπίθεσης. Ένα πολιτιστικό σενάριο επικοινωνεί κανόνες και συναισθήματα, αλλά και ιδέες για το τι σημαίνουν αυτά τα συναισθήματα. Οι άνθρωποι ερμηνεύουν και εσωτερικεύουν αυτούς τους κανόνες ανάλογα με τις συνθήκες και την ιδιοσυγκρασία τους, παραμένοντας πάντα πολύ επηρεασμένοι από τους κανόνες. Κατά συνέπεια, ο αντίκτυπος του φόβου καθορίζεται από την κατάσταση στην οποία βρίσκονται οι άνθρωποι, αλλά είναι επίσης, σε κάποιο βαθμό, προϊόν κοινωνικής κατασκευής. Ο φόβος καθορίζεται από τον εαυτό και την αλληλεπίδραση του εαυτού με τους άλλους. Διαμορφώνεται επίσης από ένα πολιτιστικό σενάριο που καθοδηγεί τους ανθρώπους για το πώς να ανταποκριθούν στις απειλές για την ασφάλειά τους.

3.5. Το φαινόμενο του διαδικτύου της μη αυτοσυγκράτησης

Όσον αφορά τον αντίκτυπο των κυβερνοεπιθέσεων στη διαδικτυακή συμπεριφορά, υπάρχουν διαφορετικές πτυχές του κυβερνοχώρου που πρέπει να ληφθούν υπόψη. Μία από αυτές τις πτυχές περιβάλλει την πραγματικότητα ότι τα άτομα λένε και κάνουν πράγματα στον κυβερνοχώρο που συνήθως δεν θα έλεγαν και δεν θα έκαναν στον εκτός σύνδεσης (πρόσωπο με πρόσωπο) κόσμο. Για παράδειγμα, μπορεί να χαλαρώσουν, να αισθάνονται λιγότερο συγκρατημένοι και να

παρουσιάζονται πιο ανοιχτά. Τόσο διάχυτο είναι αυτό το φαινόμενο που ένας όρος έχει εμφανιστεί γι 'αυτό, δηλαδή το διαδικτυακό φαινόμενο της μη αυτοσυγκράτησης.

Αυτή η μη αυτοσυγκράτηση ενδυναμώνεται λόγω διαφόρων παραγόντων. Αυτοί λαμβάνουν υπόψη το γεγονός ότι οι άνθρωποι μπορούν να σχηματίσουν μια διαφορετική ταυτότητα στο διαδίκτυο και ότι μπορεί να αισθάνονται λιγότερο ευάλωτοι στον τρόπο με τον οποίο εκφράζονται ή συμπεριφέρονται, σε σύγκριση με τον τρόπο με τον οποίο θα ενεργούσαν εκτός σύνδεσης. Επιπλέον, οι άνθρωποι μπορούν να αισθάνονται λιγότερο ορατοί στο διαδίκτυο και, ως εκ τούτου, μπορεί να συμμετέχουν σε δραστηριότητες που διαφορετικά δεν θα συμμετείχαν. Αυτός ο παράγοντας επηρεάζει τις συζητήσεις μας σχετικά με τις επιπτώσεις, καθώς οι συνέπειες ορισμένων διαδικτυακών ενεργειών ή δραστηριοτήτων ενδέχεται να μην είναι πλήρως απτές για τους ανθρώπους στον κόσμο εκτός σύνδεσης. Αυτό έχει επίσης συζητηθεί και σε άλλους τομείς, καθώς σχετίζεται με το έγκλημα στον κυβερνοχώρο.

3.6. Κατανόηση των δημόσιων αντιδράσεων σε κακόβουλα περιστατικά στον κυβερνοχώρο

3.6.1. Συναισθηματικές αντιδράσεις στο έγκλημα στον κυβερνοχώρο

Η έρευνα δείχνει ότι οι τρέχουσες μορφές κυβερνοεπιθέσεων μπορούν να προκαλέσουν και ψυχολογικές επιπτώσεις. Ανάλογα με το ποιοι είναι οι επιτιθέμενοι και τα θύματα, οι ψυχολογικές επιπτώσεις των κυβερνοαπειλών μπορεί ακόμη και να ανταγωνιστούν εκείνες της παραδοσιακής τρομοκρατίας . Τα θύματα διαδικτυακών επιθέσεων και εγκλημάτων μπορεί να υποστούν συναισθηματικό τραύμα που μπορεί να οδηγήσει σε κατάθλιψη. Υπάρχουν επίσης ορισμένες ενδείξεις περιορισμένων συμπτωμάτων οξείας διαταραχής άγχους (ASD) στα θύματα εγκληματικών πράξεων σε διαδικτυακούς εικονικούς κόσμους, όπως μερικές ανέκδοτες μαρτυρίες ενοχλητικών αναμνήσεων, συναισθηματικό μούδιασμα και αναστάτωση από θύματα εικονικής σεξουαλικής επίθεσης. Για παράδειγμα, ο αντίκτυπος της κλοπής ταυτότητας σε ένα θύμα σε συναισθηματικό επίπεδο μπορεί να οδηγήσει το άτομο να αναστατωθεί και να αφεθεί να αισθάνεται ότι έχει παραβιαστεί, προδοθεί, είναι ευάλωτο, θυμωμένο και ανίσχυρο. Συχνά, η θυματοποίηση μπορεί να οδηγήσει τα θύματα σε συναισθήματα οργής, άγχους, προτίμηση για ασφάλεια έναντι ελευθερίας και ελάχιστο ενδιαφέρον για υιοθέτηση νέας τεχνολογίας λόγω απώλειας εμπιστοσύνης στον κυβερνοχώρο. Το θύμα μπορεί να φθάσει σε στάδια θλίψης, να υποφέρει από θυμό ή οργή. Σε ορισμένες περιπτώσεις, τα θύματα μπορεί ακόμη και να κατηγορήσουν τον εαυτό τους και να αναπτύξουν μια αίσθηση ντροπής. Το sextortion είναι ένα καλό παράδειγμα αυτού δεδομένου του τρόπου με τον οποίο ξεκινά αρχικά.

Μια μελέτη της Symantec (2010) έδειξε περαιτέρω ότι τα θύματα αισθάνονται ότι τα ίδια ευθύνονται εν μέρει ή εξ ολοκλήρου. Αυτό από μόνο του έχει συνέπειες για τις προκύπτουσες ψυχολογικές επιπτώσεις. Ο αριθμός που θα δράσει ποικίλλει σημαντικά ανάλογα με την τοποθεσία. Για παράδειγμα, το 74% των ατόμων στη Σουηδία έρχονται σε επαφή με την αστυνομία, αλλά αυτό είναι σημαντικά πάνω από τον συνολικό μέσο όρο του 44%. Κατά γενικό κανόνα, περίπου τα μισά θύματα δεν θα επικοινωνήσουν με κανέναν, αν και περίπου το ένα τέταρτο μπορεί να

προσπαθήσει να λάβει κάποια μέτρα, ακόμη και αν αποφεύγει μόνο ορισμένους ιστότοπους στο μέλλον.

Σύμφωνα με τη Symantec, οι 10 κορυφαίες συναισθηματικές αντιδράσεις σε διαδικτυακές επιθέσεις και εγκλήματα στον κυβερνοχώρο είναι τα συναισθήματα θυμού, ενόχλησης και εξαπάτησης. Οι Böhme και Moore (2012) διαπίστωσαν ότι η άμεση εμπειρία του εγκλήματος στον κυβερνοχώρο μειώνει την πιθανότητα αγορών και τραπεζικών συναλλαγών στο διαδίκτυο, ενώ η έκφραση ανησυχίας για το έγκλημα στον κυβερνοχώρο έχει σχεδόν διπλάσιο αρνητικό αντίκτυπο στη συμπεριφορά στο διαδίκτυο από ό, τι την βιώνουμε άμεσα. Οι Modic και Anderson (2015) διαπίστωσαν ότι τα θύματα οικονομικής απάτης ανέφεραν συνεχώς συναισθηματικές επιπτώσεις ως πιο σοβαρές από τις οικονομικές επιπτώσεις σε όλους τους τύπους απάτης.

Μπορούμε επίσης να αντιληφθούμε πώς ακόμη και οι μη θανατηφόρες μορφές κυβερνοτρομοκρατίας έχουν σημαντικό αντίκτυπο στη στάση των θυμάτων πληθυσμών. Υπό επίθεση, τα θύματα αντιδρούν όχι μόνο με φόβο, όπως και με τα θύματα εγκληματικών πράξεων, αλλά με αιτήματα για προστασία από την κυβέρνηση, μέσω επιτήρησης και ισχυρότερων κανονισμών.

Η Εσθονία γίνεται συχνά επίκληση σε τέτοιες συζητήσεις και πολλοί συγγραφείς εφιστούν την προσοχή στον πανικό που προκλήθηκε μεταξύ του λαού της Εσθονίας, όταν τμήματα της υποδομής τους στον κυβερνοχώρο ήταν απρόσιτα λόγω επιθέσεων DoS το 2007. Ωστόσο, η δυνατότητα κακόβουλων κυβερνοεπιθέσεων μεγάλης κλίμακας μπορούν να αλλάξουν την κατανόηση και την αντίληψη του κοινού για τα συμβάντα στον κυβερνοχώρο και θα μπορούσε να οδηγήσει σε ενεργοποίηση των «τρομακτικών παραγόντων» της αντίληψης του κινδύνου (δηλ. καταστροφικές δυνατότητες, θανατηφόρες συνέπειες και υψηλούς κινδύνους για τις μελλοντικές γενιές). Αυτό προκαλεί ιδιαίτερη ανησυχία δεδομένων των διαφόρων προβλέψεων, για πιθανά μελλοντικά τεχνολογικά σενάρια και των επιπτώσεων που αφορούν την ασφάλεια και την προστασία της ιδιωτικής ζωής στο διαδίκτυο.

3.6.2 Μαθημένη ανικανότητα

Τα ευρήματα δείχνουν ότι λιγότεροι από 1 στους 10 ανθρώπους (9%), επίσης, μόνο οι μισοί (51%) των ενηλίκων που ρωτήθηκαν, θα άλλαζαν τον τρόπο που συμπεριφέρονται στο διαδίκτυο εάν γίνουν θύματα. Αυτό παρέχει μια ενδιαφέρουσα σύγκριση με τις προηγούμενες αναφορές. Οι άνθρωποι μπορεί να δεχτούν μια κατάσταση, ακόμα και αν την αισθάνονται δυσάρεστη μόνο και μόνο επειδή δεν μπορούν να την κατανοήσουν ή δεν γνωρίζουν αρκετά γι 'αυτή. Μετά από αυτό το σημείο, θα μπορούσε κανείς να υποστηρίξει ότι τα άτομα μπορούν να δεχτούν κυβερνοεπιθέσεις λόγω της αίσθησης της «μαθημένης αδυναμίας».

Λόγω της αίσθησης της μαθημένης ανικανότητας και έλλειψη γνώσεων σχετικά με τις διαδικτυακές επιθέσεις και τους τρόπους επίλυσης ενός συμβάντος, οι χρήστες μπορούν απλά να αποδεχτούν την πιθανότητα να είναι θύματα. Έμμεσα, ένα βασικό ερώτημα είναι, εάν αποδέχονται επίσης την πραγματικότητα των επιπτώσεων και ελπίζουν ότι η σοβαρότητα είναι χαμηλή. Η

ανώνυμη φύση του εγκλήματος στον κυβερνοχώρο, μπορεί να οδηγήσει (π.χ. ένα άτομο, βιομηχανία, κυβέρνηση) ώστε να γίνει θύμα εγκλήματος στον κυβερνοχώρο κάποια στιγμή.

Επιπλέον, η αίσθηση της μαθημένης αδυναμίας μπορεί ενδεχομένως να οδηγήσει σε χαμηλή υιοθέτηση προστατευτικών συμπεριφορών ασφαλείας.

Οι χρήστες καλούνται να λαμβάνουν πολλές αποφάσεις που σχετίζονται με την ασφάλεια κάθε μέρα, οι οποίες μπορούν να προκαλέσουν άγχος. Αυτές οι συμπεριφορές περιλαμβάνουν: (α) να μην ανοίγετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από έναν αποστολέα που δεν αναγνωρίζουν. β) μη πρόσβαση σε άγνωστα συνημμένα· γ) μόνο προγράμματα λήψης και εκτέλεσης από αξιόπιστες πηγές· δ) τη χρήση λογισμικού προστασίας από ιούς και λογισμικού ασφαλείας (π.χ. τείχος προστασίας)· και ε) τη δημιουργία τακτικών αντιγράφων ασφαλείας. Ορισμένες από αυτές τις αποφάσεις μπορούν επίσης να προκαλέσουν στον χρήστη συναισθήματα άγχους λόγω έλλειψης γνώσης σχετικά με τις πιθανές επιπτώσεις της λήψης λανθασμένων αποφάσεων.

Οι πολίτες έχουν συχνά αναφέρει έλλειψη γνώσεων σχετικά με ορισμένους βασικούς τομείς στον τομέα της κυβερνοασφάλειας. Μερικά παραδείγματα είναι η έλλειψη γνώσεων σχετικά με τον τρόπο χρήσης πακέτων ασφαλείας, τον τρόπο διασφάλισης των τεχνολογικών συσκευών τους και τις απειλές στο διαδίκτυο. **Ακόμη και όταν αυτά τα άτομα γνωρίζουν τις απειλές, αναφέρουν ότι δεν τις καταλαβαίνουν.** Αυτά τα χαμηλά επίπεδα κατανόησης από το κοινό των κυβερνοαπειλών και των πρακτικών ασφάλειας θα μπορούσαν να οδηγήσουν σε έλλειψη δημόσιας δέσμευσης σε θέματα ασφάλειας και σε γενική απώλεια εμπιστοσύνης στον κυβερνοχώρο ή/και την τεχνολογία. Αυτό έχει επίσης παρατηρηθεί στον τομέα της προστασίας της ιδιωτικής ζωής των πληροφοριών στο πλαίσιο νέων μορφών τεχνολογίας, όπου ορισμένοι χρήστες θεωρούν τώρα την ιδιωτικότητα ως «το βαρετό κομμάτι». Τα ζητήματα αυτά χαρακτηρίζουν τις ευρείες κοινωνικές επιπτώσεις.

3.6.3 Μεταβλητές που σχετίζονται με κυβερνοεπιθέσεις

Η δημόσια απάντηση σε μια κυβερνοεπίθεση ενημερώνεται από μια σειρά ειδικών στον κυβερνοχώρο μεταβλητών, όπως η ταυτότητα του εισβολέα, η ταυτότητα-στόχος, το μέγεθος της επίθεσης καθώς και η κυβερνητική επικοινωνία για μια κυβερνοεπίθεση και ο χρόνος αποκάλυψης ενός κακόβουλου γεγονότος.

Οι δημόσιες αντιδράσεις μπορεί να διαφέρουν ανάλογα με την αποκαλυπτόμενη ταυτότητα ενός συγκεκριμένου επιτιθέμενου. Οι κύριες κατηγορίες ενός «εισβολέα» είναι τρομοκρατικές, χακτιβιστικές και εγκληματικές – όλοι τους μπορεί να είναι σε θέση να εξαπολύσουν επιθέσεις που θα μπορούσαν να χαρακτηριστούν ως ζητήματα σοβαρής δημόσιας ανησυχίας. Οι εγκληματίες είναι, κατά μέσο όρο, λιγότερο πιθανό να αποκαλύψουν δημόσια την ταυτότητά τους (υιοθέτοντας οποιαδήποτε ταυτότητα, ψευδώνυμο ή άλλο) επειδή η ανωνυμία τους διευκολύνει καλύτερα. Επιπλέον, η ταυτότητα-στόχος μπορεί να επηρεάσει την ανταπόκριση του κοινού. Για παράδειγμα, εάν μια σειρά περιστατικών απάτης επηρεάζει τυχαία άτομα, μπορεί να αναμένεται ότι θα

προκαλέσει λιγότερο πανικό ή οργή σε σύγκριση με μια στοχευμένη επίθεση προς εθνικό χρηματοπιστωτικό, βοηθητικό ή υγειονομικό ίδρυμα.

Επιπλέον, η κλίμακα μιας επίθεσης θα επηρεάσει τον αντίκτυπό της. Η πλήρης έκταση μιας επίθεσης ενδέχεται να μην γίνει εμφανής αμέσως, ιδίως εάν αποτύχουν τα συστήματα δεύτερης και τρίτης τάξης. Τέλος, ο τρόπος με τον οποίο η κυβέρνηση θα μεταδώσει μια κυβερνοεπίθεση και ο χρόνος αποκάλυψης ενός κακόβουλου γεγονότος θα επηρεάσουν το επίπεδο της δημόσιας αντίδρασης. Αυτές οι πληροφορίες μπορούν να επηρεάσουν την κατεύθυνση και τη δυναμική της ανταπόκρισης του κοινού. Οι τρόποι με τους οποίους οι πολίτες είναι πιθανό να μάθουν για μια κυβερνοεπίθεση είναι επίσης μια σημαντική μεταβλητή. Διαφορετικά επίπεδα δημόσιας αντίδρασης μπορούν να προκληθούν λόγω απώλειας υπηρεσιών, δημόσιων ανακοινώσεων από τον επιτιθέμενο ή από κυβερνητικές ανακοινώσεις.

Ο Lawson (2013) βασίζεται στην ιστορία της τεχνολογίας και των αποτυχιών μεγάλων κοινωνιοτεχνικών συστημάτων, της στρατιωτικής ιστορίας και - πιο σχετικού εδώ - κοινωνιολογίας καταστροφών που υποδηλώνουν ότι ο «φόβος και ο πανικός» μπορεί να μην είναι τα καθοριστικά χαρακτηριστικά των δημόσιων αντιδράσεων σε μελλοντικές κυβερνοεπιθέσεις. Όπως προαναφέρθηκε, το κοινό είναι πιο πιθανό να ανταποκριθεί στο γεγονός (π.χ. απώλεια υπηρεσίας), παρά στην ίδια την κυβερνοεπίθεση.

ΚΕΦΑΛΑΙΟ 4

4.1. ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΚΥΒΕΡΝΟ ΕΠΙΘΕΣΕΩΝ – ΚΑΤΑΝΟΗΣΗ ΤΩΝ ΕΠΙΠΤΩΣΕΩΝ ΚΑΙ ΔΙΑΔΟΣΗΣ ΤΟΥΣ

Η τεχνολογική πρόοδος έχει οδηγήσει σε ψηφιοποίηση των οργανισμών και κατά συνέπεια πολλών τμημάτων των δραστηριοτήτων τους. Το απειλητικό τοπίο των κυβερνοεπιθέσεων αλλάζει γρήγορα και ο πιθανός αντίκτυπος τέτοιων επιθέσεων είναι αβέβαιος, αφού υπάρχει έλλειψη αποτελεσματικών μετρήσεων, εργαλείων και πλαισίων για κατανόηση και αξιολόγηση της ζημιάς που αντιμετωπίζουν οι οργανισμοί από κυβερνοεπιθέσεις. Σε αυτό το κεφάλαιο, εξετάζουμε τη βιβλιογραφία σχετικά με βλάβη, και πώς έχει εννοηθεί σε κλάδους όπως η εγκληματολογία και τα οικονομικά, και διερευνούμε πως άλλες έννοιες όπως ο κίνδυνος και ο αντίκτυπος σχετίζονται με τη βλάβη.

Η κοινωνία εξαρτάται σε μεγάλο βαθμό από την τεχνολογία με αλληλεπίδραση της στο εμπόριο και τη βιομηχανία. Ενώ η τεχνολογία έχει οδηγήσει σε σημαντικές εξελίξεις σε αυτούς τους τομείς, ιδιαίτερα μέσω της χρήσης του Διαδικτύου, έχει επίσης εκτεθειμένους οργανισμούς και άτομα σε μια σειρά νέων κινδύνων από επιθέσεις μέσω ψηφιακών διεπαφών.

Αυτά περιλαμβάνουν, για παράδειγμα, επιθέσεις άρνησης υπηρεσίας (DoS) σε δίκτυα, παραβιάσεις δεδομένων σε εταιρικές και προσωπικές συσκευές και ιούς που μπορούν να καταστρέψουν υποδοχές , κλοπή εταιρικών μυστικών, δολιοφθορά συστημάτων να θέσουν σε κίνδυνο τις υπηρεσίες και την ακεραιότητα των συστημάτων, και αντιγραφή δεδομένων πελατών για την πώληση των ταυτοτήτων τους στο σκοτεινό ιστότοπο (αναφέρθηκαν στο προηγούμενο κεφάλαιο σύμφωνα με την κατάταξη του ENISA).

Αρχικά ορίζουμε την κυβερνο-βλάβη ως τη ζημιά που προκύπτει ως άμεσο αποτέλεσμα επίθεσης που πραγματοποιήθηκε εξ ολοκλήρου ή εν μέρει μέσω ψηφιακών μέσων ή εφαρμογών λογισμικού. Η κατανόηση μιας τέτοιας βλάβης στον κυβερνοχώρο είναι ζωτικής σημασίας για να διασφαλιστεί ότι οι έλεγχοι και οι μέθοδοι μετριασμού που εφαρμόζουμε έχουν αποτέλεσμα και είναι ανάλογοι του κινδύνου.

Για την αντιμετώπιση των κινδύνων που προκύπτουν από κυβερνοεπιθέσεις, έχουν προταθεί πολλές και διάφορες λύσεις. Αυτές περιλαμβάνουν διαδικασίες και τεχνολογίες σχεδιασμένες για να αποτρέψουν μη εξουσιοδοτημένους και δυνητικά απειλητικούς παράγοντες από την πρόσβαση σε ψηφιακά συστήματα και περιουσιακά στοιχεία. Περιλαμβάνουν επίσης νέα συστήματα ανίχνευσης και πρόληψης εισβολών που έχουν σχεδιαστεί για να διευκρινίσουν τις επερχόμενες απειλές και να βοηθήσουν τους οργανισμούς να περιορίσουν οποιοδήποτε δυνητικό κακό. Υπάρχει μια γενική αποδοχή ότι οι ψηφιακές υποδομές είναι κοινωνικο τεχνικά συστήματα, και επομένως και οι εμπλεκόμενοι άνθρωποι θα πρέπει να θεωρούνται ως επιτιθέμενοι με σκοπό την πρόληψη των κυβερνο επιθέσεων και τον μετριασμό του κινδύνου στον κυβερνοχώρο.

Θα παρουσιαστεί λοιπόν μια πρωτότυπη ταξινόμηση της οργανωτικής βλάβης στον κυβερνοχώρο, η οποία θα βοηθήσει τόσο τους ερευνητές όσο και όλους τους ανθρώπους να εξετάσουν το πλήρες φάσμα των βλαβών που μπορεί να προκύψουν από κυβερνο επιθέσεις, κατά την ανάπτυξη θεραπειών κινδύνου. Αυτό είναι απαραίτητο για να εκτιμήσουμε τον κίνδυνο, καθώς και να ποσοτικοποιήσουμε τη ζημιά που προκύπτει από τέτοιους κινδύνους. Διερευνούμε το θέμα της κυβερνο βλάβης, με σκοπό την ανάπτυξη μιας πιο ολιστικής κατανόησης του τι συνιστά οργανωτική βλάβη στον κυβερνοχώρο από ό, τι διατίθεται στη βιβλιογραφία που σώζεται. Έτσι, εξετάζουμε κριτικά τη βλάβη στον κυβερνοχώρο, συμπεριλαμβανομένου του τρόπου με τον οποίο αυτό και συναφή θέματα όπως ο κίνδυνος στον κυβερνοχώρο, η εγκληματολογία και τα οικονομικά του κυβερνοχώρου.

Εστιάζουμε ειδικά στον καθορισμό μιας ταξινόμησης των διαφόρων τύπων βλαβών οργανωτικού επιπέδου στον κυβερνοχώρο.. Αυτό απαιτείται για την επαρκή μοντελοποίηση και την αιτιολογία των βλαβών. Θα παρουσιαστούν και θα αντληθούν πληροφορίες από κάποιες μελέτες περίπτωσης, προκειμένου να δοθούν αρχικές ενδείξεις σχετικά με το πώς συνδέονται οι διαφορετικοί τύποι βλάβης με την συγκεκριμένη ταξινόμηση αλλά και πώς διαδίδεται στον κυβερνοχώρο μια βλάβη.

4.2. Η σχέση μεταξύ βλάβης, αντίκτυπου και κινδύνου στους οργανισμούς

Δύο έννοιες που συνδέονται στενά με τη βλάβη είναι ο «αντίκτυπος» και ο «κίνδυνος». Και οι δύο αυτές έννοιες βρίσκονται σε περίοπτη θέση στη λογοτεχνία και τις πρακτικές για την ασφάλεια των οργανισμών. Σε γενικές γραμμές, ο αντίκτυπος είναι η επίδραση μιας δράσης από ένα άτομο ή πράγμα σε ένα άλλο και μπορεί να είναι είτε θετικός είτε αρνητικός. Αυτός ο χαρακτηρισμός του αντίκτυπου ως γενικού όρου υποστηρίζεται από όλους στην ασφάλεια σε ολόκληρο τον ακαδημαϊκό χώρο.

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια δικτύων και πληροφοριών (ENISA) ορίζει τον αντίκτυπο ως αποτέλεσμα ανεπιθύμητης έρευνας. Αυτός είναι ένας ορισμός που δανείζεται από τον Διεθνή Οργανισμό Τυποποίησης και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (ISO/IEC). Αν και δεν είναι οριστικό, η αναμφισβήτητη πρόταση εδώ είναι ότι ο αντίκτυπος είναι αρνητικός. Για το NIST, η ανάπτυξη της κατανόησης του αντίκτυπου αποτελεί σημαντική συνιστώσα της διαδικασίας διαχείρισης κινδύνων για τους οργανισμούς. Περιγράφουν τον αντίκτυπο ως τη «ζημία που αναμένεται να προκύψει» από τις συνέπειες μη εξουσιοδοτημένων ενεργειών ή την απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας. Η εκτίμησή τους για τον αντίκτυπό είναι σαφώς προσανατολισμένη στη βλάβη, ενδεχομένως με σκοπό να τονίσει τον «αντίκτυπο» ως ανεπιθύμητο ή ως απομείωση των οργανωτικών συμφερόντων. Μια σημαντική παρατήρηση που μπορεί να γίνει με βάση τον προβληματισμό μας μέχρι στιγμής είναι ότι, αν και ο αντίκτυπος είναι ένας μη συγκεκριμένος όρος, στην ασφάλεια, συχνά συνεπάγεται αρνητικό αποτέλεσμα. Σε ορισμένες περιπτώσεις, αυτή η δυσμενής έννοια γίνεται σαφής μέσω της χρήσης λέξεων όπως η βλάβη.

Ο όρος «κίνδυνος» συνδέεται με πολλές έννοιες και οι θεωρητικές βάσεις του παρέχονται από τα εμβληματικά έργα των Beck και Giddens. Σύμφωνα με τον Beck, ο κίνδυνος είναι μια σύγχρονη έννοια που προϋποθέτει τη λήψη αποφάσεων και είναι αποτέλεσμα της ταχύτητας εκσυγχρονισμού που έχει μετατρέψει την κοινωνία μας σε μια κοινωνία κινδύνου.

Ένα ρεύμα λογοτεχνίας όπου η βλάβη έχει κεντρικό ρόλο είναι η εγκληματολογία γενικά και η μελέτη του εγκλήματος του λευκού κολάρου ειδικότερα. Όταν εννοούμε έγκλημα του λευκού κολάρου αναφερόμαστε και σε εγκλήματα που έχουν στόχο επιχειρήσεις δηλαδή είναι ένα έγκλημα όπου το πρωταρχικό κίνητρο είναι συνήθως οικονομικού χαρακτήρα.

