ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΛΟΓΙΣΤΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ

Διπλωματική Εργασία

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ

της

ΠΑΝΑΓΟΥ ΣΠΥΡΙΔΟΥΛΑΣ
Επιβλέπων Καθηγητής: ΛΙΒΑΝΗΣ ΕΥΣΤΡΑΤΙΟΣ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος στη Λογιστική και Χρηματοοικονομική

Οκτώβριος 2019

ΕΥΧΑΡΙΣΤΙΕΣ

Πρωτίστως αμέριστη ευγνωμοσύνη και θερμές ευχαριστίες για τα τόσα, και για άλλα τόσα χρόνια αέναης και ανιδιοτελής στήριξης και ενθάρρυνσης, θα ήθελα να εκφράσω στους γονείς μου Παναγιώτη και Γεωργία, στην αδερφή μου Μαρίλια, καθώς και στους φίλους μου, για την ηθική υποστήριξη που μου πρόσφεραν σε αυτό το ταξίδι. Η παρούσα διπλωματική εργασία αφιερώνεται σε σας ως ένδειξη ευγνωμοσύνης για τα όσα έχετε προσφέρει σε μένα.

Στη συνέχεια θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα της διπλωματικής μου εργασίας, κ. Λιβάνη Ευστράτιο, για την πολύτιμη βοήθεια του, την ευκαιρία που μου έδωσε να ασχοληθώ με ένα άκρως επίκαιρο και ενδιαφέρον θέμα καθώς και για την ανταπόκρισή του κάθε φορά που χρειαζόμουν την καθοδήγησή του.

Τέλος, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του ΠΜΣ της Λογιστικής και Χρηματοοικονομικής, οι οποίοι μου παρείχαν γνώσεις, που θα μου είναι απαραίτητες για το μέλλον μου.

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή αποτελεί μια μελέτη για την σημασία των κυβερνοεπιθέσεων και τον αντίκτυπό τους στον χρηματοοικονομικό τομέα. Αποτελείται από βιβλιογραφική επισκόπηση των κυβερνοεπιθέσεων, τεχνικές λύσεις για την αποφυγή των κυβερνοεπιθέσεων και τέλος μελέτη τριών περιπτώσεων κυβερνοεπιθέσεων σε εταιρίες του χρηματοοικονομικού τομέα. Μέσα από την ενδελεχή εξέταση ορισμένων εκ των πιο καίριων ζητημάτων που αναδύονται, αποσκοπούμε σε μια, όσο το δυνατόν πιο ολιστική περιγραφή των ανωτέρω αυτών θεμάτων. Η ανασκόπηση της παγκόσμιας βιβλιογραφίας εξυπηρετεί ακόμα περισσότερο τον στόχο της εργασίας, καθότι δίνεται η ευκαιρία στον αναγνώστη να αποκτήσει άποψη για τις πιο σύγχρονες εξελίξεις, καθώς και τους προβληματισμούς που υπάρχουν, τόσο για τη σοβαρότητα των κινδύνων του κυβερνοχώρου, όσο και για τους τρόπους διαχείρισης και αντιμετώπισής τους. Στο πλαίσιο αυτό, η ασφάλιση έναντι αυτής της μορφής των κινδύνων, αποτελεί ένα θέμα που προσελκύει το αυξανόμενο ενδιαφέρον της επιστημονικής παγκόσμιας κοινότητας, δεδομένου ότι δείχνει πολλά υποσχόμενη, ως μια αποδοτική εναλλακτική μορφή διαχείρισης των κινδύνων του κυβερνοχώρου.

Abstract

The aim of this thesis is a study of the importance of cyber attacks and their impact on the financial sector. It consists of a bibliographic overview of cyber attacks, technical solutions to avoid cyber attacks and finally a study of 3 case studies of cyber attacks in companies in the financial sector. By taking a closer look at some of the key issues that are emerging, we aim to provide as holistic a description of these issues as possible. The overview of the world bibliography serves the purpose of the work further, as it gives the reader an opportunity to get an idea of the latest developments and the concerns that exist, both in terms of the seriousness of cyber risks and how they are managed and addressing them. In this context, insurance against this form of risk is an issue that is attracting the growing interest of the scientific world community as it shows great promise as an efficient alternative form of cyber risk management.

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΣΧΕΔΙΑΓΡΑΜΜΑΤΩΝ Σελ.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγικό Σημείωμα

Με την ευρεία χρήση του Διαδικτύου την δεκαετία του 1990 άλλαξαν ριζικά οι ζωές των ανθρώπων. Ξαφνικά ανοίχτηκαν άπειρες δυνατότητες για τους πολίτες και το διαδίκτυο έγινε καθημερινό εργαλείο στα χέρια τους. Η εκμηδένιση των αποστάσεων, η ελεύθερη επικοινωνία και η αποθήκευση πληροφοριών σε τεράστιας χωρητικότητας βάσεις δεδομένων αποτελούν κάποιες από τις ενέργειες τις οποίες μπορούν να εκτελέσουν μέσω των ηλεκτρονικών υπολογιστών απλοί πολίτες, αλλά και οι επιχειρήσεις και οι δημόσιοι και ιδιωτικοί φορείς. Με την αυξανόμενη χρήση του Διαδικτύου και την ανάπτυξη του ήρθε στην επιφάνεια και η έννοια του κυβερνοχώρου, του εικονικού δηλαδή περιβάλλοντος μέσα στο οποίο εκτελούνται όλες οι ενέργειες του Διαδικτύου. Χαρακτηριστικό του κυβερνοχώρου αποτελεί η έλλειψη συνόρων και η ανωνυμία που προστατεύει τους χρήστες, καθώς και η εύκολη πρόσβαση σε αυτόν. Η πρόσβαση είναι εφικτή σχεδόν από όλους, γεγονός που απέφερε συγκρούσεις και ανασφάλεια στα κράτη, τα οποία προσπαθούν να προσαρμοστούν στα καινούργια δεδομένα, σε διαφορετικού είδους απειλές, να προετοιμαστούν για νέα είδη επιθέσεων και πάνω από όλα για την αντιμετώπιση νέων αντιπάλων. Οι παραδοσιακές έννοιες της ισχύος και της κυριαρχίας μεταβάλλονται στον κυβερνοχώρο, με τα κράτη να προσπαθούν να επιβιώσουν στο καινούργιο περιβάλλον αναπροσαρμόζοντας τις στρατηγικές τους.

1.2 Σκοπός της εργασίας

Η παρούσα εργασία εντάσσεται στο ευρύτερο φάσμα της μελέτης του κυβερνοχώρου και στους κινδύνους αυτού. Παρουσιάζονται νέες έννοιες και ανεξερεύνητα πεδία, αφού επικεντρωνόμαστε σε ένα νεοσύστατο χώρο.

Οι συγκρούσεις στον κυβερνοχώρο λαμβάνουν χώρα σε καθημερινή βάση, χωρίς να γίνονται πάντοτε αντιληπτές από το ευρύ κοινό, ενώ η βασική τους ιδιαιτερότητα είναι ότι σε αυτές μπορεί να διαδραματίσει σημαντικό ρόλο ακόμα και ένας απλός πολίτης. Αν και μέχρι σήμερα ο αντίκτυπος τους είναι κυρίως οικονομικός ή/και ψυχολογικός, η συνεχής τεχνολογική εξειδίκευση που εμφανίζουν, προοικονομεί την δυνατότητα πρόκλησης ανθρώπινων απωλειών στο μέλλον.

1.3 Συνεισφορά στη Βιβλιογραφία

Η συνεισφορά της παρούσας μελέτης είναι πολύπλευρη. Ο ύψος του κινδύνου των κυβερνοεπιθέσεων είναι τεράστιος και έτσι μπορεί να ευαισθητοποιήσει τους αναγνώστες στο να προσέχουν περισσότερο στο μέλλον όταν βρίσκονται στον κυβερνοχώρο. Από την άλλη παρουσιάζει το κόστος που μπορεί να έχει σε ένα χρηματοοικονομικό ίδρυμα, αλλά και γενικά σε μια εταιρία μια κυβερνοεπίθεση. Έτσι εμβαθύνοντας στο πρόβλημα, μπορεί να βοηθήσει σε αποφυγή μελλοντικών ζημιών ή ακόμα και κλείσιμο επιχειρήσεων λόγω κυβερνοεπιθέσεων.

ΚΕΦΑΛΑΙΟ 2

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Κυβερνοχώρος

Ο κυβερνοχώρος και όροι όπως η κυβερνοασφάλεια και οι κυβερνοεπιθέσεις αναδύονται όλο και περισσότερο στην επιστήμη των διεθνών σχέσεων. Η συζήτηση γύρω από τον κυβερνοχώρο γίνεται όλο και πιο έντονη καθώς οι περισσότερες χώρες μεταφέρουν στο δίκτυο όλο και περισσότερα δεδομένα. Ο κυβερνοχώρος αποτελεί ένα χώρο δημοκρατικό και παγκόσμιο που επιτρέπει σε κράτη, οργανισμούς, εταιρείες ακόμα και ιδιώτες να έχουν παγκόσμιο αντίκτυπο. Καθημερινές λειτουργίες και συναλλαγές των πολιτών καθώς και πιο περίπλοκα στρατηγικά σχέδια δημιουργούνται και φυλάσσονται στο δίκτυο. Τα τραπεζικά συστήματα των χωρών και οι συναλλαγές των πολιτών με αυτά, λειτουργίες των επιχειρήσεων, προσωπικά δεδομένα, προσχέδια προϊόντων υψηλής τεχνολογίας, πυρηνικά προγράμματα και διάφορες λειτουργίες πυρηνικών και στρατιωτικών προγραμμάτων ψηφιοποιούνται ολοένα και περισσότερο τόσο από τις ανεπτυγμένες όσο και από τις αναπτυσσόμενες χώρες.

2.2 Ορισμός του Κυβερνοχώρου

Ο όρος «Κυβερνοχώρος» έχει πλέον εγγραφεί στο καθημερινό μας λεξιλόγιο στις δύο τελευταίες δεκαετίες του 20^{ου} αιώνα. Παρότι γενικώς μπορεί κανείς να πει ότι αναφέρεται σε μια συμπλοκή του πραγματικού χώρου (ή καλύτερα του φυσικού-κοινωνικού χώρου στην οποία βιώνεται η φυσική-κοινωνική πραγματικότητα) με τις διαμορφούμενες νέες τεχνολογικές προοπτικές, υπάρχουν διαφορετικοί τρόποι με τους οποίους γίνεται κατανοητή η έννοια του κυβερνοχώρου. (Μωυσή Α. Μπουντουρίδη, Απρ.1996).

«...ο Κυβερνοχώρος είναι η γενέτειρα της Εποχής της Πληροφορίας - η τοποθεσία όπου οι πολίτες του μέλλοντος προορίζονται για να κατοικήσουν.» (John Perry Barlow, 1990). Κυβερνοχώρος «...ο αιθέρας που περιέχεται και καταλαμβάνει το εσωτερικό όλων των Η/Υ». (Sardar Z. & Ravetz J.R., 1995).

«Το διαδίκτυο είναι ένα είδος κατσαρίδας της σύγχρονης εποχής,» λέει, «Θα επιζήσει.» (Paul Vixie, Internet Software Consortium, 23rd October 2002).

Ο Julian Jaynes αναφέρει ότι «Ο Κυβερνοχώρος είναι «in» χωρίς αμφιβολία. Είναι μία ενδελεχής κατασκευή λογισμικού για πληροφορίες, τρισδιάστατη και μέσα από έναν Η/Υ, μπορεί να έχει κανείς οπτική αντίληψη, να χειρισθεί και «να πετάξει μέσα από τις κορυφαίες αναφορές» και εκθέσεις, στοιχείων και των βοηθητικών εργαλείων.». (Joachim Paul, 1996).

Η διαφορά του κυβερνοχώρου με οποιονδήποτε άλλο χώρο είναι ότι σε οποιονδήποτε χώρο απαιτούνται σταθερά σημεία αναφοράς, στον δε κυβερνοχώρο δεν υπάρχουν καθορισμένα όρια και σημεία προσανατολισμού, άρα στερείται διαστάσεις, το μόνο υπάρχων σημείο αναφοράς είναι ο άνθρωπος και οι πράξεις που επιτελεί. Ένας ορισμός που προκύπτει από τα παραπάνω είναι ότι ο Κυβερνοχώρος είναι το σύνολο των ανθρώπινων πράξεων που αποτυπώνονται πάνω σε μαγνητικό υλικό.

2.3 Χαρακτηριστικά Κυβερνοχώρου

2.3.1 Το μέγεθος του κυβερνοχώρου

Ο υπολογισμός του μεγέθους του κυβερνοχώρου καθίσταται πάρα πολύ δύσκολος, όντας εικονικό περιβάλλον. Όπως αναφέρθηκε, ο κυβερνοχώρος δεν περιλαμβάνει μόνο το εικονικό κομμάτι όπως τα δίκτυα και το Ίντερνετ αλλά και τις υποδομές που αναφέρονται στον εξοπλισμό που χρειάζεται για να τεθεί σε λειτουργία. Επίσης, μεγάλη σημασία έχει η ανθρώπινη παρουσία η οποία θα κάνει χρήση του υλικού, θα φέρει στη ζωή το οικοσύστημα του κυβερνοχώρου και θα αλληλεπιδράσει μέσα σε αυτό. Ο κυβερνοχώρος διευρύνεται όταν προστεθούν περισσότεροι χρήστες σε αυτόν και όταν αυξήσουν την δραστηριότητα τους μέσα σε αυτόν. Σε έκθεση της η Διεθνής Ένωση Τηλεπικοινωνιών για το έτος 2015, αναφέρει πως μέχρι το τέλος του 2015, 32 δισεκατομμύρια άνθρωποι χρησιμοποιούν το Ίντερνετ παγκοσμίως, από τους οποίους τα δύο δισεκατομμύρια προέρχονται από τις αναπτυσσόμενες χώρες. Στην αντίστοιχη έκθεση της για το 2016 αναφέρει πως μέχρι το τέλος του 2016, το 56% του παγκόσμιου πληθυσμού, δηλαδή 3,9 δισεκατομμύρια άνθρωποι δεν χρησιμοποιούν το Διαδίκτυο. Βάσει των παραπάνω στοιχείων μπορεί να γίνει εύκολα κατανοητό πως ακόμα και αν παραπάνω από το μισό του παγκόσμιου πληθυσμού είτε δεν έχει πρόσβαση είτε δεν χρησιμοποιεί το Διαδίκτυο ο αριθμός των χρηστών παραμένει τεράστιος και έχει αυξητική τάση.

Αρκεί να ληφθεί υπόψιν ο αριθμός των ανθρώπων που χρησιμοποιούν ηλεκτρονικό ταχυδρομείο οι οποίοι σύμφωνα με τις εκτιμήσεις της εταιρίας Radicati Group INC το 2016, θα υπάρχουν πάνω από 2,6 δισεκατομμύρια χρήστες email σε όλο τον κόσμο, και μέχρι το τέλος του 2020 ο αριθμός των χρηστών του ηλεκτρονικού ταχυδρομείου θα ξεπεράσει τα 3 δισεκατομμύρια. Αυξητική τάση έχει και ο αριθμός των ιστοσελίδων σε λειτουργία και των ενεργών domain αφού το δεύτερο τρίμηνο του 2016 έκλεισε με περίπου 334.600.000 καταχωρίσεις domainname. Από τις παραπάνω στατιστικές έρευνες γίνεται φανερό πως καθημερινά καταγράφονται δισεκατομμύρια αλληλεπιδράσεις στο Διαδίκτυο οι οποίες σημαίνουν ότι καθημερινά διακινούνται άπειρα ψηφιακά δεδομένα.

Η αύξηση του μεγέθους του κυβερνοχώρου οφείλεται επίσης και στην εξέλιξη της ψηφιακής τεχνολογίας καθώς με την ανάπτυξη των εξοπλισμών και την ανακάλυψη νέων τεχνολογιών, αλλά και την εξέλιξη των Δικτύων και της ταχύτητας του Διαδικτύου, θα πολλαπλασιαστούν οι χρήστες και τα δεδομένα που ψηφιοποιούνται. Συμπερασματικά, το μέγεθος του κυβερνοχώρου δεν μπορεί να καθοριστεί με ακρίβεια αφού δεν μπορούν να μετρηθούν με ακρίβεια οι παράγοντες από τους οποίους εξαρτάται, εν τούτοις δεν μπορεί να παραβλεφθεί η συνεχής αύξηση της έκτασης του, δεδομένου ότι η διακίνηση δεδομένων και πληροφοριών αυξάνεται διαρκώς σε όλους τους τομείς της ανθρώπινης ζωής.

