2018

ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑ ΚΑΙ ΝΑΥΤΙΛΙΑ

Νίκος Παρασκευάς
ΑΕΝ ΜΑΚΕΔΟΝΙΑΣ 2018

Περιεχόμενα

Περίληψη/Abstract……σελ 4

Λέξεις κλειδιά/Key Words……σελ 4

Εισαγωγή

Τι είναι κυβερνοχώρος……..σελ 5

Οι κινητήριες δυνάμεις στο κυβερνοχώρο……σελ 5

ΚΕΦΑΛΑΙΟ 1ο

Ασφάλεια κυβερνοχώρου στο χώρο της ναυτιλίας…….....σελ 9

Παραβίαση Παραμέτρου…..……...σελ 10

Η πολυπλοκότητα των συστημάτων……...σελ 11

Κωδικοί πρόσβασης και προνομιούχοι χρήστες…….σελ 11

Προληπτικά μέτρα ασφαλείας (ESC)…….σελ 11

ΚΕΦΑΛΑΙΟ 2ο

Περιστατικά επιθέσεων από το κυβερνοχώρο……σελ 14

Το λιμάνι της Αμβερσας…….σελ 14

Επιθέσεις στα συστήματα ναυσιπλοΐας…….....σελ 14

Οι αντιδράσεις των ασφαλιστών για τις επιθέσεις στον κυβερνοχώρο……..σελ 16

Κλείσιμο του κενού κάλυψης…….σελ 17

Συμπεράσματα……σελ 17

ΚΕΦΑΛΑΙΟ 3ο

Lloyd's Cyber Attack…….....σελ 18

Ο λόγος που είναι απαραίτητη μια στρατηγική ενάντια στο Cyber Attack……σελ 19

Lloyd's Cyber Attack Strategy……...σελ 21

Σημαντικά ευρήματα……...σελ 21

Επόμενα βήματα…….σελ 23

ΚΕΦΑΛΑΙΟ 4ο

Ασφάλεια κυβερνοχώρο σε λιμενικές εγκαταστάσεις……σελ 24

Λιμενική ασφλάλεια……...σελ 25

Ανάπτυξη των λιμένων……...σελ 27

Ναυτική ασφάλεια και ασφάλεια λιμένων……..σελ 28

Οι κίνδυνοι που αντιμετοπίζουν οι λιμενικές εγκαταστάσεις…….σελ 30

Οι κρίσημες υποδομές…….σελ 32

Πλαίσιο κυβερνοασφάλειας για τις κρίσιμες υποδομές……..σελ 33

Cyber-risk στρατηγική και διαχείριση στα λιμάνια……σελ 35

Κώρικας ορθής πρακτικής για τους λιμένες και τα συστήματα λιμένων……...σελ 36

Βιβλιογραφία/Ιστοσελιδες……..σελ 38

ΠΕΡΙΛΗΨΗ

Στην παρακάτω πτυχιακή εργασία θα ασχοληθούμε και θα αναλύσουμε θέματα σχετικά με την ασφάλεια κυβερνοχώρου στον χώρο της ναυτιλιακής βιομηχανίας. Αρχικά θα κατανοήσουμε τι είναι σαν έννοια ο κυβερνοχώρος. Θα αναφέρουμε τις επιπτώσεις και τους κινδύνους που έχει μια επίθεση κυβερνοχώρου σε ένα πλοίο και στα συστήματα ναυσιπλοΐας του. Θα αναφερθούμε επίσης σε μερικές τεχνικές επιθέσεων του κυβερνοχώρου. Αναλύσουμε επίσης πόσο σημαντικό είναι να υπάρχει το κατάλληλο σύστημα ασφαλείας. Παρακάτω γράφουμε τις απόψεις των Lloyd's για το cyber attack και και το πόσο απαραίτητη είναι μια στρατηγική για το cyber security. Τέλος αναφέρουμε τις επιδράσεις που έχουν οι επιθέσεις του κυβερνοχώρου στις λιμενικές εγκαταστάσεις και πως αντιμετωπίζονται.

Abstract

In the following dissertation we will deal with and analyze issues related to cyber security in the shipping industry. Initially we will understand what is cyberspace. We will report the impact and risks of a cyber attack on a ship and its navigation systems. We will also refer to some cyber attack techniques. We also analyze how important it is to have an appropriate security system. Below we write Lloyd's views on cyber-attack and how necessary a strategy for cyber security is. Finally, we report on the effects of cyberspace attacks on port facilities and how they are dealt with.

Λέξεις κλειδιά/Key Words

Κυβερνοχώρος	ASE
Χρόνος	Adhoc
Χώρος	Cyber Attack
Ανωνυμία	Cyber Theat
Ασυμμετρία	Lloyd's
Αποτελεσματικότητα	National Institute Standards of Technology-NIST
Ransomware	Intelligent Transport System- ITS
Spear phishing	hard-port
Targeted phishing scam	soft-port
Dwelltime	Κρίσιμες υποδομές/ Υποδομές ζωτικής σημασίας.
Patch managment	Κώδικας ορθής πρακτικής

ΕΙΣΑΓΩΓΗ

Τι Είναι ο κυβερνοχώρος

Με τον όρο κυβερνοχώρος υποδηλώνεται το περιβάλλον που έχει δημιουργηθεί από δίκτυα επικοινωνιών που χρησιμοποιούν ηλεκτρονικούς υπολογιστές. «Παραδείγματα τέτοιων δικτύων αποτελούν τα τοπικά δίκτυα LANs στα οποία ορισμένοι ηλεκτρονικοί υπολογιστές είναι συνδεδεμένοι μεταξύ τους, μέσα στο ίδιο χώρο για να εξυπηρετείται η ροή των πληροφοριών, για να μοιράζεται η επεξεργασία ή για την διευκόλυνση των επικοινωνιών- και τα ευρείας εμβέλειας δίκτυα WANs όπως το σύστημα του Internet για τις ίδιες δραστηριότητες σε εθνικά και παγκόσμια δίκτυα.

Καθημερινά αναφέρονται πληθώρα επιτυχημένων διαδικτυακών επιθέσεων, όπως κακόβουλα λογισμικά, άρνηση υπηρεσιών, σπάσιμο κωδικών πρόσβασης, παραποιήσεις ιστοτόπων, κτλ. Επίσης, οι στοχευμένες εκστρατείες με σκοπό το κυβερνοέγκλημα αυξάνονται ραγδαία και καθώς αναδύονται καινούργιες τεχνολογίες, εξελίσσονται και οι επιθέσεις στον κυβερνοχώρο. Αν και συνήθως δημοσιοποιούνται οι επιθέσεις κατά ευρέως γνωστών οργανισμών, όλοι οι οργανισμοί και πρόσωπα μπορεί να αποτελέσουν στόχο επίθεσης και να δεχθούν σοβαρό πλήγμα. Μια επιτυχημένη επίθεση μπορεί να πλήξει ανεπανόρθωτα το προφίλ ενός οργανισμού ή προσώπου, να επιφέρει νομικές κυρώσεις καθώς επίσης να επιφέρει σοβαρό οικονομικό πλήγμα. Είναι σημαντικό οι οργανισμοί να συνειδητοποιήσουν την ανάγκη για προστασία από επιθέσεις στον κυβερνοχώρο και να διαθέσουν κατάλληλο προϋπολογισμό ο οποίος, ανάλογα με τις ανάγκες που εντοπίστηκαν, θα διοχετευτεί σε νέες θέσεις εργασίας, εκπαίδευση υφιστάμενου προσωπικού, αγορά εξοπλισμού και συμβουλευτικών υπηρεσιών, κλπ., γιατί δεν εγείρεται ζήτημα αν ένας οργανισμός θα αποτελέσει στόχο επίθεσης αλλά πλέον το ερώτημα που τίθεται είναι πότε θα πληγεί.

ΟΙ ΚΙΝΗΤΗΡΙΕΣ ΔΥΝΑΜΕΙΣ ΣΤΟ ΚΥΒΕΡΝΟΧΩΡΟ

Οι κινητήριες δυνάμεις του κυβερνοχώρου είναι ο **Χρόνος**, ο **Χώρος**, η **Ανωνυμία**, η **Ασυμμετρία** και η **Αποτελεσματικότητα**. Αυτοί οι παράγοντες δημιουργούν τον τύπο "**TSAAE**" που επηρεάζει την πραγματικότητα και την κατανόηση της ασφάλειας.

Εάν ένα άτομο ή ένας οργανισμός δεν κατανοήσει αυτούς τους βασικούς παράγοντες του TSAAE, θα υπάρξει μεγαλύτερη πιθανότητα αποτυχίας και απώλεια στρατηγικού πλεονεκτήματος. Ο τύπος υπογραμμίζει μια νέα προσέγγιση για την κατανόηση της ασφάλειας. Επειδή ο κυβερνοχώρος είναι ένα ευέλικτο περιβάλλον, αυτές οι κινητήριες δυνάμεις εμφανίζονται διαφορετικά στον φυσικό κόσμο.

Ο χρόνος είναι ένα ζωτικό και αναντικατάστατο κομμάτι της ανθρώπινης ζωής. Κάθε ενέργεια, η προετοιμασία και η υλοποίησή της, χρειάζονται χρόνο. Στον φυσικό κόσμο, οι φυσικές απειλές δεν συμβαίνουν γενικά αμέσως. Για παράδειγμα, χρειάζεται χρόνος να στρατευθούν στρατεύματα ή δυνάμεις για μάχη. Στον

κυβερνοχώρο, εντούτοις, οι ενέργειες μπορούν να εμφανιστούν στην αναλαμπή ενός ματιού και χωρίς προειδοποίηση, ή σε μεγαλύτερο χρονικό διάστημα. Από την άποψη του χρόνου, δεν πειράζει τίποτα εάν ένα cyber attack ξεκινάει από το διπλανό σπίτι ή από την άλλη πλευρά του κόσμου.

Ο χώρος είναι συνυφασμένος με το χρόνο σε ένα περίπλοκο επίπεδο. Στον κυβερνοχώρο, κανείς δεν είναι ασφαλής από ένα cyber attack, και οποιοσδήποτε μπορεί να ξεκινήσει ένα cyber attack στον ψηφιακό χώρο μάχης. Στη χειρότερη περίπτωση, ένα cyber attack χρειάζεται μόνο στο άτομο να πατήσει "enter" σε ένα πληκτρολόγιο. Στον κυβερνοχώρο, οποιοσδήποτε προορισμός μπορεί να επιτεθεί αμέσως. Ο κυβερνοχώρος δεν έχει καθιερωθεί και αλλάζει συνεχώς μέσω ενημερώσεων τεχνολογίας και αλλαγών δικτύων. Μακροπρόθεσμα, ο κυβερνοχώρος μπορεί να αλλάξει προς την επιθυμητή κατεύθυνση με διεθνείς συμβάσεις και οδηγίες. Η πρόκληση στον κυβερνοχώρο είναι η δυσκολία καθορισμού των επιπτώσεων ενός cyberattack και από πού ξεκίνησε.

Η βασική πρόκληση στην **ανωνυμία** είναι η ταυτοποίηση του κυβερνοχώρου και των λειτουργιών του. Η αναγνώριση αναφέρεται στην ταυτότητα των φορέων και στην ένδειξη της θέσης τους, η οποία είναι δύσκολη στον κυβερνοχώρο. Το επίπεδο βεβαιότητας της αναγνώρισης εξαρτάται από τρεις παράγοντες: το επίπεδο στόχευσης της αναγνώρισης, τη φύση των ενεργειών και τον επιδιωκόμενο στόχο ταυτοποίησης. Μερικές φορές, οι πολιτικά λειτουργημένες ομάδες διεκδικούν την ευθύνη για ένα cyber attack. Για παράδειγμα, η κυβέρνηση των Ηνωμένων Πολιτειών συμμετείχε ανεπίσημα στη δημιουργία και εφαρμογή του κακόβουλου λογισμικού Stuxnet που διέλυσε το πυρηνικό πρόγραμμα του Ιράν το 2011. Όταν παραδέχτηκε τη συμμετοχή της, η Ηνωμένες Πολιτείες έδειξε στον κόσμο ότι είχε τόσο την εξουσία όσο και τους πόρους για χρήση προηγμένων cyberweapons κατόπιν αιτήματος.

Ο όρος **ασυμμετρία** είναι αρκετά παλαιός, αλλά έγινε μέρος της δημόσιας συζήτησης μετά τις επιθέσεις της 9ης Σεπτεμβρίου, στις οποίες η Αλ Κάιντα διεξήγαγε συμμετρικό πόλεμο. Ο ασύμμετρος πόλεμος εκμεταλλεύεται το αδύναμο σημείο ενός αντιπάλου και προσπαθεί να χρησιμοποιήσει ανταγωνιστικό πλεονέκτημα με τον βέλτιστο τρόπο. Ο κυβερνοχώρος δημιουργεί νέες ευκαιρίες για ασύμμετρο πόλεμο. Κάθε κυβερνοεπιχειρησιακή λειτουργία, συμπεριλαμβανομένου του πολέμου πληροφοριών, είναι ασύμμετρη από τη φύση της. Η ασυμμετρία χαρακτηρίζει τις Cyber Threats. Περιέχει επίσης περιορισμένες δυνατότητες για τον εντοπισμό των παραγόντων του Cyber attacks και προσφέρει τη δυνατότητα χρήσης αυτών των μέσων από μη κρατικούς φορείς, οι οποίοι είναι άτομα ή οργανώσεις που έχουν σημαντική πολιτική επιρροή αλλά δεν είναι σύμμαχοι σε κάποια συγκεκριμένη χώρα ή κράτος. Η ασυμμετρία επιτρέπει στις Cyber attacks να επωφεληθούν από τις αλλαγές ταχύτερα και πιο εύκολα.

Η **αποτελεσματικότητα** ενός cyber attack δεν σημαίνει ότι το Internet συντρίβεται. Ο σκοπός του cyber attack είναι συνήθως να αποδυναμώσουν την αξιοπιστία και τον τρόπο με την οποία οι οργανώσεις και τα έθνη λειτουργούν χωρίς διακοπές. Το βασικό στοιχείο της αποτελεσματικότητας στον κυβερνοχώρο είναι ότι ο

χειριστής μπορεί να εκτελεί πολλαπλές ενέργειες ταυτόχρονα σε διαφορετικές διαστάσεις. Όσο μεγαλύτερο είναι το δίκτυο λειτουργίας που χρησιμοποιούν οι οργανώσεις και τα έθνη, τόσο περισσότερα δίκτυα και συστήματα πληροφοριών πρέπει να προστατεύονται. Όσον αφορά την αποτελεσματικότητα, οι μη κυβερνητικοί φορείς έχουν δύο τρόπους να ασκήσουν στρατηγικές επιρροές. Πρώτον, μπορούν να εμπορευματοποιήσουν τις δικές τους ικανότητες κυβερνοασφάλειας και να συνεργαστούν με εθνικούς ή άλλους μη κυβερνητικούς φορείς. Δεύτερον, μπορούν να σχηματίσουν διαφορετικές συμμαχίες, για παράδειγμα με τις εθνικές αρχές που μπορούν να τους προσφέρουν ικανότητες κυβερνοασφάλειας. Παρόλο που ο κυβερνοχώρος μπορεί να χρησιμοποιηθεί για κακόβουλες δραστηριότητες, έχει δημιουργήσει μια πλατφόρμα για νέες καινοτομίες, όπως η ψηφιοποίηση, η εικονικοποίηση και η αυτοματοποίηση. Χάρη σε αυτές τις καινοτομίες, οι οργανώσεις μπόρεσαν να ικανοποιήσουν διάφορους μεσάζοντες από τις αλυσίδες παραγωγής και υπηρεσιών τους.

Τα τελευταία χρόνια οι εγκληματίες του ηλεκτρονικού εγκλήματος, έχουν πετύχει πάνω από 500 παραβιάσεις δεδονμένων και πάνω από 150εκατομμύρια αρχεία εκτέθηκαν μόνο το 2015. Επομένως πρέπει όλοι να έχουν πλήρη επίγνωση του ηλεκτρονικού εγκλήματος και να εφαρμόζει μέτρα ασφαλείας και ανίχνευσης.Τομείς όπως λιανεμπόριο, τεχνολογία, χρηματοπιστωτικό και κυβερνητικό, αποτελούν τους κυριότερους στόχους όπου διαρκώς αυξάνονται με τον καιρό. Οι συνεχείς παραβιάσεις βρίσκονται σε άνοδοκαθώς και η τεχνική "**ransomware**"[1]σε στοχοποιημένα άτομα ή εταιρείες βρίσκετε επίσης σε άνοδο. Κανένα άτομο ή εταιρεία δεν αποτελούν εξαίρεση και οποιοσδήποτε μπορεί να γίνει στόχος. Το 75% των παραβιάσεων αποτελούν μικρές επιχειρήσεις που δεν είχαν ικανοποιητικό βαθμό ασφαλείας για να αποτρέψουν μια τέτοιου είδους επίθεση.