Οι εγκληματολόγοι, λόγω δυσκολιών στον ορισμό των εγκλημάτων και στον εντοπισμό των επιζήμιων επιπτώσεών τους, προτείνουν να παρεκκλίνουν από την έννοια του εγκλήματος και να επικεντρωθούν στην έννοια της κοινωνικής βλάβης. Ως εκ τούτου, η βλάβη είναι καίριας σημασίας για την κοινωνική πολιτική και οι παρατηρήσεις διαφόρων τύπων βλάβης που προέρχονται από εγκλήματα διαμορφώνουν πρακτικές κατευθυντήριες γραμμές, καθιστώντας την ανάπτυξη ορθών μεθόδων για τη συστηματική αξιολόγηση της βλάβης αυξανόμενης σημασίας. Οι Greenfield et al., παρουσιάζουν ένα πλαίσιο που περιλαμβάνει ένα σύνολο διαδικασιών για την εμπειρικά εκτίμηση της βλάβης. Προσδιορίζουν πέντε βασικές διαστάσεις στις οποίες μπορεί να εκδηλωθεί βλάβη, δηλαδή: λειτουργική ακεραιότητα, υλική υποστήριξη και παροχές, ελευθερία από την ταπείνωση, προστασία της ιδιωτικής ζωής ή αυτονομία και φήμη. Καθορίζουν επίσης πέντε επίπεδα μεγέθους αυτών των τύπων βλάβης και εξετάζουν τον διαδοχικό χαρακτήρα της βλάβης εξετάζοντας εγκλήματα του πραγματικού κόσμου που έχουν προκαλέσει σοβαρή βλάβη στην κοινωνία. Με παρόμοιο τρόπο, οι Van Slyke κ. ά. κατασκευάζουν μια ταξινόμηση των βλαβών για τα εγκλήματα του λευκού κολάρου, εστιάζοντας στο στοιχείο της θυματοποίησης αυτών των εγκλημάτων. Εξετάζουν μια σειρά από εγκλήματα οικονομικού κολάρου και απαριθμούν το κόστος που προκύπτει από αυτά τα αδικήματα. Συμπληρώνουν την έρευνα με επιπλέον έρευνες για τα θύματα και εστιάζουν στις σοβαρές μακροχρόνιες επιπτώσεις των βλαβών σε ορισμένα άτομα. Περαιτέρω πληροφορίες παρέχονται με την πρόταση ότι οι βλάβες μπορούν να εννοηθούν ως πυραμίδα, με χρόνιες ζημίες στην κορυφή, τα "μεμονωμένα" θύματα που υπέστησαν σοβαρές ζημίες στη μέση και τα θύματα που δεν γνωρίζουν την απάτη ή έχουν υποστεί μικρό κόστος, στη βάση. Οι δευτερογενείς επιπτώσεις της βλάβης εξετάζονται επίσης, με τους συγγραφείς να υποστηρίζουν ότι αυτές αφορούν τα θύματα που υφίστανται μεγάλες απώλειες ή ψυχολογικές επιπτώσεις.

Επιπλέον, η μελέτη του Van Slyke εξετάζει τις βλάβες που μπορεί να αφορούν όχι μόνο τα άτομα αλλά και άλλα ενδιαφερόμενα μέρη, όπως οι κοινότητες, οι γειτονιές, οι κυβερνήσεις και η κοινωνία στο σύνολό της. Ιδιαίτερη έμφαση δίνεται επίσης στον υπολογισμό του κόστους του εγκλήματος, με τους συγγραφείς να υποστηρίζουν ότι υπάρχουν τρεις τύποι κόστους, εκείνο που προκύπτει κατά την αναμονή ενός εγκλήματος, εκείνο που προκύπτει ως συνέπεια αυτού και εκείνο που προκύπτει κατά την αντιμετώπιση του εγκλήματος. Προτείνουν δύο προσεγγίσεις για τον υπολογισμό αυτού του κόστους: "από κάτω προς τα πάνω", με βάση την έρευνα των περιπτώσεων εγκλημάτων και την εκτίμηση των διαφόρων βλαβών- και "από πάνω προς τα κάτω", προσπαθώντας να εκτιμήσουν πόσο είναι διατεθειμένο να πληρώσει το κοινό για να αποφύγει ή να μειώσει αυτά τα εγκλήματα.

Η Brenner παρουσιάζει την πρώτη προσέγγιση για τον προσδιορισμό μετρήσεων για την εκτίμηση του εγκλήματος που προέρχεται από τον κυβερνοχώρο. Αν και αναγνωρίζει ότι ο σχεδιασμός μετρήσεων και κλίμακας για το έγκλημα στον κυβερνοχώρο είναι εξαιρετικά δύσκολος, λόγω των προβλημάτων "σύλληψης", κλίμακας και αποδεικτικών στοιχείων, προτείνει μια απλή ταξινόμηση των βλαβών που αποτελείται από τρεις κύριους τύπους, δηλαδή ατομικές, συστημικές και ατελέσφορες.

Οι ερευνητές στον τομέα της εγκληματολογίας συμφωνούν όλοι ότι η εκτίμηση του κόστους των εγκλημάτων, καθώς και η παροχή μοντέλων για την εκτίμηση των ζημιών, παρουσιάζουν σημαντικές τεχνικές και μεθοδολογικές προκλήσεις. Οι προκλήσεις αυτές προκύπτουν λόγω της περιορισμένης χρησιμότητας των συμβατικών ερευνητικών εργαλείων, όπως οι έρευνες, των ανεπαρκών στατιστικών στοιχείων που λαμβάνονται από τις υπηρεσίες επιβολής του νόμου και της τάσης των ατόμων να αποκρύπτουν εγκλήματα από τις αρχές λόγω αμηχανίας ή έλλειψης τρόπων αναφοράς των εγκλημάτων αυτών.

Επιπλέον, μόνο ένα μικρό ποσοστό των υποθέσεων διώκεται ποινικά και δεν υπάρχει ενοποιημένη πηγή πληροφοριών που να συγκεντρώνει διαφορετικά εγκλήματα ή περιστατικά. Ο προσεκτικός αναγνώστης θα έχει αναγνωρίσει τις έντονες ομοιότητες με τα περιστατικά στον κυβερνοχώρο. Υπάρχουν πολλά διδάγματα που μπορούν να αντληθούν από τον κλάδο της εγκληματολογίας, αλλά πρέπει να τονιστεί ότι όλες οι προσεγγίσεις από αυτό το πλαίσιο προσδιορίζεται η ζημία που προκύπτει από συγκεκριμένα εγκλήματα. Υπάρχουν σαφείς παραλληλισμοί μεταξύ των μη κυβερνο εγκλημάτων και των εγκλημάτων στον κυβερνοχώρο από την άποψη της βλάβης (δεδομένου ότι τα θύματά τους είναι κοινά), οι οποίοι μπορούν να χρησιμοποιηθούν για τον σχεδιασμό μιας ταξινόμησης της βλάβης στον κυβερνοχώρο.

4.3. Οικονομικά του Κυβερνοχώρου

Οι Felici κ. ά. υπογραμμίζουν την ανάγκη περαιτέρω διερεύνησης του πεδίου των οικονομικών εστιάζοντας σε περιστατικά στον κυβερνοχώρο. Υποστηρίζουν ότι οι ΤΠΕ (Τεχνολογίες της Πληροφορίας & Επικοινωνιών) διεγείρουν νέες αγορές και ενσωματώνονται σε υφιστάμενους οικονομικούς τομείς που προωθούν την ανάπτυξη. Υποστηρίζουν ότι ο τομέας των οικονομικών της κυβερνοασφάλειας είναι απαραίτητος για να βοηθήσει τις ΤΠΕ να κρατήσουν αυτόν τον διπλό ρόλο. Προτείνουν επίσης ότι οι προκλήσεις σε αυτόν τον τομέα απαιτούν μια διεπιστημονική προσέγγιση και ότι τα μοντέλα που δημιουργούν οι ερευνητές πρέπει να αναγνωρίζουν τις νέες πληροφορίες σχετικά με τα κυβερνο-περιστατικά, τις επιπτώσεις τους και τις σχέσεις τους με τη δυναμική άλλων κυβερνο-παραγόντων.

Οι Anderson et al. είναι οι πρωτοπόροι για να δώσουν μια πρώτη προσέγγιση της μέτρησης του κόστους των κυβερνο-συμβάντων. Σε άρθρο τους, επισημαίνουν τις δυσκολίες στην αξιολόγηση των επιπτώσεων λόγω του γρήγορου ρυθμού των τεχνολογικών εξελίξεων και των μεγάλων ασυμμετριών μεταξύ της εκτίμησης του κόστους, των εσόδων και των πραγματικών αξιών τους. Παρόμοια με τα μοντέλα που παρουσιάζονται στη βιβλιογραφία εγκληματολογίας, στο μοντέλο τους οι Anderson et al. εξισώνουν τη βλάβη με το κόστος και εξετάζουν το άμεσο και έμμεσο

κόστος, το κόστος άμυνας και εγκλήματος, καθώς και το κόστος για την κοινωνία. Επεκτείνουν το έργο τους εξετάζοντας έννοιες από οικονομικά όπως η «επίδραση ηθικού κινδύνου», το πρόβλημα της κρυφής δράσης και η ουδετερότητα του δικτύου, άλλες, για την παροχή ολιστικής κατανόησης σχετικά με τα οικονομικά της εσωτερικής ασφάλειας.

Στο ίδιο πνεύμα, ο Moore επισημαίνει περαιτέρω προκλήσεις στον τομέα της οικονομίας της κυβερνοασφάλειας. Αντλώντας από έννοιες από τον τομέα της οικονομίας, ο Moore εντοπίζει προκλήσεις, μεταξύ άλλων, λανθασμένα ευθυγραμμισμένα κίνητρα, όπως τη φυσική ένταση μεταξύ αποδοτικότητας και ανθεκτικότητας στα συστήματα ΤΠ, τις ασυμμετρίες πληροφοριών. Προτείνει ότι για να ξεπεραστούν αυτές οι προκλήσεις είναι απαραίτητη η ρυθμιστική παρέμβαση. Ο Moore προσδιορίζει περαιτέρω την κλοπή ταυτότητας στο διαδίκτυο, την κατασκοπεία στον κυβερνοχώρο, την προστασία υποδομών ζωτικής σημασίας και τα botnets ως τις πιο επίμονες απειλές στην ασφάλεια στον κυβερνοχώρο και προτείνει μια σειρά επιλογών ρυθμιστικών λύσεων.

Άλλες προσπάθειες επικεντρώνονται στην εξέλιξη των πλαισίων κινδύνου, υποδειγματικής ανθεκτικότητας των επιχειρηματικών συστημάτων. Σε αυτά τα μοντέλα, οι ερευνητές προσπαθούν να κατανοήσουν πώς οι καταστροφές μπορεί να διαταράξουν τις παγκοσμίως κρίσιμες υπηρεσίες εξετάζοντας τη διασύνδεση των περιουσιακών στοιχείων. Δημιουργείται ένα μοντέλο βασισμένο σε απειλές και κάθε απειλή αποδίδεται με διαφορετικούς μηχανισμούς καταστροφής. σχετίζεται με συγκεκριμένα τρωτά σημεία· και παρουσιάζει διαφορετικές προκλήσεις για την ανθεκτικότητα των συστημάτων. Ο φόρος επί των απειλών αναπτύσσεται μέσω μιας εκτενούς ανασκόπησης των ιστορικών περιστατικών που επεκτάθηκαν ήδη από το 1000 μ.Χ. Όπως και στις ταξινομήσεις εγκλημάτων, αναζητούνται συσχετισμοί και μηχανισμοί ενεργοποίησης για διάφορους τύπους καταστροφών.

Μια παρόμοια προσέγγιση προτείνεται από τη Lloyds του Λονδίνου, όπου εξετάζουν φανταστικά αλλά ρεαλιστικά σενάρια για την κατανόηση της έννοιας της συγκέντρωσης κινδύνου στον κυβερνοχώρο. Οι συντάκτες της έκθεσης σημειώνουν ότι ο κίνδυνος στον κυβερνοχώρο αποτελεί αυξανόμενη παγκόσμια απειλή λόγω της αύξησης των περιστατικών στον κυβερνοχώρο τα τελευταία χρόνια. Χρησιμοποιούν δύο φανταστικά σενάρια, δηλαδή ένα hack «παρόχου υπηρεσιών cloud» και μια «μαζική ευπάθεια», και επιδιώκουν να υπολογίσουν το άμεσο και έμμεσο κόστος τόσο για τους οργανισμούς όσο και για τους ασφαλιστές. Καταλήγουν στο συμπέρασμα ότι η πιθανότητα κυβερνοεπίθεσης να σαρώσει πολλούς οργανισμούς και οι δευτερογενείς επιπτώσεις της επίθεσης λόγω αλληλεξάρτησης μεταξύ οργανισμών θα μπορούσαν να έχουν καταστροφικές συνέπειες.

Υπάρχουν μερικά ινστιτούτα, τα οποία παρέχουν συγκεντρωτικά δεδομένα και δημοσιεύουν ετήσιες εκθέσεις για περιστατικά στον κυβερνοχώρο. Για παράδειγμα, η έρευνα για τις παραβιάσεις της ασφάλειας στον κυβερνοχώρο (CSBS) από την κυβέρνηση του Ηνωμένου Βασιλείου καταγράφει ετησίως τις τάσεις στα συμβάντα στον κυβερνοχώρο και τις λεπτομέρειες των κινδύνων κυβερνοασφάλειας. Η έκθεση παρουσιάζει στατιστικά στοιχεία σχετικά με τον τρόπο λειτουργίας των οργανισμών στον κυβερνοχώρο και προσδιορίζει κοινούς τύπους απειλής. Για να σχολιάσει εν συντομία τα βασικά ευρήματα της έκθεσης του 2017, η έρευνα επισημαίνει

ότι όλες οι επιχειρήσεις του Ηνωμένου Βασιλείου είναι δυνητικά εκτεθειμένες σε απειλές στον κυβερνοχώρο. Οι κυβερνητικές πηγές καθοδήγησης σχετικά με τις απειλές κυβερνοασφάλειας παραμένουν λίγες, αλλά το 75% των οργανισμών, οι οποίοι επωφελούνται από αυτό το σχηματισμό, το βρίσκουν χρήσιμο. Έχουν εντοπίσει ότι μια σημαντική αύξηση των επιχειρήσεων εξακολουθεί να μην διαθέτει ελέγχους ασφαλείας παρά το γεγονός ότι η συντριπτική πλειονότητα αυτών έχει αυξήσει τον προϋπολογισμό τους για την ασφάλεια στον κυβερνοχώρο. Οι πιο συνηθισμένοι τύποι επιτυχημένων επιθέσεων σχετίζονται με τη λήψη δόλιων μηνυμάτων ηλεκτρονικού ταχυδρομείου από το προσωπικό (στο 72% των περιπτώσεων όπου οι εταιρείες εντόπισαν μια αισχρή επίθεση ή μια απόπειρα). Το επόμενο πιο συνηθισμένο ζήτημα σχετίζεται με ιούς, λογισμικό υποκλοπής spyware και κακόβουλο λογισμικό (33%), άτομα που παριστάνουν τον οργανισμό σε μηνύματα ηλεκτρονικού ταχυδρομείου ή στο διαδίκτυο (27%)

Με βάση τις εκθέσεις αυτές και βασιζόμενοι στο προηγούμενο έργο τους, οι Anderson et al. παρέχουν σειρά συστάσεων για την αντιμετώπιση της έλλειψης στατιστικών στοιχείων στην Ευρωπαϊκή Ένωση (ΕΕ) και την προώθηση του τομέα της οικονομίας της ασφάλειας. Προτείνουν στην ΕΕ τη θέσπιση ενός ολοκληρωμένου νόμου για την κοινοποίηση παραβιάσεων της ασφάλειας και τη δημοσίευση στατιστικών ζημιών. Εντοπίζουν επίσης ότι οι κοινές ευπάθειες μπορούν να προκαλέσουν διαδοχικές επιπτώσεις στις κυβερνοεπιθέσεις και να προτείνουν την ποικιλομορφία ως μέτρο ασφαλείας. Τέλος, αναδεικνύεται το πρόβλημα του ηθικού κινδύνου στις (Κρίσιμες Εθνικές Υποδομές) εθνικές υποδομές ζωτικής σημασίας (Critical National Infrastructure CNI) και προτείνεται η ρύθμιση προσεγγίσεων βέλτιστης πρακτικής για την κυβερνοασφάλεια για τα εν λόγω ενδιαφερόμενα μέρη.

Εστιάζοντας στα κίνητρα για το CNI και τις ρυθμιστικές προσεγγίσεις, η Laube et al. εξετάζει τα οικονομικά της υποχρεωτικής υποβολής εκθέσεων σχετικά με την ασφάλεια στις αρχές. Σχεδιάζουν ένα μοντέλο κύριου παράγοντα ικανό να περιγράψει συγκρούσεις συμφερόντων μεταξύ ρυθμιστικών αρχών και οργάνων. Το μοντέλο τους εξετάζει τις επενδύσεις στον έλεγχο ασφαλείας και τις δια-εξαρτήσεις των επιχειρήσεων, τις υποχρεωτικές αναφορές παραβιάσεων της ασφάλειας και τους ελέγχους ασφαλείας. Καταλήγουν στο συμπέρασμα ότι οι νόμοι, οι οποίοι επιβάλλουν την υποχρεωτική αναφορά παραβιάσεων της ασφάλειας, είναι απαραίτητοι για τις αλληλεξαρτώμενες εταιρείες υψηλής ασφάλειας με την προϋπόθεση ότι το κόστος γνωστοποίησης είναι χαμηλό.

Ο Kshetri προσπαθεί να καθορίσει έναν σκεπτικισμό κόστους-οφέλους χρησιμοποιώντας μια παρόμοια μεθοδολογία με τον Laube et al., αλλά επικεντρώνεται στην προοπτική του επιτιθέμενου. Προσδιορίζει τα χαρακτηριστικά των κυβερνοεγκληματιών, των θυμάτων κυβερνοεγκλήματος και των πρακτόρων επιβολής του νόμου και υποστηρίζει ότι αυτές οι τρεις κατηγορίες οντοτήτων, όταν αλληλεπιδρούν, οδηγούν σε μια φαύλη περιφρενική περιφρούση του κυβερνοεγκλήματος. Παρέχει έναν συνειρμό που εξετάζει τα οφέλη και το κόστος για έναν εισβολέα και τους λόγους για το αν μπορεί να συμβεί ένα έγκλημα στον κυβερνοχώρο. Αξίζει να σημειωθεί ότι οι συγγραφείς υποστηρίζουν ότι οι ψυχολογικές επιπτώσεις καθώς και η ποινική καταδίκη αποτελούν μέρος των ωφελών ή των απωλειών ενός επιτιθέμενου.

Οι Edwards et al., εξερεύνησαν ένα δημόσιο διαθέσιμο σύνολο δεδομένων για παραβιάσεις δεδομένων και εφάρμοσαν ένα γενικευμένο γραμμικό μοντέλο της Bayesian για να αποκαλύψουν τάσεις στις παραβιάσεις δεδομένων. Καταλήγουν στο συμπέρασμα ότι το μέγεθος και η συχνότητα των παραβιάσεων δεδομένων ήταν σταθερά τα τελευταία χρόνια, αλλά ο αντίκτυπός τους αυξάνεται λόγω της ικανότητας των παραγόντων απειλής να δημιουργούν καλύτερα έσοδα από την προσωπική διαμόρφωση και στον αυξανόμενο αριθμό ηλεκτρονικών χρηματοπιστωτικών συναλλαγών. Μια ενδιαφέρουσα προσέγγιση, η οποία βασίζεται στη μεθοδολογία «από πάνω προς τα κάτω» που περιγράφεται στον τομέα της εγκληματολογίας, παρουσιάζεται από την Nguyen et al. Οι συγγραφείς επιχείρησαν να αποσπάσουν «ασφάλιστρα» που ορισμένοι χρήστες θα ήταν πρόθυμοι να πληρώσουν για να προστατεύσουν τα περιουσιακά τους στοιχεία από κυβερνοεπιθέσεις. Τα αποτελέσματά τους δείχνουν ότι οι συμμετέχοντες στην έρευνά τους ήταν πρόθυμοι να πληρώσουν ένα ασφάλιστρο μεταξύ $ 9 και $ 11 μηνιαίως για την προστασία των λογαριασμών τους στα μέσα κοινωνικής δικτύωσης, ενώ ήταν πρόθυμοι να περιμένουν μεταξύ 8 και 9 επιπλέον λεπτών για να λάβουν τα μηνύματα ηλεκτρονικού ταχυδρομείου τους, υπό την προϋπόθεση ότι αυτά θα ήταν απαλλαγμένα από ανεπιθύμητα μηνύματα και μηνύματα ηλεκτρονικού "ψαρέματος".

4.4. Δημιουργώντας έσοδα από τα συμβάντα στον κυβερνοχώρο

Η δυνατότητα ποσοτικοποίησης της βλάβης θα επέτρεπε σε έναν οργανισμό να λαμβάνει καλύτερες αποφάσεις σχετικά με την αντιμετώπιση ενός συγκεκριμένου κινδύνου. Υπάρχει έλλειψη αποτελεσματικών μετρήσεων, εργαλείων και πλαισίων για την εκτίμηση της ζημίας από κυβερνοεπιθέσεις σε οργανισμούς. Οι προσεγγίσεις που έχουν εντοπιστεί είναι είτε ποσοτικές είτε ποιοτικές. Οι περισσότερες προσεγγίσεις προσπαθούν να μετατρέψουν σε χρήμα τις μετρικές τιμές εξόδου, σε όρους οικονομικής απώλειας, ώστε να είναι δυνατή η σύγκριση της ζημίας μεταξύ των περιστατικών στον κυβερνοχώρο. Οι προσεγγίσεις αυτές λαμβάνουν υπόψη το άμεσο και το έμμεσο κόστος που προκύπτει από μια κυβερνοεπίθεση για διάφορες ζημίες

Οι διακυμάνσεις στις τιμές των μετοχών έχουν προσελκύσει το ενδιαφέρον πολλών ερευνητών, με την ιδέα να συγκρίνουν την τιμή της μετοχής πριν και μετά από μια κυβερνοεπίθεση. Οι Telang και Wattel εστιάζουν στις εταιρείες ανάπτυξης λογισμικού και αναφέρουν ότι κατά μέσο όρο οι επιχειρήσεις χάνουν το 0,6% της αγοραίας αξίας τους όταν αποκαλύπτονται ευπάθειες λογισμικού. Όσον αφορά την έκθεση ή τη διαρροή δεδομένων πελατών, οι Acquisti κ. ά. παρέχουν σημαντικές στατιστικές αποδείξεις ότι υπάρχει αρνητική βραχυπρόθεσμη επίπτωση στην αξία των μετοχών, αλλά η επίπτωση αυτή μειώνεται ραγδαία με την πάροδο του χρόνου.

Περαιτέρω αποδείξεις για τις αρνητικές επιπτώσεις στην αγοραστική αξία ενός οργανισμού που μπορεί να προκύψουν από μια παραβίαση στον κυβερνοχώρο μόλις αυτή δημοσιοποιηθεί, παρουσιάζονται από τους Cavusoglu, Mishra και Raghunathan. Πιο πρόσφατα, εκφράστηκαν ανησυχίες σχετικά με τη συσχέτιση των διακυμάνσεων των τιμών των μετοχών με περιστατικά στον κυβερνοχώρο και, ειδικότερα, με παραβιάσεις δεδομένων. Ωστόσο, υπάρχουν τύποι επιθέσεων που δεν φαίνεται να έχουν αντίκτυπο στην αξία των μετοχών των οργανισμών, όπως το DoS. Σε παρόμοιο πνεύμα, οι Campbell et al. υποστηρίζουν ότι δεν υπάρχει αντίκτυπος όταν η

παραβίαση της ασφάλειας αφορά μη ευαίσθητα δεδομένα. Υπάρχει όμως μια σημαντική διαφορά, όταν η παραβίαση αφορά εμπιστευτικά δεδομένα, έχει ως αποτέλεσμα η αγοραστική αξία του οργανισμού να πέσει για λίγο. Τέλος, οι Kannan, Rees και Sridhar υποστηρίζουν ότι δεν υπάρχει σημαντική διαφορά στην απώλεια της αγοραστικής αξίας ανάλογα με το αν η παραβίαση της ασφάλειας επηρεάζει την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των δεδομένων. Όλα αυτά είναι ενδιαφέροντα σημεία, αλλά μαρτυρούν τη δυσκολία χαρακτηρισμού και ποσοτικοποίησης της βλάβης στον κυβερνοχώρο.

Άλλες προσεγγίσεις επικεντρώθηκαν στη «μέτρηση» της βλάβης λόγω ποιοτικών επιπέδων σοβαρότητας (ή παρενθέσεων, παρόμοιων με υψηλά, μεσαία, χαμηλά) με βάση το κατά πόσον ορισμένες επιθέσεις έχουν βλάβες εντός καθορισμένων ορίων κριτηρίων. Ένα άρθρο, για παράδειγμα, περιγράφει έξι κύρια επίπεδα επιπτώσεων κινδύνου από μέτρια (1) έως κρίσιμα για τις επιχειρήσεις (6), και τα χαρακτηριστικά για τα κριτήρια επιπτώσεων περιλαμβάνουν τη φήμη, το ανθρώπινο ανώτατο όριο και τα οικονομικά. Για τις μικρές επιπτώσεις, τα κατώτατα όρια είναι τα εξής: το όριο φήμης είναι μηδενικό έως περιορισμένο αρνητικό και καμία επίπτωση στη φήμη του ιδρύματος· Το όριο του ανθρώπινου κεφαλαίου είναι ότι η επίθεση επηρεάζει λιγότερο από το 5% των εργαζομένων και δεν υπάρχει αντίκτυπος στις προσλήψεις ή τη διατήρηση προσωπικού· και το όριο είναι ετήσια απώλεια κάτω του 1 εκατομμυρίου δολαρίων κατά το τρέχον οικονομικό έτος. Κάθε ένα από αυτά τα κατώτατα όρια (και οι συναφείς values) αυξάνεται καθώς η αξιολόγηση εξελίσσεται από

Μια πολύ ελπιδοφόρα προσέγγιση για τον ποσοτικό προσδιορισμό της βλάβης περιγράφεται λεπτομερώς σε έκθεση που δημοσιεύθηκε από το Παγκόσμιο Οικονομικό Φόρουμ. Στόχος της προσέγγισής τους είναι να κατανοήσουν τα οφέλη από την ψηφιοποίηση των υπηρεσιών και των υπηρεσιών των οργανισμών, το κόστος που μπορεί να προκύψει όταν μπορούν να πραγματοποιηθούν οι επιθέσεις, τον προσδιορισμό της απειλής που επιβάλλεται στα όργανα και να προσπαθήσουν να βρουν τη βέλτιστη επένδυση στην κυβερνοασφάλεια. Εισάγουν την έννοια του Cyber-Value-at-Risk (VaR) ως «μέτρο κινδύνου για ένα συγκεκριμένο χαρτοφυλάκιο και χρονικό ορίζοντα ως οριακή αξία ζημίας» . Η VaR εξετάζει την πιθανότητα ότι μια ζημία θα υπερβεί τα κέρδη σε ένα δεδομένο χρονικό διάστημα. Αυτοί οι συγγραφείς περιγράφουν τις ιδιότητες που πρέπει να έχει η τιμή Cyber-VaR, αλλά τονίζουν ότι δεν προδιαγράφουν τα μέσα για τον ποσοτικό προσδιορισμό και τον υπολογισμό αυτών των ιδιοτήτων. Ένα ολοκληρωμένο μοντέλο θα ήταν σε θέση να δώσει απαντήσεις όπως «δεδομένης μιας επιτυχημένης κυβερνοεπίθεσης, μια εταιρεία δεν θα χάσει περισσότερο από Χ ποσό χρημάτων σε μια χρονική περίοδο, με ακρίβεια 95%».