2.3.2 Ανωνυμία

Ένα από τα βασικότερα χαρακτηριστικά του κυβερνοχώρου αποτελεί η ανωνυμία που προσφέρει το Διαδίκτυο στους χρήστες του. Ανωνυμία μπορεί να οριστεί όταν κάποιος δεν έχει όνομα ή χρησιμοποιεί ένα άγνωστο όνομα. Η ταυτότητα των χρηστών του Διαδικτύου έχει διττό χαρακτήρα. Από την μία πλευρά, η ανωνυμία στοχεύει στην προστασία του χρήστη, και από την άλλη πίσω από αυτή παραμονεύουν κακόβουλες ενέργειες οι οποίες βλάπτουν τον χρήστη. Η θετική πλευρά της ανωνυμίας έχει άμεση σχέση με την ιδιωτικότητα και την προστασία αυτής. Σύμφωνα με τον Clarke η ιδιωτικότητα χωρίζεται στην ιδιωτικότητα της προσωπικής συμπεριφοράς, την ελευθερία δηλαδή έκφρασης απόψεων και αντιλήψεων όπως η θρησκεία και οι πολιτικές πεποιθήσεις, και την ιδιωτικότητα των προσωπικών δεδομένων. Η ανωνυμία διασφαλίζει την ιδιωτικότητα, την εμπιστευτικότητα και την ασφάλεια των ιδιωτών. Στην αρνητική πλευρά της ανωνυμίας συγκαταλέγονται όλες οι αρνητικές ενέργειες των χρηστών όπως τα spam mails, η προπαγάνδα ή ακόμα και οι κυβερνοεπιθέσεις. Ομάδες χρηστών όπως οι hackers, αλλά και επιχειρήσεις και κράτη

χρησιμοποιούν την ανωνυμία για προσωπικό συμφέρον με αποτέλεσμα να βλάπτουν άλλους δρώντες.

2.3.3 Έλλειψη ορίων

Στον κυβερνοχώρο δεν υπάρχουν σύνορα όπως υπάρχουν στον πραγματικό κόσμο. Δεν υπάρχουν οι οριοθετήσεις των κρατών και είναι αδύνατο ο κυβερνοχώρος να χωριστεί και να κατανεμηθεί όπως το έδαφος, ο αέρας και το νερό. Αυτή η έλλειψη συνόρων προκαλεί τον ανταγωνισμό των χρηστών, και ιδιαίτερα των χωρών, οι οποίες προσπαθούν να επιβάλλουν την κυριαρχία τους στον κυβερνοχώρο. Οι χώρες που οραματίζονται την οριοθέτηση και την κυριαρχία του κυβερνοχώρου, δεν υιοθετούν στρατηγικές που περιορίζονται μόνο εσωτερικά, αλλά αναπτύσσουν αρκετά αισιόδοξες, διεθνείς στρατηγικές, οι οποίες έρχονται σε σύγκρουση με τις στρατηγικές και τα συμφέροντα των υπολοίπων δρώντων. Τέλος, η μεγαλύτερη πρόκληση που αντιμετωπίζουν τα κράτη, όσον αφορά την έλλειψη συνόρων, είναι η ασφάλεια. Σε ένα κράτος με δεδομένη εδαφική έκταση είναι ευκολότερο να αντιμετωπιστούν οι κίνδυνοι και οι απειλές από οποιαδήποτε πηγή και αν προέρχονται. Στον χαοτικό όμως κόσμο του κυβερνοχώρου, η ανάγκη ανάπτυξης νέων στρατηγικών αντιμετώπισης αυξάνεται καθώς αυξάνεται και η ανάγκη συνεργασίας κρατών και οργανισμών.

2.4 Ιντερνετ

Το διαδίκτυο ή Ίντερνετ, είναι ένα «δίκτυο δικτύων», δηλαδή ένα παγκόσμιο δίκτυο στο οποίο συνδέονται εκατοντάδες χιλιάδες άλλα δίκτυα διαφόρων μεγεθών και το οποίο επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου (δικτυωμένου) Η/Υ. Πρέπει να επισημανθεί, ότι το internet λειτουργεί σε πολύ μεγάλο ποσοστό με κονδύλια και εξοπλισμό του ιδιωτικού τομέα και δεν έχει κεντρική διοίκηση, διεύθυνση ή ‘διακυβέρνηση’, ούτε όσον αφορά τις χρησιμοποιούμενες τεχνολογίες, ούτε όσον αφορά τις πολιτικές πρόσβασης και χρήσης κάθε επιμέρους δικτύου. Σε αυτό το ιδιαίτερο και μοναδικό χαρακτηριστικό του internet οφείλεται και το γεγονός ότι αφενός μεν προσφέρεται για τη διάπραξη ‘ηλεκτρονικών’ εγκλημάτων και ‘κυβερνοεγκλημάτων’, αφετέρου δε ότι ο ‘κυβερνοχώρος’ μετατράπηκε πολύ γρήγορα —και με καταπληκτική ευκολία — σε πεδίο ανθρώπινης αντιπαράθεσης, στο οποίο είναι εξαιρετικά δύσκολο να ασκηθεί έλεγχος και να τεθούν κανόνες.

Ως γνωστόν, το Διαδίκτυο αποτελεί απόγονο του ARPANET. Αρχικά, στα μέσα της δεκαετίας του 1960 οι επιστήμονες Larry Roberts και J.C.R. Licklider δουλεύοντας πάνω σε προγράμματα έρευνας και ανάπτυξης της αρμόδιας υπηρεσίας του Πενταγώνου ARPA (Advanced Research Project Agency), δημιούργησαν το δίκτυο ARPANET, το οποίο αποτελούνταν από 4 Η/Υ οι οποίοι βρίσκονταν στα πανεπιστήμια των ΗΠΑ (UCLA, SRI, UCB και πανεπιστήμιο της Γιούτα). Μετ' έπειτα με την ανάπτυξη του δικτύου συνδέθηκαν υπολογιστές από το πανεπιστήμιο της Santa Monica, του Michigan και του Illinois. Ακολούθησαν το MIT, το Harvard, το Carnegie–Mellon και το πανεπιστήμιο του Pittsburgh. Ο αρχικός σκοπός του δικτύου ήταν η ανταλλαγή ιδεών και απόψεων της ακαδημαϊκής κοινότητας και η άμεση επικοινωνία τους. Στόχος του Πενταγώνου ήταν η απαρακώλυτη επικοινωνία ακόμα και αν η Σοβιετική Ένωση πραγματοποιούσε ένα πυρηνικό χτύπημα. Οι ερευνητές της εποχής δεν μπορούσαν να φανταστούν την έκταση που θα λάμβανε το δίκτυο που δημιούργησαν ώστε να βελτιώσουν και να δώσουν έμφαση στην ασφάλεια με αποτέλεσμα να δημιουργηθούν αρκετά σημεία τρωτότητας. Σύμφωνα με τους Clarke και Knake (5) είναι τα κύρια τρωτά σημεία του Ίντερνετ:

1. Το πρώτο τρωτό σημείο του Ίντερνετ σχετίζεται με τις ISPs (Internet Service Providers) τις εταιρίες – μεσάζοντες που διανέμουν το Ίντερνετ τοπικά. Οι εταιρίες παροχής του Δικτύου χωρίζονται σε δύο κατηγορίες: Υπάρχουν οι εθνικές ISPs που κατέχουν χιλιάδες μίλια οπτικών ινών και συνδέουν τις μεγαλύτερες πόλεις της χώρας και προκειμένου να φτάσει το Ίντερνετ σε όλες τις περιοχές συνδέονται με μικρότερες τοπικές εταιρίες όπως είναι οι τηλεφωνικές εταιρίες. Σε αυτή την διαδικασία εντοπίζεται και η τρωτότητα, αφού η μεταφορά του δικτύου και η διανομή του από μικρότερες τοπικές εταιρίες αφήνει ένα κενό ασφαλείας το οποίο μπορούν να εκμεταλλευτούν άλλοι χρήστες του Ίντερνετ. Για παράδειγμα, μπορούν να αλλάξουν τις πληροφορίες του domainname ανακατευθύνοντας τους χρήστες σε άλλον ιστότοπο από αυτή που επέλεξαν με σκοπό την υποκλοπή στοιχείων.
2. Το δεύτερο σημείο σχετίζεται με το Border Gateway Protocol (BGP). Το Border Gateway Protocol (BGP) είναι ένα τυποποιημένο πρωτόκολλο εξωτερικής δρομολόγησης που επιτρέπει την δρομολόγηση πακέτων και την ανταλλαγή πληροφοριών προσβασιμότητας μεταξύ αυτόνομων συστημάτων στο διαδίκτυο. Το BGP ανήκει στην κατηγορία των πρωτοκόλλων διανύσματος μονοπατιού (Path Vector) και οι αποφάσεις δρομολόγησης βασίζονται στα διαθέσιμα μονοπάτια δρομολόγησης. Στην διαδρομή που διανύουν τα δεδομένα από τον Server μιας

ιστοσελίδας μέχρι τον Η/Υ του χρήστη θα συναντήσουν αρκετές φορές BGP το οποίο καθορίζει την βραχύχρονη διαδρομή των δεδομένων. Η λειτουργά του BGP περιορίζεται στο να «δείχνει τον δρόμο» στα δεδομένα και όχι να ελέγχει την εγκυρότητα και ορθότητα τους. Αυτός είναι και ο λόγος που αποτελεί ευάλωτο πρωτόκολλο για κακόβουλες επιθέσεις.

3. Το τρίτο ευπρόσβλητο τμήμα του Διαδικτύου αφορά την κρυπτογράφηση των δεδομένων. Τα δεδομένα που διακινούνται στο Ίντερνετ δεν είναι κρυπτογραφημένα επιτρέποντας την πρόσβαση σε όλους τους χρήστες. Πλέον πολλές ιστοσελίδες χρησιμοποιούν κρυπτογραφημένα δεδομένα όταν γίνεται σύνδεση του χρήστη με σκοπό την προστασία των κωδικών του. Εν τούτοις, εξαιτίας του μεγάλου κόστους, από τη στιγμή της σύνδεσης και μετά παύει η κρυπτογράφηση των δεδομένων και το δίκτυο γίνεται για ακόμη μία φορά μη ασφαλές.
4. Το τέταρτο ευπαθές σημείο του Ίντερνετ αφορά το λογισμικό (software), με το οποίο λειτουργούν οι Η/Υ. Η δομή του λογισμικού είναι τέτοια, που δεν αναγνωρίζει από μόνο του τα κακόβουλα προγράμματα με αποτέλεσμα το βάρος της ασφάλειας να πέφτει όλο πάνω στον χρήστη. Σε περίπτωση που ο χρήστης υποπέσει στο σφάλμα να κατεβάσει ή να ανοίξει κάποιο αρχείο με κακόβουλο λογισμικό τότε υπάρχει ο κίνδυνος υποκλοπής στοιχείων, τραπεζικών λογαριασμών και απάτης.
5. Το πέμπτο και τελευταίο ευάλωτο σημείο του Διαδικτύου είναι η αποκέντρωση του ελέγχου. Επηρεασμένοι από τα ρεύματα της εποχής οι εμπνευστές του Διαδικτύου έδωσαν περισσότερη έμφαση στην μη ύπαρξης μιας αρχής παρά στην ασφάλεια.

Όπως αναφέρθηκε το Ίντερνετ αρχικά κατασκευάστηκε για την ανταλλαγή ιδεών και απόψεων των ακαδημαϊκών και όχι να χρησιμοποιείται από εκατομμύρια ανθρώπους σε όλο τον πλανήτη. Το ARPANET βασίστηκε σε 4 αρχές για την ομαλή λειτουργία των Η/Υ που είναι συνδεδεμένοι στο δίκτυο:

1) Κάθε ξεχωριστό δίκτυο θα στέκεται από μόνο του και δεν θα χρειάζονται εσωτερικές αλλαγές προκειμένου να συνδεθεί στο Διαδίκτυο.

2) Εάν το πακέτο των απεσταλμένων δεδομένων δεν φτάσει σύντομα στον προορισμό του τότε θα αποστέλλεται πίσω στην πηγή.

3) Για την σύνδεση των δικτύων θα χρησιμοποιούνται πύλες (gates) και δρομολογητές (routers) τα οποία δεν θα συγκρατούν τα στοιχεία των δεδομένων που διακινούνται.

4) Δεν πρέπει να υπάρχει παγκόσμιος έλεγχος στο επιχειρησιακό επίπεδο.

Αυτές οι βασικές αρχές ισχύουν μέχρι και σήμερα.

2.5 Η ισχύς στον κυβερνοχώρο

Το πρόβλημα με τις έννοιες όπως η ισχύς και η κυριαρχία στο Διαδίκτυο είναι πώς μεταβάλλονται καθώς στον κυβερνοχώρο δεν υπάρχει ένα βασικό στοιχείο: τα σύνορα. Η έλλειψη οριοθέτησης αλλάζει τον τρόπο με τον οποίο τα κράτη αντιλαμβάνονται αυτές τις έννοιες καθώς και τον τρόπο που τις επιδιώκουν.

Το πώς αντιλαμβάνεται την ισχύς ένα κράτος στον κυβερνοχώρο εξαρτάται από το πώς αντιλαμβάνονται τον ίδιο τον κυβερνοχώρο. Από την μία πλευρά αν θεωρηθεί ότι ο κυβερνοχώρος έχει τα χαρακτηριστικά ενός γεωγραφικού χώρου τότε του αποδίδονται πολλές από τις ιδιότητες ενός φυσικού χώρου με αποτέλεσμα να επηρεάζει τον τρόπο με τον οποίο τα κράτη επιδιώκουν τα συμφέροντα τους μέσα σε αυτόν. Από την άλλη πλευρά, αν τα κράτη επικεντρωθούν στην έλλειψη συνόρων που χαρακτηρίζει τον κυβερνοχώρο, στην ροή των δεδομένων και στις πηγές από τις οποίες διοχετεύονται οι πληροφορίες τότε αντιδρούν πολύ διαφορετικά απέναντι στον κυβερνοχώρο και την πολιτική που ακολουθούν.

Είναι κατανοητό λοιπόν, πως ο κυβερνοχώρος χρησιμοποιείται ως μέσο επιρροής. Οι θεσμοί πολλάκις λειτουργούν ως εργαλείο στα χέρια των κρατών για την παραγωγή ισχύος. Παρόλα αυτά, οι θεσμοί δεν είναι τα μόνα εργαλεία που χρησιμοποιούν τα κράτη αλλά οποιαδήποτε πηγή μπορούν να εκμεταλλευτούν με στόχο την επίτευξη των στρατηγικών τους στόχων.

Εντούτοις, το στοιχείο που επηρεάζει περισσότερο την χάραξη πολιτικής στον κυβερνοχώρο είναι η σχέση του κράτους με τους άλλους παίκτες που δρουν στον κυβερνοχώρο. Τα κράτη παραμένουν ισχυροί παίκτες αλλά στο Δίκτυο καλούνται να ανταγωνιστούν με ένα μεγάλο εύρος οντοτήτων, μεγαλύτερο από αυτό του Διεθνούς Συστήματος, που καρπώνονται τις ευκαιρίες που προσφέρει ο κυβερνοχώρος για το δικό τους όφελος. Το πώς αντιλαμβάνονται τα κράτη τους άλλους παίκτες είναι ικανό να καθορίσει την στρατηγική της χώρας και να τα βοηθήσει να διακρίνουν τις απειλές. Η δυσκολία που πηγάζει από την δομή του κυβερνοχώρου είναι ότι στο διαδίκτυο δεν μπορεί να βρεθεί με απόλυτη σιγουριά η πηγή των απειλών.

Γι’ αυτό το λόγο, τα κράτη με τα δεδομένα που τους δίνει η αρχιτεκτονική του κυβερνοχώρου προσπαθούν να ενισχύσουν την ισχύ τους και να επιδιώξουν όσο πιο αποτελεσματικά είναι δυνατό τα συμφέροντα τους.

2.6 Η κυριαρχία στον κυβερνοχώρο

Όπως αναφέρθηκε ένα από τα προβλήματα που προκύπτουν όσον αφορά τον κυβερνοχώρο είναι η οριοθέτηση. Είναι λογικό πως όταν δεν υπάρχει γεωγραφικός χώρος , δεν υπάρχουν σύνορα και κατ’ επέκταση δεν υφίσταται εδαφική κυριαρχία.

Τα κράτη κάνουν προσπάθειες να μεταφέρουν την κυριαρχία τους στον κυβερνοχώρο, οι οποίες όμως είναι αναποτελεσματικές, καθώς ο αντίκτυπος που έχει ο κυβερνοχώρος στην κυριαρχία πηγάζει περισσότερο από την αλληλεξάρτηση των κρατών λόγω του διακρατικού του χαρακτήρα, της ροής των πληροφοριών και την έλλειψη συνόρων παρά από την γεωγραφική θέση.

Επί παραδείγματι, αν γίνει μια επίθεση από χάκερς οι σέρβερς μπορούν να τοποθετηθούν παντού ανεξαρτήτως της χώρας από την οποία προέρχονται οι επιτιθέμενοι καταργώντας την στενή έννοια της γεωγραφικής θέσης.

