ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Cyber Risk Management

Σαρικλόγλου Μιχαήλ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Δημητρίου
Επίκουρος καθηγητής

Λαμία Ιανουάριος έτος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Cyber Risk Management

Σαρικλόγλου Μιχαήλ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Δημητρίου
Επίκουρος καθηγητής

Λαμία Ιανουάριος έτος 2023

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Cyber Risk Management

Sarikloglou Michael

FINAL THESIS

ADVISOR

George Dimitriou
Assistant Professor

Lamia January year 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 10/03/2023

Ο ~~Η~~ Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Το παρόν ερευνητικό άρθρο πραγματοποιεί ανάλυση βιβλιογραφικής ανασκόπησης που επικεντρώνεται στην κατανόηση διαφόρων πτυχών της διαχείρισης των κινδύνων στον κυβερνοχώρο. Η έρευνά μας έχει τρεις στόχους. Να προσδιορίσει τους καθοριστικούς παράγοντες των κινδύνων κυβερνοασφάλειας, να αναλύσει τις συνέπειες των επιθέσεων κυβερνοασφάλειας και να ανακαλύψει πώς οι επιχειρήσεις διαχειρίζονται τους κινδύνους κυβερνοασφάλειας.

ABSTRACT

This research article conducts a literature review analysis focused on understanding various aspects of cyber risk management. Our research has three objectives. To identify the determinants of cybersecurity risks, to analyze the consequences of cybersecurity attacks, and to discover how organizations manage cybersecurity risks.

Contents

Εισαγωγή

Οι κοινωνίες αλλάζουν με τους καιρούς και τις εξελίξεις που έρχονται άλλοτε αργά και άλλοτε πιο γρήγορα. Η σύγχρονη κοινωνία έχει αλλάξει ριζικά τον τρόπο λειτουργίας μας, με μεγαλύτερη έμφαση στη χρήση των νέων τεχνολογιών και την απελευθέρωση των αγορών και του κεφαλαίου παγκοσμίως. Οι μορφές της ανθρώπινης δραστηριότητας έχουν επηρεαστεί από την υιοθέτηση νέων τεχνολογικών εργαλείων και μέσων που προσφέρουν και οδηγούν στη διεύρυνση της ανθρώπινης συμπεριφοράς μέσω νέων μορφών αλληλεπίδρασης. Η σύγχρονη τεχνολογική επανάσταση της εποχής έχει επηρεάσει τη συντριπτική πλειονότητα των ατόμων και των οντοτήτων της κοινωνίας. Πολλοί από εμάς, ιδίως οι μεγαλύτεροι σε ηλικία, δεν είχαν ποτέ φανταστεί ότι η τεχνολογία θα είχε τόσο σημαντικό ρόλο στην καθημερινή μας ζωή. Η τεχνολογική εποχή που βιώνουμε είναι απόλυτα συνυφασμένη με τον Κυβερνοχώρο. Η εκτεταμένη χρήση των υπολογιστών και η σύνδεση στο διαδίκτυο συμβάλλουν σε αυτό. Ο παγκόσμιος επιχειρηματικός κόσμος αναδιοργανώνεται, αλλάζει και προσαρμόζεται συνεχώς για να ανταποκριθεί στις απαιτήσεις του περιβάλλοντος. Η αξιοποίηση των τεχνολογιών πληροφορικής αποτελεί βασικό παράγοντα βελτίωσης. Αλλά πάντα μια θετική κατάσταση δημιουργίας περικλείεται από κάτι αρνητικό. Έτσι, ο κυβερνοχώρος περικλείεται πάντα από τον κίνδυνο. Η ιστορία έχει δείξει ότι τα αποτελέσματα κάθε σημαντικής τεχνολογικής ανάπτυξης εξαρτώνται από τον τρόπο χρήσης της. Έτσι, η τεχνολογία μπορεί να βελτιώσει ριζικά το βιοτικό επίπεδο των ανθρώπων αλλά και να οδηγήσει σε καταστροφικές εξελίξεις.

Το οικονομικό αντίκτυπο του κυβερνοεπιχειρησιακού κινδύνου του Διαδικτύου των Πραγμάτων (IoT) αυξάνεται με την ενσωμάτωση των ψηφιακών υποδομών στην ψηφιακή οικονομία (Marwedel & Engel, 2016). Η τυποποίηση και η ρύθμιση της ασφάλειας στον κυβερνοχώρο θα διαδραματίσουν καθοριστικό ρόλο στη διαδικασία μείωσης των επιθέσεων στον κυβερνοχώρο, συνεχίζοντας παράλληλα την αξιοποίηση της οικονομικής αξίας.

Ο κίνδυνος στον κυβερνοχώρο από τις συσκευές που έχουν άμεση επαφή με το διαδίκτυο υφίσταται σε διαφορετικά και ενίοτε υψηλότερα επίπεδα σε περιοχές όπου ο κίνδυνος αυτός είναι απροσδόκητος. Για παράδειγμα, στις ΗΠΑ, η υγειονομική περίθαλψη αποτελεί πλέον τον μεγαλύτερο στόχο κυβερνοεπιθέσεων, αναφορικά έχει μεγαλύτερο κίνδυνο από τη μεταποίηση και τις τράπεζες (IBM, 2016). Σύμφωνα με την ίδια έκθεση (IBM, 2016), η αξία των κλεμμένων προσωπικών πληροφοριών υγείας είναι δέκα έως

είκοσι φορές μεγαλύτερη από την αξία ενός κλεμμένου αριθμού πιστωτικής κάρτας. Για να κατανοήσουμε και να ορίσουμε μια γενική κατάσταση-στόχο για την κυβερνοασφάλεια, πρέπει να κατανοήσουμε το επιχειρηματικό πλαίσιο και τις προτεραιότητες για την κυβερνοασφάλεια μέσω συζητήσεων μεταξύ εμπειρογνωμόνων σε θέματα κυβερνοασφάλειας και υπευθύνων λήψης αποφάσεων(Deloitte,2017).

Η παρούσα μελέτη επικεντρώνεται στο ευρύτερο πεδίο της διαχείρισης της κυβερνοασφάλειας από την άποψη της χρηματοοικονομικής ανάλυσης και των οικονομικών επιπτώσεων των κινδύνων της. Στοχεύει στο αντίκτυπο των κυβερνοεπιθέσεων στα χρηματοπιστωτικά ιδρύματα, στο κόστος που δημιουργούν και στις στρατηγικές διαχείρισης που πρέπει να αντιμετωπίσουν τα ανώτατα στελέχη κάθε επιχείρησης για την αντιμετώπιση και την εξάλειψη των κινδύνων, έτσι ώστε να παραμείνουν τα οφέλη από τη χρήση μιας διασύνδεσης με τον Κυβερνοχώρο, όπως η δυνατότητα των επιχειρήσεων να αυξήσουν την ταχύτητα των διαδικασιών τους, την αποδοτικότητα και το ανταγωνιστικό πλεονέκτημα.

Κίνδυνος κυβερνοασφάλειας είναι ο κίνδυνος οικονομικής απώλειας, διαταραχής ή ζημίας στη φήμη μιας επιχείρησης ως αποτέλεσμα αποτυχίας στα συστήματα πληροφορικής τής (Institute of Risk Management). Παραδείγματα κινδύνου κυβερνοασφάλειας περιλαμβάνουν τον κίνδυνο απώλειας ευαίσθητων δεδομένων, διαταραχής στο δίκτυο, τα συστήματα και τις υπηρεσίες μιας επιχείρησης και φυσικής ηλεκτρονικής ζημίας. Η ασφάλεια στον κυβερνοχώρο θεωρείται σήμερα μια από τις σημαντικότερες ανησυχίες για τα στελέχη των επιχειρήσεων στις προηγμένες οικονομίες. Αυτό δεν αποτελεί έκπληξη, δεδομένης της αύξησης των επιτυχημένων κυβερνοεπιθέσεων κατά μεγάλων οργανισμών τις τελευταίες δεκαετίες, με αποτέλεσμα ζημίες δισεκατομμυρίων δολαρίων στην παγκόσμια οικονομία. Για παράδειγμα, στην τρίτη έκθεσή τους, η CSIS και η McAfee διερευνούν την αύξηση του εγκλήματος στον κυβερνοχώρο από την άποψη των οικονομικών επιπτώσεων. Εκτιμάται ότι το έγκλημα στον κυβερνοχώρο μπορεί να κοστίσει στον κόσμο σχεδόν 600 δισεκατομμύρια δολάρια, ή το 0,8% του παγκόσμιου ΑΕΠ το 2019 (https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html). Παρ' όλα αυτά, οι επιχειρήσεις παραμένουν ιδιαίτερα εκτεθειμένες σε κινδύνους κυβερνοασφάλειας. Μια εκτίμηση της Cybersecurity Ventures είναι ότι οι ζημιές από το κυβερνοέγκλημα θα κοστίζουν στον κόσμο 10.5 τρισεκατομμύρια δολάρια ετησίως έως το 2025 (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/).

Μετά από αυτή τη σύντομη εισαγωγή, είναι προφανής η ανάγκη για περαιτέρω έρευνα, η οποία θα εντοπίζει και θα αναλύει τις δυνατότητες που προσφέρει η αντιστροφή του περιορισμού των σκοτεινών σημείων. Πρώτα απ' όλα, η μελέτη των κινδύνων της κυβέρνησης και στη συνέχεια η ανάλυση συγκεκριμένων τομέων, αλλά και τρόπων διαχείρισής τους.

Κεφάλαιο 1. Βασικοί κίνδυνοι και απειλές στον κυβερνοχώρο

1.1 Ορισμός του κινδύνου στον κυβερνοχώρο

Σύμφωνα με την έκθεση του Συμβουλίου Οικονομικών Συμβούλων (Council of Economic Advisors - CEA) (2018), ως κακόβουλη δραστηριότητα στον κυβερνοχώρο ορίζεται "μια δραστηριότητα, εκτός από εκείνη που επιτρέπεται από τη νομοθεσία των ΗΠΑ ή σύμφωνα με αυτήν, η οποία αποσκοπεί να θέσει σε κίνδυνο ή να βλάψει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα υπολογιστών, συστημάτων πληροφοριών ή επικοινωνιών, δικτύων, φυσικών ή εικονικών υποδομών που ελέγχονται από υπολογιστές ή συστήματα πληροφοριών ή των πληροφοριών που βρίσκονται σε αυτά". Η κακόβουλη δραστηριότητα στον κυβερνοχώρο λαμβάνει πολλές μορφές, όπως hacking, crimeware, κυβερνοκατασκοπεία, άρνηση παροχής υπηρεσιών, κακή διαχείριση εμπιστευτικών και προνομίων, skimmers για κάρτες πληρωμών, εισβολές σε σημεία πώλησης, φυσικές κλοπές και απώλειες και επιθέσεις σε διαδικτυακές εφαρμογές. Η έκθεση της Verizon (2017) σχετικά με την παραβίαση δεδομένων διαπιστώνει ότι η πλειονότητα των επιχειρήσεων στον κυβερνοχώρο περιλαμβάνει ξένες και εγκληματικές ομάδες που σκοπεύουν να επωφεληθούν από την επίθεση και οι περισσότερες εμπλέκονται στην πειρατεία. Οι κυβερνοεπιθέσεις απευθύνονται σε μεγάλο βαθμό σε παρόχους χρηματοπιστωτικών υπηρεσιών και υπηρεσιών υγειονομικής περίθαλψης (Verizon, 2017).

1.2 Κατηγορίες κινδύνων στον κυβερνοχώρο

Η έκθεση της Grant Thornton (2018) για τους κινδύνους στον κυβερνοχώρο αναφέρει ότι σε σχέση με άλλα είδη επιχειρηματικών κινδύνων, οι κίνδυνοι αυτοί παρουσιάζουν αρκετές προκλήσεις. Οι κίνδυνοι στον κυβερνοχώρο αποτελούν μια συνεχή, αδιάλειπτη, απροσδιόριστη και δύσκολα μετρήσιμη απειλή και σε αντίθεση με άλλους κινδύνους εκθέτουν τον οργανισμό σε πολύπλευρους τομείς χωρίς οριοθέτηση. Πριν από την ανάπτυξη και εφαρμογή ενός ολοκληρωμένου πλαισίου διαχείρισης, θα πρέπει να εξεταστούν τα χαρακτηριστικά αυτών των κινδύνων και η σχέση τους με τον ίδιο τον οργανισμό. Για την καλύτερη κατανόηση και διαχείριση αυτών των κινδύνων, είναι απαραίτητη η διάκριση και η ταξινόμησή τους. Είναι η πυξίδα που θα βοηθήσει στη διαδικασία διαχείρισης των κινδύνων.

Η RSA Security ταξινομεί τους κινδύνους κυβερνοασφάλειας με βάση την πηγή προέλευσης και τον σκοπό τους. Κατηγοριοποιούνται και προσδιορίζονται οι ακόλουθοι τύποι κινδύνων[1]:

Εσωτερικές κακόβουλες ενέργειες: Σχετίζονται με σκόπιμες πράξεις δολιοφθοράς, κλοπής ή άλλες κακόβουλες ενέργειες που διαπράττονται από υπαλλήλους του οργανισμού στις έμπιστες θυγατρικές τους.

Εσωτερικές μη σκόπιμες: Πρόκειται για ενέργειες που έχουν ως αποτέλεσμα την απώλεια δεδομένων ή την απώλεια από τα πληροφοριακά συστήματα του οργανισμού λόγω ανθρώπινου λάθους των εργαζομένων και άλλων έμπιστων συνεργατών.

Εξωτερικές κακόβουλες: Πρόκειται για την πιο δημοφιλή μορφή κινδύνου στον κυβερνοχώρο. Πρόκειται για οργανωμένες επιθέσεις, που δεν συνδέονται με την εταιρεία, κυρίως εγκληματικές οργανώσεις και κυβερνοπειρατές.

Εξωτερικός μη σκόπιμος: Πρόκειται για κινδύνους παρόμοιους με τους εσωτερικούς μη σκόπιμους και προκαλούν απώλεια ή ζημία στην επιχείρηση χωρίς πρόθεση.

Σύμφωνα με τους ερευνητές Cebula et al (2014), η ταξινόμηση των κινδύνων κυβερνοασφάλειας δομείται γύρω από μια ιεραρχία τεσσάρων κύριων κατηγοριών-κλάσεων. Στην πρώτη κατηγορία ανήκουν οι ενέργειες των ατόμων ή η έλλειψη ενεργειών και επηρεάζουν την ασφάλεια στον κυβερνοχώρο. Στη δεύτερη κατηγορία περιλαμβάνονται οι τεχνολογικές αποτυχίες. Ακολουθούν οι αποτυχίες των εσωτερικών διαδικασιών που επηρεάζουν την ικανότητα εφαρμογής, ελέγχου, διαχείρισης και διατήρησης της ασφάλειας. Τέλος, τα εξωτερικά γεγονότα που βρίσκονται εκτός του ελέγχου του οργανισμού (Cebula et al, 2014).

Σε μια παρόμοια, αλλά πιο εκτεταμένη, ανάλυση κινδύνων, από τον Λιβάνη (2016), η ταξινόμηση των κινδύνων στον κυβερνοχώρο αποτελείται από έξι θεμελιώδεις αρχές. Ο πρώτος πυλώνας αναφέρεται στους φορείς των κινδύνων στον κυβερνοχώρο. Ο δεύτερος πυλώνας περιλαμβάνει τα ποικίλα και πολύπλευρα κίνητρα. Ο τρίτος πυλώνας αναφέρεται στους στόχους. Ο τέταρτος πυλώνας αφορά τους τρόπους με τους οποίους θα μπορούσε να συμβεί μια παραβίαση. Ο πέμπτος πυλώνας περιγράφει τα περιουσιακά στοιχεία σε κίνδυνο. Ο έκτος πυλώνας περιλαμβάνει τις κύριες επιπτώσεις των κινδύνων στον κυβερνοχώρο.

1.3 Βασικοί όροι

1.3.1 Πρόληψη

Ως προστασία νοείται η ανάπτυξη και εφαρμογή ποικίλων αμυντικών μέτρων και στρατηγικών προσεγγίσεων, με απώτερο στόχο τον περιορισμό ή ακόμη και την απαγόρευση της πρόσβασης ή της χρήσης συγκεκριμένων πόρων ενός υπολογιστικού συστήματος τόσο από εσωτερικούς όσο και από εξωτερικούς παράγοντες απειλής. Αξίζει να σημειωθεί ότι η λειτουργία της πρόληψης δεν εγγυάται ή διασφαλίζει πλήρως ότι δεν θα συμβεί ένα παράνομο περιστατικό στον κυβερνοχώρο, απλώς μειώνει τις επιπτώσεις ενός δυσμενούς συμβάντος. Η διαδικασία αυτή είναι πολύ σημαντική, καθώς επιτρέπει στους διαχειριστές και τους υπεύθυνους ασφαλείας να λαμβάνουν τις κατάλληλες διασφαλίσεις για την εγγύηση της ασφάλειας των υποδομών (Πλαίσιο για τη βελτίωση της κυβερνοασφάλειας σε υποδομές ζωτικής σημασίας, 2017).

1.3.2 Ανίχνευση

Η ανίχνευση περιγράφει τη διαδικασία ανίχνευσης παράνομων ενεργειών και αναζήτησης των γεγονότων και των προσώπων που προκάλεσαν αυτές τις ενέργειες και τις συνέπειές τους. Η διαδικασία αυτή μπορεί να πραγματοποιηθεί με την ανάπτυξη και την εφαρμογή κατάλληλων αμυντικών και προληπτικών αντιμέτρων προκειμένου να αποτραπεί εγκαίρως μια παράνομη δραστηριότητα εμπορίας στον κυβερνοχώρο. Η λειτουργία αυτή εντοπίζει αμέσως κάθε ανεπιθύμητη εισβολή ή απόπειρα εντός του κυβερνοχώρου. Η δυνατότητα αυτή είναι ζωτικής σημασίας, διότι η χρήση κατάλληλων μέτρων, όπως η συνεχής παρακολούθηση και οι διαδικασίες πρόληψης και ανίχνευσης, αυξάνει την αξία της ασφάλειας (Framework for Improving Critical Infrastructure Cybersecurity, 2017).

