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

Διπλωματική Εργασία

ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ ΚΥΒΕΡΝΟΧΩΡΟΥ, ΤΙΜΟΛΟΓΗΣΗ ΑΣΦΑΛΙΣΤΡΟΥ & ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΕΩΝ ΣΤΟΝ ΚΛΑΔΟ ΤΗΣ ΝΑΥΤΙΛΙΑΣ

της

ΠΑΠΑΔΟΠΟΥΛΟΥ ΜΑΡΙΑΣ

Επιβλέπων Καθηγητής: Λιβάνης Ευστράτιος

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

ΝΟΕΜΒΡΙΟΣ 2019

Θα ήθελα αρχικά να ευχαριστήσω θερμά τον επιβλέπων καθηγητή της παρούσας διπλωματικής εργασίας κύριο Λιβάνη Ευστράτιο, τόσο για την παρότρυνσή του να ασχοληθώ με ένα επίκαιρο και συνάμα ενδιαφέρον θέμα, όσο και για την συνεχή καθοδήγησή του και την ενεργή παρουσία του όποτε αυτή καθίσταντο αναγκαία καθ' όλη τη διάρκεια της συγγραφής της εργασίας αυτής.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την ηθική συμπαράσταση που μου προσέφεραν και την δύναμη που αντλούσα από αυτούς όποτε το χρειαζόμουν, μέσα σε όλα αυτά τα φοιτητικά μου χρόνια.

ΠΕΡΙΛΗΨΗ

Η χρήση του διαδικτύου στην σύγχρονη πραγματικότητα θεωρείται αναγκαία και πολύτιμη για κάθε επιχείρηση ασχέτως του είδους, του μεγέθους ή της γεωγραφικής της τοποθέτησης. Τα οφέλη του είναι εύκολο να τα αναλογιστούμε μιας και τα βιώνουμε διαρκώς, όμως παράλληλα εγκυμονούν σημαντικοί κίνδυνοι και απειλέσστον καινοτόμο αυτόν τομέα που ονομάζεται κυβερνοχώρος. Σ'αυτόν τον νέο κόσμο της τεχνολογίας οποιαδήποτε επιχείρηση μπορεί να πέσει θύμα ηλεκτρονικών επιθέσεων, γνωστών και ως κυβερνοεπιθέσεων, που μπορεί να επιφέρουν καταστροφικά αποτελέσματα για την επιχείρηση, όπως η υποκλοπή και η καταστροφή δεδομένων.

Αυτή η εργασία προσπαθεί να αποσαφηνίσει τις νέες αυτές έννοιες του κυβερνοχώρου και των κυβερνοεπιθέσεων και να δώσει μια πλήρως συγκροτημένη εικόνα για το θέμα των κυβερνοεπιθέσεων μέσω μιας αναλυτικής βιβλιογραφικής επισκόπησης και της ανάλυσης των πιο πρόσφατων στατιστικών δεδομένων. Αναπτύσσεται το ζήτημα της ασφάλισης του κυβερνοχώρου αλλά και ο νέος Ευρωπαϊκός κανονισμός που διέπει την διατήρηση και μεταφορά δεδομένων. Εν συνεχεία, γίνεται μια πιο ειδική αναφορά στις κυβερνοεπιθέσεις και στον αντίκτυπό τους για τον τομέα της ναυτιλίας, η οποία ολοκληρώνεται μέσω της μελέτης τριών περιστατικών παραβίασης τεχνολογικών συστημάτων, που οδηγεί με τη σειρά της και στην εξαγωγή αρκετά σημαντικών συμπερασμάτων. Τέλος, παρουσιάζεται η πρακτική εφαρμογή της παρούσας εργασίας όπου πραγματοποιείται μια παλινδρόμηση με στοιχεία που συγκεντρώθηκαν από περιστατικά παραβίασης δεδομένων και αναλύονται τα συμπεράσματα που εξάγονται από αυτήν.

ABSTRACT

The use of the Internet in modern reality is considered necessary and valuable for any business regardless of its type, size or geographical placement. Its benefits are easy to consider because we are constantly experiencing them, but there are also important risks and threats concerning this innovative area called cyberspace. In this new technology world, any business can be a victim of online attacks, known as cyber attacks, which can bring disastrous results for the operation, such as interception and data corruption.

This paper tries to clarify these new concepts of cyber and cyber attacks and give a fully-structured insight into the cyber attacks issue through a detailed bibliographic review and analysis of the most recent statistical data. The issue of cyber-security and the new European regulation governing the preservation and transfer of data are being developed. Continuing, a more specific reference is made to cyber attacks and their impact on the maritime sector, which is completed through the study of three incidents of technology violations, which leads in turn and to export several important conclusions. Finally, the practical implementation of this paper it is presented, where a regression is performed with a data collection of incidents of data breaches that have occurred, and the inferences extracted from are being analysed.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΤΩΝ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΤΩΝ ΔΙΑΓΡΑΜΜΑΤΩΝ

Σελίδα

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Σελίδα

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1.1Σκοπός Εργασίας

Σκοπός της εργασίας αυτής είναι η βαθύτερη κατανόηση του θέματος των κυβερνοεπιθέσεων και της επίδρασής τους ειδικά στην βιομηχανία της ναυτιλίας. Για να επιτευχτείο παραπάνω στόχος γίνεται μια πρώτη γνωριμία με τους όρους που περιβάλλουν τον κυβερνοχώρο, έναν νέο και σχετικά ανεξερεύνητο τομέα και παρατίθενται μερικά πρόσφατα περιστατικά παραβίασης δεδομένων.

1.2 Ερευνητικά Ερωτήματα

Τα ερευνητικά ερωτήματα που τέθηκαν στην παρούσα εργασία είναι τα εξής:

- Επηρεάζουν την απόδοση της μετοχής των επιχειρήσεων που έχουν υποστεί κυβερνοεπίθεση, παράγοντες όπως ο κλάδος της επιχείρησης, η μέθοδος της κυβερνοεπίθεσης, η ευαισθησία των δεδομένων που παραβιάστηκαν καιτο έτος της παραβίασης;

- Ποιος είναι ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων στον κλάδο της ναυτιλίας;

- Είναι ο κλάδος της ναυτιλίας κατάλληλα προετοιμασμένος για να αντιμετωπίσει τις εκάστοτε κυβερνοεπιθέσεις;

1.3 Μεθοδολογία

Συγκεντρώθηκαν και παρουσιάστηκαν τα πιο πρόσφατα στατιστικά δεδομένα που αφορούν τις κυβερνοεπιθέσεις, δεδομένα όπως για παράδειγμα ο οικονομικός αντίκτυπός τους και οι κλάδοι που πλήττονται περισσότερο καθώς και δεδομένα γύρω από το θέμα της κυβερνοασφάλειας.

Μελετήθηκαν τρεις πρόσφατες επιθέσεις κυβερνοχώρου σε μεγάλες ναυτιλιακές εταιρίες, κάνοντας μια προσπάθεια να υπολογιστεί το κόστος των επιθέσεων αυτών αλλά και της γενικότερης επίπτωσης που είχαν οι κυβερνοεπιθέσεις στην πολιτική των εταιριών γύρω από το θέμα αυτό.

Τέλος, πραγματοποιήθηκε μια παλινδρόμηση με σκοπό να απαντηθεί το ερώτημα αν υπάρχουν μεταβλητές και ποιές είναι αυτές που επιδρούν στην απόδοση των μετοχών των εταιριών που βιώνουν παραβιάσεις δεδομένων.

1.4 Δομή Εργασίας

Η παρούσα διπλωματική εργασία μπορεί να διακριθεί σε τρία σκέλη. Στο πρώτο σκέλος γίνεται μια εκτενής και αναλυτική βιβλιογραφική επισκόπηση του θέματος του κυβερνοχώρου και των επιθέσεων που αυτός δέχεται και στο δεύτερο σκέλος η εργασία επικεντρώνεται στον κλάδο της ναυτιλίας και τους κινδύνους κυβερνοχώρου που την απειλούν. Τέλος στο τρίτο σκέλος παρουσιάζεται η πιο πρακτική προσέγγιση της εργασίας όπου πραγματοποιείται μια παλινδρόμηση με χρήση δεδομένων που συλλέχθηκαν και διεξάγονται κάποια συμπεράσματα από αυτήν.

Η βιβλιογραφική επισκόπηση καταλαμβάνει δύο διακριτά κεφάλαια, με το πρώτο να αναφέρεται στον κυβερνοχώρο, τις κυβερνοεπιθέσεις και την κυβερνοασφάλεια και με το δεύτερο να παρουσιάζει το θεσμικό πλαίσιο που αφορά τις παραβιάσεις δεδομένων. Πιο συγκεκριμένα, στο 2^{ο} κεφάλαιο περιγράφονται η έννοιες του κυβερνοχώρου και της

κυβερνοεπίθεσης, αναλύονται οι κίνδυνοι που διατρέχει ο κυβερνοχώρος, καθώς και τα κίνητρα, οι στόχοι, οι μέθοδοι και οι επιπτώσεις των κυβερνοεπιθέσεων. Τέλος, περιγράφεται μια μεθοδολογία για την αντιμετώπιση των κυβερνοεπιθέσεων και θίγεται το φλέγον θέμα της κυβερνοασφάλειας και του ασφαλίστρου αυτής.

Στο 3^{ο} κεφάλαιο, όπου συνεχίζεται η βιβλιογραφική επισκόπηση, παρουσιάζεται το θεσμικό πλαίσιο που πρέπει να εφαρμόζουν οι επιχειρήσεις που διατηρούν και διακινούν προσωπικά δεδομένα. Αναλυτικότερα, γίνεται μια ιστορική αναδρομή στα διάφορα θεσμικά πλαίσια που είχαν ισχύ μέσα στα προηγούμενα έτη, καταλήγοντας στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) που ισχύει σήμερα. Περιγράφονται τα βασικά σημεία του νέου νόμου καθώς και ο διεθνής του αντίκτυπος.

Το δεύτερο σκέλος της εργασίας που καταλαμβάνει τα δύο επόμενα κεφάλαια επικεντρώνεται αποκλειστικά στη ναυτιλιακή βιομηχανία. Στο 4^{ο} κεφάλαιο περιγράφεται η κατάσταση που επικρατεί στην ναυτιλία όσον αφορά τις κυβερνοεπιθέσεις καθώς και τα επίπεδα κυβερνοασφάλειας που διαθέτει. Στο 5^{ο} κεφάλαιο γίνεται μια μελέτη και ανάλυση των τριών πιο πρόσφατων και σοβαρών περιστατικών κυβερνοεπίθεσης που έχουν δεχθεί ναυτιλιακές επιχειρήσεις καθώς και ο αντίκτυπος των επιθέσεων αυτών στην πορεία της μετοχής τους.

Στο 6^{ο} κεφάλαιο παρουσιάζεται η συλλογή των δεδομένων από διάφορα περιστατικά παραβίασης δεδομένων που έχουν υποστεί εταιρίες για πάνω από μια δεκαετία, περιγράφεται η παλινδρόμηση που διενεργήθηκε ώστε να απαντηθεί το ερώτημα αν οι μεταβλητές που επιλέχθηκαν ως ανεξάρτητες, δηλαδή ο κλάδος, η μέθοδος, η ευαισθησία των δεδομένωνκαι το έτος, επηρεάζουν την εξαρτημένη που είναι η απόδοση της μετοχής της εταιρίας που εξετάζεται και σχολιάζονται τα αποτελέσματά της.

Τέλος, στο 7^{ο} κεφάλαιο παρατίθενται τα συμπεράσματα που προέκυψαναφενόςαπό τα διάφορα στατιστικά δεδομένα που παρουσιάστηκαν κατά τη διάρκεια όλης της εργασίας και αφετέρου από την μελέτη των τριών περιπτώσεων που μελετήθηκαν και της παλινδρόμησης που πραγματοποιήθηκε.

1.5 Συνεισφορά στην Βιβλιογραφία

Η παρούσα εργασία αποτελεί μια αρκετά σημαντική προσπάθεια να εμπλουτίσει την σχετικά περιορισμένη βιβλιογραφία γύρω από το θέμα του κυβερνοχώρου, των κυβερνοεπιθέσεων, της κυβερνοασφάλειας και των κανονισμών που διέπουν τα παραπάνω. Η παράθεση των πιο πρόσφατων στατιστικών δεδομένων αλλά και η μελέτη των περιπτώσεων και η παλινδρόμηση που παρουσιάζονται στα τελευταία κεφάλαια, οδηγούν τον αναγνώστη στην καλύτερη εμπέδωση του θέματος των κυβερνοεπιθέσεων και των κινδύνων που αυτές επιφυλάσσουν και τον εξοπλίζει καταλλήλως ώστε να μπορεί να περιορίσει στο ελάχιστο της ζημίες μιας δυνητικής κυβερνοεπίθεσης ή και ακόμη να επιφέρει την πλήρη αποφυγή της.

ΚΕΦΑΛΑΙΟ 2

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

2.1 Ορισμός Κυβερνοχώρου

Πολλοί έχουν αποπειραθεί να δώσουν έναν κοινώς αποδεκτό ορισμό για την έννοια του κυβερνοχώρου, σύμφωνα με τον F. D. Kramer έχουν δοθεί 28 διαφορετικοί ορισμοί για τον όρο "κυβερνοχώρος" παρ' όλα αυτά, κανένας ορισμός δεν έχει γίνει ευρέως αποδεκτός από όλες τις κυβερνήσεις παγκοσμίως.

Ο πιο πρόσφατος ορισμός της παραπάνω έννοιας είναι ο εξής:
Ο Κυβερνοχώρος είναι ένας παγκόσμιοστομέας που υπόκειται σε συνεχή αλλαγή και χαρακτηρίζεται από τη συνδυασμένη χρήση των ηλεκτρονίων και του ηλεκτρομαγνητικού φάσματος, σκοπός του οποίου είναι να δημιουργήσει, αποθηκεύσει, τροποποιήσει, ανταλλάξει, διανέμει, εξάγει, χρησιμοποιήσει, καθώς και ναεξαλείψει πληροφορίες και να διαταράξει τους φυσικούς πόρους. Ο κυβερνοχώρος περιλαμβάνει: α) φυσικές υποδομές και συσκευές τηλεπικοινωνιών που επιτρέπουν τη σύνδεση τεχνολογικών δικτύων και δικτύων επικοινωνίας, όπως τις ξέρουμε με την ευρύτερη έννοια (συσκευές SCADA, smartphones/tablets, υπολογιστές, διακομιστές κλπ.) β) συστήματα ηλεκτρονικών υπολογιστών (βλέπε σημείο α)) και το σχετικό (μερικές φορές ενσωματωμένο) λογισμικό που εγγυάται τη βασική επιχειρησιακή λειτουργία και συνδεσιμότητα του τομέα, γ) δίκτυα μεταξύ συστημάτων ηλεκτρονικών υπολογιστών, δ) δίκτυα δικτύων που συνδέουν συστήματα ηλεκτρονικών υπολογιστών (η διάκριση μεταξύ δικτύων και δικτύων δικτύων είναι κυρίως οργανωτική), ε) τους κόμβους πρόσβασης των χρηστών και των διαμεσολαβητών δρομολόγησης κόμβων και στ) τα συστατικά δεδομένα (ή τα δεδομένα των πολιτών). Ένα διακριτικό και συστατικό χαρακτηριστικό του κυβερνοχώρου είναι ότι καμία κεντρική οντότητα δεν ασκεί έλεγχο σε όλα τα δίκτυα που αποτελούν αυτόν τον νέο τομέα[1].

[1] Mayer, M., Martino, L., Mazurier, P. & Tzvetkova, G. (2014), "*How would you define Cyberspace?*" working paper

Οι από Κοινού Αρχηγοί Προσωπικού του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών ορίζουν τον κυβερνοχώρο ως έναν από τους πέντε αλληλεξαρτώμενους τομείς, ενώ οι υπόλοιποι τέσσερις είναι η γη, ο αέρας, η ναυτιλία και το διάστημα[2].

2.2 Κίνδυνοι Κυβερνοχώρου

Οι κίνδυνοικυβερνοχώρουεντάσσονται στους λειτουργικούς κινδύνους στους οποίους εκτίθενται οι επιχειρήσεις.Συγκεκριμένα, οι κίνδυνοι κυβερνοχώρου αναφέρονται στην πιθανή ζημία που μπορεί να προκληθεί από μη εξουσιοδοτημένη χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή δεδομένων και / ή συστημάτων πληροφοριών και επικοινωνιών ενός οργανισμού[3].

Οι λειτουργικοί κίνδυνοι κυβερνοχώρου ορίζονται ως οι λειτουργικοί κίνδυνοι των πληροφοριών και των τεχνολογικών περιουσιακών στοιχείων, που κατά συνέπεια επηρεάζουν την εμπιστευτικότητα, τη διαθεσιμότητα ή την ακεραιότητα των πληροφοριών ή των πληροφοριακών συστημάτων[4]. Στον παρακάτω πίνακα παρουσιάζονται οι πηγές των κινδύνων κυβερνοχώρου, οι οποίες κατηγοριοποιούνται σε τέσσερις *κλάσεις*: α) δράσεις ανθρώπων, β) αποτυχίες συστημάτων και τεχνολογίας, γ) αποτυχημένες εσωτερικέςδιαδικασίες, και δ) εξωτερικά γεγονότα. Κάθε κλάση χωρίζεται σε επιμέρους *υποκατηγορίες*, οι οποίες χαρακτηρίζονται από τα *στοιχεία* τους[5].

---

[2] *"DoD Joint Publication 3-12(R) Cyberspace Operations (5 February 2013)"*

[3] LivanisE. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[4] Cebula, J.J& Young, L.R. (2010), "*A Taxonomy of Operational CyberSecurity Risks*", Technical Note CMU/SEI-2010-TN-028, CEPT Carnegie Mellon University

[5] Cebula, J.J& Young, L.R. (2010), "*A Taxonomy of Operational CyberSecurity Risks*", Technical Note CMU/SEI-2010-TN-028, CEPT Carnegie Mellon University

Πίνακας 1: Κατηγοριοποίησητων Πηγών των Κινδύνων Κυβερνοχώρου.

ΚΑΤΗΓΟΡΙΑ	ΥΠΟΚΑΤΗΓΟΡΙΑ	ΣΤΟΙΧΕΙΑ	
1. Ανθρώπινη Δράση	**1.1 Ακούσια**	1.1.1 Λάθη 1.1.2 Σφάλματα 1.1.3 Παραλήψεις	
	1.2 Εσκεμμένη	1.2.1 Απάτη 1.2.2 Σαμποτάζ 1.2.3 Κλοπή 1.2.4 Βανδαλισμός	
	1.3 Αδρανής	1.3.1 Ελλιπής Δεξιότητες 1.3.2 Ελλιπής Γνώση 1.3.3 Ελλιπής Καθοδήγηση 1.3.4 Ελλιπής Διαθεσιμότητα	
2. Αποτυχία Συστημάτων & Τεχνολογίας	**2.1 Υλική**	2.1.1 Χωρητικότητα 2.1.2 Επίδοση 2.1.3 Συντήρηση 2.1.4 Παλαιότητα	
	2.2 Λογισμική	2.2.1 Συμβατότητα 2.2.2 Διαχείριση Διαμόρφωσης 2.2.3 Έλεγχος αλλαγών 2.2.4 Ρυθμίσεις ασφάλειας	2.2.5 Πρακτικές Κωδικοποίησης 2.2.6 Έλεγχοι
	2.3 Συστήματος	2.3.1 Σχεδιασμός 2.3.2 Προδιαγραφές 2.3.3 Ολοκλήρωση 2.3.4 Πολυπλοκότητα	
3. Αποτυχημένες Εσωτερικές Διαδικασίες	**3.1 Σχεδιασμός ή Εκτέλεση Διαδικασίας**	3.1.1 Ροή Διαδικασίας 3.1.2 Τεκμηρίωση Διαδικασίας 3.1.3 Ρόλοι & Ευθύνες 3.1.4 Γνωστοποιήσεις & Προειδοποιήσεις	3.1.5 Ροή Πληροφοριών 3.1.6 Κλιμάκωση Ζητημάτων 3.1.7 Μεταβίβαση Εργασιών 3.1.8 Συμφωνίες σε Επίπεδο Υπηρεσιών
	3.2 Έλεγχοι Διαδικασίας	3.2.1 Παρακολούθηση τηςΚατάστασης 3.2.2 Μετρήσεις 3.2.3 Περιοδική Αναθεώρηση 3.2.4 Κυριότητα τωνΔιαδικασιών	
	3.3 Υποστηρικτικές Διαδικασίες	3.3.1 Στελέχωση 3.3.2 Χρηματοδότηση	

		3.3.3 Εκπαίδευση &Ανάπτυξη 3.3.4 Προμήθευση	
4. Εξωτερικά Γεγονότα	**4.1 Καταστροφές**	4.1.1 Καιρικά Φαινόμενα 4.1.2 Φωτιές 4.1.3 Πλημμύρες 4.1.4 Σεισμοί	4.1.5 Αναταραχές 4.1.6 Πανδημίες
	4.2 Νομικά Ζητήματα	4.2.1 Κανονιστική Συμμόρφωση 4.2.2 Νομοθεσία 4.2.3 Αντιδικίες	
	4.3 Επιχειρηματικά Ζητήματα	4.3.1 Αποτυχία Προμηθευτή 4.3.2 Συνθήκες Αγοράς 4.3.3 Συνθήκες Οικονομίας	
	4.4 Αλληλο-εξαρτώμενες Υπηρεσίες	4.1.1 Βοηθητικές Υπηρεσίες 4.1.2 Υπηρεσίες Εκτάκτου Ανάγκης 4.1.3 Καύσιμα 4.1.4 Μεταφορά	

Πηγή: Cebula, J.J & Young, L.R. (2010), "*A Taxonomy of Operational CyberSecurity Risks*", Technical Note CMU/SEI-2010-TN-028, CEPT Carnegie Mellon University

Αναλύοντας τον παραπάνω πίνακα, ως πρώτη κλάση έχουμε την *Ανθρώπινη Δράση* η οποία χαρακτηρίζει τις κινήσεις που πραγματοποίησαν ή όχι κάποια άτομα, σε δεδομένες καταστάσεις. Περιλαμβάνονται κινήσεις που γίνανε είτε από άτομα που βρίσκονται εντός της επιχείρησης, είτε εκτός. Στις υποκατηγορίες αυτής της κλάσης, συναντάμε αρχικά της *δράσεις που έγιναν ακούσια* (συνήθως πραγματώνονται από άτομα που βρίσκονται στο εσωτερικό της επιχείρησης) και είναι κινήσεις που γίνανε χωρίς κακόβουλο σκοπό, τέτοιες δράσεις είναι τα λάθη απροσεξίας, τα σφάλματα άγνοιας και οι παραλήψεις λόγω βιασύνης. Μια δεύτερη υποκατηγορία της προαναφερθείσας κλάσης είναι οι *εσκεμμένες δράσεις* (αυτού του είδους οι δράσεις μπορούν να πραγματοποιηθούν και από άτομα εντός της επιχείρησης, αλλά και εκτός αυτής -όπως εγκληματίες, ακτιβιστές, τρομοκράτες, κυβερνήσεις και κατασκόπους[6]). Είναι κινήσεις που έχουν γίνει εσκεμμένα με απώτερο σκοπό να βλάψουν την ίδια την εταιρία, σ' αυτές συγκαταλέγονται η απάτη, το σαμποτάζ, η κλοπή και ο

[6]Livanis, E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

βανδαλισμός. Ενδιαφέρον αποτελεί σύμφωνα με την έρευνα της CSO ότι μόλις το 25% των κυβερνοεπιθέσεων προκλήθηκαν από άτομα που δουλεύουν στην επιχείρηση, εκ των οποίων το 36% λέγεται ότι οφείλεται σε ατυχήματα και μη σκόπιμες ενέργειες[7]. Τέλος, έχουμε την υποκατηγορία της *αδράνειας* η οποία περιγράφει την έλλειψη δράσης ή την αποτυχία να αποτραπεί κάποια κακόβουλη δράση σε μια δεδομένη στιγμή. Η έλλειψη δεξιοτήτων, γνώσης, καθοδήγησης και διαθεσιμότητας του κατάλληλου ατόμου μπορούν να καταλογιστούν ως αδράνεια αποφυγής των ενδεχόμενων κινδύνων.

Στην δεύτερη κλάση συναντάμε την *Αποτυχία Συστημάτων & Τεχνολογίας* η οποία περιγράφει μια κατηγορία λειτουργικών κινδύνων που χαρακτηρίζονται από προβληματικές, ασυνήθης και αναπάντεχες λειτουργίες των τεχνολογικών περιουσιακών στοιχείων που κατέχει μια επιχείρηση. Στις υποκατηγορίες της έχουμε τις *υλικές αποτυχίες* (hardwarefailure) που αφορούν τις ενδεχόμενες αποτυχίες του φυσικού εξοπλισμού λόγω χωρητικότητας, επίδοσης, κτλ., καθώς και *λογισμικές αποτυχίες* (softwarefailure) που μπορούν να προκύψουν σε κάθε λογής λογισμικό περιουσιακό στοιχείο, παραδείγματος χάρη προγράμματα και λειτουργικά συστήματα. Τέτοιες αποτυχίες είναι η συμβατότητα κάποιων στοιχείων του λογισμικού καθώς και οι ακατάλληλες ρυθμίσεις ασφαλείας μέσα σε ένα πρόγραμμα. Η Τρίτη υποκατηγορία αναφέρεται στις *αποτυχίες των συστημάτων*, δηλαδή στην ανικανότητα τα ενσωματωμένα συστήματα να εκτελέσουν τις προσδοκώμενες λειτουργίες τους. Μερικές από αυτές τις αποτυχίες είναι ο σχεδιασμός του ίδιου του συστήματος και η πολυπλοκότητά του.

Ως τρίτη κλάση έχουμε τις *Αποτυχημένες Εσωτερικές Διαδικασίες* οι οποίες αποτελούν τους λειτουργικούς κινδύνους που είναι συσχετισμένοι με την αποτυχία των εσωτερικών διαδικασιών να διενεργηθούν όπως θα έπρεπε ή αναμενόταν. Στις υποκατηγορίες περιλαμβάνονται οι *αποτυχίες στον σχεδιασμό και την εκτέλεση της διαδικασίας* που αφορούν αποτυχίες της διαδικασίας να επιτύχει τα προσδοκώμενα αποτελέσματα λόγω κακού σχεδιασμού της για το συγκεκριμένο έργο ή κακής εκτέλεσης μιας καλά σχεδιασμένης διαδικασίας. Τέτοιες αποτυχίες για παράδειγμα είναι η ροή της διαδικασίας και των πληροφοριών. Μια δεύτερη υποκατηγορία είναι οι *αποτυχίες των ελέγχων διαδικασίας* που κρίνονται ανεπαρκής, όπως οι μετρήσεις και η παρακολούθηση της

[7] The 2018 U.S. State of Cybercrime Study, CSO and CERT Division of Software Engineering Institute at Carnegie Mellon University

κατάστασης της διαδικασίας. Τέλος, συναντάμε τις *αποτυχίες των υποστηρικτικών διαδικασιών*, όπως είναι η κατάλληλη στελέχωση και χρηματοδότηση.

Ως τέταρτη και τελευταία κλάση έχουμε τα *Εξωτερικά Γεγονότα*, λειτουργικοί κίνδυνοι που συσχετίζονται με γεγονότα εκτός των τειχών της επιχείρησης και τα οποία δεν μπορεί να ελέγξει. Ως πρωταρχική υποκατηγορία εμφανίζονται οι *καταστροφές*, φυσικής ή ανθρωπίνου προελεύσεως, όπως είναι τα καιρικά φαινόμενα και οι αναταραχές λόγω τρομοκρατικών επιθέσεων για παράδειγμα. Δεύτερη υποκατηγορία είναι τα *νομικά ζητήματα* που ενδεχομένως να επηρεάσουν την επιχείρηση όπως είναι η νομοθεσία και οι αντιδικίες με μετόχους ή πελάτες της. Στην τρίτη υποκατηγορία συναντάμε τα *επιχειρηματικά ζητήματα* που προκύπτουν από αλλαγές του επαγγελματικού περιβάλλοντος της επιχείρησης όπως είναι οι συνθήκες της αγοράς. Τέλος, οι *αλληλεξαρτώμενες υπηρεσίες* απαρτίζουν την τέταρτη υποκατηγορία και αφορά τους κινδύνους που ελλοχεύει η εξάρτηση μιας επιχείρησης από εξωτερικούς συνεργάτες για να συνεχίσει την ομαλή λειτουργία της. Ως αλληλεξαρτώμενες υπηρεσίες που μπορεί να αποτύχουν θεωρούμε τις υπηρεσίες εκτάκτου ανάγκης, μεταφοράς, καυσίμων και βοηθητικές υπηρεσίες όπως υπηρεσίες ρεύματος και ύδρευσης.[8]

Αξίζει να σημειωθεί πως σύμφωνα με τη μελέτη του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISAEuropeanUnionAgencyforNetworkandInformationSecurity) για το 2018, ως πηγή κινδύνων κυβερνοχώρου στην Ευρωπαϊκή Ένωση,οι κακόβουλες και εγκληματικές επιθέσεις (εσκεμμένη ανθρώπινη δράση) αποτελούν το 39%, εμφανίζοντας μια ραγδαία αύξηση σε σχέση με το προηγούμενο έτος (7% για το σύνολο του 2017) και τα σφάλματα συστήματος το 39%, σημειώνοντας επίσης αύξηση σε σχέση με το 36% του 2017. Τα ανθρώπινα λάθη (ακούσια ανθρώπινη δράση) αποτελούν σχεδόν το 1/10 με ποσοστό 11% και το εναπομείναν 11% καταλαμβάνουν οι αποτυχίες τρίτων μελών[9].