Συνεπώς και οι ναυτιλιακές εταιρείες αποτελούν και αυτές με την σειρά τους στόχο για τους hackers. Η ανάπτυξη της **ευρυζωνικής τεχνολογίας**[2] και η μετάβαση προς "τις μεγάλες βάσεις δεδομένων" και "των αυτοματοποιημένων πλοίων" θα μπορούσε να κάνει μια ναυτιλιακή εταιρεία πολύ ευάλωτη σε επιθέσεις από τον κυβερνοχώρο εκτός και αν παρθούν τα κατάλληλα μέτρα ασφαλείας και ανίχνευσης και υπάρχει καλύτερη συνειδητοποίηση των "ΤΠΕ" (των τεχνολογιών, πληροφοριών και επικοινωνιών). Σίγουρα υπάρχει η πιθανότητα συστήματα όπως το AIS,GNSS, ENCκαι ECDISνα εμφανίσουν δυσλειτουργίες ή να τροποποιηθούν αλλά δεν συνηθίζεται διότι ο πραγματικός σκοπός των επιθέσεων του κυβερνοχώρου αποσκοπούν στη δημιουργία οικονομικού κέρδους. Τα συστήματα πληρωμών μπορούν εύκολα να διαπεραστούν χρησιμοποιώντας την τεχνική « **Spear phishing/targeted phishing scam**»[3]με σκοπό να συνάψουν ψεύτικα συμβόλαια ή ακόμα να τροποποιήσουν τα δηλωτικά φορτίου με σκοπό να μεταφέρουν παράνομα φορτία, ναρκωτικές ουσίες, όπλα και άλλα. Η απώλεια δεδομένων από τις παραβιάσεις του διαδικτύου είναι ο σημαντικότερος κίνδυνος που μπορεί να αντιμετωπίσει ο χώρος της ναυτιλιακής βιομηχανίας .Στη συνέχεια θα δούμε κάποιους τρόπους με τους οποίους μπορούν να αποκτήσουν πρόσβαση στα δεδομένα και τρόπους όπου ο πλοιοκτήτης ή ο εφοπλιστής ώστε να μετριάσουν το ρίσκο μιας τέτοιας επίθεσης.

---

1) **Ransomware**: Είναι η τακτική που ένας ή περισσότεροι "Hackers" στοχοποιούν ένα άτομο ή εταιρεία και εκβιάζουν την δημοσίευση αρχείων ή την αποκλείουν από την πρόσβαση στα δεδομένα με αντάλλαγμα ενός χρηματικού ποσού (λύτρα).
2) **Ευρυζωνική τεχνολογία**: είναι η τεχνολογία νέας γενιάς. Το κλασικό δίκτυο τηλεφωνίας για την επικοινωνία δύο συνδρομητών χρησιμοποιεί ένα ζεύγος χαλκού για να μετατρέπει την φωνή σε ηλεκτρικά σήματα.Η ευρυζωνική τηλεφωνία μετατρέπει τα φωνητικά σήματα σε μικρά πακέτα δεδομένων και τα μεταφέρει μέσω internet (voice over broadband)
3) **Spear phishing/ targeted phishing scam:** Με την συγκεκριμένη μέθοδο στέλνετε ένα emailαπό μια έμπιστη πηγή αλλά οδηγεί τον παραλήπτη σε κακόβουλες ιστοσελίδες και προγράμματα.

ΚΕΦΑΛΑΙΟ 1ο

ΑΣΦΑΛΕΙΑ ΚΥΒΕΡΝΟΧΩΡΟΥ ΣΤΟ ΧΩΡΟ ΤΗΣ ΝΑΥΤΙΛΙΑΣ

Η ασφάλεια κυβερνοχώρου στη ναυτιλιακή βιομηχανία αποτελεί ένα μείζον θέμα, λόγο μεγάλης έλλειψης της επίγνωσης και της ευθύνης επί του θέματος, ενώ ταυτόχρονα οι τεχνολογίες των επικοινωνιών εξελίσσονται όλο και περισσότερο μαζί με το επίπεδο απειλών στο κυβερνοχώρο. Υπάρχει το ενδεχόμενο να διαρρεύσουν στοιχεία μέσα από συστήματα όπως το ECDIS, AIS, RFID και το GPS. Επομένως είναι πολύ σημαντικό να υπάρχουν τα κατάλληλα μέτρα ασφαλείας και να είναι πλήρως λειτουργικά. Επίσης πρέπει οι χειριστές των συστημάτων να μπορούν να αναγνωρίσουν κάποια πιθανή απειλή ή να είναι σε θέση να αντιμετωπίσουν μια επίθεση κυβερνοχώρου.

Οι δράστεςπου δραστηριοποιούνται με την ναυτιλιακή βιομηχανία ενδιαφέρονται ως επί το πλείστον για το οικονομικό όφελος. Στόχος τους είναι να αποκτήσουν πρόσβαση, να παραμείνουν κρυμμένοι ώστε να επιτυγχάνουν οικονομικό όφελος.Παρ'όλα αυτά, εξάγοντας ευαίσθητες πληροφορίες και πνευματικά δικαιώματα επιτρέπει τους εγκληματίες ή τους τρομοκράτες να μεταφέρουν εις βάρος της εταιρείας παράνομα και επικίνδυνα φορτία, όπλα κλπ.

Σε μια προχωρημένη απειλή, οι hackersεπενδύουν πολύ χρόνο στην εύρεση ενδεχόμενων στόχων, συλλέγουν πληροφορίες σχετικά με την δομή της επιχείρησης και άλλες σημαντικές πληροφορίες που σχετίζονται με αυτήν. Τα socialmediatων εργαζομένων της εν λόγο επιχείρησης παρακολουθούνται διαρκώς ώστε να διασπάσουν πληροφορίες σχετικά για το σύστημα της επιχείρησης, να διεισδύσουν σε forumπου χρησιμοποιούνται από τους εργαζόμενους, και να αξιολογήσουν τα ευαίσθητα σημεία των συστημάτων ασφαλείας. Μόλις γίνει αντιληπτή οποιαδήποτε αδυναμία στο σύστημα ασφαλείας, ο hacker προχωράει στη παραβίαση της περιμέτρου. Τα συστήματα ασφαλείας όπου οι περισσότερες εταιρείας υιοθετούν παραβιάζονται εύκολα από τους επιτιθέμενους.

ΠΑΡΑΒΙΑΣΗ ΠΑΡΑΜΕΤΡΟΥ

Μόλις ένας εισβολέας διεισδύσει στο σύστημα της εταιρείας, ο επιτιθέμενος χαρτογραφεί το δίκτυο με μοναδικό στόχο να αποκτήσει πρόσβαση σε υψηλότερης αξίας περιουσιακών στοιχείων και πληροφοριών, και να αποκτάει το προνόμιο του δικαιώματος της πρόσβασης ώστε να κινείτε ελεύθερος χωρίς να μπορούν να τον ανιχνεύσουν. Το μεγαλύτερο ρίσκο προέρχεται από εργαζομένους που χρησιμοποιούνΗ/Υκαι βάσεις δεδομένωνκαι αγνοούν το γεγονός ότι τα μέτρα ασφαλείας δεν εφαρμόζονται πλήρως σωστά και έχουν την λάθος πεποίθηση ότι τα συγκεκριμένα μέτρα ασφαλείας αρκούν για να προστατέψουν την περίμετρο. Οπότε οι ναυτιλιακές εταιρείες πρέπει να επενδύσουν περισσότερο στην ασφάλεια κυβερνοχώρου για να έχει την δυνατότητα να εντοπίζει πότε πραγματοποιείτε κάποια επίθεση ώστε να μειώσει το ποσοστό των παραβιάσεων και τον "χρόνο παραμονής" (**dwelltime**[4]), όπου συνήθως αυτός ο χρόνος είναι κατά μέσω όρο 205 μέρες.

Στατιστικά εισβολών:

- 50% είναι το ποσοστό των εισβολών οπού οφείλονται σε λανθασμένες ρυθμίσεις από τους διαχειριστές, αφήνουν τους προεπιλεγμένους κωδικούς ή δεν αλλάζουν συχνά κωδικούς, κλπ.
- 70%οφείλετε σε απάτες μέσω των social media και από κακόβουλα λογισμικά που δημοσιεύουν σε αυτά.
- 23% αποτελεί το ποσοστό όπου οι χρήστες ανοίγουν κακόβουλα emails (**Phishing scam/Spear Phishing**).
- 50% εξαιτίας του λάθους που κάνουν οι χρήστες να χρησιμοποιούν τους ίδιους κωδικούς πρόσβασης σε προσωπικούς λογαριασμούς και σε εταιρικούς λογαριασμούς.
- 99% των παραβιάσεων της παραμέτρου ασφαλείας του κυβερνοχώρου προέρχονται από γνωστές αδυναμίες του συστήματος.
- 25% είναι το ποσοστό των επιθέσεων που μπορούν να αποφευχθούν αν ενημερώνονται σωστά οι χρήστες για το ρίσκο μιας επίθεσης στο κυβερνοχώρο.

4) **Dwelltime:** είναι η χρονική διάρκεια όπου ο εισβολέας θα διεισδύσει την περίμετρο ασφαλείας, θα αποφύγει να ανιχνευτεί, θα αποσπάσει τις πληροφορίες που χρειάζεται και θα εξέλθει χωρίς να αφήσει κανένα ίχνος.

Η ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ένα άλλο πολύ μείζον πρόβλημα είναι η διαρκώς αυξημένη πολυπλοκότητα της διαμόρφωσης των συστημάτων και των εφαρμογών. Αυτό είναι συνήθως πιο περίπλοκο στο χώρο της ναυτιλιακής βιομηχανίας εξαιτίας της διανομής, της απομακρυσμένης πρόσβασης, λόγω περιορισμένου εύρους ζωνών καθώς επίσης και την έλλειψη εκπαίδευσης των χρηστών που χρησιμοποιούν τα συστήματα. Η ύπαρξη του " **Patch Management**[5]" είναι πολύ σημαντική διότι μπορεί να μετριάσει πάνω από το 80% των απειλών του κυβερνοχώρου όπου αυξάνονται διαρκώς.

ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΠΡΟΝΟΜΙΟΥΧΟΙ ΧΡΗΣΤΕΣ

Οι κωδικοί πρόσβασης και οι προνομιούχοι λογαριασμοί να είναι το κυριότερο μέλημα σε πολλές εταιρείες .Από αυτά εξαρτάται το αν μια παραβίαση στο κυβερνοχώρο είναι απλή ή σύνθετη. Οι εταιρείες θα έπρεπε να παρέχει την κατάλληλη εκπαίδευση στους εργαζομένους σε πρακτικές για την πιο ορθή επιλογή κωδικού πρόσβασης, συνήθως χρησιμοποιείτε κάποιος περίπλοκος κωδικός πρόσβασης. Παρ' όλα αυτά πολλοί αποφεύγουν να χρησιμοποιούν τέτοιους κωδικούς πρόσβασης λόγω της δυσκολίας απομνημόνευσης και χρησιμοποιούν τους ίδιους κωδικούς πρόσβασης με αυτούς που χρησιμοποιούν στην προσωπική τους ζωή. Αυτό οδηγεί στην πιθανότητα κάποιας εξωτερικής απειλής όπου θα οδηγήσει στην εύκολη παραβίαση της περιμέτρου και την μεγάλη απώλεια δεδομένων, και στη χρηματοοικονομική απάτη. Αν η εταιρεία δίνει στους εργαζομένους λογαριασμούς διαχειριστών ή προνομιούχους λογαριασμούς αυξάνετε δραματικά η πιθανότητα της παραβίασης του κυβερνοχώρου. Η εταιρεία θα πρέπει να πραγματοποιεί συχνούς ελέγχους στους προνομιούχους λογαριασμούς, να αφαιρέσει το δικαίωμα του διαχειριστή από όπου δεν είναι απαραίτητο και να γίνεται ταυτοποίηση από δύο παραγόντων ώστε να περιοριστεί η διακινδύνευση του λογαριασμού.

ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ (ESC)

Η ESCGLOBALSECURITYπροτείνει στις εταιρείες που δραστηριοποιούνται στο χώρο της ναυτιλιακής βιομηχανίας να τοποθετήσουν στις βασικές προτεραιότητες την εκπαίδευση και την επίγνωση της ασφάλειας του κυβερνοχώρου για τους χρήστες με την τεχνολογία και με τους Η/Υ. Η εκπαίδευση είναι ένας από τις πιο αποτελεσματικές μεθόδους για να περιοριστεί η έκθεση της εταιρείας σε απειλές του κυβερνοχώρου και δημιουργεί την δυνατότητα την ανίχνευση και την αντιμετώπιση της απειλής ταυτοχρόνως.

---

5) **Patch Management:** είναι το τμήμα που ασχολείται με την διαχείριση των αναβαθμίσεων του λογισμικού και των εφαρμογών και να επιδιορθώνει τα

υπάρχοντα προβλήματα. Αρκετές από αυτές τις αναβαθμίσεις συσχετίζονται με την ασφάλεια του κυβερνοχώρου.

Είναι ζωτικής σημασίας η εκπαίδευση του προσωπικού να ξεκινάει από την κορυφή της εταιρίας προς τα κάτω. Επίσης η ESCπροτείνει η εταιρεία να διορίζει έναν πρεσβευτή της ασφάλειας κυβερνοχώρου μέσα στα τμήματα της εταιρείας

όπου θα βοηθάει στην ανίχνευση και την αντιμετώπιση μια πιθανής απειλής που προέρχεται από τον κυβερνοχώρο. Αυτό έχει ως αποτέλεσμα την αποτελεσματική λειτουργία της ομάδας ITSecurity, καθώς επίσης διασφαλίζει ότι υπάρχει κάποιος στην εταιρεία όπου είναι υπεύθυνος για την υλοποίηση και την συντήρηση των μέτρων ασφαλείας του κυβερνοχώρου. Είναι επίσης πολύ σημαντικό να υπάρχει μια πολιτικήITSecurity και να είναι αποδεκτή από την πολιτική της **ASE**[6]και να διασφαλίζει ότι όλοι οι εργαζόμενοι της εταιρείας κατανοούν πως τα αρχεία από τις βάσεις δεδομένων πρέπει να χρησιμοποιούνται. Αυτό διασφαλίζει ότι τα πρότυπα είναι κατανοητά και τηρούνται. Αυτό το βήμα είναι σημαντικό γιατί δημιουργεί την κουλτούρα της ασφάλειας κυβερνοχώρου.

Η συνδρομή στα δελτία ασφαλείας και σε συστήματα συναγερμών είναι εξίσου σημαντικά διότι αξιολογούνται οι νέες απειλές και στη συνέχεια γίνονται ενέργειες μετριασμού των κινδύνων.

Ένα σημαντικό αλλά συνήθως υποβιβασμένο μέτρο της ασφάλειας κυβερνοχώρου είναι η διάθεση κληρονομιάς, δηλαδή να αρχειοθετούνται τα παλαιά συστήματα και οι αδυναμίες τους προκειμένου την αναβάθμιση του συστήματος. Έχοντας μια “life policy” και εφαρμόζοντας την θα βοηθήσει της εταιρείες να διατηρήσουν τα κληροδοτημένα συστήματα εκθέτοντας έτσι σοβαρές απειλές και κίνδυνους για την ασφάλεια. Αυτό θα μειώσει το περιττό κόστος και θα βελτιώσει την ασφάλεια των συστημάτων.

Με το να διορθώνετε τακτικά το σύστημα και να ελέγχεται την κατάσταση της ευπάθειας του συστήματος, θα βοηθούσε να εντοπίσει τα αδύναμα σημεία του

---

6) **ASE (Adaptive Server Enterprise):** Είναι ένα λογικό σύστημα αρχείων βάσης δεδομένων το οποίο είναι μετεξέλιξη της SQL (Structured Query language) και αναπτύχθηκε από την εταιρεία Sybase και η δουλεία του είναι να διατηρεί ασφαλείς ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης κλπ.

συστήματος και να προβλέπει σε ποιο σημείο θα μπορούσε να πραγματοποιηθεί μια μελλοντική επίθεση. Αυτές οι ενέργειες παρακινούν την εξέταση αλλά και την αύξηση των τεχνικών ανιχνεύσεως σε αυτές τις περιοχές του συστήματος. ‘

Η διεξαγωγή συνεχόμενων αξιολογήσεων-ελέγχων στον τομέα της ασφάλειας του κυβερνοχώρου αποτελεί έναν ακόμα σημαντικό παράγοντα για τον μετριασμό των κινδύνων στον κυβερνοχώρο. Παρόλο που οι αξιολογήσεις αυτές θεωρούνται συχνά ως «πλαίσιο ελέγχου» είτε παραβλέπουν είτε συμμορφώνονται με τους κανονισμούς θα πρέπει να γίνεται αυτή η αξιολόγηση στον τομέα της ασφάλειας του κυβερνοχώρου. Επίσης με αυτή την αξιολόγηση γίνεται παράλληλα η αξιολόγηση των δυνατοτήτων αντιμετώπισης περιστατικών επιθέσεων, γίνεται έλεγχος ανίχνευσης εάν βρίσκεται σε εξέλιξη μια ενεργή παραβίαση αυτή την στιγμή και διατηρεί την ασφάλεια της εταιρείας.