Τα βασικά στοιχεία ενός τέτοιου μοντέλου είναι ο ποσοτικός προσδιορισμός των περιουσιακών στοιχείων που απειλούνται, ο υπολογισμός των τρωτών σημείων και η δημιουργία απειλών υπέρ των αρχείων των επιτιθέμενων. Όσον αφορά τις ζημίες, παρέχουν ένα παράδειγμα για το πώς μπορούν να επηρεαστούν τα περιουσιακά στοιχεία μιας πετρελαϊκής εταιρείας και εντοπίζουν βλάβες σχετικά με τη μελλοντική απώλεια εσόδων, τις δικαστικές διαφορές και το κόστος δημοσίων σχέσεων, το κόστος διακοπής των επιχειρήσεων και τη ζημία φήμης, ακόμη και την πτώχευση εάν η επίθεση είναι επίμονη για ορισμένο αριθμό ημερών.

Είναι προφανές ότι τα μοντέλα που συλλογίζονται για τη βλάβη είναι σπάνια και είτε βασίζονται σε φανταστικά σενάρια είτε προσπαθούν να αιτιολογούν βλάβες με βάση στατιστικά στοιχεία σχετικά με το κόστος. Ωστόσο, ο ποσοτικός προσδιορισμός της βλάβης εξακολουθεί να αποτελεί άλυτο πρόβλημα για τους οργανισμούς. Οι περισσότερες προσεγγίσεις έχουν επικεντρωθεί στη διορατικότητα από τις τιμές των χρηματιστηρίων. Ωστόσο, υπολείπονται της εκτίμησης της βλάβης που σχετίζεται με κυβερνοεπιθέσεις και περιστατικά. Αυτό οφείλεται στο ότι συνήθως οι μειώσεις στις τιμές των χρηματιστηρίων είναι σύντομες, ενώ παραμελούνται οι δαπάνες που σχετίζονται με άλλους τύπους βλάβης, όπως οι σωματικές ζημίες ή το κόστος αντιμετώπισης συμβάντων. Το Cyber-VaR είναι ελπιδοφόρο, αλλά πρέπει να γίνουν πολύ περισσότερα πριν αυτό γίνει μια βιώσιμη επιλογή για τους οργανισμούς.

Με λίγα λόγια, πιστεύουμε ότι ένα μοντέλο που βασίζεται σε περιουσιακά στοιχεία μπορεί να παρέχει μια διαφορετική προοπτική σχετικά με την έννοια της βλάβης στον κυβερνοχώρο και οι γνώσεις από την εγκληματολογία και άλλους τομείς μπορούν να στηρίζουν τέτοιες προσπάθειες. Απαιτείται περαιτέρω έρευνα σχετικά με το θέμα του ποσοτικού προσδιορισμού των βλαβών (άμεσων και έμμεσων), ενδεχομένως μέσω της σύνδεσης με περιουσιακά στοιχεία και απειλές.

4.5. Εμφάνιση της βλάβης στον κυβερνοχώρο ως έννοια στους οργανισμούς

Η προέλευση της βλάβης στον κυβερνοχώρο έχει τις ρίζες της στον ψυχολογικό τομέα και περιγράφει τη βλάβη ή τις αρνητικές επιπτώσεις σε άτομα που μπορεί να προκύψει ως αποτέλεσμα αλληλεπιδράσεων στον κυβερνοχώρο (π.χ. κυβερνοεκφοβισμός). Τα τελευταία χρόνια, ο όρος αυτός, όπως και η ίδια η «βλάβη», διευρύνθηκε και εφαρμόστηκε σε γενικότερα πλαίσια. Η προσαρμογή της κυβερνο-βλάβης στην κυβερνοασφάλεια βασίζεται ευρύτερα σε αυτήν την εννοιολογική αντίληψη και έχει ως στόχο να επικεντρωθεί στις δυσμενείς επιπτώσεις των κυβερνοεπιθέσεων σε όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των ατόμων, των κοινοτήτων, των οργανισμών και των εθνών. Για παράδειγμα, υπάρχει βιβλιογραφία που διερευνά τη βλάβη στον κυβερνοχώρο στον τομέα του κυβερνοπολέμου. Εδώ, η βλάβη στον κυβερνοχώρο γίνεται χαλαρά αντιληπτή ως βλάβη που διαπράττεται μέσω του Διαδικτύου ή παρόμοια ηλεκτρονικά μέσα, που συνήθως περιλαμβάνει κάποια μορφή κυβερνο-συμβάντος ή σκόπιμης επίθεσης (όπως ένας ξένος που «χακάρει» μια επιχείρηση ή ένας εσωτερικός γνώστης που εισάγει μια μολυσμένη μονάδα δίσκου σε ένα σταθμό εργασίας). Η περιγραφή αυτή περιλαμβάνει άλλες ερευνητικές εργασίες που δείχνουν ότι η βλάβη στον κυβερνοχώρο μπορεί επίσης να προκληθεί με άλλα μέσα, όπως η εκμετάλλευση στον κυβερνοχώρο, όπου ο στόχος της επίθεσης είναι κυρίως η λήψη δεδομένων από το στοχευμένο σύστημα.

Το να εξετάσουμε την κυβερνο-βλάβη στο πλαίσιο των οργανισμών, κατά συνέπεια, είναι να εξετάσουμε τις αρνητικές επιπτώσεις που προκύπτουν από κυβερνο-γεγονότα ή περιστατικά που θα μπορούσαν να πραγματοποιηθούν που θα εμπλέκουν τον οργανισμό με οποιονδήποτε τρόπο. Τα περιστατικά θα μπορούσαν να είναι σκόπιμες επιθέσεις, όπως συστήματα συμβιβασμού ή ακούσια λόγω λαθών, σφαλμάτων χρηστών ή γενικά φυσικών φαινομένων, και μπορεί να προέρχονται από πρώην αστικά κόμματα καθώς και από το εσωτερικό του οργανισμού.

Αυτή η διάκριση βλάβης σε σκόπιμη και ακούσια έχει παραδοσιακά εντοπιστεί σε περιουσιακά στοιχεία στον κυβερνοχώρο: για παράδειγμα, ένα δίκτυο υπολογιστών μπορεί να μολυνθεί ή ένας διακομιστής ιστού να αναγκαστεί να αποσυνδεθεί λόγω επίθεσης DoS. Αλλά η εξάρτηση της κοινωνίας από την τεχνολογία έχει προκαλέσει τέτοια βλάβη γενικότερα. Η συνέπεια αυτού είναι ότι καθώς ο κυβερνοχώρος και οι φυσικοί χώροι αλληλεπικαλύπτονται, οι επιθέσεις σε επιχειρήσεις που χρησιμοποιούν τον κυβερνοχώρο μπορεί να έχουν απτή, offline βλάβη. Όπως αναφέρει το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ, η ζημία αυτή θα μπορούσε επίσης να περιλαμβάνει υλικές ζημιές σε περιουσιακά στοιχεία ή σωματική βλάβη. Η κατανόησή μας για τη βλάβη στον κυβερνοχώρο δεν θα πρέπει να περιορίζεται στα διαδικτυακά στοιχεία ενός συστήματος, αλλά θα πρέπει να επεκταθεί ώστε να συμπεριλάβει και τα στοιχεία εκτός σύνδεσης.

Υπήρξαν αρκετές επιθέσεις που έχουν παραδειγματιστεί από τη φυσική πραγματικότητα της βλάβης στον κυβερνοχώρο. Δύο από τα πιο σημαντικά είναι το πρόσφατο ουκρανικό μπλακάουτ, όπου το κακόβουλο λογισμικό διευκόλυνε το κλείσιμο ενός σταθμού παραγωγής ενέργειας και εμπόδισε την επανεκκίνηση βασικών συστημάτων. και την απομακρυσμένη αεροπειρατεία του Jeep Cherokee, όπου χάκερ λευκών καπελών απέκτησαν τον πλήρη έλεγχο του οχήματος, με αποτέλεσμα η κατασκευαστής αυτοκινήτων Chrysler να ανακαλέσει 1,4 εκατομμύρια οχήματα πριν από οποιαδήποτε κακόβουλη επίθεση. Η επίθεση Chrysler επέστησε την προσοχή της αυτοκινητοβιομηχανίας στους κινδύνους που μπορεί να δημιουργήσει το Διαδίκτυο των Πραγμάτων (IoT) σε όλους τους κατασκευαστές. Αυτές προσθέτουν στις άλλες πιο γνωστές επιπτώσεις των επιθέσεων, συμπεριλαμβανομένης της κατεστραμμένης εταιρικής φήμης, της απώλειας πελατών και επιχειρηματικών εταίρων και της (οικονομικής) αποζημίωσης των θιγόμενων μερών. όπως μαρτυρούν η Sony, η Target και η Ashley Madison. Είναι προφανές ότι η κυβερνο-βλάβη είναι ενδεχομένως μεγαλύτερη από το άθροισμα των επιπτώσεων που λαμβάνονται υπόψη στις παραδοσιακές εκτιμήσεις κινδύνου, και ότι **απαιτείται μια νέα ταξινόμηση που επικεντρώνεται στην κατανόηση του πλήρους φάσματος της βλάβης στον κυβερνοχώρο**.

Για να διευκολυνθεί η αποτελεσματικότερη συλλογιστική σχετικά με τη βλάβη στον κυβερνοχώρο και να αντιμετωπιστούν οι διάφορες προκλήσεις που εντοπίστηκαν σχετικά με τη μοντελοποίηση, είναι χρήσιμο να περιγραφεί μια ταξινόμηση για οργανωτικές βλάβες. Αυτό θα πρέπει να περιγράφει το φάσμα των κατηγοριών βλάβης και να τις δομεί κατά τρόπο που να επιτρέπει την εξέταση διαδοχικών βλαβών και σε μορφή που οι οργανισμοί θα μπορούν να εφαρμόζουν κατά τη διάρκεια αναλύσεων κινδύνου ασφαλείας. Ένα βασικό πλεονέκτημα θα ήταν επίσης ότι θα εξανάγκαζε την εξέταση των βλαβών που συνήθως δεν θεωρούνται «εταιρικές» και, ως εκ τούτου, σπάνια αξιολογούνται δεόντως. Ένα καλό παράδειγμα αυτού είναι η ψυχολογική βλάβη σε άτομα που προκύπτουν από κυβερνο επιθέσεις. Παρουσιάζεται παρακάτω μια τέτοια ταξινόμηση στον κυβερνοχώρο. Εκτός από τη βιβλιογραφία που εξετάστηκε παραπάνω, έχει πραγματοποιηθεί μια ολοκληρωμένη έρευνα για γνωστά περιστατικά στον κυβερνοχώρο που βρέθηκαν σε δημόσια διαθέσιμες βάσεις δεδομένων, σε συνδυασμό με περιπτωσιολογικές μελέτες και ειδήσεις.

Έχουν γίνει αρκετές προσπάθειες να προσδιοριστούν οι επιπτώσεις των κυβερνο επιθέσεων, ωστόσο, η χρήση και η υιοθέτησή τους είναι περιορισμένη. Για την ταξινόμηση αυτή,

δημιουργήθηκαν και αναλύθηκαν ένα σύνολο δεδομένων άρθρων ειδήσεων, βιβλιογραφίας και βάσεων δεδομένων κυβερνο συμβάντων. Πιο συγκεκριμένα, έχουν συλλεχθεί ειδησεογραφικά άρθρα, που δημοσιεύονται σε μεγάλες εφημερίδες και περιοδικά ασφαλείας, τα οποία απευθύνονται σε εθνικό και διεθνές κοινό. Ιδιαίτερο ενδιαφέρον έχει η βιβλιογραφία που εστιάζει στην ταξινόμηση πολλαπλών βλαβών που κυμαίνονται από εγκλήματα λευκού περιλαιμίου στην ψυχολογία.

Τέλος, σύνολα δεδομένων όπως το Hackmageddon και εκείνα από την κοινοτική βάση δεδομένων VERIS (VCDB), αν και περιορισμένα στην ποικιλία των επιθέσεων στον κυβερνοχώρο, χρησιμοποιήθηκαν λόγω της απουσίας πιο ολιστικών συνόλων δεδομένων. Το VCDB είναι μια δημόσια προσπάθεια συλλογής αναφορών συμβάντων κυβερνοασφάλειας με συγκεκριμένη δομή. Η ομάδα της Verizon RISK είναι υπεύθυνη για τη συντήρηση της βάσης δεδομένων, η οποία περιέχει περισσότερα από 5 000 περιστατικά. Από αυτά τα περιστατικά, επικεντρώθηκαν στις πιο σύγχρονες αναφορές που περιείχαν πληροφορίες σχετικές με την συγκεκριμένη ταξινόμηση, εξαιρουμένων των περιστατικών των οποίων η πηγή ήταν σωματικές επιθέσεις. Το Hackmageddon είναι ένας γνωστός ιστότοπος κυβερνο συμβάντων που συλλέγει δημόσιες αναφορές και τις τεκμηριώνει σε μηνιαία βάση.

Το ίδιο σκεπτικό με αυτό που ίσχυε με το VCDB σχετικά με την εξαγωγή σχετικών περιστατικών ακολουθήθηκε εδώ, και έγινε εστίαση και πάλι σε σύγχρονες εκθέσεις.

Στη συνέχεια, εφαρμόσθηκε ανάλυση περιεχομένου για την επεξεργασία των πηγών στο σύνολο των δεδομένων. Η ανάλυση περιεχομένου είναι μια ποιοτική τεχνική ανάλυσης δεδομένων, με στόχο τον προσδιορισμό βασικών «θεμάτων» στα έγγραφα. Υπάρχουν τρεις προσεγγίσεις στην ανάλυση περιεχομένου: η πρώτη είναι η επαγωγική προσέγγιση που βασίζεται στην «ανοικτή κωδικοποίηση», πράγμα που σημαίνει ότι οι κατηγορίες ή τα θέματα δημιουργούνται ελεύθερα από τον ερευνητή.

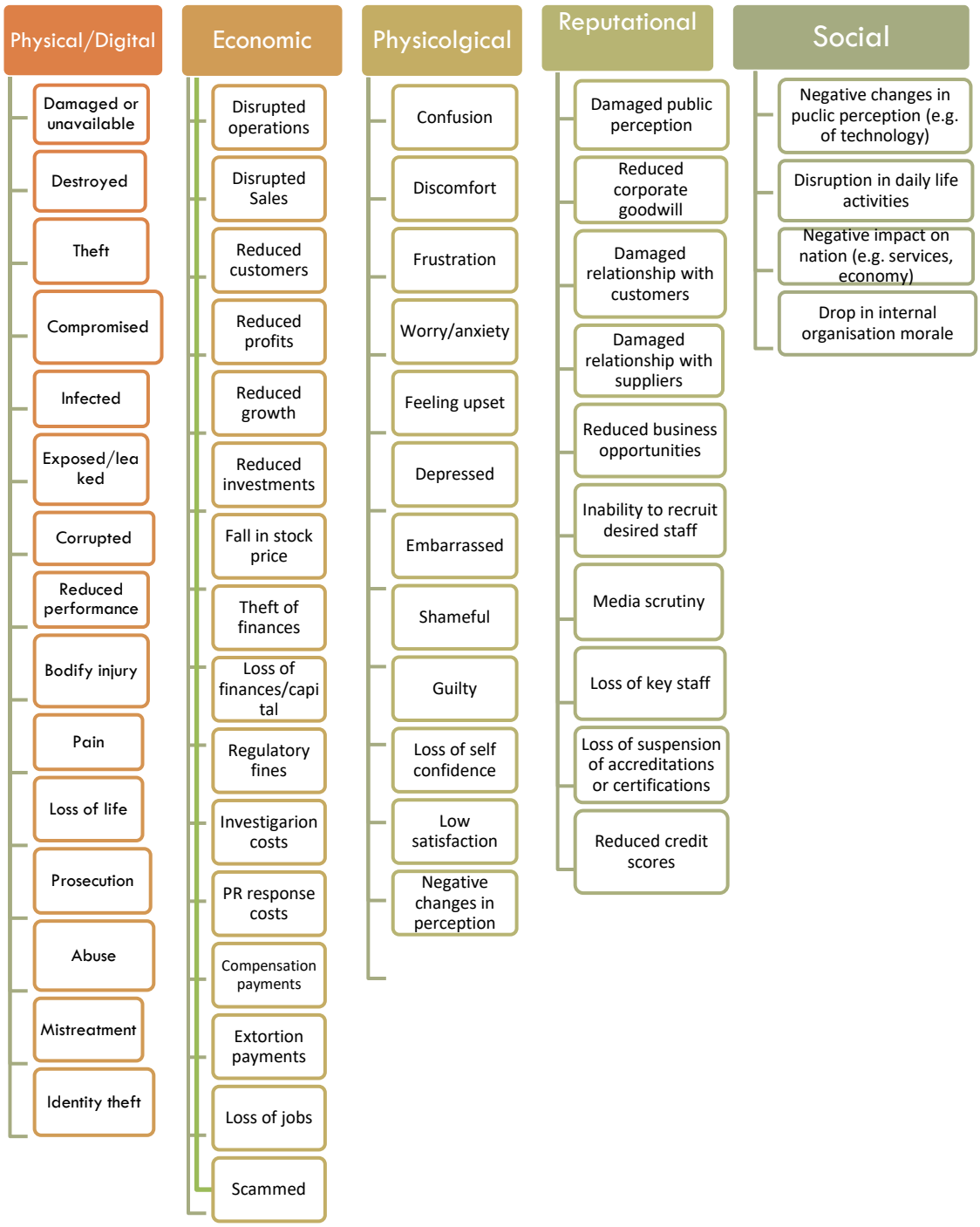
Η δεύτερη προσέγγιση είναι η αφαιρετική ανάλυση. Η προσέγγιση αυτή είναι πιο δομημένη από την επαγωγική μέθοδο και η αρχική κωδικοποίηση κατασκευάζεται από τα βασικά χαρακτηριστικά και τις μεταβλητές της υιοθετημένης θεωρίας. Κατά τη διαδικασία κωδικοποίησης, τα αποσπάσματα αποδίδονται σε κατηγορίες και τα ευρήματα υπαγορεύονται από τη θεωρία ή την προηγούμενη έρευνα. Ωστόσο, θα μπορούσαν να υπάρχουν νέες κατηγορίες που μπορεί να αντικρούσουν ή να εμπλουτίσουν μια συγκεκριμένη θεωρία. Ως εκ τούτου, εάν οι αφαιρετικές προσεγγίσεις ακολουθούνται αυστηρά, αυτές οι νέες κατηγορίες που προσφέρουν μια εκλεπτυσμένη προοπτική μπορεί να μην ληφθούν υπόψιν. Αυτός είναι ο λόγος για τον οποίο επιλέχθηκε ο τρίτος τύπος, ο οποίος είναι ένα μείγμα των αφαιρετικών και επαγωγικών προσεγγίσεων.
Χρησιμοποιήθηκαν βλάβες που εντοπίστηκαν στη βιβλιογραφία εγκλημάτων με λευκό περιλαίμιο και άλλες ταξινομήσεις βλαβών ως βασικά θέματα για την αφαιρετική προσέγγισή.
Μόλις αναπτύχθηκαν όλα τα σχετικά θέματα, χωρίστηκαν οι τύποι βλάβης σε κατηγορίες για να σχηματιστούν ιεραρχίες βλάβης. Στη συνέχεια, εξετάστηκε η προκύπτουσα δομή στο πλαίσιο ενός μικρότερου συνόλου κυβερνο συμβάντων για να καθοριστεί εάν η βλάβη από αυτά τα περιστατικά

θα μπορούσε να διαμορφωθεί και να ενσωματωθούν τυχόν βελτιώσεις (π.χ. να εντοπιστούν περιστατικά που δεν θα μπορούσαν να περιγραφούν από τα είδη βλάβης στην ταξινόμηση) που είναι απαραίτητα. Οι ιεραρχίες που ορίζουμε στην ταξινόμηση, συμβάλλουν στην καινοτομία της έρευνας, δεδομένου ότι τα υπάρχοντα μοντέλα επικεντρώνονται μόνο σε καταλόγους επιπτώσεων και απωλειών από κυβερνοεπιθέσεις. Η παροχή δομής μέσω μιας ταξινόμησης βλάβης είναι χρήσιμη, ιδίως όσον αφορά τη συνεργασία με διαφορετικούς τύπους ενδιαφερόμενων μερών που ενδέχεται να επηρεαστούν με διαφορετικούς τρόπους από κυβερνοεπιθέσεις. Επιπλέον, επιτρέπει αργότερα να εξεταστεί πώς οι βλάβες διαδίδονται μεταξύ διαφορετικών κατηγοριών υψηλού και χαμηλού επιπέδου κατά τη χρονική περίοδο μετά την εμφάνιση μιας επίθεσης.

Οι κύριοι τύποι βλαβών στους οποίους αναφερόμαστε φαίνονται στον παρακάτω Πίνακα 1

Πίνακας 1: Κύριοι τύποι βλαβών

•Φυσική ή ψηφιακή βλάβη	Βλάβη που περιγράφει μια φυσική ή ψηφιακή αρνητική επίδραση σε κάποιον ή κάτι
•Οικονομική ζημία	ζημιά που σχετίζεται με αρνητική οικονομική ή οικονομικές συνέπειες
•Ψυχολογική βλάβη	βλάβη που επικεντρώνεται σε ένα άτομο και την ψυχική του ευεξία και ψυχή
• Βλάβη φήμης	Βλάβη που σχετίζεται με τη γενική γνώμη που ισχύει για μια οντότητα
•Κοινωνική βλάβη	βλάβες που μπορούν να προκύψουν σε ένα κοινωνικό πλαίσιο ή μια ευρύτερη κοινωνία



ΕΙΚΟΝΑ 3 : ***ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΟΡΓΑΝΩΤΙΚΩΝ ΒΛΑΒΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ***

Για κάθε έναν από αυτούς τους τύπους, εντοπίσαμε πολλούς υπο-τύπους που χαρακτηρίζει την κάθε βλάβη με περισσότερες λεπτομέρειες.

Στο Σχήμα 1 παραπάνω, παρουσιάζονται και περιγράφονται οι κύριοι υπο-τύποι. Οι τύποι βλαβών είναι σχεδιασμένοι να είναι διακριτικοί, ωστόσο, όλοι οι τύποι μπορούν να επιχειρηθούν να ερμηνευτούν με οικονομικούς όρους. Έτσι, η οικονομική ζημιά μπορεί να επικαλύπτεται με άλλους τύπους βλαβών.

Εν συντομία αναλογιζόμενοι μια επιλογή των ορισμών βλάβης που περιέχονται παραπάνω: παραδείγματα βλάβης φήμης που μπορεί να υποστεί ένας οργανισμός ως αποτέλεσμα ενός κυβερνο-συμβάντος είναι κατεστραμμένη δημόσια εικόνα ενός οργανισμού (π.χ. ένας οργανισμός μπορεί να θεωρηθεί ανασφαλής ή ανίκανος να προστατεύσει τα δεδομένα των πελατών) και μειωμένη εταιρική καλή θέληση (δηλαδή η επιχείρηση γίνεται μια επιχείρηση που άλλοι διστάζουν να αλληλεπιδράσουν ή να συναλλάσσονται). Οι βλάβες στον κοινωνικό και κοινωνικό χώρο κυμαίνονται από αρνητικές αλλαγές της αντίληψης του κοινού (π.χ. μετά από μια επίθεση, το κοινό μπορεί να θεωρήσει ένα συγκεκριμένο είδος τεχνολογίας αναξιόπιστο ή ανασφαλές), έως τη διακοπή της καθημερινής ζωής του κοινού. Για παράδειγμα, η κυβερνοεπίθεση σε μια ουκρανική εταιρεία ηλεκτρικής ενέργειας προκάλεσε μπλακάουτ που επηρέασε 700 000 σπίτια, πολυάριθμες κοινότητες και την κοινωνία στο σύνολό της στη χώρα. Αυτή η επίθεση είχε άμεσο αντίκτυπο στην κοινωνία και η βλάβη που προκλήθηκε είναι ανάλογη με την ταχύτητα ανίχνευσης και τους αποτελεσματικούς ελέγχους μετριασμού. Καθώς τα κράτη και κατ επέκταση οι οργανισμοί, ποικίλλουν στην ωριμότητα τους στον κυβερνοχώρο, θα υπάρξει ποικιλία στην έκταση αυτών των βλαβών.

Η σωματική ή ψηφιακή βλάβη είναι ένας από τους πιο γνωστούς τύπους βλάβης για τους οργανισμούς και παραδείγματα της είναι: κατεστραμμένα ή μη ικανά συστήματα. κατεστραμμένα αρχεία δεδομένων. εκροή ή κλοπή ευαίσθητων δεδομένων ή δεδομένων πελατών· σωματική βλάβη των εργαζομένων ή των πελατών. Από αυτά τα παραδείγματα, μπορεί να δει κανείς ότι στο τρέχον επίπεδο περιγραφής της ταξινόμησης (όπως φαίνεται στην Σχήμα 1) τα περιουσιακά στοιχεία δεν ονομάζονται συγκεκριμένα. Αυτό είναι σκόπιμο και επιτρέπει στους χρήστες της ταξινόμησης είτε να διατηρήσουν ξεχωριστή καταχώριση περιουσιακών στοιχείων (ή ταξινόμηση περιουσιακών στοιχείων) και να χαρτογραφούν τα δύο ανάλογα με τις ανάγκες, είτε να προσθέσουν μια διαφορετική κατηγορία στην εν λόγω ταξινόμηση για να περιγράψουν λεπτομερώς τα σχετικά περιουσιακά στοιχεία που ενδέχεται να βλαφθούν με τον συγκεκριμένο τρόπο. Η απόφασή αυτή πάρθηκε από το γεγονός ότι η διαχείριση τέτοιων περιουσιακών στοιχείων επιτυγχάνεται με διαφορετικές μεθοδολογίες σε οργανισμούς. Η αφαίρεση της ταξινόμησης όπως διατάσσεται παραπάνω ακολουθεί παρόμοια προσέγγιση με μία από τις πιο γνωστές ταξινομήσεις συμβάντων υπολογιστών.

Ένα από τα επιδιωκόμενα πλεονεκτήματα της ταξινόμησης αυτής είναι η σαφής χαρτογράφηση των βασικών τύπων και των υπο-τύπων κυβερνο-βλάβης. Ενόψει ενός περιστατικού, επομένως, οι οργανισμοί θα μπορούσαν γρήγορα να αποκτήσουν κάποια γενική κατανόηση των τύπων της προκύπτουσας βλάβης που μπορεί να αντιμετωπίσουν. Αυτό είναι επίσης σημαντικό, διότι μπορεί να αναγκάσει την εξέταση πτυχών που συνήθως δεν θεωρούνται «εταιρικές» και, ως εκ τούτου, σπάνια αξιολογούνται δεόντως. Επιπλέον, αυτό διευρύνει την κατανόηση του κινδύνου και θα μπορούσε να ενσωματωθεί και κατά τις αρχικές φάσεις εκτίμησης κινδύνου. Ένα καλό παράδειγμα

αυτού είναι η ψυχολογική βλάβη στα άτομα. Εάν μια επιχείρηση πέσει θύμα κυβερνοεπίθεσης, αυτό δεν επηρεάζει μόνο αυτούς αλλά και τα άτομα, συμπεριλαμβανομένων των πελατών και των εργαζομένων. Στην επίθεση στον πάροχο υπηρεσιών Διαδικτύου του Ηνωμένου Βασιλείου Talk Talk το 2015, οι πελάτες όχι μόνο βίωσαν οικονομικές απώλειες, αλλά αισθάνθηκαν ανήσυχοι και αναστατωμένοι για την επίθεση και την απάντηση της TalkTalk.