[8] Cebula, J.J & Young, L.R. (2010), "*A Taxonomy of Operational CyberSecurity Risks*", Technical Note CMU/SEI-2010-TN-028, CEPT Carnegie Mellon University

[9] TRUST SERVICES SECURITY INCIDENTS 2018 ENISA Annual Report

Διάγραμμα 1: ΠηγέςΚινδύνωνΚυβερνοχώρου[10].

2.3 Κυβερνοεπιθέσεις

Ως *Κυβερνοεπίθεση* ορίζουμε μια επίθεση που πραγματοποιείται από έναν υπολογιστή, εναντίον ενός διαδικτυακού τόπου, ενός συστήματοςυπολογιστών, είτε ενός μεμονωμένου υπολογιστή και διακυβεύειτις τρεις βασικές έννοιες της ασφάλειας των πληροφοριακών συστημάτων: την εμπιστευτικότητα, την ακεραιότητα ή την διαθεσιμότητα του υπολογιστή ή των πληροφοριών που είναι αποθηκευμένες σ' αυτόν[11].

"Καθώς όλες οι επιχειρήσεις αγκαλιάζουν τα ψηφιακά επιχειρησιακά μοντέλα, η επιτυχία εξαρτάται σε μεγάλο βαθμό από τηντεχνολογία που διευκολύνει την επιχείρηση ", λέει ο GeorgiPachov, ηγέτης παγκόσμιας πρακτικής, Cyber, AGCS. "Οι ροές εσόδων μπορούν εύκολα να διακοπούν μετά από μια μη φυσιολογική τεχνολογική συμπεριφορά.Τα περιστατικά του κυβερνοχώρου που οδηγούν σε αναχαίτιση της συνήθη ροής της επιχείρησης θα γίνουν πολύ πιο συχνά στο μέλλον λόγω της εξάρτησης από την τεχνολογία και τα δεδομένα για τη λειτουργία των επιχειρήσεων. Στην εποχή του «InternetofThings, IoT[12]», εάν δύο κατασκευαστικάμηχανήματα δεν μπορούν να επικοινωνήσουν και να

[10] TRUST SERVICES SECURITY INCIDENTS 2018 ENISA Annual Report

[11] Practical Law Company, Whitepaper on Cyber Attacks

[12] Η έννοια Internet of Things αναφέρεται στο δίκτυο συνδεδεμένων συσκευών, με μοναδικά αναγνωριστικά στοιχεία υπό τη μορφή μιας διαδικτυακής διεύθυνσης πρωτοκόλλου, οι οποίες έχουν ενσωματωμένες

ανταλλάξουν δεδομένα μεταξύ τους, αναπόφευκτα θα οδηγήσουν σε επιχειρηματική αναστάτωση ".

Το Διαδίκτυο από την απαρχή της ιστορίας του αποτελούσε τον θεμελιώδη λίθο του σύγχρονου κόσμου που προωθούσε την εξέλιξη και την καινοτομία. Σήμερα όμως η χρήση του Διαδικτύου μας έχει οδηγήσει σε νέες προκλήσεις που ζητούν άμεση διαχείριση και επίλυση. Κακόβουλοι εγκληματίες μπορούν να απειλήσουν πλέον τα συστήματα της ψηφιακής οικονομίας από οποιοδήποτε μέρος του πλανήτη, απλά χρησιμοποιώντας τον υπολογιστή τους. Έτσι το Διαδίκτυο από απλό εργαλείο άντλησης και διακίνησης πληροφοριών έχει γίνει πολύπλοκο και εξαιρετικά επικίνδυνο αν δεν προστατευθούμε καταλλήλως. Το φαινόμενο των κυβερνοεπιθέσεων στην σύγχρονη εποχή της τεχνολογίας, ταλανίζει όλων των ειδών τις επιχειρήσεις, ανεξαρτήτου μεγέθους και γεωγραφικής περιοχής, είναι λοιπόν ένα γενικευμένο και παγκόσμιο φαινόμενο.

Αξίζει να αναφερθεί ότι με βάση την έρευνα της Germalto για το πρώτο εξάμηνο του 2018, ο αριθμός των δεδομένων που παραβιάστηκαν ανερχόταν στα 3,353,172,708, ένα νούμερο που είναι κατά 72% υψηλότερο σε σχέση με το πρώτο εξάμηνο του 2017[13].

Στους παρακάτω δύο πίνακες παρουσιάζονται τα είδη των επιχειρήσεων που πλήττονται περισσότεροαπό τις κυβερνοεπιθέσεις, με τις χρηματοοικονομικές και ασφαλιστικές επιχειρήσεις να σημειώνουν το υψηλότερο ποσοστό 19%, καθώς και το μέσο κόστος των κυβερνοεπιθέσεων ανά χώραγια το 2019 και το ποσοστό μεταβολής του κόστους σε σχέση με το προηγούμενο έτος, με τις ΗΠΑ να πρωτοστατούν σύμφωνα με τις μελέτες της IBM και την συντριπτική πλειοψηφία των χωρών να παρουσιάζει αύξηση του κόστους των κυβερνοεπιθέσεων σε σχέση με το 2018.

τεχνολογίες ή διαθέτουν τεχνολογίες που τους επιτρέπει να αντιλαμβάνονται, να συλλέγουν δεδομένα και να επικοινωνούν με το περιβάλλον στο οποίο βρίσκονται.(Review of Maritime Transport 2018, UNACTAD)

[13] Breach Level Index, 2018 First Half Review, Germalto

Πίνακας 2: Πιο Συχνές Επιχειρήσεις-Στόχοι για το 2018.

Επιχειρήσεις-Στόχοι	Ποσοστό στο σύνολο των επιθέσεων
Χρηματοοικονομικές/ Ασφαλιστικές	19%
Μεταφορικές	13%
Επαγγελματικών Υπηρεσιών	12%
Πωλήσεων	11%
Κατασκευαστικές	10%
Μέσων Μαζικής Ενημέρωσης	8%
Κυβερνητικές	8%
Υγείας	6%
Εκπαίδευσης	6%
Ενέργειας	6%

Πηγή:X-Force Threat Intelligence Index 2019, IBM Security Research

Πίνακας 3: Κόστος παραβίασης δεδομένων ανά χώρα ή περιοχήγια το 2019και ποσοστό μεταβολής σε σχέση με το 2018.

Χώρες/Περιοχές	Κόστος	Ποσοστό Μεταβολής	Χώρες/Περιοχές	Κόστος	Ποσοστό Μεταβολής
ΗΠΑ	$8.19	3.54%	**Νότια Κορέα**	$3.30	14.58%
Μέση Ανατολή	$5.97	12.43%	**Νότια Αφρική**	$3.06	5.52%
Γερμανία	$4.78	2.36%	**Ασία**	$2.62	3,56%
Καναδάς	$4.44	-6.33%	**Σκανδιναβία**	$2.30	-
Γαλλία	$4.33	1.41%	**Αυστραλία**	$2.13	7,04%
Ηνωμένο Βασίλειο	$3.88	5.43%	**Τουρκία**	$1.86	-13,89%
Ιαπωνία	$3.75	10.95%	**Ινδία**	$1.83	3,39%
Ιταλία	$3.52	2.62%	**Βραζιλία**	$1.35	8,87%

*Τα νούμερα αναφέρονται σε εκατομμύρια US$

Πηγές: Cost of Data Breach Report 2019, IBM

Cost of a Data Breach Study: Global Overview 2018, IBM

Ένα αρκετά ενδιαφέρον στοιχείο μιας αναφοράς της Accenture[14] αποτελεί το γεγονός ότι η εξάρτηση των επιχειρήσεων από το Διαδίκτυο το 2008, βρίσκονταν σε επίπεδα του 23% και μόλις μια δεκαετία αργότερα το ποσοστό αυτό έχει εκτοξευτεί στο 100%. Αυτό το στατιστικό στοιχείο μας επισημαίνει ότι όλες αυτές οι επιχειρήσεις αποτελούν δυνητικούς στόχους κυβερνοεπιθέσεων και έχουν πλέον αυξημένες πιθανότητες να υποστούν τέτοιου είδους επιθέσεις, συγκεκριμένα σύμφωνα με έρευνα που διεξήχθη στην Αμερική, εν έτη 2019 μια επιχείρηση έχει κατά ένα τρίτο μεγαλύτερη πιθανότητα να δεχθεί παραβίαση των δεδομένων της σε σχέση με το 2014[15]. Το παραπάνω αποδεικνύεται και από την τελευταία αναφορά του WorldEconomicForum, όπου αναφέρεται ότι οι κυβερνοεπιθέσεις και οι υποκλοπές δεδομένων είναι πλέον δύο από τους κορυφαίους κινδύνους που είναι πολύ πιθανό να αντιμετωπίσουν οι CEOs[16].Συγκεκριμένα με βάση την έρευνα της Marsh το 53% των επιχειρήσεων που έλαβαν μέρος σ' αυτήν κατατάσσει τους κινδύνους κυβερνοχώρου στους πέντε κορυφαίους κινδύνους όσον αφορά τις προτεραιότητές τους για την διαχείριση κινδύνων[17].

Μια λογική συνέπεια των παραπάνω είναι πως και τα κόστη των κυβερνοεπιθέσεων αυξάνονται συνεχώς. Με βάση την πρόσφατη ανάλυση της Marsh μόνο οι κυβερνοεπιθέσεις κοστίζουν στα έθνη πάνω από 1 τρισεκατομμύριοUS$, ένα νούμερο αρκετές φορές μεγαλύτερο σε σχέση με τα 300 δισεκατομμύρια US$ που αφορούν ζημιές που είχαν προκληθεί από φυσικές καταστροφές το 2017[18]. Επίσης, σύμφωνα με την αναφορά του WorldEconomicForum για το 2019, οι οικονομικές απώλειες που οφείλονται σε εγκλήματα στον κυβερνοχώρο αναμένεται να φθάσουν τα 3 τρισεκατομμύρια US$ μέχρι το 2020 και το 74% των παγκόσμιων επιχειρήσεων αναμένεται να παραβιαστεί το επόμενο έτος[19].Στο διάγραμμα που ακολουθεί παρατηρούμε την πορεία του κόστους των κακόβουλων επιθέσεων

[14] Securing the digital economy, Reinventing the Internet for Trust 2019, Accenture

[15] Cost of Data Breach Report 2019, IBM

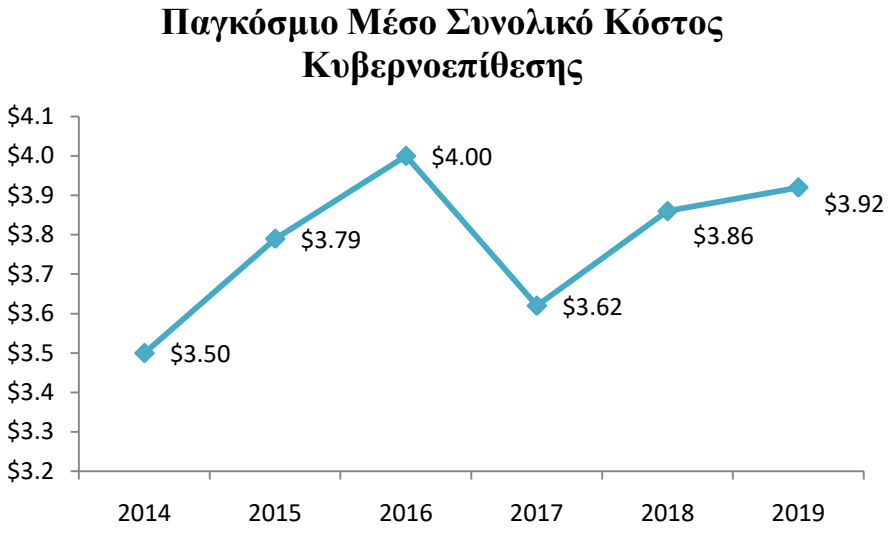
[16] The Global Risks Report 2019, World Economic Forum

[17] 2018 Cyber Risk Perception Survey Report by Marsh & McLennan Agency

[18] MMC Cyber Handbook 2019, Perspectives on Cyber Risk in the Digital Era, Marsh & McLennan Insights

[19]https://www.weforum.org/centre-for-cybersecurity

σε εκατομμύρια US$ με βάση την έρευνα που πραγματοποίησε η IBMγια 507 Αμερικάνικες επιχειρήσεις[20].



Διάγραμμα 2:Παγκόσμιο Μέσο Συνολικό Κόστος Κυβερνοεπίθεσης[21].

2.3.1 Κίνητρα Κυβερνοεπιθέσεων

Με βάση τις διάφορες έρευνες που έχουν καταγραφεί ανά τον κόσμο καθώς και τα διάφορα καταγεγραμμένα περιστατικά παραβίασης δεδομένων, τα σημαντικότερα κίνητρα των κυβερνοεπιθέσεων είναι τα εξής[22]:

Οικονομικά οφέλη: Αποτελεί ένα από τα κυριότερα κίνητρα για την ενορχήστρωση μιας κυβερνοεπίθεσης.Σύμφωνα με έρευνα του Verizonοι επιθέσεις που υποκινούνται από οικονομικά οφέλη αποτελούν το 71%[23]. Οι περισσότερες μέθοδοι που χρησιμοποιούνται από

[20] Cost of Data Breach Report 2019, IBM

[21] Cost of Data Breach Report 2019, IBM

[22]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[23]Verizon Data Breach Investigations Report 2019

κερδοσκοπικούς εισβολείς περιλαμβάνουν την κλοπή και μεταπώληση πληροφοριών πιστωτικών καρτών, Ransomwarekαι DDoS[24] εκβιαστικές επιθέσεις.[25]

Εκδίκηση: Ο δυσαρεστημένος πρώην υπάλληλος μιας επιχείρησης είναι ένας από τους πιο εύκολα αναγνωρίσιμους επιτιθέμενους που υποκινούνται από κίνητρα εκδίκησης. Αυτό το άτομο μπορεί να εξακολουθεί να έχειπρόσβαση στους πόρους του στόχου τουήναέχειδιατηρήσειεταιρικά έγγραφα που μπορεί να πωληθούν ή να δημοσιευθούν. Εξίσου καταστροφικός μπορεί να αποδειχθεί και ένας δυσαρεστημένος πελάτης της επιχείρησης.

Διαμαρτυρία: Αυτού του είδους η κυβερνοεπίθεση καθιστά το πιο σύνηθες κίνητρο των hacktivists[26], όπως είναι και οι Anonymous- μια αποκεντρωμένη διεθνής ομάδα, η οποία είναι ευρέως γνωστή για τις διάφορες DDoS επιθέσεις στον κυβερνοχώρο σε διάφορες κυβερνήσεις, κυβερνητικά ιδρύματα και κυβερνητικές υπηρεσίες και εταιρείες.

Απόκτηση Στρατηγικού Πλεονεκτήματος: Διενεργείται από ανταγωνιστικές επιχειρήσεις αποκτώντας πρόσβαση σε εμπιστευτικές πληροφορίες και δεδομένα ηλεκτρονικής μορφής, με απώτερο σκοπό την εταιρική δυσφήμιση της επιχείρησης στόχου.

Ενθουσιασμός/ Περιέργεια: Υπάρχουν περιστατικά όπου ένα μεμονωμένο άτομο ή μια ομάδα ατόμων, συνήθως μικρής ηλικίας, λόγω ενθουσιασμού ή περιέργειας για το εν δυνάμει προσβαλλόμενο υλικό παραβιάζουν τα πληροφοριακά συστήματα.

Πολιτικοί / Θρησκευτικοί Λόγοι: Υπάρχουν πολλές καταγεγραμμένες περιπτώσεις επιθέσεων που μπορούν να καταταχθούν στην κατηγορία των πολιτικά υποκινούμενων επιθέσεων από χώρεςόπως οι Ηνωμένες Πολιτείες, η Ρωσία, η Κίνα, η Ουκρανία, η Ινδονησία, η Ινδία, το Πακιστάν και η Αυστραλία. Μερικοί επιτιθέμενοι μπορεί να μην είναι άμεσαπολιτικά παρακινημένοι, ωστόσο μια κρατική πολιτική οργάνωση μπορεί να

[24]Εννοιεςπουθααναλυθούνπαρακάτω

[25] IBM X-Force® Research Managed Security Services Report 2016, IBM Security

[26]Το επίθετο hacktivist προέρχεται από τις λέξεις hacker και activist και αποτελεί μια προσπάθεια μεταφοράς ενός κοινωνικού ή πολιτικού μηνύματος.

ενθαρρύνει τέτοιου είδους επιθέσεις. Στις επιθέσεις καθοδηγούμενες από θρησκευτικούς λόγους περιλαμβάνονται και οι επιθέσεις των ISISκαι alQaida[27].

Προσέλκυση Ενδιαφέροντος της Διοίκησης της Επιχείρησης-Στόχου:Ημη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών από ένα άτομο μπορεί να γίνει για να προσελκύσει το ενδιαφέρον της διοίκησης του οργανισμού,διαφημίζοντας κατ' αυτόν τον τρόπο τις πειρατικές τουικανότητες για μελλοντικές προσλήψεις στην ασφάλεια του τμήματος IT ή για σκοπούς βιομηχανικήςκατασκοπείας. Πολλές είναι οι περιπτώσεις όπου εταιρίες έχουν προσλάβει άτομα που επιχείρησαν ή και ακόμη κατάφεραν να παραβιάσουν τα δικά τους συστήματα ή των ανταγωνιστών τους. Για παράδειγμα, η πλατφόρμα μηνυμάτων Yo προσέλαβε μια ομάδα φοιτητών της GeorgiaTech που απέκτησαν μη εξουσιοδοτημένη πρόσβαση στην εφαρμογή. Η αρχική επαφή του προγραμματιστή της εφαρμογής βίντεο του Facebook με την εταιρεία ήταν όταν δημιούργησε ένα σκουλήκι (worm) που έκανε τα προφίλ του Facebook να μοιάζουν με προφίλ MySpace.To Facebook και το Twitter έχουν και οι δύο προσλάβει χάκερς γνωστούς για τις επιθέσεις τους στα προϊόντα της Apple.

2.3.2 Στόχοι Κυβερνοεπιθέσεων

Στην εποχή της τεχνολογίας και των ηλεκτρονικών υπολογιστών, η πληθώρα όλων των ειδών επιχειρήσεων αποθηκεύει, επεξεργάζεται και μεταφέρει δεδομένα των πελατών της, αυτή η νέα πραγματικότητα τις καθιστά στόχους ηλεκτρονικών και διαδικτυακών επιθέσεων. Μπορούμε να διαχωρίσουμε τους στόχους αυτούς στις εξής κατηγορίες[28]:

Δημόσιοι Οργανισμοί: Μιας και είναι πλέον γεγονός ότι οι κρατικές υπηρεσίες ανά τον κόσμο εκσυγχρονίζονται και όλο και περισσότεροι Δημόσιοι Οργανισμοί χρησιμοποιούν πληροφοριακά συστήματα, και σε συνδυασμό με το ότι αυτού του είδους οι οργανισμοί

[27] IBM X-Force® Research Managed Security Services Report 2016, IBM Security

[28]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

διατηρούν έναν τεράστιο όγκο προσωπικών δεδομένων, αποτελούν -σύμφωνα και με την έρευνα της Verizon για το 2019- τον πιο σύνηθες στόχο κυβερνοεπιθέσεων με 23,399 περιστατικά[29].

Ιδιωτικοί Οργανισμοί: Καθώς όλο και περισσότερες επιχειρήσεις βασίζονται στα πληροφοριακά και τηλεπικοινωνιακά συστήματα για την ανάπτυξη και επέκτασή τους, είναι προφανής απόρροια η έκθεση στους κινδύνους κυβερνοχώρου.

Υπάλληλοι / Στελέχη Οργανισμών: Η ραγδαία εξάπλωση της χρήσης των ψηφιακών συσκευών όπως είναι τα smartphoneskαι τα tables καθώς και η εκτεταμένη χρήση των Μέσων Κοινωνικής Δικτύωσης (Facebook, Twitter, LinkedIn) από τα στελέχη των επιχειρήσεων τους εκθέτει στους κινδύνους κυβερνοχώρου. Τα επιτιθέμενα άτομα μπορούν μέσω των ψηφιακών συσκευών των στελεχών να υποκλέψουν εμπιστευτικά δεδομένα ή να αποσπάσουν πληροφορίες, όπως οι κωδικοί πρόσβασης, που θα τους βοηθήσουν να παρακάμψουν τα συστήματα ασφαλείας των οργανισμών που έχουν τεθεί στο στόχαστρο.

Σημαντικές Εθνικές Υποδομές: Οι εθνικές υποδομές, παραδείγματος χάρη οι οργανισμοί παροχής ενέργειας, οι αερολιμένες και οι εθνικοί σιδηρόδρομοι, είναι ο κύριος στόχος των τρομοκρατιών και των ξένων κυβερνήσεων στην απώτερη προσπάθειά τους να επιβάλλουν πολιτικές και θρησκευτικές πεποιθήσεις και να υλοποιήσουν τα στρατηγικά τους σχέδια. Το γεγονός ότι η πλειοψηφία αυτών των υποδομών βασίζεται στα πληροφοριακά συστήματα, καθιστά εύκολα αντιληπτό το μέγεθος του προβλήματος που μπορεί να προκαλέσει ένα περιστατικό κυβερνοεπίθεσης.Μια από τις πιο ανησυχητικές επιθέσεις σε εθνική υποδομή έλαβε χώρα τον Αύγουστο του 2017 όταν μια πετροχημική εταιρεία με εργοστάσιο στην Σαουδική Αραβία χτυπήθηκε από ένα νέο είδος κυβερνοεπίθεσης. Σύμφωνα με τους ερευνητές, η επίθεση δεν σχεδιάστηκε για να καταστρέψει απλώς τα δεδομένα ή να κλείσει το εργοστάσιο, αλλά για να σαμποτάρει την λειτουργία της επιχείρησης και να πυροδοτήσει έκρηξη.

[29]Verizon Data Breach Investigations Report 2019

2.3.3 Μέθοδοι Κυβερνοεπιθέσεων

Όσο η τεχνολογία εξελίσσεται, όλο και περισσότερες είναι οι νέες μέθοδοι επιθέσεων κυβερνοχώρου που προκύπτουν. Μέθοδοι που χρησιμοποιούνται για μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή δεδομένων και / ή συστημάτων πληροφοριών και επικοινωνιών ενός οργανισμού.

Με βάση την Cisco[30]και τοσύγγραμμα του Τσουραμάνη Χρήστου[31], παρακάτω αναφέρουμε κάποιες από τις βασικότερες μεθόδους:

Διασπορά κακόβουλων προγραμμάτων (Ιοί, Σκουλήκια, Δούρειοι Ίπποι):

Ιός(virus): Ο ιός είναι ένα πρόγραμμα ηλεκτρονικού υπολογιστή που έχει σχεδιαστεί για να μολύνει άλλα προγράμματα. Έχει την ικανότητα να αναπαράγεται συνεχώς και μπορεί να μεταδοθεί από ένα σύστημα σε άλλο για να εκτελέσει τον σκοπό του, δηλαδή να οδηγήσει στην δυσλειτουργία ή και την πλήρη καταστροφή ολόκληρων συστημάτων, τη διαγραφή αρχείων ή το σβήσιμο του συνόλου του περιεχομένου των σκληρών δίσκων.

Σκουλήκια (worms): Τα σκουλήκια είναι κι αυτά προγράμματα ηλεκτρονικού υπολογιστή που χρησιμοποιούνται για να μεταφέρουν άλλα προγράμματα. Η διαφορά τους με τους ιούς έγκειται στο ότι δεν απαιτείται η ανθρώπινη παρεμβολή για την ενεργοποίησή τους και στο ότι δεν χρειάζεται να προσκολλώνται σε άλλα προγράμματα για να επιβιώσουν.

ΔούρειοιΊπποι (TrojanHorses, Trojans): Οι δούρειοι ίπποι είναι και αυτοί προγράμματα ηλεκτρονικού υπολογιστή τα οποία ενώ φαίνεται ότι λειτουργούν κανονικά, συγχρόνως διενεργούν κρυφά και κάποιες άλλα μη επιτρεπόμενες ενέργειες.

Κακόβουλο Λογισμικό (Malware): Ένα κακόβουλο πρόγραμμα είναι ένας κωδικός ο οποίος έχει δημιουργηθεί για να επηρεάσει ένα σύστημα υπολογιστών χωρίς την

[30]https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

[31] Τσουραμάνης Χ., (2005), "ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ: Η (αν)ασφαλής όψη του Διαδικτύου", ΕΚΔΟΣΕΙΣ: ΒΑΣ. Ν. ΚΑΤΣΑΡΟΥ

συγκατάθεση του χρήστη του. Το κακόβουλο αυτό πρόγραμμα εξαπλώνεται μέσα στο δίκτυο, προκαλεί αλλαγές και ζημίες, αλλά παραμένει μη ανιχνεύσιμο. Το πιο διαδεδομένο τέτοιου είδους λογισμικό είναι, το ransomware το οποίο συνήθως μεταφέρεται μέσω ενός Δούρειου Ίππου παραδίδοντας το πρόγραμμα μεταμφιεσμένο ως νόμιμο.
Το ransomware, σύμφωνα με τον ορισμό της Wikipedia, είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος σε αυτά, μέχρι να δοθούν λύτρα από το θύμα[32].

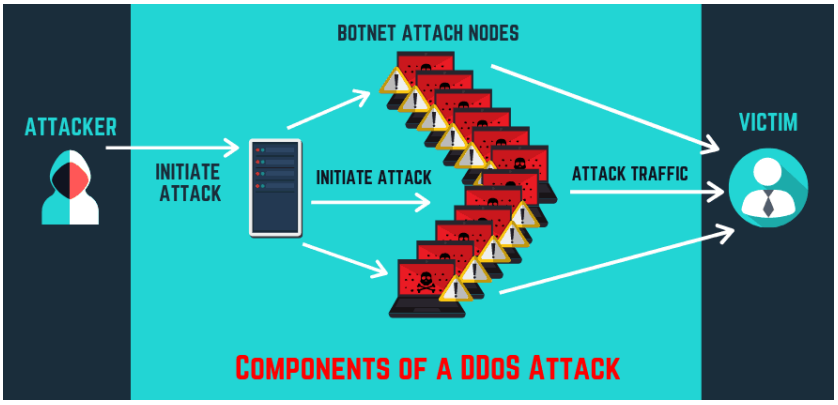
Ψάρεμα (Phishing): Το ηλεκτρονικό "ψάρεμα" είναι ένα είδος κοινωνικήςμηχανικής[33] που χρησιμοποιείται κυρίως για να υποκλέπτει δεδομένα χρηστών όπως είναι για παράδειγμα οι αριθμοί των πιστωτικών καρτών και οι κωδικοί πρόσβασης. Συμβαίνει όταν ο επιτιθέμενος, προσποιούμενος ένα αξιόπιστο άτομο, ξεγελάει το θύμα να ανοίξει ένα μήνυμα περιεχομένου, ένα ηλεκτρονικό μήνυμα ή ένα άμεσο μήνυμα. Το θύμα ανοίγοντας αυτόν τον σύνδεσμο δέχεται την επίθεση και αποκαλύπτει εν αγνοία του ευαίσθητες προσωπικές πληροφορίες ή επιτρέπει την εγκατάσταση ενός κακόβουλου λογισμικού. Αυτή η παραβίαση μπορεί να έχει καταστρεπτικά αποτελέσματα, όπως κλοπή ταυτότητας, κλοπή κεφαλαίων ή μη εξουσιοδοτημένες αγορές[34].

Άρνηση Παροχής Υπηρεσιών (DenialofService , DoS): Αυτού του είδους η επίθεση στοχεύει στην υπερφόρτωση και κατάρρευση ενός δικτύου ή μιας υπηρεσίας ώστε οι νόμιμοι χρήστες της, όπως είναι οι υπάλληλοι, οι κάτοχοι λογαριασμών και οι δυνητικοί πελάτες να μην μπορούν να αποκτήσουν πρόσβαση σε αυτήν. Ο παραπάνω σκοπός επιτυγχάνεται κατακλύζοντας τον στόχο της επίθεσης με τόσες πολλές πληροφορίες που του είναι αδύνατο να διαχειριστεί με αποτέλεσμα να καταρρεύσει. Μια ευρέως γνωστή υποκατηγορία των επιθέσεων DoS είναι μια επίθεσηDDoS(distributeddenial of service). Η ειδοποιός διαφορά της τελευταίας, είναι ότι η επίθεση προέρχεται από πολλές διαφορετικές πηγές κάτι που καθιστά αδύνατη την καταπολέμησή της.