1.3.3 Ανθεκτικότητα

Στο διαρκώς εξελισσόμενο οικοσύστημα του κυβερνοχώρου υπάρχουν πολλοί κίνδυνοι. Συνεπώς, απαιτείται από τους οργανισμούς και τις επιχειρήσεις να αναπτύξουν επαρκή ανθεκτικότητα στον κυβερνοχώρο, ώστε να μπορούν να ανταποκριθούν και να είναι σε θέση να ανακάμψουν από καταστροφικές απειλές και επιθέσεις στον κυβερνοχώρο (Achieving resilience in the cyber ecosystem, 2014). Η ευρωστία της υποδομής συμβάλλει στη μείωση των καταστροφικών συμβάντων και απαιτεί από τον οργανισμό ή την επιχείρηση να υποστηρίζει μια ευέλικτη υποδομή ικανή να προσαρμόζεται, να μπορεί να ανταπεξέλθει και να ανακάμπτει γρήγορα από καταστροφικά συμβάντα (The Cyber-Resilient Enterprise, 2015). Αυτό επιτυγχάνεται με τη χρήση κατάλληλων τεχνικών,

διαδικασιών και προσεγγίσεων που στοχεύουν στην υποδομή και την αρχιτεκτονική του συστήματος για να δώσουν τον απαιτούμενο χρόνο. Αυτό γίνεται έτσι ώστε οι οργανισμοί και οι επιχειρήσεις να είναι σε θέση να σκέφτονται και να ενεργούν προληπτικά προκειμένου να δημιουργήσουν μια ισχυρή και αποτελεσματική στρατηγική ασφάλειας για την καλύτερη δυνατή προετοιμασία, προστασία και αντίδραση στις αναδυόμενες απειλές (Berkeley, 2010). Σύμφωνα με τον ειδικό σε θέματα ανθεκτικότητας Stephen Flynn υπάρχουν τέσσερα βασικά χαρακτηριστικά για την εξασφάλιση της ανθεκτικότητας που εξαρτώνται από τα ακόλουθα χαρακτηριστικά (Berkeley, 2010):

- Ευρηματικότητα: Η λέξη αυτή αναφέρεται στον προσδιορισμό των καλύτερων επιλογών για τον έλεγχο της ζημίας και στη μετάδοση αυτών των επιλογών στα κατάλληλα μέρη. Εξαρτάται περισσότερο από την τεχνογνωσία και την κατάρτιση του εργατικού δυναμικού ενός οργανισμού ή μιας επιχείρησης, παρά από την τεχνολογία.

- Ανθεκτικότητα: Η λέξη αυτή αναφέρεται στην ικανότητα ενός συστήματος να λειτουργεί εν όψει μιας καταστροφής ή να επιβιώνει από αυτήν. Αυτό επιτυγχάνεται με την κατασκευή δομών ή συστημάτων που μπορούν να αντισταθούν σε μια σημαντική επίθεση, καθώς και με τη χρήση εναλλακτικών ή πλεονασματικών συστημάτων. Επιπλέον, σε περίπτωση καταστροφής, η απαίτηση αυτή απαιτεί συνεχείς επενδύσεις και συντήρηση ζωτικών κομματιών υποδομής.

- Προσαρμοστικότητα: Ο ορισμός αυτός περιγράφει την αναθεώρηση των σχεδίων και την κατάλληλη τροποποίηση των διαδικασιών για την κατάλληλη εισαγωγή νέων εργαλείων και τεχνολογιών για την επιτυχή βελτίωση της αντοχής, της εφευρετικότητας και της ανάκαμψης πριν από την επόμενη επίθεση.

- Ταχεία αποκατάσταση: Η έννοια αυτή αναφέρεται στην ικανότητα αποκατάστασης στην αρχική κατάσταση ενός συστήματος το συντομότερο δυνατό μετά από μια επίθεση. Αυτό επιτυγχάνεται μέσω της εφαρμογής κατάλληλων σχεδίων έκτακτης ανάγκης και των πιο αποτελεσματικών τεχνικών έγκαιρης ανίχνευσης για τον εντοπισμό των πιο εξειδικευμένων πόρων που θα χρησιμοποιηθούν όταν χρειαστούν (Berkeley, 2010).

Είναι σημαντικό να σημειωθεί ότι η ανθεκτικότητα στον κυβερνοχώρο δεν εξαλείφει όλες τις ζημιές του δικτύου, καθώς πέραν του ότι είναι και αδύνατο και ανέφικτο, δεν θα ήταν δυνατή η καινοτομία σε περιβάλλοντα πραγματικού κινδύνου (Framework for Improving Critical Infrastructure Cybersecurity, 2017).

Κεφάλαιο 2. Προσδιοριστικοί παράγοντες του κινδύνου κυβερνοασφάλειας

Οι εκστρατείες ηλεκτρονικού εγκλήματος και οι συνεχώς διευρυνόμενες ομάδες υψηλού προφίλ απειλούν να μετατοπίσουν τους στόχους των θυμάτων και να επικεντρωθούν περισσότερο στις πολύπλοκες σχέσεις με "ασφαλείς συνδικαλιστικές" συνεργασίες για την κάλυψη της δραστηριότητας (Accenture security, 2019).

Η έκθεση ανακάλυψε 5 παράγοντες που αγγίζουν το τοπίο των κυβερνοαπειλών:

1.Συμβιβαστική γεωπολιτική: Οι νέες απειλές που προκύπτουν από τις παγκόσμιες επιχειρήσεις πληροφοριών και από τις τεχνολογικές εξελίξεις θα μπορούσαν επίσης να βρίσκονται στη διαγώνιο, καθώς οι εντάσεις της πολιτικής επιστήμης παραμένουν. Καθώς οι εταιρείες κυβερνοασφάλειας επωφελούνται από τα παγκόσμια γεγονότα υψηλού προφίλ και ζητούν να επηρεάσουν την κοινή γνώμη, οι φορείς αυτοί δεν θα υποστηρίξουν αποκλειστικά τα τρέχοντα επίπεδα δραστηριότητας, όπως και τις νέες δυνατότητες, καθώς οι νέες τεχνολογίες μεταβάλλουν τις συνθήκες.

2.Οι εγκληματίες του κυβερνοχώρου προσαρμόζονται, παρενοχλούνται, διαφοροποιούνται ανάλογα με τις συνθήκες. Παρά τις θεαματικές δράσεις επιβολής της νομοθεσίας κατά εγκληματικών κοινοτήτων και κοινοπραξιών το 2018, η ευελιξία των παραγόντων απειλής να παραμείνουν λειτουργικοί μας υπενθυμίζει την πολλαπλή αύξηση στο πλαίσιο της σοβαρότητας και της ανθεκτικότητας των εγκληματικών δικτύων το 2019. Η ανάλυση δείχνει ότι το τυπικό έγκλημα και τα χρηματικά κίνητρα για την παράβαση του νόμου εξακολουθούν να δημιουργούν μεγάλη απειλή για μεμονωμένους χρήστες του δικτύου και των επιχειρήσεων. Ωστόσο, οι εγκληματικές επιχειρήσεις μπορούν ενδεχομένως να τροποποιήσουν ακόμα τους τρόπους που δρουν ώστε να μειώσουν την πιθανότητα εντοπισμού και παρενόχλησης τους.

3. Τα διαφόρων σκοπών κίνητρα δημιουργούν νέους κινδύνους για την άμυνα και την αντιμετώπιση του ransomware. Οι απειλές ransomware επιδεινώνονται επιπλέον από την πώληση εταιρικής πρόσβασης στο διαδίκτυο - μέσω αυτού του συνεργατικού βαθμού

κάποιο ανεπιθύμητο πρόσωπο μπορεί να αναπτύξει ransomware σε εταιρική κλίμακα - και ως εκ τούτου η περίπτωση ransomware με αντιαναπτυξιακές ικανότητες (όπως το WannaCry) να επανεμφανιστεί μπορεί κάλλιστα να είναι σημαντική απειλή για τις επιχειρήσεις. Ενώ τα κίνητρα πίσω από μια τέτοια επίθεση θα μπορούσαν να φαίνονται οικονομικά, οι στοχευμένες επιθέσεις ransomware θα μπορούσαν μερικές φορές να εξυπηρετούν διαφόρων σκοπών κίνητρα, είτε οικονομικά, είτε ιδεολογικά, είτε πολιτικά. Παρά το κίνητρο, ενώ η απειλή ransomware παραμένει, οι οργανισμοί θα πρέπει να διασφαλίσουν ότι λαμβάνουν τα κατάλληλα μέτρα για να οργανώσουν, να αποτρέψουν, να ανιχνεύσουν, να απαντήσουν και να περιορίσουν μια επίθεση ransomware σε κάποια εταιρεία.

4. Η βελτίωση της υγιεινής του οικοσυστήματος προωθεί τις απειλές στην αλυσίδα εφοδιασμού, μετατρέποντας τους φίλους τους αναξιόπιστους. Η παγκόσμια επιχειρηματική διασύνδεση, η ευρύτερη υιοθέτηση των αρχαίων αντιμέτρων του εμπορίου στον κυβερνοχώρο και ως εκ τούτου η βελτίωση της βασικής υγιεινής στον κυβερνοχώρο φαίνεται να ωθεί τους παίκτες της κυβερνοασφάλειας να εμφανίζονται με ολοκαίνουργιους τρόπους που να εστιάζουν στους οργανισμούς τους, καθώς και στον κώδικα, το υλικό και ως εκ τούτου το cloud.

5. Οι ευπάθειες του υπολογιστικού νέφους χρειάζονται ακριβές λύσεις. Η εφεύρεση ευπαθειών στα πολλαπλά κανάλια σε μοντέρνες CPUs τα τελευταία 2 χρόνια μπορεί να δημιουργήσει υψηλό κίνδυνο για τους οργανισμούς που εκμεταλλεύονται τις υποδομές υπολογιστικού νέφους τους. Οι αντίπαλοι θα χρησιμοποιήσουν αυτή την ευπάθεια πλευρικού καναλιού για να σαρώσουν ευαίσθητες γνώσεις από διαφορετικούς κεντρικούς υπολογιστές σε έναν ισοδύναμο φυσικό διακομιστή. Υπάρχει μετριασμός για πολλές πλατφόρμες, εφαρμογές cloud και κώδικα. Ωστόσο, οι περισσότεροι μετριασμοί καταλήγουν σε μείωση των επιδόσεων, οδηγώντας σε πιθανή αύξηση των τιμών των διεργασιών για τις επιχειρήσεις.

Οι περισσότεροι ειδικοί μπορούν να συμβιβαστούν με τις απειλές ως εξωγενείς ή περιβαλλοντικούς παράγοντες, αν και στην ουσία οι πολιτικές που υπάρχουν θα μπορούσαν να εξαλείψουν την απειλητική ατμόσφαιρα (Asghari et al., 2015). Σε γενικές

γραμμές, οι απειλές ακολουθούν τις παγκόσμιες τάσεις και τις τακτικές επιθέσεις βραχυπρόθεσμα.

Διαχωρίζοντας, τα τρωτά σημεία, οι έλεγχοι και τα περιουσιακά στοιχεία είναι κυρίως ενδογενή και οι επιχειρήσεις μπορούν να τα διαχειριστούν. Ωστόσο, δεν έχει κάθε επιχείρηση άμεση διαχείριση και των 3 παραγόντων. Αρκετές ευπάθειες προέρχονται από κώδικα ή στοιχεία που παρέχονται από εξωτερικούς προμηθευτές. Με μια ισχυρή εξειδίκευση στις αγορές κώδικα και με τον στόχο της τυποποίησης, αρκετές επιχειρήσεις δεν έχουν πολλές επιλογές σε αυτό το μέρος του σχεδιασμού τους (Carr, 2003). Ομοίως, το είδος και η τιμή των στοιχείων εξαρτάται κυρίως από την επιχείρηση, το μέγεθος και το επίπεδο υιοθέτησης της τεχνολογίας. Αντίθετα, οι έλεγχοι αποτελούν κυρίως ευθύνη των μεμονωμένων επιχειρήσεων. Ως εκ τούτου, η ανάλυση κινδύνου θα έπρεπε να εξετάζει την επένδυση στην ασφάλεια ως σχετικό προσδιοριστικό παράγοντα του επιχειρηματικού κινδύνου στον κυβερνοχώρο. Ως αποτέλεσμα των επιχειρήσεων που οικοδομούν στρατηγικές επιλογές σχετικά με τις επενδύσεις τους στην ασφάλεια, οι ασφαλιστές θα έπρεπε να αντιλαμβάνονται τα επιχειρηματικά κίνητρα για την αποφυγή δυσμενών επιλογών και ηθικού κινδύνου.

Οι επιχειρήσεις δεν μπορούν πάντα να διαχειριστούν το αντίκτυπο μιας αυτοδημιούργητης επίθεσης. Ενώ οι μικροί κωδικοί πρόσβασης μπορούν κάλλιστα να αποφευχθούν με τους σωστούς ελέγχους, είναι εύκολο να αναζητηθούν παραδείγματα όπου το αντίκτυπο είναι εξωγενώς καθοδηγούμενο. Μια παραβίαση θα δημιουργήσει χειρότερη δημόσια αντίδραση εάν μια εταιρεία είναι η 1η ή η μόνη που επηρεάζεται σε έναν κλάδο. Η επικοινωνία μετά την κρίση και η αντιμετώπιση του συμβάντος είναι συχνά ζωτικής σημασίας. Παρενθετικά, η έκθεση για το εμπόριο συνεργαζόμενου βαθμού εκτιμά το κόστος των παραβιάσεων πληροφοριών ανά αρχείο μεταξύ μερικών λεπτών και 1,6 εκατομμυρίων δολαρίων (NetDiligence, 2016). Οι διακυμάνσεις μεγέθους δείχνουν ότι οι κίνδυνοι αυτού του είδους είναι δυσανάλογοι. Με την μοντελοποίηση των επιπτώσεων των παραβιάσεων της ιδιωτικής ζωής φαίνεται ότι οι ευαίσθητες πληροφορίες προκύπτουν συνήθως από τη σύνδεση των αρχείων που λείπουν με διάφορες δημόσιες ή ιδιόκτητες βάσεις δεδομένων που είναι προσβάσιμες κατά τη στιγμή της παραβίασης ή και αργότερα (Sweeney, 2002. Narayanan and Shmatikov, 2008). Οι πιθανότητες και οι συνέπειες τέτοιων γεγονότων είναι τρομερά δύσκολο να προβλεφθούν.

Εστιάζοντας στα χαρακτηριστικά σε εταιρικό επίπεδο, οι Kamiya et al (2020) διαπίστωσαν ότι σε σύγκριση με τις εταιρείες που δεν αντιμετωπίζουν κυβερνοεπιθέσεις, εκείνες που αντιμετωπίζουν κυβερνοεπιθέσεις είναι μεγαλύτερες και παλαιότερες και έχουν μεγαλύτερη παρουσία μεταξύ των εταιρειών Fortune 500. Τα ευρήματα αυτά δείχνουν ότι οι στόχοι είναι οι πιο γνωστές εταιρείες, παρά οι νεότερες και όχι τόσο δημοφιλής. Οι εταιρίες που είναι στόχοι είναι επίσης πιο κερδοφόρες και λιγότερο επικίνδυνες, έχουν μεγαλύτερες μελλοντικές ευκαιρίες ανάπτυξης, υψηλότερη μόχλευση και υψηλότερα άυλα περιουσιακά στοιχεία και επενδύουν λιγότερο σε κεφαλαιουχικές δαπάνες και δραστηριότητες E&A. Είναι σημαντικό ότι λίγοι στόχοι είναι οικονομικά περιορισμένοι. Εστιάζοντας στα ειδικά χαρακτηριστικά του κλάδου, οι Kamiya et al (2020) διαπίστωσαν ότι οι κυβερνοεπιθέσεις είναι πιο συχνές μεταξύ των επιχειρήσεων.

Τέλος, οι Kamiya et al (2020) διαπίστωσαν ότι οι εταιρείες με μεγαλύτερη εμφάνιση στον χώρο (μετρούμενη με βάση το μέγεθος της εταιρείας, τη συμμετοχή στο Fortune 500 και την ιδιοκτησία θεσμικών πακέτων), υψηλότερες αποτιμήσεις, υψηλότερες επενδυτικές αποδόσεις (ROA), υψηλότερα υλικά περιουσιακά στοιχεία και πλούτο είναι πιο πιθανό να αποτελέσουν στόχο ηλεκτρονικής επίθεσης.