Γι αυτό το λόγο ο κυβερνοχώρος αποτελεί πηγή απειλών για την κυριαρχία των κρατών. Για την αντιμετώπιση αυτών των απειλών, πολλά κράτη προσπαθούν να ελέγξουν τους πολίτες τους και την πρόσβαση αυτών σε πληροφορίες και περιεχόμενα που εν δυνάμει θα αποτελέσουν απειλή για την εσωτερική τάξη του κράτους.

Σύμφωνα με τους David Betz και Tim Stevens υπάρχουν 3 είδη ελέγχου:

1. Ο έλεγχος της πρώτης γενιάς περιλαμβάνει την πρόσβαση σε συγκεκριμένες πηγές και περιεχόμενο.
2. Στον έλεγχο δεύτερης γενιάς τα κράτη υιοθετούν μια πολύπλευρη νομική και τεχνική προσέγγιση ώστε να μπορούν να αρνούνται στους πολίτες τους την πρόσβαση σε διάφορες πηγές όποτε κρίνεται απαραίτητο.
3. Το τελευταίο είδος ελέγχου της τρίτης γενιάς αποτελείται από την χρήση εκστρατειών ενημέρωσης και προπαγάνδας, ελεύθερη παρακολούθηση και συλλογή δεδομένων που επιτρέπουν στα κράτη τον πλήρη έλεγχο των πολιτών τους. Συνήθως αυτό το είδος ελέγχου χρησιμοποιούν κράτη με αυταρχικά καθεστώτα όπως η Μέση Ανατολή, η Κίνα και η Κεντρική Ασία καθώς κυριαρχεί ο φόβος μιας εξέγερσης ή η δράση των ακτιβιστών.

Όσον αφορά τα Δυτικά κράτη, χρησιμοποιούν αυστηρότερα μέτρα και ελέγχους στο Διαδίκτυο – υιοθετώντας και μέτρα που εμπίπτουν στον έλεγχο τρίτης γενιάς - με την πρόφαση της τρομοκρατίας.

Συμπερασματικά, με την κυρίαρχη αντίληψη ότι εάν ένα κράτος δεν μπορεί να ελέγξει τι περνάει τα σύνορα του, δεν είναι ικανό να ελέγξει το εσωτερικό του, τα κράτη επιδιώκουν να επιβάλλουν την κυριαρχία τους στον κυβερνοχώρο ανταγωνιζόμενοι όλους τους υπόλοιπους παίκτες.

2.7 Κυβερνοεπίθεση

«Οι άνθρωποι θεωρούν ότι οι κυβερνοεπιθέσεις περιορίζονται σε ορισμένους μόνο κλάδους. Στην πραγματικότητα ωστόσο, κάθε οργανισμός που έχει δεδομένα με αξία κινδυνεύει» , δήλωσε ο ΄΄Ted De Zabala, CyberRisk Services Leader, Deloitte Global΄΄. «Κανένας κλάδος δεν εξαιρείται από αυτόν τον κίνδυνο. Το να γνωρίζουμε την σημερινή αξία των δεδομένων μας και την αξία που αποκτούν με την πάροδο του χρόνου, όπως και το να γνωρίζουμε τον ενδεχόμενο εισβολέα, τους πόρους και τα κίνητρα του, είναι μερικά από τα πρώτα βήματα για την ορθή λήψη επιχειρησιακών αποφάσεων σχετικά με την αποτελεσματική προστασία από τις κυβερνο-επιθέσεις».

Σύμφωνα με την αναφορά, το να είναι ένας οργανισμός ασφαλής σχετίζεται τόσο με την αντιμετώπιση των αδυναμιών στις εφαρμογές όσο και με την ενδυνάμωση της ψηφιακής υποδομής. Οι οργανισμοί επομένως θα πρέπει να βρίσκονται σε ετοιμότητα για να εντοπίζουν κάθε κυβερνοεπίθεση το νωρίτερο δυνατό. Για να είναι ένας οργανισμός ανθεκτικός θα πρέπει να μπορεί έγκαιρα να εντοπίζει την κατεύθυνση μιας απειλής, την αιτία της απειλής και το πώς εκείνη θα εκδηλωθεί. Η γρήγορη ανίχνευση μιας επίθεσης μπορεί να ωθήσει έναν οργανισμό σε δράση ώστε να απομονώσει και να περιορίσει τον αντίκτυπο από την απειλή.

Τα σημαντικά σημεία της αναφοράς, συμπεριλαμβανομένων των απειλών ανά κλάδο, είναι τα ακόλουθα:

- Υψηλή Τεχνολογία: Η υψηλή τεχνολογία αποτελεί συστηματικό στόχο για επιθέσεις, με τις μεγαλύτερες απειλές να είναι, η απώλεια πνευματικής ιδιοκτησίας (intellectual property- IP) και ο «χακτιβισμός» («hacking» για την προώθηση ακτιβιστικών σκοπών). Οι απειλές χρησιμοποιούνται επίσης ως εφαλτήριο προς την επίθεση και τη «μόλυνση» άλλων οργανισμών.

- Online Μέσα: Έχουν τη μεγαλύτερη έκθεση στις κυβερνοαπειλές με κυριότερες αυτές που βλάπτουν τη φήμη. Και σε αυτή την περίπτωση, οι απειλές χρησιμοποιούνται ως μέσο προς την επίθεση και τη μόλυνση άλλων οργανισμών.
- Τηλεπικοινωνίες: Αντιμετωπίζουν πολλαπλές, εξελιγμένες επιθέσεις, συμπεριλαμβανόμενων και των επιθέσεων από Κυβερνητικές Υπηρεσίες με χρήση των λεγόμενων Advanced Persistent Threats (APT), μια σειρά από κρυφές και συνεχείς διαδικασίες «hacking», που σαν σκοπό έχουν την καθιέρωση κρυφής μακρόχρονης παρακολούθησης. Μια άλλη κρίσιμη απειλή μοναδική ίσως στον κλάδο των τηλεπικοινωνιών, είναι η επίθεση σε μισθωμένο εξοπλισμό υποδομών, όπως είναι οι οικιακοί δρομολογητές (routers) των Παροχών Υπηρεσιών Διαδικτύου (Internet Service Providers – ISPs).
- Ηλεκτρονικό Εμπόριο: Οι παραβιάσεις σε βάσεις δεδομένων (για παράδειγμα, η απώλεια δεδομένων καταναλωτών, συμπεριλαμβανομένων των ονομάτων, διευθύνσεων και τηλεφώνων) και στα συστήματα διαδικτυακών πληρωμών, αποτελούν κρίσιμες περιοχές, οι οποίες συχνά δέχονται επιθέσεις. Επιθέσεις τύπου άρνησης υπηρεσίας επίσης κυριαρχούν στη λίστα, ειδικά εκείνες που προέρχονται από «χακτιβιστές», οι οποίοι θέλουν να πλήξουν τη λειτουργία ενός οργανισμού με τρόπο που θα γίνει δημόσια γνωστό.
- Ασφαλιστικός κλάδος: Ο κλάδος αυτός διαθέτει πολλά ευαίσθητα δεδομένα τα οποία πρέπει να προστατεύσει. Οι κυβερνο-επιθέσεις αναπτύσσονται εκθετικά, όσο οι ασφαλιστικές εταιρίες κινούνται προς ψηφιακά εμπορικά κανάλια, με εξελιγμένες επιθέσεις που συνδυάζουν κακόβουλο λογισμικό με άλλες τεχνικές, όπως είναι η κοινωνική μηχανική (social engineering). Ενώ οι τρέχουσες επιθέσεις φαίνεται ότι διαρκούν λίγο, η αναφορά προβλέπει ότι ο αριθμός μακροχρόνιων απειλών μπορεί να αυξάνεται.
- Βιομηχανικός κλάδος: Αυξάνονται τόσο οι επιθέσεις από χάκερς και κυβερνο-εγκληματίες, όσο και οι επιθέσεις μέσω εταιρικής κατασκοπείας. Τα είδη των κυβερνο-επιθέσεων στο βιομηχανικό κλάδο ποικίλουν από το «Phishing» (την προσπάθεια δηλαδή απόκτησης ευαίσθητων δεδομένων) ως τη χρήση εξελιγμένου κακόβουλου λογισμικού, που στοχοποιεί όχι μόνο τα εμπορικά πληροφοριακά συστήματα αλλά και τα συνδεδεμένα με αυτά συστήματα βιομηχανικού ελέγχου.
- Κλάδος λιανεμπορίου: Τα δεδομένα των πιστωτικών καρτών είναι το νέο «νόμισμα» των χάκερς και των εγκληματιών. Οι εσωτερικές απειλές στον κλάδο του

λιανεμπορίου αυξάνονται, δημιουργώντας μια νέα γενιά εγκληματιών, οι οποίοι επικεντρώνονται στην κλοπή πληροφοριών –ιδιαιτέρως των δεδομένων συναλλαγών με κάρτες.

Στο πλαίσιο αυτό η κα. Αλήθεια Ιακάτου, επικεφαλής του Τμήματος Διαχείρισης Επιχειρησιακών Κινδύνων στη Deloitte Ελλάδος σχολίασε: «Οι κυβερνο-επιθέσεις αποτελούν πλέον σημαντική απειλή για όλες τις επιχειρήσεις. Εντούτοις, όπως επισημαίνεται και στην συγκεκριμένη έρευνα, πρόκειται για μια κατηγορία απειλών τις οποίες οι επιχειρήσεις μπορούν να διαχειριστούν, αναπτύσσοντας κατάλληλες αμυντικές δομές, οι οποίες πρέπει να είναι αποτελεσματικές, ανθεκτικές και πάντα σε ετοιμότητα. Παρά το γεγονός ότι δεν είναι δυνατό για έναν οργανισμό να είναι 100% ασφαλής, με το να εστιάζει η ανώτατη διοίκηση την προσοχή της στην σωστή υλοποίηση των τριών αυτών χαρακτηριστικών, μειώνει τον αντίκτυπό και περιορίζει τις πιθανότητες επιχειρησιακής αποδιοργάνωσης που δύνανται να προκύψουν μετά από μια κυβερνο-επίθεση.»

2.8 Ιστορική Αναδρομή Κυβερνοεπιθέσεων

1988 : Ο ιός τύπου worm Morris, ένας από τους πρώτους αναγνωρισμένους ιούς που επηρεάζουν την κινητήρια υποδομή του κόσμου στον κυβερνοχώρο, εξαπλώθηκε σε μεγάλο βαθμό στους υπολογιστές στις ΗΠΑ. Ο ιός αυτός χρησιμοποίησε αδυναμίες στο σύστημα UNIX 1 και επαναλήφθηκε τακτικά. Αναστέλλει τους υπολογιστές σε σημείο που δεν μπορούν να χρησιμοποιηθούν. Ο ιός ήταν το έργο του Robert Tapan Morris, ο οποίος είπε ότι προσπαθούσε μόνο να μετρήσει πόσο μεγάλο ήταν το Διαδίκτυο. Στη συνέχεια έγινε ο πρώτος που καταδικάστηκε στο πλαίσιο της απάτης και της κατάχρησης των ΗΠΑ. Τώρα εργάζεται ως καθηγητής στο MIT.

Κόσοβο 1999: Μία συνταρακτική επίθεση έγινε στο Κόσοβο στις 24 Μαρτίου του 1999, όταν το ΝΑΤΟ ξεκίνησε τους αεροπορικούς βομβαρδισμούς εναντίον της Σερβίας, επειδή η τελευταία αρνείται να υπογράψει τη συμφωνία για το μέλλον του Κοσσυφοπεδίου. Οι βομβαρδισμοί διήρκεσαν σχεδόν 3 μήνες και ακολουθήθηκαν από χερσαία εισβολή. Πρόκειται για την πρώτη επίθεση στην ιστορία της Συμμαχίας κατά κυρίαρχου κράτους. Στη διάρκεια των βομβαρδισμών, σύμφωνα με τη διεθνή οργάνωση προάσπισης των ανθρωπίνων δικαιωμάτων Human Rights Watch, 500 περίπου άμαχοι έχασαν τη ζωή τους σε 90

διαφορετικά επεισόδια, κατηγορώντας το ΝΑΤΟ για παραβιάσεις του διεθνούς δικαίου. Το Βελιγράδι, από την πλευρά του, έκανε λόγο για 5.000 νεκρούς αμάχους στη διάρκεια των 78ήμερων αεροπορικών επιχειρήσεων.

Δεκέμβριος 2006 : Η NASA αναγκάστηκε να μπλοκάρει τα μηνύματα ηλεκτρονικού ταχυδρομείου με συνημμένα πριν ξεκινήσει το λεωφορείο από το φόβο ότι θα χάσουν.
Το Business Week ανέφερε ότι τα σχέδια για τα πιο πρόσφατα αμερικανικά οχήματα εκτόξευσης διαστήματος προέρχονται από άγνωστους αλλοδαπούς εισβολείς.

Εσθονία 2007: Η Εσθονία δέχθηκε επίθεση από τέλη Απριλίου ως αρχές Μαΐου του 2007. Η επίθεση αυτή έγινε με την χρήση των Bots όπου Ρώσσοι εγκληματικοί φορείς χτύπησαν τα κοινωνικά δίκτυα της Εσθονίας. Μετά από αυτές τις επιθέσεις , η Εσθονία προσέγγισε το ΝΑΤΟ για στρατιωτική βοήθεια αλλά το ΝΑΤΟ δεν μπορούσε να χρησιμοποιήσει την τότε αρμοδιότητα και πολιτική του για να παρέμβει. Έπειτα το ΝΑΤΟ άνοιξε Συνεργατικό Κέντρο Κυβερνο Άμυνας Αριστείας στο Ταλίν της Εσθονίας το 2008. Η Εσθονία μέχρι να γίνει το Κέντρο Κυβερνο Άμυνας Αριστείας υιοθέτησε νέα νομοθεσία και πολιτική για να αντιμετωπίσει όποιες μελλοντικές παρόμοιες επιθέσεις στην υποδομή της του Διαδικτύου.

Οκτώβριος 2007: Το υπουργείο Κρατικής Ασφάλειας της Κίνας δήλωσε ότι οι ξένοι χάκερς, οι οποίοι ισχυρίστηκαν ότι το 42% προέρχονταν από το Ταϊβάν και το 25% από τις ΗΠΑ, είχαν κλέψει πληροφορίες από κινέζικους βασικούς τομείς. Το 2006, όταν εξετάστηκε το δίκτυο intranet της China Aerospace Science & Industry Corporation (CASIC), εντοπίστηκαν spyware στους υπολογιστές των διαβαθμισμένων τμημάτων και των εταιρικών ηγετών.

Γεωργία 2008: Είναι σημαντικό να αναφερθεί και ο πόλεμος μεταξύ Ρωσίας και Γεωργίας το 2008. Η Ρωσία χτύπησε την Γεωργία αποσιωπώντας τις ιστοσελίδες της κυβέρνησής της και τα μέσα ενημέρωσή της με σκοπό να μην μπορεί η κυβέρνηση να επικοινωνήσει με τον πληθυσμό της. Με την επίθεση αυτή παρέλυσαν την δημόσια διοίκηση της Γεωργίας. Οι επιθέσεις αυτές δεν έλειπαν από το επίκεντρο των συζητήσεων. Οι Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul (2008) παραθέτουν μια σειρά προτάσεων για την αντιμετώπιση των θυμάτων –περιοχών των κυβερνοεπιθέσεων μέσα από την μελέτη τους και το έργο τους. Προτείνουν ότι νέες προσεγγίσεις στο

παραδοσιακό Δίκαιο των Ένοπλων Συγκρούσεων πρέπει να αναπτυχθούν ώστε να παρέχει αποτελεσματικές νομικές επιδιορθώσεις κάτω από αυτόν τομέα του δικαίου.

Ιανουάριος 2009: Οι χάκερς επιτέθηκαν στην υποδομή διαδικτύου του Ισραήλ κατά τη διάρκεια της στρατιωτικής επίθεσης του Ιανουαρίου 2009 στη Λωρίδα της Γάζας. Η επίθεση, η οποία επικεντρώθηκε σε κυβερνητικές ιστοσελίδες, εκτελέστηκε από τουλάχιστον 5.000.000 υπολογιστές. Ισραηλινοί αξιωματούχοι πίστευαν ότι η επίθεση διεξήχθη από μια εγκληματική οργάνωση που εδρεύει σε ένα πρώην σοβιετικό κράτος και καταβάλλεται από τη Hamas ή τη Hezbollah.

Ιαπωνία 2010: Στις 19 Σεπτεμβρίου του 2010 η Ιαπωνία υποψιαζότανε ότι μία κατανεμημένη επίθεση άρνησης εξυπηρέτησης ¨χτυπούσε¨ τις ιστοσελίδες του Υπουργείου Αμύνης και της Υπηρεσίας Εθνικής Αστυνομίας λόγω μιας διένεξης που είχε με τη Λαϊκή Δημοκρατία της Κίνας («ΛΔΚ»), όπως ανέφεραν τα μέσα. Η Ιαπωνική κυβέρνηση πήρε τα μέτρα της διατάζοντας τις κυβερνητικές οντότητες να λάβουν μέτρα αυτοάμυνας, όπως να κλείσουν τις ιστοσελίδες τους, για σύντομο χρονικό διάστημα. Οι υποψίες της Ιαπωνίας βασίζονται σε ένα περιστατικό που έγινε στις 7 Σεπτέμβρη 2010 όπου μιας Κινέζικης τράτας και δύο Ιαπωνικών οχημάτων της ακτοφυλακής κοντά σε μια αμφιλεγόμενη σειρά νησιών στην Ανατολική Θάλασσα της Κίνας συγκρούστηκαν. Η σύγκρουση αυτή δεν τελείωσε ειρηνικά καθώς η μεγαλύτερη ομάδα πειρατείας της Κίνας είχε προειδοποιήσει ότι θα επιτιθόταν σε Ιαπωνικές ιστοσελίδες ως διαμαρτυρία για το περιστατικό.