Μια πολύ σημαντική συμβουλή είναι τα συστήματα ασφαλείας να είναι παραπλανητικά και απρόβλεπτα. Οι περισσότεροι οργανισμοί έχουν προγραμματισμένα και αυτοματοποιημένα τα συστήματα κυβερνοχώρου. Αυτό εν μέρει βοηθάει στην πιο αποτελεσματική άμυνα του συστήματος, αλλά από την άλλη καθιστά το σύστημα προβλέψιμο. Για παράδειγμα οι σαρώσεις εκτελούνται την ίδια ώρα κάθε εβδομάδα, οι διορθώσεις και οι αναβαθμίσεις του συστήματος μια φορά τον μήνα, οι αξιολογήσεις και οι έλεγχοι μια φορά το τρίμηνο ή τον χρόνο.

Οι εταιρείες που είναι προβλέψιμες είναι περισσότερο ευάλωτες, οπότε πρέπει να δημιουργηθεί μια νοοτροπία στην οποία τα συστήματα θα ενημερώνονται και θα αξιολογούνται με την τεχνολογία “**adhoc**”[7]**.** Επομένως είναι απαραίτητο η δραστηριότητα να είναι πιο τυχαία και απρόβλεπτη. Αυτό θα αυξήσει την ικανότητα ανίχνευσης ενεργών επιθέσεων κυβερνοχώρου και παραβιάσεων στον κυβερνοχώρο.

Τέλος είναι σημαντικό να προσληφθούν εμπειρογνώμονες από εταιρείες που ασχολούνται αποκλειστικά για την ασφάλεια κυβερνοχώρου. Οι εμπειρογνώμονες σε θέματα ασφαλείας μπορούν να εκτελέσουν αξιολογήσεις κινδύνου και ευπάθειας και να παρέχουν εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια κυβερνοχώρου, να διαχειρίζονται τις ενημερώσεις του κώδικα και να τις αξιολογούν. Επίσης αναγνωρίζουν τους προνομιούχους χρήστες και μετριάζουν τον κίνδυνο όπου αυτό είναι εφικτό.

---

7) **Adhoc**: ονομάζεται η τεχνολογία που δυο συστήματα μπορούν να συνδεθούν μεταξύ τους να επικοινωνούν και να ανταλλάσουν αρχεία χωρίς την ύπαρξη ρούτερ ή κάποιο καλώδιο.

ΚΕΦΑΛΑΙΟ 2ο

ΠΕΡΙΣΤΑΤΙΚΑ ΕΠΙΘΕΣΕΩΝ ΑΠΟ ΤΟ ΚΥΒΕΡΝΟΧΩΡΟ

ΤΟ ΛΙΜΑΝΙ ΤΗΣ ΑΜΒΕΡΣΑΣ

Οι hackers που συνεργάζονταν με μια συμμορία λαθρεμπορίου ναρκωτικών, διείσδυσαν στο μηχανογραφημένο σύστημα εντοπισμού φορτίου στο λιμένα της Αμβέρσας για να εντοπίσουν τα εμπορευματοκιβώτια τα οποία μετέφεραν φαρμακευτικά υλικά. Στη συνέχεια μέλη της συμμορίας οδήγησαν το εμπορευματοκιβώτιο εκτός λιμανιού, έκλεψαν τα φάρμακα και κάλυψαν τα ίχνη τους. Η εγκληματική δράση συνεχίστηκε για 2 χρόνια από τον Ιούνιο του 2011, ως που σταμάτησε από κοινή δράση της Βέλγικης και της ολλανδικής αστυνομίας. Οι εγκληματίες του κυβερνοχώρου παρόλα αυτά θα συνεχίσουν να εκτελούν τέτοιο είδους επιθέσεων καθώς και θα εξελιχθούν με την ανάπτυξη της τεχνολογίας.

ΕΠΙΘΕΣΕΙΣ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΝΑΥΣΙΠΛΟΙΑΣ

Έχουν αναφερθεί παραβιάσεις και επιθέσεις στα συστήματα ναυσιπλοΐας της γέφυρας. Το ECDIS(Electronic Display And Information System), AIS(Automatic Identification System) και το GPS(Global Position System) είναι τα απαραίτητα βοηθήματα για την ναυσιπλοΐα και έχει παρατηρηθεί ότι όλα είναι ευάλωτα σε μια επίθεση από τον κυβερνοχώρο.

Ο IMO είναι ο οργανισμός των Ηνωμένων εθνών που ασχολείται με την ασφάλεια της ναυσιπλοΐας. Αυτός ο οργανισμός καθιέρωσε την υποχρεωτική τοποθέτηση του AISσε όλα τα επιβατικά και εμπορικά πλοία άνω των 500GTκαι πλοίων άνω των 300GTπου ασχολούνται με το διεθνής εμπόριο. Αυτός ο κανονισμός εφαρμόστηκε από το 2004. Οι κανονισμοί του IMO απαιτούν ότι το AIS θα είναι σε θέση να ανταλλάσσει αυτόματα πληροφορίες σχετικά με την ταυτότητα, τον τύπο, τη θέση, την πορεία, την ταχύτητα, την κατάσταση της ναυσιπλοΐας και άλλες σχετικές με την ασφάλεια πληροφορίες με άλλα πλοία, εγκαταστάσεις ξηράς και αεροσκάφη. Το AISέχει χρησιμοποιηθεί ως ένα εργαλείο πλοήγησης στο πλοίο, σαν εναλλακτικό του ραντάρ και αποτελεί σημαντικό εργαλείο για τον έλεγχο των πλοίων κατά την διέλευση τους από τα VTS(vessel traffic separation).

Επειδή το AIS δεν διαθέτει δικό του σύστημα κρυπτογράφησης, καθιστάτε ένας ευάλωτος στόχος για επίθεση από το κυβερνοχώρο όπως αποδείχτηκε από τις εταιρείες Cyber Securityκαι TrendMicro. Οι επιχειρήσεις είχαν δείξει ότι μέσω του AISμπορούν να εμποδίσουν το πλοίο να παρέχει σωστές πληροφορίες για τις κινήσεις του, το φορτίο του κλπ, και δημιουργούσαν ένα πλοίο φάντασμα με λανθασμένο στίγμα GPSκαι ψεύτικες επικίνδυνες καταστάσεις κάνοντας έτσι άλλους χρήστες AISνα βλέπουν αυτό το λανθασμένο σήμα κινδύνου. Επίσης οι onlineυπηρεσίες παρακολούθησης των AISγια την παρακολούθηση της θέσης των πλοίων

παραπλανήθηκαν επίσης με το ψεύτικο στίγμα. Νωρίτερα το 2013 οι ερευνητές του πανεπιστημίου του Τέξας μπόρεσαν να αποδείξουν ότι θα μπορούσαν να στείλουν ένα super yacht εκτός πορείας χρησιμοποιώντας ένα ψεύτικο στίγμα GPS. Όπως και το AIS και το GPSγια μη στρατιωτική χρήση δεν είναι κρυπτογραφημένο ούτε επικυρωμένο και επομένως αποτελεί έναν εύκολο στόχο.

Μπορεί να υποστηριχθεί ότι το σχετικά χαμηλό δημόσιο προφίλ των περισσότερων ναυτιλιακών επιχειρήσεων σημαίνει ότι είναι λιγότερο πιθανό να αποτελέσει αντικείμενο επιθέσεων στο κυβερνοχώρο σε σχέση με χρηματοπιστωτικά ιδρύματα, εταιρείες ενέργειας, επιχειρήσεις κοινής ωφέλειας ή αεροπορικές εταιρείες. Αυτό μπορεί να συμβαίνει, παρόλα αυτά η απειλή είναι πραγματική και τα αποτελέσματα μιας επιτυχημένης επίθεσης θα μπορούσε να είναι καταστροφικά. Ασφαλώς, η έλλειψη ενσωματωμένου κώδικα στα σημαντικά συστήματα που χρησιμοποιούνται για την πλοήγηση στο πλοίο σημαίνει ότι η ναυτιλία μπορεί να θεωρηθεί ως ένας "μαλακός" στόχος για μία επίθεση και αυτή η αντίληψη μόνο είναι αρκετή για να προκληθεί μία επίθεση.

Η ανασκόπηση τεχνολογίας MIT ανέφερε οι συσκευές που χρειάζονται για τον εντοπισμό κενών ασφαλείας στα συστήματα AIS και GPS κοστίζουν περίπου 700$ όπου καθιστά το γεγονός να είναι σε θέση και ένας ενθουσιώδης έφηβος με τις απαραίτητες δεξιότητες να επιτεθεί. Στο άλλο άκρο της κλίμακας, δεν είναι δύσκολο να φανταστούμε τις συνέπειες ενός εθνικού κράτους που επιδίδεται στο κυβερνο-πόλεμο στοχεύοντας στο λογισμικό παρακολούθησης εμπορευματοκιβωτίων που χρησιμοποιούν τα λιμάνια του αντιληπτού εχθρού σε μια προσπάθεια να διαταράξει το εμπόριο.

Φυσικά, ορισμένες επιχειρήσεις στο τομέα της ναυτιλίας έχουν πολύ μεγάλη προβολή. Μια επίθεση στο κυβερνοχώρο ενός κρουαζιερόπλοιου που θα διέκοπτε την ναυσιπλοΐα του θα είχε ως αποτέλεσμα την τεράστια κάλυψη του γεγονότος από τα Μέσα μαζικής ενημέρωσης και στις χειρότερες περιπτώσεις θα μπορούσαν να είχαν χαθεί πολλές ζωές και να είχαν προκλήθεί σημαντικές ζημιές σε περιουσιακά στοιχεία.

Ο Διεθνής Ναυτιλιακός Οργανισμός αναγνώρισε ήδη από το 2004 ότι η δημοσίευση δεδομένων που προέρχονται από το AIS στο Διαδίκτυο και αλλού θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων .Εν συνεχεία, καταδίκασε όσους δημοσίευσαν τα δεδομένα αυτά και ενθάρρυνε τις εθνικές κυβερνήσεις να αποθαρρύνουν τη δημοσίευσή τους. Ωστόσο, στην ανασκόπηση τεχνολογίας MIT αναφέρθηκε ότι όταν η TrendMicro έθεσε τις ανησυχίες της στον IMO μετά την εικονική επίθεση της στο AISτο 2013, ο IMO απάντησε ότι θα μπορούσε να απαντήσει μόνο σε έγγραφο που υπέβαλε μέλος της διοίκησης του IMO ή από οργανισμό με συμβουλευτική ιδιότητα. Όταν ερωτήθηκε άμεσα τον Ιούνιο του 2014, ο IMOεπιβεβαίωσε ότι το cyberthreat δεν είχε υποβληθεί προς συζήτηση από κανένα μέλος και κατά συνέπεια δεν ήταν στο πρόγραμμα εργασίας του αυτή την στιγμή.

Εν πάση περιπτώσει, η επικαιροποίηση του υφιστάμενου πρωτοκόλλου και των κανονισμών για την αντιμετώπιση της τρέχουσας απειλής θα απαιτούσε αρκετό χρόνο, ενώ η αντικατάσταση του εξοπλισμού επί του παγκόσμιου στόλου με επαρκώς ασφαλή νέα συστήματα θα χρειαζόταν πολύ μεγαλύτερο χρονικό διάστημα. Εν τω μεταξύ, η πιθανή απειλή παραμένει και αναμφίβολα αυξάνεται.

Η λογική απάντηση σε μια απειλή είναι να εξετάσει την πιθανότητα ενός γεγονότος που θα μπορούσε να προκαλέσει μια απώλεια που συμβαίνει τόσο έναντι των αναμενόμενων όσο και των μέγιστων αρνητικών αποτελεσμάτων εάν επέλθει το συμβάν. Μόλις γίνει κατανοητή η πιθανότητα και οι πιθανές συνέπειες, μπορούν να ληφθούν τεκμηριωμένες αποφάσεις σχετικά με τον μετριασμό του κινδύνου. Ωστόσο, αυτή η συμβατική προσέγγιση της διαχείρισης κινδύνου δεν ισχύει για την απειλή του κυβερνοχώρου όπως περιγράφεται παραπάνω εξαιτίας συγκεκριμένου αποκλεισμού στα ασφαλιστήρια συμβόλαια.

ΟΙ ΑΝΤΙΔΡΑΣΕΙΣ ΤΩΝ ΑΣΦΑΛΙΣΤΩΝ ΓΙΑ ΤΙΣ ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ο κίνδυνος μιας επιδρομής στον κυβερνοχώρο υπήρξε για όσο διάστημα υπήρχαν υπολογιστές, αλλά αυξήθηκε εκθετικά στα τέλη του 20ου αιώνα με την άφιξη του Διαδικτύου και την ευρεία χρήση κλειστών δικτύων υπολογιστών ως βασικό επιχειρηματικό εργαλείο. Οι ασφαλιστές αναγνώρισαν ότι η απειλή υπήρχε, αλλά δεν την κατάλαβαν. Αυτό σήμαινε ότι δεν ήταν σε θέση να μετρήσουν την πιθανότητα μιας απώλειας η οποία, με τη σειρά της, σήμαινε ότι δεν μπόρεσαν να βάλουν τίμημα στην έκθεση. Κατά συνέπεια, οι ασφαλιστές (και οι αντασφαλιστές τους) άρχισαν να εξαιρούν ζημίες ως αποτέλεσμα μιας επίθεσης στον κυβερνοχώρο από τις πολιτικές τους.

Στον κόσμο της θαλάσσιας ασφάλισης, τα ασφαλιστήρια συμβόλαια που καλύπτουν τα πλοία, τα ναυπηγεία και τις εγκαταστάσεις διαχείρισης φορτίων έχουν συμπεριλάβει τα τελευταία 10 χρόνια την ρήτρα περί αποκλεισμού από την υπηρεσία Cyber Attack (CL 380) της 10/11/2003 ή μια παραλλαγή αυτής που έχει το ίδιο αποτέλεσμα. Το CL 380 είναι μια "ρήτρα ύψιστης σημασίας", που σημαίνει ότι αυτή τη στιγμή θα πρέπει να συμπεριληφθεί σε όλες τις ασφαλιστικές συμβάσεις θαλάσσιων μεταφορών.

Η ρήτρα ορίζει:

1.1 Σε καμία περίπτωση η ασφαλιστική κάλυψη δεν θα καλύπτει τα έξοδα των ζημιών που προκαλούνται από έμμεση ή άμεση χρήση ή λειτουργία Ηλεκτρονικών υπολογιστών

1.2 Σε περίπτωση πολέμου, εμφύλιου πολέμου, επανάστασης, εξέγερσης ή τρομοκρατικής επίθεσης η ρήτρα 1.1 δεν εφαρμόζεται και η ασφαλιστική εταιρεία υποχρεώνεται να καλύπτει τα έξοδα των ζημιών.

Στην πράξη η κάλυψη των απωλειών και ζημιών που προκληθήκαν από μια επίθεση κυβερνοχώρου θα έπρεπε να καλύπτετε από τους ασφαλιστές. Ωστόσο εάν η απώλεια ή η ζημία προκλήθηκε από την έμμεση ή άμεση χρήσης υπολογιστών και των σχετικών συστημάτων τότε την ευθύνη κάλυψης δεν την έχουν οι ασφαλιστές.

Όπως συχνά η κάλυψη προστασίας και αποζημίωσης (protection and indemnity P&I) είναι μια εξαίρεση. Τα σωματεία P&Ιπου είναι μέλη του διεθνής ομίλου P&Iισχυρίζονται ότι δεν είναι υποχρεωμένοι να καλύψουν τα έξοδα μια επίθεσης κυβερνοχώρου εκτός και αν η επίθεση είναι μια πράξη πολέμου ή τρομοκρατίας. Υπό αυτόν τον όρο οι ασφαλιστές δεν καλύπτουν ζημιές που προκλήθηκαν με την άμεση ή έμμεση χρήση ηλεκτρονικών υπολογιστών.

Εκτός από την περιορισμένη κάλυψη που παρέχεται από τη μονάδα συγκέντρωσης των συλλόγων P & I, ο αποκλεισμός "τύπου CL 380" των ζημιών που απορρέουν από επιθέσεις στον κυβερνοχώρο εφαρμόζεται παγκοσμίως από τον κλάδο της ναυτικής ασφάλισης στην κάλυψη των σκαφών και των ακτοπλοϊκών εγκαταστάσεων.

