
CYBER SECURITY
FUTURE
INFORMATION
CONNECTION
DATA
WWW
AREA
CONTACT
INFO
ELECTRONIC
RELATION
SPEED
GLOBAL
TECHNOLOGY


CYBER
SECURITY
AWARENESS

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΝΑΥΣΙΠΛΟΙΑ

Ο ΔΙΤΤΟΣ ΡΟΛΟΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

ΣΤΗΝ ΝΑΥΤΙΛΙΑ

Η ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΝΑΥΣΙΠΛΟΙΑ

Οι επικοινωνίες στην ναυτιλία είναι ένα θέμα που απασχολεί την ναυτιλιακή βιομηχανία εδω και πάρα πολλά χρόνια.

Οι δορυφορικές συνδέσεις απαιτούν μεγάλο κόστος και επιβαρύνεται το πλοίο και οι ναυτικοί ειδικά σε κάποιες περιπτώσεις σε μεγάλο βαθμό σε σχέση με το κόστος των παράκτιων επικοινωνιών.

Εδώ θα ήθελα να επισημάνω ότι στην εταιρεία που εργάζομαι το διαδίκτυο είναι δωρεάν σε όλο το πλήρωμα.

Τα παλαιότερα χρόνια περίπου λίγο πριν το 2000 για την μεταφορά των δεδομένων χρησιμοποιούσαμε TELEX η και FAX όπου την τελευταία δεκαετία έκανε δειλά δειλά την εμφάνιση του το διαδίκτυο στα πλοία για επικοινωνία μέσω e-mail.

Όλος ο όγκος εργασίας του πλοίου γινόταν πια μέσω του διαδικτύου με πάρα πολύ αργούς ρυθμούς και σε μεγάλο φυσικά κόστος λόγο των δεδομένων που αποστέλλονταν.

Οι ταχύτητες ήταν πάρα πολύ χαμηλές και το μηνιαίο κόστος πολλαπλάσιο σε σχέση με αυτές που είχαμε στα σπίτια μας.
Υπάρχει μεγάλο χάσμα μεταξύ των θαλασσίων και παρακτίων επικοινωνιών το οποίο αυξάνεται χρόνο με το χρόνο και η ψαλίδα όλο και μεγαλώνει.
Τα πακέτα παροχής των εταιριών στην στεριά όλο και αυξάνονται σε όγκο και μειώνονται σε τιμή ενώ στην θάλασσα παραμένουν ακριβά ιδιαιτέρως για τον ναυτικό.

Ενδεικτικό να σας πω ότι η εμπορική ναυτιλία μεταφέρει περίπου το 90% των εμπορευμάτων σε παγκόσμιο επίπεδο και συμβάλει στην ανάπτυξη της παγκόσμιας διεθνούς οικονομίας.
Υπάρχουν διάφορα συστήματα που έχουν τοποθετηθεί στα πλοία για να μας παρέχουν διαδίκτυο αλλά είναι ακόμη όπως είπαμε και πριν πάρα πολύ δαπανηρά.
Ελπίζουμε ότι στο μέλλον θα είναι προσιτό σε όλους τους ναυτικούς.

Οι νέοι ναυτικοί που δουλεύουν σήμερα στα πλοία όλο και περισσότερο επιζητούν / απαιτούν το διαδίκτυο στην καθημερινότητα τους διότι κατά πρώτο μεγάλωσαν με αυτό και το χρησιμοποιούν από πολύ μικρή ηλικία και κατά δεύτερο έχουν άμεση επαφή με τα αγαπημένα τους πρόσωπα σε όποια μεριά του πλανήτη και να βρίσκονται σε οποιαδήποτε ώρα το επιθυμούν. Οι στατιστικές λένε ότι περίπου το 68% των κατωτέρων πληρωμάτων και το 28% των αξ/κων δεν έχουν πρόσβαση ούτε καν σε e-mail.

Τον τελευταίο χρόνο υπάρχει έντονη κινητικότητα στην βιομηχανία των θαλασσίων επικοινωνιών με αρκετά μεγάλο ενδιαφέρων από πλοιοκτήτες όπου και στα περισσότερα νέα πλοία εγκαθιστούν γρήγορο διαδίκτυο μιας και τα περισσότερα από αυτά δουλεύουν με ECDIS και σε μεγάλο βαθμό σαν PAPERLESS. Σε αυτές τις περιπτώσεις η χρήση του επιβάλλεται μιας και μπορούμε σε καθημερινή βάση να ανανεώνουμε την βάση δεδομένων των ηλεκτρονικών χαρτών.