[32]https://el.wikipedia.org/wiki/Ransomware

[33]*Κοινωνική μηχανική (Socialengineering*) είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών

[34]17 Types of Cyber Attacks To Secure Your Company From in 2019, phoenixNAP Global IT Services



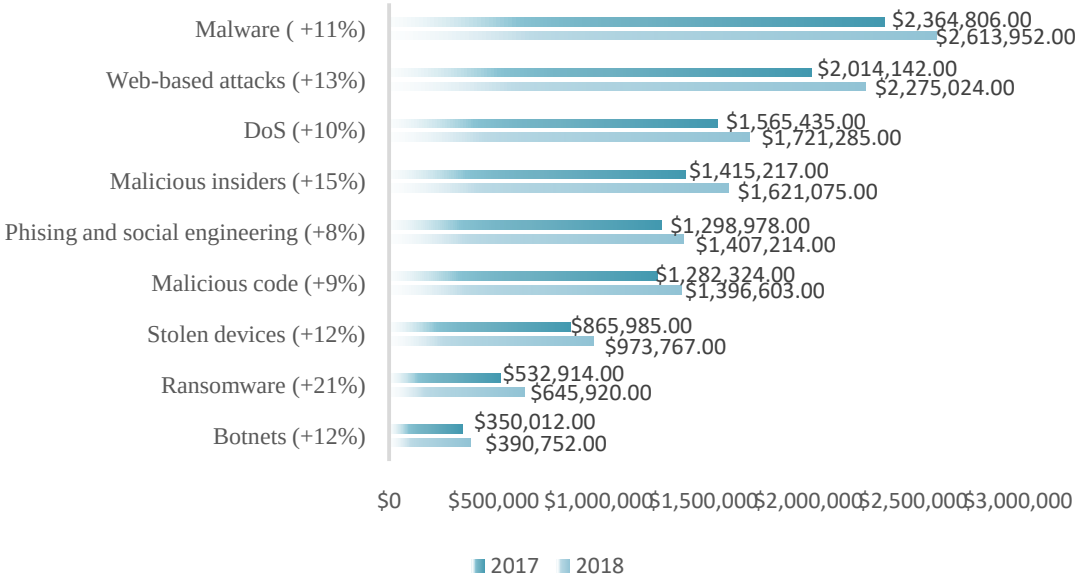
Εικόνα 1: Δομή μιας επίθεσης DDoS[35]

Ενδιάμεσος Άνθρωπος (Man-in-the-middle, MitM): Οι επιθέσεις Man-in-the-middle (MitM), επίσης γνωστές ως επιθέσεις απόκρυψης, συμβαίνουν όταν οι εισβολείς εισάγονται σε μια συναλλαγή-επικοινωνία δύο μερών. Μόλις οι επιτιθέμενοι διακόψουν την κίνηση, μπορούν να φιλτράρουν και να αποσπάσουν δεδομένα.Τα δύο μέρη φαίνεται να επικοινωνούν κανονικά χωρίς να γνωρίζουν ότι ο αποστολέας του μηνύματος είναι ένας άγνωστος δράστης που προσπαθεί να έχει πρόσβαση και να τροποποιήσει το μήνυμα πριν μεταδοθεί στον παραλήπτη. Έτσι, ο εισβολέας ελέγχει ολόκληρη την συναλλαγή-επικοινωνία. Ένα χαρακτηριστικό παράδειγμα της ανωτέρω επίθεσης είναι όταν σε μη ασφαλή δημόσια δίκτυα Wi-Fi, οι επιτιθέμενοι μπορούν να εισέλθουν μεταξύ της συσκευής ενός επισκέπτη και του δικτύου. Εν αγνοία του ο επισκέπτης περνά όλες του τις πληροφορίες μέσω του εισβολέα.

ΈνεσηSQL (injectionsSQL,StructuredQueryLanguage): Μια ένεση SQLυπάγεται στις επιθέσεις με βάση τον ιστότοπο (web-basedattacks) και συμβαίνει όταν ένας εισβολέας εισάγει κακόβουλο κώδικα σε ένα διακομιστή που χρησιμοποιεί SQL και αναγκάζει τον διακομιστή να αποκαλύψει τις πληροφορίες που κανονικά δεν θα αποκάλυπτε, συμπεριλαμβανομένων των ιδιωτικών στοιχείων του πελάτη, λίστες χρηστών ή των ευαίσθητων δεδομένων της εταιρείας. Ένας εισβολέας θα μπορούσε να πραγματοποιήσει μια ένεση SQL απλά υποβάλλοντας έναν κακόβουλο κώδικα σε ένα ευπαθές πλαίσιο αναζήτησης ιστότοπου.

[35]17 Types of Cyber Attacks To Secure Your Company From in 2019, phoenixNAP Global IT Services

Στο παρακάτω σχεδιάγραμμα παρουσιάζεται με βάση την έρευνα του PonemonInstitute[36]το μέσο ετήσιο κόστος κυβερνοεπιθέσεων με βάση τις διάφορες μεθόδους, μερικές από τις οποίες αναφέραμε και παραπάνω,για το 2018. Παρατηρούμε ότι οι επιθέσεις κακόβουλου λογισμικού(malware) και οι επιθέσεις με βάση τον ιστότοπο (web-based attacks) είναι οι πιο κοστοβόρες, με 2,613,952 US$ και 2,275,024US$ αντίστοιχα. Ένα επίσης σημαντικό στοιχείο που προκύπτει είναι ότι οι επιθέσεις ransomware σημειώνουν την μεγαλύτερη αύξηση κόστους (21%) σε σχέση με το 2017.



Διάγραμμα 3: Μέσο ετήσιο κόστος κυβερνοεπιθέσεων με βάση τις διάφορες μεθόδους επίθεσης για τα έτη 2017και 2018[37].

2.3.4 ΕπιπτώσειςΚυβερνοεπιθέσεων

Οι συνέπειες των κυβερνοεπιθέσεων είναι ένα από τα σημαντικότερα ζητήματα διότι είναι αυτό που αφήνει πίσω της μια επίθεση και οι επιχειρήσεις καλούνται να διαχειριστούν. Ανάλογα με το είδος της επιχείρησης που δέχεται την κυβερνοεπίθεση, οι επιπτώσεις της

[36] *The cost of Cybercrime* 2019, Ninth Annual Cost of Cybercrime Study, Ponemon Institute

[37] *The cost of Cybercrime* 2019, Ninth Annual Cost of Cybercrime Study, Ponemon Institute

μπορεί και να διαφέρουν. Αν η εν λόγω επιχείρηση κατανοήσει τις συνέπειες που απορρέουν από μια τέτοια επίθεση, τότε θα είναι σε θέση να προσδιορίσει καλύτερα και το δυνητικό της κόστος. Οι επιπτώσεις μπορεί να είναι χρηματοοικονομικές, νομικές ή λειτουργικές, καθώς και να προκαλέσουν δυσφήμιση της επιχείρησηςκαι αναπτύσσονται παρακάτω[38].

Καταστροφή, αποκάλυψη ή τροποποίηση πληροφοριών: Η πιο άμεση επίπτωση μιας κυβερνοεπίθεσης είναι η διαρροή των πληροφοριών που διακατέχει μια επιχείρηση, δηλαδή η κλοπή της πνευματικής της ιδιοκτησίας, κυρίως για λόγους βιομηχανικής και πολιτικής κατασκοπίας. Όπως αναφέρει η μελέτη της McAfee, οιυποκλοπές των λογαριασμών πνευματικής ιδιοκτησίας αφορούν τουλάχιστον το ένα τέταρτο του κόστους των εγκλημάτων στον κυβερνοχώρο και όταν πρόκειται δε για στρατιωτική τεχνολογία, ελλοχεύουνσοβαροί κίνδυνοι για την εθνική ασφάλεια μιας χώρας[39]. Σύμφωνα με το Ινστιτούτο Ponemonκαι τη μελέτη του για το 2019, η απώλεια πληροφοριών ως συνέπεια κυβερνοεπιθέσεων έχει αυξηθεί ραγδαία από το 2015 μέχρι και το 2018 και σημειώνει πλέον το μεγαλύτερο κόστος από μια κακόβουλη επίθεση στο ύψος των 5,9 εκατομμυρίων US$ σε σύγκριση με το 2015 που σημείωνε κόστος 2,7 εκατομμύρια US$[40].

Άμεσες Οικονομικές Απώλειες: Η κλοπή χρημάτων από μια επιχείρηση μέσω μη-εξουσιοδοτημένης πρόσβασης ή άλλων μεθόδων κυβερνοεπιθέσεων στα πληροφοριακά συστήματά της, αποτελεί την πιο συχνή επίπτωση των επιθέσεων αυτών. Επίσης, άμεση οικονομική απώλεια μπορεί να υποστούν και οι μέτοχοι της επιχείρησης, δεδομένου ότι η ανακοίνωση ενός περιστατικού παραβίασης μπορεί να οδηγήσει σε πτώση της τιμής της μετοχής της εν λόγω εταιρίας[41].Σε μια έρευνα που διεξήγαγαν οι Lin, Parsa, Ulmer και Sapp, το 71% των επιχειρήσεων του δείγματός τους υπέφερε από μείωση της τιμής των μετοχών τους στον απόηχο της κυβερνοεπίθεσης που δέχθηκαν[42].

---

[38]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[39] Economic impact of cybercrime- No slowing down, 2018, McAfee

[40] *The cost of Cybercrime* 2019, Ninth Annual Cost of Cybercrime Study, Ponemon Institute

[41]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[42] Lin, Z., Parsa, R., Rees Ulmer, J. & Sapp, T. (2018), "*Pricing Cyber Security Insurance: A Copula Model Using an Objective, Verifiable, Loss Measure*", (July 17, 2018)

Νομική Έκθεση / Αγωγές: Η απώλεια, αποκάλυψη, τροποποίηση ή καταστροφή των ψηφιακών δεδομένων μπορεί να πυροδοτήσει αγωγές από μετόχους, υπαλλήλους, πελάτες και τρίτους για αποκατάσταση της εμπιστοσύνης τους και αποζημιώσεις. Οι πιθανές νομικές υποχρεώσεις για οργανισμούς που έχουν υποστεί παραβίαση των συστημάτων τους, μπορούν να φτάσουν ακόμη και μερικές χιλιάδες δολάρια ειδικά για εκείνους που χειρίζονται αναγνωρίσιμες προσωπικές πληροφορίες. Για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, η ΕΕ έχει εφαρμόσει νομοθεσία και έχει υποστηρικτική επιχειρησιακή συνεργασία ως μέλος της στρατηγικής της ΕΕ για την ασφάλεια στον κυβερνοχώρο[43].

Δημιουργία προβλημάτων στο τμήμα IT (InformationTechnology): Το τμήμα του IT της επιχείρησης είναι αυτό που επωμίζεται τις ευθύνες της δυνητικής επίθεσης. Οι εργαζόμενοι του τμήματος θα πρέπει να είναι σε θέση να αντιληφθούν ότι έχουν υποστεί παραβίαση των συστημάτων τους και να την περιορίσουν όσο είναι δυνατόν. Η πιθανή διακοπή της λειτουργίας του τμήματος αυτού θα επιφέρει αρνητικά αποτελέσματα στην επιχείρηση μιας και στην ουσία αποτελεί τον πυρήνα της.

*Απώλεια Παραγωγικότητας:*Ένα περιστατικό παραβίασης δεδομένων μπορεί να οδηγήσει σε απώλεια παραγωγικότητας, είτε λόγω της αρνητικής ανταπόκρισης των εργαζομένων ή της ψυχολογίας τους, είτε λόγω της μη λειτουργίας των συστημάτων πληροφορικής ITσυνήθως λόγω επιθέσεων DDoS[44]. Οι επιθέσεις από σκουλήκια, ιούς κ.λπ. αφαιρούν παραγωγικό χρόνο από την επιχείρηση, τα μηχανήματα μπορεί να λειτουργούν πιο αργά από το σύνηθες, οι διακομιστές ενδέχεται να γίνουν προσπελάσιμοι και ευάλωτοι, τα δίκτυα ενδέχεται να έχουν μπλοκαριστεί και ούτω καθεξής.Σ’ αυτές τις περιπτώσεις η απώλεια που έχει η επιχείρηση προκύπτει επειδή της αφαιρείται η ευκαιρία να δημιουργήσει κέρδος[45].

---

[43]https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

[44]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[45] Saini, H., Rao, Y.S &Panda, T.C. (2012), "*Cyber-Crimes and their Impacts: A Review*", International Journal of Engineering Research and Applications, Vol 2, Issue 2, Mar-Apr 2012, pp 202-209

Κρίση της Εταιρικής Φήμης: Η ανακοίνωση ότι ένας οργανισμός έχει βιώσει μια παραβίαση δεδομένων μπορεί να βλάψει τη φήμη του λόγω της απώλειας εμπιστοσύνης των καταναλωτών και των συνεργατών του. Αυτό μπορεί όχι μόνο να επηρεάσει τα τρέχοντα και μελλοντικά έσοδα, αλλά μπορεί επίσης να οδηγήσει σε αποχώρηση του προσωπικού από και αναζήτηση εργασίας στους ανταγωνιστές λόγω της δυσφήμησης[46]. Σε μια έρευνα που διεξήχθη από την AllianzGlobalCorporate&Specialty,στο ερώτημα: "Ποιες είναι οι κύριες αιτίες της οικονομικής ζημίας μετά από μια κυβερνοεπίθεση?", το 55% των συμμετεχόντων επέλεξε την απώλεια της φήμης[47]. Ηκρίση της εταιρικής φήμης μπορεί να είναι ο άμεσος στόχος μιας επίθεσης, όπως στην περίπτωση της ηλεκτρονικής δυσφήμισης,ή μια ταυτόχρονη ή διαδοχική επίδραση άλλων μορφών βλάβης, όπως στην περίπτωση παραβίασης δεδομένων ή ηλεκτρονικής κλοπής[48].

Όπως μπορούμε να αναλογιστούμε λοιπόν οι συνέπειες των κυβερνοεπιθέσεων είναι αρκετά σημαντικές σε σημείο που μπορούν να αποβούν και μοιραίες. Όσο πιο γρήγορα αναγνωριστεί και περιοριστεί η παραβίαση των δεδομένων λοιπόν, τόσο μικρότερο θα είναι και το κόστος της. Σύμφωνα με την έρευνα της IBM του 2019 ο κύκλος ζωής της παραβίασης των δεδομένων-δηλαδή ο χρόνος που μεσολαβεί από την πραγματοποίηση της επίθεσης μέχρι τον περιορισμό της-, υπολογίζεται στις 279 ημέρες, 4.9% περισσότερο απ' ότι ήταν το 2018. Ενδιαφέρον προκαλεί το γεγονός ότι ο κύκλος ζωής μιας παραβίασης που προέρχεται από κακόβουλη ενέργεια φτάνει τις 314 ημέρες, 12.5% περισσότερο από τον μέσο κύκλο ζωής. Επίσης, αναφέρεται ότι μια κυβερνοεπίθεση με κύκλο ζωής μεγαλύτερο των 200 ημερών είναι κατά 37% πιο κοστοβόρα απ' ότι μια επίθεση με κύκλο ζωής μικρότερο των 200 ημερών (4.56 εκατομμύρια US$ και 3.34 εκατομμύρια US$ αντίστοιχα)[49].

Παρακάτω παρουσιάζονται δύο διαγράμματα, στο πρώτο διάγραμμα παρουσιάζονται ο μέσος όρος ημερών αναγνώρισης και περιορισμού της επίθεσης για τα έτη 2015 μέχρι και

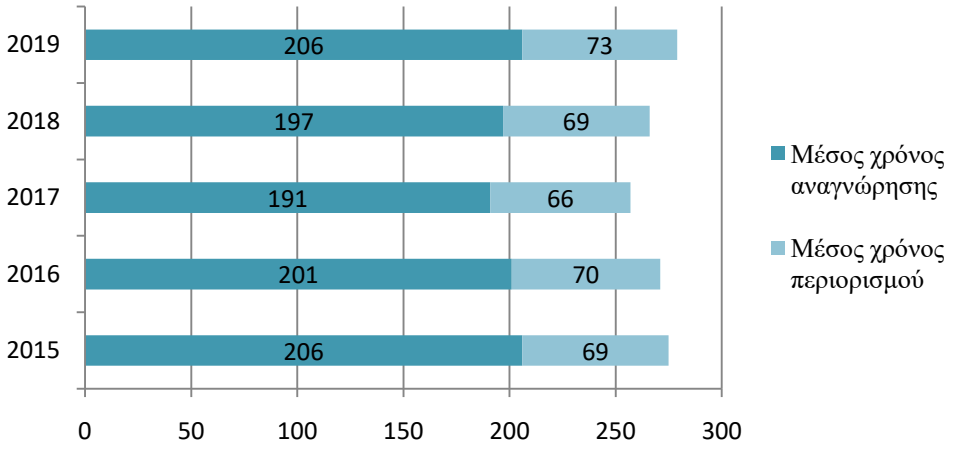
[46]Livanis E. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development
Belgrade, Serbia, 13-14 May 2016

[47] ALLIANZ RISK BAROMETER, TOP BUSINESS RISKS FOR 2019

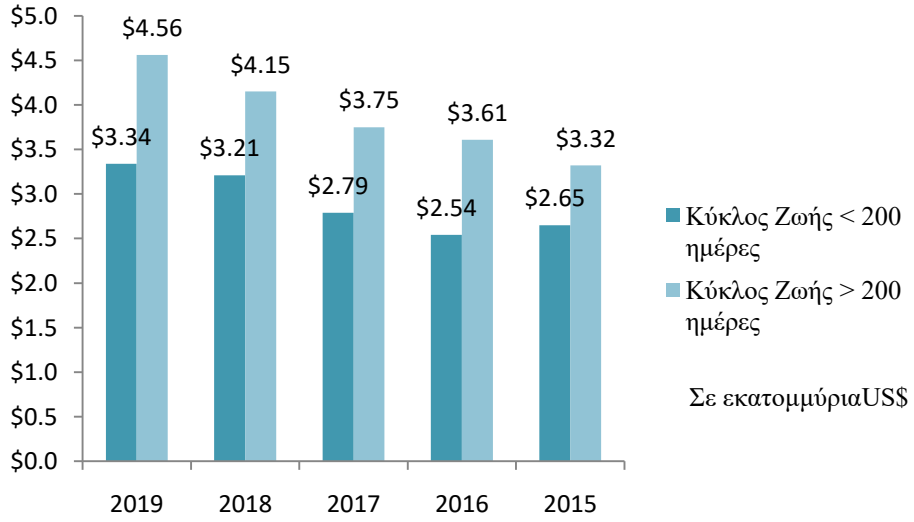
[48]Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T. &Upton D.M. (2016), "*Cyber Harm: Concepts, Taxonomy and Measurement*", Saïd Business School WP, 23

[49] Cost of Data Breach Report 2019, IBM

2019, όπου παρατηρούμε ότι για το 2019 οι ημέρες που απαιτούνται για την αναγνώριση της επίθεσης έχουν αυξηθεί σε σχέση με το προηγούμενο έτος. Στο δεύτερο απεικονίζεται η σχέση μεταξύ του κόστους της επίθεσης και της διάρκειας του κύκλου ζωής της, όπου είναι εμφανές ότι χρόνο με το χρόνο τα κόστη αυτά αυξάνονται και ότι το κόστος των επιθέσεων με διάρκεια κύκλου ζωής μεγαλύτερη των 200 ημερών είναι σημαντικά μεγαλύτερο σε σχέση με αυτών με διάρκεια μικρότερη των 200 ημερών.



Διάγραμμα 4:Μέσος όρος ημερών αναγνώρισης και περιορισμού της επίθεσης για τα έτη 2015 μέχρι 2019[50].



Διάγραμμα 5: Σχέση μεταξύ του κόστους μιας επίθεσης και της διάρκειαστου κύκλου ζωής της[51].

[50] Cost of Data Breach Report 2019, IBM

Τέλος, με βάση την ίδια έρευνα παρατηρήθηκε ότι τα κόστη των κυβερνοεπιθέσεων επηρεάζουν την επιχείρηση για χρόνια. Περίπου το ένα τρίτο του συνολικού κόστους επέρχεται μετά από έναν χρόνο από την επίθεση. Συγκεκριμένα, το 67% του κόστουςεμφανίζεται στον πρώτο χρόνο, το 22% στον δεύτερο χρόνο και το 11% σε διάστημα πάνω από τα δύο έτη[52].

2.4 Αντιμετώπιση Κυβερνοεπιθέσεων

Οι πλειοψηφία των επιχειρήσεων κατατάσσει την ασφάλεια των πληροφοριακών τους συστημάτων στα ζητήματα που πρέπει να διαχειριστεί και να επιλύσει το τμήμα πληροφορικής (IT). Η παραπάνω λανθασμένη αντίληψη αποτελεί την μεγαλύτερη απειλή για την ασφάλεια του κυβερνοχώρου. Η τελευταία θα πρέπει να αντιμετωπιστεί ως ζήτημα διαχείρισης κινδύνων σε συλλογικό επίπεδο επιχείρησης.

Δύοοργανισμοί, ηInternetSecurityAlliance (ISA) καιτοAmericanNationalStandardsInstitute (ANSI) στις αρχέςτου 2008 ανέπτυξανμιαπρακτική μεθοδολογία που μπορεί να εφαρμοστεί από τη διοίκηση των επιχειρήσεων, η οποία διευκολύνει την αντιμετώπιση των κυβερνοεπιθέσεων και των πιθανών οικονομικών ζημιών που δημιουργούνται από την έλλειψη εκτίμησης του γεγονότος ότι οι κίνδυνοι κυβερνοχώρου είναι αλληλεξαρτώμενοι[53]. Η μεθοδολογία αυτή απαρτίζεται από τα εξής έξι βήματα:

1^{ο} Βήμα: Κατανόηση του προβλήματος

Σήμερα, σχεδόν κάθε επιχείρηση έχει ενσωματώσει τα "θαύματα" της ψηφιακής επανάστασης μέσα στα επιχειρηματικά της σχέδια όσον αφορά την διατήρηση αρχείων, την διαχείριση της εφοδιαστικής αλυσίδας, τις ηλεκτρονικές πωλήσεις και άλλες επιχειρηματικές δραστηριότητες. Το μειονέκτημα της

[51] Cost of Data Breach Report 2019, IBM

[52] Cost of Data Breach Report 2019, IBM

[53] Internet Security Alliance (ISA) & American National Standards Institute (ANSI) (2010), The financial management of cyber risk, An Implementation Framework for CFOs, published by ANSI

ψηφιοποίησης που σχετίζεται με την ασφάλεια των δεδομένων, έχει κατά κύριο λόγο μετατεθεί σε ένα απομονωμένο και συχνά υπό-χρηματοδοτούμενο λειτουργικό τμήμα, αυτό της πληροφορικής.

Τα ανώτατα στελέχη με διατμηματική εξουσία, όπως οι Διευθύνοντες Σύμβουλοι (CEOs) ή οι Διευθυντές Οικονομικής Διεύθυνσης (CFOsή CROs), πρέπει να ασκούν στρατηγικό έλεγχοστα συστήματα κυβερνοχώρου που είναι το κεντρικό νεύρο της εταιρικής τους λειτουργίας. Αυτά τα στελέχη πρέπει να εκτιμήσουν ή να μάθουν, αν χρειαστεί, τον πραγματικό ρόλο που διαδραματίζει η τεχνολογία στη σύγχρονη επιχείρηση, συμπεριλαμβανομένων των οικονομικών κινδύνων που θέτει η τεχνολογία στην επιχείρηση και τα μέτρα που πρέπει να ληφθούν για την κατάλληλη διαχείριση του κινδύνου.

2^{ο} Βήμα: Διορισμός μια ομάδας διαχείρισης κινδύνων κυβερνοχώρου

Είναι ουτοπικό να αναμένουμε ότι τα ανώτερα στελέχη θα είναι σε θέση να καθορίσουν όλα τα ερωτήματα, πόσο μάλλον να απαντήσουν σε όλες τις ερωτήσεις, στην πληθώρα των ζητημάτων κυβερνοχώρου που δημιουργούνται στα διάφορα τμήματα των επιχειρήσεών τους.Ωστόσο, η οικονομική σημασία της ασφάλειας του κυβερνοχώρου και των πολλών της επιπτώσεων σημαίνει ότι τα ανώτερα στελέχη δεν δύναται να μεταβιβάσουν το θέμα αυτό αποκλειστικά σε ειδικούς ή σε νέους διευθυντές.

Αυτό σημαίνει ότι τα στελέχη πρέπει να σχηματίσουν και να καθοδηγήσουν μια ομάδα διαχείρισης κινδύνων κυβερνοχώρου που μπορεί να αντιμετωπίσει τα ζητήματα της ασφάλεια του κυβερνοχώρου που θα προκύπτουν από στρατηγική άποψη. Αυτή η ομάδα θα πρέπει να λάβει γνώση από τους άμεσα ενδιαφερόμενους και τους σχετικούς επαγγελματίες, να εκτιμάει τα δεδομένα και τα σχόλια ανατροφοδότησης καθώς και να παίρνει βασικές στρατηγικές αποφάσεις από την πλευρά της επιχείρησης.

3^{ο} Βήμα: Τακτές συνεδριάσεις της ομάδας διαχείρισης κίνδυνων κυβερνοχώρου

Όσον αφορά την πρωταρχική συνεδρίαση της ομάδας, η συνάντηση θα πρέπει να γίνει πρόσωπο με πρόσωπο, σε περίπτωση που κάτι τέτοιο αποτρέπεται λόγω γεωγραφικής απόστασης, τότε θα περατωθεί τουλάχιστον μέσω μιας τηλεδιάσκεψης.

Εν συνεχείαθα πρέπει να πραγματοποιούνται τακτικές προγραμματισμένες συνεδριάσεις, ιδανικά με τη μορφή τριμηνιαίων ελέγχων.Η συχνότητα αυτών των συναντήσεων είναι σημαντική, μιας και οι απειλές και επιθέσεις στον κυβερνοχώρο, καθώς και οι στρατηγικές μετριασμού τους, μεταβάλλονται διαρκώς.

4^{ο} Βήμα: Ανάπτυξη και υιοθέτηση ενός σχεδίου διαχείρισης των κινδύνων κυβερνοχώρου για όλα τα τμήματα της επιχείρησης

Η ομάδα διαχείρισης των κινδύνων κυβερνοχώρου πρέπει να καθορίσει ποιες δράσεις και ρόλους, είτε υφιστάμενους είτε καινούργιους, πρέπει να ανατεθούν σε κάθε λειτουργική περιοχή και να καθορίσουν τα μέσα με τα οποία θα επικοινωνούν και θα συντονίζονται μεταξύ τους οι λειτουργικές αυτές περιοχές. Το αποτέλεσμα θα πρέπει να είναι μια καλά καθορισμένη και δομημένη αρχιτεκτονική ασφάλειας πληροφοριών.

Το σχέδιο πρέπει να περιλαμβάνει διατάξεις για την συνεχή ενίσχυση της ευαισθητοποίησης των εργαζομένων όσον αφορά την κρισιμότητα των συστημάτων και των δεδομένων στον κυβερνοχώρο. Οι εργαζόμενοι θα πρέπει να έχουν κατανοήσει με σαφήνεια τις πολιτικές της εταιρείας σχετικά με την κατηγοριοποίηση και διατήρηση δεδομένων και την αντιμετώπιση των διαφόρων περιστατικώνπαραβίασής τους.Το εν λόγο σχέδιο θα πρέπει επίσης να περιλαμβάνει διατάξεις για την εξασφάλιση των διασυνδέσεων με τους επιχειρηματικούς εταίρους, τους προμηθευτές και άλλες απομακρυσμένες διασυνδέσεις της επιχείρησης.