Κεφάλαιο 3. Επιπτώσεις του κινδύνου στον κυβερνοχώρο

3.1 Επιπτώσεις για τους μετόχους

Η συχνότητα και ο κίνδυνος κυβερνοεπιθέσεων αυξάνονται συνεχώς. Η σχεδόν συνεχής εμφάνιση νέων επιθέσεων στις ειδήσεις ανησυχεί τόσο τα μεγάλα όσο και τα μικρά χρηματοπιστωτικά ιδρύματα. Ωστόσο, πολλές επιχειρήσεις εξακολουθούν να μην διαθέτουν επαρκή κυβερνοασφάλεια. Οι απειλές στον κυβερνοχώρο είναι ένα σοβαρό ζήτημα. Οι επιθέσεις στον κυβερνοχώρο έχουν τη δυνατότητα να διακόψουν την παροχή ενέργειας, να προκαλέσουν ζημιές σε στρατιωτικό υλικό, ακόμη και να εκθέσουν ευαίσθητες πληροφορίες. Μπορεί να οδηγήσουν στην κλοπή ανεκτίμητων ιδιωτικών πληροφοριών, όπως ιατρικά αρχεία. Μπορεί να παραλύσουν συστήματα, εμποδίζοντας την πρόσβαση σε δεδομένα, ή να παρεμβληθούν σε δίκτυα υπολογιστών και τηλεφώνων. Είναι αλήθεια ότι οι κίνδυνοι στον κυβερνοχώρο έχουν τη δυνατότητα να διαταράξουν την καθημερινή ζωή όπως την ξέρουμε.[2]

Η πλειονότητα των επιχειρήσεων και των υπό-οργανώσεών τους που χρησιμοποιούν Πληροφοριακά Συστήματα ανησυχούν για τον κυβερνοχώρο και το ενδεχόμενο παραβίασης δεδομένων που αφορά τις προσωπικές πληροφορίες των πελατών και των εργαζομένων τους. Τα περιστατικά αυτά αυξάνονται όλο και συχνότερα, με αποτέλεσμα να προκαλούνται υψηλά έξοδα για τις επιχειρήσεις. Πολλά περιστατικά παραβίασης δεδομένων έχουν αρνητικό αντίκτυπο στην κερδοφορία μιας εταιρείας. Το άμεσο κόστος για την εταιρεία από τα μη ασφαλισμένα δεδομένα συνδέεται με την αποζημίωση για τη διαρροή δεδομένων και τις έμμεσες οικονομικές απώλειες, όπως η μείωση των πωλήσεων και, κατά συνέπεια, η μείωση του μεριδίου αγοράς. Η απώλεια της εμπιστοσύνης των πελατών στην προστασία των προσωπικών τους δεδομένων, καθώς και η αύξηση των λειτουργικών δαπανών που συνδέονται με την υιοθέτηση νέων μέτρων ασφαλείας και το ενδεχόμενο συνεπούς εφαρμογής, αποτελούν παραδείγματα πρόσθετου έμμεσου κόστους. Οι επιθέσεις στον κυβερνοχώρο θα μειωθούν ως αποτέλεσμα αυτού. Μπορούμε εύκολα να συμπεράνουμε από όλα τα προηγούμενα ότι ο κυβερνοχώρος και οι κυβερνοαπειλές έχουν αρνητική επίδραση στην αγορά και στη χρηματιστηριακή αξία των μετοχών της

επηρεαζόμενης εταιρείας. Επιπλέον, η έρευνα αποκαλύπτει ότι οι επιθέσεις στον κυβερνοχώρο είναι πιο συχνές από τις αποτυχίες συστημάτων και από τα ανθρώπινα αίτια.

Μια επίθεση στον κυβερνοχώρο δεν θα οδηγήσει σε αλλαγή των επενδυτικών πολιτικών και των πολιτικών αντιστάθμισης κινδύνου, εκτός εάν έχει ως αποτέλεσμα την επανεκτίμηση του κινδύνου της επιχείρησης και εάν η επιχείρηση δεν έχει οικονομικούς περιορισμούς. Είναι σπάνιο μια επιτιθέμενη επιχείρηση να είναι οικονομικά περιορισμένη. Ωστόσο, καταγράφουμε σημαντικές αλλαγές στη δομή των αμοιβών των διευθυνόντων συμβούλων και στη σημασία της διαχείρισης κινδύνου. Τέτοιες αλλαγές έχουν νόημα για τις επιχειρήσεις εάν μια κυβερνοεπίθεση έχει ως αποτέλεσμα την επανεκτίμηση του κινδύνου και του κόστους των αρνητικών αποτελεσμάτων. Τα στοιχεία μας φτάνουν στο συμπέρασμα ότι μια κυβερνοεπίθεση οδηγεί σε επαναξιολόγηση από το συμβούλιο έκθεσης σε κίνδυνο και διάθεσης ανάληψης κινδύνου της επιχείρησης (Kamiya et al, 2018).

Οι εταιρείες που πέφτουν θύματα κυβερνοεπιθέσεων ή αντιμετωπίζουν διαφορετικά περιστατικά στον κυβερνοχώρο ενδέχεται να υποστούν σημαντικό κόστος και να υποστούν και άλλες αρνητικές συνέπειες, οι οποίες μπορεί να είναι (Securities and Exchange Commission, 2018):

- Κόστος ανάκτησης, όπως η ευθύνη για κλοπή περιουσιακών στοιχείων ή πληροφοριών, αποκατάσταση της βλάβης του συστήματος και κίνητρα για τους αγοραστές ή τους επιχειρηματικούς εταίρους σε μια προσπάθεια να διατηρήσουν τις επαφές τους μετά την επίθεση.

- Μεγάλο κόστος της ασφάλειας στον κυβερνοχώρο, το οποίο μπορεί να περιλαμβάνει την αξία της δημιουργίας αλλαγών στη δομή, την ανάπτυξη επιπλέον προσωπικού και τεχνολογιών προστασίας, την εξάσκηση των εργαζομένων και τη συμμετοχή ειδικών και τρίτων συμβούλων.

- Απώλεια εσόδων που προκύπτει από τη μη εξουσιοδοτημένη χρήση πληροφοριών ιδιοκτησίας ή την αποτυχία διατήρησης ή προσέλκυσης πελατών κατά την επίθεση.

- Διαδικαστικοί και νομικοί κίνδυνοι, καθώς και περιοριστική δράση από τις κρατικές, κεντρικές και πολιτικές αρχές.

- Υπερβολικά υψηλά ασφάλιστρα.

- Αμαύρωση του ονόματος που επηρεάζει αρνητικά την εμπιστοσύνη των πελατών ή των κεφαλαιούχων.

- Αμαύρωση της εταιρίας, στην αξία της μετοχής και συνεπώς στη μακροχρόνια τιμή των μετοχών της.

Οι μελέτες των Pirounias et al (2014) χρησιμοποίησαν τη μεθοδολογία μελέτης περιστατικών για να αναλύσουν τις επιπτώσεις των συνεχών παραβιάσεων ασφαλείας.

Το αντίκτυπο στο κόστος μιας παραβίασης ασφαλείας θεωρείται ως υποκατάστατο του συνόλου του κόστους που δημιουργείται εντός της βραχυπρόθεσμης και της μελλοντικής περιόδου. Η ποσοτικοποίηση του αντίκτυπου των περιστατικών ασφαλείας μπορεί να δημιουργήσει ευκαιρίες στον τομέα της παραγωγής πληροφορικής και επίσης το επίπεδο των επενδύσεων στην ασφάλεια της πληροφορικής. Το αντίκτυπο του κινδύνου μπορεί να ποσοτικοποιηθεί αντικειμενικά, με αποτέλεσμα να υπάρξουν πολλές ενδείξεις αξιοπιστίας στην έκθεση στον κίνδυνο. Αυτή ήταν η πρωταρχική μελέτη για τη διερεύνηση του αντίκτυπου του κόστους των επιχειρήσεων εντός της περιόδου 2008-2011. Η εποχή αυτή χαρακτηρίζεται από την μεγάλη αύξηση των επιθέσεων στον κυβερνοχώρο και από την αύξηση της πολυπλοκότητας των επιθέσεων αυτών. Το τελευταίο έτος αυτής της εποχής έχει ήδη χαρακτηριστεί ως "έτος γέννησης". Ωστόσο, η εποχή αυτή δημιούργησε τεράστιες μεταβολές εντός της αγοράς, κάτι που είχε ως αποτέλεσμα μία οικονομική κρίση. Ενώ αυτός ο συλλογισμός δεν ακυρώνει τη μεθοδολογία του γεγονότος, μειώνει την εφαρμοσμένη μαθηματική ισχύ των αποτελεσμάτων. Η μελέτη τους, χρησιμοποίησε ένα από τα μεγαλύτερα δείγματα σε σύγκριση με προηγούμενες παρόμοιες μελέτες. Ωστόσο, η αστάθεια που είναι διαδεδομένη στην αγορά τα τελευταία χρόνια υποδηλώνει ότι ένα καλό μεγαλύτερο σύνολο δεδομένων θα έπρεπε να συνυπολογιστεί στην έρευνα για την καλύτερη εγκυρότητα των αποτελεσμάτων.

Το μέσο συνολικό κόστος μιας παραβίασης ασφάλειας, λαμβάνοντας υπόψη το σύνολο του δείγματος, υπολογίζεται στα 168 έως 200 εκατομμύρια δολάρια. Το δείγμα των τεχνολογικών επιχειρήσεων έχει μέσο κόστος από 356 έως 381 εκατομμύρια δολάρια. Το κόστος αυτό διαφέρει κατά μέσο όρο 201-243 εκατ. δολάρια σε σχέση με το κόστος των μη τεχνολογικών επιχειρήσεων. Το αντίκτυπο στις μη χρηματοπιστωτικές επιχειρήσεις υπολογίζεται ότι θα κυμανθεί μεταξύ 216 και 294 εκατομμυρίων δολαρίων. Τα αποτελέσματα αυτά, σε σύγκριση με διάφορες προηγούμενες μελέτες, δείχνουν μια μείωση της ευαισθησίας των επενδυτών σε τέτοιου είδους επιθέσεις, κάτι το οποίο έχει ως

αποτέλεσμα την μείωση του κόστους των επιχειρήσεων. Ωστόσο, οι μέσες απώλειες είναι ζωτικής σημασίας και οι οργανισμοί θα πρέπει να τις λαμβάνουν υπόψη τους όταν δημιουργούν επενδυτικές επιλογές σχετικά με την ασφάλεια των δεδομένων. Επιπλέον, συγκεκριμένα σημεία στο δείγμα μας είχαν μια μεγάλη και πολύ ζωτικής σημασίας επίδραση στην κεφαλαιοποίηση. Αυτό σημαίνει ότι αν και το κοινό κόστος - από την άποψη των απωλειών - έχει μειωθεί, υπάρχει η πιθανότητα ενός φοβερά μεγάλου αριθμού περιστατικών, τα οποία μπορεί να έχουν σοβαρές επιπτώσεις στην ύπαρξη μιας εταιρείας (Musil, 2012). Τα κύρια αποτελέσματα αυτής της έρευνας ήταν ότι οι αγορές φαίνεται να έχουν ωριμάσει εντός της προσέγγισης που χειρίζονται τα συμβάντα ασφαλείας και επίσης το κόστος των ζημίων φαίνεται να σταθεροποιείται.

Οι Campbell et al (2003) εξέτασαν την αντίδραση της χρηματιστηριακής αγοράς στις παραβιάσεις ασφαλείας για μηδέν έως 3 ημέρες μετά την ανακοίνωση τους και διαπίστωσαν ότι δεν έχουν όλοι οι τύποι παραβιάσεων ασφαλείας παρόμοιες οικονομικές επιπτώσεις. Οι Cavusoglu et al (2004) διαπίστωσαν ότι η είδηση μιας παραβίασης της ασφάλειας στο διαδίκτυο είναι αρνητική στην αγοραία αξία της επιχείρησης που παραβιάστηκε. Η μελέτη τους έδειξε ότι οι εταιρείες που παραβιάστηκαν έχασαν κατά μέσο όρο 2,1% της αγοραίας αξίας τους σε διάστημα δύο ημερών από την ανακοίνωση της παραβιάσεις, και επιπλέον η απώλεια ήταν υψηλότερη για τις διαδικτυακές εταιρείες από ό,τι για τις κανονικές εταιρείες. Η μελέτη τους επιπλέον έδειξε ότι η εταιρεία ανάπτυξης διαδικτυακής ασφάλειας είχε αύξηση της αποτελεσματικότητας της μετά από την ανακοίνωση της παραβίασης. Οι Hovav & D'Arcy (2003) διερεύνησαν την αντίδραση της αγοράς στις ανακοινώσεις DOS για το χρονικό διάστημα από μία έως εικοσιπέντε ημέρες και διαπίστωσαν ότι δεν υπήρχαν σημαντικές επιπτώσεις από τις επιθέσεις DOS στην κεφαλαιαγορά. Ωστόσο, διαπίστωσαν ότι οι εταιρείες που δραστηριοποιούνται στο διαδίκτυο είχαν αρνητικές ανώμαλες αποδόσεις καθ' όλη τη διάρκεια των πέντε ημερών που ακολούθησαν από την ανακοίνωση. Από την άλλη πλευρά, οι Hovav & D'Arcy (2004) διερεύνησαν την αντίδραση της αγοράς σε ανακοινώσεις επιθέσεων από ιούς και διαπίστωσαν ότι δεν υπήρχε κανένα σημαντικό αποτέλεσμα στην περίοδο των εικοσιπέντε ημερών. Οι Garg κ.ά. (2003b) εξέτασαν επιπλέον την αντίδραση της αγοράς σε παραβιάσεις ασφαλείας και φημολογείται ότι όλα τα είδη παραβιάσεων ασφαλείας είχαν αρνητικές ανώμαλες αποδόσεις μεταξύ τριών ημερών από την ανακοίνωση. Ωστόσο, η μελέτη τους παρουσίασε ότι οι παραβιάσεις ασφαλείας σε σχέση με την κλοπή δεδομένων mastercard είχαν το σημαντικότερο αρνητικό αντίκτυπο. Επιπλέον, η αγοραία αξία των

εταιρειών ασφαλείας είχε ως αποτέλεσμα να έχει θετικό αντίκτυπο στις παραβιάσεις ασφαλείας (Ko et al, 2007).

Σε γενικές γραμμές, τα δημοσίως δηλωθέντα περιστατικά παραβίασης της ασφάλειας έχουν γιγαντιαίο αντίκτυπο στην αγοραία αξία των παραβιασμένων εταιρειών αλλά και στις θυγατρικές τους ακόμα και αρκετό χρόνο μετά από την ανακοίνωση. Ωστόσο, μέχρι στιγμής, το αντίκτυπο στην τελική χρηματοοικονομική απόδοση της προστασίας έχει επηρεάσει τις επιχειρήσεις για μια εκτεταμένη χρονική περίοδο, και δεν έχει παρ' όλα αυτά αντιμετωπιστεί (Ko et al, 2007).

3.2. Επιπτώσεις για τους ομολογιούχους

Οι Iyer et al (2019) ήταν οι πρώτοι που εξέτασαν το αντίκτυπο που είχαν οι κάτοχοι ομολόγων από τις κυβερνοεπιθέσεις. Ανακάλυψαν ότι οι αγορές ομολόγων δεν είχαν κάποιο αρνητικό αντίκτυπο από μικρού χρόνου κυβερνοεπιθέσεις. Ωστόσο, οι κάτοχοι ομολόγων χάνουν μεγάλο κεφάλαιο από την στιγμή της ανακοίνωσης των κυβερνοεπιθέσεων. Η κοινή αρνητική επίπτωση για τους κατόχους ομολόγων για το χρονικό διάστημα 1ος μήνα είναι περίπου 2%. Κατά συνέπεια, οι εταιρίες που δεν είχαν δεχθεί κάποια επίθεση αλλά είχαν σύνδεση με τους ομολογιούχους που δέχτηκαν κυβερνοεπίθεση, είχαν επιπλέον αρνητική απόδοση 2%. Αυτό μεταφράζεται σε απώλειες ύψους περίπου 3,8 εκατομμυρίων δολαρίων για κάθε ομόλογο, που είναι οικονομικά ζωτικής σημασίας. Επί του παρόντος, η ασφάλεια στον κυβερνοχώρο δεν καλύπτει τις απώλειες μετοχών ή ομολόγων. Οι μέτοχοι και οι κάτοχοι ομολόγων επωφελούνται από τη στιγμή που οι περισσότερες από τις απώλειες καλύπτονται από την κυβερνοασφάλεια, ωστόσο δεν φαίνεται να αποζημιώνονται για τη χαμένη αξία των χρηματικών τους περιουσιακών στοιχείων.

Η έρευνα αυτή επιβεβαιώνεται επιπλέον από ένα πρόσφατο άρθρο της Wall Street Journal (Rubin, 2019), το οποίο διαπίστωσε ότι αρκετές κυβερνοεπιθέσεις δεν αναφέρονται ποτέ παρά τις προσπάθειες της SEC. Με την παράβλεψη γνωστοποίησης των επιπτώσεων στα δίκτυα υπολογιστών και μέσω ανεπαρκών γνωστοποιήσεων γεγονότων, οι επιχειρήσεις ατιμάζουν τους επενδυτές όσον αφορά τις αναμφίβολα επιβλαβείς επιπτώσεις. Αυτό έχει ως αποτέλεσμα εσφαλμένες αποτιμήσεις των μετοχών και των ομολόγων της εταιρείας.

Κεφάλαιο 4. Κανονισμοί της ΕΕ για την ασφάλεια στον κυβερνοχώρο

4.1 Οδηγός στρατηγικής κυβερνητικής ασφάλειας του ENISA (ENISA, 2012)

Ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών (ENISA) είναι το εξειδικευμένο κέντρο ασφάλειας δικτύων και πληροφοριών για την Ευρωπαϊκή Ένωση, τα κράτη μέλη της, τον ιδιωτικό τομέα και τους ευρωπαίους πολίτες. Ο ENISA συνεργάζεται με αυτές τις ομάδες για να παρέχει συμβουλές και συστάσεις σχετικά με καλές πρακτικές ασφάλειας πληροφοριών. Βοηθάει τα κράτη μέλη της ΕΕ να εφαρμόσουν τη σχετική νομοθεσία της ΕΕ και να εργαστούν για τη βελτίωση της ανθεκτικότητας των ζωτικών ευρωπαϊκών υποδομών και δικτύων πληροφοριών. Ο ENISA στοχεύει να ενισχύσει την υπάρχουσα τεχνογνωσία των κρατών μελών της ΕΕ υποστηρίζοντας την ανάπτυξη μιας διασυνοριακής κοινότητας που δεσμεύεται να βελτιώσει την ασφάλεια δικτύων και πληροφοριών σε ολόκληρη την ΕΕ. Αυτός ο οδηγός προσδιορίζει τα πιο κοινά και συνεχιζόμενα τμήματα και πρακτικές στις εθνικές μεθόδους κυβερνοασφάλειας της ΕΕ και τρίτων χωρών. Ο ENISA εξετάζει τις υπάρχουσες μεθόδους για να επαληθεύσει την καταλληλότητα των σχεδιαζόμενων μέτρων για τη βελτίωση της ασφάλειας και της ανθεκτικότητας. Για να υποστηρίξει αυτήν την ανάλυση, έχει αναπτύξει οδηγίες για τους υπεύθυνους δημιουργίας πολιτικής στα κράτη μέλη που είναι περίεργοι για το πώς να διαχειριστούν τις διαδικασίες κυβερνοασφάλειας στις χώρες τους. Σε αυτή την περίπτωση, είναι γνωστό ένα συγκεκριμένο σύνολο ενεργειών. Ένας οδηγός μελέτης που κάνει διάκριση μεταξύ των ακόλουθων ενεργειών:

4.1.1 Καθορισμός οράματος, πεδίου εφαρμογής, στόχων και προτεραιοτήτων

Σκοπός της στρατηγικής για την ασφάλεια στον κυβερνοχώρο είναι να βελτιώσει τη συνολική ανθεκτικότητα και ασφάλεια των πόρων ΤΠΕ της χώρας, ώστε να εξυπηρετούνται βασικές λειτουργίες του έθνους ή της κοινωνίας στο σύνολό της. Επομένως, ο καθορισμός σαφών προσωπικών στόχων και προτεραιοτήτων είναι ζωτικής σημασίας για την επίτευξη αυτού του στόχου. Οι ακόλουθοι είναι οι σημαντικότεροι παράγοντες που πρέπει να αντιμετωπιστούν σε αυτό το στάδιο:

- Σε μια χρονική περίοδο(συνήθως 5-10 χρόνια), ο καθορισμός του στόχου και του πεδίου εφαρμογής.