Μπορούμε επίσης να αποστέλλουμε ημερήσιες πληροφορίες ως προς την κίνηση κατανάλωση της μηχανής , διάφορες πληροφορίες για τις πιέσεις των εξωτερικών γραμμών φορτίου σε έναν τερματικό σταθμό σε πραγματικό χρόνο η ακόμη και προς την πορεία του πλοίου με τα διάφορα προγράμματα καιρού που υπάρχουν για εξοικονόμηση εργατοώρας καύσιμων και μιλιών.

Με λίγα λόγια σε καλύτερη εκμετάλλευση πλοίου άρα και σε μεγαλύτερα κέρδη.

Με όλα αυτά τα γρήγορα συστήματα που έχουν δημιουργηθεί και την τεχνολογία υπάρχει η ανάγκη στις εταιρείες επανδρώσεως εξειδικευμένων τμημάτων IT και τεχνικών ηλεκτρονικών υπολογιστών ώστε να παρέχουν άμεσες πληροφορίες και τεχνική υποστήριξη σε τυχών προβλήματα που προκύπτουν είτε στο πλοίο είτε στην στεριά.

Με όλα αυτή όμως την γρήγορη και αλματώδη ανάπτυξη καταλαβαίνεται ότι μεγαλώνει και η απειλή για την ναυτιλία από διάφορους κακόβουλους εισβολείς όπου και θα δούμε αμέσως μετά.

ΚΥΒΕΡΝΟ – ΑΣΦΑΛΕΙΑ / ΑΠΕΙΛΕΣ ΚΑΙ ΚΙΝΔΥΝΟΙ

Η ανταλλαγή των ηλεκτρονικών δεδομένων ανάμεσα στο πλοίο και την ακτή έχει αυξηθεί σημαντικά την τελευταία δεκαετία. Η χρήση των συστημάτων απομακρυσμένης παρακολούθησης, διάγνωσης και απομακρυσμένης αποκατάστασης θα συνεχίσει να αυξάνεται στη Ναυτιλία, καθώς επίσης η ανταλλαγή πληροφοριών ανάμεσα στα πλοία και τις αρχές, στους παρόχους υπηρεσιών, στους ναυλωτές και στους πλοιοκτήτες/διαχειριστές.

Ευάλωτα και πολύ σημαντικά τα συστήματα του πλοίου απαιτούν ενημερώσεις και υποστήριξη μέσω διαδικτυακής τεχνολογίας ώστε τα πλοία να μπορούν συχνότερα να συνδέονται στον παγκόσμιο ιστό (π.χ. ECDIS, Engine Maintenance Systems κ.α.) Από την άλλη πλευρά οι εταιρείες έχουν αναπτύξει τμήματα IT για να υποστηρίζουν ενέργειες που μπορούν να γίνουν από την στεριά και την διαχείριση των αναγκών των πλοίων που χρειάζονται συνδέσεις στο διαδίκτυο και επικοινωνία.

Η παρατεταμένη χρήση της ανταλλαγής ηλεκτρονικών δεδομένων αυξάνει την πιθανότητα των κυβερνό – επιθέσεων σε ποικιλία, συχνότητα και πολυπλοκότητα. Αυτές μπορεί να προέλθουν από ένα USB stick που εισάγει κακόβουλο λογισμικό για απόκτηση εμπιστευτικών εμπορικών πληροφοριών, καθώς και από ένα e-mail με λεπτομερείς πληροφορίες του πλοίου που στέλνονται σε άγνωστους

παραλήπτες έως και την πλήρη ανατροπή της βάσης δεδομένων του συστήματος ΙΤ της εταιρείας, ή την προοπτική κατάρρευσης των συστημάτων του πλοίου. Ο αριθμός των πιθανών επικίνδυνων σεναρίων είναι σημαντικός και αυξάνεται. Εγκληματίες εξαγοράζουν οποιαδήποτε πειρατική τεχνολογία που είναι εφαρμόσιμη και συχνά προσαρμοζόμενη σε συγκεκριμένους στόχους.