Αυτό θα μπορούσε να ενδιαφέρει έναν οργανισμό, επειδή τέτοιες βλάβες θα μπορούσαν να επηρεάσουν περαιτέρω τη φήμη της εταιρείας και να επηρεάσουν τις επιχειρήσεις πελατών ή να οδηγήσουν τους πελάτες να συστήσουν στους φίλους και τους συναδέλφους τους να αποφεύγουν εντελώς την εταιρεία. Πλατφόρμες μέσων κοινωνικής δικτύωσης όπως το Twitter μπορούν να επιδεινώσουν αυτή τη βλάβη λόγω της μεγάλης προβολής που δίνουν στους πελάτες και στο κοινό. Αυτό αναδεικνύει ένα υποσύνολο του ευρέος φάσματος των επακόλουθων βλαβών, που καταγράφονται στην ταξινόμηση, που προκύπτουν από κυβερνο-περιστατικά.

Σε επόμενη ενότητα θα εξετάσουμε μελέτες περίπτωσης επιθέσεων στον πραγματικό κόσμο, οι οποίες παρέχουν αρχικές πληροφορίες σχετικά με τον τρόπο με τον οποίο η παραπάνω ταξινόμηση μπορεί να χρησιμοποιηθεί για τον εντοπισμό αλληλουχιών διάδοσης διαφορετικών τύπων κυβερνο-βλαβών, δείχνοντας έτσι πώς μπορεί να προκύψει επίθεση στον κυβερνοχώρο και να διαδοθεί.

Οι τέσσερις περιπτωσιολογικές μελέτες επιλέχθηκαν με βάση τις λεπτομερείς μαρτυρίες για τον αντίκτυπο των κυβερνοεπιθέσεων στις οργανώσεις που ήταν διαθέσιμες στο κοινό και λόγω των μακροχρόνιων επιπτώσεων αυτών των επιθέσεων. Χρησιμοποιώντας τις βλάβες στην προτεινόμενη ταξινόμηση στόχος είναι να διερευνηθούν κοινές αλληλουχίες βλαβών, οι οποίες μπορεί να προκύψουν δεδομένου ότι έχει συμβεί μια αρχική βλάβη.

Αυτή η ανάλυση πραγματοποιείται για να δειχθεί ότι η ταξινόμηση μπορεί να χαρακτηρίσει επαρκώς τις βλάβες που προκύπτουν σε τέτοια σενάρια. Αυτό θα μπορούσε, ωστόσο, να χρησιμοποιηθεί και για την καλύτερη κατανόηση του ευρύτερου κινδύνου που αντιμετωπίζει ο οργανισμός ή η επιχείρηση κατά μήκος των διαστάσεων που προτείνουν οι Beck και Giddens.

ΚΕΦΑΛΑΙΟ 5

5.1. ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΑΠΟ ΤΙΣ ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

5.1.1. Έρευνα του Ponemon Institute

Σε ένα συνεχώς εξελισσόμενο ψηφιακό περιβάλλον, είναι σημαντικό να διατηρήσουμε τον βηματισμό μας με τις τάσεις στην κυβερνο απειλή. Ανακαλύψαμε ότι οι κυβερνοεπιθέσεις αλλάζουν εξαιτίας:

Εξελισσόμενων στόχων: Η κλοπή πληροφοριών είναι η πιο ακριβή και ταχύτερη αυξανόμενη συνέπεια του εγκλήματος στον κυβερνοχώρο – αλλά τα δεδομένα δεν είναι ο μόνος στόχος

Εξελισσόμενων αντίκτυπων: Ενώ τα δεδομένα παραμένουν στόχος, η κλοπή δεν είναι πάντα το αποτέλεσμα. Ένα νέο κύμα κυβερνοεπιθέσεων βλέπει δεδομένα όχι πλέον απλά να αντιγράφονται αλλά να καταστρέφονται –ή να αλλάζουν–, οπότε επιφέρουν μια δυσπιστία. Η επίθεση στην ακεραιότητα των δεδομένων είναι το επόμενο σύνορο

Εξελισσόμενων τεχνικών: Οι εγκληματίες του κυβερνοχώρου προσαρμόζουν τις μεθόδους των επιθέσεων τους. Χρησιμοποιούν τον άνθρωπο – τον πιο αδύναμο κρίκο – ως μονοπάτι σε επιθέσεις, όπως αυξημένο ηλεκτρονικό «ψάρεμα» και κακόβουλων λογισμικών. Άλλες τεχνικές, όπως αυτές που χρησιμοποιούνται από έθνη-κράτη σε επιχειρήσεις – στόχους, μεταβάλλουν τη φύση της ανάκαμψης, με ασφαλιστικές εταιρείες να προσπαθούν να χαρακτηρίσουν τις κυβερνοεπιθέσεις ως θέμα «πολέμου».

Σύμφωνα με την έκθεση Accenture "Διασφάλιση της ψηφιακής οικονομίας" [5]οι επιχειρήσεις δεν εξαρτώνταν ποτέ περισσότερο από την ψηφιακή οικονομία και το Διαδίκτυο για την ανάπτυξη τους. Λιγότερες από μία στις τέσσερις εταιρείες βασίστηκαν στο Διαδίκτυο για τις επιχειρηματικές τους δραστηριότητες πριν από 10 χρόνια· τώρα, αυτό το ποσοστό αγγίζει το 100%. Σύμφωνα με το 90% των στελεχών των επιχειρήσεων η ψηφιακή οικονομία είναι ζωτικής σημασίας για την μελλοντική ανάπτυξη του οργανισμού τους ή της επιχείρησής τους η ώθηση όμως για την ψηφιακή καινοτομία εισάγει νέους κινδύνους.

Ενώ η εξάρτηση από το Διαδίκτυο και η ψηφιακή οικονομία ανθίζουν, το 68% των ηγετών των επιχειρήσεων δήλωσαν ότι οι κίνδυνοι κυβερνοασφάλειας ομοίως αυξάνεται. Σχεδόν το 80% των οργανισμών εισάγουν ψηφιακά τροφοδοτούμενη καινοτομία ταχύτερα από την ικανότητά τους να προστατευτούν από τις κυβερνοεπιθέσεις. Δεν είναι περίεργο, λοιπόν, ότι οι κυβερνοεπιθέσεις και η απάτη δεδομένων ή η κλοπή είναι τώρα δύο από τους πέντε κορυφαίους κινδύνους που είναι πιο

[5] *Securing the digital economy, Accenture https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy*

πιθανό να αντιμετωπίσουν οι διευθύνοντες των οργανισμών ή επιχειρήσεων σύμφωνα με την τελευταία έκθεση του Παγκόσμιου Οικονομικού Φόρουμ για τους παγκόσμιους κινδύνους.

Στο πλαίσιο αυτού του δύσκολου περιβάλλοντος, η έρευνά του Ponemon Institute αποκαλύπτει ότι το έγκλημα στον κυβερνοχώρο αυξάνεται σε μέγεθος και πολυπλοκότητα. Η έκθεση προσφέρει μια πρόσθετη προοπτική, μια μακρόπνοη προβολή της οικονομικής αξίας που κινδυνεύει από μελλοντικές κυβερνοεπιθέσεις κατά την επόμενη πενταετία.

Καθώς ο αριθμός των κυβερνοεπιθέσεων αυξάνεται και χρειάζεται περισσότερο χρόνο για να επιλυθεί, το κόστος του εγκλήματος στον κυβερνοχώρο συνεχίζει να αυξάνεται.

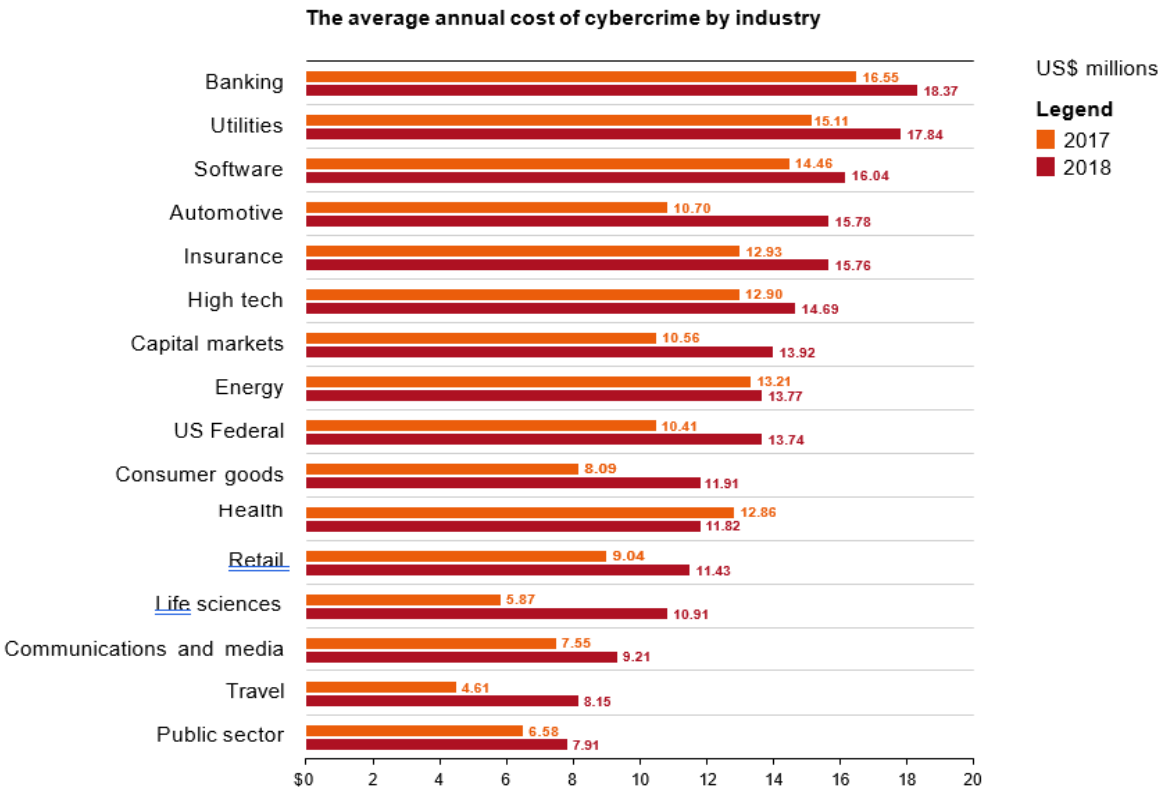
Τον τελευταίο χρόνο, παρατηρήθηκαν πολλές μυστικές, εξελιγμένες και στοχευμένες κυβερνοεπιθέσεις εναντίον οργανισμών του δημόσιου και του ιδιωτικού τομέα. Σε συνδυασμό με το διευρυνόμενο τοπίο απειλών, οι οργανισμοί βλέπουν μια σταθερή αύξηση στον αριθμό παραβιάσεων ασφάλειας — από 130 το 2017 σε 145 το 2018.

Για τους σκοπούς αυτής της μελέτης, ορίστηκαν οι κυβερνοεπιθέσεις ως κακόβουλη δραστηριότητα που διεξάγεται κατά του οργανισμού μέσω της υποδομής πληροφορικής μέσω των εσωτερικών ή εξωτερικών δικτύων ή του Διαδικτύου.

Οι κυβερνοεπιθέσεις περιλαμβάνουν επίσης επιθέσεις κατά βιομηχανικών συστημάτων ελέγχου (ICS). Μια παραβίαση ασφαλείας είναι αυτή που έχει ως αποτέλεσμα στη διείσδυση των βασικών δικτύων ή εταιρικών συστημάτων μιας εταιρείας. Δεν περιλαμβάνει την πληθώρα των επιθέσεων που σταμάτησαν οι άμυνες τείχους προστασίας μιας εταιρείας.

Ο αντίκτυπος αυτών των κυβερνοεπιθέσεων σε οργανισμούς, βιομηχανίες και κοινωνία είναι σημαντικός. Παράλληλα με τον αυξανόμενο αριθμό παραβιάσεων της ασφάλειας, το συνολικό κόστος του εγκλήματος στον κυβερνοχώρο για κάθε εταιρεία αυξήθηκε από 11,7 εκατομμύρια δολάρια ΗΠΑ το 2017 σε νέο υψηλό 13,0 εκατομμυρίων δολαρίων ΗΠΑ το 2018 — μια αύξηση 12 τοις εκατό).

Η λεπτομερής αυτή ανάλυσή δείχνει ότι οι τραπεζικοί κλάδοι και οι κλάδοι κοινής ωφέλειας εξακολουθούν να έχουν το υψηλότερο κόστος ηλεκτρονικού εγκλήματος σε όλο το δείγμα μας με αύξηση 11 τοις εκατό και 16 τοις εκατό αντίστοιχα. Ο ενεργειακός τομέας παρέμεινε αρκετά σταθερός κατά τη διάρκεια του έτους με μικρή αύξηση 4 τοις εκατό, αλλά ο κλάδος της υγείας σημείωσε ελαφρά μείωση του κόστους του εγκλήματος στον κυβερνοχώρο κατά οκτώ τοις εκατό (βλέπε Εικόνα 4).



ΕΙΚΟΝΑ 4: ΤΟ ΜΕΣΟ ΕΤΗΣΙΟ ΚΟΣΤΟΣ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΑΝΑ ΠΕΡΙΟΧΗ

"The Cost of Cybercrime" Ninth Annual Cost of Cybercrime Study, Unlocking the Value of improved Cybersecurity Protection, Ponemon Institute

Η ανάλυση σχεδόν 1.000 κυβερνοεπιθέσεων ανέδειξε το κακόβουλο λογισμικό ως τις πιο συχνές επιθέσεις συνολικά και, σε πολλές χώρες, τις πιο ακριβές για επίλυση. Οι επιθέσεις που βασίζονται σε ανθρώπους δείχνουν μερικές από τις μεγαλύτερες αυξήσεις κατά τη διάρκεια του έτους. Ο αριθμός των οργανισμών που αντιμετωπίζουν επιθέσεις ransomware αυξήθηκαν κατά 15 τοις εκατό σε διάστημα ενός έτους και έχει υπερτριπλασιαστεί σε συχνότητα σε διάστημα δύο ετών. Ηλεκτρονικό ψάρεμα (phishing) και επιθέσεις κοινωνικής μηχανικής βιώνουν τώρα το 85 τοις εκατό των οργανισμών, μια αύξηση 16 τοις εκατό σε διάστημα ενός έτους - κάτι που αποτελεί ανησυχία όταν οι άνθρωποι εξακολουθούν να είναι ο πιο αδύναμος κρίκος στην άμυνα στον κυβερνοχώρο.

• Υπάρχουν διάφοροι τρόποι με τους οποίους διαφορετικοί τύποι κυβερνοεπιθέσεων συμβάλλουν στις συνέπειες του εγκλήματος στον κυβερνοχώρο. Ο χάρτης θερμότητας υποδεικνύει τη μεγαλύτερη συμβολή από κάθε τύπο επίθεσης. Για παράδειγμα, η κύρια συνέπεια μιας κακόβουλης επίθεσης κώδικα είναι η απώλεια πληροφοριών, ακολουθούμενη από απώλεια εσόδων παράλληλα με την επιχειρηματική διαταραχή.

• Οι διαδικτυακές επιθέσεις έχουν ελάχιστες επιπτώσεις σε ζημιές στον εξοπλισμό.

• Ομοίως, ο χάρτης υποδεικνύει επίσης ότι το κακόβουλο λογισμικό, οι επιθέσεις που βασίζονται στο Web και οι επιθέσεις άρνησης υπηρεσίας είναι οι κύριοι παράγοντες που συμβάλλουν στην απώλεια εσόδων.

Με την απώλεια πληροφοριών να προκαλεί αυξανόμενη ανησυχία, ο χάρτης θερμότητας επισημαίνει το κακόβουλο λογισμικό, τις επιθέσεις που βασίζονται στο Web και τον κακόβουλο κώδικα ως τους κύριους παράγοντες που συμβάλλουν. Οργανισμοί που επιθυμούν να μειώσουν τον αντίκτυπο της απώλειας πληροφοριών θα πρέπει να επικεντρώσουν τους πόρους σε αυτού του είδους τις επιθέσεις. Η επιχειρηματική διαταραχή συνεχίζει να αυξάνεται σταθερά και είναι η δεύτερη μεγαλύτερη συνέπεια του εγκλήματος στον κυβερνοχώρο. Οι πόροι θα πρέπει να επικεντρώνονται σε επιθέσεις άρνησης υπηρεσίας, κακόβουλους insiders και επιθέσεις κακόβουλου λογισμικού για τη μείωση αυτού του κόστους. Θα πρέπει επίσης να δοθεί προσοχή στον ρυθμό ανάπτυξης σε κάθε είδος επίθεσης. Οι οικονομικές συνέπειες του ransomware έχουν αυξηθεί κατά 21 τοις εκατό μόνο τον τελευταίο χρόνο. Αν και είναι ένα από τα μικρότερα κόστη του εγκλήματος στον κυβερνοχώρο συνολικά, οι οργανισμοί δεν πρέπει να παραβλέπουν αυτή την ταχέως αναπτυσσόμενη απειλή.

Ο πιο ακριβός τύπος επίθεσης για τους οργανισμούς σύμφωνα με τη μελέτη είναι το Malware. Έχει αυξηθεί 11% σε ένα χρόνο αλλά και το κόστος του τύπου malicious insider έχει σημειώσει αύξηση 15%.

ΕΙΚΟΝΑ 5 ΣΥΝΕΠΕΙΕΣ ΔΙΑΦΟΡΕΤΙΚΩΝ ΤΥΠΩΝ ΚΥΒΕΡΝΟΑΠΕΙΛΩΝ
"The Cost of Cybercrime" Ninth Annual Cost of Cybercrime Study, Unlocking the Value of improved Cybersecurity Protection, Ponemon Institute

(average annual cost; figures in US$ million; 2018 total = US$13.0 million)

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ –	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ –	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ –	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ –	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

5.1.2. Μελέτη του Κέντρου Στρατηγικών και Διεθνών Μελετών (CSIS) [6]

Το Κέντρο Στρατηγικών και Διεθνών Μελετών (CSIS) είναι ένας μη κερδοσκοπικός ερευνητικός οργανισμός αφιερωμένος στην παροχή στρατηγικών πληροφοριών και λύσεων πολιτικής για να βοηθήσει τους υπεύθυνους λήψης αποφάσεων να χαράξουν μια πορεία προς έναν καλύτερο κόσμο.

Το 2014, το CSIS υπολόγισε ότι το έγκλημα στον κυβερνοχώρο κοστίζει στην παγκόσμια οικονομία σχεδόν 500 δισεκατομμύρια δολάρια, ή περίπου το 0,7% του παγκόσμιου εισοδήματος. Αυτό είναι περισσότερο από το εισόδημα όλων εκτός κάποιων μικρών χωρών, καθιστώντας το έγκλημα στον κυβερνοχώρο μια πολύ προσοδοφόρα ενασχόληση. Η τρέχουσα εκτίμησή είναι ότι το έγκλημα στον κυβερνοχώρο μπορεί τώρα να κοστίσει στον κόσμο σχεδόν 600 δισεκατομμύρια δολάρια, ή 0,8% του παγκόσμιου ΑΕΠ. Οι λόγοι αυτής της αύξησης είναι οι εξής:

* Γρήγορη έγκριση των νέων τεχνολογιών από εγκληματίες του κυβερνοχώρου
* Ο αυξημένος αριθμός νέων χρηστών στο διαδίκτυο (αυτοί τείνουν να προέρχονται από χώρες χαμηλού εισοδήματος με αδύναμη ασφάλεια στον κυβερνοχώρο)
* Η αυξημένη ευκολία διάπραξης του εγκλήματος στον κυβερνοχώρο, με την ανάπτυξη του Cybercrime-as-a-Service
* Ένας διευρυνόμενος αριθμός «κέντρων» εγκλήματος στον κυβερνοχώρο που περιλαμβάνει τώρα τη Βραζιλία, την Ινδία, τη Βόρεια Κορέα και το Βιετνάμ
* Μια αυξανόμενη οικονομική πολυπλοκότητα μεταξύ των κορυφαίων εγκληματιών στον κυβερνοχώρο που, μεταξύ άλλων, διευκολύνει τη δημιουργία εσόδων.

Και σε αυτή την έρευνα οι τράπεζες παραμένουν ο αγαπημένος στόχος των ειδικευμένων εγκληματιών στον κυβερνοχώρο. Αυτό φυσικά ισχύει για περισσότερο από μια δεκαετία. Το έγκλημα στον κυβερνοχώρο επιβάλλει βαρύ κόστος στα χρηματοπιστωτικά ιδρύματα καθώς αγωνίζονται να καταπολεμήσουν την απάτη και την καθαρή κλοπή. Μια έκθεση αναφέρει ότι οι τράπεζες δαπανούν τρεις φορές περισσότερα για την ασφάλεια στον κυβερνοχώρο από τα μη χρηματοπιστωτικά ιδρύματα, και υπάρχει συμφωνία μεταξύ των ρυθμιστικών αρχών των τραπεζών σχετικά με ότι το έγκλημα στον κυβερνοχώρο συνιστά «συστηματικό» κίνδυνο για τη χρηματοπιστωτική σταθερότητα.

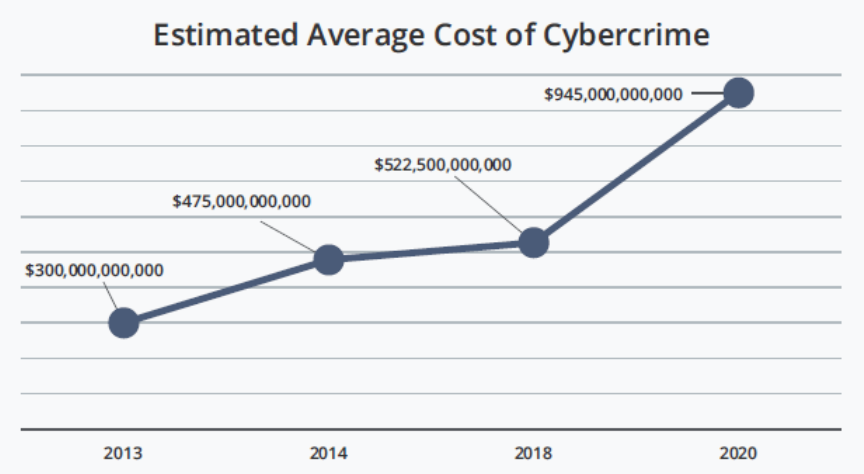
Το 2016, η ηλεκτρονική βάση δεδομένων της SEC για οικονομικές αρχειοθετήσεις παραβιάστηκε και οι εισβολείς ήταν σε θέση να έχουν πρόσβαση σε απόρρητες πληροφορίες. Η Επιτροπή Κεφαλαιαγοράς αναγνώρισε δημόσια την εισβολή τον Σεπτέμβριο του 2017, λέγοντας ότι οι χάκερ μπορεί να χρησιμοποίησαν τις πληροφορίες για να πραγματοποιήσουν επικερδείς συναλλαγές.

Από το 2018, εκτιμήθηκε ότι το κόστος του παγκόσμιου εγκλήματος στον κυβερνοχώρο ξεπέρασε το 1 τρισεκατομμύριο δολάρια.

[6] Report (The Hidden Costs of Cybercrime, by Zhanna Malekos Smith and Eugenia Lostri, James A. Lewis, Project Director), December 2020)

Υπολογίσαμε τη χρηματική απώλεια από το έγκλημα στον κυβερνοχώρο σε περίπου 945 δισεκατομμύρια δολάρια. Σε αυτό προστέθηκαν οι παγκόσμιες δαπάνες για την κυβερνοασφάλεια, οι οποίες αναμενόταν να ξεπεράσουν τα 145 δισεκατομμύρια δολάρια το 2020. Σήμερα, αυτό είναι $1 τρισεκατομμύριο δολάρια σύρετε στην παγκόσμια οικονομία.

Η έκθεσή αυτή για το 2018 διαπίστωσε ότι το έγκλημα στον κυβερνοχώρο κόστισε στην παγκόσμια οικονομία περισσότερα από 600 δισεκατομμύρια δολάρια. Η νέα εκτίμηση δείχνει αύξηση άνω του 50% σε δύο χρόνια.



ΕΙΚΟΝΑ 6 ***(THE HIDDEN COSTS OF CYBERCRIME, DECEMBER 2020)***

Αμέσως μετά αναφέρεται ότι το ransomware είναι το ταχύτερο αναπτυσσόμενο έγκλημα στον κυβερνοχώρο. Θύματα είναι μεγάλες εταιρείες, μικρές και μεσαίες επιχειρήσεις και ενώ το κόστος ανά άτομο είναι χαμηλό περίπου 200 $ ανά άτομο, μπορεί αυτό να είναι μια εξήγηση γιατί αυτή η κατηγορία είναι τόσο δημοφιλής. Πολλά θύματα δεν πληρώνουν λύτρα ενώ το FBI ανέφερε ότι πληρώθηκαν 209 εκατομμύρια δολάρια σε λύτρα το πρώτο τρίμηνο του 2016 με μόνο 24 εκατομμύρια δολάρια λύτρα για όλο το 2015. Τι ήταν αυτό που ώθησε αυτή την έκρηξη?

Η απάντηση είναι ότι, δυστυχώς, οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν πιο αποτελεσματικές τεχνικές. Περισσότερες χώρες και οργανισμοί αναφέρουν εγκλήματα στον κυβερνοχώρο. Επιπλέον, τα προγράμματα ransomware και phishing έχουν αυξηθεί δραματικά, με τους εγκληματίες του κυβερνοχώρου *"να στοχεύουν ενεργά οργανισμούς που περιλαμβάνουν φορείς υγειονομικής περίθαλψης, φαρμακευτικές εταιρείες, ακαδημαϊκούς οργανισμούς, οργανισμούς ιατρικής έρευνας και τοπικές κυβερνήσεις"*.

Δεν είναι μυστικό ότι το έγκλημα στον κυβερνοχώρο μπορεί να βλάψει τη δημόσια ασφάλεια, να υπονομεύσει την εθνική ασφάλεια και να βλάψει τις οικονομίες. Αυτό που είναι λιγότερο γνωστό είναι το κρυφό κόστος που οι οργανισμοί μπορεί να μην γνωρίζουν, όπως χαμένες ευκαιρίες,

χαμένοι πόροι και κατεστραμμένο ηθικό του προσωπικού. Αυτή η έκθεση παρέχει πληροφορίες σχετικά με το κρυφό κόστος του εγκλήματος στον κυβερνοχώρο. Έχει ως στόχο να βοηθήσει τους υπεύθυνους λήψης αποφάσεων σε εταιρείες και κυβερνήσεις να βελτιώσουν την κατανόησή τους για το κρυφό κόστος του εγκλήματος στον κυβερνοχώρο.

Με βάση τα δεδομένα της έρευνας, το λογισμικό υποκλοπής spyware και το κακόβουλο λογισμικό (συμπεριλαμβανομένων των ιών, των σκουληκιών, του λογισμικού υποκλοπής spyware, των keyloggers και των δούρειων ίππων) στοίχισε περισσότερο στους οργανισμούς το 2019. Το κακόβουλο λογισμικό διευκολύνει μια σειρά εγκληματικών δραστηριοτήτων, από το ransomware και την εξαγωγή δεδομένων έως την ενεργή διακοπή των δικτύων.

Οι παράνομες συναλλαγές στον κυβερνοχώρο ως υπηρεσία επέτρεψαν στο κακόβουλο λογισμικό να γίνει ταυτόχρονα πιο προηγμένο και επίσης πιο προσβάσιμο σε όσους δεν διαθέτουν βαθιά τεχνική εμπειρογνωμοσύνη. Καθώς οι αγορές ηλεκτρονικού εγκλήματος έχουν γίνει όλο και πιο εξελιγμένες, έχουν δει την εμφάνιση εξειδικευμένων προμηθευτών που είναι ειδικοί όχι μόνο στο σχεδιασμό κακόβουλου λογισμικού, αλλά και στη δημιουργία της απαραίτητης υποδομής για μια επίθεση. Προσφέρουν να μισθώσουν κακόβουλο λογισμικό σε επίδοξους εγκληματίες του κυβερνοχώρου έναντι αμοιβής, δημιουργώντας ένα περιβάλλον όπου μια μικρή ομάδα τεχνικά σκεπτόμενης εγκληματίες μπορεί να εστιάσει την πλήρη προσοχή τους στην ανάπτυξη νέων δυνατοτήτων επίθεσης, και όπου μια μεγάλη ομάδα λιγότερο εξελιγμένων ηθοποιών μπορεί εύκολα να τους εκμεταλλευτεί.