- Επεξήγηση του τι είναι οι υπηρεσίες.

- Διενέργεια πλήρους εθνικής αξιολόγησης κινδύνου για τον προσδιορισμό των στόχων και του πεδίου εφαρμογής της στρατηγικής.

- Οι στόχοι ιεραρχούνται ανάλογα με την επιρροή τους στην κοινωνία, την οικονομία και τους πολίτες.

- Καταγραφή της παρούσας κατάστασης.

- Η διατύπωση συγκεκριμένων πρωτοβουλιών που θα βοηθήσουν το σχέδιο να επιτευχθεί.

4.1.2 Μελέτη των υφιστάμενων πολιτικών, κανονισμών και δυνατοτήτων

Πριν από τον καθορισμό του στόχου της στρατηγικής για την ασφάλεια στον κυβερνοχώρο, είναι σημαντικό να αξιολογηθεί η κατάσταση σε υπερεθνικό και εθνικό επίπεδο. Κατά την ολοκλήρωση αυτής της άσκησης θα πρέπει να επισημανθούν σημαντικά κενά. Η έρευνα θα πρέπει να περιλαμβάνει:

- Καταγραφή των υφιστάμενων πολιτικών για την ασφάλεια στον κυβερνοχώρο που έχουν αναπτυχθεί με την πάροδο του χρόνου (π.χ. ηλεκτρονικές επικοινωνίες, προστασία δεδομένων, ασφάλεια πληροφοριών).

- Κατάλογο όλων των κανονιστικών μέτρων που ισχύουν σε διάφορους τομείς (π.χ. υποχρεωτική αναφορά συμβάντων στον τομέα των ηλεκτρονικών επικοινωνιών).
- Καταγραφή και απαρίθμηση των υφιστάμενων δυνατοτήτων για την αντιμετώπιση απειλών κυβερνοασφάλειας (π.χ. εθνική ή κυβερνητική CERT).
- Καθορισμός της ύπαρξης υφιστάμενων δεσμευτικών ρυθμιστικών συστημάτων.
- Εξέταση των ρόλων και των καθηκόντων των σημερινών οργανισμών κυβερνοασφάλειας του δημόσιου τομέα για τον εντοπισμό επικαλύψεων και κενών.

4.1.3 Δημιουργία ενός σαφώς καθορισμένου πλαισίου διακυβέρνησης

Οι υπεύθυνοι για τη διαμόρφωση της πολιτικής θα πρέπει να οργανώσουν εθνικές ασκήσεις στον κυβερνοχώρο για την αξιολόγηση του βαθμού διαχείρισης, ελέγχου και επικοινωνίας της παρούσας δομής διακυβέρνησης, προκειμένου να αξιολογηθεί το πλαίσιο διακυβέρνησης.

4.1.4 Εντοπισμός και συμμετοχή των ενδιαφερομένων μερών

Για την επιτυχή εκτέλεση της στρατηγικής απαιτείται μεγάλος αριθμός ενδιαφερομένων. Είναι σημαντικό να ληφθεί υπόψη ο αριθμός των ενδιαφερομένων τόσο από τον εμπορικό όσο και από τον κυβερνητικό τομέα. Σε εθνικό επίπεδο, θα πρέπει επίσης να ληφθεί υπόψη ο αριθμός των μελών που συμμετέχουν στο θέμα της ασφάλειας στον κυβερνοχώρο.

4.1.5 Δημιουργία σύμπραξης δημόσιου και ιδιωτικού τομέα

Η σύμπραξη δημόσιου και ιδιωτικού τομέα αναπτύσσει ένα κοινό όραμα και στόχους, καθώς και τις ευθύνες και τις μεθόδους για την επίτευξή τους.

4.1.6 Ανταπόκριση σε γεγονότα

Τα εθνικά/κυβερνητικά CERT διαδραματίζουν ζωτικό ρόλο στην οργάνωση των αρχών σε περίπτωση παραβίασης της ασφάλειας. Είναι επίσης υπεύθυνες για τη συνεργασία με εθνικές/κυβερνητικές ομάδες από άλλα έθνη. Είναι ζωτικής σημασίας το εθνικό σχέδιο ασφάλειας στον κυβερνοχώρο να παρέχει στις CERT τα κατάλληλα εργαλεία προκειμένου να εκπληρώσουν αποτελεσματικά τα καθήκοντά τους.

4.1.7 Καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Η αποτελεσματική καταπολέμηση του εγκλήματος στον κυβερνοχώρο απαιτεί τη συνεργασία πολλών αρχών, οργανισμών και κοινοτήτων. Σε αυτό το πλαίσιο, η κατάλληλη προετοιμασία και η συντονισμένη αντίδραση για την αντιμετώπιση και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο είναι ζωτικής σημασίας. Ακολουθούν ορισμένα κοινά θέματα προς σκέψη:

- Υιοθέτηση των απαιτούμενων νόμων και επικύρωσει των διεθνών συμφωνιών που ήδη υπάρχουν.
- Δημιουργία εξειδικευμένων εθνικών κέντρων διοίκησης για το έγκλημα στον κυβερνοχώρο.

- Διασφάλιση της διαρκούς και εξειδικευμένης κατάρτισης του αστυνομικού και δικαστικού προσωπικού (π.χ. στην ψηφιακή εγκληματολογία).
- Ανταλλαγή πληροφοριών σε εθνικό και διεθνές επίπεδο για την ανάπτυξη της κατανόησης των αναδυόμενων κινδύνων κυβερνοεγκλήματος.
- Καθιέρωση ενός ενιαίου συνόλου κανόνων τήρησης αρχείων.
- Δημιουργία πλατφορμών για την προώθηση της συνεργασίας μεταξύ διαφόρων φορέων (π.χ. ομάδες CERT).
- Προώθηση της εξειδίκευσης στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο στον ιδιωτικό τομέα.
- Διαμόρφωση σχέσεων σε καινοτόμες τεχνικές ψηφιακής εγκληματολογίας με κορυφαία ακαδημαϊκά ιδρύματα και ερευνητικούς οργανισμούς.
- Προώθηση της συνεργασίας μεταξύ οργανισμών του δημόσιου και του εμπορικού τομέα για τον γρήγορο εντοπισμό του εγκλήματος στον κυβερνοχώρο.

4.1.9 Ενίσχυση των προγραμμάτων εκπαίδευσης

Η κυβερνοασφάλεια δεν αποτελεί συνήθως ένα ξεχωριστό διδακτικό θέμα, ωστόσο αποτελεί μέρος ενός προγράμματος εφαρμοσμένων επιστημών. Η ασφάλεια στον κυβερνοχώρο είναι πλέον συνδεδεμένο μεταβαλλόμενο ζήτημα που χρειάζεται συνεχή εξάσκηση και εκπαίδευση. Οι στόχοι ενός εκπαιδευτικού προγράμματος θα πρέπει να είναι:

- Βελτίωση των επιχειρησιακών ικανοτήτων του σημερινού προσωπικού ασφάλειας δεδομένων.

- Ενθάρρυνση των σπουδαστών να συμμετέχουν και στη συνέχεια να προετοιμάζονται για να εισέλθουν στην ασφάλεια στον κυβερνοχώρο.

- Εθνικά δεδομένα και εξάσκηση σχετικά με τα προβλήματα ασφάλειας και τα εκπαιδευτικά προγράμματα.

- Προσθήκη μαθημάτων ασφάλειας δεδομένων στα σχολικά προγράμματα σπουδών - όχι μόνο για εκείνα που αφορούν την εφαρμοσμένη επιστήμη, αλλά και για εκείνα που αφορούν το συγκεκριμένο επάγγελμα.

4.1.10 Οργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο

Οι υποχρεωτικές ασκήσεις αποτελούν κρίσιμα εργαλεία για την αξιολόγηση της ετοιμότητας της κοινότητας για φυσικές καταστροφές, τεχνολογικές βλάβες και επιθέσεις

στον κυβερνοχώρο. Επιτρέπουν στις αρμόδιες αρχές να κάνουν τα υπάρχοντα σχέδια έκτακτης ανάγκης, να στοχεύουν σε συγκεκριμένα τρωτά σημεία, να διευκολύνουν την ενισχυμένη συνεργασία μεταξύ διαφορετικών οργανισμών, να καθορίζουν τις αλληλεξαρτήσεις, να βελτιώνουν το στυλ και να οικοδομούν μια κουλτούρα συνεργατικής προσπάθειας.

4.1.11 Διεθνής συνεργασία

Υπάρχουν διεθνείς κίνδυνοι και αδυναμίες στην ασφάλεια στον κυβερνοχώρο. Η συνεργασία με διεθνείς εταίρους για την ανταλλαγή δεδομένων είναι κρίσιμη για τη βελτίωση της γνώσης και της αντίδρασης σε ένα μεταβαλλόμενο περιβάλλον απειλών:

- Αύξηση της διεθνούς συνεργασίας μέσω της ανταλλαγής δεδομένων (για παράδειγμα, συγκριτική ανάλυση, τεχνολογικές πληροφορίες και βασικές εκτιμήσεις απειλών).
- Συμμετοχή σε συνθήκες και συμφωνίες για την ασφάλεια δεδομένων σε διμερές, τριμερές ή διεθνές επίπεδο (π.χ. Διεθνής κώδικας δεοντολογίας για την ασφάλεια δεδομένων, Σύμβαση για την παραβίαση του δικαίου).
- Συμμετοχή σε παγκόσμιες προσπάθειες για την ανάπτυξη τυποποιημένων διαδικασιών λειτουργίας για την ανταλλαγή δεδομένων και την αντιμετώπιση σημαντικών κρίσεων.
- Ενθάρρυνση των βασικών εταίρων να συμμετέχουν σε περιφερειακές, ευρωπαϊκές και παγκόσμιες ασκήσεις ως μέθοδο προώθησης της συνεργασίας.

4.2 Εγχειρίδιο πλαισίου κυβερνητικής ασφάλειας του CCDoE του NATO[3]

Ο οδηγός έχει σχεδιαστεί για να χρησιμεύσει ως οδηγός για τους ενδιαφερόμενους φορείς στα κράτη μέλη του NATO και στις χώρες εταίρους του NATO, συμπεριλαμβανομένων των ηγετών, των νομοθετών, των ρυθμιστικών αρχών και των παρόχων υπηρεσιών Διαδικτύου, κατά την ανάπτυξη και τη βελτίωση των εθνικών πολιτικών, της νομοθεσίας και των κανονισμών, καθώς και άλλων πτυχών της εθνικής ασφάλειας στον κυβερνοχώρο. Το Εγχειρίδιο εξετάζει πολυάριθμα ζητήματα και επιλογές που πρέπει να σκεφτεί κανείς κατά την οικοδόμηση μιας εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, καθώς και ποικίλες τεχνικές και παραδείγματα βέλτιστων πρακτικών στον τομέα. Ακολουθούν ορισμένες προτεινόμενες δράσεις με βάση τη μελέτη του οδηγού:

4.2.1 Στρατιωτικές επιχειρήσεις, Στρατιωτική ασφάλεια

Οι στρατιωτικές δραστηριότητες ασφάλειας στον κυβερνοχώρο διαφέρουν από χώρα σε χώρα. Σε γενικές γραμμές, αντί να γίνονται όλες σε κάθε έθνος, η δράση αυτή μπορεί να περιλαμβάνει ένα μεγάλο εύρος συγκεκριμένων πράξεων. Αρχικά, περιλαμβάνει την "κυβερνοάμυνα" - την προστασία των συστημάτων ΤΠΕ, η οποία συνήθως γίνεται μέσω μιας ομάδας CERT/CSIRT (Computer Emergency Response Team). Δεύτερον, θα μπορούσε να ενσωματώσει τακτικές για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Τρίτον, θα μπορούσε να ενσωματώσει συγκεκριμένες ικανότητες καταπολέμησης του κυβερνοχώρου, όπως αυτές που μπορούν να χρησιμοποιηθούν τόσο σε επιχειρηματικό όσο και σε τακτικό επίπεδο. Τέλος, μπορούν να συμπεριληφθούν πρωτοβουλίες για τον εκσυγχρονισμό πιο παραδοσιακών στρατιωτικών δυνατοτήτων.

4.2.2 Άμυνα κατά του εγκλήματος στον κυβερνοχώρο

Ένα ευρύ φάσμα οργανισμών συμμετέχει στη μάχη κατά του εγκλήματος στον κυβερνοχώρο. Το Υπουργείο Δικαιοσύνης θα πρέπει να δραστηριοποιηθεί στη θέσπιση και διατήρηση της νομοθεσίας για την ασφάλεια στον κυβερνοχώρο σε εθνικό και διεθνές επίπεδο. Ένα υπουργείο πρέπει επίσης να επιβλέπει τις εξειδικευμένες αστυνομικές μονάδες. Η πρόληψη του εγκλήματος στον κυβερνοχώρο είναι επίσης ένα πολυεπίπεδο πρόβλημα. Είναι ένα θέμα διαχείρισης που επηρεάζει όλες τις κυβερνητικές υπηρεσίες και οργανισμούς. Μια αστυνομική μονάδα είναι απαραίτητη σε επιχειρησιακό/τακτικό επίπεδο για τη διερεύνηση του εγκλήματος στον κυβερνοχώρο, την παρακολούθηση και την καταδίκη των κυβερνοεγκληματιών. Θα πρέπει επίσης να καθιερωθεί σύνδεση και ανταλλαγή πληροφοριών με ξένες αστυνομικές δυνάμεις, είτε μέσω διμερούς συνεργασίας είτε μέσω τμημάτων ηλεκτρονικού εγκλήματος διεθνών αστυνομικών οργανισμών όπως η Europol και η Interpol. Η αστυνομική δύναμη μπορεί να συνεργαστεί με την εθνική ομάδα CERT και άλλους οργανισμούς για να είναι πιο επιτυχημένη.

4.2.3 Διπλωματία για το έγκλημα στον κυβερνοχώρο και διακυβέρνηση του διαδικτύου

Η εφαρμογή των διπλωματικών διαδικασιών μιας χώρας στον τομέα της παγκόσμιας κυβερνοασφάλειας είναι γνωστή ως διπλωματία του κυβερνοεγκλήματος. Αναφέρεται σε μια πολυεθνική ή διμερή δράση που αποσκοπεί στη ρύθμιση των σχέσεων μεταξύ κρατών στον κυβερνοχώρο. Τα παραδοσιακά είδη διπλωματίας, όπως ο έλεγχος των όπλων και η αντιμετώπιση των απειλών, είναι ανάλογα με τη διπλωματία του κυβερνοεγκλήματος.

4.2.4 Προστασία κρίσιμων υποδομών και διαχείριση κρίσεων κυβερνοεγκλήματος

Υπάρχει ανάγκη για μια εθνική ομάδα αντιμετώπισης εκτάκτων αναγκών στον κυβερνοχώρο (CERT/CSIRT). Σοβαρά συμβάντα στον κυβερνοχώρο μπορούν να προκαλέσουν μεγάλη κοινωνική αναστάτωση και αποσύνθεση. Εάν διαταραχθούν βασικές δραστηριότητες στον κυβερνοχώρο, τα περιστατικά που επηρεάζουν κρίσιμες υποδομές (όπως η ηλεκτρική ενέργεια και οι τηλεπικοινωνίες) μπορεί να έχουν καταστροφικές εθνικές επιπτώσεις. Τόσο στον δημόσιο όσο και στον εμπορικό τομέα, απαιτείται επίσης ο καθορισμός ή η αποδοχή προτύπων ασφάλειας πληροφοριών.

4.2.5 Συντονισμός

Οι προσπάθειες συντονισμού της κυβερνοασφάλειας πιστεύεται ότι θα βοηθήσουν στη διακυβέρνηση της εθνικής κυβερνοασφάλειας.

4.2.6 Προστασία δεδομένων και ανταλλαγή πληροφοριών

Αρκετές πρωτοβουλίες επικεντρώνονται στην προστασία των δεδομένων και την ανταλλαγή πληροφοριών. Οι κύριοι στόχοι της ανταλλαγής πληροφοριών και της προστασίας των δεδομένων είναι η πρόληψη, η θεραπεία και η αποκατάσταση. Οι πληροφορίες θα πρέπει να ανταλλάσσονται μεταξύ οργανισμών, όπως και σε ομάδες διαχείρισης κρίσεων και στα ερευνητικά ινστιτούτα. Η προστασία των δεδομένων θα πρέπει να εξετάζεται σε επίπεδο πολιτικής καθώς και κατά την εφαρμογή νέων νόμων και λειτουργιών για το έγκλημα στον κυβερνοχώρο.