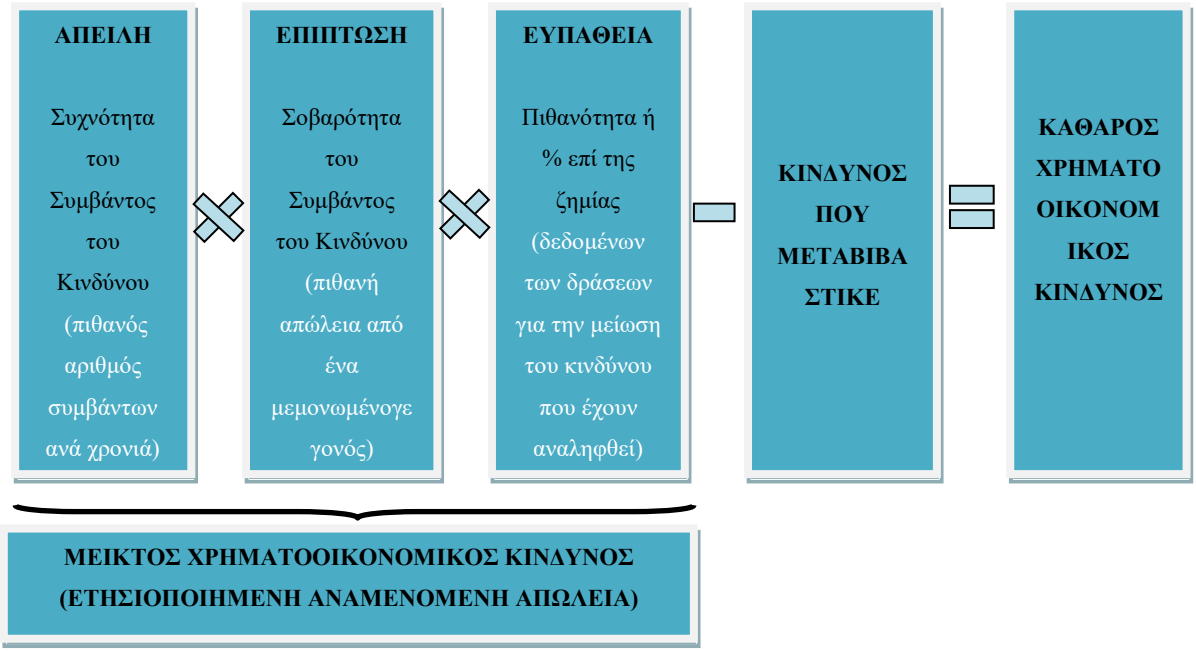
Τέλος, θα πρέπει να περιλαμβάνει ένα επίσημα τεκμηριωμένο σχέδιο αντιμετώπισης περιστατικών και επικοινωνίας σε περίπτωση κρίσεων για την ενημέρωση των ενδιαφερομένων (χρησιμοποιώντας ακόμη και τα μέσα μαζικής ενημέρωσης, όταν ενδείκνυται), δεδομένου ότι ακόμη και οι καλύτερα προστατευόμενες εταιρείες δεν μπορούν να εξαλείψουν τον πραγματικό κίνδυνο ενός κυβερνοχώρου που οδηγεί σε μια κρίση, της οποίας επιτακτική ανάγκη είναι η διαχείρισή της. Μετά από την εκδήλωση ενός περιστατικού που διακυβεύει την ασφάλεια του κυβερνοχώρου, μια αποτελεσματική επικοινωνιακή στρατηγική μπορεί να ελαχιστοποιήσει ουσιαστικά τις πιθανές οικονομικές ζημίες - συμπεριλαμβανομένου του "έμμεσου" κόστους δυνητικής ζημίας στη φήμη της εταιρείας, στο εμπορικό της σήμα, στην εμπιστοσύνη των πελατών της και στο ηθικό

των υπαλλήλων της, παράγοντες μπορούν να έχουν σημαντικό αντίκτυπο στην αξία των μετόχων της.

5^{ο} Βήμα: Ανάπτυξη και υιοθέτηση προϋπολογισμού για το συνολικό κόστος των κινδύνων κυβερνοχώρου

Με βάση το σχέδιο διαχείρισης των κινδύνων κυβερνοχώρου, η ομάδα που έχει συγκροτηθεί πρέπει να υπολογίζει τον ακαθάριστο οικονομικό κίνδυνο για τον οργανισμό. Πρωτίστως, είναι υψίστης σημασίας τα ανώτερα στελέχη να κατανοήσουντις πιθανές οικονομικές επιπτώσεις μιας επίθεσης στον κυβερνοχώρο. Είναι προφανές ότι ο αντίκτυπος αυτός θα εξαρτηθεί από το είδος της επιχείρησης καθώς και το είδος του περιστατικού μιας και το συνολικό κόστος ορισμένων τύπων επιθέσεων στον κυβερνοχώρο είναι ευκολότερο να εκτιμηθεί από άλλα.

Σύμφωνα με την μεθοδολογία, η πιο διαδεδομένη τεχνική υπολογισμού του κινδύνου του κυβερνοχώρου είναι η μέθοδος ALE (AnnualLossExpectancy), η οποία συνδυάζει την ετήσια αναμενόμενη απώλεια με την πιθανότητα και την σοβαρότητα των επιθέσεων, δίνοντας το ποσό που μια επιχείρηση αναμένει να χάσει σε ένα δεδομένο έτος στην πραγματικότητα. Σχηματικά η μέθοδος ALE παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 2: Μέθοδος ALE για τη μέτρηση των κινδύνων κυβερνοχώρου[54].

[54] Internet Security Alliance (ISA) & American National Standards Institute (ANSI) (2010), The financial management of cyber risk, An Implementation Framework for CFOs, published by ANSI

Είναι σημαντικό να γίνει κατανοητό ότι ο προσδιορισμός των παραπάνω παραγόντων πρέπει να πραγματοποιηθεί με μεγάλη ακρίβεια. Με άλλα λόγια, εκτός από την πιθανότητα απώλειας, υπάρχει και η πιθανότητα να είναι ακριβής η εκτίμηση της πιθανότητας απώλειας. Συνεπώς όταν οι παράγοντες αυτοί προσδιοριστούν με ακρίβεια, η μέθοδος αυτή παρέχει μια καλή βάση για την καθοδήγηση όλων των αποφάσεων διαχείρισης κινδύνου.

Η μεθοδολογία αναφέρει ότι με βάση την βιβλιογραφία (όπως για παράδειγμα από τους Gordonκαι Loeb) υπάρχουν διαθέσιμα και άλλα εργαλεία που μπορούν να βοηθήσουν τα στελέχη των επιχειρήσεων στην διαδικασία της αξιολόγησης του κόστους. Υπάρχουν και κάποιες γενικευμένες προσεγγίσεις για τον υπολογισμό του κόστους, όπως το 5-6% του προϋπολογισμού για τα συστήματα πληροφοριών ή το 1.5% των εσόδων μιας επιχείρησης (όπως προτείνουν αρχές όπως οι Forester ή Gartner).Όποια μέθοδο υπολογισμού του κόστους επιλέξει η κάθε επιχείρηση, είναι σημαντικό να δημιουργήσει αυτόν τον προϋπολογισμού μέσω της διατμηματικής ομάδας διαχείρισης του κινδύνου ώστε να υπάρχει μια γενικευμένη εικόνα για να παρθεί η τελική απόφαση.

6^{ο} Βήμα: Εφαρμογή, ανάλυση, έλεγχος και ανατροφοδότηση

Είναι σημαντικό το σχέδιο διαχείρισης των κινδύνων κυβερνοχώρου να αποτελείται, όπως επισημάναμε παραπάνω, από ακριβείς μετρήσεις και ότι αυτές οι μετρήσεις, συμπεριλαμβανομένων των ελέγχων και των δοκιμών διείσδυσης, πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα τόσο όσον αφορά τη διαχείριση των κινδύνων του κυβερνοχώρου όσο και τον προϋπολογισμότους.Τα αποτελέσματα αυτών των εξετάσεων και δοκιμών θα πρέπει να χρησιμοποιούνται ως ανατροφοδότηση για την ενημέρωση και αναβάθμιση κάθε τμήματος του σχεδίου διαχείρισης του κυβερνοχώρου.

Επίσης, θα πρέπει το σχέδιο διαχείρισης να καλύπτει τα βασικά ζητήματα ασφάλειας και να μην επικεντρώνεται σε εξειδικευμένους τύπους επιθέσεων. Οι επιχειρήσεις θα πρέπει να παρακολουθούν και να βελτιώνουν συνεχώς τις πολιτικές τους στον τομέα της ασφάλειας του κυβερνοχώρου στο πέρασμα του χρόνου, προκειμένου να μεγιστοποιήσουν την ασφάλειά τους και κατά συνέπεια και την κερδοφορία τους.

Αξίζει να αναφερθεί ότι σύμφωνα με την έρευνα που διεξήγαγε η IBM,το μέσο συνολικό κόστος των κυβερνοεπιθέσεων που δέχθηκαν οι εταιρίες που είχαν συγκροτημένη ομάδα διαχείρισης κινδύνων κυβερνοχώρου (IncidentResponseTeam, IRTeam) και πραγματοποιούσαν συχνούς ελέγχους πάνω στο σχέδιο διαχείρισης των κινδύνων αυτών,ήταν $1.23 εκατομμύρια χαμηλότερο σε σχέση με άλλες εταιρίες που δεν διέθεταν ούτε ομάδα, ούτε σχέδιο διαχείρισης κινδύνων κυβερνοχώρου[55]. Επίσης, με βάση την ίδια έρευνα παρατηρήθηκε ότι οι επιχειρήσεις που είχαν υιοθετήσει αυτοματοποιημένες μεθόδους ασφαλείας -οι οποίες μείωναν ή ακόμη και εξάλειφαν την ανθρώπινη επέμβαση-, είδαν σημαντικά χαμηλότερα κόστη μετά από ένα περιστατικό παραβίασης δεδομένων. Συγκεκριμένα οι επιχειρήσεις που είχαν πλήρως αυτοματοποιημένα συστήματα σημείωναν κόστος $2.65 εκατομμύρια, ενώ αυτές που δεν είχαν καθόλου αυτοματοποιημένα συστήματα σημείωναν κόστος $5.16 εκατομμύρια, μια διαφορά του ύψους του 95%[56].

2.5 ΑσφάλισηΚυβερνοχώρου

Η *Ασφάλιση Κυβερνοχώρου*είναι μια τεχνική διαχείρισης κινδύνου, στην οποία οι κίνδυνοι των χρηστών του δικτύου μεταφέρονται σε μια ασφαλιστική εταιρεία έναντι αντιτίμου, δηλαδή ενός ασφαλίστρου[57]. Η Gartner έχει ορίσει την ασφάλεια στον κυβερνοχώρο ως "προστασία έναντι των απωλειών που σχετίζονται με τους κινδύνους του κυβερνοχώρου, όπως η κλοπή / απώλεια δεδομένων, η διακοπή της επιχείρησης λόγω δυσλειτουργίας ή ιού υπολογιστών και πρόστιμα ή απώλεια εισοδήματος εξαιτίας διακοπών δικτύου, ή /και παραβιάσεων δικτύων"[58].Η ασφάλιση κυβερνοχώρου αποτελεί ένα σημαντικό εργαλείο διαχείρισης κινδύνων. Συμπληρωματικά με τις τεχνολογικές λύσεις για την ασφάλεια στον κυβερνοχώρο, η ασφάλιση κυβερνοχώρου μπορεί να μετριάσει την απώλεια του

[55] Cost of Data Breach Report 2019, IBM

[56] Cost of Data Breach Report 2019, IBM

[57] Shoukat, S. & Bashir, A. (2017), "*Cyber Crime- Techniques, Prevention and Cyber Insurance*", International Journal of Computing and Network Technology, Volume 6, No1

[58] Odel, L.A., Fauntleroy, J.C. & Wagner, R.R. (2015), "*Cyber Insurance - Managing Cyber Risk*", (No. IDA-NS-D-5481), INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA

στοχευόμενου συστήματος και να αυξήσει την ανθεκτικότητα του θύματος, επιτρέποντας την ταχεία ανάκαμψη του συστήματος και των χρηματοπιστωτικών συστημάτων από τα περιστατικά κυβερνοεπιθέσεων[59]. Η υιοθέτηση της ασφάλειας στον κυβερνοχώρο θα βοηθήσει το ηλεκτρονικό εμπόριο και γενικότερα τους ηλεκτρονικούς οργανισμούς να προωθήσουν τις συναλλαγές μέσω ηλεκτρονικών συστημάτων μιας και οι πιθανές απώλειες από τα περιστατικά παραβίασης θα αποζημιώνονται από τις ασφαλιστικές εταιρίες. Ολοένα και περισσότερες επιχειρήσεις πλέον αρχίζουν να επενδύουν σε ασφαλιστικά προϊόντα για την αντιμετώπιση των κυβερνοεπιθέσεων, κάτι που αυξάνει την εμπιστοσύνη των πελατών τους δημιουργώντας εν κατακλείδι έναν θετικό αντίκτυπο για την ίδια την επιχείρηση[60].

Η ασφάλιση για τους κινδύνους του κυβερνοχώρου έχει κάνει την είσοδό της στις ασφαλιστικές αγορές τα τελευταία μόλις 20 χρόνια και ιδίως στην Αμερική. Μέχρι πρότινος τα ασφαλιστικά πακέτα που παρέχονταν στις επιχειρήσεις περιείχαν ασφάλιση ιδιοκτησίας -που κάλυπτε τις ζημίες των φυσικών περιουσιακών της στοιχείων-, καθώς και ασφάλιση αστικής ευθύνης. Και οι δύο αυτές μορφές ασφάλισης δεν περιλάμβαναν τους κινδύνους που ελλοχεύουν στον κόσμο του κυβερνοχώρου[61].

Σήμερα, αυτού του είδους η ασφάλιση θεωρείται ότι βρίσκεται ακόμη στα πρώιμα στάδιά της διότι αντιμετωπίζει διάφορες δυσχέρειες. Οι κυριότερες δυσκολίες περιλαμβάνουν την τυχαία εμφάνιση των ζημιών, την ασύμμετρη πληροφόρηση και τα όρια κάλυψης[62]. Ένα σημαντικό πρόβλημα που εντάσσεται και μέσα στην τυχαία εμφάνιση των ζημιών, είναι η έλλειψη στοιχείων η οποία κατά κύριο λόγο απορρέει από το γεγονός ότι η ουσιαστική πλειονότητα των παραβιαζόμενων επιχειρήσεων δεν αποκαλύπτουν ότι έχουν πέσει θύμα κυβερνοεπιθέσεων λόγω του φόβου τους για βλάβη της φήμης τους, νομικές ευθύνες και τον αυξημένο εξονυχιστικό έλεγχο που θα δεχθούν από τους πελάτες τους και το ευρύ κοινό[63]. Συνεπώς η αποσιώπηση της πραγματικής συχνότητας των περιστατικών

[59] Zhu, Q. (2018), "*Cyber Insurance*", New York University, Brooklyn

[60] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhuklan, S.K. (2013), "*Cyber-risk decision models: To insure IT or not?*", Decision Support Systems, Volume 56, December 2013, Pages 11-26

[61] Eling, M. & Werner, S. (2016), "*What do we know about cyber risk and cyber risk insurance?*", The Journal of Risk Finance Vol. 17 No. 5, 2016, pp. 474-491

[62] Biener, C., Eling, M. & Wirfs, J.H (2015), "*Insurability of Cyber Risk: An Empirical Analysis*", Geneva Papers on Risk and Insurance, Vol. 40, No. 1, 2015

[63] MMC Cyber Handbook 2019, Perspectives on Cyber Risk in the Digital Era, Marsh & McLennan Insights

παραβίασης δεδομένων οδηγεί στην υποτίμηση των περισσότερων μοντέλων που έχουν αναπτυχθεί για την ασφάλιση του κυβερνοχώρου[64].

Σύμφωνα με έρευνα της PwC η σημερινή ανεξάρτητη αγορά ασφάλισης του κυβερνοχώρου στις ΗΠΑ υπολογίζεται στα 2.5 έως 3.5 δισεκατομμύρια US$ ετησίως και αναμένεται να αυξηθεί κατά άλλα 2 δισεκατομμύρια δολάρια κατά τα επόμενα τρία χρόνια[65]. Η μελέτη της Marsh για το 2018διαπίστωσε ότι από το σύνολοτων επιχειρήσεων που πήραν μέρος στην έρευνα που διεξήγαγε, το 56% διέθεταν ήδη ασφάλεια για τους κινδύνους του κυβερνοχώρου, ενώ το 30% δεν είχε καμία κάλυψη έναντι των κινδύνων αυτών και ούτε σκόπευε να αγοράσει[66].

Υπάρχουν δύο είδη ασφαλιστικής κάλυψης, αυτές του πρώτου και τρίτου βαθμού. Η διαφορά τους έγκειται στα μέρη που καλύπτονται από την ασφάλεια, η κάλυψη πρώτου βαθμού αφορά τις ζημίες που θα υποστεί ο ίδιος ο ασφαλιζόμενος, ενώ η κάλυψη τρίτου βαθμού αφορά τις ζημίες που θα υποστούν οι τρίτοι εκτός της επιχείρησης[67].Στον απόηχο μιας παραβίασης δεδομένων, η ασφαλιστική κάλυψη πρώτου βαθμού που παρέχεται στον ασφαλιζόμενο περιλαμβάνει την ενημέρωση των πελατών ότι οι πληροφορίες τους διακυβεύονται ή έχουν εκτεθεί, τις υπηρεσίες παρακολούθησης των πιστώσεων για τους πελάτες που έχουν πληγεί από την παραβίαση, τις εκστρατείες δημοσίων σχέσεων για την αποκατάσταση της φήμης της επιχείρησης, αποζημιώσεις για τα έσοδα που η επιχείρηση δεν ήταν σε θέση να κερδίσει μέχρι να ανακάμψει από την παραβίαση, τα έξοδα που σχετίζονται με την κανονιστική συμμόρφωση, και την πληρωμή σε έναν κυβερνο-εκβιασμό που απειλεί να εκδώσει δεδομένα που έχει ανακτήσει ή απειλεί να πραγματοποιήσει μια επίθεση.Η κάλυψη από τρίτους προστατεύει μια επιχείρηση όταν οι πελάτες της υφίστανται παραβίαση λόγω υποτιθέμενου σφάλματος από την πλευρά της επιχείρησης και καλύπτουν

---

[64] MMC Cyber Handbook 2019, Perspectives on Cyber Risk in the Digital Era, Marsh & McLennan Insights

[65] Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey, 2018

[66] 2018 Cyber Risk Perception Survey Report by Marsh & McLennan Agency

[67] Marotta, A., Martinelli, F., Nanni, S., Orlando, A. &Yautsiukhin, A. (2017), "*Cyber-insurance survey*", Computer Science Review Vol. 24, pp 35–61

συμβιβασμούς ή αποφάσεις και τυχόν δικαστικά έξοδα που προκύπτουν από την παραβίαση των δεδομένων[68].

Οι περισσότερες ασφάλειες αποτελούνται από τέσσερα στοιχεία: σφάλματα και παραλείψεις, ευθύνη μέσων μαζικής ενημέρωσης, ασφάλεια δικτύων και προστασία ιδιωτικότητας. Όσον αφορά την ασφάλιση για σφάλματα και παραλείψεις, καλύπτονται δυνητικά συμβάντα που αφορούν την παροχή υπηρεσιών όπως υπηρεσίες ανάπτυξης λογισμικού ή συμβουλευτικές υπηρεσίες που σχετίζονται με συστήματα πληροφορικής. Η ασφάλιση για την ευθύνη στα μέσα μαζικής ενημέρωσης καλύπτει περιστατικά που σχετίζονται με πνευματική ιδιοκτησία ή παραβίαση πνευματικών δικαιωμάτων / εμπορικού σήματος, δυσφήμησης και συκοφαντίας. Η ασφάλεια δικτύου καλύπτει μια πιθανή αποτυχία στην ασφάλεια του δικτύου, η οποία μπορεί να οδηγήσει σε παραβιάσεις δεδομένων, καταστροφή δεδομένων, μετάδοση ιών και εκβιασμούς. Τέλος, όσον αφορά την προστασία της ιδιωτικότητας, η ασφάλειακαλύπτει την απώλεια προσωπικών δεδομένων, συμπεριλαμβανομένων φυσικών αρχείων, απώλεια φορητού υπολογιστή που περιέχει προσωπικές πληροφορίες, αποστολή αρχείου που περιέχει δεδομένα πελατών σε λάθος διεύθυνση ηλεκτρονικού ταχυδρομείου ή επιστροφή μισθωμένου εξοπλισμού χωρίς καθάρισμα των δεδομένων του σκληρού δίσκου[69].

2.5.1 ΑσφάλιστροΚυβερνοχώρου

Αν και η ασφάλιση του κυβερνοχώρου όπως ήδη αναφέραμε αναπτύσσεται τις τελευταίες δεκαετίες με ραγδαίους ρυθμούς και γίνεται ολοένα και πιο ευρέως αποδεκτή από τις επιχειρήσεις, η *εκτίμηση του ασφαλίστρου* που απαιτείται για την πραγματοποίηση της ασφάλισης αποτελεί μια σημαντική πρόκληση για την ασφάλεια του κυβερνοχώρου. Για το ακριβές υπολογισμού του ασφαλίστρου προαπαιτείτε τόσο από τις ίδιες τις επιχειρήσεις όσο και από τις ασφαλιστικές εταιρίες να κατανοήσουν, τουλάχιστον κατά προσέγγιση, την αξία

[68] Odel, L.A., Fauntleroy, J.C. & Wagner,R.R. (2015),"*Cyber Insurance – Managing Cyber Risk*", (No. IDA-NS-D-5481), INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA

[69] Odel, L.A., Fauntleroy, J.C.& Wagner, R.R. (2015), "*Cyber Insurance – Managing Cyber Risk*", (No. IDA-NS-D-5481), INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA

των περιουσιακών τους στοιχείων, είτε αυτά αφορούν φυσικά είτε ψηφιακά στοιχεία[70]. Για να γίνει το παραπάνω πιο κατανοητό, ενώ η εκτίμηση της αξίας ενός σκληρού δίσκου είναι απλή, η αξία των δεδομένων που εμπεριέχονται σ' αυτόν είναι πολύ πιο δύσκολο να εκτιμηθεί.

Σύμφωνα με τη βιβλιογραφία, δεν υπάρχει κάποιος κοινώς αποδεκτός τρόπος μέτρησης της αξίας των ψηφιακών περιουσιακών στοιχείων κυρίως εξαιτίας της αδυναμίας κατανόησης του ότι οι πληροφορίες αποτελούν ένα υποβόσκων περιουσιακό στοιχείο που προσδίδει αξία και οικονομικά οφέλη στην επιχείρηση που τις διαθέτει. Μέχρι τώρα οι επιχειρήσεις εφάρμοζαν εξειδικευμένες μεθόδους μέτρησης της αξίας των ψηφιακών στοιχείων βασιζόμενοι για παράδειγμα στο κόστος παραγωγής ή αντικατάστασής τους. Η σύνθεση της ψηφιακής αξίας μιας επιχείρησης αποτελεί το κύριο χαρακτηριστικό της και είναι αυτό που θα προσδιορίσει και τον κίνδυνο του κυβερνοχώρου στον οποίο είναι εκτεθειμένη[71].

Η Keyun Ruan λοιπόν εισάγει την έννοια του *Cybernomics* δηλαδή της *Κυβερνο-οικονομίας*. Η κυβερνο-οικονομίασυνδυάζει την διαχείριση των κινδύνων κυβερνοχώρου με την οικονομία υπό τη παγκόσμια σκοπιά και τη σκοπιά της ίδιας της επιχείρησης και του χαρτοφυλακίου, με σκοπό να μελετήσει τις απαιτήσεις μιας "τράπεζας" δεδομένων η οποία θα βελτιώσει τις λύσεις ανάλυσης κινδύνου όσον αφορά πρώτον την αποτίμηση των ψηφιακών περιουσιακών στοιχείων, δεύτερον τη μέτρηση της έκθεσης των στοιχειών αυτών στον κίνδυνο και τρίτων τη βελτιστοποίηση της χρήσης των κεφαλαίων για τη διαχείριση του εναπομείναντα κινδύνου κυβερνοχώρου. Βασιζόμενη αρχικά στα χαρακτηριστικά κάποιων μεθόδων υπολογισμού κινδύνου, όπως η VaR και η MM, γίνεται ανάπτυξη δύο καινούργιων μεθόδων της BM και της hekla για την μέτρηση της αποτελεσματικότητας του κόστους κάποιων παραγόντων ελέγχου, οι μέθοδοι αυτοί περιγράφουν την "προθυμία" της επιχείρησης να πληρώσει για τη μείωση του κινδύνου κυβερνοχώρου που διατρέχει[72].

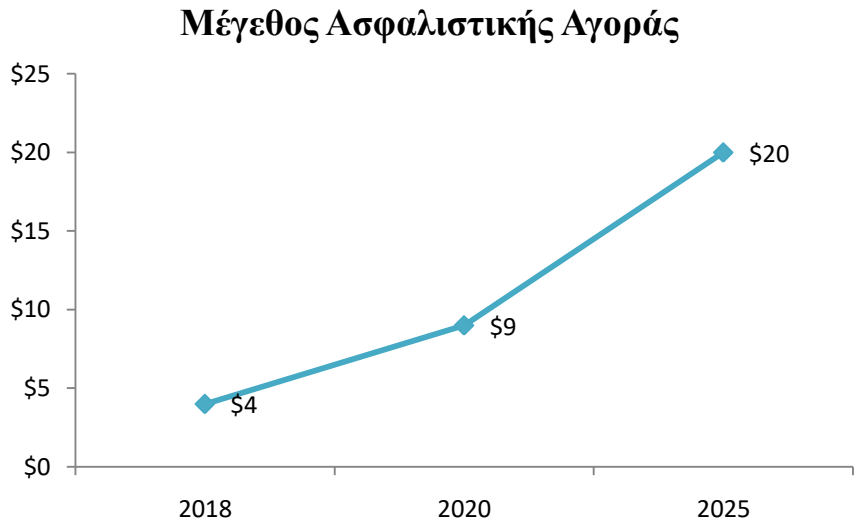
[70] Lin, Z., Parsa, R., Rees Ulmer, J. & Sapp, T. (2018), "*Pricing Cyber Security Insurance: A Copula Model Using an Objective, Verifiable, Loss Measure*", (July 17, 2018)

[71] Ruan, K. (2016), "*Introducing cybernomics: A unifying economic framework for measuring cyber risk* ", Computers & Security, Vol. 65, pp. 77-89

[72] Ruan, K. (2016), "*Introducing cybernomics: A unifying economic framework for measuring cyber risk* ", Computers & Security, Vol. 65, pp. 77-89

Η Αμερικάνικη αγορά κυβερνοασφάλισης είναι αυτή που πρωτοστατεί μεταξύ των υπολοίπων αγορών παγκοσμίως[73] και μάλιστα ηVerisk αναφέρει ότι αναμένεται να ανέλθει σε 6.2 δισεκατομμύρια US$ μέχρι το 2020, από τα περίπου 2.5 δισεκατομμύρια US$ γραπτών ασφαλίστρων που σημείωσε το 2016[74].

Στο παρακάτω διάγραμμα παρουσιάζεται η αυξανόμενη πορεία της αξίας των ασφαλίστρων κυβερνοχώρου παγκοσμίως σε US$ σύμφωνα με την στατιστική εταιρία Statista για τα έτη 2018, 2020 και 2025[75].



Διάγραμμα 6: Η αξία των ασφαλίστρων κυβερνοχώρου παγκοσμίως για τα έτη 2018, 2020 και 2025[76].

Ο λόγος που η τιμή των ασφαλίστρων βρίσκεται σε τόσο υψηλά επίπεδα έγκειται στην έλλειψη δεδομένων για τα περιστατικά των κυβερνοεπιθέσεων. Οι ασφαλιστές προσπαθούν να προστατευθούν μιας και δεν μπορούν να υπολογίσουν με ακρίβεια τις δυνητικές ζημίες που θα προκύψουν από ένα περιστατικό παραβίασης ώστε να τιμολογήσουν καταλλήλως και την ασφάλισή τους. Σύμφωνα με μία παλαιότερη έρευνα της PonemonInstitute από το ποσοστό των επιχειρήσεων που δεν διέθεταν κάποιο προϊόν

[73] Kshetri, N. (2018), "*The Economics of Cyber-Insurance*", IEEE IT Professional, Vol. 20, pp. 9-14

[74] Sizing the Standalone Commercial Cyber Insurance Market, 2018 Verisk

[75] https://www.statista.com/statistics/976526/global-cyber-insurance-market-size/

[76] https://www.statista.com/statistics/976526/global-cyber-insurance-market-size/

κάλυψης, ο σημαντικότερος λόγος (52%) ήταν η υπερβολικά υψηλή τιμή του ασφαλίστρου[77]. Βέβαια αξίζει να σημειωθεί ότι από τις επιχειρήσεις που ήταν ασφαλισμένες, το 62% θεωρούσε την τιμή του ασφαλίστρου δίκαιη σε σχέση με την προστασία που της παρείχε[78].

Η τιμολόγηση των ασφαλίστρων είναι ένα από τα πιο καίρια ζητήματα στον χώρο της ασφάλισης όπως προαναφέραμε και πολλοί είναι αυτοί που το επιχείρησαν σύμφωνα με την βιβλιογραφία. Με βάση τους Bandyopadhyaykαι Mookerjee υπάρχουν δύο στρατηγικές τιμολόγησης: η παραδοσιακή και η προσαρμοσμένη. Στην παραδοσιακή στρατηγική τιμολόγησης, υπολογίζεται το ασφάλιστρο όπως συμβαίνει σε οποιοδήποτε τυποποιημένο ασφαλιστικό συμβόλαιο χωρίς να λαμβάνονται υπόψη οι συνέπειες των δευτερογενών επιπτώσεων στην επιχείρηση, όπως η βλάβη στην φήμη της. Αντιθέτως η προσαρμοσμένη στρατηγική λαμβάνει υπόψη την πιθανότητα εμφάνισης τωνμη άμεσων επιπτώσεων. Οι παραπάνω συγγραφείς καταλήγουν ότι η δεύτερη στρατηγική είναι η ορθότερη μιας και τα έμμεσα κόστη των κυβερνοεπιθέσεων είναι αρκετά σημαντικά και ζημιογόνα[79].