Το πρώτο εξάμηνο του 2019 αναφέρθηκαν περισσότερες από 3.800 παραβιάσεις δεδομένων, εκθέτοντας περισσότερα από τέσσερα δισεκατομμύρια αρχεία σε εγκληματίες του κυβερνοχώρου. Ένα ιδιαίτερα ανησυχητικό υποσύνολο παραβιάσεων δεδομένων είναι εκείνες που επηρεάζουν τα δεδομένα προσωπικής υγείας. Αυτά τα δεδομένα μπορεί συχνά να είναι μία από τις πιο πολύτιμες μορφές δεδομένων για εγκληματίες λόγω του τρόπου με τον οποίο επιτρέπει την ακριβή στόχευση δόλιων συστημάτων σε ευάλωτα άτομα με βάση το ιατρικό ιστορικό τους. Από τον Αύγουστο του 2020, το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών των ΗΠΑ διερευνούσε περισσότερες από 550 περιπτώσεις παραβιάσεων προσωπικών πληροφοριών υγείας που προκλήθηκαν από κλοπή, Hacking, περιστατικά πληροφορικής ή μη εξουσιοδοτημένη πρόσβαση. Αυτές οι περιπτώσεις αφορούν τα δεδομένα σχεδόν 35 εκατομμυρίων ατόμων.

Οι παραβιάσεις δεδομένων είναι κυρίως αποτέλεσμα εξωτερικών παραγόντων, αλλά μια πρόσφατη μελέτη διαπίστωσε ότι πολλές είναι το αποτέλεσμα επιθέσεων εκ των έσω. Ένα πρόσφατο παράδειγμα ήταν η παραβίαση του 2019 περισσότερων από 100 εκατομμυρίων εγγραφών Capital One από έναν μηχανικό λογισμικού που εργάζεται για την Amazon Web Services,

Οι εμπιστευτικές πληροφορίες μπορούν επίσης να αποτελέσουν απειλή για την ευαίσθητη εταιρική πνευματική ιδιοκτησία (IP). Ένα παράδειγμα αυτού ήταν η περίπτωση της Tesla το 2018, όταν ένας εργαζόμενος καταχράστηκε την πρόσβασή του για να κάνει «επιζήμιες» αλλαγές στον πηγαίο

κώδικα του λειτουργικού συστήματος κατασκευής της Tesla και εξήγαγε gigabytes πληροφοριών σχετικά με τις διαδικασίες παραγωγής της Tesla σε τρίτους11.

Σύμφωνα με την Ομάδα Εργασίας κατά του Phishing (APWG), το πρώτο τρίμηνο του 2020 καταγράφηκαν περισσότεροι από 165.000 μοναδικοί ιστότοποι ηλεκτρονικού "ψαρέματος" (Phishing). Το phishing έχει γίνει ευκολότερο τα τελευταία χρόνια, καθώς έχουν προκύψει προσφορές phishing ως υπηρεσία σε αγορές ηλεκτρονικού εγκλήματος. Χάρη σε αυτές τις προσφορές, οι εγκληματίες του κυβερνοχώρου δεν χρειάζεται πλέον να έχουν εμπειρία στο σχεδιασμό μιας υποδομής ηλεκτρονικού "ψαρέματος" (phishing) πριν στείλουν τις καμπάνιες τους. Αντ 'αυτού, οι εγκληματίες μπορούν απλά να αγοράσουν από προμηθευτές που προσφέρουν τα δικά τους κιτ και φιλοξενία και να επικεντρωθούν στα θύματα (των οποίων τα στοιχεία επικοινωνίας είναι επίσης εύκολα διαθέσιμα από τις ίδιες αγορές).

Το Ransomware παραμένει το ταχύτερα αναπτυσσόμενο μέρος του εγκλήματος στον κυβερνοχώρο. Κατά τη διάρκεια της πανδημίας COVID-19, οι επιθέσεις ransomware γενικά έχουν αυξηθεί κατά 148% από τα επίπεδα βάσης που αναφέρθηκαν τον Φεβρουάριο του 2020. Μία από τις πιο ανησυχητικές τάσεις στο ransomware είναι η στροφή προς τους στόχους στη μεταποιητική βιομηχανία. Οι ερευνητές ασφάλειας αρχίζουν να βλέπουν την εμφάνιση στελεχών ransomware που στοχεύουν σε βιομηχανικά συστήματα ελέγχου και εκατομμύρια λύτρα έχουν ήδη πληρωθεί από τα θύματα της βιομηχανίας που έχουν πέσει θύματα αυτών των παραλλαγών. Αυτή η τάση είναι πιθανό να συνεχιστεί καθώς εργοστάσια και άλλοι φορείς του κλάδου ετοιμάζονται να επεκτείνουν την ανάπτυξη ευάλωτων συσκευών IoT σε όλες τις εγκαταστάσεις τους - διευρύνοντας την επιφάνεια επίθεσης του δικτύου τους και δημιουργώντας νέους στόχους για κακόβουλους παράγοντες

Το έγκλημα στον κυβερνοχώρο εξακολουθεί να επιβάλλει βαρύ κόστος στα χρηματοπιστωτικά ιδρύματα. Σήμερα, υπάρχουν πέντε δισεκατομμύρια μοναδικά διαπιστευτήρια χρήστη (για παράδειγμα, συνδυασμοί ονόματος χρήστη και κωδικών πρόσβασης) διαθέσιμα στο darknet σε εγκληματίες του κυβερνοχώρου. Αυτά τα πλαστά διαπιστευτήρια μπορούν να χορηγήσουν πρόσβαση σε εταιρικά δίκτυα ή τραπεζικούς λογαριασμούς. Υπάρχουν περισσότερα από 15 δισεκατομμύρια κλαπούντα διαπιστευτήρια προς πώληση στο darknet, πέντε δισεκατομμύρια από τα οποία είναι μοναδικά αναγνωριστικά για πρώτη φορά.

Η "Έκθεση εγκλήματος διαδικτύου 2019" του FBI αναφέρει: "Μερικοί εγκληματίες αγοράζουν διαπιστευτήρια σε αγορές darknet, όπου ένας μόνο λογαριασμός κοστίζει κατά μέσο όρο 15,43 δολάρια. Αλλά τα πιο περιζήτητα τραπεζικά διαπιστευτήρια πωλούνται κατά μέσο όρο 71 δολάρια.

Τα χρηματοπιστωτικά ιδρύματα έχουν επίσης δεχθεί επίθεση από εθνικά κράτη. Το 2016, βορειοκορεάτες χάκερ κατάφεραν να κλέψουν 81 εκατομμύρια δολάρια από την κεντρική τράπεζα του Μπανγκλαντές, εκμεταλλευόμενοι τα κλεμμένα διαπιστευτήρια και υποβάλλοντας ψευδή αιτήματα μεταφοράς χρημάτων στην Federal Reserve Bank of New York.122 Πιο πρόσφατα, το 2018 η ίδια ομάδα χάκερ κατάφερε να κλέψει 20 εκατομμύρια δολάρια από τη μεξικανική τράπεζα Bancomext. Το μέγεθος της απειλής που αντιμετωπίζουν τα χρηματοπιστωτικά ιδρύματα μπορεί

να φανεί με μεγαλύτερη σαφήνεια στη σύλληψη ενός ηγέτη συμμορίας ηλεκτρονικού εγκλήματος το 2018 του οποίου η ομάδα έκλεψε 1,2 δισεκατομμύρια δολάρια από περισσότερες από 100 τράπεζες σε μια περίοδο πέντε ετών

Αν και οι τράπεζες εξακολουθούν να παραμένουν αγαπημένος στόχος των εγκληματιών στον κυβερνοχώρο, έχει επίσης αυξηθεί η χρήση του BEC (Business email compromise), μιας ειδικής κατηγορίας κλοπής ταυτότητας. Συνήθως, αυτά τα προγράμματα στοχεύουν στο τμήμα ανθρώπινου δυναμικού ή στο τμήμα μισθοδοσίας μιας εταιρείας, παριστάνοντας τον υπάλληλο που ζητά να αλλάξει τα στοιχεία άμεσης κατάθεσης. Στη συνέχεια, ο μισθός του υπαλλήλου είναι συνδεδεμένος σε έναν δόλιο προπληρωμένο λογαριασμό κάρτας. Άλλες μορφές απάτες BEC (Business email compromise) περιλαμβάνουν πλαστογραφημένους λογαριασμούς ηλεκτρονικού ταχυδρομείου προμηθευτών και δικηγόρων, αιτήματα φόρμας W-2 και πλαστά αιτήματα για δωροκάρτες. Αυτό επιτρέπει στους εγκληματίες του κυβερνοχώρου να στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου που παριστάνουν οποιονδήποτε υπάλληλο — από νέες προσλήψεις στον Διευθύνοντα Σύμβουλο.

Συνολικά, οι απάτες Bec (Business email compromise) παρουσιάζουν ιδιαίτερες προκλήσεις για τις τράπεζες, καθώς ένα αίτημα μεταφοράς χρημάτων μπορεί να φαίνεται ότι έχει υποβληθεί από νόμιμο πελάτη. Ωστόσο, τα διαπιστευτήρια αυτού του ατόμου μπορούν στην πραγματικότητα να αξιοποιηθούν από τον εγκληματίες του κυβερνοχώρου για κακόβουλους σκοπούς.

Τον Μάιο του 2020, μία από τις κορυφαίες εταιρείες χρηματοπιστωτικών υπηρεσιών και αγορών στον κόσμο, η Virtual Financial, ανέφερε ότι έπεσε θύμα απάτης 6,9 εκατομμυρίων δολαρίων BEC. Σύμφωνα με τα έγγραφα του νομικού δικαστηρίου που κατέθεσε η Virtu, χάκερ διείσδυσαν στον λογαριασμό ηλεκτρονικού ταχυδρομείου του Διευθύνοντος Συμβούλου και έστειλαν αρκετά μηνύματα ηλεκτρονικού ταχυδρομείου που παριστάνουν τον Διευθύνοντα Σύμβουλο στο λογιστήριο. Οι χάκερ ζήτησαν "δύο εμβάσματα σε υπερπόντιες τράπεζες - ένα στο ποσό των περίπου 3,6 εκατομμυρίων δολαρίων, το άλλο στο ποσό των περίπου 7,2 εκατομμυρίων δολαρίων — για υποτιθέμενες κεφαλαιακές κλήσεις.

Πιστεύοντας ότι τα αιτήματα ήταν νόμιμα, το λογιστήριο της Virtu συμμορφώθηκε με τα αιτήματα. Μόνον αφού το λογιστήριο μετέφερε τα κεφάλαια, ο εσωτερικός έλεγχος της Virtu χαρακτήρισε τις μεταφορές δυνητικά δόλιες.

Η κλοπή κρυπτονομισμάτων εξακολουθεί να αποτελεί σημαντική τάση στο έγκλημα στον κυβερνοχώρο, με πάνω από 4 δισεκατομμύρια δολάρια σε κρυπτονομίσματα να κλέβονται κατά τη διάρκεια του 2019 και σχεδόν 1,4 δισεκατομμύρια δολάρια να κλέβονται το πρώτο πεντάμηνο του 2020. Αυτές οι κλοπές συχνά συμβαίνουν από ανταλλαγές και πορτοφόλια όπου οι χρήστες κρατούν τα κέρματά τους, χρησιμοποιώντας ένα συνδυασμό τακτικών, συμπεριλαμβανομένου του phishing, κακόβουλο λογισμικό και κλοπή εμπιστευτικών πληροφοριών. Μια άλλη αναδυόμενη τάση είναι το cryptojacking, όπου το κακόβουλο λογισμικό εγκαθίσταται στους υπολογιστές των θυμάτων για απομακρυσμένη εξόρυξη για κρυπτονομίσματα. Οι χρήστες μπορεί να μην

παρατηρούν πότε λαμβάνει χώρα το cryptojacking, αλλά μπορεί να επιβραδύνει τις επηρεαζόμενες συσκευές και να προσελκύσει το κόστος ηλεκτρικής ενέργειας κατά τη διάρκεια της εξόρυξης.

Τα συστήματα κυβερνοεγκλήματος με δυνατότητα τεχνητής νοημοσύνης που χρησιμοποιούν συνθετικά παραγόμενα μέσα γίνονται όλο και πιο διαδεδομένα. Τα συνθετικά μέσα περιλαμβάνουν όχι μόνο "βαθύ ψεύτικο" περιεχόμενο φωτογραφιών και βίντεο, αλλά και ψευδή φωνή και γραπτά μέσα. Ενώ η τεχνητή νοημοσύνη αναπτύσσεται επίσης ως αμυντικό εργαλείο για το έγκλημα στον κυβερνοχώρο, όπως η αυτοματοποίηση της νοημοσύνης απειλών με τη χρήση μηχανικής μάθησης, οι ειδικοί της βιομηχανίας εξακολουθούν να ανησυχούν για τις επιθετικές χρήσεις της τεχνητής νοημοσύνης στο έγκλημα στον κυβερνοχώρο.

Η έκθεση αναφέρει ότι «τα προγράμματα που σχετίζονται με ransomware και phishing έχουν αυξηθεί δραματικά, με τους εγκληματίες του κυβερνοχώρου να στοχεύουν ενεργά οργανισμούς που περιλαμβάνουν φορείς υγειονομικής περίθαλψης, φαρμακευτικές εταιρείες, ακαδημαϊκό κόσμο, οργανισμούς ιατρικής έρευνας και τοπικές κυβερνήσεις». Μόνο 4 εταιρείες από τις 1.500 εταιρείες που συμμετείχαν στην έρευνα (από επαγγελματίες της τεχνολογίας στην κυβέρνηση και τις επιχειρήσεις στις ΗΠΑ, τον Καναδά, τη Βρετανία, τη Γαλλία, τη Γερμανία, την Ιαπωνία και την Αυστραλία) στη μελέτη ισχυρίστηκαν ότι δεν αντιμετώπισαν κανένα είδος εγκλήματος στον κυβερνοχώρο το 2019. Το 92% των εταιρειών είπε ότι η μεγαλύτερη απώλεια ήταν μη χρηματική, όπως η απώλεια παραγωγικότητας και οι χαμένες ώρες εργασίας.

Μερικές από τις απώλειες που πραγματοποιούνται από οργανισμούς εκτός από χρηματικές απώλειες περιλαμβάνουν χρόνο διακοπής λειτουργίας συστήματος, μειωμένη απόδοση, κόστος απόκρισης περιστατικών, ζημιά στο εμπορικό σήμα και τη φήμη, ζημιά στο ηθικό των εργαζομένων, ασφάλιση στον κυβερνοχώρο, κλοπές IP και κόστος ευκαιρίας. Το μέσο κόστος για τους οργανισμούς από το μεγαλύτερο διάστημα διακοπής λειτουργίας τους το 2019 ήταν 762.231 $. Επιπλέον η μελέτη διαπίστωσε ότι οι περισσότεροι οργανισμοί δεν είχαν εκπονήσει σχέδια για τη μείωση των επιπτώσεων των συμβάντων ασφαλείας στις δραστηριότητές τους, γεγονός που οφείλεται στο ότι η ανώτερη διοίκηση σε αυτές τις περιπτώσεις δεν ενημερώνεται για τα συμβάντα ασφαλείας. Περισσότεροι από τους μισούς από τους ερωτηθέντες οργανισμούς δήλωσαν ότι δεν έχουν σχέδια τόσο για την πρόληψη όσο και για την αντιμετώπιση ενός περιστατικού στον κυβερνοχώρο.

5.2. ΣΥΜΠΕΡΑΣΜΑΤΑ ΠΟΥ ΠΡΟΕΚΥΨΑΝ ΑΠΟ ΤΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΜΕΛΕΤΕΣ

Η ασφάλεια θα πρέπει να αποτελεί βασική αρμοδιότητα σε ολόκληρο τον οργανισμό και να ενσωματώνεται σε όλα όσα είναι και κάνει μια επιχείρηση. Από τους ανθρώπους , τα δεδομένα και κάθε πτυχή μιας επιχείρησης μπορεί να κινδυνεύουν. Οι ηγέτες των επιχειρήσεων πρέπει ακόμη να βελτιώσουν τα οικονομικά που ξοδεύουν για την στρατηγική της κυβερνοασφάλειας τους.

1. **Να δοθεί προτεραιότητα στην προστασία των επιθέσεων που βασίζονται σε ανθρώπους:** Εξουδετέρωση εσωτερικών απειλών, αφού εξακολουθεί να είναι μία από τις

μεγαλύτερες προκλήσεις που αντιμετωπίζουν οι ηγέτες των επιχειρήσεων σήμερα. Αυξήσεις σε επιθέσεις ηλεκτρονικού "ψαρέματος", ransomware και κακόβουλων εμπιστευτικών πληροφοριών σημαίνει ότι πρέπει να δοθεί μεγαλύτερη έμφαση στην καλλιέργεια του προσωπικού πάνω σε αυτά τα θέματα.. Η λογοδοσία είναι το κλειδί. Η κατάρτιση και η εκπαίδευση είναι ουσιαστικής σημασίας για την ενίσχυση ασφαλών συμπεριφορών, τόσο για τα άτομα εντός του οργανισμού όσο και για άτομα εκτός του οργανισμού και σε ολόκληρο το επιχειρηματικό πλαίσιο. Συνεργάτες, τρίτα μέρη και οι σχέσεις αυξάνονται ως αποτέλεσμα της διεξαγωγής των επιχειρηματικών λειτουργιών ηλεκτρονικά. Οι οργανισμοί θα πρέπει να συνεργάζονται με αυτό το σύστημα αλλά να προστατεύουν και να υπερασπίζονται από κοινού τις δραστηριότητές τους.

2. **Να γίνουν επενδύσεις ώστε να περιοριστούν οι απώλειες πληροφοριών και τη διακοπή των εργασιών:**
   Οι πληροφορίες είναι η ζωογόνος φύση οποιουδήποτε οργανισμού — είτε σχετίζεται με πελάτες, υπαλλήλους, προϊόντα, επιχειρηματικές διαδικασίες ή υπηρεσίες. Ως νέοι κανονισμοί περί απορρήτου, όπως ο ΓΚΠΔ, επιβάλλει σημαντικά πρόστιμα για μη συμμόρφωση, το βάρος είναι στους οργανισμούς για την στάση που θα έχουν απέναντι στις κρίσιμες πληροφορίες τους. Η προστασία των πληροφοριών βρίσκεται στην καρδιά των αξιόπιστων επιχειρηματικών πρακτικών και είναι σημαντικό να μη διακοπεί η επιχειρηματική δραστηριότητα. Λαμβάνοντας μια προσέγγιση με επίκεντρο τα δεδομένα στην ασφάλεια, υιοθέτηση τεχνολογιών πρόληψης απώλειας δεδομένων και χρήση κρυπτογραφικών η τεχνολογία μπορεί να συμβάλει σε μεγάλο βαθμό στη μείωση του κόστους του εγκλήματος στον κυβερνοχώρο.
   Ενίσχυση των μέτρων ασφαλείας γύρω από το χειρισμό, τη συντήρηση και η ανταλλαγή πληροφοριών μπορεί να μετατοπίσει την προσέγγιση ενός οργανισμού στις πληροφορίες απώλεια από τον περιορισμό της ζημίας σε ισχυρές ιδιοκτησιακές πρακτικές.

3. **Τεχνολογίες-στόχοι που μειώνουν το αυξανόμενο κόστος**: Οι οργανισμοί θα πρέπει να διαχειρίζονται το μεγαλύτερο μέρος των δαπανών, το κόστος της ανακάλυψης μια επίθεσης. Όπως ήταν αναμενόμενο, καθώς ο αριθμός των κυβερνοεπιθέσεων αυξάνεται, οπότε το κόστος ανακάλυψης αυξάνεται — και οι πρωτοποριακές τεχνολογίες θα μπορούσαν να είναι η απάντηση στην εύρεση και την αντιστροφή αυτής της αυξανόμενης δαπάνης. Επενδύσεις σε ενεργοποίηση τεχνολογιών ασφαλείας, όπως η ευφυΐα και η απειλή για την ασφάλεια μπορεί να συμβάλουν στη μείωση του κόστους του εγκλήματος στον κυβερνοχώρο. Οι υπηρεσίες cloud μπορούν να καταστήσουν την έρευνα για τις απειλές στον κυβερνοχώρο πιο αποτελεσματική.

ΚΕΦΑΛΑΙΟ 6

ΜΕΛΕΤΕΣ ΠΕΡΙΠΤΩΣΗΣ

6.1. Η περίπτωση SONY

Τον Απρίλιο του 2011, εν μέσω ασταθών οικονομικών συνθηκών, η Sony ανακοίνωσε ότι οι προσωπικές πληροφορίες για 77 εκατομμύρια συνδρομητές του PlayStation Network (PSN) καθώς και για 24,6 εκατομμύρια λογαριασμούς Sony Online Entertainment είχαν εκτεθεί λόγω εξωτερικής παραβίασης[7].

Η παραβίαση αφορούσε πληροφορίες σχετικά με συνδέσεις λογαριασμών, κωδικούς πρόσβασης, στοιχεία πιστωτικών καρτών, ιστορικά αγορών και διευθύνσεις χρέωσης. Οι εγκαταστάσεις της Sony στην Ιαπωνία επηρεάστηκαν επίσης σε μεγάλο βαθμό από τον σεισμό του Μαρτίου του 2011, με αποτέλεσμα την αναστολή αρκετών κρίσιμων επιχειρήσεων, οι οποίες κατέστησαν την κυβερνοεπίθεση καλά χρονομετρημένη για να προκαλέσει τη μέγιστη ζημιά. Η Sony έπρεπε να θέσει τις υπηρεσίες PSN εκτός σύνδεσης την επομένη της επίθεσης για να αξιολογήσει την έκταση του συμβάντος, με αποτέλεσμα την απώλεια εσόδων. Το κόστος απόκρισης που προκύπτει από τον εντοπισμό και την αντιμετώπιση των τρωτών σημείων που αποτελούν αντικείμενο εκμετάλλευσης και την ενημέρωση των πελατών· μια πρόχειρη εκτίμηση του κόστους είναι 171 εκατομμύρια δολάρια. Ο αριθμός αυτός, ωστόσο, δεν περιλαμβάνει ποινικές αποζημιώσεις από αγωγές, δαπάνες από κλοπή ταυτότητας ή οποιαδήποτε άλλη κατάχρηση κλεμμένων πιστωτικών καρτών, ούτε απώλεια της νομιμότητας και της κεφαλαιοποίησης της αγοράς[8].

Στα τέλη Απριλίου 2011, η Sony παρείχε ένα ολοκληρωμένο σχέδιο ανάκαμψης και έναν ακριβή υπολογισμό του κόστους που προκλήθηκε από τον σεισμό της γης, αλλά δεν ήταν ακόμη σε θέση να υπολογίσει την πλήρη οργανωτική βλάβη από την κυβερνοεπίθεση. Ο συνολικός αντίκτυπος του σεισμού και της παραβίασης δεδομένων είχε ως αποτέλεσμα σημαντική μείωση της αξιολόγησης της αγοράς της Sony, όπως απεικονίσθηκε στις χρηματιστηριακές αγορές. Η τιμή της μετοχής της Sony μειώθηκε κατά 19% μετά τον σεισμό, μια πτώση ισοδύναμη με τη γενική ιαπωνική χρηματιστηριακή αγορά, αλλά σύντομα ανέκαμψε το 50% αυτής της απώλειας. Μετά την κυβερνοεπίθεση, ωστόσο, η τιμή της Sony υπέστη απώλεια 12% (αυτή τη φορά δεν αντικατέστησε την υπόλοιπη ιαπωνική οικονομία) και η αποκάλυψη των αδυναμιών ασφαλείας μόλις η Sony είχε αποκαταστήσει την υπηρεσία παρέτεινε τη φάση ανάκαμψης.

Dark Reading. Sony data breach cleanup to cost $171million, 2011 http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-\$171-million/d/d-id/1097898

PwC. Limiting the impact of data breachesthe case of the Sony Play Station Network, 2011 http://www.strategyand.pwc.com/reports/limiting-impact-data-breaches-case

Τρία χρόνια μετά από αυτά τα περιστατικά, τον Νοέμβριο του 2014, διέρρευσαν για άλλη μια φορά εμπιστευτικά δεδομένα από τη Sony Pictures. Τα δεδομένα περιελάμβαναν περισσότερα από 30 000 εσωτερικά έγγραφα, 170 000 μηνύματα ηλεκτρονικού ταχυδρομείου, αριθμούς κοινωνικής ασφάλισης των υπαλλήλων της Sony, κριτικές προσωπικού και ιατρικές ιστορίες, καθώς και ταινίες που δεν είχαν ακόμη κυκλοφορήσει. Η ίδια κυβερνοεπίθεση παρέλυσε όλα τα συστήματα της Sony, καθιστώντας την on-line βάση δεδομένων του stock footage ανενεργή, το τηλεφωνικό σύστημα εκτός σύνδεσης, υπολογιστές και διακομιστές άχρηστους. Αυτό περιγράφηκε από το FBI ως μια «άνευ προηγουμένου ψηφιακή επίθεση που θα είχε πέσει το 90 τοις εκατό των εταιρειών που χτύπησε»[9].

Η Sony αναγκάστηκε να αντικαταστήσει μεγάλο αριθμό συστημάτων της, να δημιουργήσει μια τηλεφωνική γραμμή για απάτη ταυτότητας, να παρέχει ψυχολογική συμβουλευτική στους υπαλλήλους και να οργανώσει σεμινάρια για την ασφάλεια των δεδομένων. Μετά την αποτυχία, οι υπάλληλοι της Sony έλαβαν μηνύματα ηλεκτρονικού ταχυδρομείου που απειλούσαν τις οικογένειές τους εάν δεν κατήγγειλαν τη Sony, οι πιστωτικές τους κάρτες ήταν διαθέσιμες προς πώληση στις αγορές του σκοτεινού διαδικτύου και ορισμένοι είδαν τους τραπεζικούς λογαριασμούς τους να υπερβαίνουν τα πιστωτικά όρια. Μια έρευνα που διεξήχθη από το Κέντρο Πόρων Κλοπής Ταυτότητας σχετικά με τα θύματα κλοπής ταυτότητας, ανέφερε ότι τα θύματα βίωσαν «άρνηση, απογοήτευση, οργή, φόβο, προδοσία και αδυναμία τις ημέρες, τις εβδομάδες και τα χρόνια μετά την παραβίαση». Κατατέθηκαν αγωγές κατηγορίας από υπαλλήλους, είτε επειδή η Sony δεν ενημέρωσε εκείνους των οποίων τα δεδομένα διέρρευσαν, είτε λόγω φόβων για το πώς θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν οι προσωπικές πληροφορίες που διέρρευσαν. Αυτό συνέβαλε επίσης στο γεγονός ότι ορισμένα βασικά στελέχη αποχώρησαν από την εταιρεία· και επιπλέον, ο τύπος ανακάλυψε τα ζητήματα ποικιλομορφίας της Sony, τα οποία συζητήθηκαν εκτενώς στο περιεχόμενο των μηνυμάτων ηλεκτρονικού ταχυδρομείου που διέρρευσαν.[10]

6.2. Η περίπτωση JP Morgan

Η JP Morgan, μία από τις μεγαλύτερες τράπεζες στις ΗΠΑ, ανέφερε ότι χάκερ απέκτησαν πρόσβαση διαχειριστή σε αρκετούς από τους διακομιστές της. Οι πληροφορίες σχετικά με τα ονόματα, τους αριθμούς τηλεφώνου, το ηλεκτρονικό ταχυδρομείο και τις φυσικές διευθύνσεις των κατόχων λογαριασμών διέρρευσαν επηρεάζοντας 76 εκατομμύρια νοικοκυριά και επτά εκατομμύρια μικρές επιχειρήσεις. Η JP Morgan είχε ανακοινώσει αύξηση του προϋπολογισμού της για την κυβερνοασφάλεια κατά 250 εκατομμύρια δολάρια ετησίως λίγο πριν από την επίθεση[11].