4.2.7 Εκπαίδευση, ανάπτυξη και έρευνα

Όταν υπάρχει ανεπαρκής βαθμός γνώσης και εκπαίδευσης σχετικά με την ασφάλεια στον κυβερνοχώρο, μπορεί να αποτύχει σε εθνικό επίπεδο. Τα στρατηγικά/επιχειρησιακά προγράμματα ευαισθητοποίησης και εκπαίδευσης για την κυβερνοασφάλεια δεν μπορούν να υλοποιηθούν χωρίς τη συμμετοχή της εκπαίδευσης ή/και της επιστήμης. Ορισμένα από αυτά τα προγράμματα, ωστόσο, μπορούν να οργανωθούν από τον ιδιωτικό τομέα (π.χ. μια τηλεοπτική εκστρατεία κατά του phishing από χρηματοπιστωτικά ιδρύματα). Εκτός από τον τελικό πληθυσμό απαιτείται ένα πλαίσιο προπόνησης για την κυβερνοασφάλεια, ώστε να διασφαλιστεί ότι ένα ευρύ σύνολο επαγγελματιών της κυβερνοασφάλειας είναι διαθέσιμο για να βοηθήσει όλες τις επιχειρήσεις. Η ευαισθητοποίηση των βασικών υπευθύνων λήψης αποφάσεων σε όλους τους κυβερνητικούς και μη κυβερνητικούς οργανισμούς είναι εξίσου σημαντική με τη βασική εκπαίδευση. Μόνο όταν αυτοί οι

υπεύθυνοι λήψης αποφάσεων είναι απολύτως δεκτικοί μεταξύ τους μπορούν να συνεργαστούν.

4.3 Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο (ΕΚ, 2013)

Η Kathryn Aston, εκπρόσωπος της ΕΕ για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας, παρουσίασε το σχέδιο ασφάλειας της ευρωπαϊκής κυβέρνησης τον Φεβρουάριο του 2013. Η στρατηγική περιγράφει μια σειρά από στόχους για την ενίσχυση των υποδομών ΤΠ, την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και την ανάπτυξη μιας πολιτικής για το έγκλημα στον κυβερνοχώρο σε επίπεδο Ευρωπαϊκής Ένωσης. Το όραμα της στρατηγικής αυτής για την ΕΕ οργανώνεται γύρω από πέντε βασικές προτεραιότητες:

- Ανάπτυξη της ανθεκτικότητας στον κυβερνοχώρο
- Ανάπτυξη πολιτικής και δυνατοτήτων άμυνας στον κυβερνοχώρο σύμφωνα με την Κοινή Πολιτική Ασφάλειας και Άμυνας.
- Βιομηχανικοί και τεχνολογικοί πόροι για την ανάπτυξη της ασφάλειας στον κυβερνοχώρο.
- Ανάπτυξη και υποστήριξη μιας εξωτερικής κυβερνοπολιτικής σε επίπεδο Ευρωπαϊκής Ένωσης που να συνάδει με τις αρχές της.

4.3.1 Ανάπτυξη ανθεκτικότητας στον κυβερνοχώρο

Για να προωθηθεί η ανθεκτικότητα του δικτύου στην ΕΕ, κάθε δημόσιος και προσωπικός τομέας θα πρέπει να αναπτύξει τις ικανότητές του και να συνεργαστεί αποτελεσματικά.

Η στρατηγική θα έπρεπε να περιλαμβάνεται σε μια νομοθετική πρόταση που να ορίζει:

- Δημιουργία ενιαίων ελάχιστων κριτηρίων για την ασφάλεια δικτύων και δεδομένων σε εθνικό επίπεδο, τα οποία θα μπορούσαν να υποχρεώσουν τα κράτη μέλη να ορίσουν εθνικές αρμόδιες αρχές, να συγκροτήσουν επιχειρησιακή ομάδα με προκαθορισμένο αποτέλεσμα και να καταρτίσουν εθνική στρατηγική και εθνική συμφωνία συνεργασίας.
- Καθιέρωση συντονισμένων μηχανισμών παρεμβολής, ανίχνευσης και αντιμετώπισης, που επιτρέπουν την ανταλλαγή δεδομένων και την κοινή βοήθεια μεταξύ των αρμόδιων αρχών όλων των χωρών.

- Αύξηση της συμμετοχής του κράτους και του ιδιωτικού τομέα. Η συμμετοχή του ιδιωτικού τομέα στην αύξηση της ασφάλειας στον κυβερνοχώρο είναι κρίσιμη, δεδομένου ότι η μεγάλη πλειοψηφία των συστημάτων δικτύων και δεδομένων ανήκει και συντηρείται στενά.
- Τέλος, για να αναπαραχθεί η συνεργασία μεταξύ των κρατών μελών και του ιδιωτικού τομέα, απαιτούνται ασκήσεις νομοθέτησης σε επίπεδο ΕΕ.

Αύξηση της ευαισθητοποίησης του κοινού

Η κυβερνοασφάλεια είναι κάτι που μπορεί να μοιραστεί. Οι τελικοί χρήστες διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της ασφάλειας των δικτύων και των συστημάτων δεδομένων. Πρέπει να γνωρίζουν τους κινδύνους που αντιμετωπίζουν και να λαμβάνουν τις απαραίτητες προφυλάξεις για την προστασία τους.

4.3.2 Δραματική μείωση των παραβάσεων του νόμου

Για την καταπολέμηση του εγκλήματος, θα πρέπει να υπάρχουν τα κατάλληλα εταιρικά εργαλεία και ευκαιρίες και η επιβολή του νόμου θα πρέπει να υιοθετεί μια συντονισμένη και συνεργατική προσέγγιση.

Ισχυρή και αποδοτική νομοθεσία

Για την καταπολέμηση του εγκλήματος, η ΕΕ και τα κράτη μέλη της επιθυμούν ισχυρή και αποτελεσματική νομοθεσία. Η Ευρωπαϊκή Ένωση έχει ψηφίσει στο παρελθόν νόμους περί παραβατικότητας, καθώς και μια οδηγία για την πρόληψη της σεξουαλικής εκμετάλλευσης παιδιών και της πορνογραφικής λογοτεχνίας στο διαδίκτυο.

Ενισχυμένη επιχειρησιακή ικανότητα για την αντιμετώπιση της παράβασης του νόμου

Η εξέλιξη των τεχνικών παραβίασης του νόμου έχει διπλασιαστεί ταχύτατα. Η επιβολή της νομοθεσίας δεν μπορεί να καταπολεμήσει την παραβίαση του νόμου με παρωχημένα επιχειρησιακά εργαλεία. Δεν έχουν πλέον όλα τα κράτη μέλη της ΕΕ την επιχειρησιακή ικανότητα να αντιδράσουν αποτελεσματικά στην παράβαση του νόμου. Κάθε κράτος μέλος επιθυμεί να διαθέτει ισχυρές εθνικές μονάδες καταπολέμησης της απάτης.

Δημιουργία καλύτερης συνεργασίας σε επίπεδο ευρωπαϊκής ένωσης

Η ΕΕ θα στηρίξει τις προσπάθειες των κρατών μελών υποστηρίζοντας μια συντονισμένη και συνεργατική προσέγγιση με τη συμμετοχή φορέων επιβολής του νόμου, δικαστικών, δημόσιων και ιδιωτικών φορέων, τόσο εντός όσο και εκτός της ΕΕ, κατά περίπτωση.

4.3.3 Ανάπτυξη προγράμματος και δυνατοτήτων στον κυβερνοχώρο που περιλαμβάνουν το πλαίσιο της κοινής ασφάλειας και του προγράμματος

Για την αποφυγή επικαλύψεων, η ΕΕ μπορεί να διερευνήσει τις πιθανότητες του πώς η ΕΕ και οι διεθνείς οργανισμοί θα συνεργαστούν για την ενίσχυση της ανθεκτικότητας των βασικών κυβερνητικών και εναλλακτικών πληροφοριακών υποδομών στις οποίες βασίζονται τα μέλη κάθε οργανισμού.

4.3.4 Ανάπτυξη επιχειρηματικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο

Ενθάρρυνση των επενδύσεων και της επέκτασης Επενδύσεις

Η έρευνα και η ανάπτυξη θα στηρίξουν μια ισχυρή βιομηχανική πολιτική, θα προωθήσουν μια αξιόπιστη ευρωπαϊκή επιχείρηση ΤΠΕ, θα ενισχύσουν την εγχώρια αγορά και θα μειώσουν την εξάρτηση της Ευρώπης από ξένες τεχνολογίες. Η ανάλυση και η ανάπτυξη θα πρέπει να καλύψουν τα κενά στην τεχνολογία ασφάλειας ΤΠΕ, λαμβάνοντας υπόψη τις εξελισσόμενες ανάγκες των χρηστών.

4.3.5 Ανάπτυξη μιας στρατηγικής για τον εξωτερικό κυβερνοχώρο σε επίπεδο Ευρωπαϊκής Ένωσης και προώθηση των βασικών αρχών της ΕΕ

Η εξωτερική στρατηγική της ΕΕ για τον κυβερνοχώρο θα πρέπει να αναπτυχθεί από την Επιτροπή, την Ύπατη Εκπρόσωπο και τα κράτη μέλη, με στόχο την αύξηση της δέσμευσης και την ενίσχυση των σχέσεων με βασικούς διεθνείς εταίρους και οργανισμούς, καθώς και με την κοινωνία των πολιτών και τον εμπορικό τομέα.

4.4 Κριτήρια για τη δημιουργία του πλαισίου κυβερνητικής ασφάλειας

Το πρώτο καθήκον, όπως είδαμε με τον ENISA, είναι να αναπτυχθεί ένα όραμα που να καθορίζει στόχους και προτεραιότητες. Αυτό πρέπει να γίνει με γνώμονα τις υφιστάμενες πολιτικές. Ο κύριος στόχος και η προτεραιότητα του Εγχειριδίου του ΝΑΤΟ είναι να βοηθήσει τα μέλη του στην ανάπτυξη μιας στρατηγικής. Η ανάπτυξη στρατηγικών και ικανοτήτων της ΕΕ για την άμυνα στον κυβερνοχώρο, οι οποίες συνδέονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας, είναι επίσης ζωτικής σημασίας. Λαμβάνοντας αυτά υπόψη, μπορούμε να συμπεράνουμε ότι η πρώτη απαίτηση που πρέπει να ικανοποιήσουν τα έθνη είναι η ύπαρξη μιας εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, η οποία καθορίζει τους στόχους και τις δραστηριότητες που θα αναλάβει κάθε χώρα, καθώς και τους αρμόδιους φορείς και άλλα μέτρα που θα γίνουν.

Προκειμένου να επιτευχθεί ένα καλύτερο επίπεδο ασφάλειας στον κυβερνοχώρο, είναι επίσης σημαντικό για τον ENISA να μειωθεί δραστικά η εγκληματικότητα. Ένα από τα μέσα για την επίτευξη αυτού του στόχου θεωρείται η ύπαρξη ισχυρής και αποτελεσματικής νομοθεσίας. Η στρατηγική της ΕΕ επικεντρώνεται επίσης σε αυτόν τον στόχο. Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο αναφέρεται επίσης στο εγχειρίδιο του ΝΑΤΟ, το οποίο συμβάλλει στην ανάπτυξη και διατήρηση κατάλληλης νομοθεσίας. Για το λόγο αυτό, ένα δεύτερο κριτήριο αξιολόγησης που πρέπει να ληφθεί υπόψη είναι η νομική δομή κάθε χώρας.

Σύμφωνα με τον ENISA, απαιτείται επίσης η ανάπτυξη ενός σαφούς πλαισίου διακυβέρνησης του κυβερνοχώρου, ο προσδιορισμός των εμπλεκόμενων φορέων, η καθιέρωση συνεργασίας μεταξύ δημόσιων και ιδιωτικών φορέων και η ύπαρξη φορέων που θα ανταποκρίνονται σε συμβάντα κυβερνοασφάλειας και θα συμβάλλουν στη μείωσή τους. Μια από τις σημαντικές προκλήσεις που πρέπει να αντιμετωπίσει μια χώρα, σύμφωνα με το Εγχειρίδιο του ΝΑΤΟ, είναι η δημιουργία φορέων ελέγχου του εγκλήματος στον κυβερνοχώρο, καθώς και η προστασία ζωτικών υποδομών και η διαχείριση κρίσεων κυβερνοασφάλειας. Είναι επίσης ζωτικής σημασίας ο συντονισμός και η συνεργασία μεταξύ των υπηρεσιών για την ανταλλαγή πληροφοριών και την ασφάλεια των δεδομένων. Για την Ευρωπαϊκή Ένωση ο διορισμός των αρμόδιων κυβερνητικών αρχών, η εφαρμογή συντονισμένων διαδικασιών πρόληψης, ανίχνευσης και αντιμετώπισης και η εμπλοκή του ιδιωτικού τομέα είναι απαραίτητα για την επίτευξη ανθεκτικότητας στον κυβερνοχώρο. Η εξέταση της ύπαρξης αρμόδιων αρχών και οργανισμών, καθώς και της συνεργασίας τους,

μπορεί να περιγραφή ως συμπληρωματικό κριτήριο όταν τα προηγούμενα στοιχεία θεωρούνται συνδυαστικά.

Σύμφωνα με το Εγχειρίδιο του NATO, η εθνική ασφάλεια στον κυβερνοχώρο θα αποτύχει εάν δεν υπάρχει επαρκής βαθμός ευαισθητοποίησης και εκπαίδευσης. Τα προτεινόμενα βήματα του ENISA, καθώς και οι στόχοι της ΕΕ, περιλαμβάνουν την αύξηση της ευαισθητοποίησης των χρηστών και την επέκταση των προγραμμάτων εκπαίδευσης και κατάρτισης. Και οι τρεις οργανισμοί προτείνουν την ταυτόχρονη διεξαγωγή ασκήσεων κυβερνοασφάλειας. Όλα τα παρακάτω μπορούν να ταξινομηθούν ως δραστηριότητες ευαισθητοποίησης και κατάρτισης τόσο για τους ειδικούς όσο και για το ευρύ κοινό.

Τέλος, ο ENISA πιστεύει ότι η κρατική συνεργασία και η ανταλλαγή πληροφοριών είναι ζωτικής σημασίας για την καλύτερη κατανόηση και αντιμετώπιση ενός διαρκώς μεταβαλλόμενου περιβάλλοντος απειλών. Μια πολυμερής ή διμερής δράση με στόχο τη ρύθμιση των κρατικών σχέσεων στον κυβερνοχώρο περιλαμβάνεται ιδιαίτερα στο Εγχειρίδιο του NATO. Τέλος, η ΕΕ δίνει ιδιαίτερη σημασία στη συνεργασία μεταξύ των κρατών μελών, καθώς και με έθνη εκτός της ΕΕ. Κατά συνέπεια, η Διεθνής Συνεργασία θα μπορούσε να θεωρηθεί ως κριτήριο πλαισίου μελέτης.

Κεφάλαιο 5. Κανονισμοί για την ασφάλεια στον κυβερνοχώρο στην Ελλάδα

5.1 Κυβερνητική πολιτική ασφάλειας και εθνική στρατηγική

Στην Ελλάδα δεν υπάρχει επί του παρόντος εθνική στρατηγική για την κυβερνητική ασφάλεια. Οι μόνες επίσημες εθνικές στρατηγικές είναι η "Ψηφιακή στρατηγική 2006-2013" και η "Στρατηγική ψηφιακής ανάπτυξης 2014-2020", οι οποίες στοχεύουν στην αύξηση της οικονομικής παραγωγής και στη βελτίωση της ποιότητας ζωής των ανθρώπων μέσω της χρήσης της τεχνολογίας της πληροφορίας. Αν και στην τελευταία δεν υπάρχουν συγκεκριμένοι στόχοι ή στρατηγικές για την ασφάλεια στον κυβερνοχώρο, γίνεται αναφορά στην ανάγκη ενίσχυσης της εμπιστοσύνης και της ασφάλειας στο Διαδίκτυο. Η Ελλάδα, από την άλλη πλευρά, έχει δηλώσει ότι μέχρι την ολοκλήρωση της Προεδρίας της στην ΕΕ το πρώτο εξάμηνο του 2014, θα έχει υιοθετήσει ένα εθνικό σχέδιο για την ασφάλεια στον κυβερνοχώρο.

5.2 Νομοθετικό πλαίσιο

Προστασία δεδομένων προσωπικού χαρακτήρα/ιδιωτικότητας [156]

Ο νόμος 2472/1997 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθορίζει τις συνθήκες υπό τις οποίες γίνεται ο χειρισμός των δεδομένων προσωπικού χαρακτήρα και οι νομικές διαδικασίες για τη διασφάλιση των βασικών δικαιωμάτων και ελευθεριών των φυσικών προσώπων. Τα βασικά δικαιώματα και οι ελευθερίες των φυσικών προσώπων, ιδίως η ιδιωτική τους ζωή. Αναφορά από τους νόμους 2774/1999 για την προστασία των δεδομένων προσωπικού χαρακτήρα στις τηλεπικοινωνίες και 3115/2003 για τη σύσταση της Αρχής Προστασίας του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Ο νόμος 3471/2006 ψηφίστηκε στις 28 Ιουνίου 2006, ως τροποποίηση του νόμου 2472/1997, για τη θέσπιση κριτηρίων για τον χειρισμό των προσωπικών δεδομένων και τη διατήρηση του απορρήτου των τηλεπικοινωνιών. Οι απαιτήσεις των παρόχων υπηρεσιών

σε σχέση με την ασφάλεια των τηλεφωνικών υπηρεσιών περιγράφονται στο νόμο 3674/2008.

Νομοθεσία για το ηλεκτρονικό εμπόριο

Η οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου σχετικά με ορισμένα νομικά ζητήματα των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εγχώρια αγορά εφαρμόζεται από το προεδρικό διάταγμα 131/2003 για το ηλεκτρονικό εμπόριο.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες[10]

Ο νόμος 3431/2006 καθορίζει ένα ευρύ πλαίσιο για την παροχή δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελλάδα, καθώς και την πλήρη ενσωμάτωση στο εθνικό δίκαιο των κανονισμών της ΕΕ 2002/19/ΕΚ, 2002/20/ΕΚ, 2002/21/ΕΚ, 2002/22/ΕΚ και 2002/77/ΕΚ.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Ποινικός Κώδικας της Ελλάδας περιγράφει τα αδικήματα που σχετίζονται με το έγκλημα στον κυβερνοχώρο.

Άρθρο 292Α Εγκληματικές πράξεις που αποσκοπούν στην υπονόμευση της ασφάλειας των τηλεφωνικών συνδέσεων.

Άρθρο 370 Παραβίαση του απορρήτου των εγγράφων.

Άρθρο 370Α Το απόρρητο των τηλεφωνικών και προφορικών συζητήσεων έχει παραβιαστεί.

Άρθρο 370Β, άρθρο 370Γ Παραβίαση του απορρήτου προγραμμάτων - δεδομένων ηλεκτρονικού υπολογιστή.