Ένας άλλος τρόπος τιμολόγησης που προτείνεται από τους Lin, Parsa, Ulmer καιSappείναι ένα μοντέλο που αφορά τις επιχειρήσεις με διασυνδεδεμένο χαρακτήρα, όπως είναι αυτές του ίδιου είδους, ή αυτές που χρησιμοποιούν τον ίδιο εξωτερικό προμηθευτή δεδομένων. Αυτό το μοντέλο καταγράφει την συσχετιζόμενη φύση των παραβιάσεων του κυβερνοχώρου και των δεδομένων, που τείνουν να εμφανίζονται σε ομάδες εταιρειών εντός μιας σύντομης χρονικής περιόδου και μπορεί να συνθέσει τις ζημίες που θα έχει ο ασφαλιστής όταν χτυπηθούν πολλοί πελάτες του[80].

Τέλος, οι συγγραφείς Mukhopadhyay, Chatterjee, Saha, Mahanti και Sadhukhanπροτείνουν ένα μοντέλο UBPP (UtilityBasedPreferentialPricing) για τον υπολογισμού του ασφαλίστρου από τις ασφαλιστικές εταιρίες και λαμβάνει υπόψη του το προφίλ κινδύνου όπως είναι τα έσοδα, τα σχέδια ανάπτυξης και άλλα οικονομικά

[77] Managing cyber security as a business risk: Cyber insurance in the digital age, Ponemon Institute LLC 2013

[78] Managing cyber security as a business risk: Cyber insurance in the digital age, Ponemon Institute LLC 2013

[79] Bandyopadhyay, T. & Mookerjee, V. (2017), "*A model to analyze the challenge of using cyber insurance*", Information Systems Frontiers, Volume 21, Issue 2, pp 301–325

[80] Lin, Z., Parsa, R., Rees Ulmer, J. & Sapp, T. (2018), "*Pricing Cyber Security Insurance: A Copula Model Using an Objective, Verifiable, Loss Measure*", (July 17, 2018)

χαρακτηριστικά της δυνητικά ασφαλισμένης επιχείρησης. Μια σωστή τιμολόγηση του ασφαλίστρου βοηθά τις ασφαλιστικές εταιρείες να προσελκύσουν πελάτες και επίσης να εξασφαλίσει ότι εταιρείες αυτές στον τομέα του κυβερνοχώρου δεν είναι προκαθορισμένες[81].

[81] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. &Sadhuklan, S.K. (2013), "*Cyber-risk decision models: To insure IT or not*?", Decision Support Systems, Volume 56, December 2013, Pages 11-26

ΚΕΦΑΛΑΙΟ 3

ΘΕΣΜΙΚΟΠΛΑΙΣΙΟ

3.1 Ορισμός Προσωπικών Δεδομένων

Σύμφωνα με την επίσημη εφημερίδα της Ευρωπαϊκής Ένωσηςως *δεδομένα προσωπικού χαρακτήρα*θεωρούμε κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων[82]»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, αριθμό ταυτότητας, δεδομένα θέσης, επιγραμμικό αναγνωριστικό ταυτότητας ή έναν ή περισσότερους παράγοντες που προσιδιάζουν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου[83].

3.2 Το χρονικό του κανονισμού για την προστασία των δεδομένων

Ο νόμος που θεωρείται ως ο πρωτοπόρος στην προστασία δεδομένων εγκρίθηκε το 1970 στο Γερμανικό ομοσπονδιακό κράτος της Έσσης, ο οποίος δεν αφορούσε διεθνείς μεταφορές δεδομένων. Με το πέρασμα των χρόνων και την έγκριση των μετέπειτα νόμων για την

[82]Ως υποκείμενα των δεδομένων νοούνται άτομα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία, όπως είναι οι πελάτες και οι επισκέπτες του ιστότοπου μιας επιχείρησης.

[83]ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (27 Απριλίου 2016) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

προστασία δεδομένων τόσο στο εσωτερικό της Ευρωπαϊκής Ένωσης όσο και εκτός αυτής, έγινε αντιληπτό ότι ήταν μάταιο να δημιουργούνται νομοθετικά πλαίσια για την προστασία των προσωπικών δεδομένων εάν αυτά τα μέτρα προστασίας μπορούσαν εύκολα ναπαραβιαστούν απλώς μεταφέροντας τα δεδομένα των ατόμων που σχεδιάστηκαν να προστατεύουν σε άλλες δικαιοδοσίες[84].

Τα πρώτα δύο νομοθετικά πλαίσια για την προστασία των δεδομένων αποτέλεσαν οι κατευθυντήριες γραμμές ιδιωτικότητας του Οικονομικού Οργανισμού Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) το 1980 και το Συμβούλιο της Ευρωπαϊκής Σύμβασης για την προστασία των ατόμων όσον αφορά την αυτόματη επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Συμβούλιο της Ευρώπης του 1981), γνωστή και ως Σύμβαση 108. Αν και τα δύο αυτά πλαίσια είχαν μια κοινή προοπτική, μπορούμε να αναγνωρίσουμε μια διάκριση όσον αφορά την προσέγγιση της μεταφοράς των δεδομένων. Από τη μια η Σύμβαση 108 είχε καθιερώσει μια οριστική λίστα δικαιοδοσιών στις οποίες τα δεδομένα θα επιτρέπονταν να μεταφερθούν (για παράδειγμα άλλα συμμετέχοντα έθνη), ενώ από την άλλη οι κατευθυντήριες γραμμές του ΟΟΣΑ για την ιδιωτικότητα επέτρεπαν να τεθούν περιορισμοί στην μεταφορά δεδομένων ακόμη και σε χώρες που δεν τηρούσαν ακόμη αυτές τις κατευθυντήριες γραμμές στο σύνολό τους. Η παραπάνω διαφορά οδήγησε τελικά στην δημιουργία δυο διαφορετικών προσεγγίσεων αυτές της επάρκειας και την λογοδοσίας, για την ρύθμιση της διεθνούς μεταφοράς προσωπικών δεδομένων.

Η *προσέγγιση τηςεπάρκειας* απαιτεί οι μεταφορές να συμμορφώνονται σε έναν μηχανισμό ο οποίος έχει εγκριθεί εκ των προτέρων από κάποια αρχή για να δηλώσει ότι εγγυάται την προστασία των δεδομένων, ως έναν επιτρεπτό βαθμό, στην ξένη δικαιοδοσία.

Αντιδιαμετρικά, η *προσέγγιση της ευθύνης* απαιτεί από την οντότητα που επιθυμεί να μεταφέρει προσωπικά δεδομένα να προβεί σε μια δική της αυτοσχέδια αξιολόγηση και να καθορίσει για τον εαυτό της τις απαραίτητες διασφαλίσεις ώστε η μεταφορά να θεωρηθεί επιτρεπτή[85]. Η προσέγγιση της επάρκειας ενισχύθηκε από μεταγενέστερες εξελίξεις στην Ευρώπη που θα αναφερθούν παρακάτω, όπως η Οδηγία Ευρωπαϊκής Ένωσης του 1995 (Data

[84] Phillips, M. (2018), "*International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*", Human Genetics, Vol 137, Issue 8, pp. 575-582

[85] Phillips, M. (2018), "*International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*", Human Genetics, Vol 137, Issue 8, pp. 575-582

Protection Directive 1995) και ο διάδοχός της, ο Γενικός Κανονισμός Προστασίας Δεδομένων του 2016 (General Data Protection Regulation, GDPR)[86].

Το χρονοδιάγραμμα[87] των νομοθετικών κανονισμών για την προστασία των προσωπικών δεδομένων ξεκινά από τη δεκαετία του ’80 και συγκεκριμένα το 1984 όπου εγκρίθηκε ο Νόμος περί Προστασίας Δεδομένων (DataProtectionAct) στο Ηνωμένο Βασίλειο. Εισήχθησαν οι βασικοί κανόνες εγγραφής για τους χρήστες όσον αφορά τα δεδομένα και τα δικαιώματα πρόσβασης σ΄αυτά τα δεδομένα των ατόμων που είναι συνδεδεμένα με αυτά[88]. Καθώς η τεχνολογία εξελισσόταν και ανακαλύφθηκε το Διαδίκτυο, η Ευρωπαϊκή Ένωση αναγνώρισε την επιτακτική ανάγκη για πιο σύγχρονες μεθόδους προστασίας. Έτσι το 1995 εγκρίνεται η Οδηγία Ευρωπαϊκής Ένωσης (Data Protection Directive) θεσπίζοντας ελάχιστα πρότυπα για την προστασία της ιδιωτικότητας και της ασφάλειας, βάσει των οποίων κάθε κράτος μέλος βασίζεται στον δικό του νόμο εφαρμογής[89]. Εν έτη 1998 στο Ηνωμένο Βασίλειο εγκρίνεται ένας νέος νόμος, που αντικαθιστά των Νόμο περί Προστασίας Δεδομένων του 1984, σύμφωνα με τον οποίο τα μεμονωμένα άτομα είχαν το νόμιμο δικαίωμα να ελέγχουν τις πληροφορίες που τους αφορούσαν. Ο νόμος αυτός όρισε οκτώ αρχές προστασίας δεδομένων για να διασφαλίσει την νόμιμη επεξεργασία δεδομένων[90].

Το 2000 αναπτύχθηκαν οι Αρχές για την Προστασία της Ιδιωτικότητας στο πλαίσιο του Διεθνούς Ασφαλούς Λιμένα (International Safe Harbor Privacy Principles) προκειμένου να αποτρέψουν ιδιωτικούς οργανισμούς εντός της Ευρωπαϊκής Ένωσης ή των Ηνωμένων Πολιτειών, οι οποίοι αποθηκεύουν δεδομένα πελατών,να αποκαλύψουν τυχαία ή να χάσουν προσωπικές πληροφορίες[91]. Το 2012 μερικούς μήνες μετά από μια μήνυση που υπέστη η Google, η Ευρωπαϊκή Επιτροπή ανακοινώνει τα σχέδιά της για έναν Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) που θα ενίσχυε το νομοθετικό πλαίσιο του 1995. Το 2015 αναιρούνται οι Αρχές για την Προστασία της Ιδιωτικότητας στο πλαίσιο του Διεθνούς

[86] Phillips, M. (2018), "*International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*", Human Genetics, Vol. 137, Issue 8, pp. 575-582

[87] https://www.privacyrisksadvisors.com/gdpr-infographic/

[88] https://www.pinsentmasons.com/out-law/guides/data-protection

[89] https://gdpr.eu/what-is-gdpr/

[90] https://en.wikipedia.org/wiki/Data_Protection_Act_1998

[91] https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

Ασφαλούς Λιμένα (International Safe Harbor Privacy Principles). Η πορεία των κανονισμών περί της προστασίας δεδομένων φτάνει στο πρόσφατο παρελθόν, με το GDPR να τίθεται σε ισχύ το 2016 μετά τη διάσκεψη του Ευρωπαϊκού Κοινοβουλίου και από τις 25 Μαΐου του 2018 όλοι οι οργανισμοί είναι πλέον υποχρεωμένοι να συμμορφώνονται με τις διατάξεις του, αντικαθιστώντας την προηγούμενη νομοθεσία 95/46/ΕΚ.

Σήμερα εν έτη 2019 με βάση την έρευνα που διεξήγαγε η Cisco το 59% των επιχειρήσεων που έλαβαν μέρος σ' αυτήν καλύπτουν τις περισσότερες αν όχι όλες απαιτήσεις του GDPR, το 29% αναμένουν μέσα στο επόμενο έτος να καλύψουν τις περισσότερες απαιτήσεις του, το 9% θα χρειαστεί πάνω από έναν χρόνο να συμμορφωθεί με τις απαιτήσεις του νόμου, ενώ μόλις το 3% δεν έχει εφαρμόσει καθόλου το GDPR και θεωρούν ότι δεν είναι κάτι που τους αφορά[92].

3.3 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR), 2016/679, είναι ένας κανονισμός της νομοθεσίας της ΕΕ περί της προστασίας των δεδομένων και της ιδιωτικότητας για όλους τους μεμονωμένους πολίτες της Ευρωπαϊκής Ένωσης (ΕΕ) και του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).

Οαπώτεροςσκοπόςτου *GDPR*είναι κατά κύριο λόγο να εναποθέσει στα χέρια των μεμονωμένων ατόμων τον έλεγχο των προσωπικών τους δεδομένων και να αποτελέσει έναν απλούστερο και ενοποιημένο κανονισμό εντός της ΕΕ.Η μεγαλύτερη διαφορά που επιφέρει το GDPRστο μέχρι πρότινος νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων έγκειται στο γεγονός της πιο διευρυμένης δικαιοδοσίας, μιας και πλέον αφορά όλες τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα υποκειμένων (datasubjects) που θεωρούνται κάτοικοι Ευρωπαϊκής Ένωσης, ανεξαρτήτως της τοποθεσίας της ίδιας της επιχείρησης. Πριν από την εφαρμογή του γενικού αυτού κανόνα, όπως είδαμε στην

[92] Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

προηγούμενη παράγραφο,υπήρχε μια σύγχυση όσον αφορά την εδαφική εφαρμογή των νομοθετικών πλαισίων.

3.3.1 Εδαφική εφαρμογή του GDPR

Το GDPR καθιστά σαφή την εφαρμογή του στο άρθρο 3 τονίζοντας ότι ισχύει για την επεξεργασίαδεδομένων προσωπικού χαρακτήρα από άτομα της ΕΕ που ελέγχουν και επεξεργάζονται τα δεδομένααυτά, ανεξάρτητα από το εάν η επεξεργασία πραγματοποιείται στην ΕΕ ή όχι. Ισχύει επίσης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα των υποκειμένωντων δεδομένων στην ΕΕ από ένα άτομο που ελέγχει ή επεξεργάζεταιδεδομένα και δεν είναι εγκατεστημένος στην ΕΕεάν οι δραστηριότητές του αφορούν την προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή ή όχι) και την παρακολούθηση της συμπεριφοράς τους που λαμβάνει χώρα εντός της ΕΕ. Οι επιχειρήσεις εκτός ΕΕ που επεξεργάζονται τα δεδομένα των πολιτών της ΕΕ πρέπει επίσης να διορίσουν εκπρόσωπο στην ΕΕ[93].

3.3.2 Απαιτήσεις του GDPR

Για να θεωρηθούν οι επιχειρήσεις ότι έχουν συμμορφωθεί με τους κανονισμούς της ισχύουσας νομοθεσίας θα πρέπει να τηρούν κάποιους κανόνες – απαιτήσεις[94]. Το άρθρο 15 δίνει το δικαίωμα της πρόσβασης στους Ευρωπαίους πολίτες, το οποίο έμμεσα απαιτεί οι επιχειρήσεις να παρουσιάζουν με λεπτομέρειαποια προσωπικά δεδομένα έχουν επεξεργαστεί και πως, σε περίπτωση που ζητηθούν. Τα άρθρα 33 και 34 απαιτούν από τις επιχειρήσεις να αναφέρουν τα περιστατικά παραβίασης δεδομένων σε εποπτικές αρχές, μέσα στις πρώτες 72

[93]ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (27 Απριλίου 2016) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

[94]https://www.privacyrisksadvisors.com/gdpr-infographic/

ώρες. Επίσης με βάση το άρθρο 37, η νομοθεσία απαιτεί από ορισμένες επιχειρήσεις να ορίσουν έναν Υπεύθυνο Προστασίας Δεδομένων (DataProtectionOfficer, DPO) για να επιβλέπει την στρατηγική που ακολουθείται για την ασφάλεια των δεδομένων και να ελέγχει την συμμόρφωση με τον GDPR.

Το άρθρο 17 δικαιοδοτεί τους πολίτες της ΕΕ με το δικαίωμα διαγραφής (δικαίωμα στη λήθη), το οποίο απαιτεί από τις επιχειρήσεις να διακόψουν την διαδικασία επεξεργασίας και να διαγράψουν προσωπικά δεδομένα όταν κριθεί αναγκαίο. Τα άρθρα 25 και 32 απαιτούν από τις επιχειρήσεις να εφαρμόσουν λογικά μέτρα προστασίας των δεδομένων για να προστατέψουν τους Ευρωπαίους πολίτες και την ιδιωτικότητά τους. Τέλος, σύμφωνα με το άρθρο 35 θα πρέπει οι επιχειρήσεις να πραγματοποιούν αξιολογήσεις για την εκτίμηση του αντίκτυπου σχετικά με την προστασία δεδομένων, για να προσδιοριστούν οι κίνδυνοι που διατρέχουν τα δεδομένα αυτά και να περιγραφούν μέτρα κατάλληλα για να διασφαλιστεί η αντιμετώπισή τους.

3.3.3 Αρχές που διέπουν την επεξεργασία δεδομένων

Η επεξεργασία των προσωπικών δεδομένων σύμφωνα με το άρθρο 5 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) πρέπει να υπακούει στις 7 εξής αρχές:

Νομιμότητα, Αντικειμενικότητα και Διαφάνεια: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.

Περιορισμός του σκοπού:Θα πρέπει να συλλέγονται δεδομένα για καθορισμένους, ρητούς και νόμιμους λόγους και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς.

Ελαχιστοποίηση των δεδομένων: Τα δεδομένα θα πρέπει να είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

Ακρίβεια: Τα προσωπικά δεδομένα θα πρέπει να είναι ακριβή και να επικαιροποιούνται όταν κρίνεται αναγκαίο. Θα πρέπει δηλαδή να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Περιορισμός της περιόδου αποθήκευσης: Η αποθήκευση δεδομένων προσωπικού χαρακτήρα θα πρέπει να γίνεται μόνο για το διάστημα που απαιτείται ώστε να γίνει η επεξεργασία τους και να μην το υπερβαίνει.

Ακεραιότητα και εμπιστευτικότητα: Η επεξεργασία θα πρέπει να γίνει με τέτοιον τρόπο ώστε να διασφαλίζεται η ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων (όπως η κρυπτογράφηση).

Λογοδοσία: Ο υπεύθυνος της επεξεργασίας φέρει την απόλυτη ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή της με την νομοθεσία.

3.3.4 Περιορισμοί του GDPR

Υπάρχουν δύο βασικές εξαιρέσεις με βάση τα άρθρα 2 και 30 όπου δεν εφαρμόζονται οι διατάξεις του Γενικού Κανονισμού Προστασίας δεδομένων. Η πρώτη έγκειται στο ότι το GDPR δεν αφορά καθαρά προσωπική και οικιακή δραστηριότητα αλλά εφαρμόζεται μόνο σε οργανισμούς που ασχολούνται με επαγγελματική και εμπορική δραστηριότητα. Ένα παράδειγμα για να καταστεί το παραπάνω κατανοητό είναι ότι σε περίπτωση που ένα άτομο συγκεντρώσει τις διευθύνσεις ηλεκτρονικού ταχυδρομείου για να οργανώσει μια κοινή τους έξοδο εκτός εργασίας, δεν απαιτείται να κρυπτογραφηθούν οι πληροφορίες επικοινωνίας τους για να συμμορφωθούν με τον κανονισμό του GDPR. Αντιθέτως αν ο σκοπός της συγκέντρωσης των διευθύνσεων ηλεκτρονικού ταχυδρομείου είναι για να οργανώσει μια

χρηματοδότηση για κάποιο έργο της επιχείρησης, τότε πρέπει να ακολουθηθούν οι διατάξεις της νομοθεσίας.

Η δεύτερη εξαίρεση αφορά τις επιχειρήσεις που απασχολούν λιγότερους από 250 υπαλλήλους. Οι μικρές και μεσαίες επιχειρήσεις δεν απαλλάσσονται εξ ολοκλήρου από τον GDPR, αλλά απαλλάσσονται από την υποχρέωση τήρησης αρχείων σε πολλές περιπτώσεις.

3.3.5 Κυρώσεις του GDPR

Η μη συμμόρφωση με τους κανονισμούς του GDPR οδηγεί στην επιβολή ποινών στις επιχειρήσεις. Σύμφωνα με το άρθρο 83 της νομοθεσίας, μερικές παραβιάσεις δημιουργούν διοικητικά πρόστιμα έως 10 εκατομμύρια € ή έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους(ανάλογα με το ποιο είναι υψηλότερο). Ενώ άλλες παραβιάσεις οδηγούν σε πιο κοστοβόρα πρόστιμα του ύψους των 20 εκατομμυρίων € ή του 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους (ανάλογα και πάλι με το ποιο είναι υψηλότερο)[95].

3.4 Παγκόσμιες επιπτώσεις του GDPR

Σήμερα τα δύο ισχυρότερα νομοθετικά πλαίσια που αφορούν την προστασία των προσωπικών δεδομένων είναι το Ευρωπαϊκό GDPRκαι το Σύστημα Κανόνων Διασυνοριακής Προστασίας (Cross Border Privacy Rules system, CBPR) της Οικονομικής συνεργασίας Ασίας και Ειρηνικού (Asia-Pacific Economic Cooperation, APEC). Αυτά τα δύο θεσμικά πλαίσια παρουσιάζουν αρκετές ομοιότητες αλλά και κάποιες σημαντικές διαφορές. Σύμφωνα με την βιβλιογραφία το μοντέλο της Ευρωπαϊκής Ένωσης θεωρείται καταλληλότερο για να ανταποκριθεί στην σύγχρονη πραγματικότητα του IoT (InternetofThings). Οι μηχανισμοί

[95]https://www.privacyrisksadvisors.com/gdpr-infographic/

συμμόρφωσης με το GDPR καθιστούν δυνατή την επεξεργασία προσωπικών δεδομένων ως τμήμα των εργασιών των επιχειρήσεων, ενώ παράλληλα παρέχουν υψηλό επίπεδο προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας. Έτσι, η ΕΕ είναι αυτή που θέτει ένα διεθνές νομοθετικό πρότυπο για την προστασία των δεδομένων και πολλές είναι οι χώρες εκτός των συνόρων της που εφαρμόζουν παρόμοια μέτρα[96].

Ακόμη και χώρες όπως η Αμερική που μέχρι πρότινος δεν διέθεταν καμία ομοσπονδιακή νομοθεσία περί ιδιωτικότητας δεδομένων, μετά τα πρόσφατα γεγονότα υποκλοπής δεδομένων που υπέστη η Facebook ενέκρινε τον Νόμο Ιδιωτικότητας Καταναλωτών της Καλιφόρνιας στις 28 Ιουνίου το 2018 που θα τεθεί σε λειτουργία από τις αρχές του 2020. Είναι εμφανές λοιπόν ότι αρχίζουν να αναθεωρούν την στρατηγική τους ως αποτέλεσμα της ύπαρξης της νομοθεσίας του GDPR.

Στον παρακάτω πίνακα παρουσιάζεται το ποσοστό κατά το οποίο χώρες ανά τον κόσμο θεωρούνται συμμορφωμένες με τους κανονισμούς του GDPR με βάση την έρευνα που πραγματοποίησε η Ciscogια το 2019. Το ποσοστό αυτό παρατηρούμε ότι κυμαίνεται από 42% μέχρι 76% με τις χώρες τις Ευρωπαϊκής Ένωσης όπως είναι αναμενόμενο να καταλαμβάνουν τις υψηλότερες θέσεις αυτής της κατάταξης.

Πίνακας 4: Ποσοστό συμμόρφωσης χωρών στις απαιτήσεις του GDPR.

Χώρες	Ποσοστό Συμμόρφωσης με το GDPR
Κίνα	42%
Ιαπωνία	45%
Ρωσία	46%
Τουρκία	47%
Αυστραλία	50%
Βραζιλία	53%
Σαουδική Αραβία	55%
ΗΠΑ	57%
Γερμανία	58%
Καναδάς	60%

[96] Sullivan, C. (2019), "*EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era*", Computer Law & Security Review, Vol. 35, pp. 380–397

Γαλλία	62%
Ινδία	65%
Αγγλία	69%
Αργεντινή	69%
Ιταλία	72%
Μεξικό	73%
Ισπανία	76%

Πηγή: Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

Είναι αδιαμφισβήτητο πως η συμμόρφωση των επιχειρήσεων με τους κανονισμούς του GDPR επιφέρει πολλά οφέλη, όπως η σωστή διαχείριση των δεδομένων, η βελτίωση της φήμης της μιας και γίνεται πιο αξιόπιστη διατηρώντας ασφαλή τα προσωπικά δεδομένα των πελατών της καθώς και η βελτίωση της λειτουργικής της απόδοσης της επιχείρησης και η πιθανή δημιουργία ανταγωνιστικού πλεονεκτήματος[97].Με βάση μια διαδικτυακή έρευνα το 33% των ερωτηθέντων επιχειρήσεων θεωρεί ότι το σημαντικότερο όφελος της εφαρμογής του GDPR ήταν η απόκτηση στρατηγικού πλεονεκτήματος[98].

Μια εκ των απαιτήσεων του νόμου είναι οι επιχειρήσεις να γνωρίζουν που βρίσκονται επακριβώς τοποθετημένες οι εύκολα αναγνωρίσιμες προσωπικές πληροφορίες των πελατών τους αλλά και να μπορούν να παρέχουν τα κατάλληλα μέτρα για την προστασία τους. Το γεγονός αυτό έχει οδηγήσει τις επιχειρήσεις να κατανοήσουν σε βάθος τα δεδομένα που διατηρούν και τους κινδύνους που διατρέχουν. Με βάση την προαναφερθείσα έρευνα τις Cisco παρατηρήθηκε ότι η συμμόρφωση των επιχειρήσεων με το νομοθετικό πλαίσιο τους βοήθησε και να μειώσουν την πιθανότητα να δεχθούν μια παραβίαση δεδομένων αλλά και σε περίπτωση που υποστούν να μειωθούν σημαντικά τα αρχεία που επηρεάζονται από αυτή[99].

Στη συνέχεια παρουσιάζονται δύο διαγράμματα που απεικονίζουν τα παραπάνω αποτελέσματα της έρευνας, με το 74% των συμμετεχόντων να απαντά ότι έχουν

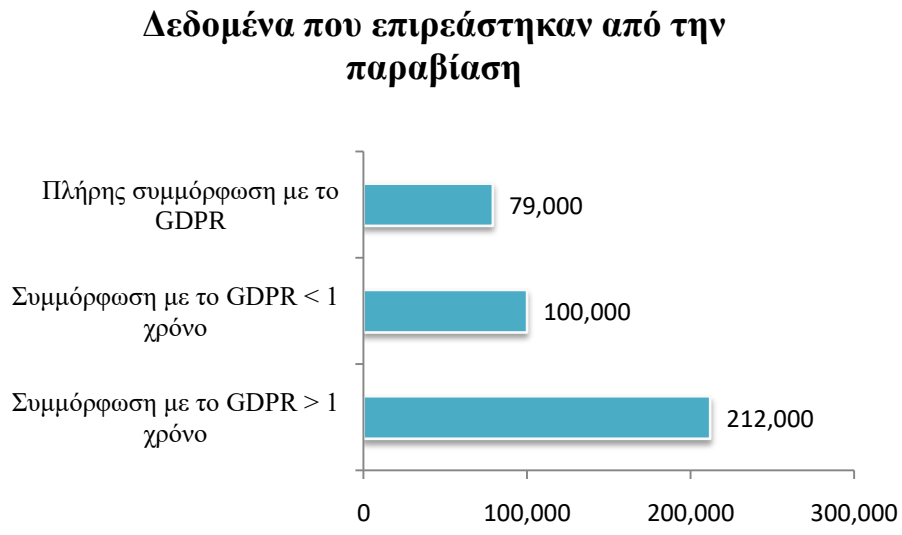
[97] Teixeira, G.A., Silva, M.M. & Pereira, R. (2019), "The critical success factors of GDPR implementation: a systematic literature review", DIGITAL POLICY, REGULATION AND GOVERNANCE,Vol. 21 No. 4, pp. 402-418

[98] Presthus, W., Sørum, H. & Andersen, L.R. (2018), “GDPR compliance in Norwegian companies”, Norwegian Conference for IT Use in Organisations (NOKOBIT), pp. 1-15

[99] Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

συμμορφωθεί πλήρως με τις απαιτήσεις του GDPR και με την μείωση των αρχείων που υπόκεινται σε παραβίαση να είναι εμφανής για αυτές τις εταιρίες που έχουν ήδη συμμορφωθεί με τον κανονισμό.

Διάγραμμα 7: Πιθανότητα να συμβεί περιστατικό παραβίασηςμε βάση τη συμμόρφωση στον GDPR[100].



Διάγραμμα 8:Δεδομένα που επηρεάστηκαν από την παραβίαση με βάση τη συμμόρφωση στον GDPR[101].