Hess A. Inside the Sony hack. Slate, 2015 http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html

Variety Sony hack attack opens minefield of legal questions that has hollywood worried, 2015,07–13 http://variety.com/2015/biz/news/sony-hack-attack-opens-minefield-of-legal-questions-that-has-hollywood-worried-1201471664

Η εταιρεία αναγκάστηκε να αντικαταστήσει το μεγαλύτερο μέρος της υποδομής πληροφορικής της, μια διαδικασία που ήταν χρονοβόρα και εμπόδιζε την καθημερινή ζωή των εργαζομένων. Ο υπόλοιπος προϋπολογισμός δαπανήθηκε για την πρόσληψη περισσότερων από 1000 υπαλλήλων για την παρακολούθηση των συστημάτων της εταιρείας . Σημαντικό ενδιαφέρον παρουσιάζουν οι δύο μακροπρόθεσμες επιπτώσεις, οι οποίες προέκυψαν από αυτή την επίθεση. Η πλειοψηφία των πελατών των οποίων οι πληροφορίες διέρρευσαν ήταν υποχρεωμένοι να παρακολουθούν τα οικονομικά τους υπό τον φόβο απάτης, ενώ έλαβαν ψεύτικα μηνύματα ηλεκτρονικού ταχυδρομείου που τους κατηύθυναν σε ιστότοπους απατεώνων για οικονομικές ανταλλαγές.

Το δεύτερο αποτέλεσμα ήταν η αντικατάσταση του επικεφαλής του υπεύθυνου ασφάλειας πληροφοριών λόγω της ανεπαρκούς συνεργασίας του με τις ομοσπονδιακές αρχές σε μια προσπάθεια να προσπαθήσει να ελέγξει την έρευνα και να αποκρύψει τη διαρροή πληροφοριών.

6.3. Η περίπτωση Ashley Madison

Τον Ιούλιο του 2015, διέρρευσαν στοιχεία 33 εκατομμυρίων λογαριασμών και προσωπικών πληροφοριών σχετικά με άτομα εγγεγραμμένα στην Ashley Madison, έναν ιστότοπο που διευκολύνει τις εξωσυζυγικές υποθέσεις [12]. Μια βασική αρχή του επιχειρηματικού μοντέλου της Ashley Madison ήταν η ιδιωτικότητα και η ασφάλεια, μέσω της οποίας θα έχτιζαν μια σχέση εμπιστοσύνης με τους πελάτες τους. Ως εκ τούτου, η κυβερνοεπίθεση είχε δραματικές συνέπειες για τη φήμη της εταιρείας, όχι μόνο επειδή εξέθεσε τα τρωτά σημεία του συστήματος, αλλά επειδή απέδειξε ότι η υπόσχεση της Ashley Madison να διαγράψει δεδομένα κατόπιν αιτήματος των πελατών δεν τηρήθηκε. Ως αποτέλεσμα αυτής της πρακτικής, η Ashley Madison έγινε υπεύθυνη για αγωγές με πολλές οργανώσεις να ζητούν διαδίκους στο Twitter. Αυτό που παρουσιάζει μεγάλο ενδιαφέρον σε αυτή την περίπτωση, ωστόσο, είναι οι επιπτώσεις αυτού που επινοήθηκε ως "παράπλευρες απώλειες" οι οποίες είναι ιδιόμορφες για τη φύση των υπηρεσιών που προσέφερε ο ιστότοπος.

Μόλις τα δεδομένα ήταν διαθέσιμα στο κοινό και εύκολα αναζητήσιμα, οι πελάτες έγιναν επιρρεπείς σε εκβιασμούς, με επαγγελματικές επιπτώσεις. [13] Πολλές από τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που διέρρευσαν περιείχαν τον τομέα '.mil', υποδεικνύοντας ανθρώπους που υπηρετούν στον αμερικανικό στρατό. Η μοιχεία, ωστόσο, είναι έγκλημα στον αμερικανικό στρατό και τα μέλη της Ashley Madison υποβλήθηκαν σε ένα έτος εγκλεισμού ή ατιμωτικής απαλλαγής. Στο ίδιο πνεύμα, οι ιδιοκτήτες 1.200 διευθύνσεων ηλεκτρονικού

P Morgan Chase reveals massive data breach affecting 76m households. The Guardian, 2014 http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach.

InfoSec Institute. Ashley Madison revisited: legal, business and security repercussions, 2015, 8. http://resources.infosecinstitute.com/ashley-madison-revisited-legal-business-and-security-repercussions.

The Verge. ***The mind-bending messiness of the Ashley Madison data dump***, 2015 http://www.theverge.com/2015/8/19/9178855/ashley-madison-data-breach-implications

ταχυδρομείου '.sa' εκτέθηκαν σε πιθανή θανατική ποινή, η οποία είναι η τιμωρία στη Σαουδική Αραβία για μοιχεία. Προέκυψαν νέες πρακτικές κυβερνοεγκλήματος, με εγκληματίες να απειλούν να εκθέσουν άτομα των οποίων οι διευθύνσεις ηλεκτρονικού ταχυδρομείου βρέθηκαν στο σύνολο δεδομένων Ashley Madison στο «σημαντικό άλλο», εκτός εάν καταβλήθηκαν 225 δολάρια σε bitcoin. Τα δημόσια πρόσωπα εξαναγκάστηκαν σε «οδυνηρές προσωπικές ομολογίες», άλλα χώρισαν, ενώ η αστυνομία του Τορόντο ανέφερε δύο αυτοκτονίες που ενδεχομένως συνδέονται με την κυβερνοεπίθεση.[14]

6.4. Επίθεση ransomware WannaCry το 2017

Το WannaCry ήταν ένα σκουλήκι υπολογιστών υπεύθυνο για μια από τις πιο καταστροφικές κυβερνοεπιθέσεις στην πρόσφατη ιστορία. Εκτός από τη διάδοση σε δίκτυα υπολογιστών χρησιμοποιώντας το λειτουργικό σύστημα των Windows, τα κρυπτογραφημένα αρχεία WannaCrypt (επίσης γνωστά ως WannaCrypt και WanaCrypt0r) του κεντρικού υπολογιστή και επέτρεψαν την πρόσβαση σε αυτά τα αρχεία μόνο μετά από πληρωμή λύτρων bitcoin. Ενώ το ίδιο το ransomware δεν ήταν νέο, το WannaCry ήταν ιδιαίτερα επιτυχημένο επειδή στόχευε σε μια ευπάθεια υπολογιστή που πολλοί οργανισμοί και άτομα δεν είχαν ακόμη εγκαταστήσει ενημερώσεις κώδικα ασφαλείας (δηλαδή ενημερώσεις λογισμικού) για να αντιμετωπίσουν.

Αναλογιζόμενοι τον κοινωνικό αντίκτυπο της επίθεσης, ο WannaCry μόλυνε πάνω από 200.000 θύματα σε τουλάχιστον 150 χώρες. [15]Σε αυτές περιλαμβάνονταν μέλη του κοινού, αλλά και οργανισμοί υγειονομικής περίθαλψης, κατασκευαστές αυτοκινήτων, εταιρείες τηλεπικοινωνιών, υπηρεσίες παράδοσης και ο τομέας της εκπαίδευσης. [16]

Λόγω της φύσης της επίθεσης, η αναστάτωση που προκάλεσε σε κοινωνικό επίπεδο ήταν αρκετά σημαντική. Οι οργανισμοί έκλεισαν (προκαλώντας την αποστολή ανθρώπων στο σπίτι), η παραγωγή σταμάτησε (με αποτέλεσμα καθυστερήσεις προϊόντων) και πολλές επιχειρήσεις δεν γνώριζαν τον καλύτερο τρόπο αποκατάστασης των υπηρεσιών. Συνολικά, οι άνθρωποι αισθάνθηκαν απώλεια ελέγχου καθώς η απειλή ήταν τόσο διάχυτη και η μόνη επιλογή για ανάκτηση - υποθέτοντας ότι δεν έγιναν πρόσφατα αντίγραφα ασφαλείας - ήταν να πληρώσουν τα

Ashley M. ***Aftermath: confessions, suicide reports and hot on the hacker's trail. National Post***,2015 http://news.nationalpost.com/news/canada/ashley-madison-aftermath-confessions-suicide-reports-and-hot-on-the-hackers-trail

[15] Reuters. (2017). Cyber attack hits 200,000 in at least 150 countries: Europol. Retrieved August 14 2018, from https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX

[16] Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 32, 665-683.

λύτρα. Συνολικά, αυτές οι διαταραχές οδήγησαν σε εκτιμώμενο οικονομικό κόστος 8 δισεκατομμυρίων δολαρίων παγκοσμίως.[17]

Στο Ηνωμένο Βασίλειο, επηρεάστηκαν επίσης υποδομές ζωτικής σημασίας, όπως η Εθνική Υπηρεσία Υγείας (NHS). Συνολικά 48 NHS Trusts μολύνθηκαν στην Αγγλία και 13 στη Σκωτία (BBC, 2017a). Αυτό είχε ως αποτέλεσμα την άμεση διακοπή της ζωής των ανθρώπων στο πλαίσιο της υγείας τους. Συγκεκριμένα, υπήρξαν ακυρωμένες επεμβάσεις, ορισμένες θεραπείες αναβλήθηκαν και τα ασθενοφόρα εκτράπηκαν. Αυτή είναι μια ιδιαίτερα ανησυχητική κατάσταση, δεδομένου του πόσο καιρό οι ασθενείς συχνά πρέπει να περιμένουν για ορισμένες θεραπείες. Το WannaCry προκάλεσε επίσης κυβερνητικές αντιδράσεις – στο Ηνωμένο Βασίλειο συγκλήθηκε συνεδρίαση της Επιτροπής (δηλαδή, συνεδρίαση της κυβερνητικής επιτροπής αντιμετώπισης έκτακτης ανάγκης) και στις ΗΠΑ, ο σύμβουλος εσωτερικής ασφάλειας, διατάχθηκε να συντονίσει την απάντηση της κυβέρνησης και να βοηθήσει στην οργάνωση της αναζήτησης των υπεύθυνων μερών. Αυτό το επίπεδο αντίδρασης από τις κυβερνήσεις υπογράμμισε περαιτέρω τον αντίκτυπο της απειλής στα μάτια του κοινού.

Ένα ενδιαφέρον σημείο που πρέπει να σημειωθεί εδώ είναι τα σχόλια της κυβέρνησης σχετικά με την επίθεση. Ειδικότερα, δόθηκε έμφαση στο γεγονός ότι η επίθεση δεν είχε στόχο το NHS και ότι ήταν διεθνής. Σύμφωνα με τον Independent, ο υπουργός Εσωτερικών του Ηνωμένου Βασιλείου δήλωσε: *«Αν κοιτάξετε ποιος έχει επηρεαστεί από αυτόν τον ιό, είναι μια τεράστια ποικιλία σε διαφορετικούς κλάδους και σε όλες τις διεθνείς κυβερνήσεις. ... Αυτός είναι ένας ιός που επιτέθηκε στις πλατφόρμες των Windows.*

Το γεγονός είναι ότι το NHS έπεσε θύμα αυτού. ... Δεν νομίζω ότι έχει να κάνει με την ετοιμότητα» (The Independent, 2017). Αυτό το μήνυμα είχε πιθανότατα ως στόχο να εξαλείψει την κατήφεια και την πιθανή δημόσια απελπισία που σχετίζεται με στοχευμένη επίθεση του NHS, καθώς επίσης να καθησυχάσει τον κόσμο ότι η χώρα δεν είναι προετοιμασμένη για τέτοια γεγονότα. Αυτό έχει ως στόχο να υποστηρίξει την εμπιστοσύνη των ανθρώπων στην κυβέρνηση και στα τεχνολογικά συστήματα.

Ο ψυχολογικός αντίκτυπος του WannaCry ήταν επίσης σημαντικός. Για πολλούς είχε ως αποτέλεσμα ανησυχία, αγωνία, δυσπιστία και μια αίσθηση αδυναμίας - αυτά είναι πολλά από τα θέματα που συζητήθηκαν νωρίτερα. Εάν χρησιμοποιήσουμε τη μόλυνση των τοποθεσιών του NHS ως παράδειγμα, υπάρχουν πολλές περιπτώσεις που πρέπει να εξετάσουμε. Ίσως ένα από τα πιο καλά αναφερόμενα στο σετ είναι αυτό ενός ανθρώπου που προετοιμαζόταν για μια εγχείρηση καρδιάς και το ακύρωσε ώρες πριν από την υλοποίηση του. Αυτό οδήγησε στην απογοήτευσή του, την ταλαιπωρία των μελών της οικογένειας που ταξίδεψαν για να μείνουν κοντά και την αμηχανία ως προς το γιατί κάποιος θα ήθελε να επιτεθεί σε ένα νοσοκομείο. Επηρεάστηκε επίσης

[17] Barlyn, S. (2017). Global cyber attack could spur $53 billion in losses - Lloyd's of London. Reuters. Retrieved July 14 2018, from https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of london-idUKKBN1A20AH

ψυχολογικά δεδομένου ότι είχε προετοιμαστεί για την εγχείρηση καρδιάς εκείνη την ημερομηνία, και τώρα θα πρέπει να επαναπρογραμματιστεί σε κάποιο σημείο στο μέλλον.

Ψυχολογικά, υπήρξε επίσης η συνειδητοποίηση από πολλούς ότι οι κυβερνοεπιθέσεις θα μπορούσαν τώρα να προκαλέσουν την απώλεια ζωών. Όπως αναφέρει το BBC, ένα μέλος του προσωπικού του NHS σημείωσε: *"Απόλυτο μακελειό στο NHS σήμερα. Δύο κέντρα hyperacute εγκεφαλικού επεισοδίου (το πεδίο στο οποίο εργάζομαι) στο Λονδίνο έκλεισαν από σήμερα το απόγευμα. Οι ασθενείς είναι σχεδόν βέβαιο ότι θα υποφέρουν και θα πεθάνουν εξαιτίας αυτού». Αυτή η άποψη αναφέρεται επίσης από ένα άλλο άτομο - έναν ειδικό πληροφορικής*

– συνέντευξη στο άρθρο: *«Αυτού του είδους η επίθεση συνήθως προκαλεί κάποια ταλαιπωρία ή οικονομική απώλεια στα θύματά της, αλλά στην περίπτωση αυτή μπορεί κάλλιστα να προκαλέσει απώλεια ζωής».* Αυτό είναι ένα σημαντικό σημείο, καθώς σχετίζεται με τη σοβαρότητα της απειλής, αλλά μπορεί επίσης να προκαλέσει περαιτέρω ζητήματα, δεδομένου ότι η συμπεριφορά των ατόμων δεν θα αποτρέψει απαραίτητα αυτό το είδος επίθεσης.

6.5. Επίθεση άρνησης υπηρεσίας (DoS) του Τραπεζικού Ομίλου Lloyds το 2017

Τον Ιανουάριο του 2017, ο όμιλος Lloyds Banking Group και άλλες τράπεζες στο Ηνωμένο Βασίλειο έπεσαν θύματα επίθεσης άρνησης εξυπηρέτησης (DoS) που συνεχίστηκε για μια περίοδο δύο ημερών. Το DoS περιγράφει μια επίθεση όπου τα συστήματα βομβαρδίζονται με παράνομα δεδομένα ή αιτήματα και, ως εκ τούτου, δεν είναι σε θέση να ανταποκριθούν εγκαίρως σε νόμιμα αιτήματα (π.χ. για πρόσβαση σε ιστοσελίδα ή υπηρεσία) εγκαίρως. Σε αυτή την περίπτωση, τα χρηματοπιστωτικά ιδρύματα «χτυπήθηκαν» από ένα κατανεμημένο DoS (DDoS) στο οποίο τα παράνομα αιτήματα προέρχονταν από πολλαπλές, δυναμικά μεταβαλλόμενες τοποθεσίες. Ο όμιλος Lloyds ήταν μία από τις πιο σημαντικά στοχευμένες τράπεζες κατά τη διάρκεια αυτής της επίθεσης και οι επιπτώσεις της επίθεσης περιελάμβαναν τη μη διαθεσιμότητα του συστήματος και την περιορισμένη πρόσβαση σε ηλεκτρονικές υπηρεσίες για τους πελάτες του.

Σε ευρύ κοινωνικό επίπεδο, η επίθεση επηρέασε εκατομμύρια πελάτες τραπεζών. Σύμφωνα με αναφορές, οι δράστες επιχείρησαν να εμποδίσουν την πρόσβαση στους 20 εκατομμύρια λογαριασμούς της τράπεζας στο Ηνωμένο Βασίλειο.

Το αποτέλεσμα ήταν ένας αντίκτυπος σε άτομα και επιχειρήσεις, ιδιαίτερα στην ικανότητά τους να συνδεθούν σε διαδικτυακά συστήματα. Ως εκ τούτου, ορισμένοι πελάτες δεν θα ήταν σε θέση να δουν τα υπόλοιπα, να πραγματοποιήσουν πληρωμές (π.χ. για ενοίκια και λογαριασμούς) και να πραγματοποιήσουν τραπεζικές μεταφορές (π.χ. για τις απαραίτητες εφάπαξ συναλλαγές). Ένας άλλος σχετικός παράγοντας εδώ ήταν ότι αυτό το είδος επίθεσης DDoS με στόχο τον τραπεζικό τομέα είχε συμβεί στο παρελθόν.

Το 2015, σημειώθηκε παρόμοια κυβερνοεπίθεση η οποία έθεσε σε κίνδυνο τις υπηρεσίες των τραπεζών του Ηνωμένου Βασιλείου, RBS και Natwest. Μια ιδιαίτερα ανησυχητική

πραγματικότητα αυτής της επίθεσης ήταν ο χρόνος κατά τον οποίο συνέβη, δηλαδή κοντά στην ημέρα πληρωμής· Αυτό είχε ως αποτέλεσμα τον μέγιστο αντίκτυπο σε ορισμένα άτομα και κάποιο διαδεδομένο πανικό.

Μια αξιοσημείωτη διαφορά και ένας βασικός παράγοντας στην πιο πρόσφατη επίθεση ήταν ο αριθμός των ημερών κατά τις οποίες έλαβε χώρα. Αυτή η παρατεταμένη περίοδος δύο ημερών (με ορισμένες αναφορές μάλιστα να υποδηλώνουν ότι ήταν μεγαλύτερη για ορισμένους πελάτες) σήμαινε ότι όχι μόνο η φήμη της τράπεζας υπέστη ζημία, αλλά και ότι οι ζωές των πελατών μπορεί να έχουν διαταραχθεί σοβαρά κατά τη διάρκεια αυτής της περιόδου.

Ένας βουλευτής ανέφερε ότι η κυβερνοεπίθεση ήταν ανησυχητική για την κοινωνία και ότι έπρεπε να παρθούν περισσότερα μέτρα. Σύμφωνα με τον Guardian, ο τότε βουλευτής δήλωσε: *«Η επίθεση στην Lloys ήταν βαθιά ανησυχητική. Χιλιάδες πελάτες επηρεάστηκαν από αυτό, το τελευταίο σε μια μακρά λίστα αποτυχιών και παραβιάσεων των τραπεζικών συστημάτων πληροφορικής. ... Όπως έχω ήδη επισημάνει, είναι καιρός να εξετάσουμε κατά πόσον απαιτείται τώρα ένα μόνο σημείο υπεύθυνο για τον κίνδυνο στον κυβερνοχώρο στον τομέα των χρηματοπιστωτικών υπηρεσιών».*

Αυτό καταδεικνύει κάποια υψηλού επιπέδου ανησυχία για τον χρηματοπιστωτικό τομέα σε γενικές γραμμές ως αποτέλεσμα αυτού του είδους κυβερνοεπιθέσεων. Υπάρχουν επίσης παραλληλισμοί για την ευρύτερη εμπιστοσύνη του κοινού στην τεχνολογία. Για να εξετάσει την επίθεση του 2015, ένας πελάτης της Natwest τουίταρε: "Δεν μπορώ να συνδεθώ σε #natwest για άλλη μια φορά για να ελέγξω ορισμένες συναλλαγές... και θέλουν να εξαιρεθώ από τις έντυπες δηλώσεις; Καμία πιθανότητα». Αυτό είναι οδυνηρό, καθώς σχετίζεται με τον τρόπο με τον οποίο τα άτομα αντιλαμβάνονται την τεχνολογία και τον κίνδυνο και πώς οι επιθέσεις μπορούν να οδηγήσουν σε λιγότερη εμπιστοσύνη στην τεχνολογία.

Αναλύοντας τον ψυχολογικό αντίκτυπο της επίθεσης Lloyds DDoS, που προκάλεσε στους πελάτες είναι αναστάτωση και απογοήτευση - αυτό ήταν επομένως κυρίως μια συναισθηματική απάντηση. Όπως αναφέρει το BBC, ένας πελάτης εξέφρασε: *"Δεν έχει καταφέρει να έχει πρόσβαση στον ιστότοπο ή την εφαρμογή για πάνω από 36 ώρες τώρα - γίνεται κάτι γι 'αυτό;".* Αυτό ήταν ένα από μια σειρά παραπόνων που έγιναν στα μέσα κοινωνικής δικτύωσης σχετικά με το τρέχον ζήτημα. Εδώ βλέπουμε μία από τις πρωταρχικές χρήσεις των μέσων κοινωνικής δικτύωσης (π.χ. twitter, Facebook και πλατφόρμες blogging) σήμερα – δηλαδή, επιτρέποντας στο κοινό να επικοινωνήσει απευθείας με εταιρείες (ειδικά για παράπονα) και να ακουστεί δημόσια η φωνή τους.

Αν και είναι δύσκολο να γνωρίζουμε την πλήρη έκταση των ψυχολογικών επιπτώσεων, μπορούμε να υποθέσουμε ότι η έλλειψη πρόσβασης σε τραπεζικούς λογαριασμούς και ενδεχομένως σε προσωπικά κεφάλαια (π.χ. εάν τα χρήματα έπρεπε να μεταφερθούν από τον έναν λογαριασμό στον άλλο για να διευκολυνθεί η ανάληψη), θα είχε αυξήσει σημαντικά το άγχος και το άγχος των πελατών. Από την στιγμή που οι πελάτες δεν μπορούν να έχουν πρόσβαση στους λογαριασμούς τους τα συναισθήματα που θα κυριαρχούσαν θα ήταν άγχος, θυμός, πόνος, κατάθλιψη ή αδυναμία. Όπως αναφέρθηκε προηγουμένως, η διάρκεια της διαταραχής ήταν ένας βασικός παράγοντας, καθώς θα επιδείνωνε οποιαδήποτε αρχική ταλαιπωρία.

Όλες αυτές είναι σημαντικές ανησυχίες, διότι θα μπορούσαν να υποκινήσουν μια αλλαγή στον τρόπο με τον οποίο το κοινό αντιλαμβάνεται τις κυβερνοεπιθέσεις και να πιστέψει ότι έχει οποιονδήποτε έλεγχο ή δεξιότητες για να προστατεύσει τον εαυτό του ή τις οικογένειές του.

ΚΕΦΑΛΑΙΟ 7

7.1. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ

Για να μπορέσει κάποιος να προσεγγίσει τα νομικά θέματα που αφορούν το κυβερνοχώρο θα πρέπει να έχει όχι μόνο νομικές γνώσεις αλλά και τεχνικές. Επιπλέον, υπάρχει μεγάλη έλλειψη βιβλιογραφίας όσον αφορά αυτή τη νέα μορφή εγκλήματος. Επειδή η τεχνική αλλά και η νομική ορολογία είναι κυρίως στην αγγλική γλώσσα, υπάρχει πρόβλημα με την ελληνική νομική ορολογία. Είναι δύσκολο να μεταφερθούν οι όροι στα ελληνικά. Ως λύση στο πρόβλημα λοιπόν ακολουθήθηκε η παραδοσιακή δικονομική ορολογία και μόνο εάν είναι απαραίτητο να ακολουθηθεί μικρή ορολογία. Τα ηλεκτρονικά μέσα δεν μπορούν να ταυτιστούν με τα παραδοσιακά, αφού αντιλαμβανόμαστε ότι τα παραδοσιακά αποδεικτικά μέσα που λαμβάνουν χώρα σε φυσικό χώρο δεν μπορούν να συγκριθούν με τα αποδεικτικά μέσα ενός ηλεκτρονικού εγκλήματος. Αυτό σημαίνει ότι αυτά τα αποδεικτικά μέσα δεν μπορούν να είναι απτά, υπάρχει δυνατότητα εξαφάνισης τους.[18]

Ως ένα νέο μέσο επικοινωνίας το Διαδίκτυο έφερε νέες προκλήσεις στην επιστήμη του ποινικού δικαίου, αφού έκαναν την εμφάνισή τους νέα αδικήματα που έχουν σχέση με αυτό. Η νομοθεσία λοιπόν τόσο στον Ευρωπαϊκό χώρο όσο και στην Ελλάδα άρχισε να προσαρμόζεται σε αυτή την πραγματικότητα και θεσπίστηκαν νέες διατάξεις.

Η Σύμβαση του Συμβουλίου της Ευρώπης για το Κυβερνοέγκλημα αποτελεί τον θεμέλιο λίθο. Ασχολήθηκε λοιπόν πως θα αντιμετωπιστεί το ηλεκτρονικό έγκλημα, γι αυτό το λόγο εξέδωσε τη σύσταση R(89) που αγορά το έγκλημα που διαπράττεται με τον ηλεκτρονικό υπολογιστή και τη σύσταση R (95) για προβλήματα ποινικού δικονομικού δικαίου που έχουν σχέση με την τεχνολογία της πληροφορικής. Στις 23-11-2001 στη Βουδαπέστη υπογράφηκε η Σύμβαση για το έγκλημα στον Κυβερνοχώρο και στις 28-1-2003 υπογράφηκε το Πρόσθετο Πρωτόκολλο στη Σύμβαση.[19]

Στην Ελλάδα, δημοσιεύθηκε στο ΦΕΚ 142/Α/3-8-2016 ο Νόμος 4411/2016 με το οποίο γίνεται επικαιροποίηση της ποινικής νομοθεσίας στον τομέα της «κυβερνοεγκληματικότητας» («cybercriminality») και ειδικότερα κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο που υπογράφηκε στη Βουδαπέστη και το Πρόσθετο Πρωτόκολλο αυτής αναφορικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω συστημάτων υπολογιστών. Με το νόμο τιμωρούνται πράξεις που αποσκοπούν στην από πρόθεση πρόκληση βλάβης στα δίκτυα και στρέφονται κατά της ακεραιότητας, της διαθεσιμότητας των δεδομένων ή των συστημάτων πληροφορικής. Επιπλέον τιμωρούνται πράξεις που αφορούν την παράνομη πρόσβαση, την υποκλοπή, την παρεμβολή σε δεδομένα και τις παρεμβολές σε συστήματα.[20]

Νομοθεσία - Ηλεκτρονικό Έγκλημα (google.com)
Ιωάννης Ιγγλεζάκης, Δίκαιο της Πληροφορικής σελ.327

Όπως έχουμε ήδη προαναφέρει ως κυβερνοέγκλημα θεωρείται παράνομη ή παράνομες ψηφιακές ενέργειες που έχουν ως στόχο να ζημιώσουν είτε ιδιώτη είτε επιχείρηση είτε οργανισμό. Όταν αναφερόμαστε στον όρο κυβερνοέγκλημα , υπάρχουν τρεις κατηγορίες ποινικών αδικημάτων:

1. Τα ποινικά αδικήματα που γίνονται μέσω ηλεκτρονικού υπολογιστή ή κάποιου πληροφοριακού συστήματος
2. Τα ποινικά αδικήματα που έχουν σχέση με διακίνηση παράνομου περιεχόμενου
3. Τα ποινικά αδικήματα που έχουν ως στόχο την εμπιστευτικότητα, την ακεραιότητα αλλά και τη διαθεσιμότητα πληροφοριακών συστημάτων

Άρα το βασικό στοιχείο για την εκτέλεση αυτών των ποινικών αδικημάτων είναι ο ηλεκτρονικός υπολογιστής είτε ως εργαλείο, είτε ως βοηθητικό μέσο είτε ως το βασικό μέσο.