ΚΛΕΙΣΙΜΟ ΤΟΥ ΚΕΝΟΥ ΚΑΛΥΨΗΣ

Από την άποψη του αγοραστή του ασφαλιστικού συστήματος, η ιδανική λύση θα ήταν να καταργηθεί οποιαδήποτε ρήτρα αποκλεισμού από το cyberattack από όλα τα εφαρμοστέα ασφαλιστήρια συμβόλαια. Αυτό δεν θα συμβεί, τουλάχιστον βραχυπρόθεσμα, επειδή οι ίδιοι οι ασφαλιστές βασίζονται σε προγράμματα αντασφάλισης για προστασία και αυτά τα προγράμματα αντασφάλισης περιλαμβάνουν επίσης το CL 380 ή ισοδύναμη διάταξη περί αποκλεισμού.

Μέχρι πρόσφατα, το γεγονός αυτό άφησε τις επιχειρήσεις με μια σαφώς καθορισμένη έκθεση κινδύνου που δεν μπορούσαν να αποφύγουν ούτε να μεταφέρουν. Ο ασφαλιστικός κλάδος μπορεί να είναι δημιουργικός ως απάντηση στις εξελισσόμενες εκθέσεις κινδύνου και τώρα υπάρχει ένας μικρός αριθμός σημαντικών ασφαλιστών που είναι έτοιμοι να εξετάσουν το ενδεχόμενο να προσφέρουν σημαντική αναδοχή για την κάλυψη των κινδύνων που αποκλείονται λόγω ρήτρας αποκλεισμού από κυβερνοχώρο.

ΣΥΜΠΕΡΑΣΜΑ

Τα μηχανογραφημένα συστήματα που χρησιμοποιούν και βασίζονται οι ναυτιλιακές εταιρίες για να ανταποκριθούν στις απαιτήσεις του 20^{ου} αιώνα δεν είναι κατάλληλα για να ανταποκριθούν στις απειλές επιθέσεων του 21^{ου} αιώνα. Οι ευπάθειες που υπάρχουν σε αυτά τα ευαίσθητα συστήματα αποτελούν μια ανοιχτή πόρτα και είναι θέμα χρόνου να την διαβούν οι κακόβουλοι που σχεδιάζουν να επιτεθούν.

Η ρήτρα αποκλεισμού του Ινστιτούτου Cyber Attack (CL 380) 10/11/2003 ή μια παραλλαγή αυτής της ρήτρας εμφανίστηκε στις θαλάσσιες πολιτικές τα τελευταία 15 χρόνια, εξαιρουμένης οποιασδήποτε απώλειας, ζημίας ή ευθύνης που προκλήθηκε είτε άμεσα είτε έμμεσα από τη χρήση ενός ηλεκτρονικού υπολογιστή και των σχετικών συστημάτων και λογισμικού του "ως μέσο πρόκλησης βλάβης". Παρόλο που φαίνεται να μην υπάρχει καμία πρόταση από τη βιομηχανία ότι αυτή η ρήτρα θα αποσυρθεί σύντομα, υπάρχει τώρα ένας μικρός αριθμός σημαντικών ασφαλιστών που είναι προετοιμασμένοι να εξετάσουν το ενδεχόμενο να προσφέρει σημαντική ικανότητα αναδοχής για την κάλυψη των κινδύνων που έχουν αποκλειστεί από το 2003.

ΚΕΦΑΛΑΙΟ 3ο

Lloyd’s Cyber Attack

Το επίκεντρο αυτής της ενότητας είναι οι ασφαλιστικές ζημίες που προέρχονται από κακόβουλες ηλεκτρονικές ενέργειες, που αναφέρονται ως "επιθέσεις στον κυβερνοχώρο". Η κακόβουλη ενέργεια είναι η άμεση αιτία της απώλειας, αν και οι συνέπειες ενδέχεται να περιλαμβάνουν υλικές ζημιές, τραυματισμούς, οικονομικές απώλειες ή άλλες ζημίες.

Οι επιθέσεις στον κυβερνοχώρο αυξάνονται με συχνότητα ανά τον κόσμο, οι αναφερόμενες επιθέσεις αυξήθηκαν κατά 48% το 2013 σε 42,8 εκατομμύρια το 2014, ισοδύναμα με 117,339 επιθέσεις ημερησίως. Ο σύνθετος ετήσιος ρυθμός αύξησης των ανιχνευμένων περιστατικών ασφάλειας αυξήθηκε κατά 66% ετησίως από το 2009.

Όχι μόνο έχει αυξηθεί η συχνότητα των επιθέσεων, αλλά και το κόστος διαχείρισης και μετριασμού των παραβιάσεων. Οι εκτιμώμενες μέσες οικονομικές απώλειες από περιστατικά επιθέσεων στον κυβερνοχώρο σε όλο τον κόσμο το 2014 ήταν 2,7 εκατομμύρια δολάρια, αυξημένο κατά 34% σε σχέση με το 2013.

Επί του παρόντος, πάνω από το 80% των εισοδημάτων από ασφαλιστικά ταμεία της Lloyd's προέρχεται από τις ΗΠΑ, με 6% από το Ηνωμένο Βασίλειο, 1% από την υπόλοιπη Δυτική Ευρώπη και τα υπόλοιπα από τον υπόλοιπο κόσμο.

Η οδηγία της ΕΕ για την ασφάλεια των πληροφοριών σχετικά με τα δίκτυα και ο γενικός κανονισμός για την προστασία των δεδομένων, οι οποίες και οι δύο συμφωνήθηκαν το 2015 και, στην περίπτωση της τελευταίας, θα εισαγάγουν υποχρεωτική κοινοποίηση συμβάντων και πρόστιμα για τις πιο σοβαρές παραβιάσεις των νέων κανόνων. Αυτά είναι πιθανό να αυξήσουν περαιτέρω την ευαισθητοποίηση του Διοικητικού Συμβουλίου σχετικά με τους κινδύνους στον κυβερνοχώρο και, συνεπώς, να οδηγήσουν τη ζήτηση για ασφάλιση του κυβερνοχώρου από ευρωπαϊκές επιχειρήσεις.

Σε παγκόσμιο επίπεδο, ορισμένοι αναλυτές εκτιμούν ότι η παγκόσμια αγορά ασφάλισης στον κυβερνοχώρο θα μπορούσε να ανέλθει σε 18 δισεκατομμύρια δολάρια μέχρι το 2025 από 2,5 δισεκατομμύρια δολάρια που είναι σήμερα.

Ο ΛΟΓΟΣ ΠΟΥ ΕΙΝΑΙ ΑΠΑΡΑΙΤΗΤΗ ΜΙΑ ΣΤΡΑΤΗΓΙΚΗ ΕΝΑΝΤΙΑ ΣΤΟ CYBERATTACK

Η εμφάνιση μιας νέας κοινωνικής απειλής με τη μορφή επιθέσεων στον κυβερνοχώρο δημιουργεί την επείγουσα ανάγκη για κατάλληλους μηχανισμούς μετριασμού των κινδύνων και μεταφοράς κινδύνου.

Η αγορά της Lloyd's είναι σε θέση να προσφέρει λύσεις risktransfer, αξιοποιώντας την αποδεδειγμένη ικανότητά της να καινοτομεί ανταποκρινόμενη στο μεταβαλλόμενο επιχειρηματικό περιβάλλον. Ωστόσο, είναι επίσης αναγκαίο να εξεταστούν οι κίνδυνοι. Η Lloyd's πρέπει να εξισορροπήσει την ανάγκη για ταχεία καινοτομία με την ανάγκη κατάλληλης εποπτείας και ελέγχου.

Υπάρχουν δύο κύριες προκλήσεις. Πρώτον, ο Lloyd's πρέπει να διασφαλίσει ότι η ασφάλεια επιθέσεων στον κυβερνοχώρο δεν παραδίδεται ακούσια «ελεύθερη» ως μέρος των τυποποιημένων διατυπώσεων πολιτικής. Αυτό δεν είναι για να αποθαρρύνεται η συμπερίληψη της κάλυψης από κυβερνο-επιθέσεις, μόνο για να διασφαλιστεί ότι ο κίνδυνος είναι σαφώς προσδιορισμένος και κατανοητός και ότι το δυνητικό κόστος αντικατοπτρίζεται στο ασφάλιστρο. Μόνο με κατάλληλη τιμολόγηση του κινδύνου μπορούν οι ασφαλιστές να προσφέρουν έναν βιώσιμο μηχανισμό μεταφοράς κινδύνου για επιθέσεις στον κυβερνοχώρο.

Δεύτερον, ο Lloyd's και ο ασφαλιστικός τομέας γενικά πρέπει να κατανοήσουν το ενδεχόμενο μεγάλης συσσώρευσης κινδύνου για επιθέσεις στον κυβερνοχώρο. Με απλά λόγια, ποιο είναι το χειρότερο που μπορεί να συμβεί;

Ο Lloyd's πρωτοπορεί στην έρευνα και των δύο προκλήσεων.

Το υπόλοιπο του κεφαλαίου επικεντρώνεται στα βήματα που λαμβάνει η Lloyd's για τη διαχείριση της δεύτερης πρόκλησης: πολύ μεγάλες συσσωρεύσεις έκθεσης (επαν)ασφάλισης σε κίνδυνο επιθέσεων στον κυβερνοχώρο.

Στο πλαίσιο της στρατηγικής Cyber-Attack, ο Lloyd's στοχεύει στην ανάπτυξη ορθών πρακτικών για την αγορά Lloyd's για την κατανόηση του καταστροφικού κινδύνου και στην ανταλλαγή γνώσεων που μπορεί να βοηθήσει στη διαμόρφωση του μελλοντικού επιχειρηματικού σχεδιασμού και της δημόσιας πολιτικής ευρύτερα.

Η αγορά του Lloyd's ασφαλίζει επί του παρόντος τον κίνδυνο επιθέσεων στον κυβερνοχώρο με δύο βασικούς τρόπους:

- Ειδικά ασφαλιστήρια συμβόλαια στον κυβερνοχώρο, που καλύπτουν κινδύνους όπως παραβίαση δεδομένων, απώλεια δεδομένων και εκβιασμούς στον κυβερνοχώρο
- Παραδοσιακές πολιτικές (π.χ. Ακίνητα, Ναυτιλία, Ατύχημα) όπου η επιθέσεις στον κυβερνοχώρο μπορεί να προκαλέσουν απώλειες.

Καταστροφικές απώλειες από επιθέσεις στον κυβερνοχώρο μπορούν να προέλθουν από οποιαδήποτε γραμμή επιχειρήσεων, μεταξύ άλλων και από πολιτικές που δεν ορίζουν εάν η επιδρομή στον κυβερνοχώρο καλύπτεται ή όχι (γνωστή ως "σιωπηλός κυβερνοχώρος").

Το πρώτο στάδιο της Στρατηγικής Lloyd's Cyber-Attack περιελάμβανε ζητώντας από τα συνδικάτα να παράσχουν λεπτομέρειες σχετικά με τα πλαίσια διαχείρισης κινδύνων που εφαρμόζουν για της επιθέσεις στον κυβερνοχώρο και τους παράγοντες που λαμβάνουν υπόψη κατά την αναδοχή και την τιμολόγηση αυτής της επιχείρησης.

Το δεύτερο βήμα αφορούσε συνδικάτα που ανέπτυσσαν και αναφέρουν τα δικά τους εσωτερικά "σενάρια επιθέσεων στον κυβερνοχώρο" ως μέσο αντιμετώπισης της χειρότερης συσσώρευσης κινδύνου. Τα σενάρια χρησιμοποιούνται ευρέως για την εκτίμηση καταστροφικών (επαν)ασφαλιστικών ζημιών κάθε είδους. Αυτές οι τεχνικές είναι ευρέως εφαρμόσιμες στην επιθέσεις στον κυβερνοχώρο.

Για να ενθαρρύνει μια πληθώρα απόψεων και προσεγγίσεων, ο Lloyd's παρείχε ελάχιστη καθοδήγηση για την ανάπτυξη σεναρίων - εναπόκειται στα ίδια τα συνδικάτα να καθορίσουν τι έκαναν πώς και γιατί.

Η απαίτηση ήταν τα συνδικάτα να δημιουργήσουν τουλάχιστον τρία εσωτερικά αληθοφανή αλλά ακραία σενάρια επιθέσεων στο κυβερνοχώρο ως δοκιμές καταπόνησης για καταστροφικές απώλειες στον κυβερνοχώρο και να υπολογίσουν τη συνολική έκθεση σε κάθε σενάριο σε όλες τις κατηγορίες επιχειρήσεων, συμπεριλαμβανομένου του σιωπηλού κυβερνοχώρου.

Για τον πρώτο κύκλο υποβολής εκθέσεων, τα συνδικάτα είχαν την επιλογή να συμπεριλάβουν εκτιμήσεις ζημιών για τα σενάρια καθώς και συνολική ακαθάριστη συνολική έκθεση. Στο μέλλον, αυτό θα είναι υποχρεωτικό μέρος των επιστροφών τους στο Lloyd's.

Από αυτές τις πληροφορίες, ο Lloyd's έχει καθορίσει:

- Πόσο προετοιμασμένοι είναι οι χρήστες για την αποδοχή του κινδύνου των επιθέσεων στον κυβερνοχώρο σε όλες τις κατηγορίες επιχειρήσεων
- Ποιες κατηγορίες επιχειρήσεων θεωρείται ότι κινδυνεύει περισσότερο από επιθέσεις στον κυβερνοχώρο
- πώς τα συνδικάτα δημιουργούν και χρησιμοποιούν σενάρια για την αξιολόγηση της συνολικής έκθεσης στον κυβερνοχώρο.

Lloyd’sCyber-AttackStrategy

Από τις 31 Δεκεμβρίου του 2017 ο Lloyd’s διαθέτει:

- Υποστήριξε τη συνεχιζόμενη εξέλιξη των (επαν) ασφαλιστικών προϊόντων στον τομέα της επιβολής κυρώσεων εντός της αγοράς της Lloyd's, με την κατάλληλη ανάληψη και κεφαλαιοποίηση.
- ενθάρρυνε την ανάπτυξη και χρήση κατάλληλων εξαιρέσεων ή / και υπο-περιθωρίων για επιθέσεις στον κυβερνοχώρο, ίσως με την εξαίρεση σε περίπτωση πολέμου ή τρομοκρατίας.
- Ανάπτυξη δομημένης κατανόησης του κινδύνου συσσώρευσης στον κυβερνοχώρο, συμπεριλαμβανομένων μετρήσεων για τη μέτρηση του δυναμικού απώλειας, συμπεριλαμβανομένου του σιωπηλού κυβερνοχώρου.
- Ορθή πρακτική για την εκπροσώπηση των κινδύνων για επιθέσεις στον κυβερνοχώρο, συμπεριλαμβανομένου τους κινδύνους καταστροφής σε κεφαλαιουχικά μοντέλα των συνδικάτων και του εσωτερικού μοντέλου Lloyd's.
- Αναπτύχθηκε ο Lloyd's με τεχνογνωσία στον κυβερνοχώρο με υφιστάμενους ασφαλιζόμενους, νέους πελάτες, κυβερνητικούς οργανισμούς και ρυθμιστικούς φορείς.
- Μείωσε τις δυνατότητες για την ανάπτυξη σιωπηρής συσσώρευσης επιθέσεων στον κυβερνοχώρο με:
  - Προσδιορισμός κατηγοριών επιχειρήσεων και τύπων πολιτικής που υπόκεινται ιδιαίτερα στην υπολειπόμενη σιωπηρή διαρροή στον κυβερνοχώρο.
  - Ανάπτυξη προσεγγίσεων για την τιμολόγηση και τον καθορισμό κεφαλαίου για σιωπηλό κίνδυνο επιθέσεων στον κυβερνοχώρο.

ΣΗΜΑΝΤΙΚΑ ΕΥΡΗΜΑΤΑ

Τα σενάρια των συνδικάτων για επιθέσεις στον κυβερνοχώρο έδειξαν ότι η αγορά Lloyd's φέρνει μια μεγάλη ποικιλία τεχνικών για να αντιμετωπίσει το πρόβλημα της συστηματικής εξέτασης του κινδύνου καταστροφής.

Από τη συνολική αναφερόμενη έκθεση, για όλα τα συνδυασμένα σενάρια, οι επιχειρήσεις που ταξινομούνται ως Ατυχήματα συνεισέφεραν 53% και όσες ταξινομούνται ως Ακίνητα συνεισέφεραν 21%.

Σενάρια που περιλαμβάνουν τους τύπους συμβάντων που εξετάστηκαν:

- Διακοπή των online υπηρεσιών.

- Διαδεδομένη διακοπή ρεύματος.
- Επιχειρηματική διακοπή μετά από υλικές ζημιές.
- Θαλάσσια σύγκρουση.
- Βλάβη στην υποδομή υγειονομικής περίθαλψης
- Συγκρούσεις αεροπορικών μεταφορών.
- Διαρροή ιδιωτικών πληροφοριών.
- Παραβίαση της ασφάλειας του διακομιστή.
- Ζημιές σε βιομηχανικές εγκαταστάσεις.
- Διαδεδομένες επιθέσεις άρνησης εξυπηρέτησης.