Νατάνζ 2010 : Το πρώτο χτύπημα που έκανε την αρχή για την εμφάνιση του Stuxnet ήταν τον Ιούνιο του 2010 οι Ιρανικές πυρηνικές εγκαταστάσεις που χτυπήθηκαν στο Νατάνζ. Μόλυνε πάνω από 60.000 υπολογιστές που οι περισσότεροι από αυτούς βρίσκονταν στο Ιράν, χωρίς να περιοριστεί μόνο εκεί. Από το χτύπημα αυτό επηρεάστηκαν επίσης και άλλες χώρες όπως η Ινδία, η Ινδονησία η Κίνα το Αζερμπαϊτζάν, η Φινλανδία και η Γερμανία. Ο ιός δεν έμεινε εκεί. Προχώρησε μέσα από το διαδίκτυο και σε άλλα συστήματα υπολογιστών χωρίς βέβαια να προκαλέσει τον ίδιο βαθμό ζημίας αφού η χρήση αντιδότων περιόρισε σημαντικά την εξάπλωση του μέχρι και τις 24 Ιουνίου του 2012.

Ιανουάριος 2011 : Η καναδική κυβέρνηση ανέφερε μια σημαντική κυβερνητική επίθεση εναντίον των οργανισμών της, συμπεριλαμβανομένης της Άμυνας Έρευνας και Ανάπτυξης του Καναδά, μιας ερευνητικής υπηρεσίας για το Υπουργείο Εθνικής Άμυνας του Καναδά.
Η επίθεση ανάγκασε το Υπουργείο Οικονομικών και το Συμβούλιο Δημοσίου, οι κυριότερες οικονομικές υπηρεσίες του Καναδά, να αποσυνδεθούν από το Διαδίκτυο.

Ιούλιος 2011: Σε μια ομιλία που αποκαλύπτει την κυβερνητική στρατηγική του Υπουργείου Άμυνας, ο Αναπληρωτής Γραμματέας της Άμυνας των ΗΠΑ ανέφερε ότι ένας εργολάβος υπεράσπισης παραβιάστηκε και κλέφθηκαν 24.000 αρχεία από το Υπουργείο Άμυνας.

Οκτώβριος 2012: Η ρωσική εταιρεία Kaspersky ανακάλυψε μια παγκόσμια επίθεση στον κυβερνοχώρο που ονομάστηκε "Κόκκινος Οκτώβριος", που λειτουργούσε τουλάχιστον από το 2007. Οι χάκερς συγκέντρωσαν πληροφορίες μέσω ευπάθειας στα προγράμματα Word και Excel της Microsoft. Οι πρωταρχικοί στόχοι της επίθεσης φαίνεται να είναι χώρες της Ανατολικής Ευρώπης, της πρώην ΕΣΣΔ και της Κεντρικής Ασίας, αν και η Δυτική Ευρώπη και η Βόρεια Αμερική ανέφεραν και τα θύματα. Ο ιός συνέλεξε πληροφορίες από κυβερνητικές πρεσβείες, ερευνητικές εταιρείες, στρατιωτικές εγκαταστάσεις, παροχές ενέργειας, πυρηνικές και άλλες κρίσιμες υποδομές.

Μάρτιος 2013: Τα χρηματοπιστωτικά ιδρύματα της Νότιας Κορέας καθώς και ο κορεάτικος ραδιοτηλεοπτικός φορέας YTN είχαν μολυνθεί από τα δίκτυά τους σε ένα περιστατικό το οποίο αναφέρθηκε ότι μοιάζει με προηγούμενες προσπάθειες στον κυβερνοχώρο της Βόρειας Κορέας.

2.9 Τύποι Κυβερνοεπιθέσεων

Οι διαφορετικοί τύποι επιθέσεων μπορούν να κατηγοριοποιηθούν ανάλογα με τον τρόπο που πλήττουν ένα σύστημα και με τη μεθοδολογία που ακολουθείται με τους πιο γνωστούς να είναι το λογισμικό τύπου malware, το phishing, η man-in-the-middle, η επίθεση άρνησης υπηρεσίας, η SQL injection, η zero-day exploit, η cross-site scripting και η credential reuse, που θα αναλυθούν στη συνέχεια.

2.9.1 Malware (Malicious Software)

Αυτός ο ιός χρησιμοποιείται για να περιγραφούν τα διάφορα είδη κακόβουλου λογισμικού όπως ιοί, worms, trojans, ransomware, spyware, adware, rootkits κτλ. Αυτού του είδους το λογισμικό έχει ως στόχο είτε να βλάψει το σύστημα του θύματος με την υποκλοπή ή καταστροφή ευαίσθητων δεδομένων, είτε την παρακολούθηση των ενεργειών του χρήστη, είτε ακόμα και την λήψη του ελέγχου του συστήματος. Οι μέθοδοι με τις οποίες μπορεί να προσβληθεί ένας υπολογιστής έχουν διάφορες μορφές, αλλά στο τέλος απαιτούν πάντα απ τον χρήστη να προβεί σε κάποια ενέργεια, όπως η εκτέλεση και εγκατάσταση λογισμικού. Αυτό μπορεί να γίνει με το κατέβασμα ενός "αθώου" συνημμένου αρχείου, καθώς και με την εκτέλεση κάποιου πρόσθετου που προτείνεται από μια μολυσμένη ιστοσελίδα. Όσον αφορά τα διαφορετικά είδη κακόβουλου λογισμικού, ακολουθεί παρακάτω μια σύντομη περιγραφή των κυριότερων μορφών αυτού.

Ιός(virus): Λογισμικό, το οποίο είναι κρυμμένο μέσα σε κάποιο άλλο, αβλαβές δημιουργώντας αντίγραφα του εαυτού του. Τα αντίγραφα αυτά μεταδίδονται, εξαπλώνονται και ενσωματώνονται σε άλλο λογισμικό, περνώντας δικτυακά από τον έναν υπολογιστή στον άλλον. Στόχος είναι η δυσλειτουργία των συστημάτων και η καταστροφή των δεδομένων.

Worm: Έχει παρόμοια λογική με τον ιό αφού κι αυτό δημιουργεί αντίγραφα του εαυτού του και έχει ως κύριο στόχο να πλήξει τα συστήματα και να καταστρέψει τα δεδομένα. Η διαφορά τους εντοπίζεται στο ότι είναι αυτόνομο και δεν απαιτείται η ύπαρξη άλλου λογισμικού. Η εξάπλωση γίνεται μέσω εκμετάλλευσης πιθανών ευπαθειών του συστήματος, οπότε ο χρήστης πέφτει στη παγίδα εκτέλεσης τους.

Trojan: Η μορφή του είναι τέτοια που πείθει τον χρήστη ότι είναι χρήσιμο προκειμένου αυτός να προχωρήσει στην εγκατάσταση του. Δεν έχει ως στόχο τη την εξάπλωση και την μόλυνση άλλων αρχείων, σαν τον ιό. Σκοπός του είναι η υποκλοπή και η διαγραφή αρχείων, καθώς και η διαγραφή ευπαθειών στα συστήματα.

Ransomware: Λογισμικό που κρυπτογραφεί τα δεδομένα του χρήστη, μην επιτρέποντας την πρόσβαση σε αυτά, και στη συνέχεια απαιτεί την καταβολή ενός χρηματικού αντιτίμου για την αποκρυπτογράφηση και ανάκτηση τους. Ο τρόπος με τον οποίο μεταδίδεται είναι είτε μέσω phishing emails, είτε μέσω ιστοσελίδων που περιέχουν κακόβουλο κώδικα.

Spyware: Συνήθως είναι κρυμμένο μέσα σε άλλο λογισμικό και ο χρήστης το εγκαθιστά δίχως να γίνεται αντιληπτό. Χρησιμοποιείται για τη συλλογή δεδομένων και την αποστολή τους σε κάποια άλλη δικτυακή οντότητα, χωρίς ο ίδιος να το γνωρίζει. Γνωστή μορφή του το

key logger, λογισμικό που παρακολουθεί την πληκτρολόγηση του χρήστη και μπορεί να επιτύχει την καταγραφή των δεδομένων, όπως είναι οι κωδικοί πρόσβασης

Adware: Λογισμικό που εγκαθίσταται χωρίς τη συγκατάθεση του χρήστη, έχοντας τη μορφή ενοχλητικών διαφημίσεων ή παραθύρων που δεν είναι δυνατόν να κλείσουν. Εμφανίζονται κατά τη διάρκεια της εγκατάστασης μιας εφαρμογής και μπορεί να έχουν τη μορφή αναδυόμενων παραθύρων, προβάλλοντας διαφημίσεις στο χρήστη.

Rootkit: Πακέτο λογισμικού, το οποίο λειτουργεί βοηθητικά κατά την προσβολή ενός συστήματος από malware. Έχει την ικανότητα να επιτρέπει στο κακόβουλο λογισμικό να παραμένει μη ανιχνεύσιμο σε ελέγχους, λόγω του ότι βρίσκεται πολύ κοντά στον πυρήνα του συστήματος. Στόχος του είναι η εγκατάσταση των απαραίτητων εργαλείων, τα οποία θα δώσουν τη δυνατότητα στον κακόβουλο χρήστη να αποκτήσει μελλοντικά απομακρυσμένη πρόσβαση στο σύστημα του θύματος του.

Backdoor: Αποτελεί τακτική που ακολουθείται στην ανάπτυξη συστημάτων λογισμικού και δίνει τη δυνατότητα απομακρυσμένης πρόσβασης σε αυτό, από τους δημιουργούς του, για την διενέργεια διαδικασιών επίλυσης προβλημάτων, αναβαθμίσεων και ελέγχων. Αυτές οι δίοδοι πρόσβασης μπορούν να μετατραπούν σε ευπάθειες και αποτελούν στόχο του κακόβουλου χρήστη, ο οποίος μπορεί να τις ανακαλύψει με τη χρήση worm ή trojan. Έτσι, με την ύπαρξη αυτών, παρακάμπτει τις διαδικασίες αυθεντικοποίησης του συστήματος και έχει πρόσβαση σ αυτό.

2.9.2 Phising

Πρόκειται για μια τακτική που εφαρμόζεται με τη χρήση emails, σύμφωνα με την οποία το μήνυμα περιέχει τα στοιχεία ενός αποστολέα που ο χρήστης θα εμπιστευόταν, όπως η τράπεζα ή ένας επαγγελματικός συνεργάτης. Το μήνυμα έχει τη μορφή που θα είχε ένα νόμιμο email και περιλαμβάνει κάποιο συνημμένο αρχείο ή σύνδεσμο. Έτσι επιτυγχάνεται η εγκατάσταση του κακόβουλου λογισμικού όταν ο χρήστης ανοίξει το αρχείο, είτε στην άλλη περίπτωση, ο σύνδεσμος οδηγεί σε μια πλαστή ιστοσελίδα (ίδια σε εμφάνιση πχ εκείνης της τράπεζας) όπου στόχος είναι η υποκλοπή των διαπιστευτηρίων του χρήστη ή των στοιχείων της πιστωτικής του κάρτας.

Βασική κατηγορία του Phising είναι το **Deceptive Phishing** το οποίο κάνει χρήση των emails, έχει γενικό χαρακτήρα και καλεί το θύμα του να προβεί σε επιβεβαίωση των διαπιστευτηρίων του, ακολουθώντας ένα σύνδεσμο που περιέχεται στο μήνυμα.

Spear Phishing: Πρόκειται για στοχευμένη υλοποίηση, η οποία απευθύνεται σε συγκεκριμένα άτομα μιας εταιρείας, κάνοντας χρήση του ονόματος, της θέσης, των στοιχείων επικοινωνίας και οποιασδήποτε άλλης πληροφορίας θα πείσει το θύμα για την αυθεντικότητα του μηνύματος. Συχνά είναι το πρώτο βήμα στη διαδικασία παράκαμψης της άμυνας ενός εταιρικού στόχου.

2.9.3 Man-in-the-middle (MITM)

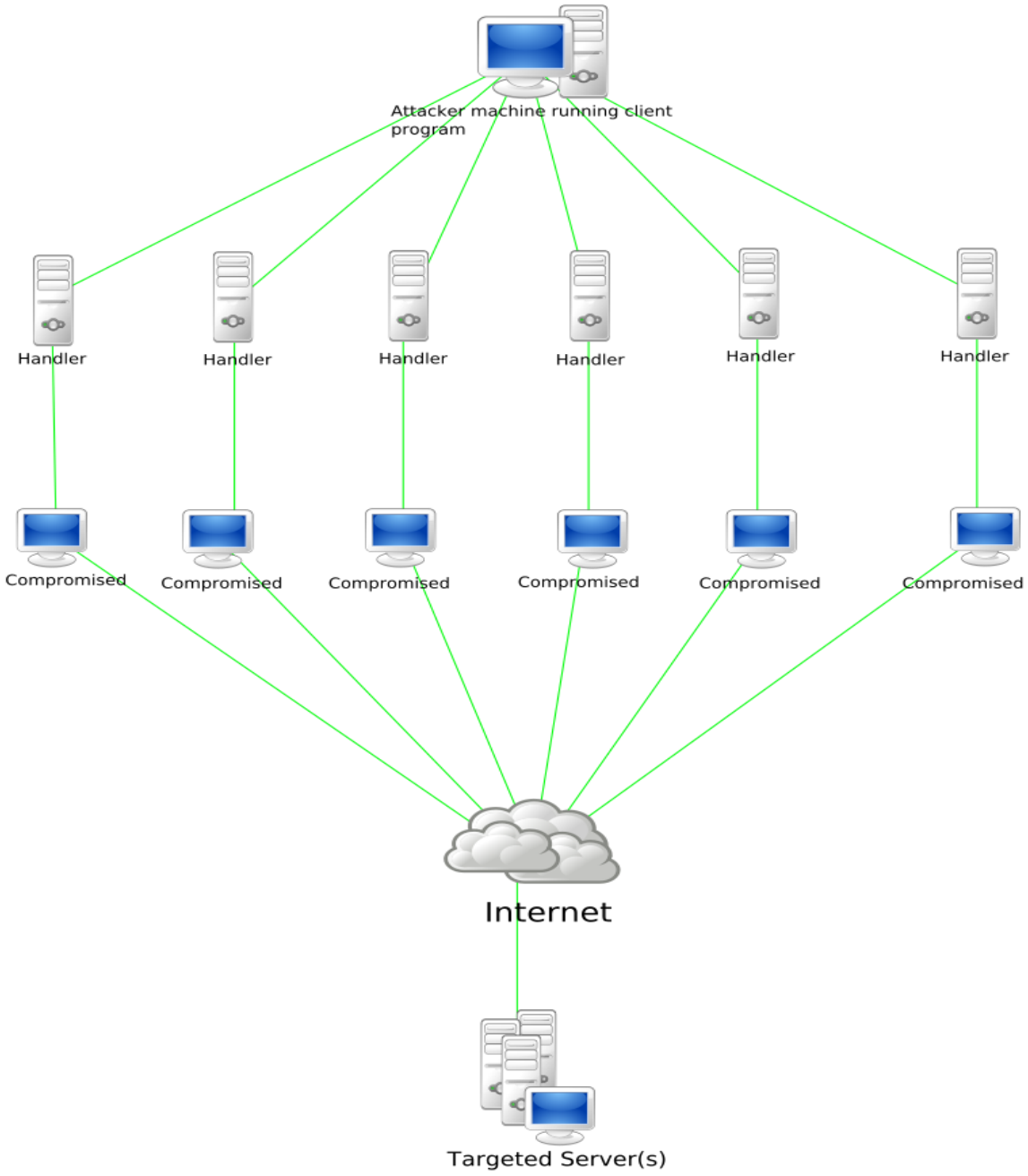
Ένας επιτιθέμενος κατορθώνει να διεισδύσει σε ένα σύστημα επικοινωνιών εφόσον υποδυθεί ότι πρόκειται για τερματικό σημείο της σύνδεσης. Αυτό μπορεί να επιτευχθεί πολύ εύκολα εάν ο επιτιθέμενος σε ένα μη κρυπτογραφημένο ασύρματο σημείο εισόδου. Ο επιτιθέμενος τότε μπορεί να ανακόψει την πληροφορία που στέλνεται από ένα ανυποψίαστο θύμα. Για παράδειγμα, το online banking, όπου ο εισβολέας μπορεί να κλέψει όλες τις πληροφορίες σχετικές με τη μεταφορά χρημάτων και τον λογαριασμό του θύματος.