Όλες οι εγκληματικές πράξεις που τελούνται χρησιμοποιώντας ηλεκτρονικούς υπολογιστές ή και συστήματα επεξεργασίας δεδομένων τιμωρούνται και θεωρούνται ως ηλεκτρονικά εγκλήματα.

Η ελληνική ποινική νομοθεσία θεωρεί ως εγκλήματα που γίνονται με τη χρήση ηλεκτρονικού υπολογιστή την παράνομη αντιγραφή απορρήτων δεδομένων , την παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ και την απάτη.

Η ποινική δίωξη του κυβερνοεγκλήματος είναι δύσκολη και επίπονη γιατί

- Λόγω ταχύτητας, διαπράττεται σε μικρό χρονικό διάστημα και δεν μπορεί να το αντιληφθεί το θύμα
- Γίνεται με ευκολία από τον προσωπικό χώρο του δράστη και από ηλεκτρονικό υπολογιστή
- Υπάρχει ανωνυμία
- Έχει διασυνοριακό χαρακτήρα, υπάρχει περίπτωση οι πράξεις να γίνονται ταυτόχρονα
- Τα ψηφιακά ίχνη του κυβερνοεγκλήματος αλλά και ο διασυνοριακός χαρακτήρας κάνουν την διαλεύκανση του πιο δύσκολη
- Θα πρέπει να υπάρχει διακρατική συνεργασία λόγω του διασυνοριακού του χαρακτήρα
- Τα κυβερνοεγκλήματα που τελούνται είναι περισσότερα από τα περιστατικά και τις περιπτώσεις που έχουν καταγραφεί

Στο πρώτο μέρος του νόμου γίνεται η κύρωση της σύμβασης του συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο και του πρόσθετου πρωτοκόλλου της σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης που διαπράττονται μέσω ηλεκτρονικών υπολογιστών.

Στο δεύτερο μέρος, ουσιαστικά γίνεται μεταφορά στο ελληνικό δίκαιο της οδηγίας 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης πλαισίου

2005/222/ΔΕΥ, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.

Πληροφοριακά συστήματα και ψηφιακά δεδομένα

Στο άρθρο δεύτερο παρατίθενται οι διατάξεις ουσιαστικού ποινικού δικαίου, ώστε να μπορέσει να προσαρμοστεί στην ελληνική νομοθεσία η Σύμβαση και η οδηγία. Στο άρθρο 13 του Π.Κ., με στοιχεία η' και θ', εισάγονται, δύο (2) επιπλέον ορισμοί, του πληροφοριακού συστήματος και των ψηφιακών δεδομένων, οι οποίοι αναφέρονται στην Σύμβαση και την Οδηγία και είναι απαραίτητη προϋπόθεση ώστε να ερμηνεύονται οι νέες διατάξεις που εισάγονται στον Ποινικό Κώδικα, όσο και εκείνων που τροποποιούνται με τον παρόντα νόμο.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

1.Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η' και θ' ως εξής:

«η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

Εγκλήματα σε Σχέση με Εργαλεία για την Τέλεση Κυβερνοεγκλημάτων

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

Προστίθεται νέο άρθρο 292Β, μετά το άρθρο 292Α του Ποινικού Κώδικα που αφορά την Παρακώλυση λειτουργίας πληροφοριακών συστημάτων βάση του οποίου προσαρμόζεται η ποινική προστασία αφού λαμβάνει υπόψιν την αντίστοιχη ποινική πρόβλεψη για τις επιθέσεις που εκδηλώνονται κατά συστημάτων τηλεφωνικών επικοινωνιών (άρθρο 292Α Π.Κ.), οι ποινές όμως που προβλέπονται από την Οδηγία και με τήρηση της αρχής της αναλογικότητας ανάλογα με το είδος και την ένταση της προσβολής που οι πράξεις αυτές επιφέρουν. Σύμφωνα με αυτά που ορίζονται στην Οδηγία γίνεται πρόβλεψη αυστηρότερου πλαισίου όσον αφορά την ποινή , όπου δηλαδή η πράξη αυτή επιφέρει ζημία σε μεγάλο αριθμό πληροφοριακών συστημάτων μέσω της χρήσης εργαλείων που έχουν σχεδιαστεί κυρίως για τον σκοπό αυτόν, γίνεται στο πλαίσιο δράσης εγκληματικής οργάνωσης, σε αντιστοιχία με τον ορισμό αυτής στο άρθρο 187 Π.Κ., προκαλεί ιδιαίτερα σημαντική ζημία ή πλήττει πληροφοριακά συστήματα τα οποία αποτελούν μέρος υποδομής που παρέχει ζωτικής σημασίας αγαθά ή υπηρεσίες για την κοινωνία και το κράτος.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

2.Μετά το άρθρο 292Α του Ποινικού Κώδικα προστίθεται άρθρο 292Β ως εξής:

« Άρθρο 292Β

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

1.Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.

2.Η πράξη της πρώτης παραγράφου τιμωρείται:

α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4.Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

Ποινικοποίηση αυτοτελών συμπεριφορών

Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται νέο άρθρο 292Γ σύμφωνα και με το άρθρο 7 της Οδηγίας, οι συμπεριφορές που κατατείνουν στην τέλεση των εγκλημάτων του άρθρου 292Β Π.Κ. και ειδικότερα παραγωγή, πώληση, διανομή, εισαγωγή, κατοχή κ.λπ. προγραμμάτων ή συσκευών σχεδιασμένων ή προσαρμοσμένων για την τέλεση των πράξεων του άρθρου αυτού ποινικοποιούνται αυτοτελώς.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

3.Μετά το άρθρο 292Β του Ποινικού Κώδικα προστίθεται άρθρο 292Γ ως εξής:

« Άρθρο 292Γ

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο

τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

4.Οι παράγραφοι 2 και 5 του άρθρου 348Α του Ποινικού Κώδικα αντικαθίστανται ως εξής:

«2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

5.Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους».

Πορνογραφία ανηλίκων

Το άρθρο 348Β του Ποινικού Κώδικα «Προσέλκυση παιδιών για γενετήσιους λόγους» τροποποιήθηκε και πάλι (έχει τροποποιηθεί ήδη, την τελευταία φορά με το ν. 4267/2014, που εναρμόνισε την ελληνική νομοθεσία με την Οδηγία 2011/93/ΕΕ.) και την συγκεκτριμένη τροποποίηση προστίθεται στις παραγράφους 2 και 5 ο όρος του πληροφοριακού συστήματος, όπως αυτός ορίζεται στο άρθρο 13 Π.Κ. προκειμένου να μην υπάρχει ανομοιογένεια στην ορολογία στις διάφορες διατάξεις του Ποινικού Κώδικα.

Γίνεται τροποποίηση και στο άρθρο 348Β Π.Κ. με την εισαγωγή του όρου « πληροφοριακά συστήματα» για τους ίδιους λόγους.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

5.Το άρθρο 348Β του Ποινικού Κώδικα αντικαθίσταται ως εξής:

«Άρθρο 348Β

Προσέλκυση παιδιών για γενετήσιους λόγους

Όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ».

Παράνομη πρόσβαση σε πληροφοριακό σύστημα

Γίνεται τροποποίηση στο άρθρο 370Γ Π.Κ. και αφού επαναδιατυπωθεί στην δεύτερη παράγραφο τιμωρείται και η χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα ενός πληροφοριακού

συστήματος, αυτό που αποκαλείται στην γλώσσα των δραστών hacking.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

6.Το άρθρο 370Γ του Ποινικού Κώδικα αντικαθίσταται ως εξής:

«Άρθρο 370Γ

Παράνομη πρόσβαση σε πληροφοριακό σύστημα

1.Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2.Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3.Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

4.Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση»

Παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων

Με τις νέες διατάξεις του άρθρου 370Δ ΠΚ για παραβίαση του απορρήτου των επικοινωνιών και χρήση πληροφοριών μέσω πληροφοριακών συστημάτων τιμωρούνται αυτοτελώς, όπως και οι κυρώσεις για παραβίαση του απορρήτου των τηλεφωνικών επικοινωνιών σύμφωνα με το άρθρο 370Α του Ποινικού Κώδικα (εως δέκα χρόνια φυλάκιση). Εάν οι ενέργειες αυτές συνεπάγονται παραβιάσεις του στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν το απόρρητο της εθνικής ασφάλειας σε καιρό πολέμου, τιμωρούνται σύμφωνα με το άρθρο 146 του Ποινικού Νόμου.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

7.Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:

«Άρθρο 370Δ

1.Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

2.Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.

3.Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

Παρεμβολές σε δεδομένα - Παράνομη Υποκλοπή Ψηφιακών Δεδομένων

Με τη νέα διάταξη του άρθρου 370Ε Π.Κ. η εισαγωγή, διανομή, κατοχή και διανομή προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα, για τη διάπραξη των εγκλημάτων που αναφέρονται στα άρθρα 370Α έως 370Δ του Ποινικού Κώδικα, τιμωρείται αυτοτελώς. . Με το νέο άρθρο 38ΙΑ Π.Κ. Η ελληνική νομοθεσία είναι εναρμονισμένη με το άρθρο 4 της Σύμβασης και το άρθρο 5 της Οδηγίας. Αυτή η νέα διάταξη καλύπτει ένα κενό στην ελληνική νομοθεσία και πλέον προστατεύει τα ψηφιακά δεδομένα από πράξεις καταστροφής, διαγραφής, αλλοίωσης κ.λπ. Έτσι αποφεύγεται το άτοπο τα ψηφιακά δεδομένα να προστατεύονται αντανακλαστικά μόνο στον βαθμό και την έκταση που πλήττεται ο υλικός τους φορέας (σκληρός δίσκος, φορητή μνήμη κ.λπ.) στις παραγράφους 2 και 3 προβλέπονται διακεκριμένες παραλλαγές σύμφωνα με τις ρυθμίσεις της Οδηγίας, ενώ στην παρ. 4 προβλέπεται ότι το βασικό έγκλημα της παρ. 1 διώκεται κατ' έγκληση.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

8.Μετά το άρθρο 370Δ του Ποινικού Κώδικα προστίθεται άρθρο 370Ε ως εξής:

«Άρθρο 370Ε

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

Παράνομη Παρεμβολή σε Ψηφιακά Δεδομένα -Φθορά ηλεκτρονικών δεδομένων

Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται νέο άρθρο 381Α φθορά ηλεκτρονικών δεδομένων, με τα οποία η ελληνική νομοθεσία εναρμονίζεται με το άρθρο 7 της Οδηγίας, που προβλέπει την ποινική ευθύνη προσώπων για πράξεις αγοράς, πώλησης, προμήθειας, κατοχής κ.λπ. προγραμμάτων ή κωδικών που μπορούν να χρησιμοποιηθούν σε διάφορες αξιόποινες πράξεις, συμπεριλαμβανομένων αυτών που προβλέπονται πλέον στο άρθρο 38ΙΑ του Ποινικού Κώδικα.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

9.Μετά το άρθρο 381 του Ποινικού Κώδικα προστίθεται άρθρο 381Α ως εξής:

«Άρθρο 381Α

Φθορά ηλεκτρονικών δεδομένων

1.Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

2.Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4.Για την ποινική δίωξη της πράξης της παραγράφου 1απαιτείται έγκληση».

<u>Απάτη υπολογιστών</u>

Τροποποίηση του άρθρου 386Α του Αστικού Νόμου (Ηλεκτρονική απάτη) όπως ορίζεται στο άρθρο 8 της Σύμβασης. Σύμφωνα με τους νέους κανονισμούς, η μη εξουσιοδοτημένη χρήση (ορθών) δεδομένων περιλαμβάνεται πλέον ρητά στις υποθέσεις ηλεκτρονικής απάτης, όπως αυτές που αποκτούν παράνομα το όνομα χρήστη και τον κωδικό πρόσβασης του δικαιούχου.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο

11.Το άρθρο 386Α του Ποινικού Κώδικα αντικαθίσταται ως εξής:

«Άρθρο 386Α

Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη

περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα».

Άρση του απορρήτου

Στο άρθρο 3 τροποποιήθηκε ο Ν. 2225/1994, ιδίως το άρθρο 2 επικαιροποιήθηκε. Λόγω της φύσης και της εφαρμογής αυτών των εγκλημάτων, είναι εξαιρετικά δύσκολο να εντοπιστούν χωρίς να αρθεί το απόρρητο των επικοινωνιών. Ωστόσο εξαιτίας της συνάφειας των νεοεισαχθέντων εγκλημάτων, πρέπει στον κατάλογο του άρθρου 4 ν. 2225/1194, να συμπληρωθούν τα αδικήματα των άρθρων 370Α ΠΚ, 292Α ΠΚ, 11 Ν. 3917/11, 15 Ν. 3471/2006 και 10 Ν. 3115/2003.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο τρίτο

Τροποποιήσεις του Ν. 2225/1994

1.Η παρ. 1 του άρθρου 4 του Ν. 2225/1994 αντικαθίσταται ως εξής:

«1. Η άρση του απορρήτου είναι επιτρεπτή για τη διακρίβωση των κακουργημάτων που προβλέπονται από: α) τα άρθρα 134, 135 παράγραφοι 1, 2, 135Α, 137Α, 137Β, 138, 139, 140, 143, 144, 146, 148 παρ. 2,150, 151, 157 παρ. 1, 159, 159Α, 168 παρ. 1, 187 παράγραφοι 1, 2, 187Α παράγραφοι 1 και 4, 207, 208 παρ. 1, 235 παρ. 2, 236 παρ. 2, 237 παράγραφοι 2 και 3β', 264 περιπτώσεις β' και γ', 270, 272, 275 περίπτωση β', 291 παρ. 1 περιπτώσεις β' και γ', 292Α παρ. 4 εδάφιο β' και παρ. 5, 299, 322, 323Α παράγραφοι 1, 2, 4, 5 και 6, 324 παράγραφοι 2 και 3, 336 σε βάρος ανηλίκου, 338 παρ. 1 σε βάρος ανηλίκου, 339 παράγραφοι 1 περιπτώσεις α' και β', 342 παράγραφοι 1 και 2, 348Α παρ. 4, 348Γ παρ. 1 περιπτώσεις α' και β', 349 παρ. 1 και 2, 351 παράγραφοι 1, 2, 4 και 5, 351Α παράγραφοι 1 περιπτώσεις α' και β' και 3, 370Α, 370Δ, 374, 380, 385 παρ. 1 περιπτώσεις α' και β' του Ποινικού Κώδικα, β) τα άρθρα 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 28,29, 30, 46, 47, 59, 140 και 144 του Στρατιωτικού Ποινικού Κώδικα,

γ) το άρθρο 15 παρ. 1 του Ν. 2168/1993,

δ) τα άρθρα 20, 22 και 23 του Ν. 4139/2013,

ε) το άρθρο 157 παρ. 1γ του Ν. 2960/2001,

στ) το άρθρο 3 περίπτωση ιε' του Ν. 3691/2008, σε συνδυασμό με το άρθρο δεύτερο του Ν. 2656/1998,

ζ) το άρθρο 3 παρ. 2 του Ν. 2803/2000,

η) το άρθρο 45 παρ. 1 περιπτώσεις α', β' και γ' του Ν. 3691/2008,

θ) το άρθρο 28 του Ν. 1650/1986.

Επίσης, επιτρέπεται η άρση του απορρήτου για τη διακρίβωση των προπαρασκευαστικών πράξεων για το έγκλημα της παραχάραξης νομίσματος κατά το άρθρο 211 του Ποινικού Κώδικα, καθώς επίσης και για τα εγκλήματα των παραγράφων 1, 2, 3, 4 εδάφιο α' και 6 του άρθρου 292Α, του άρθρου 292Β, του άρθρου 292Γ, των παραγράφων 1 περίπτωση γ' και 4 του άρθρου 339, της παρ. 3 του άρθρου 342, του άρθρου 348, των παραγράφων 1, 2 και 5 του άρθρου 348Α, του άρθρου 348Β, της παρ. 1 περιπτώσεις γ' και δ' του άρθρου 348Γ και της παρ. 1 περίπτωση γ' του άρθρου 351Α, των άρθρων 370Γ και 370Ε, του άρθρου 381Α, του άρθρου 381Β και του άρθρου 386Α του Ποινικού Κώδικα.

Επιπλέον, η άρση του απορρήτου είναι επιτρεπτή για τη διακρίβωση των εγκλημάτων που προβλέπονται από το άρθρο 11 του Ν. 3917/2011, το άρθρο 15 του Ν. 3471/2006 και το άρθρο 10 του Ν. 3115/2003».

2.Στο τέλος της παρ. 11 του άρθρου 5 του Ν. 2225/1994 προστίθεται εδάφιο ως εξής:

«Με την ίδια ποινή τιμωρείται αν ανακοινώνει σε τρίτους ή γνωστοποιεί οπωσδήποτε το γεγονός της άρσης του απορρήτου, καθώς και αν παραβιάσει την υποχρέωση εχεμύθειάς του κατά τη διαδικασία άρσης του απορρήτου που προβλέπεται από το άρθρο 8 του π.δ. 47/2005 (Α' 64)».

Ευθύνη νομικών προσώπων

Με το άρθρο τέταρτο ρυθμίζεται το ζήτημα των διοικητικών κυρώσεων κατά νομικών προσώπων σύμφωνα με το άρθρο 12 της Σύμβασης και το άρθρο 10 της Οδηγίας. Η υιοθέτηση του συστήματος διοικητικών κυρώσεων ακολουθεί το πρότυπο αντίστοιχων ρυθμίσεων κατά την εναρμόνιση της ελληνικής νομοθεσίας με άλλες οδηγίες.

Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο τέταρτο

Ευθύνη νομικών προσώπων

(Άρθρο 11 της Οδηγίας)

1.Αν κάποια από τις πράξεις των άρθρων 292Β, 370Γ, 370Δ, 370Ε, 381Α και 386Α του Ποινικού Κώδικα τελέστηκε, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, από φυσικό πρόσωπο που ενεργεί είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου ή της ένωσης προσώπων και έχει εξουσία εκπροσώπησής τους ή εξουσιοδότηση για τη λήψη αποφάσεων για λογαριασμό τους ή για την άσκηση ελέγχου εντός αυτών, επιβάλλονται στο νομικό πρόσωπο ή στην ένωση προσώπων με ειδικά αιτιολογημένη απόφαση της Αρχής Διασφάλισης του Απόρρητου των Επικοινωνιών, κατά περίπτωση, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις,

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 20.000 έως 1.000.000 ευρώ,

γ) ανάκληση ή αναστολή της άδειας λειτουργίας τους για χρονικό διάστημα από ένα (1) μήνα έως δύο (2) έτη ή απαγόρευση άσκησης της επιχειρηματικής τους δραστηριότητας για το ίδιο χρονικό διάστημα,

δ) αποκλεισμός από δημόσιες παροχές, ενισχύσεις, επιδοτήσεις, αναθέσεις έργων και υπηρεσιών, προμήθειες, διαφημίσεις και διαγωνισμούς του Δημοσίου ή των νομικών προσώπων του δημόσιου τομέα για το ίδιο διάστημα.

Σε περίπτωση υποτροπής οι κυρώσεις των περιπτώσεων γ' και δ' μπορεί να έχουν οριστικό χαρακτήρα και εφόσον πρόκειται περί σωματείων ή ενώσεων προσώπων, η υποτροπή μπορεί να έχει ως συνέπεια τη διάλυσή τους, σύμφωνα με τις εκάστοτε ισχύουσες διατάξεις.

2.Όταν η έλλειψη εποπτείας ή ελέγχου από φυσικό πρόσωπο που αναφέρεται στην παράγραφο 1, κατέστησε δυνατή την τέλεση από πρόσωπο που τελεί υπό την εξουσία του κάποιας από τις αξιόποινες πράξεις που αναφέρονται στην ίδια ως άνω παράγραφο, προς όφελος ή για λογαριασμό νομικού προσώπου ή ένωσης προσώπων, επιβάλλονται στο νομικό πρόσωπο, σωρευτικά ή διαζευκτικά, οι ακόλουθες κυρώσεις:

α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης,

β) διοικητικό πρόστιμο από 10.000 έως 1.000.000 ευρώ,

γ) οι προβλεπόμενες στις περιπτώσεις γ' και δ' της προηγούμενης παραγράφου κυρώσεις για χρονικό διάστημα από δέκα (10) ημέρες έως έξι (6) μήνες.

3.Για τη σωρευτική ή διαζευκτική επιβολή των κυρώσεων που προβλέπονται στις προηγούμενες παραγράφους και για την επιμέτρηση των κυρώσεων αυτών λαμβάνονται υπόψη ιδίως η βαρύτητα της παράβασης, ο βαθμός της υπαιτιότητας, η οικονομική επιφάνεια του νομικού προσώπου ή της ένωσης προσώπων και η τυχόν υποτροπή τους.

4.Η εφαρμογή των διατάξεων των προηγούμενων παραγράφων είναι ανεξάρτητη από την αστική, πειθαρχική ή ποινική ευθύνη των αναφερόμενων σε αυτές φυσικών προσώπων. Καμιά κύρωση δεν επιβάλλεται χωρίς προηγούμενη κλήτευση των νόμιμων εκπροσώπων του νομικού προσώπου ή της ένωσης προσώπων προς παροχή εξηγήσεων. Η κλήση κοινοποιείται τουλάχιστον δέκα (10) ημέρες πριν από την ημέρα της ακρόασης. Κατά τα λοιπά, εφαρμόζονται οι διατάξεις των παραγράφων 1 και 2 του άρθρου 6 του Κώδικα Διοικητικής Διαδικασίας. Σε περίπτωση άσκησης ποινικής δίωξης για κάποια από τις προβλεπόμενες στην παράγραφο 1 αξιόποινες πράξεις που τελέστηκε από πρόσωπο αναφερόμενο στις παραγράφους 1 και 2 και προκειμένου να εφαρμοστεί η προβλεπόμενη στο άρθρο αυτό διαδικασία επιβολής διοικητικών κυρώσεων, οι εισαγγελικές αρχές ενημερώνουν αμέσως τον Υπουργό Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων και αποστέλλουν σε αυτόν αντίγραφα της δικογραφίας.

5.Σε περίπτωση αμετάκλητης απαλλαγής του παραπεφθέντος οι κατά τα ανωτέρω αποφάσεις επιβολής διοικητικών κυρώσεων ανακαλούνται.

6.Οι διατάξεις των προηγουμένων παραγράφων δεν εφαρμόζονται στο κράτος, στους φορείς δημόσιας εξουσίας και στους διεθνείς οργανισμούς δημοσίου δικαίου, χωρίς αυτό να επηρεάζει την εφαρμογή των ισχυουσών κάθε φορά διατάξεων περί αστικής, πειθαρχικής ή ποινικής ευθύνης.

<u>Έκδοση και αμοιβαία δικαστική συνδρομή</u>

Το άρθρο 5 της Σύμβασης για την έκδοση και την αμοιβαία νομική συνδρομή ορίζει το Υπουργείο Δικαιοσύνης ως την αρμόδια αρχή, ενώ το άρθρο 6 το ορίζει ως το σημείο επαφής για την εφαρμογή του άρθρου 35 της Σύμβασης («Δίκτυο 24/7») την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας υπό την εποπτεία Εισαγγελέα Εφετών.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι κυβερνοεπιθέσεις έχουν γίνει τόσο συνηθισμένες όσο και το ίδιο το Διαδίκτυο. Κάθε χρόνο, σε όλα τα μέσα μαζικής ενημέρωσης αλλά και ακαδημαϊκά άρθρα τονίζουν αυτόν τον αυξημένο επιπολασμό, ο οποίος είναι εξαιρετικά μεγάλος όσο και η ποικιλία των επιθέσεων και των κυβερνοεγκλημάτων. Σε αυτή τη μελέτη και μέσα από συγκεκριμένα άρθρα, επιδίωξη ήταν η προώθηση συζητήσεων σχετικά με τις απειλές στον κυβερνοχώρο. Επιπλέον να εστιασθούν γνωστικές ευπάθειες από την σκοπιά της ψυχολογίας μέσω ενός κριτικού προβληματισμού σχετικά με τις κοινωνικές και ψυχολογικές πτυχές που σχετίζονται με τις κυβερνοεπιθέσεις.

Ειδικότερα, το ενδιαφέρον ήταν να κατανοήσουμε τον τρόπο με τον οποίο οι πολίτες αντιλαμβάνονται και επιδίδονται σε κίνδυνο και τον τρόπο με τον οποίο επηρεάζονται κατά τη διάρκεια και μετά από μια κυβερνοεπίθεση. Η μελέτη λοιπόν επικεντρώθηκε σε βασικά γνωστικά ζητήματα που σχετίζονται με την κατανόηση, τις δημόσιες αντιδράσεις σε κακόβουλα συμβάντα στον κυβερνοχώρο, συμπεριλαμβανομένης της αντίληψης κινδύνου, της προστασίας , τα χαρακτηριστικά κινήτρων, πολιτισμού και επιτιθέμενου (π.χ. ταυτότητα επιτιθέμενου, κλίμακα της επίθεσης). Έγινε ένα σημαντικό βήμα ώστε να διερευνηθεί πως αντιλαμβάνονται τα άτομα την κυβερνοεπιθεση. Επικεντρωθήκαμε στις κοινωνικές και ψυχολογικές επιπτώσεις των επιθέσεων καθώς τις περισσότερες φορές παραβλέπονται. Είναι όμως παράγοντες ζωτικής σημασίας για την καλύτερη κατανόηση.

Αναφέρθηκαν περιπτωσιολογικές μελέτες κάτω από αυτό το πρίσμα.

Οι τεχνολογικές εξελίξεις ανάγκασαν τους οργανισμούς να ψηφιοποιήσουν πολλές από τις λειτουργίες τους. Ενώ οι επενδύσεις στην πληροφορική μπορεί να οδηγήσουν σε κέρδος και ευημερία, παραμονεύει πάντα ο κίνδυνος κυβερνοεπιθέσεων και περιστατικών. Το τοπίο απειλής των κυβερνοεπιθέσεων αλλάζει ραγδαία και ο αντίκτυπος τέτοιων επιθέσεων αβέβαιος. Ωστόσο, στην αναφορά που έγινε για το «Τι είναι η βλάβη στον κυβερνοχώρο για τους οργανισμούς;», καταλάβαμε την έλλειψη αποτελεσματικών μετρήσεων, εργαλείων και πλαισίων για την καλύτερη κατανόηση των βλαβών που αντιμετωπίζουν οι οργανισμοί από κυβερνοεπιθέσεις. Οι οργανισμοί ή οι εταιρείες γενικότερα δεν έχουν κίνητρα να επενδύσουν και να δώσουν προτεραιότητα στην ασφάλεια. Είναι υψίστης σημασίας να γίνει μια ολοκληρωμένη ανάλυση κόστους-οφέλους σχετικά με τον τρόπο με τον οποίο οι τεχνολογίες αιχμής και οι επενδύσεις στην εφαρμογή ισχυρών πρακτικών κυβερνοασφάλειας ενδέχεται να αντισταθμίσουν τον κίνδυνο κυβερνοεπίθεσης και τον επιβλαβή αντίκτυπό της. Οι περιπτωσιολογικές μελέτες που παρουσιάστηκαν κατέδειξαν ότι οι οργανισμοί δεν διαθέτουν επαρκή μοντέλα κατανόησης της βλάβης είτε άμεση είτε έμμεση, από κυβερνοεπιθέσεις. Αυτό που προκύπτει περαιτέρω από την ανάλυση των περιπτωσιολογικών μελετών είναι ότι οι οργανισμοί εξακολουθούν να αγνοούν τις βλάβες που προκαλούν στους καταναλωτές ή τους υπαλλήλους τους. Ως εκ τούτου, είναι αδύνατο χωρίς μια ολιστική κατανόηση όλων των πιθανών βλαβών για τους οργανισμούς να δοθεί προτεραιότητα στους μετριασμούς αυτών των βλαβών. Τρέχουσες πρακτικές που υιοθετούν οι οργανισμοί είτε για να υπολογίσουν «μυωπικά» τη βλάβη από μια κυβερνοεπίθεση είτε να υπολογίσουν τυχόν οικονομικές ζημίες

παραμελούν τις έμμεσες βλάβες που προκύπτουν από κυβερνοεπιθέσεις και βλάπτουν τους καταναλωτές.· Αυτές οι βλάβες δεν είναι πάντα ορατές.