Όλες οι τάξεις του Lloyd's αναφέρθηκαν σε κάποιο βαθμό στα σενάρια που υποβλήθηκαν.

Ένα παράδειγμα ενός σεναρίου πολλαπλών τάξεων έχει ως εξής:

Οι τρομοκράτες στοχεύουν να ξεκινήσουν επιθέσεις στον κυβερνοχώρο ενάντια στα βιομηχανικά συστήματα που χρησιμοποιούνται σε μια μεγάλη βιομηχανική εγκατάσταση στις ΗΠΑ, όπου στεγάζονται πολλές επιχειρήσεις, εργαζόμενοι και υλικά περιουσιακά στοιχεία. Αμέσως, οι έλεγχοι παρακολούθησης θερμοκρασίας της εγκατάστασης αποτυγχάνουν και η εγκατάσταση συνεχίζει να λειτουργεί σε λανθασμένες θερμοκρασίες. Μια έκρηξη βλάπτει σοβαρά το εργοστάσιο, προκαλώντας πυρκαγιά. Οι εργαζόμενοι, οι πρώτοι ανταποκρινόμενοι και οι πολίτες τραυματίζονται στην πυρκαγιά και οι βλαβερές χημικές ουσίες απελευθερώνονται στην ατμόσφαιρα.

Από τα σενάρια στον κυβερνοχώρο που υπέβαλαν τα συνδικάτα, ο Lloyd's κατάφερε να εντοπίσει κοινά θέματα. Συγκεκριμένα, η ανάλυση έδειξε ότι λαμβάνονται υπόψη τρεις βασικές εκτιμήσεις όταν τα συνδικάτα σχεδιάζουν σενάρια:

1. Ποιο είναι το κίνητρο για την επίθεση;
2. Ποιοι τομείς της κοινωνίας στοχεύονται;
3. Ποιος διεξάγει την επίθεση;

Είναι σαφές ότι η αγορά του Lloyd αναπτύσσει μια ισχυρή κατανόηση των κινδύνων των καταστροφών που προκαλούν οι επιθέσεις που στοχεύουν στην υποδομή του κυβερνοχώρου για οικονομικό όφελος - με άλλα λόγια, επιθέσεις σε δεδομένα (πχ πειρατεία, άρνηση υπηρεσίας, παραβίαση δεδομένων, κλοπή προσωπικών πληροφοριών). Αυτοί οι τύποι ζημιών είναι - τουλάχιστον θεωρητικά - ικανοί να ποσοτικοποιηθούν και να ελεγχθούν με κατάλληλη διαχείριση. Δεν είναι συμπτωματικά, είναι επίσης οι κίνδυνοι που καλύπτονται πρωτίστως από τα υφιστάμενα κυβερνητικά ασφαλιστήρια συμβόλαια που παρέχονται στην αγορά Lloyd's.

Αντίθετα, είναι πολύ πιο δύσκολο να προσδιοριστεί ποσοτικά η έκθεση σε επιθέσεις στον κυβερνοχώρο που ξεκίνησαν με ευρύτερους πολιτικούς ή κοινωνικούς στόχους ή κατά της εθνικής υποδομής φυσικών ή κυβερνοχώρων. Και πάλι, δεν είναι

συμπτωματικά, υπάρχουν λιγότερα συγκεκριμένα προϊόντα και μεγαλύτερες περιπτώσεις σιωπηρής έκθεσης στον κυβερνοχώρο. Αυτό έχει τη δυνατότητα να εκθέσει τα συνδικάτα σε μεγαλύτερο κίνδυνο από απροσδόκητες συσσωρεύσεις.

Υπό το φως αυτών των ευρημάτων, ο Lloyd's έχει καθορίσει τα επόμενα βήματα της στρατηγικής Cyber-Attack, ώστε να κατανοήσει με μεγαλύτερη λεπτομέρεια την έκθεση των συνδικάτων στη συσσώρευση και τους παράγοντες που λαμβάνουν υπόψη κατά την εκτίμηση των πιθανών καταστροφικών ζημιών.

ΕΠΟΜΕΝΑ ΒΗΜΑΤΑ

Κατανόηση και τιμολόγηση του κυβερνο-επιθετικού κινδύνου:

Η Lloyd's θα συνεχίσει να διαβουλεύεται με την αγορά και την Lloyd's Market Association για να καθορίσει το βαθμό στον οποίο οι υπάρχουσες εξαιρέσεις για πράξεις πολέμου και τρομοκρατίας μπορεί να καλύπτουν επιθέσεις στον κυβερνοχώρο.

Εποπτεία και ρύθμιση της αγοράς:

Η ομάδα διαχείρισης έκθεσης του Lloyd's επανεξετάζει τακτικά τις επιδόσεις των συνδικάτων με βάση τα ελάχιστα πρότυπα αναδοχής. Αυτά θα περιλαμβάνουν πλέον συγκεκριμένες αναθεωρήσεις των πλαισίων διαχείρισης των κινδύνων στον κυβερνοχώρο των συνδικάτων.

Ανεξάρτητοι αναθεωρητές έχουν κληθεί να επικεντρωθούν στην κάλυψη των κυβερνο-επιθέσεων που παρέχονται στο επίπεδο των περιπτώσεων και να εξετάσουν πώς αυτό ταιριάζει στα πλαίσια διαχείρισης των κινδύνων του συνδικαλιστικού κινήτρου

Ο Lloyd's θα συνεργαστεί με την ρυθμιστική αρχή - την PRA - για να διασφαλίσει ότι η ανταπόκρισή του στο έργο του Lloyd's cyber θεωρείται και είναι αναλογική.

Αναφορά: Στο πλαίσιο της αναφοράς του 2ου τριμήνου στις 30 Ιουνίου, η Lloyd's θα ζητήσει από τα συνδικάτα να χωρίσουν το εσωτερικό τους σενάριο σχετικά με το cyberattack για τις κατηγορίες ατυχημάτων μεταξύ κυβερνητικών πολιτικών (CY / CZ κωδικοί κινδύνου) και άλλων ατυχημάτων

Ο Lloyd's δημοσίευσε οκτώ έως δέκα νέα σενάρια για το cyberattack τον Σεπτέμβριο του 2016:

Μετά την επανεξέταση των σεναρίων για τα cyberattack των συνδικάτων, η Lloyd's συμβουλεύει τους συμμετέχοντες στην αγορά και συνεργάζεται με άλλους εμπειρογνώμονες, συμπεριλαμβανομένης της εταιρίας μοντελοποίησης Cyence και συναδέλφων που εργάζονται για την πρωτοβουλία CYRIM στη Σιγκαπούρη.

Το έργο αυτό έχει σχεδιαστεί για να βοηθήσει τον Lloyd's να αναπτύξει μια σειρά από σενάρια για της επιθέσεις στον κυβερνοχώρο, τα οποία επικεντρώνονται σε μία από τις 10 κύριες κατηγορίες επιχειρηματικών δραστηριοτήτων της Lloyd's.

Αυτά τα σενάρια πρέπει να επιτρέπουν για πρώτη φορά τη δυνατότητα να αποκτήσουν μια συνολική εικόνα του κινδύνου συσσώρευσης - συμπεριλαμβανομένου του σιωπηλού κυβερνοχώρου - στην αγορά, με τρόπο που να σχετίζεται με τις ευρείες κατηγορίες των επιχειρήσεων που καλύπτονται από την αγορά του Lloyd's.

Αυτά τα σενάρια επιθέσεων στον κυβερνοχώρο δεν θα θεωρηθούν Ρεαλιστικά σενάρια καταστροφών ή θα χρησιμοποιηθούν επισήμως για σκοπούς επιχειρηματικού σχεδιασμού ή / και καθορισμού κεφαλαίων σε αυτό το στάδιο. Συγκεκριμένα, τα σενάρια δεν θα αποτελέσουν με κανέναν τρόπο την επίσημη, τελική, θεωρημένη άποψη της εταιρείας για τον κίνδυνο επιθέσεων στον κυβερνοχώρο.

Ωστόσο, τα σενάρια θα είναι ένα επόμενο σημαντικό βήμα, και η Lloyd's μπορεί να τα αναπτύξει περαιτέρω σε συνεννόηση με την αγορά και το εξελισσόμενο δίκτυο συναδέλφων εμπειρογνωμόνων σε όλο τον κόσμο (συμπεριλαμβανομένων των κυβερνητικών υπηρεσιών).

ΚΕΦΑΛΑΙΟ 4ο

ΑΣΦΑΛΕΙΑ ΚΥΒΕΡΝΟΧΩΡΟΥ ΣΕ ΛΙΜΕΝΙΚΕΣ ΕΓΚΑΤΑΣΤΚΑΣΕΙΣ

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) των Ηνωμένων Πολιτειών έχει εντοπίσει ότι η εθνική και οικονομική ασφάλεια εξαρτάται από την αξιοπιστία και τη λειτουργικότητα των υποδομών ζωτικής σημασίας (NIST 2014). Επίσης, η Ευρωπαϊκή Ένωση (ΕΕ) υπογράμμισε τη σημασία του τομέα των υποδομών ζωτικής σημασίας για τα κράτη μέλη της και την οικονομική τους ασφάλεια. Οι τομείς κρίσιμης υποδομής περιλαμβάνουν βιομηχανίες όπως τα δίκτυα μεταφορών, ενέργειας και τηλεπικοινωνιών. Οι αρνητικές επιπτώσεις από τις φυσικές καταστροφές, την τρομοκρατία, την εγκληματική δραστηριότητα ή την κακόβουλη συμπεριφορά στον τομέα των υποδομών ζωτικής σημασίας επηρεάζουν την ασφάλεια των κρατών μελών της ΕΕ και των πολιτών της. (Ευρωπαϊκή Επιτροπή 2017.) Μια υποδομή, που θεωρείται η ραχοκοκαλιά μιας οικονομίας, είναι υποδομή υλικοτεχνικής υποδομής, επειδή παρέχει και λειτουργεί ως σύνδεσμος μεταξύ εθνών, οργανισμών και ατόμων. Η λειτουργικότητα των υποδομών ζωτικής σημασίας βελτιώνεται συνεχώς δημιουργώντας νέες καινοτομίες, ευκαιρίες και απειλές

Το 2015, ο όγκος του παγκόσμιου θαλάσσιου εμπορίου ήταν 10 δισεκατομμύρια τόνοι (UNCTAD 2016). Τα λιμάνια και οι τερματικοί σταθμοί διαχειρίζονται περισσότερο από το 70% της αξίας του ναυτιλιακού εμπορίου και αποτελούν τον κύριο σύνδεσμο μεταξύ του εδάφους και του διεθνούς εμπορίου. Τα λιμάνια χαρακτηρίζονται ως υποδομές ζωτικής σημασίας, επηρεάζοντας την οικονομική και κοινωνική ευημερία μιας χώρας.

Η Cybersecurity έχει αυξήσει τη σημασία της στον ναυτιλιακό τομέα, ιδιαίτερα στις λιμενικές επιχειρήσεις. Το Παγκόσμιο Οικονομικό Φόρουμ ανέδειξε τον κυβερνοχώρο ως τον τέταρτο κορυφαίο παγκόσμιο κίνδυνο τον Ιανουάριο του 2012. Ένα χρόνο αργότερα, τα cyberattacks θεωρήθηκαν ότι αποτελούν ακόμη μεγαλύτερο κίνδυνο για την παγκόσμια οικονομία. Ο ναυτιλιακός τομέας είναι πολύ σημαντικός για την ΕΕ και τα κράτη μέλη της. Στην περιοχή της ΕΕ, το 52% της κυκλοφορίας εμπορευμάτων το 2010 πραγματοποιήθηκε με θαλάσσιες μεταφορές. Στην ΕΕ, 22 κράτη μέλη διαθέτουν θαλάσσια σύνορα και διαχειρίζονται περισσότερους από 1.200 θαλάσσιους λιμένες για τη στήριξη της δραστηριότητας του θαλάσσιου τομέα.

Τα υπολογιστικά δίκτυα επικοινωνιών αποτελούν τον πυρήνα των ευφυών συστημάτων μεταφορών (Iintelligent Ttransport Systems -ITS). Τα ITS είναι τεχνολογίες, εφαρμογές ή πλατφόρμες που βελτιώνουν την ποιότητα της μεταφοράς ή επιτυγχάνουν άλλα αποτελέσματα βασισμένα σε εφαρμογές που παρακολουθούν, διαχειρίζονται ή βελτιώνουν τα συστήματα μεταφορών. Έχουν βελτιώσει την αποτελεσματικότητα, τη συνοχή και την αποδοτικότητα του δικτύου μεταφορών. Τρεις κοινοί στόχοι του συστήματος μεταφορών υπαγορεύουν την προσέγγιση στον κυβερνοχώρο:

1) την ασφαλή λειτουργία όλων των τρόπων μεταφοράς. ·
2) η εκμετάλλευση και η αποτελεσματική μετακίνηση ανθρώπων, αγαθών και υπηρεσιών.
3) επικοινωνία με το κοινό για δημόσιο συμφέρον και ασφάλεια.

Το ζήτημα της ασφάλειας στη θάλασσα έχει καταστεί μεγαλύτερη ανησυχία για τη διεθνή θαλάσσια ατζέντα. Ιστορικά, τα πρώτα θέματα της ασφάλειας στη θάλασσα αφορούσαν την πειρατεία και την κλοπή φορτίου. Αυτό έχει επεκταθεί και περιλαμβάνει λαθρεπιβάτες και λαθρομετανάστες. Την 1η Ιουλίου 2004, ο Διεθνής Ναυτιλιακός Οργανισμός (IMO) αποδέχθηκε τον Κώδικα Διεθνούς Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ISPS), ο οποίος συνδέει τα πλοία και τους λιμένες, επιτρέποντάς τους να συνεργάζονται για την πρόληψη και την αντιμετώπιση απειλών για την ασφάλεια στον τομέα των θαλάσσιων μεταφορών.

ΛΙΜΕΝΙΚΗ ΑΣΦΑΛΕΙΑ

Ορισμοί λιμένων

Τα λιμάνια αποτελούν μία από τις σημαντικότερες πτυχές της υποδομής μεταφορών μιας χώρας. Σε πολλά εμπορικά έθνη, είναι η κύρια σύνδεση μεταφοράς μεταξύ των εμπορικών εταίρων και των κέντρων των αυτοκινητοδρόμων και των σιδηροδρόμων. Τα λιμάνια είναι ο μεγαλύτερος οικονομικός παράγοντας για την ευημερία ενός έθνους και θεωρούνται συνήθως ως πύλη για το εμπόριο. Οι περισσότεροι λιμένες προσελκύουν επίσης εμπορικές υποδομές, όπως τράπεζες, γραφεία και βιομηχανικές δραστηριότητες. Συνολικά, περίπου το 90% του παγκόσμιου εμπορίου μεταφέρεται με πλοίο, υπογραμμίζοντας την τεράστια σημασία των λιμένων στον κόσμο των μεταφορών.

Τα λιμάνια μπορούν να θεωρηθούν ως πολύπλοκες οργανώσεις με θεσμούς και λειτουργίες που διασχίζουν πολλαπλά επίπεδα. Ο στρατηγικός ρόλος των λιμένων είναι πολύ σημαντικός δεδομένου ότι είναι ο μοναδικός δεσμός μεταξύ της διεθνούς ναυτιλίας και της εφοδιαστικής κοινότητας και ο μοναδικός συνδυασμός όλων αυτών των θεσμών, λειτουργιών, περιουσιακών στοιχείων, διεργασιών και άλλων στοιχείων. Με λιμάνι και λιμενικές εγκαταστάσεις, τα αγαθά και οι πρώτες ύλες, όπως το πετρέλαιο και τα σιτηρά, έχουν πρόσβαση σε εθνικές βιομηχανίες και τοπικά σούπερ μάρκετ και άλλα καταστήματα.

Ένα λιμάνι είναι ένα περίπλοκο cyberenvironment που αποτελείται από λειτουργίες και συστήματα στη ξηρά και τη θάλασσα. Οι τέσσερις κύριοι τύποι περιουσιακών στοιχείων είναι κτίρια, κάθετες υποδομές, εργοστάσια και μηχανήματα, καθώς και συστήματα πληροφοριών και δεδομένων. Με αυτά τα περιουσιακά στοιχεία, η ποικιλία στις επιχειρησιακές υπηρεσίες μπορεί να εξασφαλιστεί και η τεχνολογία έχει σημαντικό ρόλο σε αυτήν. Η μείωση της απειλής ενός ή περισσοτέρων περιουσιακών στοιχείων μπορεί να επηρεάσει την ταχύτητα και την αποτελεσματικότητα της λειτουργίας του λιμένα και την παρατήρηση των λειτουργιών. Αυτό επηρεάζει την ασφάλεια και την αξιόπιστη κατανομή των καθηκόντων.