Ενδιαφέρον προκαλούν τα στοιχεία που παρουσιάζονται στο παρακάτω διάγραμμα που αφορά το επίπεδο ετοιμότητας των επιχειρήσεων σε σχέση με την συμμόρφωσή τους

[100] Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

[101] Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

στον GDPR ανάλογα με το είδος της επιχείρησης. Η έρευνα αυτή διενεργήθηκε από την PWC για το έτος 2018[102]. Αξίζει να τονίσουμε ότι οι επιχειρήσεις που παρέχουν χρηματοοικονομικές υπηρεσίες σημειώνουν το μεγαλύτερο ποσοστό συμμόρφωσης με το νομοθετικό πλαίσιο, γεγονός που δεν εγείρει ερωτήματα και είναι αναμενόμενο μιας και όπως έχουμε ήδη αναφέρει, αυτός ο κλάδος επιχειρήσεων είναι στην κορυφή των επιχειρήσεων που δέχονται τις περισσότερες κυβερνοεπιθέσεις.

Διάγραμμα 9: Επίπεδο ετοιμότητας ως προς τη συμμόρφωση με τον GDPR ανά είδος επιχείρησης[103].

Σύμφωνα με την βιβλιογραφία η συμμόρφωση των επιχειρήσεων με τον GDPR περιλαμβάνει και κάποιες προκλήσεις που καθυστερούν ή αναχαιτίζουν την εφαρμογή του. Επιγραμματικά μερικά από τα εμπόδια που καλούνται να αντιμετωπίσουν οι επιχειρήσεις είναι η εκτεταμένη και πολύπλοκη δομή του κανονισμού και η υποκειμενικότητα, μιας και δεν παρέχει συγκεκριμένες κατευθυντήριες γραμμές, γεγονός που οδηγεί την κάθε

[102] General Data Protection Regulation, Luxembourg market status: Smooth Sailing or Hot Water? December 2018, PWC

[103] General Data Protection Regulation, Luxembourg market status: Smooth Sailing or Hot Water? December 2018, PWC

επιχείρηση να προσπαθεί να ανιχνεύσει από μόνη της τις κατάλληλες πρακτικές για την συμμόρφωση στις απαιτήσεις του νόμου. Επίσης η εφαρμογή του νόμου είναι αρκετά δαπανηρή και χρονοβόρα καθώς απαιτεί σημαντικούς οικονομικούς και ανθρώπινους πόρους[104].Βάση μιαςδιαδικτυακής έρευνας, το 23% των ερωτηθέντων θεώρησε ότι η μεγαλύτερη πρόκληση στην εφαρμογή του νόμου ήταν η έλλειψη χρημάτων και το 18% η έλλειψη της απαραίτητης τεχνολογίας. Το μεγαλύτερο ποσοστό 46%, σημειώνει η αδυναμία κατανόησης των απαιτήσεων του GDPR και ένα ποσοστό 44% κατονόμασε άλλες δυσκολίες[105].

Μήνες μετά την καταληκτική ημερομηνία εφαρμογής του κανονισμού στις 28 Μαΐου το 2018, πολλές εταιρίες βρέθηκαν να μην έχουν συμμορφωθεί ακόμη με τις απαιτήσεις του ή να τις παραβιάζουν, με απώτερη συνέπεια την επιβολή προστίμων. Το μεγαλύτερο πρόστιμο που έχει δοθεί από τις γαλλικές αρχές ήταν του ύψους των 50 εκατομμυρίων € στο διαδικτυακό κολοσσό της Google. Ο λόγος της επιβολής του προστίμου ήταν η έλλειψη διαφάνειας ως προς την πληροφόρηση των χρηστών για τα δεδομένα προσωπικού χαρακτήρα αλλά και την αθέτηση των όσων ορίζονται στη λήψη της συγκατάθεσης των χρηστών[106].

[104] Teixeira, G.A., Silva, M.M. & Pereira, R. (2019), "The critical success factors of GDPR implementation: a systematic literature review", DIGITAL POLICY, REGULATION AND GOVERNANCE,Vol. 21 No. 4, pp. 402-418

[105] Presthus, W., Sørum, H. & Andersen, L.R. (2018), "GDPR compliance in Norwegian companies", Norwegian Conference for IT Use in Organisations (NOKOBIT), pp. 1-15

[106] https://www.insurancedaily.gr/galliko-prostimo-50-ekat-evro-stin-google-logo-gdpr/

ΚΕΦΑΛΑΙΟ 4

ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΚΑΙ ΝΑΥΤΙΛΙΑ

4.1 Η Ναυτιλία Σήμερα

Πάνω από το 90% του παγκόσμιου εμπορίου εξυπηρετείται από την ναυτιλιακή βιομηχανία, με περίπου 60,000 εμπορικά πλοία να μεταφέρουν επί καθημερινής βάσης κάθε λογής φορτία. Το παγκόσμιο θαλάσσιο εμπόριο βρέθηκε το 2017 στα καλύτερά του σημειώνοντας έναν ρυθμό αύξησης 4%, η ταχύτερη αύξηση που καταγράφηκε την τελευταία πενταετία. Λόγω της παγκόσμιας οικονομικής ανάπτυξης και το βελτιωμένο παγκόσμιο εμπόριο αγαθών, το διεθνές ναυτιλιακό εμπόριο υπολογίστηκε στους 10.7 δισεκατομμύρια τόνους, με τα ξηρά εμπορεύματα να καταλαμβάνουν σχεδόν το ήμισυ αυτού του όγκου[107].

4.2 Η Ναυτιλία ως Στόχος Κυβερνοεπιθέσεων

Η ναυτιλία υπάγεται στον κλάδο των μεταφορών, που με τη σειρά του ανήκει στις κρίσιμες υποδομές μιας χώρας και όπως έχουμε ήδη αναφέρει σύμφωνα με έρευνα της IBM, οι επιχειρήσεις που ανήκουν σ' αυτόν τον κλάδο αποτελούν τους δεύτερουςσυχνότερους στόχους κυβερνοεπιθέσεων μετά τις επιχειρήσεις του χρηματοοικονομικού κλάδου, σημειώνοντας ένα ποσοστό 13%[108]. Ο λόγος που η βιομηχανία των μεταφορών είναι ένας στόχος που προσελκύει τις κακόβουλες επιθέσεις είναι το γεγονός ότι σαν βιομηχανία εξαρτάται κατά έναν πολύ μεγάλο βαθμό στην τεχνολογία των πληροφοριώνπροκειμένου να

[107] REVIEW OF MARITIME TRANSPORT 2018, UNCTAD

[108] X-Force Threat Intelligence Index 2019, IBM Security Research

βελτιστοποιήσει τις λειτουργίεςτης, να αυξήσει την παραγωγικότητα της,να παραμείνει ανταγωνιστική, να μειώσει το κόστος και να βελτιώσει τη διαχείριση των φορτίων.

Έτσι λοιπόν και η ναυτιλία βασίζεται σε πληθώρα τεχνολογικών συστημάτων, όπως εξειδικευμένα συστήματα επικοινωνίας που χρησιμοποιούνται στην πλοήγηση, συστήματα ανταλλαγής πληροφοριών από πλοίο σε πλοίο αλλά και μεταξύ ενός πλοίου και της στεριάς, συστήματα διαχείρισης και προγραμματισμού των φορτίων καθώς και συστήματα ψυχαγωγίας και ασφάλειας των επιβατών.Τα περισσότερα απ' αυτά τα τεχνολογικά συστήματα όμως δημιουργήθηκαν χωρίς να έχουν ως γνώμονά τους την ολοένα και πιο συχνή εμφάνιση περιστατικών κυβερνοεπίθεσης[109].Επιθέσεις που επιφέρουν σημαντικές συνέπειες, όπως απώλεια ανθρώπινων ζωών, τραυματισμούς, ρύπανση των θαλασσών, αναχαίτιση των λειτουργιών της επιχείρησης καθώς και πολλές φορές ανεπανόρθωτη ζημία στην εταιρική φήμη.

Δεν χωράει αμφιβολία ότι η αυξανόμενη χρήση της τεχνολογίας στην ναυτιλία αναμένεται να είναι ευεργετική τόσο για την ανάπτυξή όσο και για την ασφάλειά της. Τα παραπάνω συστήματα που αναφέραμε αποδεικνύονται αναγκαία και σωτήρια βοηθώντας για παράδειγμα στην αποφυγή προσθαλασσώσεων και συγκρούσεων. "Ωστόσο, η τεχνολογία σημαίνει επίσης ότι οι κίνδυνοι κυβερνοχώρουαποτελούν έναν μεγάλο προβληματισμό για τη ναυτιλία", αναφέρει ο Captain RahulKhanna, Επικεφαλής της Παγκόσμιας Συμβουλευτικής για τον Κινδύνου Ναυτιλίας στο AGCS. "Δεδομένου ότι όλο και περισσότερα συστήματα απαιτούν συνδεσιμότητα με την ακτή, έτσι και τα σκάφη γίνονται ολοένα και πιο ευάλωτα σε επιθέσεις στον κυβερνοχώρο".

Οι GlobalMaritimeForum, MarshκαιIUMIμε βάση την μελέτη που πραγματοποίησαν, κατατάσσουν τις κυβερνοεπιθέσεις και την υποκλοπή δεδομένων ως το πιο πιθανό ζήτημα που θα κληθούν να αντιμετωπίσουν για τα επόμενα 10 έτη, με τις διακυμάνσεις των τιμών της ενέργειας και την μεταβολή των εμπορικών προτύπων να ακολουθούν. Επίσης η ίδια έρευνα τοποθετεί τις κυβερνοεπιθέσεις ως το τρίτο κατά σειρά ζήτημα που σε περίπτωση που συμβεί θα προκαλέσει τις μεγαλύτερες συνέπειες στο θαλάσσιο εμπόριο για την επόμενη

[109] Kessler, G.C. & Craiger, J.P. (2018), "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System", The International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 12, No. 3, pp. 429-437

δεκαετία, με την παγκόσμια οικονομική κρίση και την διακύμανση των τιμών της ενέργειας να προηγούνται[110].

Ενδιαφέρον προκαλούν τα συμπεράσματα μιας έρευνας που διεξήγαγε η JonesWalkerLLP για τον κλάδο της ναυτιλίας στην Αμερική, όπου αναφέρεται ότι ένα ποσοστό μεγαλύτερο των δύο τρίτων των ερωτηθέντων, συγκεκριμένα το 69%, θεωρεί ότι η βιομηχανία της ναυτιλίας είναι μερικώς ή καλά προετοιμασμένη να αντιμετωπίσει περιστατικά κυβερνοεπιθέσεων, εκ των οποίων μόνο το 36% βρέθηκε να θεωρεί ότι είναι σε ετοιμότητα να αντιμετωπίσει ένα τέτοιο περιστατικό όσον αφορά τις δικές τους επιχειρήσεις[111]. Στον παρακάτω πίνακα, με βάση την προαναφερθείσα έρευνα, παρουσιάζονται οι κύριες πηγές των πιο καταστροφικών περιστατικών παραβίασης που βίωσαν μικρές, μεσαίες και μεγάλες ναυτιλιακές επιχειρήσεις, με τις κακόβουλες εξωτερικές επιθέσεις να λαμβάνουν το μεγαλύτερο ποσοστό.

Πίνακας 5: Πηγές των πιο καταστροφικών περιστατικών παραβίασης ανάλογα με το μέγεθος της επιχείρησης.

	ΜικρέςΕπιχειρήσεις	Μεσαίες Επιχειρήσεις	Μεγάλες Επιχειρήσεις
Κακόβουλες εξωτερικές επιθέσεις	17%	45%	97%
Αποτυχία συστημάτων	3%	0%	0%
Εσωτερική υποκλοπή/ παραβίαση	11%	16%	0%
Ανθρώπινο λάθος	11%	3%	0%
Αβέβαιη πηγή	36%	19%	3%
Καμία απάντηση	22%	17%	0%

Πηγή: Jones Walker LLP 2018, Maritime Cybersecurity Survey

[110] Global Maritime Issues Monitor 2018, by Global Maritime Forum, Marsh and IUMI

[111] Jones Walker LLP 2018, Maritime Cybersecurity Survey

4.3 Ασφάλεια Κυβερνοχώρου στην Ναυτιλία

Μέχρι πρότινος δεν υπήρξε κάποια νομοθεσία που να αφορά αποκλειστικά την κυβερνοασφάλεια στον κλάδο της ναυτιλίαςκαι να είναι υποχρεωτική η τήρησή της. Το 2017 ο Διεθνής Ναυτιλιακός Οργανισμός (International Maritime Organization , IMO) της Επιτροπής Θαλάσσιας Ασφάλειας (Marine Safety Commission , MSC) πρότεινε ένα σχέδιο για τη διαχείριση των κινδύνων θαλάσσιου κυβερνοχώρου λόγοτηςαυξημένης απειλής των κυβερνοεπιθέσεων με στόχο την βιομηχανία της ναυτιλίας, το οποίο θα τεθεί σε ισχύ αρχής γενομένης από το 2021.

Ο IMO είναι ένας διεθνής οργανισμός που δημιουργήθηκε με σκοπό την αντιμετώπιση των διεθνώς ζητημάτων που σχετίζονται με την ναυτιλιακή και την ναυπηγική βιομηχανία. Η κατευθυντήρια γραμμή του οργανισμού αυτού για την αντιμετώπιση των κινδύνων της ασφάλειας του κυβερνοχώρου παρουσιάζει τη διαχείριση της ναυτιλίας και των φορτίων, τη διαχείριση των επιβατών και τα συστήματα των κινητήρων και των επικοινωνιών ως τα πιο ευάλωτα συστήματα του πλοίου. Το σχέδιο του IMO υιοθετεί ένα αποτελεσματικό πλαίσιο διαχείρισης κινδύνων τουNIST (National Institute of Standards and Technology) για την κυβερνοασφάλεια με την λειτουργία των πέντε βημάτων:αναγνώριση – προστασία – ανίχνευση – ανταπόκριση – ανάκτηση[112].

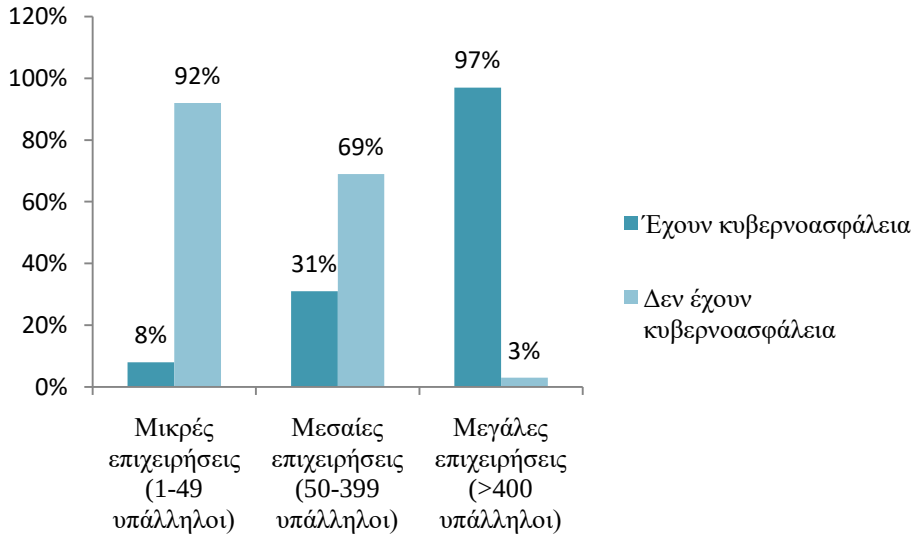
Η εφαρμογή του GDPR ένα χρόνο αργότερα τον Μάιο του2018, έχει σημαντικό αντίκτυπο και στις ναυτιλιακές επιχειρήσεισμιας και διατηρούν πολλά προσωπικά δεδομένα –όπως ηλεκτρονικές διευθύνσεις, πληροφορίες του πληρώματος ή των επιβατών των πλοίων καθώς και των δικό της υπαλλήλων-, δεδομένα που αρκετές φορές χρειάζεται να μεταφερθούν σε παγκόσμιο επίπεδο. Όπως και στα υπόλοιπα είδη επιχειρήσεων, το GDPR υποχρεώνειτις ναυτιλιακές επιχειρήσεις να πραγματοποιούν εκτιμήσεις των επιπτώσεων στην προσωπική ιδιωτικότητα ανά πάσα στιγμή όταν υπάρχει αυξημένος κίνδυνος παραβίασης, καθώς και να αναφέρουν μέσα σε 72 ώρες οποιοδήποτε περιστατικό παραβίασης ώστε να μπορούν να αντιδράσουν έγκαιρα και αποτελεσματικά σε μια δυνητική κυβερνοεπίθεση[113].

[112] Jo, Y., Kang, J. & Cha, Y. (2018), "*Cyber Piracy Threat Analysis*", Cryptology and Information Security Series, October 2018

[113] Mraković, I. & Vojinović. R. (2019), "*Maritime Cyber Security Analysis – How to Reduce Threats?*", TRANSACTIONS ON MARITIME SCIENCE, Vol. 13, pp. 132-139

Τον ίδιο μήνα μια λιγότερο γνωστή οδηγία της Ευρωπαϊκής Ένωσης έκανε την εμφάνισή της με εξίσου σημαντικές συνέπειες στον ναυτιλιακό κλάδο. Η Ευρωπαϊκή Οδηγία Ασφάλειας Δικτύων και Πληροφοριών (Network and Information Security Directive, NIS) απαιτεί από τους "μεγάλους παρόχους υπηρεσιών", όπως τα μεγάλα λιμάνια και οι θαλάσσιες υπηρεσίες μεταφορών στην ΕΕ, να αποδείξουν ότι έχουν λάβει τα επαρκή και απαραίτητα μέτρα για να διαχειριστούν τους κινδύνους του κυβερνοχώρου[114].

Στο παρακάτω διάγραμμα παρουσιάζεται το ποσοστό των επιχειρήσεων -ανάλογα με το μέγεθός τους-, που διαθέτει εργαλεία και προγράμματα κυβερνοασφάλειας, σύμφωνα με την μελέτη της JonesWalkerLLP και παρατηρούμε ότι η πλειοψηφία των μικρών και μεσαίων ναυτιλιακών επιχειρήσεων δεν διαθέτουν κυβερνοασφάλεια και είναι εκτεθειμένες στους κινδύνους του κυβερνοχώρου που εγκυμονούν[115].



Διάγραμμα 10: Ποσοστό επιχειρήσεων βάση του μεγέθους τους που διαθέτουν ή όχι κυβερνοασφάλεια[116].

[114] SAFETY AND SHIPPING REVIEW 2018: An annual review of trends and developments in shipping losses and safety, Allianz

[115] Jones Walker LLP 2018, Maritime Cybersecurity Survey

[116] Jones Walker LLP 2018, Maritime Cybersecurity Survey

Το μεγαλύτερο πρόβλημα όμως πέρα και από την μέχρι πρότινος έλλειψη της κατάλληλης νομοθεσίας, είναι ο ανθρώπινος παράγοντας. Γενικά υπάρχει μια δυσκολία στην βαθύτατη κατανόηση από πλευράς ατόμων μέσα στην ναυτιλιακή βιομηχανία στο τι είναι ακριβώς οι κυβερνοεπιθέσεις και τι συνέπειες έχουν[117].Συχνά, το γεγονός ότι μερικά άτομα του πληρώματος έχουν ελάχιστες ή και καθόλου γνώσεις περί αυτού του θέματος, ο λανθασμένος χειρισμός κάποιων διεργασιών έχει ως αποτέλεσμα τα συστήματα να είναι εκτεθειμένα και ευάλωτα σε τυχόν επιθέσεις. Έτσι, η ευαισθητοποίηση του προσωπικού παίζει καθοριστικό ρόλο στην ομαλή λειτουργία της επιχείρησης.

Σύμφωνα με την έρευνα της JonesWalkerLLP, από τις συμμετέχοντες επιχειρήσεις, όλες οι μεγάλες ναυτιλιακές επιχειρήσεις πραγματοποιούν προγράμματα εκπαίδευσης για το ζήτημα των κυβερνοεπιθέσεων στους εργαζομένους που έχουν πρόσβαση στα συστήματά τους, αντιδιαμετρικά όσον αφορά τις μικρές επιχειρήσεις μόνο το 11% εξ αυτών θέτει σε εφαρμογή τέτοιου είδους προγράμματα, γεγονός που εξηγεί γιατί αυτές οι επιχειρήσεις βρίσκονται σε μεγαλύτερο κίνδυνο[118].

[117] Silgado, D.M. (2018), "*Cyber-attacks: a digital threat reality affecting the maritime industry*", World Maritime University Dissertations, 663

[118] Jones Walker LLP 2018, Maritime Cybersecurity Survey

ΚΕΦΑΛΑΙΟ 5

ΜΕΛΕΤΗΠΕΡΙΠΤΩΣΕΩΝ

Στο κεφάλαιο που ακολουθεί θα παρουσιαστούν τρία περιστατικά κυβερνοεπιθέσεων που έχουν υποστεί ναυτιλιακές επιχειρήσεις και αποτέλεσαν ορόσημα στην ιστορία των κυβερνοεπιθέσεων.

5.1 Περίπτωση της A.P.Moller -Maersk

5.1.1 Ηεπιχείρηση

Η*A.P. Møller–MærskA/S*,γνωστή και ως *Maersk*, είναι ένας Δανέζικος όμιλος επιχειρήσεων με τις δραστηριότητές του να περιλαμβάνουν τους τομείς της μεταφοράς, της εφοδιαστικής αλυσίδας και της ενέργειας. Έχοντας προϊστορία πάνω από έναν αιώνα, συγκεκριμένα η ίδρυση της πρώτης εταιρίας έγινε το 1904, η οικογένεια Møllerκατάφερε να δημιουργήσει ένα ισχυρό όνομα στον κλάδο της ναυτιλίας και να βρίσκεται στην πρώτη θέση ως ο μεγαλύτερος διαχειριστής πλοίων και εμπορευμάτων σ' ολόκληρο τον κόσμο από το 1996[119] μεταφέροντας σχεδόν το 15% των φορτίων του παγκόσμιου εμπορίου. Η βάση της επιχείρησης βρίσκεται στην Κοπεγχάγη της Δανίας, έχοντας πάνω από 900 θυγατρικές εταιρίες και γραφεία σε 130 χώρες ανά την υφήλιο και πάνω από 75,000 εργαζομένους.

Από χρηματοοικονομικής απόψεως αξίζει να σημειωθεί πως για το φορολογικό έτος 2018, η Maerskείχε πραγματοποιήσει ετήσια έσοδα 39,019,000US$, ποσό μεγαλύτερο κατά

[119] https://en.wikipedia.org/wiki/Maersk#Piracy

26% σε σχέση με το περασμένο φορολογικό έτος [120]. Η μετοχή της διαπραγματεύεται στο χρηματιστήριο της NasdaqCopenhagen υπό τα ονόματα MAERSKA καιMAERSKB.

5.1.2 Η κυβερνοεπίθεση

Στις 27 Ιουνίου το 2017, η Maersk έπεσε θύμα μιας σοβαρής κυβερνοεπίθεσης που προκλήθηκε από το κακόβουλο λογισμικό NotPetya, μια επίθεση ransomware που εμποδίζει τους ανθρώπους να έχουν πρόσβαση στα δεδομένα τους εκτός αν πληρώσουν 300 δολάρια σε bitcoin[121]. Η πρώτη ανακοίνωση της επίθεσης ήρθε μια ημέρα μετά στην επίσημη ιστοσελίδα της εταιρίας[122]. ToNotPetyaείναιένα λογισμικό που στοχεύει συστήματα που χρησιμοποιούν τα Microsoft Windows και έχει επηρεάσει πολλές επιχειρήσεις σε παγκόσμιο επίπεδο προκαλώντας συνολικές ζημίες 10 δισεκατομμυρίων US$.

Όλα ξεκίνησαν όταν ένας υπάλληλος της εταιρίας στην Ουκρανία απάντησε σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο και περιείχε το κακόβουλο λογισμικό, επηρεάζοντας όλο το σύστημα της Maersk. Η επίθεση του NotPetya είχε ως στόχο τα συστήματα των τερματικών σταθμών στα λιμάνια, προσβάλλοντας το λογισμικό που διαχειρίζεται τα ηλεκτρονικά αρχεία τα οποία στέλνανε τα καράβια με πληροφορίες σχετικές τα φορτία που κουβαλούσαν. Έτσι όλα τα πλοία της εταιρίας έμειναν καθηλωμένα αλλά ασφαλήστην θάλασσα και κανένας από τους 76 λιμενικούς τερματικούς σταθμούς που διαχειρίζεται η Maerskδεν παρελάμβανε ή παρέδιδε φορτία, με τους 17 εκ των οποίων, από το Λος Άντζελες των ΗΠΑ μέχρι το Αλγκεθίρας της Ισπανίας, στο Ρότερνταμ στις Κάτω Χώρες και στη Βομβάη στην Ινδία, να διακόπτουν εξ ολοκλήρου τις λειτουργίες τους μέχρι την αποκατάσταση του προβλήματος[123].Η εταιρία δεν μπορούσε πλέον να πραγματοποιήσει νέες κρατήσεις, αποκόπτοντας έτσι την βασική πηγή εσόδωντης.

[120] 2018 Annual Report by A.P. Møller – Mærsk A/S

[121] https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

[122] http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

[123] Silgado, D.M. (2018), "*Cyber-attacks: a digital threat reality affecting the maritime industry*", World Maritime University Dissertations, 663

Αν και το περιστατικό της κυβερνοεπίθεσης ήταν αρκετά σοβαρό, η εταιρία της Maersk κινήθηκε με γρήγορους ρυθμούς για την αντιμετώπιση των συνεπειών της. Η ομάδα της πληροφορικής που συστάθηκε εντόπισε, αναγνώρισε και αφαίρεσε το κακόβουλο λογισμικό από τα μολυσμένα συστήματα ώστε να μπορέσει να επαναφέρει την ομαλή τους λειτουργία. Την ίδια στιγμή τα Μέσα Μαζικής Ενημέρωσης χειρίστηκαν άψογα το θέμα ενημερώνοντας συνεχώς τους ενδιαφερόμενους για την κατάσταση της εταιρίας. Μέσα σε ένα διάστημα 10 ημερών από την ημέρα της επίθεσης η Maersk κατάφερε να πάρει στα χέρια της τον πλήρη έλεγχο των συστημάτων και να χτίσει από την αρχή ολόκληρο το δίκτυο 4,000 διακομιστών και 45,000 υπολογιστών. Πέντε μήνες μετά την αντιμετώπιση της επίθεσης, στην συνάντηση του World Economic Forum ο πρόεδρος της Maersk, Jim Hagemann Snabe ανακοίνωσε την τρομερή προσπάθεια που κατέβαλαν για την διάσωση της εταιρίας[124].

Όσον αφορά τους λόγους για τους οποίους αυτή η εταιρία έπεσα θύμα της επίθεσης, οι υπάλληλοι ασφαλείας της Maersk ανέφεραν ότι ορισμένοι από τους διακομιστές έτρεχαν τα Windows 2000 την περίοδο της επίθεσης, ένα λειτουργικό σύστημα τόσο απαρχαιωμένο που και η ίδια η Windows δεν υποστήριζε πια. Το 2016, μια ομάδα ατόμων από τον τομέα της πληροφορικής θεώρησε ότι ήταν επιτακτική ανάγκη ο επανασχεδιασμός της ασφάλειας του συνολικού παγκόσμιου δικτύου της εταιρίας, λόγω της ατελής εφαρμογής του λογισμικού που χρησιμοποιούνταν, των ξεπερασμένων λειτουργικών συστημάτων και του ανεπαρκούς καταμερισμού του δικτύου. Η τελευταία αυτή ευπάθεια, είχαν προειδοποιήσει ότι θα μπορούσε να επιτρέψει σε ένα κακόβουλο λογισμικό να εισέλθει σε ένα τμήμα του δικτύου και έπειτα να εξαπλωθεί άτακτα σε όλο το σύστημα. Κάτι που όντως συνέβη ένα χρόνο μετά[125].

5.1.3 Τα αποτελέσματα

Όσον αφορά τον αντίκτυπο που είχε η επίθεση αυτή, αν και η ανάκαμψη από την επίθεση ήταν αρκετά γρήγορη, η Maerskυπέστη οικονομικές απώλειες του ύψους των 250 με 300

[124] https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

[125] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

εκατομμυρίων US$ καλύπτοντας, μεταξύ άλλων, την απώλεια εσόδων που αναφέραμε, το κόστος αποκατάστασης του τμήματος πληροφορικής και όλα τα έκτακτα έξοδα που σχετίζονταν με τις λειτουργίες της εταιρίας[126].

Στην παρακάτω εικόνα παρουσιάζεται η πορεία της τιμής της μετοχής της Maersk για ένα διάστημα 6 μηνών. Την ημέρα της επίθεσης 27 Ιουνίου 2017 η τιμή της μετοχής ήταν στις 11,185.10 US$. Παρατηρούμε ότι στον απόηχο της επίθεσης, αν και όχι αμέσως μετά την ανακοίνωσή της, η τιμή της μετοχής έχει μια ευδιάκριτη καθοδική πορεία συγκεκριμένα από τις 17 Ιουλίου και μετά. Στα τέλη Νοεμβρίου, πέντε μήνες αργότερα όταν όπως αναφέραμε ο πρόεδρος της Maersk μίλησε δημόσια για το περιστατικό και τις προσπάθειες που κατέβαλαν, η μετοχή σημειώνει τις χαμηλότερες τιμές της για το έτος 2017.