2.9.4 Denial-of-Service Attacks (DoS)

Μία DoS επίθεση είναι μία ειδική μορφή κυβερνοεπίθεσης που επικεντρώνεται στη διακοπή της λειτουργίας του δικτύου. Αυτό επιτυγχάνεται όταν ένας εισβολέας στέλνει μεγάλο όγκο δεδομένων προς το δίκτυο- στόχο μέχρι να υπερφορτωθεί το δίκτυο.

Μέθοδοι εκτέλεσης

Τυπικά, μία DoS επίθεση διεξάγεται από έναν υπολογιστή ή από μία κεντρική τοποθεσία υπολογιστών. Μια δημοφιλή υποκατηγορία DoS επιθέσεων είναι η DDoS επίθεση. Μία DDoS επίθεση διαφέρει από μία DoS επίθεση στο ότι εμπεριέχονται πολλαπλοί υπολογιστές. Οι υπολογιστές δουλεύουν μαζί στέλνοντας φορτίο στο δίκτυο-στόχο. Το σχήμα απεικονίζει τη βασική δομή μιας DDoS επίθεσης.



Εικόνα 2.9.4

Επίθεση DDoS

2.9.5 SQL Injection

Πρόκειται για μια τεχνική έγχυσης κώδικα που έχει ως στόχο την επίθεση σε συστήματα που χρησιμοποιούν τη γλώσσα SQL. Τέτοια συστήματα είναι οι βάσεις δεδομένων, καθώς και online εφαρμογές ή ιστοσελίδες που είναι συνδεδεμένες με μια βάση

δεδομένων. Αυτός ο κώδικας εισάγεται συνήθως σε σημεία της εφαρμογής ή της σελίδας όπου ζητούνται τα διαπιστευτήρια του χρήστη. Στόχος της επίθεσης είναι να αποστείλει ερωτήματα τύπου SQL στη βάση δεδομένων, με τα οποία θα την αναγκάσει να λειτουργήσει με τρόπο που δεν προέβλεψε ο κατασκευαστής της. Εφόσον το σύστημα δε διαθέτει μηχανισμούς ασφαλείας απέναντι σε τέτοιου είδους επιθέσεις, ο κακόβουλος χρήστης έχει τη δυνατότητα να το παραβιάσει και να εκμεταλλευτεί τα περιεχόμενα προς όφελός του.

2.9.6 Zero-day Exploit

Όταν μια κυβερνοεπίθεση πραγματοποιείται την ίδια μέρα που γνωστοποιείται η ευπάθεια ενός λογισμικού, τότε αυτή έχει την ονομασία zero-day exploit. Αυτό, διότι ο επιτιθέμενος εκμεταλλεύεται τη συγκεκριμένη ευπάθεια πριν την έκδοση της απαραίτητης ενημέρωσης που θα σφαλίσει το λογισμικό που θα το προστατεύσει. Συνήθως όταν ένας χρήστης ανακαλύψει ένα κενό ασφαλείας, το αναφέρει στην κατασκευάστρια εταιρεία προκειμένου εκείνη να το διορθώσει. Επίσης, υπάρχει η πιθανότητα να το αναφέρει σε κοινότητες χρηστών, ούτως ώστε να είναι και εκείνοι ενήμεροι για την ύπαρξη του. Ο κακόβουλος χρήστης προσπαθεί να ενημερωθεί εγκαίρως παρακολουθώντας αυτού του είδους τις ενημερώσεις, με στόχο να καταφέρει να ενεργήσει πριν από την εταιρεία και εκμεταλλευόμενος το κενό ασφαλείας, να πλήξει συστήματα των χρηστών.

2.9.7 Cross-site Scripting

Το Cross-site Scripting είναι τύπος επίθεσης που εκμεταλλεύεται τα κενά ασφαλείας σε ιστοσελίδες και διαδικτυακές εφαρμογές. Αυτά επιτρέπουν την ενσωμάτωση κακόβουλου κώδικα στο δυναμικό περιεχόμενο μιας σελίδας, ο οποίος στη συνέχεια θα εκτελεστεί στην πλευρά του χρήστη μέσω του περιηγητή του. Συνήθως εφαρμόζεται σε περιπτώσεις που αυτός καταχωρεί δεδομένα όπως οι μηχανές αναζήτησης, οι φόρμες εισόδου, όπου πληκτρολογεί τα διαπιστευτήρια του, ή οι πίνακες μηνυμάτων και σχολίων που υπάρχουν σε forums.

2.9.8 Credential reuse ή stuffing

Ο συνεχώς αυξανόμενος αριθμός εφαρμογών λογισμικού έχει ως αποτέλεσμα να είναι δύσκολο για τον μέσο χρήστη να απομνημονεύσει και να χρησιμοποιήσει αποτελεσματικά ένα πλήθος διαπιστευτηρίων που αντιστοιχούν σ αυτές. Αυτός είναι και ο κύριος λόγος που μεγάλος αριθμός των χρηστών επαναχρησιμοποιεί τα διαπιστευτήριά του σε διαφορετικές εφαρμογές, τακτική που αποτελεί στόχο των κακόβουλων χρηστών. Καταφέρνοντας να αποκτήσουν πρόσβαση στα διαπιστευτήρια μιας εφαρμογής, ιστοσελίδας ή υπηρεσίας, υπάρχουν αυξημένες πιθανότητες να αποκτήσουν πρόσβαση και σε άλλες, των οποίων οι χρήστες-πελάτες είναι κοινοί. Η πιο συνηθισμένη μέθοδος υποκλοπής των στοιχείων είναι μέσω εφαρμογών που έχουν δημιουργηθεί γι αυτό το σκοπό, υποσχόμενες κάποιες δελεαστικές και ¨αθώες¨ λειτουργίες ώστε να παρασύρουν τους χρήστες. Δεν είναι λίγα τα περιστατικά που τέτοιου είδους δεδομένα πωλούνται στη διαδικτυακή μαύρη αγορά και αφορούν γνωστές εφαρμογές όπως το Facebook.

ΚΕΦΑΛΑΙΟ 3

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ & ΤΕΧΝΙΚΕΣ/ ΟΡΓΑΝΩΤΙΚΕΣ ΛΥΣΕΙΣ

3.1 Τεχνικές Λύσεις για την αποφυγή των Κυβερνοεπιθέσεων

Πέρα από τις μακροπρόθεσμες και βραχυπρόθεσμες προσεγγίσεις του Scott Shackelford υπάρχουν και μερικές τεχνικές λύσεις για την αποφυγή των κυβερνοεπιθέσεων. Μερικές από αυτές είναι:

- Hash-Based IP Trace back (Βασισμένη στην ανίχνευση της IP προς τα πίσω) – Οι δρομολογητές αποθηκεύουν τις τιμές κατακερματισμού των πακέτων δικτύου. Η απόδοση γίνεται με την ανίχνευση προς τα πίσω των τιμών κατακερματισμού μέσα από τους δρομολογητές δικτύων.
- Ingress Filtering (Φιλτράρισμα εισροής) – Όλα τα μηνύματα που εισέρχονται σε ένα δίκτυο απαιτείται να έχουν μια διεύθυνση πηγής σε μια έγκυρη περιοχή. Αυτό περιορίζει την περιοχή των πιθανών πηγών των επιθέσεων.
- ICMP Return to Sender (Πρωτόκολλο Ελέγχου Μηνυμάτων Διαδικτύου Επιστροφή στον Αποστολέα) – Όλα τα πακέτα που προορίζονται για το θύμα απορρίπτονται και επιστρέφονται στους αποστολείς τους.
- Overlay Network for IP Trace back (Επικαλυπτικό Δίκτυο για Ανίχνευση πίσω της IP) – Ένα επικαλυπτικό δίκτυο συνδέει όλους τους ISP ακραίους δρομολογητές με έναν κεντρικό δρομολογητή παρακολούθησης, οι προσεγγίσεις hop-by-hop χρησιμοποιούνται για να βρεθεί η πηγή.
- Trace Packet Generation (Ανίχνευση γενιάς πακέτου) (π.χ. iTrace) – Ένας δρομολογητής στέλνει ένα ICMP μήνυμα ανίχνευσης πίσω περιοδικά (π.χ. 1 ανά 20000 πακέτα) στην ίδια διεύθυνση προορισμού όπως το πακέτο δείγμα. Ο προορισμός (ή ο οριζόμενος επόπτης) συλλέγει και συσχετίζει τις πληροφορίες παρακολούθησης.

- Probabilistic Packet Marking (Πιθανολογική Σήμανση Πακέτου) – Ένας δρομολογητής προσδιορίζει τυχαία αν θα ενσωματώσει δεδομένα διαδρομής μηνύματος σε ένα μήνυμα. Αυτά τα δεδομένα διαδρομής χρησιμοποιούνται για τον προσδιορισμό διαδρομών.
- Hack back – Σε έναν ξενιστή ενσωματώνεται η υποβολή ερωτήσεων λειτουργικότητας χωρίς την άδεια του ιδιοκτήτη. Εάν ένας επιτιθέμενος ελέγχει τον ξενιστή, αυτό δεν θα τον προειδοποιήσει, οπότε οι πληροφορίες είναι πιο αξιόπιστες.
- Honey pots (Δοχεία μελιού) – Συστήματα δολώματα συλλαμβάνουν πληροφορίες για τους επιτιθέμενους που μπορούν να χρησιμοποιηθούν για την απόδοση.
- Υδατογράφησης – Τα αρχεία μαρκάρονται όπως ανήκουν στους δικαιούχους ιδιοκτήτες τους.

Οι τεχνικές αυτές, θα πρέπει να ασφαλίζουν την ακεραιότητα τους. Το λογισμικό που χρησιμοποιείται για τον έλεγχο ταυτότητας και τα στοιχεία που χρησιμοποιούνται για την απόδοση πρέπει να προστατεύονται.

3.2 Ασφάλεια Δικτύων

Για την προστασία των δικτύων από κυβερνοεπιθέσεις σημαντικό ρόλο έχει η ενίσχυση των τεχνικών μέτρων ασφάλειας και πολιτικών ασφάλειας. Η καλύτερη άμυνα των κρίσιμων υποδομών πληροφοριών για την προστασία των δεδομένων είναι μία στρατηγική τοποθέτηση των συστημάτων πληροφοριών και του προσωπικού ασφαλείας. Για να βγάλουν εις πέρας αυτό το έργο οι διαχειριστές και το προσωπικό ασφαλείας θα πρέπει:

- Να γνωρίζουν πώς δουλεύουν τα συστήματά τους, με σκοπό να μπορούν να προφυλάξουν τα τυχόν εκμεταλλεύσιμα σημεία τους από αυτούς που θέλουν να επιτεθούν στο σύστημα.
- Να διεξάγουν τακτικές δοκιμές διείσδυσης και ελέγχου της τεχνολογίας πληροφοριών ώστε να εξετάζουν τις τρωτότητες των συστημάτων και να εξασφαλίζουν ορθή αποτροπή.
- Να γνωρίζουν τις ικανότητες πιθανόν επιτιθέμενων και τις τελευταίες τεχνολογίες, για καλύτερη ασφάλεια από κακόβουλα λογισμικά και τεχνικές DDOS των χάκερς.

Μερικά μέτρα προστασίας για την εξάλειψη των απειλών στο διαδίκτυο μπορούμε να πούμε ότι είναι:

- Antivirus και Antispyware: Προληπτική προστασία ενάντια σε όλες τις online και offline απειλές.
- Σάρωση βασισμένη στο Cloud: Διαδικασία σάρωσης, η οποία χρησιμοποιεί την online βάση δεδομένων για να διακρίνει τα ασφαλή αρχεία.
- Anti-Phishing: Προστασία από απόπειρες ψεύτικων websites να υποκλέψουν τα ευαίσθητα δεδομένα, όπως usernames, κωδικοί ή πληροφορίες τραπεζικών συναλλαγών και στοιχεία πιστωτικών καρτών.
- Σάρωση από Download Αρχεία: Έλεγχος των μεγάλων αρχείων τη στιγμή που γίνονται download και ελαχιστοποίηση του χρόνου σάρωσης.
- Έλεγχος Αφαιρούμενων Μέσων: Μπλοκάρει τα άγνωστα CDs, DVDs, USBs και άλλα μέσα, εμποδίζοντας έτσι τη μη εξουσιοδοτημένη αντιγραφή των προσωπικών δεδομένων σε εξωτερικές συσκευές αποθήκευσης.
- Host-based Intrusion Prevention System (HIPS): Προσαρμόζει την συμπεριφορά του συστήματος με μεγαλύτερη λεπτομέρεια.

ΚΕΦΑΛΑΙΟ 4

ΠΛΑΙΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ

4.1 Διαχείριση των Κινδύνων του Κυβερνοχώρου

Στην έκθεση της Deloitte (2016), σχετικά με την ορθή εκτίμηση και την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου, παρουσιάζονται δέκα καίριες ερωτήσεις, τις οποίες καλούνται να απαντήσουν οι διοικούντες των οργανισμών προκειμένου να αξιολογήσουν τον βαθμό της ετοιμότητας της επιχείρησής τους (αλλά και των ιδίων, καθώς και των υπαλλήλων) απέναντι στους κινδύνους του κυβερνοχώρου. Κεντρικός στόχος είναι να εκτιμηθεί το κατά πόσον η επιχείρηση: α) είναι ασφαλής, β) βρίσκεται σε συνεχή επαγρύπνηση και γ) διαθέτει ανθεκτικές δομές έναντι αυτής της μορφής των κινδύνων.

1. Επιδεικνύεται η δέουσα επιμέλεια ως προς την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου;
2. Η ηγεσία της επιχείρησης διαθέτει τις απαιτούμενες γνώσεις και την αντίστοιχη διορατικότητα προκειμένου να διαχειριστεί σωστά αυτούς τους κινδύνους;
3. Έχει δημιουργηθεί ένα κατάλληλο πλαίσιο προσδιορισμού των κινδύνων του κυβερνοχώρου, καθώς και ταξινόμησής τους αναλόγως του αντικτύπου τους για τον οργανισμό, που να περιλαμβάνει την όρεξη για ανάληψη κινδύνου, αλλά και τα κατώτατα όρια αναφοράς;
4. Επικεντρωνόμαστε και επενδύουμε στα σωστά πράγματα; Και αν ναι, πώς αξιολογούμε και μετράμε τα αποτελέσματα των αποφάσεών μας;
5. Ευθυγραμμίζεται το εταιρικό πρόγραμμα διαχείρισης των κινδύνων του κυβερνοχώρου, καθώς και οι επιμέρους δυνατότητές μας με τα πρότυπα του κλάδου, αλλά και τις αντίστοιχες επιχειρήσεις του ίδιου κλάδου;
6. Η κουλτούρα του οργανισμού είναι προσανατολισμένη προς την αναγνώριση και την ευαισθητοποίηση έναντι των κινδύνων του κυβερνοχώρου;
7. Τι έχουμε πράξει έτσι ώστε να προστατέψουμε τον οργανισμό από τους κινδύνους του κυβερνοχώρου;

8. Μπορούμε να μετριάσουμε σύντομα τις ζημίες και να κινητοποιήσουμε άμεσα πόρους απόκρισης όταν συμβαίνει μια επίθεση κατά των πληροφοριακών μας συστημάτων;
9. Πώς αξιολογούμε την αποτελεσματικότητα του προγράμματος εταιρικής διαχείρισης των κινδύνων του κυβερνοχώρου;
10. Είμαστε ένας ισχυρός και ασφαλής κρίκος των εξαιρετικά συνδεδεμένων οικοσυστημάτων στα οποία λειτουργούμε;

Επισκοπώντας βιβλιογραφικά το θέμα της διαχείρισης των κινδύνων του κυβερνοχώρου, οι Eling και Schnell (2016), αναφέρουν ότι μια σημαντική πτυχή του ζητήματος αυτού είναι ότι ο κυβερνοχώρος δεν αποτελεί αποκλειστική ευθύνη του τμήματος πληροφορικής της επιχείρησης, αλλά απαιτεί έναν γενικό διάλογο μεταξύ των διαφόρων τμημάτων, αλλά κυρίως την άμεση ευαισθητοποίηση και εμπλοκή της ανώτατης διοίκησης και του διοικητικού συμβουλίου. Κατόπιν, συγκεντρώνουν την διαδικασία οργάνωσης και διαχείρισης των κινδύνων του κυβερνοχώρου, μέσα από τα εξής βήματα:

- ✓ Το πρώτο βήμα στην κλασική διαδικασία διαχείρισης των κινδύνων του κυβερνοχώρου είναι ο καθορισμός της αρχικής κατάστασης και των στόχων που η επιχείρηση επιθυμεί να επιτύχει μέσα από την αποτελεσματική διαχείριση των κινδύνων αυτών.
- ✓ Έπειτα, για την εκτίμηση του κινδύνου πρέπει να προσδιορίζονται τα σχετικά περιουσιακά στοιχεία που απειλούνται (άμεσα ή έμμεσα), καθώς και οι αντίστοιχες επιχειρηματικές διαδικασίες που σχετίζονται (ή εξαρτώνται) με αυτά. Στη συνέχεια, πρέπει να προσδιοριστούν οι πιθανές απειλές και οι πηγές τους.
- ✓ Το επόμενο βήμα εμπεριέχει τον προσδιορισμό του εκτιμώμενου κόστους και των συνεπειών που δύναται να προκληθούν στον οργανισμό από την ανεπιτυχή αντιμετώπιση μιας επίθεσης στον κυβερνοχώρου του.
- ✓ Το τέταρτο βήμα, είναι αυτό της συνεχούς παρακολούθησης των κινδύνων του κυβερνοχώρου. Καθώς ο κυβερνοχώρος είναι εξαιρετικά δυναμικός και εξελίσσεται συνεχώς η αδιάκοπη παρακολούθηση των κινδύνων που εγκυμονεί είναι ένα ακόμα κλειδί στην αποτελεσματική διαχείρισή τους. Δεδομένου ότι οι στρατηγικές επίθεσης αλλάζουν διαρκώς, η διαχείριση του κινδύνου πρέπει να βελτιώνεται συνεχώς.