Οι κύριες λειτουργίες ενός λιμένα περιλαμβάνουν συνήθως λειτουργικά έργα πολιτικού μηχανισμού, διοικητικές λειτουργίες και λειτουργικές λειτουργίες. Τα χαρακτηριστικά πολιτικού μηχανισμού ασχολούνται με την πρόσβαση στη θάλασσα και τη γη, την υποδομή αγκυροβόλησης, το δίκτυο με τη διαχείριση οδικών και σιδηροδρομικών και βιομηχανικών χώρων. Οι διοικητικές λειτουργίες λειτουργούν όλες τις γραφειοκρατικές διαδικασίες που πρέπει να γίνουν όταν φτάνουν τα πλοία στο λιμάνι, όπως ο έλεγχος των επικίνδυνων φορτίων, η μετανάστευση, η υγεία, τα τελωνεία και ο έλεγχος του εμπορικού εγγράφου. Οι λειτουργικές λειτουργίες περιλαμβάνουν δραστηριότητες πλοήγησης, ρυμούλκησης και πρόσδεσης, χρήση αγκυροβολίων, καθώς και φόρτωση, εκφόρτωση, αποθήκευση και διανομή φορτίου.

Μπορούν να οριστούν σε τρεις κατηγορίες με βάση τις λειτουργίες τους. Ο πρώτος ορισμός αφορά τη διασύνδεση φορτίου που μπορεί να αναφέρεται ως κεντρικός λιμένας. Η δεύτερη αφορά την ανάπτυξη της ναυτιλιακής βιομηχανίας και δημιουργήθηκε στα μέσα του 1960 για να απεικονίσει την ανάπτυξη μετά τον Δεύτερο Παγκόσμιο Πόλεμο. Η εξέλιξη αυτή παρατηρείται στις μεγαλύτερες βιομηχανικές

περιοχές με δικό τους θαλάσσιο τερματικό σταθμό, τελωνειακό λιμένα ή πετρελαϊκό λιμάνι. Ο τρίτος ορισμός αναφέρεται σε εξειδικευμένους λιμένες, όπως είναι ένας ναυτικός λιμένας, ένας αλιευτικός λιμένας ή ένας λιμένας που ειδικεύεται στη μεταφορά ορισμένων εμπορευμάτων.

Οι λιμένες μπορούν επίσης να χαρακτηρίζονται από την ποιότητα των υπαρχουσών εγκαταστάσεων, την υποδομή και τον βαθμό υπηρεσιών που καθορίζονται από τα χαρακτηριστικά τους. Υπάρχουν τρεις κατηγορίες ταξινόμησης: θέση του λιμένα, hardportή softport. Η θέση ενός λιμένα μπορεί να βρίσκεται στην ενδοχώρα, στη θάλασσα, ή σε κάποιο ποτάμι. Η θέση του λιμένα είναι ο σημαντικότερος παράγοντας για την απόδοση του.

Η υποδομή, το μέγεθος του λιμένα, το μέγεθος του τερματικού, το βάθος του νερού της περιοχής και η ύπαρξη του κατάλληλου εξοπλισμού είναι τα καθοριστικά χαρακτηριστικά για ένασκληρό λιμένα (hardport). Τα χαρακτηριστικά ενός μαλακού λιμένα (softport) περιλαμβάνουν τον βαθμό εξειδίκευσης στον χειρισμό φορτίου, το μοντέλο διακυβέρνησης, οι υπηρεσίες θαλάσσιων μεταφορών που παρέχονται από το λιμάνι και ο βαθμός ολοκλήρωσης με παγκόσμια ναυτιλιακά δίκτυα. Αυτά τα χαρακτηριστικά παρέχουν επίσης μια επιλογή για τους πλοιοκτήτες, μεγαλύτερη ευελιξία και μικρότερους χρόνους διέλευσης που οδηγούν σε βελτιωμένη απόδοση των λιμένων.

ΑΝΑΠΤΥΞΗ ΤΩΝ ΛΙΜΕΝΩΝ

Οι δομές των λιμένων αλλάζουν συνεχώς και μεγαλώνουν με πολυπλοκότητα, καθιστώντας τους εξαρτώμενες από τις τεχνολογίες πληροφοριών και επικοινωνιών καθ 'όλη τη διάρκεια του κύκλου ζωής τους. Ορισμένες ενσωματωμένες τεχνολογίες είναι σε σταθερά ή κινητά στοιχεία που απαιτούνται για τις λιμενικές επιχειρήσεις. άλλοι μπορούν να λειτουργούν εξ αποστάσεως, όπως συστήματα που χρησιμοποιούνται για τον προγραμματισμό πλοίων και τη μετακίνηση φορτίου. Ο Alderton (2008, 10) επισημαίνει ότι η τεχνολογία διαχείρισης φορτίου αναπτύχθηκε ριζικά τις τελευταίες δεκαετίες.

Τα λιμάνια μπορούν να αλλάξουν και να αναπτυχθούν, ή ακόμη και να πεθάνουν εάν προκύψουν αλλαγές στην υποδομή χερσαίων μεταφορών ή / και σε εμπορικά μοντέλα. Ο κύκλος ζωής του λιμένα είναι συνήθως πολύ μεγάλος, γεγονός που οδηγεί τους λιμένες να προσαρμοστούν και να μετασχηματιστούν με την πάροδο του χρόνου. Τα λιμάνια αναπτύχθηκαν αρχικά για να καλύψουν τη ζήτηση του θαλάσσιου εμπορίου και των μεταφορών. Έφεραν νέο ανταγωνισμό και αλλαγές στα πρότυπα συναλλαγών. (Alderton 2008, 14.) Αυτό το στοιχείο συνδυάζει τις έννοιες από το βιβλίο του Alderton και ένα άρθρο του Pettit και του Beresford.

Ο λιμένας πρώτης γενιάς αναφέρεται σε λιμένες που λειτουργούσαν πριν από το 1960. Αυτοί οι λιμένες ήταν η μοναδική διασύνδεση φορτίου μεταξύ χερσαίων και θαλάσσιων μεταφορών. Ήταν συνήθως ξεχωριστά από τις δραστηριότητες των μεταφορών και του εμπορίου και θεωρήθηκαν ως ανεξάρτητοι φορείς με ελάχιστη ή

καθόλου συνεργασία με τις τοπικές αρχές. Επιπλέον, οι δραστηριότητες του λιμένα ήταν ξεχωριστές μεταξύ τους. Αυτές οι θύρες χειρίζονται χύδην φορτία.

Οι λιμένες δεύτερης γενιάς λειτουργούσαν μετά το 1960 και αναπτύχθηκαν ως κέντρα μεταφορών, βιομηχανίας και εμπορικών υπηρεσιών. Προσφέρουν βιομηχανικές και εμπορικές υπηρεσίες που δεν συνδέονταν άμεσα με τις δραστηριότητες φόρτωσης ή εκφόρτωσης. Οι πολιτικές και οι στρατηγικές αυτών των λιμένων βασίστηκαν σε ευρύτερες έννοιες και οι προσεγγίσεις διαχείρισης ήταν πιο εξελιγμένες. Οι λιμένες δεύτερης γενιάς ανέπτυξαν σχέσεις με τις τοπικές αρχές και με εταίρους μεταφορών και εμπορίου

Τη δεκαετία του 1980 παρατηρήθηκε η εμφάνιση λιμένων τρίτης γενιάς, οι οποίοι λειτουργούσαν με παγκόσμια εμπορευματοποίηση που συνδέονται με τις αυξανόμενες απαιτήσεις του διεθνούς εμπορίου. Αυτοί οι λιμένες θεωρούνταν κόμβοι ενός διεθνούς δικτύου παραγωγής και διανομής. Οι περιβαλλοντικές προσεγγίσεις ενσωματώθηκαν στις στρατηγικές τους. Ήταν πιο εκσυγχρονισμένοι από τους λιμένες πρώτης και δεύτερης γενιάς. Οι λιμένες τρίτης γενιάς προσφέρουν υπηρεσίες προστιθέμενης αξίας, όπως η αποθήκευση και η συσκευασία εκτός από τη διακίνηση φορτίων. Παρέχουν επίσης παραδοσιακές δραστηριότητες όπως υπηρεσίες πλοίων και διακίνηση φορτίων.

Οι λιμένες της τέταρτης γενιάς εμφανίστηκαν τη δεκαετία του 1990 παράλληλα με την επέκταση της παγκοσμιοποίησης και την ανάπτυξη μεγάλων διεθνών εταιρειών. Οι στρατηγικές και οι προσεγγίσεις τους ήταν πιο εξελιγμένες και περιλάμβαναν τη χρήση αυτοματισμού. Η εξέλιξη αυτή συνοδεύτηκε από την τυποποίηση των πληροφοριών και την παγκοσμιοποίηση των λιμενικών κοινοτήτων. Τα λιμάνια είχαν πλέον τον καλύτερο έλεγχο των περιβαλλοντικών δραστηριοτήτων τους και την απόκτηση γνώσεων. Ο αποφασιστικός παράγοντας ήταν η τεχνολογία της πληροφορίας. Η πολυπλοκότητα των λιμένων τέταρτης γενιάς παρουσιάζεται στο εύρος των υπηρεσιών εφοδιαστικής και των υπηρεσιών προστιθέμενης αξίας. Αυτοί οι λιμένες έχουν κοινούς φορείς εκμετάλλευσης ή διοίκηση, αλλά βρίσκονται χωριστά σε όλο τον κόσμο και μπορούν να θεωρηθούν παγκόσμιες εταιρείες.

Το μοντέλο «WORKPORT» δείχνει ότι τα στάδια ανάπτυξης δεν μπορούν να καθοριστούν εγκαίρως και ότι τα λιμάνια δεν ξεπερνούν σαφώς ορισμένα στάδια. Το μοντέλο βλέπει ότι τη δεκαετία του 1960 και τη δεκαετία του 1970 οι λιμένες ήταν κυρίως διακριτικοί από άποψη τρόπων μεταφοράς. Στη δεκαετία του 1980 οι λιμένες άρχισαν να διαφοροποιούνται στον τομέα της εφοδιαστικής και προσέφεραν υπηρεσίες προστιθέμενης αξίας. Στη δεκαετία του 1990, στο πλαίσιο της παγκοσμιοποίησης, οι λιμένες θεωρούνταν ως συγχωνεύσεις, εξαγορές και κοινές επιχειρήσεις που οδήγησαν σε πιο πολύπλοκες και κοινές επιχειρήσεις. Όσον αφορά την παγκοσμιοποίηση, τα λιμάνια αποτελούν μεγαλύτερο μέρος των παγκόσμιων αλυσίδων εφοδιασμού.

ΝΑΥΤΙΛΙΑΚΗ ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΛΙΜΕΝΩΝ

Οι κανονισμοί ασφαλείας των λιμένων δεν υπήρχαν καθ 'όσο τα λιμάνια. Οι Ηνωμένες Πολιτείες αποφάσισαν να επενδύσουν στον Διεθνή Ναυτιλιακό Οργανισμό το 1948. Αυτό ακολουθήθηκε το 1974 από τις πρώτες συμβάσεις της Ασφάλειας της Ζωής στη Θάλασσα (SOLAS). Έκτοτε, έχουν αναπτυχθεί και καθιερωθεί ένα πλήθος άλλων διεθνών κανονισμών. Είναι στην πραγματικότητα ένα αξιόλογο περιουσιακό στοιχείο, διευκολύνοντας τις ροές ανθρώπων και αγαθών μεταξύ χωρών σε όλο τον κόσμο. Η ύπαρξη αβεβαιότητας στη θάλασσα οδήγησε τους λιμένες να επικεντρωθούν στις αποβάθρες.

Με την πάροδο των ετών, τα λιμάνια έχουν γίνει όλο και περισσότερο αντικείμενο διεθνών και εθνικών ομάδων ασφαλείας που προσπαθούν να υποκινήσουν τον καλύτερο έλεγχο και την πρόληψη πιθανών απειλών. Το κυριότερο κοινό συμφέρον ασφάλειας των λιμανιών σε παγκόσμιο επίπεδο είναι η παροχή ασφαλούς διέλευσης και αγκυροβόλησης. Την τελευταία δεκαετία, η προσοχή επικεντρώθηκε σε ανασφάλειες που σχετίζονται με μηχανισμούς μεταφορών, όπως τα εμπορευματοκιβώτια. Είναι γνωστό ότι τα εμπορευματοκιβώτια είναι εξαιρετικός τρόπος μεταφοράς παράνομων ναρκωτικών και μεταναστών και ότι συχνά δεν ελέγχονται για παρατυπίες. Στις Ηνωμένες Πολιτείες, περίπου 10 εκατομμύρια εμπορευματοκιβώτια περνούν από λιμάνια ετησίως και μόνο το 2% εξετάζονται.

Το 2004, ο IMO υιοθέτησε τον Κώδικα Διεθνούς Ασφάλειας Πλοίων και Λιμενικών Εγκαταστάσεων (ISPS). Αρχικά, ο Κώδικας ISPS βασικά καλύπτει την παραδοσιακή συρροή μεταξύ πλοίων και λιμενικών εγκαταστάσεων. Επίσης, καλύπτει λιμάνια που εξυπηρετούν πλοία που εκτελούν διεθνή ταξίδια, αφήνοντας κενά ασφαλείας για τα πλοία σε εσωτερικά δρομολόγια. Ορισμένες απειλές για την ασφάλεια μπορούν επίσης να προκύψουν από επιχειρήσεις που βασίζονται στην ξηρά. Οι χερσαίες επιχειρήσεις συνδέουν εταιρίες φορτοεκφόρτωσης, εταιρείες οδικών και σιδηροδρομικών μεταφορών και μεταφορείς εμπορευμάτων. Οι ενέργειες αυτές μπορούν να έχουν άμεσες επιπτώσεις στις θαλάσσιες μεταφορές και στις λιμενικές εγκαταστάσεις.

Το πρότυπο πλαίσιο για την ασφάλεια και την προστασία του περιβάλλοντος της θαλάσσιας κυκλοφορίας και των λιμένων περιλαμβάνει νομικά εργαλεία όπως UNCLOS, SOLAS, MARPOL, κώδικες ISM και ISPS και μέτρα διαχείρισης, όπως η επίσημη αξιολόγηση της ασφάλειας και η ολοκληρωμένη διαχείριση των παράκτιων ζωνών. Οι κανονισμοί για τη θαλάσσια ασφάλεια εφαρμόζονται σε εθνικό και διεθνές επίπεδο. Τα μεμονωμένα κράτη καθορίζουν τους δικούς τους κανόνες και κανονισμούς σχετικά με τις διαφορετικές τεχνικές προοπτικές των πλοίων και της ναυσιπλοΐας προκειμένου να αυξηθεί η ασφάλεια. Το κράτος σημαίας είναι μια χώρα που ρυθμίζει τα πλοία υπό τις καταχωρίσεις του. Ασκεί τη δική του αρμοδιότητα και τον έλεγχο των διοικητικών, τεχνικών και κοινωνικών θεμάτων που αφορούν τα πλοία που λειτουργούν υπό τη σημαία του, προκειμένου να διασφαλιστεί η ασφάλεια στη θάλασσα.

Λόγω της αύξησης των **cyberattacks** και **cyberthreats**, πολλοί διεθνείς οργανισμοί έχουν αναπτύξει νέα πλαίσια, πρότυπα και κατευθυντήριες γραμμές για τις

λιμενικές εγκαταστάσεις και τα πλοία για να προστατευθούν από αυτές τις απειλές. Ο στόχος του κώδικα ISPS είναι να ενισχύσει την ασφάλεια στη θάλασσα τόσο στα πλοία όσο και στους λιμένες. Η παραδοσιακή προσέγγιση της ασφάλειας στη ναυτιλία ήταν η ασφάλεια των εμπορευματοκιβωτίων, πράγμα που σήμαινε την ασφαλή φύλαξη του φορτίου μέσα στο δοχείο. Σήμερα, η ασφάλεια των εμπορευματοκιβωτίων περιλαμβάνει επίσης τη διατήρηση αγαθών που δεν ανήκουν στο δοχείο από αυτά, όπως τα όπλα μαζικής καταστροφής.

Οι Cyberattackers συνήθως στοχεύουν τους χειριστέστων λιμένων επειδή οι χειριστές τείνουν να έχουν λιγότερους ελέγχους ασφαλείας από ό, τι τον ίδιο τον λιμένα και κατά συνέπεια είναι πιο εύκολο να επιτεθούν. Για τα λιμάνια, τα cyberthreats περιλαμβάνουν, για παράδειγμα, μια ενέργεια για τη διαγραφή λειτουργικών δεδομένων που περιέχουν χρονοδιαγράμματα και πληροφορίες για αποστολές εμπορευματοκιβωτίων.