Εικόνα 3: Πορεία μετοχής της A.P. Møller - Mærsk A/S την περίοδο της κυβερνοεπίθεσης[127].

Μετά την επίθεση που δέχτηκε, η A.P. Møller – MærskA/S αναθεώρησε την μέχρι πρότινος στάση της απέναντι στις κυβερνοεπιθέσεις και την προστασία της από αυτές. Η ίδια στην αναφορά της για το έτος 2017 αναφέρει ότι έχει ήδη υλοποιήσει αλλά και σχεδιάσει πολλές άμεσες και πιο μακροπρόθεσμες ενέργειες για να διασφαλίσει την σωστή λειτουργία της επιχείρησης στον νέο ψηφιακό κόσμο, να βελτιώσει την πλατφόρμας του τμήματος της πληροφορικής, να ενισχύσει τις υπηρεσίες του τμήματος πληροφορικής ώστε να μπορούν να

[126] 2017 Annual Report by A.P. Møller – Mærsk A/S

[127] Yahoo Finance

συνεχίσουν τις λειτουργίες τους και να ανακάμπτουν σε περίπτωση επίθεσης, καθώς και να ενδυναμώσουν τα σχέδια της επιχειρήσεις για την συνέχιση της ομαλής λειτουργίας της. Επίσης, έχουν προβεί στην αγορά ασφάλειας για τον κυβερνοχώρο ώστε να μεταβιβαστούν κάποιες δυνητικές οικονομικές επιπτώσεις των κυβερνοεπιθέσεων που μπορεί να υποστεί στο μέλλον. Αξίζει να σημειωθεί ότι μετά την επίθεση που δέχτηκε κατατάσσει τις κυβερνοεπιθέσεις ανάμεσα στους τρείς πιο πιθανούς κινδύνους με τις μεγαλύτερες συνέπειες που έχει να αντιμετωπίσει[128].

Ενάμιση χρόνο μετά την επίθεση, ο εκπρόσωπος της εταιρίας Mikkel Elbek Linnet αναφέρει ότι "Με αυτή τη σύγχρονη υποδομή, στην πραγματικότητα προχωράμε προς την ασφάλεια στον κυβερνοχώρο ως ανταγωνιστικό πλεονέκτημα ", συνεχίζει λέγοντας πως "Παρόλο που δεν μοιραζόμαστε συγκεκριμένες λεπτομέρειες σχετικά με τα συστήματα άμυνας στον κυβερνοχώρο, τη διαμόρφωση κ.λπ., μπορούμε να επιβεβαιώσουμε ότι μέσω των προσπαθειών ανοικοδόμησης που έχουμε αναλάβει για να ανακάμψουμε από την κυβερνοεπίθεση του 2017, επιτύχαμε σημαντική βελτίωση των επιπέδων ασφαλείας και της ευρωστίας έναντι σε παρόμοιες επιθέσεις"[129].

5.2 Περίπτωση της ClarksonPLC

5.2.1 Η επιχείρηση

Η *ClarksonPLC*, που συχνά αναφέρεται απλά και ως *Clarksons*, αποτελεί τον κορυφαίο πάροχο ολοκληρωμένων ναυτιλιακών υπηρεσιώνμε έδρα το Λονδίνο της Αγγλίας. Οι λειτουργίες της εταιρίας χωρίζονται σε τέσσερες διακριτούς τομείς: τον επενδυτικό, τον χρηματοοικονομικό, της υποστήριξης και της έρευνας. Η εταιρία μεσιτεύει πλοία για μερικούς από τους μεγαλύτερους παραγωγούς και εμπόρους φυσικών πόρων σε παγκόσμιο

[128] 2017 Annual Report by A.P. Møller – Mærsk A/S

[129] https://www.tradewindsnews.com/safety/ap-moller-maersk-more-than-a-year-on-from-notpetya-cyber-attack/2-1-426819

επίπεδο. Η δραστηριότητα αυτή επιφέρει περισσότερο από το 75% των εσόδων της Clarksons. Ο τομέα της έρευνας επικεντρώνεται κυρίως στην περισυλλογή, επικύρωση, ανάλυση και διαχείριση δεδομένων σχετικά με την εμπορική ναυτιλία και τις υπεράκτιες αγορές[130].

Με την ιστορία της να ξεκινάει το μακρινό 1852, είναι πλέον ένας όμιλος που απασχολεί πάνω από 1,580 άτομα σε 23 διαφορετικές χώρες. Τα έσοδά της για το έτος 2018 με βάση την ετήσια αναφορά, ανήλθαν στο ποσό των 337,600,000 £[131]. Η Clarksons είναι εισηγμένη στην κύρια αγορά του Χρηματιστηρίου του Λονδίνου υπό το όνομα CKN και είναι μέλος του δείκτη FTSE 250.

5.2.2 Η κυβερνοεπίθεση

Στις 7 Νοεμβρίου το 2017 η Clarksons μαθαίνει ότι έχει πέσει θύμα ενός περιστατικού κυβερνοεπίθεσης μέσω μη εξουσιοδοτημένης πρόσβασης ενός τρίτου μέλους στο σύστημα ενός συγκεκριμένου υπολογιστή της εταιρίας στην Αγγλία, αντιγράφοντας δεδομένα και ζητώντας λύτρα για την ασφαλή επιστροφή τους. Η ανακοίνωση έρχεται αρκετές ημέρες μετά στις 29 Νοεμβρίου με ανάρτηση που πραγματοποίησαν οι ίδιοι στην ιστοσελίδα τους. Με την ανακάλυψη του γεγονότος αυτού η εταιρία ξεκίνησε να διεξάγει έρευνα για να προσδιορίσει την φύση και την έκταση της επίθεσης. Ειδοποιήθηκαν οι αρμόδιες αρχές και εξωτερικοί δικαστικοί ερευνητές για να αντιμετωπιστεί η επίθεση που δέχθηκαν, χωρίς να διακοπεί στο ελάχιστο η λειτουργία της επιχείρησης. Μετά από τις έρευνες αυτές διαπιστώθηκε πως η μη εξουσιοδοτημένη πρόσβαση στο σύστημα αποκτήθηκε από τις 31 Μαΐου το 2017 και συνέχιζε να γίνεται μέχρι και τις 4 Νοεμβρίου το 2017. Η Clarksons έμαθε ότι η πρόσβαση αυτή είχε αποκτηθεί μέσω ενός και μόνο απομονωμένου λογαριασμό χρήστη, ο οποίος και αμέσως μετά απενεργοποιήθηκε[132].

[130] https://en.wikipedia.org/wiki/Clarkson_plc

[131] Annual Results 2018 by Clarkson

[132] UPDATE ON 2017 DATA BREACH – REGULATORY NOTICE by Clarkson

Τα δεδομένα που κλάπηκανμπορεί να εμπεριείχαν ημερομηνίες γεννήσεως, πληροφορίες επικοινωνίας, υπογραφές, φορολογικές και ασφαλιστικές πληροφορίες, ιατρικές, εθνικές και θρησκευτικές πληροφορίες καθώς και πολλά άλλα ευαίσθητα προσωπικά δεδομένα. Αν και η εταιρία κατάφερε να εντοπίσει και ανακτήσει το αντίγραφο αυτών των πληροφοριών, για προληπτικούς λόγους συνέχισαν να συνεργάζονται με τις αρχές ώστε να διασαφηνίσουν ποια από αυτά τα δεδομένα εκλάπη και αρχίζουν με μεγάλη προσοχή να ειδοποιούν τα άτομα που πιθανώς είχαν πληγεί από αυτή την κυβερνοεπίθεση και ζήτησαν δημόσια συγνώμη για το γεγονός αυτό[133]. Η Clarksons δεν επέτρεψε το περιστατικό της κυβερνοεπίθεσης να αναχαιτίσει την ομαλή λειτουργία της επιχείρησης και το ζήτημα περιορίστηκε και επιλύθηκε στις αρχές Δεκεμβρίου[134].

5.2.3 Τα αποτελέσματα

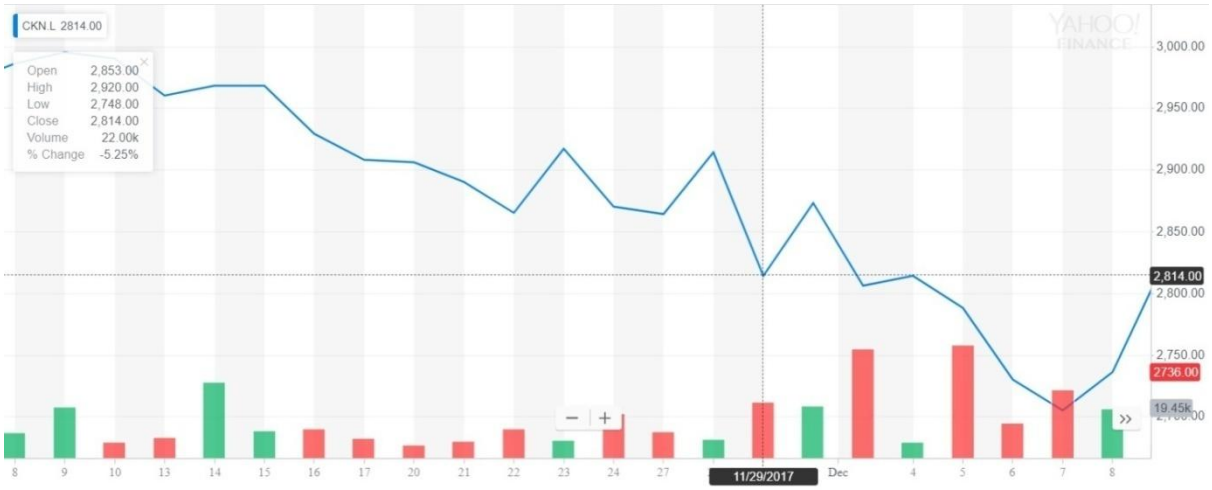
Αν και η Clarksons δεν προέβη στην πληρωμή των λύτρων και έσπευσε να ενημερώσει τους άμεσα ενδιαφερόμενους –μετόχους και πελάτες της- για το περιστατικό σύμφωνα με την ενημέρωση που εξέδωσε στο Χρηματιστήριο του Λονδίνου στις 29 Νοεμβρίου, είδε την τιμή της μετοχής της να κατρακυλά και να σημειώνει πτώση 5%[135] με την τιμή να διαμορφώνεται στα 2,814 £.

Στην εικόνα που ακολουθεί παρουσιάζεται η πορεία της μετοχής της εταιρίας όπου παρατηρούμε ότι στον απόηχο της ανακοίνωσης του περιστατικού παραβίασης υπήρξε μεγάλος όγκος συναλλαγών με πώληση των μετοχών για μερικές μέρες.

[133] UPDATE ON 2017 DATA BREACH – REGULATORY NOTICE by Clarkson

[134] Rethinking our Industry, Annual Report 2017 by Clarkson PLC

[135] https://www.logisticsmiddleeast.com/article-13696-cyberattack-on-clarkson's-shipbroker-reaffirms-industry's-vulnerability



Εικόνα 4: Πορεία μετοχής της Clarkson PLC την περίοδο της κυβερνοεπίθεσης[136].

Μετά το περιστατικό της παραβίασης των δεδομένων που διατηρούσε, η εταιρία στην ετήσια αναφορά του 2017 ανέφερε ότι θα εφαρμοστούν επιπρόσθετες βελτιώσεις στους ελέγχους για να μειώσουν τους κινδύνους και να μπορούν να αποτρέψουν τέτοιου είδους επιθέσεις στο μέλλον. Τονίζουν ότι θα συνεχίσουν να επενδύουν σημαντικά σε πιο ενισχυμένα μέτρα ασφαλείας, σε ανθρώπινο δυναμικό και πόρους κατάλληλους για την αποτροπή κυβερνοεπιθέσεων[137]. Σύμφωνα με την TradeWinds, η Clarksons πλήρωσε για έναν ολόκληρο χρόνο υπηρεσίες προστασίας ταυτότητας για τα άτομα που επηρεάστηκαν από την παραβίαση των προσωπικών δεδομένων[138].

5.3 Περίπτωση της COSCO

5.3.1 Η επιχείρηση

[136] Yahoo Finance

[137] Rethinking our Industry, Annual Report 2017 by Clarkson PLC

[138] https://www.tradewindsnews.com/ship-sales/clarksons-reveals-details-of-cyber-attack-and-blackmail-attempt/2-1-389004

Η*ChinaOceanShippingCo. Ltd.*,ήενσυντομία*COSCO*, είναι μια Κινέζικη ναυτιλιακή εταιρία-όμιλος με διεθνή δραστηριότητα και έδρα το Ocean Plaza στην περιοχή Xicheng του Πεκίνο με την ιστορία της να ξεκινά το 1961. Οι υπηρεσίες που προσφέρει είναι η μεταφορά φορτίων και επιβατών, η εφοδιαστική αλυσίδα –ο τομέας που της επιφέρει το μεγαλύτερο ποσοστό των εσόδων της-, η ναυπήγηση και επισκευή πλοίων καθώς και υπηρεσίες που παρέχονται στους λιμενικούς τερματικούς σταθμούς. Η COSCO επίσης πραγματοποιεί χρηματοδοτικές μισθώσεις πλοίων και ασχολείται με τις χρηματοοικονομικές επενδυτικές σε εγχώριες και διεθνείς αγορές[139].

Η εταιρεία έχει επενδύσει σε 56 λιμενικούς τερματικούς σταθμούς, συμπεριλαμβανομένων πάνω από 51 λιμενικούς τερματικούς σταθμούς containers, σε όλο τον κόσμο[140].Τα έσοδα της εταιρίας για το 2018 με βάση την ετήσια αναφορά της ανήλθαν στα 163,673,000US$[141].Τέλος, είναι εισηγμένη στα χρηματιστήρια της Σαγκάης και του Χονγκ Κονγκ και εξετάζεται η εισαγωγή της και στο χρηματιστήριο του Λονδίνου.

5.3.2 Ηκυβερνοεπίθεση

Στις 24 Ιουλίου το 2018, ο ναυτιλιακός τερματικός σταθμός της Cosco στο LongBeach της Αμερικής δέχεται μια ransomwareεπίθεση, αποτελώντας τη σημαντικότερη επίθεση που συνέβη μέσα στο έτος. Η επίσημη ανακοίνωση έρχεται μια ημέρα αργότερα στην ιστοσελίδα της ίδιας της εταιρίας, όπου ανακοινώνεται ότι λόγο της κατάρρευσης του τοπικού δικτύου και των συστημάτων στην Αμερική, οι τοπικές διευθύνσεις ηλεκτρονικού ταχυδρομείου και το δίκτυο των τηλεφώνων δεν λειτουργούν. Αν και η λειτουργία των πλοίων της έμεινε ανεπηρέαστη και οι κύριες λειτουργίες της εταιρίες συνέχισαν να διαδραματίζονται ομαλά, για προληπτικούς λόγους διέκοψαν κάθε είδους επικοινωνία μεταξύ της Αμερικής και τον

[139] https://www.bloomberg.com/profile/company/COSCZ:CH

[140] http://en.coscocs.com/col/col6918/index.html

[141] Delivering Our Growth Strategies Annual Report 2018, COSCO

υπολοίπων περιοχών μέχρις ότου να εντοπιστούν τα ευάλωτα σημεία του συστήματός τους και να αντιμετωπιστεί η επίθεση[142].

Στις 26 Ιουλίου ενημερώνουν το κοινό ότι μετά την απομόνωση των δικτύων για την διεξαγωγή της έρευνας, όλα τα δίκτυα εκτός αυτό της Αμερικής επανέρχονται στην κανονική τους λειτουργία όντας ασφαλή προς χρήση. Επίσης προειδοποιούν ότι επειδή οι έρευνες για το πρόβλημα της Αμερικής συνεχίζονται, μπορεί να προκύψουν καθυστερήσεις στην ανταπόκριση των υπηρεσιών που προσφέρει ο τερματικός σταθμός του LongBeach. Πέντεημέρες μετά την επίθεση, στις 30 Ιουλίου, ανακοινώνεται η πλήρης επαναφορά του δικτύου της Αμερικής με όλα τα μέσα επικοινωνίας να είναι πλέον σε λειτουργία και ασφαλή[143].

5.3.3 Τα αποτελέσματα

Αν και ακόμη δεν έχουν δοθεί πιο συγκεκριμένες πληροφορίες για την επίθεση, όπως η πηγή της κυβερνοεπίθεσης καθώς και ο αντίκτυπός της, το γεγονός ότι το περιστατικό περιορίστηκε και αντιμετωπίστηκε μέσα σε πέντε ημέρες δείχνει την ετοιμότητα της εταιρίας σε τέτοιου είδους επιθέσεις. Επίσης εκτιμάται ότι λόγο της γρήγορης ανταπόκρισής τους οι επιπτώσεις της κυβερνοεπίθεσης δεν είναι τόσο σοβαρές όσο ήταν στην περίπτωση της Maersk που προαναφέραμε[144].

Στην παρακάτω εικόνα παρουσιάζεται η πορεία της τιμής της μετοχής της Cosco στην περίοδο της επίθεσης. Παρατηρούμε ότι ενώ η τιμή της μετοχής την ημέρα της επίθεσης ήταν στα 3.4 δολάρια Χονγκ Κονγκ, μια ημέρα αργότερα,όταν δηλαδή ανακοινώθηκε επίσημα η επίθεση, η τιμή σημείωσε μια πτώση της τάξης σχεδόν του 2%. Στις ημέρες που

142 http://lines.coscoshipping.com/home/News/detail/1532508126128661104 2/5000000000000231?id=500000000000231

143 http://lines.coscoshipping.com/home/News/detail/1532923256561461356 9/5000000000000231?id=500000000000231

144 https://www.maritime-executive.com/article/cosco-reports-cyberattack-at-its-u-s-operations

ακολούθησαν όπου η εταιρία προέβαινε σε νέες ανακοινώσεις περί του περιστατικού η τιμή της μετοχής παρατηρούμε ότι ανέβαινε και κατέβαινε συνεχώς αντικατοπτρίζοντας και την ανησυχία του κοινού.

Εικόνα 5:Πορεία μετοχής της ChinaOceanShippingCo. Ltd., την περίοδο της κυβερνοεπίθεσης[145].

[145] Yahoo Finance

ΚΕΦΑΛΑΙΟ 6

ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ

6.1 Περιγραφή Δεδομένων

Αυτό το κεφάλαιο αποτελεί το πρακτικό τμήμα της εργασίας όπου αρχικά γίνεται μια συγκέντρωση δεδομένων από περιστατικά παραβίασης δεδομένων και εν συνεχεία αναλύονται και διεξάγονται κάποια συμπεράσματα.

Τα δεδομένα που χρησιμοποιήθηκαν έχουν αντληθεί από τον διαδικτυακό χώρο Information Is Beautiful[146], μια ιστοσελίδα που παρουσιάζει διάφορες απεικονίσεις με διαγράμματα και γραφήματα, οι οποίες είναι βασισμένες σε γεγονότα και δεδομένα διαρκώς ενημερωμένα και αναθεωρημένα.

Συγκεντρώθηκαν 346περιστατικά παραβίασης δεδομένων που υπέστησαν εταιρίες καθώς και ιδιωτικοί και δημόσιοι οργανισμοί απ' όλο τον κόσμο, από διάφορους κλάδους όπως αυτούς της υγείας, των χρηματοοικονομικών, της τεχνολογίας, των πωλήσεων και άλλους,καταλαμβάνοντας ένα μεγάλο εύρος ετών από το 2004 μέχρι και τον Σεπτέμβριο του 2019. Στα δεδομένα που συγκεντρώθηκαν αναφέρεται επίσης η μέθοδος που χρησιμοποιήθηκε για την εκάστοτε παραβίαση καθώς και η ευαισθησία των δεδομένων που εκλάπησαν.

Το δείγμα των 346 περιστατικών περιορίστηκε σημαντικά θέτοντας ως κριτήριο το ανοι ίδιες οι εταιρίες ή οι μητρικές αυτών ήταν εισηγμένες στα χρηματιστήρια την περίοδο της ανακοίνωσης της παραβίασης των δεδομένων τους και καταλήξαμε σε 117 περιστατικά παραβίασης δεδομένων. Για το σύνολο των εταιριών που ήταν εισηγμένες σε χρηματιστήρια

[146] https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

βρέθηκε η απόδοση της μετοχής τους για μια περίοδο ενός μηνός από την ημερομηνία ανακοίνωσης του περιστατικού παραβίασης στο ευρύ κοινόχρησιμοποιώντας τις ιστοσελίδες Yahoo Finance και Investing.com.

Οι κλάδοι των επιχειρήσεων που εμφανίζονται στο τελικό δείγμα των 117 περιστατικών παραβίασης είναι οι εξής:

- Διαδικτύου
- Τηλεπικοινωνίας
- Υγείας
- Τεχνολογίας
- Εφαρμογή (app)
- Τεχνολογίας και Λιανικού Εμπορίου
- Χρηματοοικονομικός
- Λιανικού Εμπορίου
- Παιχνιδιού
- Μεταφοράς
- Μέσων Μαζικής Ενημέρωσης
- Τεχνολογίας και Διαδικτύου

Οι μέθοδοι που εφαρμόστηκαν στις παραπάνω περιπτώσεις κυβερνοεπιθέσεων είναι οι εξής:

- Εσωτερική επίθεση
- Μη εξουσιοδοτημένη πρόσβαση
- Αδυναμία συστημάτων ασφάλειας
- Απώλεια συσκευής
- Σφάλμα

Τέλος η ευαισθησία των δεδομένων που παραβιάστηκαν στα 117 περιστατικά διαχωρίζεται στις παρακάτω κατηγορίες:

- Διευθύνσεις ηλεκτρονικού ταχυδρομείου / Διαδικτυακές πληροφορίες
- Πληροφορίες πιστωτικών καρτών
- Πλήρης πληροφορίες δεδομένων τραπεζικών λογαριασμών
- Αριθμός κοινωνικής ασφάλειας (SSN) / Προσωπικά δεδομένα
- Κωδικοί πρόσβασης ηλεκτρονικού ταχυδρομείου/ Δεδομένα υγείας

Στο παράρτημα 1 παρουσιάζονται οι παραπάνω εταιρίεσμε τα αντίστοιχα δεδομένα τους αναλυτικά.

6.2 Παλινδρόμηση

6.2.1 Δεδομένα Παλινδρόμησης

Με βάση τα παραπάνω δεδομένα και αφού τα μετατρέψαμε σε ποσοτικές μεταβλητές αντιστοιχίζοντας τον κάθε κλάδο των επιχειρήσεων, τη μέθοδο και την ευαισθησία των δεδομένων με έναν αριθμό (παραδείγματος χάρη: 1 - χρηματοοικονομικός κλάδος, 2 - κλάδος τηλεπικοινωνιών, κλπ και αντίστοιχα 1 - απώλεια συσκευής, 2 - μη εξουσιοδοτημένη πρόσβαση, κλπ), πραγματοποιήσαμε μια παλινδρόμηση με τη βοήθεια του προγράμματος eViews 9χρησιμοποιώντας τις εξής πέντεμεταβλητές:

- Απόδοση μετοχών (return) *Εξαρτημένη Μεταβλητή*
- Κλάδος επιχείρησης (sector)*Ανεξάρτητη Μεταβλητή*
- Μέθοδος παραβίασης των δεδομένων (method) *Ανεξάρτητη Μεταβλητή*
- Ευαισθησία των δεδομένων (datasensitivity) *Ανεξάρτητη Μεταβλητή*
- Έτος παραβίασης των δεδομένων (year) *Ανεξάρτητη Μεταβλητή*

Η εξίσωση της παλινδρόμησης,δηλαδή το θεωρητικό μοντέλο που συνδέει τις μεταβλητές και χρησιμοποιήθηκε, είναι η εξής:

$$return = \beta_0 + \beta_1 * sector + \beta_2 * method + \beta_3 * datasensitivity + \beta_4 * year + u$$

(όπου β_0 ο σταθερός όρος, β_1, β_2, β_3,β_4 οι συντελεστές των ανεξάρτητων μεταβλητών και u τα σφάλματα της παλινδρόμησης)

ηοποία στο πρόγραμμα του eViewsσυντάχθηκε ως εξής:

return c sector method datasensitivity year

Σκοπός της παλινδρόμησης αυτής ήταν η απάντηση στο ερώτημα εάν οι τέσσερις ανεξάρτητες μεταβλητές: ο κλάδος της επιχείρησης, η μέθοδος παραβίασης των δεδομένων, η ευαισθησία των δεδομένων που παραβιάστηκαν και το έτος της παραβίασης, επηρεάζουν την απόδοση της μετοχής των εταιριών που υπέστησαν την παραβίαση των δεδομένων τους, δηλαδή αν οι ανεξάρτητες μεταβλητές που θέσαμε είναι στατιστικά σημαντικές ή όχι.

Για να θεωρηθεί μια μεταβλητή στατιστικά σημαντική με επίπεδο σημαντικότητας 5% θα πρέπει το probability της κάθε ανεξάρτητης μεταβλητήςνα είναι μικρότερο από 0.05 ανεξαρτήτου μεγέθους του δείγματος ή διαφορετικά ελέγχουμε το t-Statistic το οποίο θα πρέπει να είναι μεγαλύτερο κατ΄ απόλυτη τιμή από το +2, δηλαδή να είναι εντός των ορίων (-∞,-2] και [+2, +∞), υπό την προϋπόθεση ότι το δείγμα υπερβαίνει τις 40 παρατηρήσεις.

6.2.2 Αποτελέσματα Παλινδρόμησης

Τρέχοντας την παραπάνω παλινδρόμηση των 117 παρατηρήσεων παίρνουμε ταεξής αποτελέσματααπό το eViews:

Dependent Variable: RETURNS
Method: Least Squares
Date: 10/26/19 Time: 22:24
Sample: 1 117
Included observations: 117

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	6.594150	5.424907	**1.215532**	**0.2267**
SECTOR	0.001733	0.001863	**0.929983**	**0.3544**
METHOD	0.003876	0.011946	**0.324424**	**0.7462**
DATASENSITIVITY	-0.010200	0.007918	**-1.288097**	**0.2004**
YEAR	-0.003274	0.002703	**-1.210963**	**0.2285**
R-squared	0.038656	Mean dependent var		-8.45E-05

Εικόνα 6:Αποτελέσματα παλινδρόμησης eViews

Παρατηρούμε λοιπόν ότι όλες οι ανεξάρτητες μεταβλητές που θέσαμε στο θεωρητικό μοντέλο(sector, method,datasensitivityκαιyear) καθώς και ο σταθερός όροςc είναι στατιστικά ασήμαντα μιας και τα t-Statisticείναι εκτός των ορίων (-∞,-2] και [+2,+∞) και τα

probabilities τους είναι σημαντικά μεγαλύτερα του 0.05.Έτσι, με βάση το δείγμα των 117 περιπτώσεων παραβίασης που συγκεντρώσαμε, συμπεραίνουμε ότι ο κλάδος των επιχειρήσεων που δέχθηκε την επίθεση, η μέθοδος που χρησιμοποιήθηκε, η ευαισθησία των δεδομένων που παραβιάστηκαν καιτο έτος κατά το οποίο έλαβε χώρα η παραβίαση, δεν αποτελούν καθοριστικούς παράγοντες που επηρεάζουντην απόδοση των μετοχών των εταιριών που υπέστησαν την παραβίαση δεδομένων.

Επίσης μπορούμε να σχολιάσουμε το R-squared της παλινδρόμησης, το οποίο μας δείχνει ότι μόλις το 3.86% της εξαρτημένης μεταβλητής εξηγείται από το σύνολο των ανεξάρτητων μεταβλητών, ένα ποσοστό που είναι αρκετά μικρό και μας αποδεικνύει κι αυτό με τη σειρά του ότι οι ανεξάρτητες μεταβλητές του μοντέλου μας δεν επηρεάζουν την απόδοση της μετοχής των εταιριών.

Στην συνέχεια παρατίθεται ένας πίνακας που συγκεντρώνει τους συντελεστές συσχέτισης των μεταβλητών που απαρτίζουν το θεωρητικό μοντέλο με το όριο των τιμών να κυμαίνεται από -1 μέχρι και +1 ανάλογα και στο οποίο παρατηρούμε ότι οι πληθώρα των ανεξάρτητων μεταβλητών παρουσιάζει αρνητικό συντελεστή συσχέτισης με την απόδοση των μετοχών που είναι η εξαρτημένη μεταβλητή. Η μεγαλύτερη συσχέτιση παρουσιάζεται μεταξύ της μεθόδου και του έτους με ποσό 0.4857564, ενώ τη μικρότερη συσχέτιση παρουσιάζουν ο κλάδος με την ευαισθησία των δεδομένων με ποσό -0.010927.