- ✓ Το τελευταίο βήμα είναι αυτό της εφαρμογής των διαφόρων μεθόδων διαχείρισης των κινδύνων του κυβερνοχώρου. Σύμφωνα με τους συγγραφείς, εντοπίζονται τέσσερις βασικές μέθοδοι, οι οποίοι είναι η αποφυγή του ρίσκου, ο μετριασμός των κινδύνων, η μεταφορά του ρίσκου (ή μέρους αυτού) και η διατήρηση/ανάληψη των κινδύνων και του ρίσκου που αυτοί συνεπάγονται.

Σχολιάζοντας περαιτέρω την τελευταία παράγραφο, οι συγγραφείς επεξηγούν ότι η αποφυγή/αποτροπή των κινδύνων του κυβερνοχώρου συνεπάγεται την μη λειτουργία εταιρικών πληροφοριακών συστημάτων, πράγμα αρκετά δύσκολο, ειδικά βάσει των απαιτήσεων της σημερινής εποχής. Από την άλλη πλευρά, η ανάληψη των κινδύνων απαιτεί την πολύ προσεκτική εκτίμηση του ρίσκου που αυτοί εγκυμονούν, καθώς και την ενδελεχή προετοιμασία για το ενδεχόμενο του να βρεθεί η επιχείρηση άμεσα αντιμέτωπη με κρούσματα επιθέσεων κατά των πληροφοριακών της συστημάτων. Όσον αφορά την μεταφορά του ρίσκου, αναγνωρίζουν τα γενναία βήματα που έχουν πραγματοποιηθεί, ειδικά τη τελευταία δεκαετία, προς την άνθιση της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου. Τέλος, σχετικά με το θέμα του μετριασμού των κινδύνων, επισημαίνουν ότι πρόκειται για τον πιο δημοφιλή τρόπο διαχείρισής τους, καθώς μπορεί να στοχεύσει παράλληλα στον μετριασμό τόσο της πιθανότητας εμφάνισης κρουσμάτων επιθέσεων έναντι των εταιρικών πληροφοριακών συστημάτων (π.χ. μέσα από την εκτεταμένη χρήση προγραμμάτων προστασίας του εταιρικού κυβερνοχώρου), όσο και των πιθανών απωλειών που μπορεί να προκύψουν από τα κρούσματα αυτά.

Επί του θέματος του μετριασμού/περιορισμού της πιθανότητας εμφάνισης των κινδύνων του κυβερνοχώρου, η Allianz (2015) αναφέρει στην σχετική της έκθεση πέντε βασικά βήματα για την αποτελεσματικότερη οργάνωση προς αυτή την κατεύθυνση.

1. Προσδιορισμός των βασικών στοιχείων του ενεργητικού που βρίσκονται σε κίνδυνο, καθώς και των οργανικών αδυναμιών όπως ο ανθρώπινος παράγοντας ή η υπερβολική εξάρτηση από τρίτα (συνδεδεμένα) μέρη.
2. Δημιουργία (ή ενδυνάμωση) μιας εταιρικής κουλτούρας που σέβεται και αναγνωρίζει την σημαντικότητα των κινδύνων του κυβερνοχώρου. Αυτό θα πρέπει να συνοδεύεται και από την επαρκή εκπαίδευση των εργαζομένων και των ενδιαφερομένων μερών της επιχείρησης.

3. Εφαρμογή ενός σχεδίου διαχείρισης κρίσεων και αντιμετώπισης παραβιάσεων, το οποίο θα πρέπει να δοκιμαστεί και να αξιολογηθεί προκειμένου να εντοπιστούν τυχόν αστοχίες ή/και παραλείψεις.
4. Ενδελεχής εξέταση του πώς οι εταιρικές δραστηριότητες που σχετίζονται με τα τρίτα (συνεργαζόμενα) μέρη, ενδέχεται να επηρεαστούν από κάποια πιθανή επίθεση στον κυβερνοχώρο. Επιπροσθέτως, θα πρέπει να προσδιοριστούν και τα περισσότερα πιθανά σενάρια παραβιάσεων που δύναται να κληθεί να αντιμετωπίσει η επιχείρηση.
5. Θα πρέπει να ληφθούν αποφάσεις σχετικά με τους κινδύνους που η επιχείρηση θα πρέπει να αποφύγει, να αναλάβει, να μετριάσει ή και να μεταφέρει.

Τέλος, παραθέτουμε τις προτάσεις των Siegel et al. (2002), οι οποίες αν και προέρχονται από μια χρονικά «παλαιότερη» δημοσίευση (τουλάχιστον για το πολύ δυναμικό περιβάλλον των σύγχρονων πληροφοριακών συστημάτων), εντούτοις περιγράφουν πολύ περιεκτικά τα αναγκαία βήματα για την αποτελεσματική διαχείριση των κινδύνων του κυβερνοχώρου. Σύμφωνα με τα όσα αναφέρουν, η διαχείριση των κινδύνων του κυβερνοχώρου απεικονίζεται μέσα από μια κυκλική διαδικασία, η οποία περιλαμβάνει πέντε βασικά στάδια. Αυτά έχουν ως εξής:

Εκτίμηση (Assessment)

- Αξιολόγηση των ασφαλιστικών δικλίδων του οργανισμού, διενέργεια δοκιμαστικών προσομοιώσεων αντοχών και συνεντεύξεων με το προσωπικό που εμπλέκεται πιο άμεσα με την διαχείριση και την λειτουργία των εταιρικών πληροφοριακών συστημάτων.
- Χρησιμοποίηση τυποποιημένων προτύπων και μεθοδολογιών (όπως για παράδειγμα τα σχετικά πρότυπα ISO) και διενέργεια αξιολόγησης επ' αυτών.

Περιορισμός (Mitigation)

- Δημιουργία και εφαρμογή πολιτικών και διαδικασιών που διασφαλίζουν υψηλά επίπεδα ασφάλειας εντός του οργανισμού.
- Εφαρμογή μηχανισμών μετριασμού και μεταφοράς του χρηματοοικονομικού κινδύνου.
- Συνεχόμενος έλεγχος της διατήρησης του επιθυμητού επιπέδου ασφαλείας.

Ασφάλιση (Insurance)

- Επιλογή του βέλτιστου ασφαλιστικού φορέα με βάση την τεχνογνωσία, την οικονομική ισχύ και την παγκόσμια εμβέλειά του.
- Επιλογή της σωστής πολιτικής ασφάλισης, συμπεριλαμβανομένης της άμεσης κάλυψης της επιχείρησης αλλά και των πλησιέστερων ενδιαφερομένων μερών.
- Η διενέργεια ασφάλισης έναντι των κινδύνων του κυβερνοχώρου θα πρέπει να θεωρείται ως μια λύση μετατόπισης του κινδύνου και θα πρέπει να προκύπτει μέσα από μια λεπτομερή και τεκμηριωμένη αξιολόγηση των εταιρικών κινδύνων.
- Συνεργασία με τον ασφαλιστικό πάροχο για τον έγκυρο και τεκμηριωμένο προσδιορισμό πιθανών απωλειών, καθώς και των επιχειρηματικών επιπτώσεων που μπορεί να συνεπάγεται μια παραβίαση του εταιρικού κυβερνοχώρου.

Ανίχνευση (Detection)

- Παρακολούθηση των περιουσιακών στοιχείων για την ανακάλυψη τυχόν ασυνήθιστων δραστηριοτήτων.
- Εφαρμογή ενός συστήματος 24ωρης παρακολούθησης που θα περιλαμβάνει ανίχνευση εισβολών για τον έγκαιρο εντοπισμό και αποτροπή οποιασδήποτε πιθανής εισβολής.
- Ανάλυση των αρχείων καταγραφής για τον προσδιορισμό τυχόν παρελθόντων συμβάντων που δεν εντοπίστηκαν την στιγμή που έπρεπε.

Αποκατάσταση (Remediation)

- Κατανόηση των οργανικών προβλημάτων και των αναγκών για βελτίωση των πιο ευπαθών και τρωτών σημείων του πληροφοριακού συστήματος.
- Προσδιορισμός των πιο ευάλωτων περιοχών που χρήζουν άμεσης προσοχής.
- Διενέργεια όλων των απαραίτητων βημάτων και διαδικασιών για την αντιμετώπιση και θωράκιση των ευπαθών αυτών σημείων.
- Ανάκτηση χαμένων δεδομένων από τα συστήματα δημιουργίας αντιγράφων ασφαλείας.
- Εξασφάλιση της συνεχιζόμενης δραστηριότητας της επιχείρησης μέχρι την αποκατάσταση των όποιων τυχόν ζημιών έχουν σημειωθεί από κάποιο περιστατικό παραβίασης του κυβερνοχώρου.

4.2 ISO 31000:2009 και Αρχές του COBIT 5GEIT

Ο Διεθνής Οργανισμός Τυποποίησης (ISO) αποτελεί σημείο αναφοράς, δεδομένου ότι τα πρότυπά του προτείνονται από πολλούς μεγάλους φορείς και εφαρμόζονται από σημαντικό πλήθος επιχειρήσεων ανά τον κόσμο. Στο πλαίσιο αυτό, ο οργανισμός διαχείρισης κινδύνων (RIMS), προτρέπει την εφαρμογή του Διεθνούς Προτύπου Τυποποίησης 31000:2009 (το οποίο και αναθεωρήθηκε πρόσφατα το 2018), ως ένα ισχυρό και αποτελεσματικό εργαλείο για την αντιμετώπιση και διαχείριση των κινδύνων του κυβερνοχώρου. Για τις ανάγκες της παρουσίασης του προτύπου, ο Antonucci (2017), επικεντρώνεται στις πέντε βασικές αρχές του «COBIT 5 GEIT Principles», τις οποίες και συσχετίζει με τις βασικές θέσεις του ISO 31000:2009. Η αποτελεσματική εταιρική διακυβέρνηση και η διαχείριση των πληροφοριών και της σχετικής τεχνολογίας (GEIT) αποτελεί πρωτίστως ευθύνη του διοικητικού συμβουλίου. Το COBIT 5 είναι ένα διεθνώς αποδεκτό επιχειρηματικό πλαίσιο GEIT από την ISACA, το οποίο αναπτύχθηκε από και για τους επαγγελματίες και περιλαμβάνει πληροφορίες σχετικά με την πληροφοριακή τεχνολογία και τη βιβλιογραφία περί της αποτελεσματικότερης διοίκησης. Σύμφωνα με τα όσα αναφέρει ο συγγραφέας, μπορούμε να εξάγουμε τον κάτωθι συσχετισμό μεταξύ των κατευθυντήριων γραμμών του ISO 31000:2009 και των θέσεων του COBIT 5 GEIT, ο οποίος και παρουσιάζεται στον ακόλουθο πίνακα. Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι το Πρότυπο ISO 31000:2009 δεν αφορά συγκεκριμένα την διαχείριση των κινδύνων του κυβερνοχώρου, αλλά επισκοπεί και προτείνει ένα γενικότερο πλαίσιο διαδικασιών διαχείρισης των εταιρικών κινδύνων.

Σκοπός του συγγραφέα είναι να προσπαθήσει να συσχετίσει ορισμένα κομμάτια του πλαισίου αυτού, με τις αρχές του COBIT 5, προκειμένου να παρουσιάσει μια ολοκληρωμένη πρόταση περί της αποτελεσματικής διαχείρισης των κινδύνων του κυβερνοχώρου.

Πίνακας 1

ISO 31000:2009 RISK MANAGEMENT PRINCIPLES	COBIT 5 GEIT PRINCIPLES				
	1)Ικανοποίηση των αναγκών των ενδιαφερόμενων μερών	**2)Συνολική κάλυψη του οργανισμού**	**3)Εφαρμογή ενός ενιαίου πλαισίου**	**4)Εφαρμογή μιας ολιστικής προσέγγισης**	**5)Διαχωρισμός διακυβέρνησης από το μάνατζμεντ**
	Η διαχείριση των κινδύνων πρέπει να είναι διαφανής και περιεκτική.	Η διαχείριση κινδύνων δημιουργεί και προστατεύει την αξία.	Η διαχείριση κινδύνων είναι συστηματική, δομημένη και έγκαιρη.	Η διαχείριση κινδύνων αποτελεί αναπόσπαστο μέρος των διαδικασιών της οργάνωσης.	Η διαχείριση των κινδύνων διευκολύνει τη συνεχή βελτίωση του οργανισμού.
	Η διαχείριση των κινδύνων είναι δυναμική, αδιάλειπτη και ανταποκρίνεται στην αλλαγή.	Η διαχείριση κινδύνων είναι προσαρμοσμένη στις ανάγκες του οργανισμού.		Η διαχείριση του κινδύνου λαμβάνει υπόψη τους ανθρώπινους και πολιτισμικούς παράγοντες.	
		Η διαχείριση κινδύνων αντιμετωπίζει ρητά την αβεβαιότητα.		Η διαχείριση κινδύνων αποτελεί μέρος της διαδικασίας λήψης αποφάσεων.	
				Η διαχείριση των κινδύνων βασίζεται στις καλύτερες διαθέσιμες πληροφορίες.	

1) Ικανοποίηση των αναγκών των Ενδιαφερομένων Μερών

Η πρώτη αρχή του COBIT 5, επικαλείται την ανάγκη εναρμόνισης των στόχων και των προτεραιοτήτων των μεμονωμένων ατόμων και των τμημάτων του οργανισμού, με τις ανάγκες της επιχείρησης και των ενδιαφερομένων μερών. Επιπροσθέτως, η αρχή αναγνωρίζει ότι οι ανάγκες των ενδιαφερομένων μερών και οι επιχειρησιακοί στόχοι δύναται να αλλάζουν με την πάροδο του χρόνου. Στο πλαίσιο αυτό, το IS0 31000:2009 αναγνωρίζει δύο βασικές συνδρομές της εταιρικής διαχείρισης των κινδύνων του κυβερνοχώρου την διαχείριση των κινδύνων να είναι διαφανής, περιεκτική, δυναμική, αδιάλειπτη και να ανταποκρίνεται στην αλλαγή.

2) Συνολική κάλυψη του οργανισμού

Η δεύτερη αρχή του COBIT 5 αναγνωρίζει ότι η διαχείριση της πληροφοριακής τεχνολογίας ως περιουσιακού στοιχείου της επιχείρησης αποτελεί ουσιαστικό στοιχείο της δημιουργίας επιχειρηματικής αξίας που καλύπτει όλες τις λειτουργίες και τις διαδικασίες εντός της οργάνωσης για να της επιτρέψει να επιτύχει αποτελεσματικότερα το στόχο της ικανοποίησης των αναγκών των ενδιαφερομένων μερών. Η λογοδοσία για τη διαχείριση των στοιχείων της πληροφοριακής τεχνολογίας ανήκει στα ανώτερα διαχειριστικά στελέχη του οργανισμού και όχι στους υπαλλήλους και τους υπευθύνους λειτουργίας των συστημάτων αυτών.

3) Εφαρμογή ενός ενιαίου πλαισίου

Βάσει της τρίτης αρχής του COBIT 5, προβλέπεται η χρήση ενός γενικού πλαισίου που ενσωματώνει τα σχετικά πρότυπα και τις ρυθμιστικές διαδικασίες που σχετίζονται με το γενικότερο πρόγραμμα διαχείρισης των εταιρικών κινδύνων, έτσι ώστε να εφαρμόζεται ένα συνεκτικό και ολοκληρωμένο πρόγραμμα με αποτελεσματικό τρόπο για την αντιμετώπιση των κινδύνων του κυβερνοχώρου.

4) Εφαρμογή μιας ολιστικής προσέγγισης

Η τέταρτη αρχή του COBIT 5 υπογραμμίζει ότι η αποτελεσματική και αποδοτική εφαρμογή της διακυβέρνησης απαιτεί μια ολιστική προσέγγιση που λαμβάνει υπόψη διάφορες αλληλεπιδρούσες συνιστώσες ή μηχανισμούς. Τέσσερις από αυτές - διαδικασίες,

κουλτούρα, πληροφορίες και άνθρωποι, δεξιότητες και ικανότητες - σχετίζονται άμεσα με τέσσερις αρχές του ISO31000.