Άρθρο 386Α Απάτη με υπολογιστή.

5.3 Αρχές και οργανώσεις

Δημόσιοι φορείς

Μαζί με τα αρμόδια υπουργεία, το Υπουργείο Υποδομών, Μεταφορών και Δικτύων είναι υπεύθυνο για τη δημιουργία πολιτικών για την ασφάλεια των δημόσιων δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών (νόμος 3431/2006). Ο οδικός χάρτης για την εφαρμογή της ηλεκτρονικής διακυβέρνησης στη χώρα σχεδιάζεται και υλοποιείται από το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης. Το Κέντρο Μελετών Ασφάλειας (ΚΕΜΕΑ) είναι ερευνητικός και συμβουλευτικός οργανισμός στο θέμα της ασφάλειας για το Υπουργείο Δημόσιας Τάξης και Προστασίας του Πολίτη. Αποτελεί την Εθνική Αρχή της χώρας για την Προστασία Κρίσιμων Υποδομών, καθώς και το Εθνικό Σημείο Επαφής της χώρας με τις αρμόδιες υπηρεσίες της Ευρωπαϊκής Επιτροπής και των κρατών μελών. Το Ελληνικό Κέντρο για την Καταπολέμηση του Ηλεκτρονικού Εγκλήματος έχει το ΚΕΜΕΑ ως ένα από τα συμβατικά του μέλη (HCCE). Το Κέντρο αποτελεί μέρος μιας πανευρωπαϊκής πρωτοβουλίας για την προώθηση της εκπαίδευσης προκειμένου να αντιμετωπιστεί η αύξηση του ηλεκτρονικού εγκλήματος. Ταυτόχρονα, το ΕΚΚΕ επιθυμεί να καταστεί κέντρο αριστείας στον τομέα της διερεύνησης του ηλεκτρονικού εγκλήματος, με βάση τη στενή συνεργασία του με το ΚΕΜΕΑ και την ερευνητική εμπειρία των μελών του. Το GCC συγκεντρώνει τις γνώσεις των εθνικών υπηρεσιών επιβολής του νόμου, της βιομηχανίας και των ακαδημιών. Η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ)[11], η Αρχή Ασφάλειας Πληροφοριών (INFOSEC) (Ν. 39/2008), η Εθνική CERT (Π.Δ. 325/2003) και η Εθνική Αρχή είναι υπεύθυνοι για την Αντιμετώπιση των Κυβερνοεπιθέσεων (Π.Δ. 325/2003). Στόχος της Αρχής είναι η αντιμετώπιση των ηλεκτρονικών επιθέσεων σε δίκτυα επικοινωνιών, εγκαταστάσεις αποθήκευσης δεδομένων και συστήματα πληροφοριών, καθώς και η πρόληψη και αντιμετώπισή τους. Είναι η αρχή που είναι υπεύθυνη για τη διασφάλιση του δημόσιου τομέα καθώς και των βασικών εθνικών υποδομών.

Σε εθνικό επίπεδο, η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (DIKYB / GEETHA)[12] έχει εκτελεστική αρμοδιότητα. Σε συνεργασία με την Εθνική Υπηρεσία Πληροφοριών, το GEETHA είναι υπεύθυνο για την έκδοση του κανονισμού εθνικής ασφάλειας (ΕΚΑ) (διάταγμα 17/1974). (ΕΥΡ). Ο ΕΚΑ εφαρμόζεται σε όλη την ελληνική επικράτεια και την κρατική διοίκηση. Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας[13] υπάγεται στο Υπουργείο Δημόσιας Τάξης και Προστασίας του Πολίτη και έχει ως στόχο να συμβάλει στην πρόληψη, διερεύνηση και δίωξη εγκλημάτων και αντικοινωνικών συμπεριφορών που διαπράττονται μέσω διαδικτυακής επικοινωνίας ή άλλων ηλεκτρονικών μεθόδων. Η Αρχή Προστασίας του Απορρήτου των Επικοινωνιών (CSA)[14] είναι αρμόδια για τη διατήρηση της

εμπιστευτικότητας και της ελεύθερης επικοινωνίας, καθώς και για την πιστοποίηση των προϊόντων ασφαλείας και τον έλεγχο των ενδιαφερομένων (νόμος 3115/2003). Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)[15] είναι υπεύθυνη για τους παρόχους υπηρεσιών ηλεκτρονικής υπογραφής (ΠΔ150/2001), καθώς και για την ακεραιότητα και τη διαθεσιμότητα των δημόσιων δικτύων επικοινωνίας - ακόμη και σε καταστάσεις έκτακτης ανάγκης. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[16] είναι υπεύθυνη για την προστασία των δεδομένων προσωπικού χαρακτήρα και την εποπτεία των ενδιαφερομένων (Ν. 2472/1997, Ν. 2774/1999).

Ομάδες περιστατικών ασφαλείας

Η εθνική CERT, NCERT-GR[17], λειτουργεί στο πλαίσιο του ΕΥΡ. Στόχος της είναι η προστασία και η καταπολέμηση των δικτύων επικοινωνίας, των εγκαταστάσεων αποθήκευσης δεδομένων και των πληροφοριακών συστημάτων από ηλεκτρονικές επιθέσεις. Είναι επίσης υπεύθυνη για τη συλλογή και ανάλυση ηλεκτρονικών δεδομένων καθώς και για την παρουσίαση πληροφοριών στις αρμόδιες αρχές. Άρθρο 6 παρ. 1 του Ν. 3649/2008 Το ΙΤΕ CERT[18] είναι μια ομάδα του Ινστιτούτου Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας-Ελλάς που παρέχει υπηρεσίες ασφάλειας πληροφοριών. Οι σημαντικότερες υπηρεσίες είναι η ειδοποίηση, η διαχείριση συμβάντων και ο συντονισμός δράσεων. Το Ελληνικό Δίκτυο Έρευνας & Τεχνολογίας (ΕΔΕΤ) και όλα τα ελληνικά πανεπιστήμια, ερευνητικά ινστιτούτα και εκπαιδευτικά δίκτυα επωφελούνται από τις υπηρεσίες διαχείρισης συμβάντων του GRNET-security CERT[19]. Το AUTH-CERT[20] είναι υπεύθυνο για τη διαχείριση συμβάντων ασφαλείας που επηρεάζουν τους χρήστες του Αριστοτελείου Πανεπιστημίου.

Ιδιωτικοί φορείς

Περισσότερες από 400 εταιρείες του κλάδου της πληροφορικής και των τηλεπικοινωνιών της χώρας είναι μέλη του Ελληνικού Συνδέσμου Επιχειρήσεων Πληροφορικής και Επικοινωνιών (ΣΕΠΕ)[21]. Βασικός στόχος του είναι η προώθηση της τεχνολογίας της πληροφορίας και των επικοινωνιών (ΤΠΕ). Επιπλέον, ο ΣΕΠΕ υπερασπίζεται τα συμφέροντα των ελληνικών επιχειρήσεων πληροφορικής και επικοινωνιών στην ελληνική κυβέρνηση και την Ευρωπαϊκή Επιτροπή.

Ακαδημαϊκοί και ερευνητικοί φορείς

Το Εργαστήριο Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου διενεργεί έρευνα σε τομείς όπως η ασφάλεια και η προστασία προσωπικών δεδομένων, το ασφαλές ηλεκτρονικό εμπόριο και την ανάπτυξη ασφαλών πληροφοριακών συστημάτων, καθώς και εμπλέκεται σε διάφορα εθνικά και διεθνή έργα ασφάλειας. Το Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών του Οικονομικού Πανεπιστημίου Αθηνών διενεργεί επίσης έρευνες σε διάφορα θέματα της ασφάλεια υπολογιστών. Το Εργαστήριο Ασφάλειας Συστημάτων του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς διενεργεί έρευνα και διδασκαλία σε πολλούς τομείς της ασφάλειας συστημάτων. Το Ελληνικό Ινστιτούτο Έρευνας και Τεχνολογίας (ΙΤΕ) είναι ένα από τα κύρια ερευνητικά ιδρύματα της χώρας, το οποίο εποπτεύεται από τη Γενική Γραμματεία Έρευνας και Τεχνολογίας (ΓΓΕΤ). Η πληροφορική και οι τηλεπικοινωνίες είναι δύο από τους τομείς έρευνας και τεχνολογίας του ΙΤΕ. Το ΙΤΕ είναι επικεφαλής του Ελληνικού Κέντρου για το Κυβερνοέγκλημα, όπου πραγματοποιεί έρευνα για την κυβερνοασφάλεια, δημοσιεύει σε έγκριτες εκδόσεις και συνέδρια και εργάζεται πάνω σε ενέργειες σχετικά με την κυβερνοασφάλεια.

Συνεργασία φορέων

Δεν υπάρχει δομημένο σχέδιο για την αλληλεπίδραση των ενδιαφερομένων φορέων στην Ελλάδα. Η Εθνική CERT είναι υπεύθυνη για το συντονισμό των ατόμων που ασχολούνται με θέματα ασφάλειας στον κυβερνοχώρο και θα πρέπει να αναφέρει τα συμβάντα χρησιμοποιώντας τα στοιχεία επικοινωνίας που παρέχονται στον ιστότοπό της. Η ίδρυση του Ελληνικού Κέντρου Καταπολέμησης Ηλεκτρονικού Εγκλήματος, από την άλλη πλευρά, αποτελεί ένα πρώτο βήμα προς την κατεύθυνση της επίσημης και συντονισμένης συνεργασίας μεταξύ των αρχών. Το ΚΕΤΕΑ, το ΙΤΕ και η Νομική Υπηρεσία του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης είναι πλέον μέλη του Κέντρου.

5.4 Δράσεις κατάρτισης και ευαισθητοποίησης

Στην Ελλάδα εφαρμόζονται διάφορες προσπάθειες ευαισθητοποίησης και ενημέρωσης, τόσο από τις αρμόδιες αρχές όσο και από εμπορικές επιχειρήσεις, ακαδημαϊκά ιδρύματα και μη κυβερνητικές οργανώσεις (ΜΚΟ). Ο δικτυακός τόπος της Ελληνικής Αρχής Προστασίας Δεδομένων περιλαμβάνει πόρους για την ευαισθητοποίηση σχετικά με τα ανεπιθύμητα μηνύματα. Οι ελληνικές τράπεζες και οι πάροχοι υπηρεσιών διαδικτύου προσφέρουν συμβουλές για την ασφάλεια στο διαδίκτυο στους ιστοτόπους τους. Το Ελληνικό Κέντρο Ασφάλειας Διαδικτύου[22], το οποίο ιδρύθηκε το 2009 με την ενσωμάτωση

των προηγούμενων κόμβων ευαισθητοποίησης Saferinternet.gr, της τηλεφωνικής γραμμής Safeline.gr και της γραμμής SUPPORT, είναι ο σημαντικότερος πάροχος πληροφοριών. Οι τρεις οργανισμοί συνεργάζονται στενά για την επίτευξη των στόχων της Ευρωπαϊκής Επιτροπής για ασφαλέστερο διαδίκτυο από το 2009. Το Κέντρο διεξάγει δραστηριότητες όπως εκδηλώσεις ενημέρωσης του κοινού, σεμινάρια για εκπαιδευτικούς, προώθηση των προβλημάτων ασφάλειας στο διαδίκτυο και στα μέσα ενημέρωσης, παραγωγή ψηφιακού και φυσικού ενημερωτικού υλικού, καθώς και τηλεοπτικές και ραδιοφωνικές διαφημίσεις. Για τη βελτίωση της ασφάλειας στο διαδίκτυο για τα παιδιά, τους εκπαιδευτικούς, τους γονείς και άλλες ευάλωτες ομάδες, εξειδικευμένοι εμπειρογνώμονες έχουν επισκεφθεί εκατοντάδες σχολεία σε όλη την Ελλάδα και έχουν δημιουργήσει μια σειρά από εγχειρίδια σωστής χρήσης του διαδικτύου. Η SafeLine συγκεντρώνει πληροφορίες σχετικά με τις αναφορές που λαμβάνει σε μηνιαία βάση. Σύμφωνα με την επίσημη κατηγοριοποίηση της INHOPE, της Ευρωπαϊκής Ένωσης Παρόχων Γραμμών Ασφαλείας, οι αναφορές χωρίζονται σε πολλές κατηγορίες. Σε μηνιαία βάση, τα στοιχεία αναρτώνται στον ιστότοπο της INHOPE, συμβάλλοντας στις διεθνείς στατιστικές που συγκεντρώνονται. Επιπλέον, ο δικτυακός τόπος SafeLine δημοσιεύει σωρευτικές στατιστικές εκθέσεις. Η Ελληνική Γραμμή Ασφαλείας συνεργάζεται στενά με τις υπηρεσίες επιβολής του νόμου, ιδίως με τη Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας. Όλες οι αναφορές παράνομου περιεχομένου διαβιβάζονται στους αρμόδιους αστυνομικούς υπαλλήλους μέσω της SafeLine. Επίσης εκπρόσωποι της Ελληνικής Αστυνομίας παίρνουν μέρος στις συμβουλευτικές συνεδριάσεις του διοικητικού συμβουλίου της Ελληνικής Γραμμής, όπου συζητούνται τρόποι καταπολέμησης της παράνομης συμπεριφοράς στο Διαδίκτυο. Σύμφωνα με πρόσφατη δημοσκόπηση, πάνω από το ήμισυ του ελληνικού πληθυσμού γνωρίζει την ύπαρξη και τον στόχο της SafeLine. Στην ιστοσελίδα της, η Δίωξη Ηλεκτρονικού Εγκλήματος παρέχει πληθώρα πληροφοριών και συμβουλών σχετικά με την ασφαλή χρήση του Διαδικτύου. Διαθέτει επίσης τη δική της σελίδα ευαισθητοποίησης, η οποία απευθύνεται κυρίως στα παιδιά και τους γονείς τους. Επιπλέον, η άσκηση κυβερνοάμυνας "Panoptis" διεξάγεται κάθε χρόνο στην Ελλάδα, με στόχο τη βελτίωση της συνεργασίας των ενδιαφερομένων φορέων. Δημόσιες υπηρεσίες, πανεπιστημιακά ιδρύματα, κρατικές υπηρεσίες ασφαλείας και ιδιωτικοί πάροχοι υπηρεσιών διαδικτύου συμμετέχουν στον έλεγχο του συνολικού δικτύου της χώρας.

5.5 Διεθνής συνεργασία

Η Ελλάδα, ως πλήρες μέλος της ΕΕ και του ΝΑΤΟ, συνμπράτη σε θέματα ασφάλειας υπολογιστών με τους αρμόδιους φορείς, όπως η Αρχή Διαχείρισης της Κυβερνοάμυνας του ΝΑΤΟ και ο ENISA, οι οποίοι βρίσκονται στην Ελλάδα. Στο πλαίσιο αυτών των σχέσεων πραγματοποιήθηκε στην Αθήνα το 2013 το 2ο Διεθνές Συνέδριο του ENISA για τη συνεργασία σε κυβερνητικές κρίσεις και ασκήσεις[23] , ενώ το 2014, στο πλαίσιο της ελληνικής Προεδρίας της ΕΕ, πραγματοποιήθηκε το Συνέδριο της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Η Ελλάδα συμμετέχει επίσης στην πανευρωπαϊκή άσκηση Cyber Europe που διοργανώνει ο ENISA (ENISA, 2012). Το ΔΙΚΥΒ/ΓΕΩΤΕΕ, καθώς και άλλες κυβερνητικές υπηρεσίες, συμμετέχουν σε ασκήσεις του ΝΑΤΟ, όπως η Cyber Coalition, η οποία διεξάγεται από το 2011. Η Ελλάδα συμμετείχε σε άσκηση κυβερνοάμυνας το 2010. (NCDEX 10). Στόχος αυτών των ασκήσεων είναι να βελτιωθούν οι διαδικασίες λήψης αποφάσεων, οι τεχνικές διαδικασίες σε επιχειρησιακό επίπεδο και η συνεργασία των μελών του ΝΑΤΟ στις προκλήσεις της κυβερνοάμυνας. Τέλος, η ομάδα CERT του Ιδρύματος Τεχνολογίας και Έρευνας-Hellas είναι μέλος του FIRST[24], του Διεθνούς Φόρουμ για τη συνεργασία ομάδων διαχείρισης εκτάκτων αναγκών.

Κεφάλαιο 6. Η επιχειρηματική σημασία των επιθέσεων στον κυβερνοχώρο

6.1 Το κόστος που συνδέεται με τις παραβιάσεις της ασφάλειας των δεδομένων

Σε μια προσπάθεια να βοηθήσουν τις επιχειρήσεις να ποσοτικοποιήσουν τις απώλειες αυτές, πολλές μελέτες έχουν υιοθετήσει μια ερευνητική προσέγγιση και έχουν ελέγξει τις αντιδράσεις της αγοράς στις παραβιάσεις της ασφάλειας των πληροφοριών των επιχειρήσεων. Ωστόσο, τα αποτελέσματα είναι μικτά και οι απώλειες που σχετίζονται με τις παραβιάσεις της ασφάλειας των πληροφοριών παραμένουν ασαφείς.

Οι Telang και Wattel (2007) διεξάγουν μια μελέτη σχετικά με την αποκάλυψη των ευπαθειών στον κώδικα υπολογιστών και δείχνουν ότι οι πωλητές λογισμικού χάνουν περίπου το 0-6% της αγοραίας τιμής τους μόλις πρόκειται για ευπάθεια. Οι Garg κ.ά. (2003) και Goel και Shawky (2009) ενσωματώνουν μια ευρύτερη κατηγορία παραβιάσεων και παρατηρούν μια στατιστικά σημαντική αρνητική απόδοση κατά την ημερομηνία του συμβάντος παραβίασης. ειδικεύοντας σε συμβάντα που ενσωματώνουν την έκθεση σε επιτεύξιμες εμπιστευτικές πληροφορίες, οι Acquisti κ.ά. (2006) και οι Gatzlaff και McCullough (2010) συμβουλεύουν ότι το αντίκτυπο μιας παραβίασης πληροφοριών στον πλούτο των επενδυτών είναι αρνητικός και στατιστικά σημαντικός. Οι Acquisti et al. (2006) συμβουλεύουν επίσης ότι οι συσσωρευμένες αρνητικές επιπτώσεις αυξάνονται κατά την διάρκεια της ημέρας αμέσως μετά την ανακοίνωση της παραβίασης, στη συνέχεια μειώνονται και πάλι και χάνουν την εφαρμοσμένη μαθηματική σημασία τους.