	RETURNS	SECTOR	METHOD	DATASENSITIVITY	YEAR
RETURNS	1.000000	0.087509	-0.020389	-0.133761	-0.121251
SECTOR	0.087509	1.000000	0.153221	**-0.010927**	0.049330
METHOD	-0.020389	0.153221	1.000000	0.046355	0.487564
DATASENSITIVITY	-0.133761	-0.010927	0.046355	1.000000	0.110857
YEAR	-0.121251	0.049330	**0.487564**	0.110857	1.000000

Εικόνα 7: Μήτρα συντελεστών συσχέτισης μεταξύ των μεταβλητών της παλινδρόμησης

ΚΕΦΑΛΑΙΟ 7

ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Συμπεράσματα

Φτάνοντας στο τέλος αυτής της εργασίας οι πρωταρχικοί στόχοι που τέθηκαν έχουν απαντηθεί πλήρως, με τα στατιστικά δεδομένα κατά μήκος όλης της διπλωματικής και την παλινδρόμηση του τελευταίου ενεργού κεφαλαίου να δίνουν μια ολοκληρωμένη εικόνα που αποτελείται από τα συμπεράσματα που παραθέτουμε παρακάτω.

Ο κυβερνοχώρος είναι μια ολοζώντανη υπόσταση που εξελίσσεται και αλλάζει μορφή συνεχώς δημιουργώντας νέες και ολοένα και περισσότερες προκλήσεις. Η πλειονότητα των εταιριών ανεξαρτήτου γεωγραφικής τοποθέτησης και τομέα απασχόλησης επαφίεται με το πέρασμα των δεκαετιών όλο και περισσότερο στα "θαυματουργά χέρια" του Διαδικτύου, γεγονός που αυξάνει κατά συνέπεια και τον κίνδυνο που εγκυμονεί από τη χρήση του. Οι κυβερνοεπιθέσεις κατατάσσονται από πολλές και διαφορετικές μελέτες μέσα στους πέντε κορυφαίους κινδύνους που καλούνται να αντιμετωπίσουν οι διάφορες ανά το κόσμο επιχειρήσεις αποτελώντας τον "εφιάλτη" των CEOs μιας και το κόστος τους το οποίο παρουσιάζει συνεχή αύξηση μπορεί να αποβεί μοιραίο.

Όσον αφορά το θεσμικό πλαίσιο που σχετίζεται με τα θέματα γύρω από τις κυβερνοεπιθέσεις και την προστασία από αυτές έγινε πλήρως αντιληπτό πως βρίσκεται σε μια ατέρμονη αλλαγή μέσα στα χρόνια προσπαθώντας να προλάβει και να καλύψει τις νέες απαιτήσεις αλλά και τους κινδύνους του κυβερνοχώρου μιας και καινούργιες μέθοδοι και τρόποι παραβίασης δεδομένων γεννιούνται συνεχώς. Τον βενιαμίν μέσα στο χρονικό των νομικών πλαισίων αποτελεί ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, ο οποίος αν και δεν έχει εφαρμοστεί πλήρως από της εταιρίες που πρέπει να τηρούν τις απαιτήσεις του, σύμφωνα με μελέτες που αναφέρθηκαν συμβάλει σημαντικά στην μείωση των κυβερνοεπιθέσεων και των ζημιών τους.

Προσεγγίστηκε το ζήτημα της ασφάλισης του κυβερνοχώρου η οποία ακόμη τελεί τα πρώτα της βήματα στην αγορά της ασφάλισης, με το ασφάλιστρο που απαιτείται να καταβάλλουν οι επιχειρήσεις να θεωρείται πολλές φορές υπέρογκο. Οι υψηλές τιμές των ασφαλίστρων είναι απόρροια των περιορισμένων ιστορικών δεδομένων που διατίθενται για τις κυβερνοεπιθέσεις μιας και της αποσιώπησης τέτοιου είδους περιστατικών από τις περισσότερες επιχειρήσεις αλλά και της αδυναμίας αποτίμησης των ψηφιακών περιουσιακών στοιχείων που διαθέτουν οι επιχειρήσεις καθιστώντας δύσκολο των υπολογισμό μιας δυνητικής απώλειας τους.

Νούμερο ένα στόχος κυβερνοεπιθέσεων είναι οι χρηματοοικονομικές και ασφαλιστικές επιχειρήσεις, με τις επιχειρήσεις στον κλάδο της μεταφοράς,στις οποίες συγκαταλέγονται και αυτές της ναυτιλίας, να τις διαδέχονται. Η ναυτιλία δέχεται συνεχώς χτυπήματα από τους επίδοξους ψηφιακούς εγκληματίες με τεράστιες επιπτώσεις, οικονομικής αλλά και όχι μόνο φύσεως, λόγω της μεγάλης εξάρτησής της από την τεχνολογία και το Διαδίκτυο. Με βάση διάφορες έρευνες που έχουν διεξαχθεί πάνω στο θέμα των κυβερνοεπιθέσεων που δέχεται η ναυτιλία, αν εξαιρέσουμε τις μεγάλες επιχειρήσεις του κλάδου που έχουν επιτελέσει το μέγιστο επίπεδο κυβερνοασφάλειας και κρατούν διαρκώς ενημερωμένο και καλά εκπαιδευμένο το προσωπικό τους, είναι ανησυχητικό το ότι η πλειοψηφία των ναυτιλιακών εταιριών δεν θεωρείται καταλλήλως προετοιμασμένη να αντιμετωπίσει περιστατικά παραβίασης δεδομένων, κάτι που επαληθεύτηκε και μέσα από τις μελέτες περιπτώσεων που αναλύσαμε στο 5^{ο} κεφάλαιο, με τις εταιρίες να οχυρώνονται καλύτερα και να λαμβάνουν μέτρα προστασίας στον απόηχο των κυβερνοεπιθέσεων που δέχθηκαν.

Τέλος, με βάση την παλινδρόμηση που πραγματοποιήσαμε στο 6^{ο} κεφάλαιο, έχοντας υπόψη το μικρό μέγεθος του δείγματος που ήταν στη διάθεσή μας, συμπεραίνουμε ότι ούτε ο κλάδος της επιχείρησης, ούτε η μέθοδος που εφαρμόστηκε αλλά ούτε και η ευαισθησία των δεδομένων που παραβιάστηκαν και το έτος όπου διενεργήθηκε η παραβίασηεπηρέασαν την απόδοση της μετοχής των εταιριών που δέχθηκαν κυβερνοεπίθεση. Το παραπάνω συμπέρασμα μπορεί να μεταφραστεί και ως εξής: η αγορά και το ευρύ κοινό δεν αντιδρά τελικά στις ανακοινώσεις παραβίασης δεδομένων ίσως διότι δεν κατανοεί τα βαθύτερα και πραγματικά αποτελέσματα μιας τέτοιας επίθεσης. Επίσης σημαντικό ρόλο παίζει και το γενικό οικονομικό κλίμα που επικρατούσε τα χρόνια αυτά μιας και σ’ αυτά περιλαμβάνονται

και τα χρόνια της οικονομικής κρίσης, οπότε οι αποδόσεις των μετοχών των εταιριών αυτών μπορεί να είναι αποτέλεσμα των γενικών οικονομικών συνθηκών και όχι αποκλειστικά και μόνο από τις κυβερνοεπιθέσεις που δέχθηκαν.

6.2 Περιορισμοί Έρευνας

Η πιο βασική δυσκολία που συναντήθηκε κατά την συγγραφή της παρούσας εργασίας ήταν το γεγονός ότι ο κλάδος της ναυτιλίας δεν είναι ακόμη αρκετά ανοικτός στο θέμα της γνωστοποίησης των κυβερνοεπιθέσεων. Έτσι πολλές είναι εκείνες οι επιχειρήσεις, που ενώ έχουν υποστεί παραβίαση των δεδομένων τους, προτιμούν να αποσιωπήσουν το συμβάν ή να αποκρύψουν τις βασικές λεπτομέρειες -όπως την μέθοδο της επίθεσης και το κόστος της-, με φόβο την δυνητική ζημία που θα υποστεί η φήμη τους αλλά και την πιθανότητα να ξανά πέσουν θύματα κυβερνοεπιθέσεων. Ένας ακόμη σημαντικός περιορισμός είναι το μικρό δείγμα που συλλέχθηκε και χρησιμοποιήθηκε στην παλινδρόμηση που πραγματοποιήθηκε στο τελευταίο κεφάλαιο της εργασίας.

6.3 Προτεινόμενες Θεματικές Περιοχές για Μελλοντική Έρευνα

Ενδιαφέρον θα αποτελούσε η πραγματοποίηση μιας έρευνας που θα εξέταζε, πέρα από τον κλάδο δραστηριότητας που ήδη ερευνήθηκε στην παρούσα εργασία, αν κάποια άλλα χαρακτηριστικά εταιριών που έχουν υποστεί παραβίαση δεδομένων,όπως είναι το μέγεθός τους, δηλαδή ο αριθμός των εργαζομένων που απασχολούν, ή η γεωγραφική τους τοποθέτηση, αποτελούν παράγοντες που σχετίζονται με τη θετική ή αρνητική απόδοση των μετοχών τους μετά την ανακοίνωση της παραβίασης.

Επίσης για τις 117 περιπτώσεις παραβίασης δεδομένων που συγκεντρώθηκαν για τους σκοπούς της παλινδρόμησης θα μπορούσε να πραγματοποιηθεί μελέτη των περιστατικών (eventstudy) ώστε να εξεταστούν πιο λεπτομερώς και να εξαγχθούν συμπεράσματα για κάθε περίπτωση ξεχωριστά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξένα Άρθρα σε Επιστημονικά Περιοδικά

1. Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T. &Upton D.M. (2016), "*Cyber Harm: Concepts, Taxonomy and Measurement*", Saïd Business School WP, 23

2. Bandyopadhyay, T. & Mookerjee, V. (2017), "*A model to analyze the challenge of using cyber insurance*", Information Systems Frontiers, Volume 21, Issue 2, pp 301–325

3. Biener, C., Eling, M. & Wirfs, J.H (2015), "*Insurability of Cyber Risk: An Empirical Analysis*", Geneva Papers on Risk and Insurance, Vol. 40, No. 1, 2015

4. Cebula, J.J& Young, L.R. (2010), "*A Taxonomy of Operational CyberSecurity Risks*", Technical Note CMU/SEI-2010-TN-028, CEPT Carnegie Mellon University

5. Eling, M. & Werner, S. (2016), "*What do we know about cyber risk and cyber risk insurance?*", The Journal of Risk Finance Vol. 17 No. 5, 2016, pp. 474-491

6. Jo, Y., Kang, J. & Cha, Y. (2018), "*Cyber Piracy Threat Analysis*", Cryptology and Information Security Series, October 2018

7. Kshetri, N. (2018), "*The Economics of Cyber-Insurance*", IEEE IT Professional, Vol. 20, pp. 9-14

8. Kessler, G.C. & Craiger, J.P. (2018), "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System", The

International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 12, No. 3, pp. 429-437

9. Lin, Z., Parsa, R., Rees Ulmer, J. & Sapp, T. (2018), "*Pricing Cyber Security Insurance:A Copula Model Using an Objective, Verifiable, Loss Measure*", (July 17, 2018)

10. LivanisE. (2016), "*Financial aspects of cyber risks and taxonomy for the efficient handling of these risks*", 14th International Scientific Conference on Economic and Social Development Belgrade, Serbia, 13-14 May 2016

11. Mraković, I. & Vojinović. R. (2019), "*Maritime Cyber Security Analysis – How to Reduce Threats?*", TRANSACTIONS ON MARITIME SCIENCE, Vol. 13, pp. 132-139

12. Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhuklan, S.K. (2013), "*Cyber-risk decision models: To insure IT or not?*", Decision Support Systems, Volume 56, December 2013, Pages 11-26

13. Odel, L.A., Fauntleroy, J.C. & Wagner, R.R. (2015), "*Cyber Insurance - Managing Cyber Risk*", (No. IDA-NS-D-5481), INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA

14. Phillips, M. (2018), "*International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*", Human Genetics, Vol 137, Issue 8, pp. 575-582

15. Presthus, W., Sørum, H. & Andersen, L.R. (2018), "GDPR compliance in Norwegian companies", Norwegian Conference for IT Use in Organisations (NOKOBIT), pp. 1-15

16. Ruan, K. (2016), "*Introducing cybernomics: A unifying economic framework for measuring cyber risk* ", Computers & Security, Vol. 65, pp. 77-89

17. Saini, H., Rao, Y.S &Panda, T.C. (2012), "*Cyber-Crimes and their Impacts: A Review*", International Journal of Engineering Research and Applications, Vol 2, Issue 2, Mar-Apr 2012, pp 202-209

18. Shoukat, S. & Bashir, A. (2017), "*Cyber Crime- Techniques, Prevention and Cyber Insurance*", International Journal of Computing and Network Technology, Volume 6, No1

19. Sullivan, C. (2019), "*EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era*", Computer Law & Security Review, Vol. 35, pp. 380–397

20. Teixeira, G.A., Silva, M.M. & Pereira, R. (2019), "The critical success factors of GDPR implementation: a systematic literature review", DIGITAL POLICY, REGULATION AND GOVERNANCE,Vol. 21 No. 4, pp. 402-418

Μελέτες-Αναφορές

1. ALLIANZ RISK BAROMETER, TOP BUSINESS RISKS FOR 2019

2. Annual Report 2017 by A.P. Møller – Mærsk A/S

3. Annual Report 2018 by A.P. Møller – Mærsk A/S

4. Annual Report 2017 by Clarkson PLC

5. Annual Report 2018 by Clarkson PLC

6. Breach Level Index, 2018 First Half Review, Germalto

7. Cost of a Data Breach Study: Global Overview 2018, IBM

8. Cost of Data Breach Report 2019, IBM

9. Cyber Risk Perception Survey Report 2018 by Marsh & McLennan Agency

10. Delivering Our Growth Strategies Annual Report 2018, COSCO

11. Economic impact of cybercrime- No slowing down, 2018, McAfee

12. General Data Protection Regulation, Luxembourg market status: Smooth Sailing or Hot Water? December 2018, PWC

13. Global Maritime Issues Monitor 2018, by Global Maritime Forum, Marsh and IUMI

14. Know your cyber enemy: Understanding the motives behind cyber attacks, IBM X-Force® Research, IBM Security

15. Internet Security Alliance (ISA) & American National Standards Institute (ANSI) (2010), The financial management of cyber risk, An Implementation Framework for CFOs, published by ANSI

16. Jones Walker LLP 2018, Maritime Cybersecurity Survey

17. Managing cyber security as a business risk: Cyber insurance in the digital age, Ponemon Institute LLC 2013

18. Maximizing the value of your data privacy investments Data Privacy Benchmark Study 2019, Cisco

19. MMC Cyber Handbook 2019, Perspectives on Cyber Risk in the Digital Era, Marsh & McLennan Insights

20. REVIEW OF MARITIME TRANSPORT 2018, UNCTAD

21. SAFETY AND SHIPPING REVIEW 2018: An annual review of trends and developments in shipping losses and safety, Allianz

22. Securing the digital economy, Reinventing the Internet for Trust 2019, Accenture

23. Sizing the Standalone Commercial Cyber Insurance Market, 2018 Verisk

24. The cost of Cybercrime 2019, Ninth Annual Cost of Cybercrime Study, Ponemon Institute

25. The Global Risks Report 2019, World Economic Forum

26. TRUST SERVICES SECURITY INCIDENTS 2018 ENISA Annual Report

27. The U.S. State of Cybercrime Study 2018 by CSO and CERT Division of Software Engineering Institute at Carnegie Mellon University

28. Verizon Data Breach Investigations Report 2019

29. X-Force Threat Intelligence Index 2019, IBM Security Research

Λοιπή Ξένη Βιβλιογραφία

1. *DoD Joint Publication 3-12(R) Cyberspace Operations (5 February 2013)*(https://web.archive.org/web/20180127164919/http:/www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf)

2. Mayer, M., Martino, L., Mazurier, P. & Tzvetkova, G. (2014), "*How would you define Cyberspace?*" working paper

3. Practical Law Company, Whitepaper on Cyber Attacks

4. Silgado, D.M. (2018), "*Cyber-attacks: a digital threat reality affecting the maritime industry*", World Maritime University Dissertations, 663

5. 17 Types of Cyber Attacks To Secure Your Company From in 2019, phoenixNAP Global IT Services

6. Zhu, Q. (2018), "*Cyber Insurance*", New York University, Brooklyn

Ελληνική Βιβλιογραφία

1. ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ (27 Απριλίου 2016) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Ηλεκτρονικές Πηγές

1. https://www.weforum.org/centre-for-cybersecurity

2. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

3. https://el.wikipedia.org/wiki/Ransomware

4. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

5. https://www.statista.com/statistics/976526/global-cyber-insurance-market-size/

6. https://www.privacyrisksadvisors.com/gdpr-infographic/

7. https://www.pinsentmasons.com/out-law/guides/data-protection

8. https://gdpr.eu/what-is-gdpr/

9. https://en.wikipedia.org/wiki/Data_Protection_Act_1998

10. https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

11. https://en.wikipedia.org/wiki/Maersk#Piracy

12. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

13. http://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

14. https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

15. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

16. https://finance.yahoo.com

17. https://www.tradewindsnews.com/safety/ap-moller-maersk-more-than-a-year-on-from-notpetya-cyber-attack/2-1-426819

18. https://en.wikipedia.org/wiki/Clarkson_plc

19. https://www.logisticsmiddleeast.com/article-13696-cyberattack-on-clarkson's-shipbroker-reaffirms-industry's-vulnerability

20. https://www.tradewindsnews.com/ship-sales/clarksons-reveals-details-of-cyber-attack-and-blackmail-attempt/2-1-389004

21. https://www.bloomberg.com/profile/company/COSCZ:CH

22. http://en.coscocs.com/col/col6918/index.html

23. http://lines.coscoshipping.com/home/News/detail/1532508126128661104 2/50000000000000231?id=50000000000000231

24. http://lines.coscoshipping.com/home/News/detail/1532923256561461356 9/50000000000000231?id=50000000000000231

25. https://www.maritime-executive.com/article/cosco-reports-cyberattack-at-its-u-s-operations

26. https://www.insurancedaily.gr/galliko-prostimo-50-ekat-evro-stin-google-logo-gdpr/

27. https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

28. https://www.investing.com

Βιβλία

1. Τσουραμάνης Χ., (2005), "ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ: Η (αν)ασφαλής όψη του Διαδικτύου", ΕΚΔΟΣΕΙΣ: ΒΑΣ. Ν. ΚΑΤΣΑΡΟΥ

ΠΑΡΑΡΤΗΜΑ 1

ΕΤΑΙΡΙΑ	ΕΤΟΣ	ΚΛΑΔΟΣ	ΜΕΘΟΔΟΣ	ΕΥΑΙΣΘΗΣΙΑ ΔΕΔΟΜΕΝΩΝ	ΣΥΜΒΟΛΟ ΜΕΤΟΧΗΣ	ΑΠΟΔΟΣΗ ΜΕΤΟΧΗΣ
Ameritrade Inc.	2005	financial	lost device	SSN/Personal details	AMTD	0.2864
Citigroup	2005	financial	lost device	Credit card information	C	-0.0291
Automatic Data Processing	2006	financial	poor security	SSN/Personal details	ADP	0.0372
KDDI	2006	telecoms	hacked	Just email address/ Online information	9433.T	0.1106
Hewlett Packard	2006	tech, retail	lost device	SSN/Personal details	HPQ	-0.0013
Monster.com	2007	web	hacked	SSN/Personal details	MWW	-0.0122
Fidelity National Information Services	2007	financial	inside job	Credit card information	FIS	-0.1203
Gap Inc	2007	retail	lost device	SSN/Personal details	GPS	0.0092
Dai Nippon Printing	2007	retail	inside job	Just email address/ Online information	7912.T	0.1003
TK / TJ Maxx	2007	retail	hacked	Credit card information	TJX	0.0694
JP Morgan Chase	2007	financial	lost device	Credit card information	JPM	-0.0069
TD Ameritrade	2007	financial	hacked	Just email address/ Online information	AMTD	0.094
BNY Mellon Shareowner Services	2008	financial	lost device	Just email address/ Online information	BK	-0.0689
Countrywide Financial Corp	2008	financial	inside job	SSN/Personal details	BAC*	-0.0619
Countrywide Financial Corp	2008	financial	inside job	Credit card information	BAC*	-0.0619
AT&T	2008	telecoms	lost device	Just email address/ Online information	T	-0.1744
Starbucks	2008	retail	lost device	SSN/Personal details	SBUX	0.1066
T-Mobile, Deutsche Telecom	2008	telecoms	lost device	Just email address/ Online information	DTE.DE*	-0.01069
Heartland	2009	financial	hacked	Credit card information	HTLF	-0.2082
Health Net	2009	healthcare	lost device	Email password/ Health records	CNC*	0.1379
Triple-S Salud, Inc.	2010	healthcare	lost device	Email password/ Health records	GTS*	0.0185

AT&T	2010	telecoms	hacked	Just email address/ Online information	T	-0.0028
Sony PSN	2011	gaming	hacked	Just email address/ Online information	SNE	-0.0838
Sega	2011	gaming	hacked	SSN/Personal details	6460.T*	0.0854
Citigroup	2011	financial	hacked	Credit card information	C	0.1128
Sony Pictures	2011	web	hacked	Just email address/ Online information	SNE*	0.0011
Accendo Insurance Co.	2011	healthcare	poor security	SSN/Personal details	CNC*	0.0746
Sony Online Entertainment	2011	gaming	hacked	Credit card information	SNE*	-0.0785
Honda Canada	2011	retail	hacked	SSN/Personal details	HMC*	-0.0223
Nexon Korea Corp	2011	web	hacked	SSN/Personal details	041140.KQ	-0.0367
Global Payments	2012	financial	hacked	Credit card information	GPN	-0.0223
Blizzard	2012	gaming	hacked	SSN/Personal details	ATVI*	0.0318
Zappos	2012	web	hacked	SSN/Personal details	AMZN*	0.0046
KT Corp.	2012	telecoms	hacked	SSN/Personal details	030200.KS	0.0734
Yahoo Voices	2012	tech, web	hacked	Just email address/ Online information	AABA*	-0.0344
Last.fm	2012	web	hacked	Just email address/ Online information	CBS*	0.0258
Apple	2012	tech, retail	accidentally published	SSN/Personal details	AAPL	-0.012
Citigroup	2013	financial	accidentally published	SSN/Personal details	C	-0.0286
Living Social	2013	web	hacked	Just email address/ Online information	AMZN*	0.0272
Yahoo	2013	web	hacked	SSN/Personal details	AABA	0.0332
Apple	2013	tech, web	hacked	Just email address/ Online information	AAPL	0.1798
NASDAQ	2013	financial	hacked	Just email address/ Online information	NDAQ	-0.0885
UbiSoft	2013	gaming	hacked	SSN/Personal details	UBI	0.1238
Nintendo	2013	gaming	hacked	SSN/Personal details	7974.T	0.0755
Facebook	2013	web	accidentally published	Just email address/ Online information	FB	0.0281
Yahoo Japan	2013	tech, web	hacked	Just email address/ Online information	4689.T	-0.0607

Court Ventures	2013	financial	inside job	SSN/Personal details	EXPN*	-0.0648
Vodafone	2013	telecoms	inside job	Credit card information	VOD	0.0608
Adobe	2013	tech	hacked	Full bank account details	ADBE	0.0733
Target	2013	retail	hacked	Credit card information	TGT	-0.0521
Sony Pictures	2014	media	hacked	SSN/Personal details	SNE	-0.0521
Ebay	2014	web	hacked	Just email address/ Online information	EBAY	-0.049
UPS	2014	retail	hacked	Credit card information	UPS	0.0065
JP Morgan Chase	2014	financial	hacked	Credit card information	JPM	-0.0737
HSBC Turkey	2014	financial	hacked	Email password/Health records	HSBC*	-0.0566
Japan Airlines	2014	transport	hacked	SSN/Personal details	9201.T	-0.0076
Gmail	2014	web	hacked	Just email address/ Online information	GOOGL*	-0.0357
Home Depot	2014	retail	hacked	Credit card information	HD	0.036
Dominios Pizzas (France)	2014	retail	hacked	Just email address/ Online information	DPZ*	0.0153
Twitch.tv	2015	web	hacked	Just email address/Online information	AMZN*	0.1898
Sanrio	2015	web	poor security	SSN/Personal details	8136.T	-0.0951
VTech	2015	web	hacked	Full bank account details	0303.HK	-0.0934
TalkTalk	2015	telecoms	hacked	SSN/Personal details	TALK.L	-0.1238
Experian / T-mobile	2015	telecoms	hacked	Credit card information	EXPN.L	0.0774
CarPhone Warehouse	2015	telecoms	hacked	Full bank account details	DC*	-0.0646
British Airways	2015	transport	hacked	Just email address/ Online information	IAG.L*	-0.073
Anthem	2015	healthcare	hacked	SSN/Personal details	ANTM	0.0647
LinkedIn	2016	web	hacked	Just email address/ Online information	LNKD	0.4861
Tumblr	2016	web	hacked	Just email address/ Online information	AABA*	-0.0054
Yahoo	2016	web	hacked	SSN/Personal details	AABA	-0.0448
Minecraft	2016	gaming	hacked	Just email address/ Online information	MSFT*	0.0087

Mail. ru	2016	web	hacked	SSN/Personal details	MAILRq	0.0388
Lynda.com	2016	web	hacked	Just email address/ Online information	MSFT*	-0.0207
Wendy's	2016	retail	hacked	Credit card information	WEN	0.0366
World Check	2016	media	poor security	Credit card information	TRI*	0.052
VK	2016	web	hacked	Email password/ Health records	MAILRq*	-0.0792
MySpace	2016	web	hacked	Just email address/ Online information	TIME*	0.0372
Three	2016	telecoms	hacked	SSN/Personal details	0001.HK*	-0.0385
Dailymotion	2016	web	hacked	Just email address/ Online information	VIV*	0.024
Weebly	2016	web	hacked	Email password/ Health records	SQ*	0.0867
Interpark	2016	web	hacked	SSN/Personal details	035080.KQ	-0.0893
Quest Diagnostics	2016	healthcare	hacked	Email password/ Health records	DGX	0.0154
Yahoo	2017	web	hacked	Email password/ Health records	AABA	0.0037
Snapchat	2017	app	hacked	Just email address/ Online information	SNAP	-0.002
Cellebrite	2017	tech	hacked	SSN/Personal details	6736.T*	0.0962
Bell	2017	telecoms	hacked	Just email address/ Online information	BCE*	-0.002
TIO Networks	2017	financial	hacked	Email password/ Health records	PYPL*	-0.0146
Instagram	2017	web	hacked	Just email address/ Online information	FB*	-0.0067
Viacom	2017	web	hacked	Email password/ Health records	VIAB	-0.0225
Equifax	2017	financial	hacked	Email password/ Health records	EFX	-0.2199
Cathay Pacific Airways	2018	transport	hacked	Credit card information	0293.HK	0.1111
Google+	2018	web	poor security	SSN/Personal details	GOOGL	-0.053
Marriott Hotels	2018	retail	hacked	Credit card information	MAR	-0.0677
Facebook	2018	web	hacked	Just email address/ Online information	FB	-0.0258
Dixons Carphone	2018	telecoms	hacked	Just email address/	DC	-0.0114

				Online information		
Saks and Lord & Taylor	2018	retail	hacked	Credit card information	HBC*	0.0011
British Airways	2018	transport	hacked	Email password/ Health records	IAG.L*	-0.0902
T-Mobile	2018	telecoms	hacked	Just email address/ Online information	DTE.DE*	-0.0191
MyFitnessPal	2018	app	hacked	Just email address/ Online information	UAA*	0.0905
Ticketmaster	2018	web	hacked	Credit card information	LYV*	0.0717
Firebase	2018	app	poor security	Full bank account details	GOOGL*	0.0248
Orbitz	2018	web	hacked	Credit card information	EXPE*	-0.0049
Twitter	2018	app	poor security	Just email address/ Online information	TWTR	0.195
Amazon	2018	retail	accidentally published	Just email address/ Online information	AMZN	-0.0918
Amazon	2018	tech	poor security	Just email address/Online information	AMZN	-0.0918
Dell	2018	tech	hacked	Just email address/ Online information	DELL	-0.2304
SKY Brasil	2018	telecoms	poor security	Just email address/ Online information	T*	-0.069
Facebook	2018	web	hacked	SSN/Personal details	FB	-0.1161
Newegg	2018	retail	hacked	Credit card information	002280.SZ*	-0.2263
Quest Diagnostics	2019	healthcare	poor security	Email password/ Health records	DGX	0.0812
First American Financial Corporation	2019	financial	poor security	Email password/ Health records	FAF	-0.0041
Toyota	2019	transport	hacked	SSN/Personal details	7203.T	0.0644
HauteLook	2019	retail	hacked	Just email address/ Online information	JWN*	-0.0227
500px	2019	web	hacked	SSN/Personal details	000681.SZ*	0.159
Capital One	2019	financial	hacked	Credit card information	COF	-0.1104
Suprema	2019	tech	poor security	Full bank account details	236200.KQ	-0.1812
Facebook	2019	web	poor security	SSN/Personal details	FB	-0.0357

*Μετοχή της μητρικής εταιρίας στην οποία ανήκει η εταιρία που υπέστη την παραβίαση δεδομένων