5) Διαχωρισμός διακυβέρνησης από το μάνατζμεντ

Η πέμπτη και τελευταία αρχή του COBIT 5 προχωράει στη διάκριση μεταξύ διακυβέρνησης (governance) και διαχείρισης (management). Η αρχή διαχωρίζει τις δραστηριότητες εταιρικής διακυβέρνησης όπως η αξιολόγηση, η καθοδήγηση και η παρακολούθηση (κυρίως των επιχειρησιακών αναγκών και στο σύνολο του οργανισμού) από τις δραστηριότητες διαχείρισης, όπως ο σχεδιασμός, η υλοποίηση, και η παρακολούθηση των διαδικασιών. Η αρχή αυτή προβλέπει ένα επαναλαμβανόμενο σύστημα κλειστού βρόχου στο οποίο παρέχεται η απαιτούμενη ανατροφοδότηση από τα διαχειριστικά στελέχη για να εξασφαλιστεί η εναρμόνιση με την κατεύθυνση που έθεσαν τα διοικητικά όργανα και κατά συνέπεια, να επιτευχθούν οι επιχειρηματικοί στόχοι.

ΚΕΦΑΛΑΙΟ 5

(3) CASE STUDY ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΕ ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

Σε αυτό το κεφάλαιο θα μελετήσουμε 3 περιπτώσεις σοβαρών κυβερνοεπιθέσεων που πραγματοποιήθηκαν την τελευταία 10ετία στον χρηματοοικονομικό τομέα.

5.1 Η περίπτωση της Epsilon Hack

5.1.1 Προφίλ Εταιρίας

Η Epsilon ήταν η μεγαλύτερη εταιρεία μάρκετινγκ ηλεκτρονικού ταχυδρομείου στον κόσμο . Το 2011, η εταιρεία χειριζόταν πάνω από 40 δισεκατομμύρια μηνύματα ηλεκτρονικού ταχυδρομείου και πάνω από 2.000 εμπορικά σήματα σε όλο τον κόσμο. Μεταξύ των πελατών της Epsilon βρίσκονται τρεις από τις δέκα πρώτες τράπεζες των ΗΠΑ - η JP Morgan Chase, η Citibank και η U.S. Bank - καθώς και η Barclays Bank και η Capital One. Πολλές εταιρείες, όπως το Best Buy, χρησιμοποιούν την Epsilon για την αποστολή προωθητικών μηνυμάτων ή άλλων ηλεκτρονικών μηνυμάτων στους πελάτες τους. Φυσικά, η εταιρεία έχει πρόσβαση σε πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου.

5.1.2 Περιστατικό Κυβερνοεπίθεσης

Στις 4 Απριλίου, το σύστημα παραβιάστηκε με αποτέλεσμα οι ιδιωτικές διευθύνσεις ηλεκτρονικού ταχυδρομείου εκατομμυρίων ανθρώπων να έρθουν στη δημοσιότητα. Το συγκεκριμένο είδος επίθεσης που εξαπολύθηκε στις Epsilon ονομάζεται spear phishing.

Στις 30 Μαρτίου 2011, ένα μη εξουσιοδοτημένο μέλος κατόρθωσε να εισβάλει στο σύστημα της Epsilon και να αποκτήσει πρόσβαση σε ηλεκτρονικά μηνύματα και ονόματα

πελατών για ένα υποσύνολο πελατών της. Αρχικά, η παραβίαση ηλεκτρονικού ταχυδρομείου θεωρήθηκε ότι επηρεάζει μόνο την Kroger, έναν εθνικό λιανοπωλητή και έναν πελάτη Epsilon. Μόλις η Epsilon και άλλοι πελάτες ξεκίνησαν να ερευνούν την παραβίαση, ανακάλυψαν την πλήρη έκταση και απέκτησαν μια πλήρη εικόνα του πώς το σύστημα τους παραβιάστηκε και τι ακριβώς ελήφθη. Στις 2 Απριλίου 2011, η Epsilon άρχισε να ειδοποιεί τους καταναλωτές ότι χάκερ είχαν κλέψει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου πελατών. Η Epsilon δεν διευκρίνισε ποιοι από τους 2.500 πελάτες της επηρεάστηκαν ή πόσα e-mails αποκτήθηκαν από μη εξουσιοδοτημένα άτομα. Ωστόσο η Epsilon ενημέρωσε τις εταιρείες -πελάτες της που επηρέασε η παραβίαση και αφέθηκε σ΄αυτές στη συνέχεια να ενημερώσουν τους ενδιαφερόμενους. Οι εταιρίες επιδιώκοντας την εξασφάλιση της ορθότητας της πληροφόρησης σε ένα τόσο ευαίσθητο θέμα όπως η ασφάλεια των προσωπικών πληροφοριών, ενημέρωσαν σε διαφορετικούς χρόνους, με διαφορετικούς τρόπους και με διαφορετικές ταχύτητες τους πελάτες τους. Αξίζει να σημειωθεί πως μεταξύ των επηρεαζόμενων επιχειρήσεων υπήρχαν και εταιρείες χρηματοπιστωτικών υπηρεσιών όπως η Capital One Financial Corp, η Barclays Bank.

5.1.3 Αποτελέσματα Επίθεσης

Ο αναλυτής της Gartner Group, Avivah Litan, δήλωσε ότι η υπόθεση Epsilon έδειξε ότι μπορεί να χρειαστούν καλύτεροι κανόνες ασφαλείας. Κανείς δεν είναι ασφαλής από τις όλο και πιο εξελιγμένες και πιο στοχευμένες επιθέσεις. Δεδομένου ότι οι επιθέσεις παραβιάζουν συνεχώς ακόμα και τα πιο σκληρά συστήματα ασφαλείας, οι οργανισμοί πρέπει να επικεντρωθούν στην ανάπτυξη σχεδίων αντιμετώπισης περιστατικών για την άμβλυνση των επιπτώσεων. Αυτό θα διευκολύνει αποτελεσματικά τους οργανισμούς να εντοπίσουν από πού προέρχονται οι επιθέσεις και να καθορίσουν την πλήρη έκταση της επίθεσης, βελτιώνοντας έτσι τους ελέγχους και τις διαδικασίες ώστε να διασφαλιστεί ότι η απειλή δεν θα επανεισαχθεί.

Διάγραμμα 5.1: Capital One Financial Corporation (COF)

Πηγή: Finance.yahoo.com

5.2 Η Περίπτωση της Target Corporation

5.2.1 Προφίλ Εταιρίας

Η Target Corporation είναι η δεύτερη μεγαλύτερη αλυσίδα καταστημάτων λιανικής πώλησης με έκπτωση στις Ηνωμένες Πολιτείες. Ιδρύθηκε στις 24 Ιουλίου του 1902 από τον George Dayton και σήμερα διαθέτει 1.834 καταστήματα.

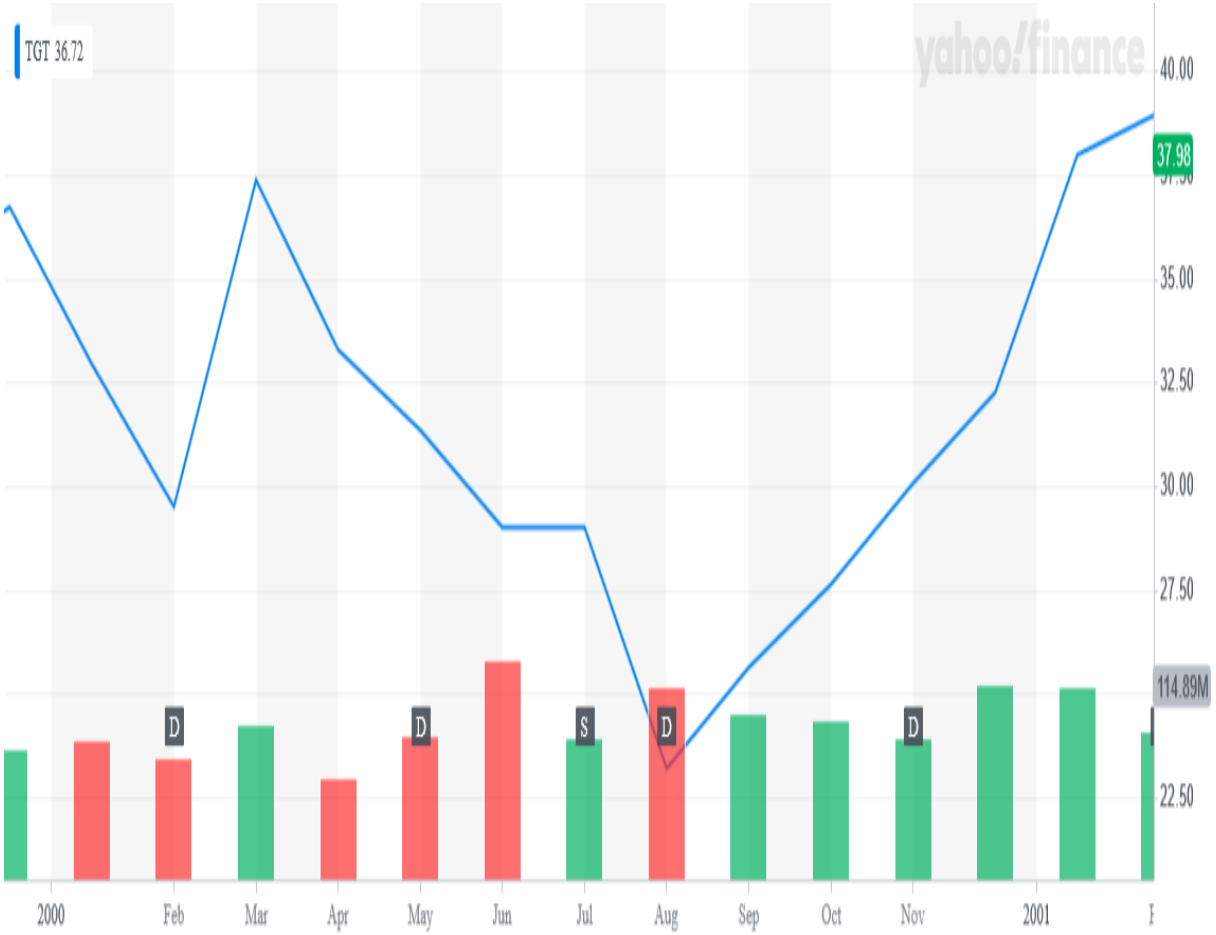
5.2.2 Περιστατικό Κυβερνοεπίθεσης

Στις αρχές τις δεκαετίας του 2000, η Target Corporation έπεσε θύμα ηλεκτρονικής επίθεσης η οποία είχε διάρκεια 19 ημερών. Πιο συγκεκριμένα, την παραμονή της ημέρας των Ευχαριστιών η εταιρία υποβλήθηκε σε μια μαζική παραβίαση ασφαλείας των δεδομένων των πιστωτικών καρτών των πελατών της που επηρέασε πάνω από 110 εκατομμύρια πελάτες. Οι εκτεθειμένες πληροφορίες περιείχαν ονόματα, αριθμούς τηλεφώνου, διευθύνσεις

αλληλογραφίας, διευθύνσεις ηλεκτρονικού ταχυδρομείου και δεδομένα λογαριασμών πιστωτικών και χρεωστικών καρτών. Επιπλέον, τα δεδομένα που αφορούσαν πιστωτικές κάρτες περιελάμβαναν τους αριθμούς λογαριασμών, τους κωδικούς ασφαλείας CVV και τις ημερομηνίες λήξεις.

5.2.3 Αποτελέσματα Επίθεσης

Ενώ η βιομηχανία πληρωμών με κάρτες απαιτεί από κάθε οργανισμό που συλλέγει και χρησιμοποιεί πληροφορίες καρτών για χρέωση να κρυπτογραφεί αυτές τις πληροφορίες με ένα περίπλοκο σύνολο κανόνων ασφαλείας, οι χάκερ κατάφεραν να βρουν και να εκμεταλλευτούν ένα προηγουμένως άγνωστο ελάττωμα. Για να εισέλθουν στο σύστημα χρησιμοποίησαν κλεμμένα στοιχεία από μια εταιρεία HVAC που συνεργαζόταν με την Target Corporation με αποτέλεσμα να έχουν πρόσβαση στα δεδομένα σε ένα σημείο που δεν είχαν ακόμη πραγματοποιηθεί όλες οι διαδικασίες κρυπτογράφησης. Η εταιρεία ενημερώθηκε για την επίθεση από το σύστημα ασφαλείας του κυβερνοχώρου και είχε τον χρόνο να σταματήσει την κλοπή των δεδομένων. Ωστόσο απέτυχε να ενεργήσει έγκαιρα με αποτέλεσμα να βρεθεί αντιμέτωπη με δεκάδες αγωγές και πρόστιμα ύψους 3.6 δισεκατομμυρίων για αυτή της την καθυστέρηση. Τον Μαρτίου του 2015 η εταιρεία έφτασε σε συμβιβασμό με τους πελάτες για 10 εκατομμύρια δολάρια και τον Μάιο του 2016 με τις πληγείσες τράπεζες και πιστωτικούς οργανισμούς για 39 εκατομμύρια δολάρια.



Διάγραμμα 5.2: Target Corporation

Πηγή: Finance.yahoo.com

5.3 Η περίπτωση της Sony

5.3.1 Προφίλ Εταιρίας

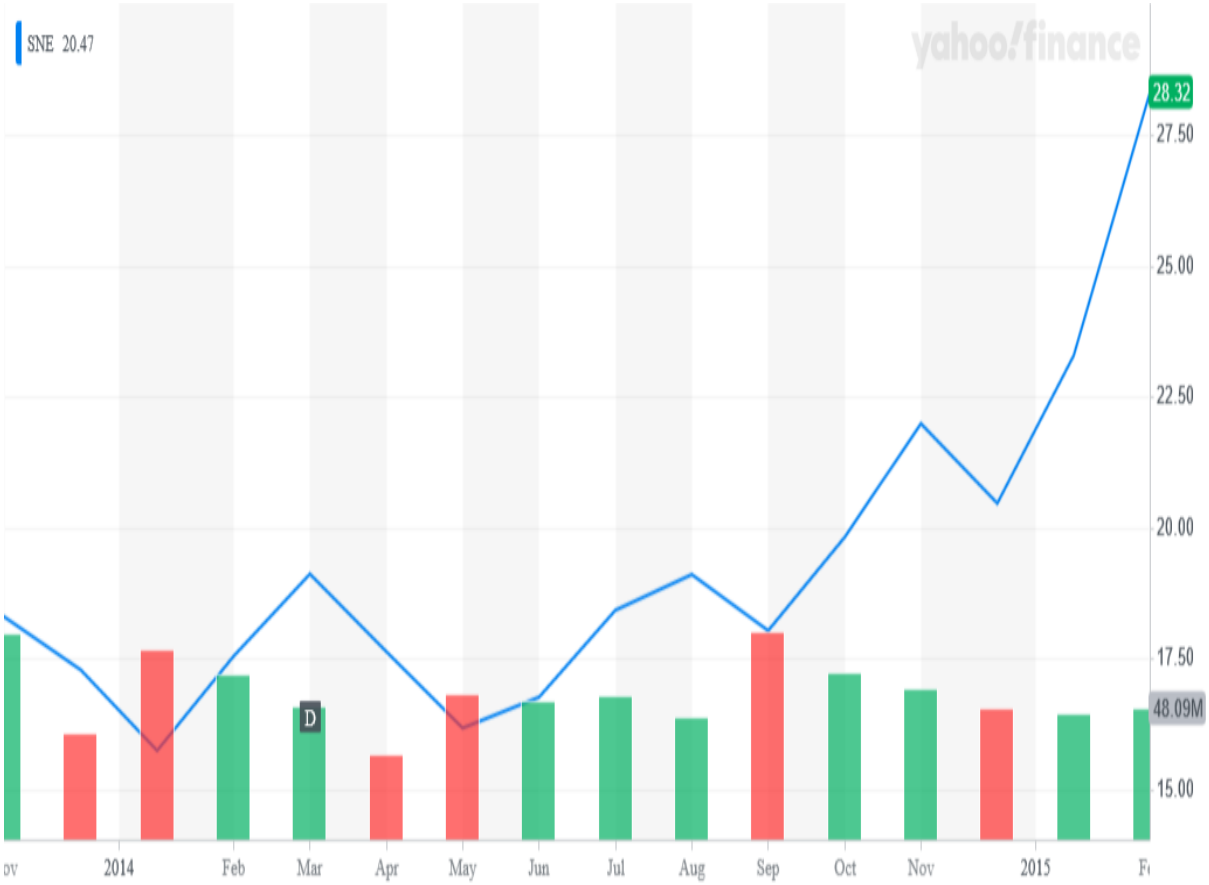
Ενώ πολλές επιθέσεις στον κυβερνοχώρο στοχεύουν τους πελάτες και τις προσωπικές τους πληροφορίες, η επίθεση κατά της Sony Pictures Entertainment είχε στόχο τους εργαζόμενους. Αξιωματούχοι των μυστικών υπηρεσιών των Η.Π.Α ισχυρίστηκαν ότι πίσω από τις επιθέσεις ήταν χάκερ της Βόρειας Κορέας που κατάφεραν να διεισδύσουν στα συστήματα της Sony Pictures. Η Βόρεια Κορέα αρνήθηκε τις κατηγορίες.