Σε διάκριση, οι Hovav και D'Arcy (2003) εξετάζουν την αντίδραση της χρηματιστηριακής αγοράς σε επιθέσεις DOS και δεν παρατηρούν σημαντική απώλεια της εισαγωγής για τις εταιρείες που παραβιάζουν. Ειδικευόμενοι στις κακόβουλες παραβιάσεις, οι Campbell κ.ά. (2003) δεν παρατηρούν καμία απόδειξη μιας πλήρους αρνητικής αντίδρασης της χρηματιστηριακής αγοράς στις δημόσιες ανακοινώσεις παραβιάσεων της ασφάλειας δεδομένων. Ωστόσο, βλέπουν μια εξαιρετικά δυσμενή αντίδραση της αγοράς σε

περιστατικά ασφάλειας δεδομένων που αφορούν παράνομη πρόσβαση σε προσωπικά δεδομένα. Ειδικευόμενοι σε μια ευρεία κατηγορία παραβιάσεων, οι Kannan et al. (2007) συμβουλεύουν ότι οι παραβιασμένες εταιρείες δεν αποκτούν σημαντικές αρνητικές ημιμόνιμες ή βραχυπρόθεσμες ανώμαλες αποδόσεις. Επιπροσθέτως, σημειώνουν ότι κατά την περίοδο της dot-com, οι παραβιασμένες εταιρείες παρουσίασαν υψηλότερες αρνητικές βραχυπρόθεσμες μη κανονικές αποδόσεις. Ωστόσο, οι αντιδράσεις των επενδυτών δεν διαφέρουν μεταξύ μικρότερων και μεγαλύτερων εταιρειών ή μεταξύ παραβιάσεων που σχετίζονται με την εμπιστευτικότητα, την ακεραιότητα και την ετοιμότητα.

Σε αντίθεση με τις εναλλακτικές μελέτες, οι knockout και Dorantes (2006) χρησιμοποιούν συγκριτική ανάλυση ενός πανομοιότυπου δείγματος για να αναλύσουν την επίδραση των παραβιάσεων ασφαλείας σε ένα εύρος λογιστικών μέτρων. Παρομοίως, η μελέτη των knockout και Dorantes (2006) απέδωσε ανάμεικτα αποτελέσματα. Οι δυσμενείς επιπτώσεις των παραβιάσεων διαπιστώνονται αποκλειστικά σε ορισμένα μέτρα (απόδοση του ενεργητικού), όχι όμως και σε άλλα (πωλήσεις και λειτουργικό εισόδημα). Οι ερευνητές αποδίδουν τις αντικρουόμενες πληροφορίες στα συγκριτικά μικρά μεγέθη δείγματος που χρησιμοποιήθηκαν σε αρκετές μελέτες, αλλά και στο είδος των παραβιάσεων που εξετάστηκαν από προηγούμενες μελέτες (Gatzlaff & McCullough, 2010). Πράγματι, προηγούμενες μελέτες έχουν δείξει ότι οι διαστάσεις και η κατεύθυνση της απόκρισης της αξίας των μετοχών στις ειδήσεις για παραβιάσεις της ασφάλειας των πληροφοριών εξαρτώνται από περιβαλλοντικούς παράγοντες που θυμίζουν τον χαρακτήρα της παραβίασης (τη σοβαρότητα των παραβιάσεων, τις παραβιάσεις εμπιστευτικότητας έναντι των παραβιάσεων μη εμπιστευτικότητας), τα επιχειρηματικά χαρακτηριστικά (μικρές έναντι μαζικών εταιρειών, καθαρές έναντι εταιρειών με τούβλα και αυτοκίνητα) και επίσης την ημερομηνία του γεγονότος (προηγούμενα έτη έναντι πρόσφατων ετών) (Acquisti et al. 2006- Campbell et al. 2003- Gatzlaff & McCullough, 2010- Hovav & D'Arcy, 2003- Telang, 2007). Δεδομένου ότι η αξιολόγηση του κινδύνου θα μπορούσε να είναι ένα βασικό μέρος της δημιουργίας πολιτικής και των ελέγχων της ασφάλειας των πληροφοριών (Hovav & D'Arcy, 2003), αυτά τα αντικρουόμενα ευρήματα χρειάζονται ανάλυση για να παράγουν ένα πιο ολοκληρωμένο αποτέλεσμα για τις οικονομικές συνέπειες τους και για το αν οι παραβιάσεις ασφάλειας των πληροφοριών θα οδηγήσουν σε αρνητικές νομισματικές συνέπειες για τις επιχειρήσεις που τις έχουν υποστεί.

6.2 ΕΚΕ και κίνδυνος στον κυβερνοχώρο

Ο Anderson (2001) υποστηρίζει ότι οι παραβιάσεις της ασφάλειας των δεδομένων δείχνουν την αποτυχία της εταιρείας να προστατεύσει τα ενδιαφερόμενα μέρη της από την κλοπή. Αυτό μπορεί να είναι μια μορφή προβλήματος απεικόνισης κατά την οποία η διοίκηση, η οποία προορίζεται να προστατεύσει τα ενδιαφερόμενα μέρη, δεν το πράττει ,ως εκ τούτου, γεγονός που προκαλεί ζημία στα ενδιαφερόμενα μέρη, όχι όμως άμεση ζημία στη διοίκηση. Οι εταιρείες έχουν διάφορους εσωτερικούς και εξωτερικούς ελέγχους, συγκρίσιμους με το διοικητικό συμβούλιο, την αποζημίωση των στελεχών και επίσης την αγορά της διοίκησης της εταιρείας. Μια εταιρεία με ισχυρότερη διακυβέρνηση είναι φαινομενικά σε θέση να υπερασπιστεί τον εαυτό της από παραβιάσεις πληροφοριών, χρηματοδοτώντας μέσα τους απαραίτητους πόρους για να προλάβουν μία επίθεση. Επιπλέον, οι καλά διοικούμενες εταιρείες μπορεί να έχουν βελτιωμένη ικανότητα να παρατηρούν παραβιάσεις πληροφοριών νωρίτερα, γεγονός που μπορεί να μειώσει τη σοβαρότητα της παραβίασης. Ωστόσο, αρκετές εταιρείες αναθέτουν σε τρίτους την παρεμπόδιση των παραβιάσεων πληροφοριών και την ανίχνευση εντός της ίδιας της εταιρείας(Cezar, Cavusoglu and Raghunathan, 2014). Εάν μια εταιρεία έχει αδύναμους ελέγχους, η διοίκηση μπορεί να μην αισθάνεται την ανάγκη να επενδύση στην ασφάλεια των δεδομένων.

Τα εταιρικά συμβούλια λειτουργούν ως εσωτερική διοίκηση που παρακολουθεί τα στελέχη και παρέχει στρατηγική κατεύθυνση (Gillan, 2006). Αυτή η παρακολούθηση από τα διευθυντικά στελέχη έχει ως στόχο να μειώσει τις συγκρούσεις των υπηρεσιών που προκύπτουν από τον διαχωρισμό της κατοχής και της διαχείρισης. Ο Yermack (2004) προτείνει ότι οι διευθυντές έχουν 2 κίνητρα για τη θωράκιση των μετόχων: το όνομα και την αποζημίωση. Καθώς η αξία μιας εταιρείας θα αυξάνεται, τα εξωτερικά μέλη του διοικητικού συμβουλίου γνωρίζουν υψηλότερη αποζημίωση και αύξηση των μελλοντικών θέσεων εκτός του διοικητικού συμβουλίου (λόγω της μεγεθυμένης φήμης). Αντίθετα, μόλις η αξία μειωθεί, τα μέλη του διοικητικού συμβουλίου μπορεί να χάσουν τις θέσεις τους στο διοικητικό συμβούλιο (Fich and Shivdasani, 2006).

Οι παραβιάσεις δεδομένων είναι επίσης δαπανηρές για τους διαχειριστές, επομένως είναι λογικό οι διαχειριστές να προλαμβάνουν την εμφάνισή τους. Ωστόσο, η χρηματοδότηση στην ασφάλεια των πληροφοριών είναι δαπανηρή και οι διαχειριστές μπορούν να αντισταθμίσουν αυτές τις τιμές σε σχέση με τις παραβιάσεις δεδομένων. Επιπλέον, οι διαχειριστές μπορεί να στρέφονται προς τους μετόχους παρά προς τους εργαζόμενους ή τους πελάτες που υποφέρουν από παραβιάσεις πληροφοριών. Εάν οι παραβιάσεις πληροφοριών έχουν ως αποτέλεσμα αρνητική αποτίμηση, οι διαχειριστές μπορούν να δημιουργήσουν ασφάλεια των πληροφοριών. Εάν συμβούν παραβιάσεις πληροφοριών, τα

μέλη του διοικητικού συμβουλίου είναι επίσης σε εγρήγορση για την τιμή των παραβιάσεων πληροφοριών και εφαρμόζουν μεθόδους για την ενίσχυση της διακυβέρνησης και τη μείωση της πιθανότητας πρόσθετων παραβιάσεων δεδομένων.

Το διοικητικό συμβούλιο της Yahoo έχει διορίσει συνεργαζόμενη επιτροπή ελευθέρων επαγγελματιών για να αναλύσει το ρόλο των στελεχών κατά τη διάρκεια μιας παραβίασης πληροφοριών το 2014 που συνέβη μετά από μια σημαντική παραβίαση (Seetharman and McMillan, 2017). Το διοικητικό συμβούλιο της Yahoo διαπίστωσε ότι τα ζητήματα διαχείρισης και επικοινωνίας "συνέβαλαν στην έλλειψη σωστής κατανόησης και χειρισμού του περιστατικού ασφαλείας του 2014" (Seetharman and McMillan, 2017) και διακήρυξε ότι το πρώην εταιρικό στέλεχος Marissa Mayer θα λάβει περικοπή μισθού χάρη στο χειρισμό του. Ο διορισμός της επιτροπής αλλά και η μείωση των μισθών δείχνουν ότι το διοικητικό συμβούλιο ανέλαβε την ευθύνη ως απάντηση στην παραβίαση των πληροφοριών. Ωστόσο, αυτή ήταν η δεύτερη παραβίαση πληροφοριών σε 2 χρόνια και επίσης το διοικητικό συμβούλιο μπορεί να μην είχε ενεργήσει σωστά για να μειώσει τις παραβιάσεις δεδομένων εγκαίρως για να προλάβει μια δεύτερη παραβίαση. Αν και οι παραβιάσεις πληροφοριών μπορεί να μην είναι ακριβές σε σύγκριση με την τιμή της παρεμπόδισης, κοστίζουν στους μετόχους της Yahoo 350 εκατομμύρια δολάρια, καθώς η Verizon μείωσε την αξία εξαγοράς της Yahoo τον Φεβρουάριο του 2017, όταν έγινε η αποκάλυψη της παραβίασης πληροφοριών (Seethailan και McMechanics). 2017).

Η δομή του διοικητικού συμβουλίου θα οδηγήσει σε θέματα οργάνωσης των επιχειρήσεων που μειώνουν τις τρέχουσες τιμές εν όψει των κινδύνων. Ενα μικρό διοικητικό συμβούλιο, εκτός κυριαρχίας, θα μπορούσε να παρακολουθεί στενά τη διαχείριση προς όφελος των μετόχων (Lehn, Patro και Zhao, 2009). Αυτό το κινητό συμβούλιο με τα συμφέροντα των μετόχων ως πρωταρχικό στόχο θα διασφαλίσει ότι υπάρχουν συστήματα για τη μείωση της έκθεσης σε παραβιάσεις πληροφοριών (Boone, Field, Karpoff and Raheja, 2007). Επίσης, ο πίνακας εξωτερικής κυριαρχίας θα φέρει την εξωτερική εμπειρογνωμοσύνη και την πραγματικότητα της έκθεσης σε πληροφορίες. Ενώ η δομή του πίνακα δεν μπορεί να εξαλείψει τον κίνδυνο παραβίασης πληροφοριών, ένας πίνακας που είναι ενεργός και έχει τα μέλη του ΟΗΕ να είναι τρομερά επικεντρωμένα στο όνομά τους θα διασφαλίσει ότι τα μέτρα πέρνονται γρήγορα μόλις συμβεί παραβίαση πληροφοριών. Τα μέλη του διοικητικού συμβουλίου με χρηματική εμπειρία είναι επίσης επιπλέον σε εγρήγορση για τις οικονομικές επιπτώσεις των επικίνδυνων συστημάτων πληροφοριών που οδηγούν σε παραβιάσεις. Ως εκ τούτου, έχουμε την τάση να αναμένουμε επιπλέον ελεύθερους επαγγελματίες και μικρότερα διοικητικά συμβούλια να εφαρμόσουν πολιτικές

για να μειώσουν την πιθανότητα παραβίασης πληροφοριών. Εάν συμβούν παραβιάσεις πληροφοριών, έχουμε την τάση να περιμένουμε από μη κυρίαρχα διοικητικά συμβούλια να διαφυλάξουν το όνομά τους λαμβάνοντας μέτρα για να μειώσουν την πιθανότητα νέας παραβίασης πληροφοριών. Είναι πιθανό ότι αυτά τα εξωτερικά κυρίαρχα διοικητικά συμβούλια μπορούν να λάβουν μέτρα (όπως η απόλυση του διευθύνοντος συμβούλου) για να διαφυλάξουν το όνομά τους, ωστόσο μπορεί να μην μειώσουν την πιθανότητα πρόσθετων παραβιάσεων πληροφοριών.

Τόσο ο διευθυντής όσο και ο υπεύθυνος αποζημίωσης έχουν ως αποτέλεσμα τη λήψη αποφάσεων και επομένως μπορούν να μετριάσουν τα προβλήματα της εταιρείας ή να τα κάνουν χειρότερα. Οι Denis, Hanouna και GB (2006) δείχνουν ότι η αποζημίωση με κίνητρα περιλαμβάνει μια σκοτεινή πτυχή, αυξάνοντας τον κίνδυνο κατάσχεσης από τους αποδέκτες. Οι Johnson, Ryan και Tian (2009) παρατηρούν ότι οι απατεώνες διευθύνοντες σύμβουλοι δημιουργούν μεγαλύτερα χρηματικά κίνητρα για να προσπαθήσουν να το κάνουν: Το Persons (2012) διαπιστώνει ότι η εναλλακτική λύση της αμοιβής του διευθυντή σχετίζεται πλήρως με τις περιπτώσεις απάτης, ενώ η έκταση της κατοχής μετοχών και επίσης η καταβολή χρημάτων δεν φαίνεται να αφορά την απάτη. Οι Peng και Roell (2008) παρατηρούν ότι οι πρόσθετες επιλογές μετοχών οδηγούν σε πιο ριψοκίνδυνη συμπεριφορά, με τελικό αποτέλεσμα να απαιτείται κάποια δράση. Εάν η αποζημίωση με κίνητρα καταλήγει σε υπερβολική ανάληψη κινδύνου, η διοίκηση μπορεί να επιλέξει να μειώσει τις τιμές και να αποφύγει τη σπατάλη μετρητών για να μειώσει τον κίνδυνο, σε σύγκριση με την προστασία από πιθανές παραβιάσεις πληροφοριών.

Υπάρχει ένας αυξανόμενος όγκος βιβλιογραφίας που μελετά την κοινωνική ευθύνη της εταιρείας ως συνδεδεμένη επένδυση στη διαχείριση κινδύνου. Μια εταιρεία που είναι κοινωνικά ή περιβαλλοντικά υπεύθυνη θα μπορούσε να έχει αυξημένο όνομα(Oikonomou, Brooks and Pavelin, 2014). Οι McGuire, Sundgren και Schneeweis (1988) συνιστούν ότι η χρηματοδότηση στην κοινωνική ευθύνη της εταιρείας θα μειώσει κάθε πιθανότητα επίλυσης και ρυθμιστικών ζητημάτων. Επιπλέον, οι McGuire, Sundgren και Schneeweis (1988) συνιστούν ότι πολλές κοινωνικά υπεύθυνες εταιρείες έχουν πιο σωστά ενδιαφερόμενα μέρη και θα είναι οικονομικά κερδοφόρες μέσω πλήρους επιρροής αποτελεσμάτων. Οι Eccles, Ioannou και Serafeim (2014) πιστεύουν ότι οι εταιρείες υψηλής βιωσιμότητας είναι πολύ πιθανόν να υιοθετήσουν λειτουργίες για μεγαλύτερες αποκαλύψεις, λαμβάνοντας υπόψη τα συμφέροντα των ενδιαφερόμενων μερών και να έχουν μεγαλύτερες μακροπρόθεσμες αποδόσεις.

Σε αντίθεση, οι εταιρείες που είναι κοινωνικά αναξιόπιστες θα μπορούσαν να έχουν κακό όνομα και οι ακτιβιστές θα μπορούσαν έτσι να είναι πολύ πιο πιθανό να επικεντρωθούν σε αυτές για παραβιάσεις. Οι κοινωνικές ή περιβαλλοντικές πολιτικές μπορούν επιπλέον να επηρεάσουν τις τιμές χάρη στον αυξημένο εταιρικό κίνδυνο. Η Chava (2014) διαπιστώνει ότι οι εταιρείες με υψηλότερες περιβαλλοντικές εκτιμήσεις έχουν τόσο υψηλότερες τιμές κεφαλαίου όσο και λιγότερη πρόσβαση σε κεφάλαια, γεγονός που δείχνει ότι οι περιβαλλοντικές εκτιμήσεις αποτελούν πηγή κινδύνου. Αυτοί οι οικονομικοί περιορισμοί θα οδηγήσουν τη διοίκηση να μειώσει τις κόστος της ασφάλειας. Για αυτό τον λόγο, έχουμε την τάση να αναμένουμε ότι οι επιχειρήσεις με άσχημο περιβαλλοντικό όνομα θα είναι πολύ πιο πιθανό να επικεντρωθούν σε παραβιάσεις γνώσεων.