Με βάση μια διεξοδική βιβλιογραφική ανασκόπηση και την ανάλυση μιας σειράς κυβερνο-περιστατικών, παρουσιάσαμε μια ταξινόμηση των κυβερνοβλαβών, άμεσες ή έμμεσες που μπορεί να βιώσουν οργανισμοί και άτομα. Η προσδοκία είναι ότι η ταξινόμηση θα πρέπει να παρέχει την ουσιαστική ευρεία γνώση των βλαβών για τους οργανισμούς, επιτρέποντάς τους να εξετάσουν το ενδεχόμενο να βλάπτει τους καταναλωτές και άλλους εταιρικούς και μη εταιρικούς παράγοντες, καθώς και να μετατοπίσει την τρέχουσα τάση των οργανισμών να παραμένουν ανενεργοί ή να ανέχονται βλάβες που επηρεάζουν μη εταιρικούς παράγοντες. Η πραγματικότητα είναι ότι οι κυβερνοεπιθέσεις μπορούν να έχουν πολλές πιο σημαντικές και μακροχρόνιες βλάβες πέρα από αυτές που αρχικά είναι αντιληπτές.

Η ταξινόμηση αυτή ίσως θα βοηθούσε στην αποσαφήνισή τους, και ως εκ τούτου την υποστήριξη της καλύτερης λήψης αποφάσεων για τη διαχείριση κινδύνων και την επιλογή των ελέγχων ασφαλείας.

Έγινε λοιπόν προσπάθεια κατανόησης του αντίκτυπου των συμβάντων στον κυβερνοχώρο. Οικονομικές μελέτες από διακεκριμένα Ινστιτούτα ανέδειξαν και τον οικονομικό αντίκτυπο στους οργανισμούς ή στις επιχειρήσεις.

Οι απειλές στον κυβερνοχώρο αυξάνονται. Οι κυβερνοεπιθέσεις συνέχισαν να αυξάνονται τόσο σε πολυπλοκότητα όσο και σε αριθμό, αλλά και σε σχέση με τον αντίκτυπό τους. Θα πρέπει λοιπόν να αναπτυχθούν δράσεις σε διάφορα μέτωπα για να προστατευτούν όχι μόνο οι πολίτες αλλά και οι επιχειρήσεις και οργανισμοί από το κυβερνοέγκλημα, καθώς και να διαμορφωθεί ένας ασφαλής, ανοικτός και προστατευμένος κυβερνοχώρος.

Αυτό που είναι το πιο σημαντικό να κάνει κάποιος σε αυτή την ψηφιακή εποχή είναι να είναι πάντα επιφυλακτικός στο διαδίκτυο και να ακολουθεί τις βέλτιστες πρακτικές που προτείνονται από τους ειδικούς στον τομέα της κυβερνοασφάλειας.

Η ασφάλεια θα πρέπει να αποτελεί βασική αρμοδιότητα σε ολόκληρο τον οργανισμό και να ενσωματώνεται σε όλα όσα είναι και κάνει μια επιχείρηση. Από τους ανθρώπους , τα δεδομένα και κάθε πτυχή μιας επιχείρησης μπορεί να κινδυνεύουν. Επενδύσεις σε ενεργοποίηση τεχνολογιών ασφαλείας, όπως η ευφυΐα και η απειλή για την ασφάλεια μπορεί να συμβάλουν στη μείωση του κόστους του εγκλήματος στον κυβερνοχώρο. Οι υπηρεσίες cloud μπορούν να καταστήσουν την έρευνα για τις απειλές στον κυβερνοχώρο πιο αποτελεσματική.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. "The Cost of Cybercrime" Ninth Annual Cost of Cybercrime Study, Unlocking the Value of improved Cybersecurity Protection, Ponemon Institute
2. The Social and Psychological Impact of Cyber-Attacks Maria Bada , Jason R. C. Nurse, To be published in: Benson & McAlaney (2019/20) Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press
3. Beck U. Risk Society: Towards a New Modernity. Vol. 17. London: Sage, 1992 .
4. Beck U. The terrorist threat: world risk society revisited. Theory Cult Soc 2002;19:39–55
5. Van Slyke SR, Van Slyke S, Benson ML. The Oxford Handbook of White-Collar Crime. Oxford University Press, 2016.
6. Greenfield VA, Paoli L. A framework to assess the harms of crimes. Br J Criminol 2013;53:864–885.
7. National Institute of Standards Technology. Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. http://dx.doi.org/10. 6028/NIST.SP.800-30r1
8. New Zealand Government. Risk Assessment Process: Information Security. https://www.ict.govt.nz/assets/ICT-System-Assurance/RiskAssessment-Process-Information-Security.pdf
9. Pemberton S. Social harm future (s): exploring the potential of the social harm approach. Crime Law Soc Change 2007; 48:27–41.
10. Anderson R, Moore T. The economics of information security. Science 2006;314:610–613.
11. Moore T. The economics of cybersecurity: principles and policy options. IJCIP2010;3:103–17.
12. Punter A, Coburn A, Ralph D. Evolving risk frameworks: modelling resilient business systems as interconnected networks. Centre for Risk Studies, University of Cambridge 2016. http://cambridgeriskframework.com/ page/17
13. Lloyds of London. Counting the cost. https://www.lloyds.com/news-andinsight/risk-insight/library/technology/countingthecost
14. Klahr R, Shah J, Sheriffs P, et al. Cyber security breaches survey 2017: main report, 2017. https://www.gov.uk/government/statistics/cyber-secur ity-breaches-survey-2017
15. Anderson R, Bo¨hme R, Clayton R, et al. Security economics and European policy. In: Pohlmann N., Reimer H., Schneider W. (eds). ISSE 2008 Securing Electronic Business Processes 2009; 55–80.
16. Laube S, Bo¨hme R. The economics of mandatory security breach reporting to authorities. J Cybersecur 2016;2:29–41.
17. Kshetri N. The simple economics of cybercrimes. IEEE Secur Priv 2006;4: 33–39.
18. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cybersecur 2016;2:3–14.
19. Nguyen KD, Rosoff H, Richard SJ. Valuing information security from a phishing attack. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2017.

20. Why it pays to complain via Twitter. BBC News, 2014. http://www.bbc.co.uk/news/business-27381699
21. Cavusoglu H, Mishra B, Raghunathan S. The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. IJEC 2004; 9:70–104.
22. Hovav A, D'Arcy J. The impact of denial-of-service attack announcements on the market value of firms. RMIR 2003;6:97–121.
23. Campbell K, Gordon LA, Loeb MP, et al. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 2003;11:431–448.
24. World Economic Forum. Partnering for cyber resilience towards the quantification of cyber threats. http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf
25. C¸etin B, Yaman E, Peker A. Cyber victim and bullying scale: a study of validity and reliability. Comput Educ 2011;57:2261–2271.
26. Harvard Mental Health Letter. Protecting children and teens from cyberharm. Harvard Health Pubs 2008;25:4–5.
27. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. Int Secur 2013;38:41–73.
28. Charles P, Pfleeger SL. Analyzing Computer Security: A Threat/ Vulnerability/Countermeasure Approach. Upper Saddle River, NJ: Prentice Hall, 2012 .
29. Kesan JP, Hayes CM. Thinking through active defense in cyberspace. In: Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options, Washington, DC: The National Academies Press; 2010, 327–42.
30. US Department of Homeland Security. Cyber risk management and cybersecurity insurance. http://www.dhs.gov/cybersecurity-insurance
31. Titcomb J. Ukrainian blackout blamed on cyber-attack. The Telegraph, 2015 http://www.telegraph.co.uk/technology/news/12082758/Ukrainianblackout-blamed-on-cyber-attack-in-world-first.html
32. Greenberg A. Hackers remotely killed a jeep on the highway- with me in it. Wired, 2015; http://www.wired.com/2015/07/hackers-remotely-killjeep-highway/
33. Lee T. Forget the Ashley Madison or Sony Hacks – a crippling cyberattack is imminent in the US. The Guardian, 2015. http://www.theguardian.com/technology/2015/jul/26/cybercrime-hacking-internet-of-things-target
34. Paolo Passeri, Hackmageddon. Cyber attacks timeline, 2016; http://www.hackmageddon.com/category/security/cyber-attacks-timeline
35. Veris Community D. http://veriscommunity.net/vcdb.html
36. Hess A. Inside the Sony hack.Slate, 2015 [CrossRef][10.3998/mij.15031809. 0002.203] http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html
37. Elo S, Kyngaॅs H. The qualitative content analysis process. J Adv Nurs 2008;62:107–15.
38. Hsieh HF, Shannon SE. Three approaches to qualitative content analysis. Qual Health Res 2005;15:1277–88

39. Talktalk hackers go on £600 spending spree with stolen card details as boss says its too early to consider compensation. The Mirror, 2015. http:// www.mirror.co.uk/news/uk-news/talktalk-hackers-go-600-spending6694321
40. McDaid L. Talktalk cyber-attack: county Londonderry man targeted. BBC News, 2015. http://www.bbc.co.uk/news/uk-34613921.
41. Howard JD, Longstaff TA. A common language for computer security incidents. Sandia National Laboratories, 1998. https://prod.sandia.gov/ techlib-noauth/access-control.cgi/1998/988667.pdf
42. Adams, J. (2013). Risk compensation in cities at risk. In: Joffe, H., Rossetto, T., Adams, J. (eds.) Cities at Risk. ANTHR, pp. 25–44. Springer, Netherlands.
43. Agrafiotis I, Bada M, Cornish P, et al. Cyber harm: concepts, taxonomy and measurement. Saı¨d Business School Working Paper 2016; 23. doi: http://dx.doi.org/10.2139/ssrn.2828646.
44. Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 32, 665-683.
45. Altheide, D.L. (2002) Creating Fear; News and the Construction of Crisis, (Aldine De Gruyter; New York).: p.24.
46. Anderson R, Bo¨hme R, Clayton R, et al. Security economics and European policy. In: Pohlmann N., Reimer H., Schneider W. (eds). ISSE 2008 Securing Electronic Business Processes 2009; 55–80.
47. Anderson R, Moore T. The economics of information security. *Science* 2006; 314:610–613
48. Anderson R, Moore T. The economics of information security. Science 2006; 314:610–613.
49. Ashley M. Aftermath: confessions, suicide reports and hot on the hacker's trail. National Post,2015 http://news.nationalpost.com/news/canada/ashley-madison-aftermath-confessions-suicide-reports-and-hot-on-the-hackers-trail
50. Bada, M., Sasse, A.M. & Nurse, J. R. C. (2015) Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, in proceedings of the International Conference on Cyber Security for Sustainable Society (CSSS) Coventry, UK, 118-131. SSN+.
51. Bandura, A. (1986). Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy. American Psychologist, 41(12), 1389-1391.
52. Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes, 50, 248-287.
53. Bandura, A. & Adams N.E., (1977). Analysis of Self-Efficacy Theory of Behavioral Change. Cognitive Therapy and Research, Vol. 1, No. 4, pp. 287-310.
54. Barlyn, S. (2017). Global cyber attack could spur $53 billion in losses - Lloyd's of London. Reuters. Retrieved July 14 2018, from https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH
55. BBC. (2017a). NHS 'robust' after cyber-attack Retrieved July 14 2018, from

https://www.bbc.co.uk/news/uk-39909441
56. Beck, U. (1999). World Risk Society. Cambridge: Polity Press.
57. Betz, D. J. & Stevens, T. (2011). Cyberspace and the State. London: Routledge.
58. Blythe J. & Camp, J. L. (2012). Implementing mental models. IEEE Symposium on Security and Privacy Workshops, 24-25 May 2012, San Francisco, CA, 86-90.
59. Blythe, J., Camp, J. & Garg, V. (2011). Targeted risk communication for computer security, in 15th International Conference on Intelligent User Interfaces, pp. 295–298.
60. Böhme, R. & Moore, T. (2012). How do consumers react to cybercrime? eCrime Researchers Summit, Las Croabas, pp. 1-12.
61. Brenner SW. Cybercrime metrics:old wine, new bottles? Va. JL & Tech 2004; 9:13–13
62. Campbell K, Gordon LA, Loeb MP, et al. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 2003;11:431–448.
63. Collinson, P. (2015). Cyber attack hits RBS and NatWest online customers on payday. The Guardian. Retrieved July 4 2018, from https://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problemss
64. Collinson, P. (2017). Lloyds bank accounts targeted in huge cybercrime attack. The Guardian. Retrieved July 4 2018, from https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack
65. Dallaway, E. (2016). #ISC2Congress: Cybercrime Victims Left Depressed and Traumatized. Infosecurity Magazine. Retrieved July 4 2018, from https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/
66. Dark Reading. Sony data breach cleanup to cost $171million, 2011 http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanup-to-cost-\$171-million/d/d-id/1097898
67. Dickert, S., Västfjäll, D., Mauro, R., & Slovic, P. (2015). The feeling of risk: Implications for risk perception and communication. In H. Cho, T. Reimer, & K. A. McComas (Eds.), The SAGE handbook of risk communication (pp. 41–54). Thousand Oaks, CA: Sage Publications.
68. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cybersecur 2016;2:3–14.
69. Elo S, Kyngaॅ s H. The qualitative content analysis process. J Adv Nurs 2008;62:107–15.
70. Felici M, Wainwright N, Cavallini S, *et al*. What's new in the economics of cybersecurity? *IEEE Secur Priv* 2016; 14:11–13
71. Fisher, M., Therrien, A., Hand, J. & McCague, B. (2017). How cyber-attack is disrupting NHS. BBC News. Retrieved July 4 2018, from https://www.bbc.com/news/live/39901370
72. Furedi, F. (2002). Culture of fear: Risk-taking and the morality of low expectation.

London: Continuum.
73. Furedi, F. (2002). Culture of fear: Risk-taking and the morality of low expectation. London: Continuum.
74. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. & Laplante, P. (2011). Dimensions of cyber attacks: Social, political, economic, and cultural. IEEE Technology & Society Magazine, 30(1), 28-38.
75. Garland, D. (2001) The Culture of Control; Crime and Social Order in Contemporary Society, OUP: Oxford.
76. Greenberg A. Hackers remotely killed a jeep on the highway- with me in it. Wired, 2015; http://www.wired.com/2015/07/hackers-remotely-kill- jeep-highway/
77. Gross, M. L., Canetti, D., & Vashdi, D.R. (2016). The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists, 72(5), 284-291.
78. Gross, M.L., Canetti, D., Vashdi, D.R. (2017) Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes, Journal of Cybersecurity, 3(1), 49–58.
79. Hale, C. (1996). Fear of crime: a review of the literature. International Review of Victimology 4:79–150.
80. Hess A. Inside the Sony hack. Slate**,** 2015 http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html
81. Hess A. Inside the Sony hack.Slate, 2015 [CrossRef][10.3998/mij.15031809.0002.203] http://www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html
82. Hirtz, Rob. (1998). Martin Seligman's journey from learned helplessness to learned happiness. The Pennsylvania Gazette. Retrieved August 4 2018, from http://www.upenn.edu/gazette/0199/hirtz.html
83. Howard JD, Longstaff TA. A common language for computer security incidents. Sandia National Laboratories, 1998. https://prod.sandia.gov/ techlib-noauth/access-control.cgi/1998/988667.pdf
84. Hsieh HF, Shannon SE. Three approaches to qualitative content analysis.Qual Health Res 2005;15:1277–88.
85. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats
86. InfoSec Institute. Ashley Madison revisited: legal, business and security repercussions, 2015, 8. http://resources.infosecinstitute.com/ashley-madison-revisited-legal-business-and-security-repercussions.
87. Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. Human-centric Computing and Information Sciences, 6(8). https://doi.org/10.1186/s13673-016-0065-2
88. Journal of Cybersecurity 2018, 1-15 I. Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese and David Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate"

89. Journal of Cybersecurity 2018, 1-15 I. Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese and David Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate"
90. Kannan K, Rees J, Sridhar S. Market reactions to information security breach announcements: an empirical analysis. IJEC 2007;12:69–91.
91. Kesan JP, Hayes CM. Thinking through active defense in cyberspace. In: Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options, Washington, DC: The National Academies Press; 2010, 327–42.
92. Kirwan, G. & Power, A. (2011). The Psychology of Cyber Crime: Concepts and Principles. IGI Global.
93. Klahr R, Shah J, Sheriffs P, et al. Cyber security breaches survey 2017: main report, 2017. https://www.gov.uk/government/statistics/cyber-secur ity-breaches-survey-2017
94. Kleinot, M.C., & Rogers, R.W. (1982). Identifying effective components of alcohol misuse prevention programs. Journal of Studies on Alcohol, 43, 802-811.
95. Kshetri N. The simple economics of cybercrimes. IEEE Secur Priv 2006;4: 33–39.
96. Laube S, Bö hme R. The economics of mandatory security breach reporting to authorities. J Cybersecur 2016;2:29–41.
97. Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. Journal of Information Technology & Politics 10(1), 86-103.
98. Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), Advances in experimental social psychology. 5:119-186. New York: Academic Press.
99. Lloyds of London. Counting the cost. https://www.lloyds.com/news-and- insight/risk-insight/library/technology/countingthecost (13 July 2018, date last accessed).
100. Lynn, R. (2007). Virtual Rape is Traumatic, but is it a Crime? Retrieved August 4 2018, from http://www.wired.com/culture/lifestyle/commentary/sexdrive/ 2007/05/sexdrive_0504
101. Maddux, J.E., & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19, 469-479.
102. McDaid L. Talktalk cyber-attack: county Londonderry man targeted. BBC News, 2015. http://www.bbc.co.uk/news/uk-34613921 (13 July 2018, date last accessed).
103. Minei, E. & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. Journal of Human Behaviour in the Social Environment, 21(8),995-1019
104. Minei, E. & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. Journal of Human Behaviour in the Social Environment, 21(8), 995-1019.
105. Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. IEEE Security & Privacy, 13(5), 99-103.
106. Moore T. The economics of cybersecurity: principles and policy options

IJCIP2010;3:103–17.
107. Nguyen KD, Rosoff H, Richard SJ. Valuing information security from a phishing attack. In: International Conference on Applied Human Factors and Ergonomics. Cham: Springer, 2017.
108. Nurse, J. R. C. & Bada, M. (2018). The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), Oxford Handbook of Cyberpsychology 2nd Edition. Oxford: OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.36
109. Nurse, J. R. C. (2018). Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), Oxford Handbook of Cyberpsychology 2nd Edition. Oxford: OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.35
110. Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. IT Professional, 19(5), 20-26. IEEE. https://doi.org/10.1109/MITP.2017.3680959
111. Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. In Proceedings ofInternational Workshop on Socio-Technical Aspects in Security and Trust (STAST), pp. 60-68. IEEE. https://doi.org/10.1109/STAST.2011.6059257
112. P Morgan Chase reveals massive data breach affecting 76m households. The Guardian, 2014 http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach.
113. Paolo Passeri, Hackmageddon. Cyber attacks timeline, 2016; http://www. hackmageddon.com/category/security/cyber-attacks-timeline
114. Peachey, K. (2017). Lloyds online banking problems enter second day. BBC News. Retrieved August 14 2018, from https://www.bbc.co.uk/news/business-38594058
115. Pemberton S. Social harm future (s): exploring the potential of the social harm approach. Crime Law Soc Change 2007; 48:27–41.
116. Prochaska, J.O., Redding, C.A., & Evers, K. (2002). The Transtheoretical Model and Stages of Change. In K. Glanz, B.K. Rimer & F.M. Lewis, (Eds.) Health Behavior and Health Education: Theory, Research, and Practice (3rd Ed.). San Francisco, CA: Jossey-Bass, Inc.
117. Punter A, Coburn A, Ralph D. Evolving risk frameworks: modelling resili- ent business systems as interconnected networks. Centre for Risk Studies, University of Cambridge 2016. http://cambridgeriskframework.com/ page/17 (13 July 2018, date last accessed).
118. PwC. Limiting the impact of data breachesthe case of the Sony Play Station Network, 2011 http://www.strategyand.pwc.com/reports/limiting-impact-data-breaches-case
119. Reeve, T. (2017). Once bitten, twice shy: ONS stats reveal public response to cyber-crime. Magazine. Retrieved August 14 2018, from https://www.scmagazineuk.com/once-bitten-twice-shy-ons-stats-reveal-public-response-cyber-crime/article/1475468
120. Reid, L. W., Roberts, J. T., & Hilliard, H. M. (1998). Fear of crime and collective action: An analysis of coping strategies. Sociological Inquiry, 68(3), 312-328.
121. Reuters. (2017). Cyber attack hits 200,000 in at least 150 countries: Europol. Retrieved August

14 2018, from https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX

122. Rippetoe, P.A., & Rogers, R.W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. Journal of Personality and Social Psychology, 52, 596-604.
123. Rogers, M. B., Amlôt, R., Rubin, G., Wessely, S. & Krieger, K. (2007). Mediating the Social and Psychological Impacts of Terrorist Attacks: The Role of Risk Perception and Risk Communication. International Review of Psychiatry, 19, 279-288.
124. Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91, 93-114.
125. Rogers, R.W., & Mewborn, C.R. (1976). Fear appeals and attitude change: Effects of a threat's noxiousness, probability of occurrence, and the efficacy of the coping responses. Journal of Personality and Social Psychology, 34, 54-61.
126. Rogers, R.W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. Gochman (Ed.), Handbook of health behavior research: Vol. 1. Determinants of health behavior: Personal and social (pp. 113-132). New York, NY: Plenum.
127. Sanger, D.E., Chan, S. and Scott, M. (2017). Ransomware's Aftershocks Feared as U.S. Warns of Complexity. The New York Times. Retrieved July 14 2018, from https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html
128. Seligman, Martin E. P. (1975). Helplessness: On Depression, Development, and Death. San Francisco: W.H. Freeman.
129. Sjöberg, L. (2000). Factors in Risk Perception. Risk Analysis, 20: 1-12
130. Sjöberg, L. (2000). Factors in Risk Perception. Risk Analysis, 20: 1-12.
131. Slovic, P. (1988). Risk perception. In C. C. Travis (Ed.), Contemporary issues in risk analysis: Vol. 3: Carcinogen risk assessment (pp. 171-181). New York: Plenum.
132. Slovic, P. (2000). The perception of risk. London: Earthscan.
133. Stekel, W. (1930). Les etats d' angoisse nerveux. Payot.
134. Suler, J. (2004). The Online Disinhibition Effect. Cyberpsychology and behaviour, 7(3), 321-324.
135. Sutherland, S. (2007). Irrationality: The Enemy Within. London: Pinter & Martin.
136. Symantec. (2010). Norton Cybercrime Report: The Human Impact. Retrieved June 14 2018, from https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf
137. Talktalk hackers go on £600 spending spree with stolen card details as boss says its too early to consider compensation. The Mirror, 2015. http:// www.mirror.co.uk/news/uk-news/talktalk-hackers-go-600-spending- 6694321 (13 July 2018, date last accessed).
138. The Economic Impact of Cybercrime— No Slowing Down McAfee February 2018
139. The Independent. (2017). NHS cyber attack: International manhunt to find criminals behind WannaCry ransomware that crippled hospital systems. Retrieved July 14 2018, from https://www.independent.co.uk/news/uk/home-news/wannacry-wanna-detector-accident-and-emergency-patient-appointment-operation-a7734831.html

140. The Verge *The mind-bending messiness of the Ashley Madison data dump***,** 2015 http://www.theverge.com/2015/8/19/9178855/ashley-madison-data-breach-implications
141. Titcomb J. Ukrainian blackout blamed on cyber-attack. The Telegraph, 2015 http://www.telegraph.co.uk/technology/news/12082758/Ukrainian- blackout-blamed-on-cyber-attack-in-world-first.html
142. UK Government and Marsh, Ltd. UK cyber security: the role of insurance in managing and mitigating the risk. https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance
143. US Department of Homeland Security. Cyber risk management and cyber-security insurance. http://www.dhs.gov/cybersecurity-insurance (13 July 2018, date last accessed).
144. Variety Sony hack attack opens minefield of legal questions that has hollywood worried**,** 2015,07–13 http://variety.com/2015/biz/news/sony-hack-attack-opens-minefield-of-legal-questions-that-has-hollywood-worried-1201471664
145. Veris Community D. http://veriscommunity.net/vcdb.html
146. Verizon. (2018). 2018 Data Breach Investigations Report. Retrieved August 4 2018, from https://www.verizonenterprise.com/verizon-insights-lab/dbir/
147. Verizon. (2018). 2018 Data Breach Investigations Report. Retrieved August 4 2018, from https://www.verizonenterprise.com/verizon-insights-lab/dbir/
148. Virtanen, S. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities, Psychiatry, Psychology and Law, 24:3, 323-338.
149. Why it pays to complain via Twitter. BBC News, 2014. http://www.bbc.co.uk/news/business-27381699
150. Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1-13.
151. Williams, M., Axon, L., Nurse, J. R. C., & Creese, S. (2016). Future scenarios and challenges for security and privacy. In Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016 IEEE 2nd International Forum on (pp. 1-6). IEEE. https://doi.org/10.1109/RTSI.2016.7740625
152. Williams, M., Nurse, J. R. C., & Creese, S. (2017). Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things. In Proceedings of the 15th International Conference on Privacy, Security and Trust (PST). https://doi.org/10.1109/PST.2017.00029
153. Witte, K. (1991). Preventing AIDS through persuasive communication: Fear appeals and preventive-action efficacy. Doctoral dissertation, University of California, Irvine.
154. Witte, K. (1992). The role of threat and efficacy in AIDS prevention. International Quarterly of Community Health Education, 12, 225-249.
155. Witte, K. (1992a). Putting the Fear Back in Fear Appeals: The Extended Parallel Process Model. Communication Monographs, 59, 329-349.
156. Witte, K. (1994). Fear control and danger control: A test of the Extended Parallel Process Model (EPPM). Communication Monographs, 61, 113-134.
157. World Economic Forum. Partnering for cyber resilience towards the quantification of cyber threats http://www3.weforum.org/docs/WEFUSA Quantification of Cyber Threats_Report2015.pdf

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ιωάννης Ιγγλεζάκης, Δίκαιο της Πληροφορικής σελ.327
2. Νομοθεσία - Ηλεκτρονικό Έγκλημα (google.com)
3. Νόμος 4411/2016 : Κύρωση της Σύμβασης για το έγκλημα στον Κυβερνοχώρο - Χρηστικές Πληροφορίες (e-nomothesia.gr)
4. Νόμος 4411/2016 : Κύρωση της Σύμβασης για το έγκλημα στον Κυβερνοχώρο www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

ΠΑΡΑΡΤΗΜΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