5.3.2 Περιστατικό Κυβερνοεπίθεσης

Στις 24 Νοεμβρίου του 2014, μία ομάδα από χάκερς με την ονομασία "Guardians of Peace" (GOP), απέκτησαν πρόσβαση και διέρρευσαν πολλά εμπιστευτικά αρχεία από την εταιρεία παραγωγής ταινιών "Sony Pictures". Οι χάκερς χρησιμοποίησαν διακομιστές υπολογιστών στη Βολιβία, την Κύπρο, την Ιταλία, την Πολωνία, τη Σιγκαπούρη, την Ταϊλάνδη και τις Ηνωμένες Πολιτείες. Οι διευθύνσεις IP που σχετίζονται με αυτούς τους διακομιστές έχουν συνδεθεί με τη Βόρεια Κορέα από το FBI. Τα αρχεία αυτά περιελάμβαναν πολλές προσωπικές πληροφορίες των υπαλλήλων και των οικογενειών τους, της Sony Pictures, πολλά e-mails μεταξύ των υπαλλήλων της εταιρείας, πληροφορίες σχετικά με τους μισθούς των εκτελεστικών στελεχών της εταιρείας και αντίγραφα από τις τότε ακυκλοφόρητες παραγωγές της εταιρείας. Οι δράστες της συγκεκριμένης επίθεσης χρησιμοποίησαν στη συνέχεια μια παραλλαγή του κακόβουλου λογισμικού Shamoon για την διαγραφή των υποδομών και των πόρων των υπολογιστών της Sony. Το κακόβουλο αυτό λογισμικό είχε αυτό που ο FBI ονομάζει "γραμμές κώδικα" και "διαγραφή δεδομένων", παρόμοιες με τις κακόβουλες εφαρμογές βορειοκορεατών.

5.3.3 Αποτελέσματα επίθεσης

Τον Νοέμβριο του 2014 η ομάδα GOP απαίτησε από την Sony να μην κυκλοφορήσει στους κινηματογράφους την ταινία "The Interview" η υπόθεση της οποίας πραγματεύονταν την δολοφονία του προέδρου της Βόρειας Κορέας Kim Jong-un, απειλώντας παράλληλα για πιθανές τρομοκρατικές επιθέσεις σε κινηματογράφους που θα γινόταν η προβολή. Αξιωματούχοι των Ηνωμένων Πολιτειών της Αμερικής μετά από έρευνα που πραγματοποίησαν στο λογισμικό, στο δίκτυο και στις τεχνικές που χρησιμοποιήθηκαν γι'αυτήν την επίθεση, υποστήριξαν πως η επίθεση χρηματοδοτήθηκε από την Βόρεια Κορέα. Το κράτος αρνήθηκε κάθε κατηγορία και ευθύνη.



Διάγραμμα 5.3: Sony Pictures Enertainment

Πηγή: Finance.yahoo.com

ΚΕΦΑΛΑΙΟ 6

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΠΕΡΑΙΤΕΡΩ ΈΡΕΥΝΑ

6.1 Συμπεράσματα

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η θεωρητική επισκόπηση των Κινδύνων του Κυβερνοχώρου (Cyber Risks). Πρόκειται για μια μορφή κινδύνων που έχει εξελιχθεί ραγδαία, κατά τη τελευταία 15ετία, σκαρφαλώνοντας πλέον στην κορυφή της λίστας μεταξύ των πιο σημαντικών κινδύνων που απειλούν, τόσο τις επιχειρήσεις, όσο και τους μεμονωμένους ιδιώτες, στο σύνολο της παγκόσμιας οικονομίας. Η ραγδαία ανάπτυξη της τεχνολογίας και των πολύπλοκων πληροφοριακών συστημάτων, έχει οδηγήσει σε μια παράλληλη αύξηση, όχι μόνο των κρουσμάτων επιθέσεων στον παγκόσμιο κυβερνοχώρο, αλλά και της σοβαρότητας των κινδύνων αυτών, καθώς και των δυνητικών ευπαθειών των πληροφοριακών συστημάτων απέναντι στους κινδύνους αυτούς. Σύμφωνα μάλιστα με ορισμένες πρόσφατες εκτιμήσεις, το κόστος που συνεπάγονται οι κίνδυνοι του κυβερνοχώρου ανέρχεται έως και τα 600 δις. δολάρια, παγκοσμίως. Ενδιαφέρον ωστόσο έχει η παρατήρηση ότι ενώ η πλειοψηφία των επιχειρήσεων, έως και πριν μια δεκαετία, δεν απέδιδε στους κινδύνους του κυβερνοχώρου την απαιτούμενη αναγνώριση, ως προς τις δυνητικές τους συνέπειες και τις επιπτώσεις τους, σήμερα η κατάσταση έχει αντιστραφεί σε πολύ μεγάλο βαθμό. Πλέον, οι προσπάθειες στρέφονται προς την πιο αποτελεσματική και επαγγελματική διαχείριση των κινδύνων αυτών, ενώ τα δεκάδες ηχηρά παραδείγματα παραβιάσεων εταιρικών πληροφοριακών συστημάτων έχουν ευαισθητοποιήσει την παγκόσμια επιχειρηματική κοινότητα προς την ανάληψη των ευθυνών της για την βελτίωση των εταιρικών δομών και τη θωράκισή τους έναντι αυτής της μορφής των κινδύνων.

Η ραγδαία αύξηση των κινδύνων του κυβερνοχώρου (τόσο σε απόλυτα μεγέθη, όσο και σε βαρύτητα των καταγεγραμμένων περιστατικών παραβιάσεων), έχει οδηγήσει στην άνθιση του επαγγέλματος της ασφάλισης έναντι των κινδύνων αυτών. Για τις επιχειρήσεις,

αυτό αποτελεί μια επιπρόσθετη επιλογή για τον σχεδιασμό του βέλτιστου προγράμματος διαχείρισης των εταιρικών κινδύνων. Τα κύρια ζητήματα που αντιμετωπίζουν οι ασφαλιστικές εταιρίες επικεντρώνονται στην έλλειψη ιστορικών δεδομένων και στη δυσκολία μοντελοποίησης των υφιστάμενων δεδομένων λόγω της εξελισσόμενης φύσης των κινδύνων στον κυβερνοχώρο. Επιπρόσθετα ζητήματα όπως η ασυμμετρία της πληροφόρησης και ο ηθικός κίνδυνος που συνεπάγεται το κάθε ασφαλιστικό εγχείρημα, φαίνεται ότι δυσχεραίνουν ακόμα περισσότερο, την ήδη περίπλοκη εικόνα που παρουσιάζει αυτή η αγορά. Παρόλα αυτά, η εικόνα για το μέλλον της ασφάλισης έναντι των κινδύνων του κυβερνοχώρου φαίνεται ιδιαίτερα ενθαρρυντική, δεδομένου ότι αποτελεί κοινή γνώμη ότι υπάρχει τεράστιο περιθώριο ανάπτυξης.

6.2 Περιορισμοί Έρευνας

Καταρχάς. όσα στοιχεία παραθέσαμε στη παρούσα εργασία, αφορούν την επισκόπηση βιβλιογραφικών, αμιγώς, πηγών, γεγονός που δεν προσδίδει κάποια ιδιαίτερη ερευνητική αποδεικτική ισχύ στα λεγόμενά μας. Αυτό αποτελεί και έναν βασικό περιορισμό της παρούσας διατριβής, ότι δηλαδή δεν προχωρήσαμε στην διενέργεια κάποιας έρευνας αναφορικά με το θέμα που επιλέχθηκε προς εξέταση.

Οι κίνδυνοι του κυβερνοχώρου, καθώς και η διαχείρισή τους σε εταιρικό επίπεδο, είναι ένα θέμα για το οποίο θα μπορούσαμε να προχωρήσουμε σε πολύ πιο εκτενής και τεχνικές αναλύσεις, κάτι όμως που, εν τέλει, δεν υλοποιήθηκε στην παρούσα διατριβή. Τα πληροφοριακά συστήματα, περικλείουν πλήθος πολύπλοκων και τεχνικών όρων, οι οποίοι αν και είναι ιδιαίτερα χρήσιμοι για την βαθύτερη ανάλυση του θέματος, εντούτοις δεν θα εξυπηρετούσαν την επισκόπησή του μέσα από την πιο θεωρητική οργανωσιακή οπτική που στοχεύσαμε να του προσδώσουμε.

Τέλος, η ασφάλιση έναντι των κινδύνων του κυβερνοχώρου, αποτελεί και αυτή ένα εξίσου σημαντικό θέμα, για το οποίο θα μπορούσαμε να έχουμε αναφερθεί εκτενέστερα, αναλύοντας περαιτέρω, τόσο τα ζητήματα που ανακύπτουν από πλευράς του ασφαλιστή, όσο και τις προκλήσεις που καλείται να αντιμετωπίσει ο ασφαλισμένος. Η μοντελοποίηση των στοιχείων που σχετίζονται με τους κινδύνους του κυβερνοχώρου, είναι ένα ακόμα θέμα που δεν επισκοπήθηκε, αλλά αποτελεί βασική πηγή προβληματισμού για πλήθος ερευνητών και επιστημόνων.

6.3 Προτάσεις για Περαιτέρω Έρευνα

Βασική διαπίστωση κατά την επισκόπηση των πηγών που χρησιμοποιήθηκαν για την συγγραφή της παρούσας εργασίας ήταν ότι η υφιστάμενη έρευνα στον τομέα των κινδύνων του κυβερνοχώρου και της ασφάλισης έναντι αυτών επικεντρώνεται κυρίως στην πλευρά της προσφοράς, δηλαδή εξετάζει το θέμα δυσανάλογα περισσότερο από την οπτική των ασφαλιστικών εταιριών. Η πλευρά της ζήτησης – δηλαδή των επιχειρήσεων που καλούνται να αντιμετωπίσουν τους κινδύνους που απειλούν τα πληροφοριακά τους συστήματα, καθώς και να αποφασίσουν το εάν θα αναζητήσουν την συνδρομή της ασφαλιστικής κάλυψης έναντι των κινδύνων αυτών - ωστόσο, μπορεί να προσελκύσει εξίσου σημαντικό ερευνητικό ενδιαφέρον στο μέλλον.

Πιο συγκεκριμένα, προτείνουμε την εξέταση του αντιληπτού επιπέδου της σοβαρότητας των κινδύνων του κυβερνοχώρου. Μια τέτοια έρευνα θα μπορούσε να αναδείξει τα όποια προβλήματα και τις γνωστικές ελλείψεις του επιχειρηματικού κόσμου αναφορικά με την έκταση και την βαρύτητα των κινδύνων του κυβερνοχώρου, καθώς επίσης και να αναδείξει τη σημασία της ασφάλισης έναντι των κινδύνων αυτών.

Επιπρόσθετα ζητήματα όπως η διερεύνηση των συνθηκών που δημιουργούν ένα ευνοϊκότερο κλίμα προς την αναζήτηση των ασφαλιστικών υπηρεσιών για την κάλυψη των κινδύνων του κυβερνοχώρου, η εξέταση των πιθανών τρόπων και μέσων βελτίωσης της αυτοπροστασίας έναντι των κινδύνων αυτών, καθώς και η εύρεση της ισορροπίας μεταξύ των ποικίλων τεχνικών διαχείρισης των εταιρικών κινδύνων προκειμένου να προταθεί ένα βέλτιστο μίγμα πολιτικής, θα μπορούσαν να αποτελέσουν έμπνευση για μελλοντική έρευνα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία

Ξένη Βιβλιογραφία

- David Betz, Tim Stevens, cyberspace and the state toward a strategy for cyber-power, iiss, November 2011, p.37-39, p 58-60, p 65-66
- Mark Dun, Ibid: A Novel, p.46-47
- Richard A. Clarke, Robert. Knake , Cyber War: The Next Threat to National Security and What to Do About It ,Harper Collins E-books, p.4

Επιστημονικά Άρθρα και Μελέτες

- BGP https://el.wikipedia.org/wiki/Border_Gateway_Protocol
- Buehrer G., Weide B., Sivilotti P. "Using parse tree validation to prevent SQL injection attacks", 2005 https://www.researchgate.net/profile/Bruce_Weide/publication/221215947_Using_parse_tree_validation_to_prevent_SQL_injection_attacks/links/02bfe5117c849676a6000000/Using-parse-tree-validation-to-prevent-SQL-injection-attacks.pdf
- Deloitte (2016), “Assessing Cyber Risk. Critical questions for the board and the C-suite” https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-assessing-cyber-risk-200516.pdf
- International Telecommunications Union (ITU) Facts and Figures 2015 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf
- International Telecommunications Union (ITU) Facts and Figures 2016 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf
- Kabay, M. E, PhD, CISSP Director of Education, Munich, Germany 16-8 March 1998International Computer Security Association p .4 http://www.mekabay.com/overviews/anonpseudo.pdf
- Kaspersky, Website "What is a Zero-day Exploit?" [Online] 22September 2018 https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

- Roger Clarke, What's 'Privacy'? Version of 7 August 2006 Prepared for a Workshop at the Australian Law Reform Commission ,July 2006 http://www.rogerclarke.com/DV/Privacy.html
- Spett K. "Cross-Site Scripting -Are your web applications vulnerable?", SPI Dynamics, 2005 http://people.cs.ksu.edu/~hankley/d764/Topics/SPIcross-sitescripting.pdf
- Techopedia, Website "Credential stuffing" [Online] https://www.techopedia.com/definition/32586/credential-stuffing
- The Radicati Group, Inc. A Technology Market Research Firm Email Statistics Report, 2016-2020 (p. 2) https://www.radicati.com/wp/wp content/uploads/2016/01/Email_Statistics_Report_2016-2020_Executive_Summary.pdf
- THE VERISIGN DOMAIN REPORT p.2 https://www.verisign.com/assets/domain-name-report-sept2016.pdf
- Βασιλειάδου Χριστίνα, Ευρωπαϊκός Γενικός Κανονισμός Προστασίας Δεδομένων, Κίνδυνοι του Κυβερνοχώρου και ο ρόλος της ασφάλισης έναντι των διαδικτυακών Κινδύνων, Ιανουάριος 2019
- Μαυρίδης Παύλος, Κυβερνοεπιθέσεις στον Χρηματοοικονομικό τομέα, Δεκέμβριος 2017
- Σίμου Φλώρας, Κυβερνοπόλεμος και επιθέσεις στο Διαδίκτυο, Οκτώβριος 2016
- Τουμπόγλου Ιωάννης, Άντληση πληροφοριών για κυβερνο-απειλές από το σκοτεινό διαδίκτυο, 2019
- Χαιδής Λεωνίδας, Οι Συγκρούσεις στον Κυβερνοχώρο: Ο Κυβερνοπόλεμος και η Αποτροπή, Πειραιάς 2012
- Χρήστος Βεράτης, ΚΕΔΙΣΑ, Κυβερνοχώρος-Κυβερνοεπιθέσεις-Κυβερνοάμυνα-Μέρος 1ο, Νοέμβριος 2015 http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe

Ηλεκτρονικές πηγές

- http://www.insuringtech.com/2012/02/cyber-attack-insurance-history-of-computer-hacking/

- https://el.wikibooks.org/wiki
- https://el.wikibooks.org/wiki/Να_περιγράψετε_ένα_σημαντικό_περιστατικό_κυβερνοεγκλήματος_(8η_Εργασία_2017-18)#Epsilon_Hack_(%CE%9A%CE%BB%CE%B5%CE%B9%CE%BD%CE%AC%CE%BA%CE%B7%CF%82_%CE%93%CE%B9%CF%8E%CF%81%CE%B3%CE%BF%CF%82_%CE%91%CE%9C:4415252)
- https://en.wikipedia.org/wiki/Denial-of-service_attack
- https://en.wikipedia.org/wiki/Sony_Pictures_hack
- https://en.wikipedia.org/wiki/Target_Corporation#Customer_privacy
- https://krebsonsecurity.com/2015/03/feds-indict-three-in-2011-epsilon-hack/
- https://list25.com/25-biggest-cyber-attacks-in-history/
- https://www.angelkings.com/target-corporation/
- https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html
- https://www.cyberinsurancegreece.com/
- https://www.cyberinsurancequote.gr/
- https://www.infosecurity-magazine.com/news/epsilon-hack-50-companies-hit-by-data-breach/
- https://www.isaca.org/pages/default.aspx
- https://www.iso.org/home.html
- https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219
- https://www.rims.org/home