Η παρούσα μελέτη περιλαμβάνει επίσης τις κατατάξεις των Kinder, Lydenberg, Domini analysis & Analytics (KLD) σχετικά με την ποικιλομορφία, τις σχέσεις με τους εργαζομένους, τα ανθρώπινα δικαιώματα, την ασφάλεια των προϊόντων και την κοινότητα. Οι χάκερς, ιδίως οι hacktivists, ειδικεύονται στην δημιουργία κοινωνικών προβλημάτων μόλις επιλέξουν μια εταιρεία. Ας πούμε, το 2015, οι χάκερς αυτοαποκαλούνταν το "σύμπλεγμα αντιτύπων", χαρτογραφώντας την Ashley Madison - έναν ιστότοπο αφιερωμένο στην υποστήριξη παράνομων σχέσεων - ως αποτέλεσμα του ότι οι χάκερς θεωρούσαν την τοποθέτηση ανήθικη. Οι χάκερς αποκάλυψαν προφίλ με όλες τις μυστικές σεξουαλικές φαντασιώσεις των πελατών και τις αντίστοιχες συναλλαγές με mastercard, τα πραγματικά ονόματα και τις διευθύνσεις, επιπλέον ως έγγραφα και μηνύματα ηλεκτρονικού ταχυδρομείου των εργαζομένων" (Riley, 2015). Παρομοίως, το πειρατικό σύμπλεγμα των Anonymous δημιούργησε 2 ιστότοπους της κυβέρνησης της Ουγκάντα, αντιτιθέμενο στις πολιτικές της κατά των ομοφυλοφίλων (Ford, 2012).

Εάν οι υψηλές βαθμολογίες σε οποιαδήποτε διάσταση της κοινωνικής ευθύνης των πληροφοριών KLD αυξάνουν το όνομα της εταιρείας και οι χαμηλές βαθμολογίες μειώνουν τη φήμη, έχουμε την τάση να αναμένουμε χαμηλότερες βαθμολογίες KLD. Σε περίπτωση παραβίασης της γνώσης, η διοίκηση θα μπορούσε να προσπαθήσει να αποκαταστήσει το όνομα της εταιρείας με τη δημιουργία αλλαγών σε αυτές τις εκτιμήσεις για να επεκτείνει την κατάταξή τους εντός του KLD. Οι παραβιάσεις των ανθρωπίνων δικαιωμάτων και της ασφάλειας των προϊόντων θα μπορούσαν να βρεθούν στις ειδήσεις και να επηρεάσουν τη φήμη σε ορισμένες από τις αντίθετες διαστάσεις.

Κεφάλαιο 7. Συμπεράσματα

Όλοι οι ιδιώτες και οι επιχειρήσεις υιοθετούν τεχνολογίες νέφους, ρομποτικής και τεχνητής νοημοσύνης, αλλά λίγοι συνειδητοποιούν τους κινδύνους του κυβερνοχώρου. Αν θέλετε ειρήνη, ετοιμαστείτε για πόλεμο, συμβούλευαν οι Ρωμαίοι στρατηγοί. Για πολλούς οργανισμούς, η στρατηγική διαχείριση κινδύνων στον κυβερνοχώρο παραμένει μόνο η πρόληψη. Αλλά μόνο ένας συνδυασμός πρόληψης και προγραμματισμένων στρατηγικών αντιμετώπισης σε περίπτωση πλήγματος θα μπορούσε να εξαλείψει την απώλεια δεδομένων και συνεπώς, τις οικονομικές επιπτώσεις μιας επίθεσης στον κυβερνοχώρο.

Οι επιχειρήσεις επικεντρώνονται στον πρωταρχικό τους ρόλο στη δημιουργία και την προσπάθεια με τον καλύτερο τρόπο για την επιβίωση και την κερδοφορία τους. Έτσι, είναι πιο πιθανό να παραμελήσουν την ασφάλεια. Η έλλειψη χρόνου για τα ανώτερα στελέχη να επικεντρωθούν στους κινδύνους του κυβερνοχώρου είναι ένα ζήτημα που προκαλεί ανησυχία, καθώς οι απειλές στον κυβερνοχώρο βρίσκονται σε υψηλά επίπεδα και η εμπιστοσύνη στην ικανότητα ενός οργανισμού να τις διαχειριστεί έχει μειωθεί. Με τη σωστή διαχείριση των κινδύνων του κυβερνοχώρου, όλα τα τμήματα της εταιρείας θα πρέπει να ενημερώνουν το αφεντικό τους και στη συνέχεια τα ανώτατα στελέχη της διοίκησης. Η συνεργασία του Διευθυντή Πληροφορικής (CIO), του Διευθυντή Τεχνολογίας (CTO), του Οικονομικού Διευθυντή (CFO) και του Διευθύνοντος Συμβούλου (CEO) θα έχει ως αποτέλεσμα την εξάλειψη του κινδύνου απώλειας δεδομένων και πληροφοριών και κατά συνέπεια οικονομικής ζημίας. Η ποσοτικοποίηση, η αξιολόγηση και η διαχείριση του κινδύνου και των επιπτώσεων με την υποστήριξη των εταιρικών σχέσεων και ο κρίσιμος ρόλος των υψηλόβαθμων αξιωματούχων στην ολιστική προσέγγιση του κινδύνου αυτού με την οργάνωση και το σχεδιασμό στρατηγικής πρόληψης και διαχείρισης θα επιφέρει επιπτώσεις και πιθανές επιπτώσεις. της απώλειας σε περίπτωση επιτυχίας. Η στρατηγική εστίαση της αντιμετώπισης των απειλών μέσω της συνεχούς ενημέρωσης των χρηστών σε συνδυασμό με τη βελτίωση καινοτόμων εφαρμογών και συστημάτων κυβερνοασφάλειας μπορεί να εξαλείψει την αβεβαιότητα των επιθέσεων στον κυβερνοχώρο.

Ο χρηματοπιστωτικός τομέας είναι ένας από τους κύριους στόχους των επιθέσεων στον κυβερνοχώρο. Αυτές οι επιθέσεις εκτελούνται εξαιτίας του μεγάλου όγκου συναλλαγών που γίνονται καθημερινά, αλλά και εξαιτίας του είδους των συναλλαγών ο οποίος είναι

ηλεκτρονικός. Το κόστος των εταιρειών λόγω της απώλειας δεδομένων είναι πολύ υψηλό, αν και υπάρχουν λίγα στοιχεία για τις κυβερνοεπιθέσεις στον χρηματοπιστωτικό τομέα, καθώς οι εταιρείες που επηρεάζονται δεν επιδιώκουν να τα δημοσιεύουν. Οι οικονομικές επιπτώσεις από τη δημοσιοποίηση αυτών των δεδομένων είναι πολύ μεγάλες. Ο τρόπος επίθεσης στα συστήματα των εταιρειών που έχουν πληγεί και το μέγεθος της βλάβης είναι δύσκολο να προσδιοριστούν. Στην έκθεση του Ινστιτούτου Ponemon και της IBM, η μέση συνολική δαπάνη μιας παραβίασης δεδομένων εκτιμάται σε 7,35 εκατομμύρια δολάρια για κάθε κυβερνοεπίθεση. Σε μια μεγάλη κυβερνοεπίθεση, η δαπάνη εκτοξεύεται σε εκατοντάδες εκατομμύρια. Η άμεση δαπάνη για την εταιρεία λόγω της ανεπαρκούς ασφάλειας λόγω των αγωγών, των αποζημιώσεων, των ρητρών και την κατάπαυση των συμβάσεων καθώς και το έμμεση συνέπεια της μείωσης των πωλήσεων και επαγωγικά της μείωσης του μεριδίου αγοράς λόγω της απώλειας της εμπιστοσύνης των πελατών τους και της δυσφήμισης. Είναι επίσης σημαντικό να σημειωθεί ότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) αυξάνει τα ποσά λόγω των αυστηρότερων κυρώσεων και αποζημιώσεων που πρέπει να καταβληθούν, ενώ πρέπει να υπολογιστεί το αυξημένο κόστος αποκατάστασης και αναβάθμισης των συστημάτων ασφαλείας. Οι ηλεκτρονικοί και διαδικτυακοί κίνδυνοι επηρεάζουν αρνητικά την αγορά και τη διαμόρφωση της χρηματιστηριακής αξίας της μετοχής της επιχείρησης που επηρεάζεται. Τέλος, θα πρέπει να σημειωθεί ότι το κόστος προετοιμασίας και προστασίας από επιθέσεις στον κυβερνοχώρο είναι πάντα μικρότερο από τις οικονομικές επιπτώσεις μιας επίθεσης στον κυβερνοχώρο.

Παρά τα προβλήματα και τις ανησυχίες, η μελλοντική εικόνα της διαχείρισης των κινδύνων στον κυβερνοχώρο φαίνεται ιδιαίτερα ενθαρρυντική, καθώς πιστεύεται ευρέως ότι υπάρχει τεράστιο περιθώριο ανάπτυξης. Επιπλέον, όλο και περισσότερες εταιρείες εφαρμόζουν στρατηγικές πρόληψης και αντιμετώπισης, ενώ είναι ενθαρρυντική η επέκταση των ασφαλιστικών αγορών έναντι αυτής της μορφής κινδύνου και αποτελεί ένα θέμα που απασχολεί όλο και περισσότερο την παγκόσμια επαγγελματική και επιστημονική κοινότητα. Πρόκειται για μια πολλά υποσχόμενη εναλλακτική λύση για τη διαχείριση των κινδύνων στον κυβερνοχώρο.

Θα πρέπει να γίνει κατανοητό από όλους ότι οι περικοπές στις δαπάνες για την ασφάλεια στον κυβερνοχώρο αυξάνουν τις πιθανότητες απώλειας τεράστιων χρηματικών ποσών. Η χαμηλή ασφάλεια των επιχειρήσεων δημιουργεί έφορο έδαφος για κυβερνοεπιθέσεις που έχουν στόχο την κλοπή της πνευματικής ιδιοκτησίας και των προσωπικών δεδομένων. Όλες οι επιχειρήσεις πρέπει να υπόκεινται σε νομικούς περιορισμούς και διεθνείς συμφωνίες.

Βιβλιογραφία

A. J. Duncan, S. Creese, and M. Goldsmith, "Insider attacks in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012,pp. 857-862.

Achieving resilience in the cyber ecosystem. (2014). *Insights on governance, risk and compliance, Available: http://www.ey.com*

Acquisti, A., A. Friedman, and R. Telang, 2006. Is there a cost to privacy breaches? An event study, in: *ICIS 2006 Proceedings* 94. http://aisel.aisnet.org/icis2006/94/

Asghari, H., Ciere, M. & van Eeten. M. J. G. Post-mortem of a zombie:Con_cker cleanup after six years. In USENIX Security Symposium, Washington, D. C., USA, 2015.

B. Schneier, Secrets and lies: digital security in a networked world. JohnWiley& Sons, 2011.

Berkeley A.R.M. W. (2010). A Framework for Establishing Critical Infrastructure Resilience Goals. *National Infrastructure Advisory Council, Available: https://www.dhs.gov*

Boone A.L., L.C. Field, J.M. Karpoff, and C.G. Raheja, 2007. The determinants of corporate board size and composition: An empirical analysis, *Journal of Financial Economics* 851, 66–101.

C. Wilson, "Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress." DTIC Document, 2008.

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security, 2003, **11**, 431–448.

Carr, N.G. IT doesn't matter. Harvard Business Review, May:5{12, 2003.

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, International Journal of Electronic Commerce, Fall, 2004, **9**, 1, 69-104.

Cebula, J., Popeck, M. & Young, L.A. (2014). Taxonomy of Operational Cyber Security Risks Version 2,(www.sei.cmu.edu) Carnegie Mellon University.

Cezar C., H. Cavusoglu, and S. Raghunathan, 2014. Outsourcing information security: Contracting issues and security implications, *Management Science* 60, 638–657.

Chava, S., 2014. Environmental externalities and cost of capital, *Management Science* 60, 2223–2247.

Council of Economic Advisors (CEA). (2018). The Cost of Malicious Cyber Activity to the U.S. Economy | The White House. Washington D.C. Retrieved from https://www.whitehouse.gov

Deloitte. (2017). Cyber security: everybody's imperative A guide for the C-suite and boards on guarding against cyber risks.

Denis D., P. Hanouna, and A. Sarin, 2006. Is there a dark side to incentive compensation? *Journal of Corporate Finance* 12, 467–488.

E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures.Springer, 2010, pp. 25-44.

Eccles, R.G., I. Ioannou, and G. Serafeim, 2014. The impact of corporate sustainability on organizational processes and performance, *Management Science* 60, 2835–2857.

ENISA (2012). National Cyber Security Strategies. Practical Guide on Development and Execution.

European Commission (2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS.

Fich, E. and A. Shivdasani, 2006. Are busy boards effective monitors? *The Journal of Finance* 612, 689–724.

Ford, Z., 2012. Anonymous hacks Ugandan government in retaliation for anti-LGBT policies. *Think Progress*. https://thinkprogress.org

Framework for Improving Critical Infrastructure Cybersecurity. (2017). *National Institute of Standards and Technology, Version 1.1 Draft 2.*

Garg, A., Curtis, J. & Halper, H. Quantifying the financial impact of IT security breaches, Information Management & Computer Security. 2003b, **11**, 2/3, 74-83.

Gatzlaff, K.M. and K.A. McCullough, 2010. The effect of data breaches on shareholder wealth, *Risk Management and Insurance Review* 13, 61–83.

Gillan, S., 2006. Recent developments in corporate governance: An overview, *Journal of Corporate Finance* 123, 381–402.

Goel, S. and H.A. Shawky, 2009. Estimating the market impact of security breach announcements on firm values, *Information and Management* 46, 404–410.

Grant Thornton, (2018). Taking AIM at cyber risk.

Hovav, A. & D'Arcy, J. The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review, 2003, **6,** 2, 97-121.

Hovav, A. & D'Arcy, J. The impact of virus attack announcements on the market value of firms. Information Systems Security, 2004, May/June, 32-40.

I. Naumann and G. Hogben, "Privacy features of europeaneid card specifications," Network Security, vol. 2008, no. 8, pp. 9-13, 2008.

IBM. (2016). Cyber Security Intelligence Index infographic for Healthcare.

J. M. Kizza, Guide to Computer Network Security. Springer, 2013.

Johnson, S., H. Ryan, and Y. Tian, 2009. Managerial incentives and corporate fraud: The sources of incentives matter, *Review of Finance* 13, 115–145.

Kamiya, S., Kang, J-K., and Kim, J., Milidonis, A. & Stulz, R.M. (2019) What is the Impact of Successful Cyber-attacks on Target Firms? Journal of Financial Economics, forthcoming.

Kannan, K., J. Rees, and S. Sridhar, 2007. Market reactions to information security breach announcements: An empirical analysis, *International Journal of Electronic Commerce* 12, 69–91.

Ko, M. and C. Dorantes, 2006. The impact of information security breaches on financial performance of the breached firms: An empirical investigation, *Journal of Information Technology Management* 17, 13–22.

Lehn, K., S. Patro, and M. Zhao, 2009. Composition of US corporate boards: 1935–2000, *Financial Management* 38, 747–780.

Livanis, E. (2016). Financial Aspects of Cyber Risks and Taxonomy for the Efficient Handling of These Risks. *Economic and Social Development* (Book of Proceedings),14th International Scientific Conference on Economic and Social Development, Belgrade, Serbia.

M. Kelleye, “Business Insider. The Stuxnet attack on Irans Nuclear Plant was Far more Dangerous Than Previously Thought,” http://www.businessinsider.com

Marwedel, P. & Engel, M. (2016). Cyber-Physical Systems: Opportunities, Challenges and (Some) Solutions. in 1–30. Springer International Publishing.

McGuire J., A. Sundgren, and T. Schneeweis, 1988. Corporate social responsibility and firm financial performance, *Academy of Management Journal* 31, 854–872.

Musil S. (2012). Symantec says source code stolen in 2006 hack.

Myung Ko & Kweku-Muata Osei-Bryson & Carlos Dorantes, 2009. "Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms," Information Resources Management Journal (IRMJ), IGI Global, vol. 22(2), pages 1-21, April.

Narayanan, A. and Shmatikov, V. Robust de-anonymization of large sparse datasets. In IEEE Symposium on Security and Privacy (S&P), pages 111{125, Oakland, CA, USA, 2008.

NetDiligence. NetDiligence 2016 cyber claims study. Technical report, NetDiligence, 2016.

Oikonomou, I., C. Brooks, and S. Pavelin, 2014. The effects of corporate social performance on the cost of corporate debt and credit ratings, *The Financial Review* 49, 49–75.

Peng L. and A. Roell, 2008. Executive pay and shareholder litigation, *Review of Finance* 12, 141–184.

R. K. Rainer and C. G. Cegielski, Introduction to information systems: Enabling and transforming business. JohnWiley& Sons, 2010.

Riley, C., 2015. Hackers threaten to release names from adultery website. *CNN Tech*. http://money.cnn.com/2015/07/20/technology/ashley-madison-hack/

Rubin, G. T. (2019). Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts. *Wall Street Journal,* February 26.

S Pirounias, D Mermigas, C Patsakis (2014) The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study

S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," Potentials, IEEE, vol. 21, no. 5, pp. 17-19, 2002.

Securities and Exchange Commission (2018). CF Disclosure Guidance: Commission Statement and Guidance on Public Company Cybersecurity Disclosures.

Seetharman, D. and R. McMillan, 2017. Review highlights board failures in Yahoo security breach. *The Wall Street Journal*, March 3.

SR Iyer, BJ Simkins, H Wang - Finance Research Letters, 2019 – Elsevier Cyberattacks and impact on bond valuation

Sweeney, L. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557{570, 2002.

The Cyber-Resilient Enterprise, (2015). Harnessing Your Security Intelligence. *WHITE PAPER: THE CYBER-RESILIENT ENTERPRISE*

Verizon Communications, 2014. 2014 Data breach investigations report. http://www.verizonenterprise.com

Yermack, D., 2004. Remuneration, retention, and reputation incentives for outside directors, *Journal of Finance* 59, 2281–2308.

Zaw T. and Yew R., Data breach investigations report, Verizon Media 2017