ΟΙ ΚΙΝΔΥΝΟΙ ΠΟΥ ΑΝΤΙΜΕΤΟΠΙΖΟΥΝ ΟΙ ΛΙΜΕΝΙΚΕΣ ΕΓΚΑΤΑΣΤΑΣΕΙΣ

Τα λιμάνια θεωρούνται από καιρό ως μια αόρατη βιομηχανία, έχοντας πάντα λειτουργήσει σχεδόν μόνοι τους με ελάχιστη προσοχή και συνειδητοποίηση από την κοινωνία. Για τις λιμενικές εγκαταστάσεις, διαφέρουν πολλοί διαφορετικοί κίνδυνοι κατά τη διάρκεια του κύκλου ζωής τους. Οι κίνδυνοι μπορούν να εμφανιστούν στην αρχή του κύκλου ζωής με τη μορφή κακής διερεύνησης εγγράφων ή ανεπαρκούς χρόνου ή προϋπολογισμού. Για παράδειγμα, η εφαρμογή πιο συγκεκριμένης ασφάλειας λιμένων στον σχεδιασμό ασφάλειας έχει αυξήσει την έμφαση των σχεδίων τοποθεσίας. Οι κίνδυνοι για τους λιμένες επηρεάζουν όχι μόνο τους ίδιους τους λιμένες, αλλά και τους πελάτες τους και άλλους ενδιαφερόμενους. Οι κίνδυνοι μπορεί να περιλαμβάνουν, για παράδειγμα, οικονομικές απώλειες, κλοπές φορτίου ή πληροφοριών και απεργίες ή δυσλειτουργίες στην ασφάλεια, οι οποίες μπορούν να οδηγήσουν σε διακοπή λειτουργίας ενός λιμένα. Οι κίνδυνοι που συνδέονται με τους λιμένες μπορούν να επηρεάσουν ολόκληρη την αλυσίδα εφοδιασμού.

Συνήθως, τα περιστατικά λιμένων είναι ακούσια γεγονότα, όπως βλάβες στο περιβάλλον, διακοπή συστήματος μεταφοράς ή ζημιές σε εργαζόμενους και προσωπικό. Τα ατυχήματα σε λιμένες μπορούν να ταξινομηθούν ανά τύπο, προέλευση και αιτία. Περίπου το 50% των ατυχημάτων σχετίζεται με την απώλεια του φορτίου, το 29% με τις πυρκαγιές και το 17% με τις εκρήξεις. Παρατηρήθηκε επίσης ότι σχεδόν το 40% των λιμενικών περιστατικών συμβαίνουν στη θάλασσα, το 21% στην ξηρά σχετικά με την αποθήκευση, τις διεργασίες και τις μεταφορές και το 39% σε μια διεπαφή θαλάσσης.

Οι περισσότερες από τις ανασφάλειες που συμβαίνουν στη θάλασσα και στα λιμάνια μπορούν να κατηγοριοποιηθούν με τον όρο ναυτιλιακή τρομοκρατία. Η ναυτιλιακή τρομοκρατία υποδηλώνει ότι υπάρχουν τρομοκρατικές ομάδες που στοχεύουν ή χρησιμοποιούν πλοία στη θάλασσα ή στα λιμάνια ως όπλα για να

επιτεθούν επιβάτες και προσωπικό. Τα λιμάνια μπορούν να χρησιμοποιηθούν στην κυβερνο-τρομοκρατία για να δημιουργήσουν φυσικές και οικονομικές διαταραχές.

Η φάση σχεδιασμού είναι το πιο πολύπλοκο στάδιο του κύκλου ζωής ενός λιμένα, επειδή απαιτεί συνεργασία μεταξύ διαφόρων ενδιαφερομένων. Οι κίνδυνοι περιλαμβάνουν επίσης τη χρήση τεχνολογίας ή προμηθευτών που δεν έχουν καταδειχθεί.

Οι λειτουργίες κατά τη διάρκεια του κύκλου ζωής ενός λιμένα έχουν τρεις τύπους κινδύνου: τους κινδύνους των περιουσιακών στοιχείων και του εξοπλισμού χειρισμού, τους κινδύνους ροής κύκλου εργασιών και τους κινδύνους αστικής ευθύνης. Οι κίνδυνοι περιουσιακών στοιχείων και εξοπλισμού περιλαμβάνουν την απώλεια ή τη ζημία σε περιουσιακά στοιχεία, τη ζημία στις προβλήτες και τις αποβάθρες που προκαλούνται από φυσικούς κινδύνους ή τρομοκρατία. Οι κίνδυνοι ροής κύκλου εργασιών περιλαμβάνουν δράσεις όπως απεργίες, άρνηση πρόσβασης ή ατυχήματα μεταφοράς ή βλάβη που επηρεάζει τον κρίσιμο εξοπλισμό χειρισμού φορτίου. Οι κίνδυνοι αστικής ευθύνης περιλαμβάνουν τραυματισμούς έναντι τρίτων φορέων, απώλεια ή ζημία πλοίων ή φορτίου, πρόστιμα και δασμούς και κίνδυνους ρύπανσης.

Το ποσό των πληροφοριών που κατέχει ένας λιμένας, οι μεγάλες νομισματικές μεταβιβάσεις και ο αριθμός των ενδιαφερομένων μερών προσελκύουν τους cyberattackers να στοχεύουν στους λιμένες και τις λιμενικές εγκαταστάσεις. Συνήθως, τα συστήματα υπολογιστών και οι βάσεις δεδομένων των λιμένων περιέχουν πληροφορίες σχετικά με 5-10 διαφορετικούς ενδιαφερόμενους. Για παράδειγμα, οι cyberattackers μπορούν να επιτάσσουν ένα πλοίο, να κλείσουν ένα λιμάνι ή το τερματικό του, να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες όπως έγγραφα τιμολόγησης ή χρονοδιαγράμματα και να αλλάξουν δηλώσεις ή αριθμούς εμπορευματοκιβωτίων. Ακόμα και οι μικρότερες κυβερνοεπιθέσεις μπορούν να οδηγήσουν σε απώλειες επιχειρήσεων εκατομμυρίων δολαρίων.

Τα λιμενικά ατυχήματα, τα σφάλματα του λιμενικού εξοπλισμού, η κακή διαχείριση των επικίνδυνων εμπορευμάτων, οι παραβιάσεις της ασφάλειας και οι απεργίες στην εργασία αποτελούν τις κύριες κατηγορίες διακοπών λειτουργίας των λιμένων. Οι διαταραχές αυτές έχουν επίσης άμεσες και έμμεσες συνέπειες για τις επιχειρήσεις και τις λειτουργίες ολόκληρου του δικτύου μεταφορών και παροχής. Οι συνέπειες επηρεάζουν επίσης την οικονομική και κοινωνική ευημερία του περιβάλλοντος που περιβάλλει το λιμάνι και τις επιχειρήσεις του. Για παράδειγμα, το 2011 ένας σεισμός διαταράσσει σοβαρά τις δραστηριότητες των βορειοανατολικών ιαπωνικών λιμένων. Επίσης, επηρέασε τις δραστηριότητες των αποθηκών και των εγκαταστάσεων παραγωγής που εξυπηρετούν τις λιμενικές περιοχές. Οι πιθανές ευπάθειες των λιμένων περιλαμβάνουν, για παράδειγμα, περιορισμένη εκπαίδευση και ετοιμότητα για ασφάλεια στον κυβερνοχώρο, σφάλματα λογισμικού και σύμπτωση, σύνδεση και αλληλεξάρτηση των δικτύων.

ΚΡΙΣΗΜΕΣ ΥΠΟΔΟΜΕΣ

Η ιστορία των υποδομών ζωτικής σημασίας χρονολογείται από τη δεκαετία του 1980, όταν πραγματοποιήθηκαν αρκετά έργα για την δημιουργία σημαντικών υποδομών στον δημόσιο τομέα. Στη συνέχεια, σημαντικές υποδομές ορίστηκαν για να συμπεριλάβουν αυτοκινητόδρομους, γέφυρες, αεροδρόμια, δημόσια συγκοινωνία, εγκαταστάσεις ύδρευσης και αποχέτευσης και υπηρεσίες στερεών αποβλήτων και επικίνδυνων αποβλήτων. Καθώς η διεθνής τρομοκρατία αυξήθηκε στη δεκαετία του '90, ο όρος επανεξετάστηκε στο πλαίσιο της έννοιας της εθνικής ασφάλειας. Η κρίσιμη υποδομή επεκτάθηκε για να περιλαμβάνει, μεταξύ άλλων, ενεργειακά συστήματα, πυρηνικά συστήματα, ναυτιλιακές υπηρεσίες και συστήματα μεταφορών.

Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology-NIST) ορίζει τις κρίσιμες υποδομές ως εικονικά ή φυσικά συστήματα και περιουσιακά στοιχεία που είναι θεμελιώδη για τα έθνη. Η ανικανότητα και η κατεδάφιση αυτών των συστημάτων και περιουσιακών στοιχείων έχει αξιοσημείωτο αντίκτυπο στην ασφάλεια, την εθνική οικονομία, τη δημόσια υγεία και την ασφάλεια. Η Ευρωπαϊκή Επιτροπή έχει προσδιορίσει την υποδομή ζωτικής σημασίας ως εγκαταστάσεις, δίκτυα, υπηρεσίες και περιουσιακά στοιχεία της τεχνολογίας των πληροφοριών.

Η κρίσιμη υποδομή θεωρείται πολύ πολύπλοκη ένωση, οπότε υπάρχει ζήτηση να αναπτυχθεί μια σταθερή έννοια που θα μπορούσε να χρησιμοποιηθεί σε περιόδους τρομοκρατίας. Η έννοια ονομάζεται "lifelinesystem" και μετρά την απόδοση μεγάλων γεωγραφικά διανεμημένων δικτύων όταν υπάρχουν, για παράδειγμα, σεισμοί, τυφώνες και άλλα κακόβουλα φυσικά φαινόμενα. Αυτές οι σωληνώσεις ταξινομούνται σε έξι κύρια συστήματα: ηλεκτρική ενέργεια, φυσικό αέριο και υγρά καύσιμα, τηλεπικοινωνίες, μεταφορές, διάθεση αποβλήτων και παροχή νερού. Αυτή η έννοια συμβάλλει στην αποσαφήνιση των χαρακτηριστικών που είναι συνδεδεμένα με τα απαραίτητα συστήματα υποστήριξης. Επίσης, οργανώνει τις αντιλήψεις σε μηχανικές προκλήσεις για τη βελτίωση της απόδοσης των μεγάλων δικτύων.

Σήμερα η τεχνολογία των δικτύων και των υπολογιστών αυξάνεται ραγδαία και η κρίσιμη υποδομή εξαρτάται όλο και περισσότερο από αυτές. Υπάρχουν πολλές πτυχές στην προστασία της υποδομής ζωτικής σημασίας, όπως η προστασία των πολιτικών και εμπορικών συστημάτων και υπηρεσιών και των στρατιωτικών δυνάμεων και συστημάτων. Η πολιτική πτυχή καθορίζει ένα υψηλό επίπεδο, σύμφωνα με το οποίο τα έθνη δεν θα δεχθούν μια ενιαία επίθεση στην κρίσιμη υποδομή τους. Η στρατιωτική πτυχή θεωρεί τις επιθέσεις λιγότερο αξιοσημείωτες εάν δεν βλάπτουν τις εθνικές δυνατότητες.

Για το μέλλον, είναι σημαντικό να δημιουργηθούν ευέλικτες και συλογικές μέθοδοι για τα έθνη και τις κοινότητες ώστε να κατανοήσουν τη σημασία αυτών των υποδομών. Οι ανθεκτικές κοινότητες πρέπει να ενισχύσουν την ευαισθητοποίηση μέσω της εκπαίδευσης και της επικοινωνίας σχετικά με τον κίνδυνο. Οι κοινότητες πρέπει επίσης να έχουν ισχυρή και καινοτόμο ηγετική θέση, αποτελεσματικό προγραμματισμό και μακροπρόθεσμη δέσμευση πόρων που θα βοηθήσουν στην τοποθέτηση σύνθετων συστημάτων. Αυτά τα συστήματα και η υποδομή απαιτούν ακριβείς πληροφορίες σχετικά με την ώρα, την ενημερωμένη επιστήμη, την τεχνολογία και τις πληροφορίες που παρέχονται από εταιρικές σχέσεις και δίκτυα μεταξύ κοινοτήτων, κυβερνήσεων, επιστημόνων και μηχανικών.

Η υλικοτεχνική υποδομή είναι ένας από τους σημαντικότερους τύπους υποδομών που χρειάζονται τα έθνη, οι οργανισμοί και τα άτομα για να αλληλεπιδράσουν. Αναφέρεται σε όλες τις επιχειρήσεις και τις λειτουργίες που απαιτούνται για την υλοποίηση της αποστολής υλικοτεχνικής υποστήριξης. Υπάρχουν δύο τρόποι ταξινόμησης των βασικών υλικοτεχνικών διεργασιών: 1) οι κόμβοι υλικοτεχνικής υποστήριξης που περιλαμβάνονται στην υλικοτεχνική υποδομή και περιλαμβάνουν την αποθήκευση και τον χειρισμό αγαθών και 2) τις άκρες υλικοτεχνικής υποστήριξης που λειτουργούν ως σύνδεσμοι μεταξύ των υλικοτεχνικών κόμβων. Η καλή υποδομή υπάρχει μόνο όταν οι λειτουργίες είναι γρήγορες και αποδοτικές και υπάρχουν μόνο χαμηλού επιπέδου εμπόδια στην απόδοση.

Επειδή η υποδομή ζωτικής σημασίας είναι σημαντική για κάθε έθνος του κόσμου και η ασφάλεια του κυβερνοχώρου είναι παγκόσμιο θέμα, πρέπει να αναπτυχθούν στρατηγικές και πολιτικές και για τα δύο. Υπάρχουν τρία προβλήματα όσον αφορά τις κυβερνοαπειλές και τις υποδομές ζωτικής σημασίας:

1) Οι αξιόπιστες πληροφορίες σχετικά με αυτές δεν είναι διαθέσιμες στο κοινό.
2) οι αποκαλούμενοι «cyber gurus» τείνουν να δραματοποιούν και να απλοποιούν αρκετά τους κινδύνους για της υποδομή ζωτικής σημασίας.
3) οι πληροφορίες περιορίζονται επίσης από τη θεσμική κουλτούρα, τον ανταγωνισμό σε απλές ευπάθειες κρίσιμης υποδομής.

ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

Το 2014, ΤοΕθνικόΙνστιτούτοΠροτύπωνκαιΤεχνολογίας (NationalInstituteofStandardsandTechnology-NIST)δημοσίευσε το πρώτο της πλαίσιο για την ασφάλεια στον κυβερνοχώρο στις υποδομές ζωτικής σημασίας. Η διαδικασία ξεκίνησε στις 12 Φεβρουαρίου 2013, όταν ο Πρόεδρος των Ηνωμένων Πολιτειών υπέγραψε την εκτελεστική εντολή 13636 για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Ο κύριος στόχος του πλαισίου είναι η δομή διαφόρων προσεγγίσεων που συμβάλλουν στη συγκέντρωση προτύπων, κατευθυντήριων γραμμών και πρακτικών για την ασφάλεια στον κυβερνοχώρο. Εξαρτάται επίσης από ήδη υπάρχουσες γενικές κατευθυντήριες γραμμές, πρότυπα και πρακτικές. Περιέχει τρία διαφορετικά μέρη, τα οποία είναι ο πυρήνας πλαισίου, οι κλίμακες υλοποίησης

πλαισίου και το προφίλ πλαισίου. (NIST 2014, 2017.) Το πλαίσιο αυτό μπορεί να εφαρμοστεί και στους λιμένες επειδή αποτελούν σημαντικό τμήμα της υποδομής ζωτικής σημασίας για τις μεταφορές.

Ο πυρήνας περιλαμβάνει ένα σύνολο δραστηριοτήτων για την ασφάλεια του κυβερνοχώρου, τα αποτελέσματα και τις ενημερωτικές αναφορές που εμφανίζονται σε όλους τους κλάδους κρίσιμης υποδομής. Ο πυρήνας παρέχει επίσης έναν λεπτομερή οδηγό για το πώς η υποδομή ζωτικής σημασίας μπορεί να αναπτύξει μεμονωμένα οργανωτικά προφίλ. Ωστόσο, όταν οι οργανώσεις έχουν μέσα από αυτό στο πλαίσιο της ασφάλειας του κυβερνοχώρου, παρέχει μια στρατηγική άποψη υψηλού επιπέδου για τον κύκλο ζωής της διαχείρισης κινδύνων στον κυβερνοχώρο. Ο πυρήνας περιλαμβάνει πέντε συνεχείς λειτουργίες:

- Προσδιορισμός - διαχείριση πιθανών κινδύνων για συστήματα, περιουσιακά στοιχεία και δυνατότητες.
- Προστασία –εφαρμογή κατάλληλων μέτρων ασφαλείας που εξασφαλίζουν την παροχή υπηρεσιών κρίσιμης υποδομής.
- Εντοπισμός - ενέργειες που εντοπίζουν το περιστατικό ενός συμβάντος ή επίθεσης στον κυβερνοχώρο.
- Αντιμετώπιση - ενέργειες που συμβάλλουν στον εντοπισμό και την καταπολέμηση ενός γεγονότος στον κυβερνοχώρο.
- Ανάκτηση - ενέργειες για τη διατήρηση στρατηγικών και για την αποκατάσταση των δυνατοτήτων μετά την αντιμετώπιση ενός συμβάντος στον κυβερνοχώρο.

Το πλαίσιο περιλαμβάνει επίπεδα μηχανισμών για την διερεύνηση και την κατανόηση των χαρακτηριστικών των υποδομών ζωτικής σημασίας με σκοπό τον έλεγχο των κινδύνων της ασφάλειας στον κυβερνοχώρο. Οι οργανώσεις σκέφτονται με τις τρέχουσες πρακτικές για τη διαχείριση κινδύνων, το περιβάλλον απειλών και όλες τις απαιτήσεις, τους στόχους για τις επιχειρήσεις και τους οργανωτικούς περιορισμούς. Υπάρχουν τέσσερα επίπεδα. Στο πρώτο επίπεδο (Partial) οι πρακτικές είναι ανεπίσημες και υπάρχει περιορισμένη συνειδητοποίηση. Η δεύτερη βαθμίδα (Risk Informed) περιλαμβάνει μεγαλύτερη ευαισθητοποίηση σε οργανωτικό επίπεδο, αλλά δεν εφαρμόζεται σε ολόκληρη την οργάνωση. Στην τρίτη βαθμίδα (Repeatable) οι πρακτικές εγκρίνονται τυπικά και περιλαμβάνονται στις πολιτικές. Στην τέταρτη βαθμίδα (Adaptive) οι πρακτικές είναι ευέλικτες και έχουν πλήρη επίγνωση των κινδύνων στον κυβερνοχώρο.

Τα Προφίλ του Πλαισίου βοηθούν τους οργανισμούς να ευθυγραμμίσουν τις δράσεις τους στον τομέα της ασφάλειας του κυβερνοχώρου με τις επιχειρηματικές απαιτήσεις, τις ανοχές κινδύνου και τους πόρους τους. Αυτά τα Προφίλ παρέχουν στους οργανισμούς την ευκαιρία να εντοπίσουν ευκαιρίες για την ενίσχυση της στάσης τους στον κυβερνοχώρο. Το Τρέχον Προφίλ αναφέρεται στα αποτελέσματα των κινδύνων στον κυβερνοχώρο που ήδη εντοπίζονται. Το Προφίλ Στόχου αναφέρεται στα απαιτούμενα αποτελέσματα που βοηθούν τους οργανισμούς να επιτύχουν τους επιθυμητούς στόχους για τη διαχείριση του κινδύνου ασφάλειας στον κυβερνοχώρο.

CYBER-RISK ΣΤΡΑΤΗΓΙΚΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΣΤΑ ΛΙΜΑΝΙΑ

Επειδή οι λιμένες και οι λιμενικές επιχειρήσεις είναι διάσπαρτες σε όλο τον κόσμο, είναι πολύ δύσκολο να αναπτυχθεί μια συνολική στρατηγική για όλα τα μέλη των λιμένων και των λιμενικών δικτύων. Για παράδειγμα, τα γραφεία μιας μεγάλης ναυτιλιακής γραμμής κοντέινερ μπορούν να διανεμηθούν σε 150 χώρες και η ναυτιλιακή γραμμή μπορεί να λειτουργήσει 300 σκάφη. Όταν η διαχείριση του cyber-risk είναι αποτελεσματική, εξετάζει τις επιπτώσεις ασφάλειας καιτις συνέπειες της αποκάλυψης ή εκμετάλλευσης των τρωτών σημείων στα συστήματα τεχνολογίας πληροφοριών. Η διαχείριση Cyber-risk πρέπει να είναι ανθεκτική και να εξελίσσεται ως φυσική επέκταση των ήδη υπαρχουσών πρακτικών και στρατηγικών διαχείρισης της ασφάλειας.

Η διαχείριση του Cyber-risk συνίσταται στη διαδικασία εντοπισμού, ανάλυσης, αξιολόγησης και επικοινωνίας ενός κυβερνοχώρου. Περιλαμβάνει επίσης την αποδοχή, την αποφυγή, τη μεταφορά ή την άμβλυνση του cyber-risk σε επιθυμητό επίπεδο. Λαμβάνει υπόψη το κόστος και τα πλεονεκτήματα των ενεργειών των ενδιαφερομένων. Σκοπός της είναι η υποστήριξη και να διασφαλίσει την ασφαλής ναυτιλίας που είναι λειτουργικά ανθεκτική στοCyber-risk και εκτείνεται από τα ανώτερα διοικητικά στελέχη σε όλους τους φορείς των λιμενικών εγκαταστάσεων.

Υπάρχουν πέντε λειτουργικά στοιχεία στη διαχείριση του cyberrisk: προσδιορισμός, προστασία, ανίχνευση, αντιμετώπιση και ανάκτηση. Ο «προσδιορισμός» καλύπτει όλους τους ρόλους και τις ευθύνες του προσωπικού που πρέπει να καθοριστούν για τη διαχείριση του κυβερνοχώρου και όλων των συστημάτων, περιουσιακών στοιχείων, δεδομένων και δυνατοτήτων που όταν απειλούνται μπορούν να δημιουργήσουν κινδύνους για το λιμένα και τα πλοία του. Πρέπει να ληφθεί απόφαση σχετικά με τα πρότυπα ασφαλείας της τεχνολογίας πληροφοριών που είναι τα πλέον κατάλληλα για τα συστήματα του οργανισμού. Στη συνέχεια, τα συστήματα και τα πρότυπα πρέπει να ελέγχονται για ομοιότητες και να βεβαιώνονται ότι οι τελευταίες ενημερώσεις εγκαταστάθηκαν.

Η «προστασία» αναφέρεται στην εφαρμογή διαδικασιών και μέτρων ελέγχου των κινδύνων και στον προγραμματισμό έκτακτης ανάγκης για την προστασία των cyber-activities και στην επιβεβαίωση της συνέχειας των πράξεων. Δεν είναι μόνο ο κύριος οργανισμός που κινδυνεύει να αντιμετωπίσει απειλές στον κυβερνοχώρο, αλλά και τους προμηθευτές, πελάτες και άλλους φορείς εκμετάλλευσης. Οι κύριοι οργανισμοί πρέπει να εμπλέκουν τις ομάδες συμφερόντων στη συζήτηση για τις απειλές και τις αδυναμίες στον κυβερνοχώρο.

Ως «ανίχνευση» νοείται η ανάπτυξη και η υλοποίηση όλων των απαραίτητων δραστηριοτήτων που χρειάζεται ένας λιμένας και οι εγκαταστάσεις του για την έγκαιρη ανίχνευση ενός cyberattack. Οι επιλεγμένες πρακτικές στον τομέα της

ασφάλειας στον κυβερνοχώρο πρέπει να εκτελούνται και να ελέγχονται μέσω ασκήσεων και γυμνασίων για τον εντοπισμό πιθανών κενών και ελλείψεων ασφαλείας για βελτίωση. Η "απάντηση" αναφέρεται στις δραστηριότητες και ενέργειες που απαιτούνται για την παροχή ανθεκτικότητας και την αποκατάσταση των συστημάτων που είναι απαραίτητα για τις επιχειρήσεις και τις υπηρεσίες.

«Ανάκτηση» σημαίνει τον προσδιορισμό των μέτρων που είναι απαραίτητα για την υποστήριξη ή την αποκατάσταση cybersystem για τις λειτουργίες. Όλες αυτές οι στρατηγικές και διαδικασίες που έχουν επιλεγεί για τα cyberthreats πρέπει να αναθεωρηθούν και να αξιολογηθούν για τα νέα cybersystems. Αυτά τα πέντε λειτουργικά στοιχεία περιλαμβάνουν τις δραστηριότητες και τα επιθυμητά αποτελέσματα της αποτελεσματικής διαχείρισης του κυβερνοχώρου σε όλα τα κρίσιμα συστήματα που επηρεάζουν τις θαλάσσιες επιχειρήσεις και την ανταλλαγή πληροφοριών.

Κώδικας ορθής πρακτικής για τους λιμένες και τα συστήματα λιμένων

Το Ινστιτούτο μηχανικής και Τεχνολογίας (Institution of Engineering and Technology-IET) δημιούργησε την ιδέα του κώδικα ορθής πρακτικής βασισμένη σε επισκέψεις σε πολλά λιμάνια του Ηνωμένου Βασιλείου, μαζί με το Εργαστήριο Επιστήμης και Τεχνολογίας της Άμυνας. Η ιδέα του Κώδικα Πρακτικής ορίζει γιατί είναι σημαντικό να συνδέεται η ασφάλεια στον κυβερνοχώρο με μια συνολική προσέγγιση για ολόκληρο τον κύκλο ζωής των περιουσιακών στοιχείων. Αυτή η προσέγγιση μπορεί να εντοπίσει πιθανά οικονομικά αποτελέσματα, αποτελέσματα φήμης και ασφάλειας που θα μπορούσαν να προκύψουν όταν δεν εντοπίζονται οι απειλές. Η ιδέα προορίζεται να αποτελέσει μέρος ενός ολοκληρωμένου συστήματος διαχείρισης κινδύνου και επιχειρηματικού σχεδίου ενός οργανισμού. Αυτό σημαίνει ότι η ασφάλεια στον κυβερνοχώρο διατηρείται ως οικονομικά αποδοτικό μέρος της κύριας επιχείρησης. Υπάρχουν δύο κύριες στρατηγικές του Κώδικα Ορθής Πρακτικής η "**CyberSecurityEvaluation**" και η "**CyberSecurityPlan**".

Σύμφωνα με συμφωνίες σχετικά με τα πρότυπα ασφάλειας λιμένων, οι αξιολογήσεις του κυβερνοχώρου πραγματοποιούνται σε εγκαταστάσεις λιμένων και λιμενικών εγκαταστάσεων. Ο στόχος των αξιολογήσεων ασφαλείας είναι ο προσδιορισμός των τρωτών σημείων των φυσικών δομών, των συστημάτων ασφάλειας του προσωπικού και των επιχειρηματικών διαδικασιών που μπορεί να οδηγήσουν σε συγκρούσεις ή ατυχήματα.

Υπάρχουν 4 βασικά στοιχεία της αξιολόγησης του κυβερνοχώρου (**CyberSecurityEvaluation**). Η αναγνώριση των περιουσιακών στοιχείων και των πόρων του λιμένα που σχετίζονται με τις διάφορες εγκαταστάσεις, τα κτίρια, τα συστήματα και τα δεδομένα του λιμένα. Αυτά τα περιουσιακά στοιχεία είναι πολύ σημαντικά και πρέπει να προστατευθούν. Η ταυτοποίηση και η αξιολόγηση του κινδύνου βοηθά στην παρακολούθηση των απειλών που μπορούν να βλάψουν έγκαιρα τα περιουσιακά στοιχεία, τις υποδομές και τις ευπάθειες. Με τα κατάλληλα μέτρα

ασφαλείας, τα λιμάνια προετοιμάζονται προληπτικά για τυχόν cyberattacks και cyberthreats. Βοηθά επίσης στη μείωση των κινδύνων και οποιωνδήποτε άλλων επιπτώσεων που μπορεί να εμφανιστούν σε επιχειρήσεις από cyberthreats. Η ολοκληρωμένη αξιολόγηση των κινδύνων αποτελείται από ανθρώπινους παράγοντες, αδυναμίες υποδομής, κανονισμούς και μεθόδους.

Τα σχέδια για την ασφάλεια στον κυβερνοχώρο(**CyberSecurityplan**) βασίζονται σε αξιολογήσεις της ασφάλειας στον κυβερνοχώρο και στους παράγοντες κινδύνου και απειλής που εντοπίστηκαν από την αξιολόγηση. Θα πρέπει να τονίζουν και να βελτιώνουν τόσο τα λιμάνια όσο και τα σχέδια ασφαλείας των επιχειρήσεων τους. Το σχέδιο για την ασφάλεια του κυβερνοχώρου λαμβάνει υπόψη τις επιπτώσεις των λιμενικών επιχειρήσεων που έχουν μετρηθεί στο σχέδιο ασφαλείας.

Για ένα λειτουργικό σχέδιο ασφάλειας στον κυβερνοχώρο, είναι σημαντικό να υιοθετηθεί η εγκεκριμένη προσέγγιση μέσω των ανθρώπων, των διαδικασιών, των φυσικών και τεχνολογικών πτυχών του λιμένα. Από την προοπτική του κυβερνοχώρου, το σχέδιο πρέπει να περιλαμβάνει ή να αναφέρεται στους κανονισμούς και τις διαδικασίες του λιμένα. Οι κανονισμοί βασίζονται συνήθως σε κανονισμούς που επηρεάζουν την ασφάλεια των επιχειρήσεων που καθοδηγούν το σχέδιο ασφάλειας στον κυβερνοχώρο. Οι διαδικασίες διαχειρίζονται με τους κανονισμούς ασφαλείας και παράγουν οδηγίες για τη συνεχή παραγωγή τους μέσω της χρήσης περιουσιακών στοιχείων του λιμένα καθ 'όλη τη διάρκεια του κύκλου ζωής τους. Οι διαδικασίες περιέχουν λεπτομερείς οδηγίες που συνδέονται με επαναλαμβανόμενους και σταθερούς μηχανισμούς. Με αυτές τις οδηγίες, οι διαδικασίες μηχανισμού μπορούν να υλοποιηθούν και να παραχθούν λειτουργικά.

Το σχέδιο πρέπει να ενσωματωθεί σωστά στον μηχανισμό του επιχειρησιακού χρονοδιαγράμματος τουλάχιστον σε ετήσια βάση. Θα πρέπει επίσης να επιθεωρείται ώστε να διασφαλίζεται ότι ευθυγραμμίζεται με τις επιθυμητές προθέσεις. Το σχέδιο πρέπει να επικαιροποιείται κάθε φορά που εμφανίζονται κενά, ελλείψεις ή οργανωτικές αλλαγές που μπορεί να προκύψουν από πολιτικούς, οικονομικούς, κοινωνικούς, τεχνολογικούς, νομικούς ή περιβαλλοντικούς παράγοντες. Το σχέδιο θα πρέπει να θέτει κατάλληλα και σχετικά μέτρα επιτήρησης και ελέγχου που θα εφαρμόζονται σε ολόκληρο τον κύκλο ζωής κάθε περιουσιακού στοιχείου λιμένα, δηλαδή τον έλεγχο και τη διαχείριση του λιμένα και του ελέγχου, τον τελωνειακό και συνοριακό έλεγχο, την παραλαβή εμπορευμάτων, την αποθήκευση και τον χειρισμό και τις εγκαταστάσεις αλυσίδας εφοδιασμού. Τα μέτρα αυτά θα πρέπει να περιλαμβάνουν την εφαρμογή κάθε κανονισμού ασφαλείας και διαδικασιών που επηρεάζουν τα περιουσιακά στοιχεία του λιμένα.

ΒΙΒΛΙΟΓΡΑΦΙΑ/ΙΣΤΟΣΕΛΙΔΕΣ

- MaritimeCyberSecurityWhitePaper (ESC) (https://www.safety4sea.com/wp-content/uploads/2016/02/ESC-White-paper-on-Maritime-Cyber-Security-2016_02.pdf)
- https://en.wikipedia.org/wiki/Ransomware
- https://en.wikipedia.org/wiki/Broadband
- https://www.kaspersky.com/resource-center/definitions/spear-phishing
- https://www.slideshare.net/GeorgePouraimis/maritime-cyber-security
    - https://www.techopedia.com/definition/13835/patch-management
- https://en.wikipedia.org/wiki/Adaptive_Server_Enterprise
- https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html
- Lloyd's Cyber Attack strategy.Pdf
- https://el.wikipedia.org/wiki/Κυβερνοχώρος
- Ασφάλεια στον κυβερνοχώρο-Προκλήσεις και προοπτικές (Δρ. Ιλιάνα Σταύρου) http://www.uclancyprus.ac.cy/en/courses/school-sciences/news/asfaleia-ston-kybernoxwro-proklhseis-kai-prooptikes/
- https://guardian.ng/technology/csean-decries-increasing-cyber-attack-threats-in-nigeria/
- Hazard publication 3 CYBER SECURITY IN PORTS-JENNA AHOKAS TUOMAS KIISKI https://www.utu.fi/en/sites/hazard/publications/Documents/HAZARD%20Publication%203%20CYBERSECURITY%20IN%20PORTS.pdf