Υπάρχουν δύο κατηγορίες κυβερνο- επιθέσεων που μπορεί να επηρεάσουν τόσο τις εταιρείες όσο και τα πλοία:

1. Μη συγκεκριμένου στόχου επιθέσεις, όπου μια εταιρεία ή το σύστημα ενός πλοίου και τα δεδομένα είναι ένας από τους πιθανούς στόχους. Αυτές οι επιθέσεις χρησιμοποιούν συνηθισμένη τεχνολογία για να εντοπίσουν γνωστές αδυναμίες συνηθισμένες για πολλές εταιρείες ή πλοία.

2. Στοχευμένες επιθέσεις, όπου μια εταιρεία ή τα συστήματα ενός πλοίου και τα δεδομένα είναι ο επιδιωκόμενος στόχος. Αυτές οι επιθέσεις χρησιμοποιούν πιο προηγμένη τεχνολογία και εργαλεία ειδικά ανεπτυγμένα για να βλάψουν ένα συγκεκριμένο στόχο (εταιρεία ή πλοίο).

Πιθανοί εισβολείς που μπορούν να κάνουν μια κυβερνο-επίθεση μπορεί να είναι καιροσκόποι (για την πρόκληση), Ακτιβιστές (για την ανεπανόρθωτη ζημιά ή δυσλειτουργία των διαδικασιών), Εγκληματίες (για κέρδη) ή τρομοκράτες(για πολιτικά οφέλη).

Σχεδόν όλες οι κυβερνο- επιθέσεις έχουν τα ίδια στάδια ανάπτυξης:

1. Έρευνα – συγκέντρωση πληροφοριών και ανάπτυξη της μεθόδου επίθεσης.
2. Παράδοση -- το εργαλείο της επίθεσης παραδίδεται στο σύστημα της εταιρείας ή του πλοίου.
3. Παραβίαση- απόκτηση πρόσβασης στο σύστημα.
4. Επίδραση – Τα αποτελέσματα της επίθεσης.

Όλα τα παραπάνω μπορούν να παράγουν ποικίλα αποτελέσματα εναντίον της Εταιρείας ή πλοία όπως η καταστροφή των δεδομένων ή έκδοση εμπιστευτικών δεδομένων, δυσλειτουργία του συστήματος, προσοχή των ΜΜΕ (σπίλωση της φήμης) ανεπιθύμητο τίμημα (λύτρα, διόρθωση κόστους κ.λ.π.)

Η αντίδραση του κλάδου

Ο κλάδος με σκοπό να προετοιμαστεί για πιθανή κυβερνο- επίθεση πρόσφατα ξεκίνησε να κάνει τα πρώτα του βήματα για την αντιμετώπισή τους. Τον Μάρτιο του 2015 κατά την διάρκεια της 95ης επιτροπής, ICS, BIMCO, INTERTANKO και INTERCARGO πρότειναν ένα προσχέδιο κατευθυντήριων γραμμών σχετικά με υπολογισμούς για βελτίωση της ναυτικής ασφάλειας και κατευθυντήριες γραμμές για κυβερνο- ασφάλεια εν πλω, καλώντας την Επιτροπή λαμβάνοντας υπ’ όψη το θέμα.

Τον Ιανουάριο του 2016 το **USCG** έκανε λόγο για δυο κυβερνο- ενημερωτικά δελτία (MCB 001- 16 και MCB 002-16) παρέχοντας καθοδήγηση σε θέματα για λύτρα και διακωμωδώντας την επαγγελματική αλληλογραφία που χρησιμοποιήθηκε για να προσπαθήσει να καταχραστεί τον ναυτιλιακό οργανισμό.

Επιπρόσθετα το **BIMCO** έκανε λόγο για « The Guidelines on Cyber Security onboard Ships» (version 1.0 – Jan.16) παρέχοντας λεπτομερείς πληροφορίες στους πλοιοκτήτες και στους διαχειριστές πώς να αξιολογήσουν τους χειρισμούς τους και να ταξινομήσουν τις απαραίτητες διαδικασίες και ενέργειες για να διατηρήσουν την ασφάλεια στα συστήματα του κυβερνοχώρου στα καράβια που είναι εν πλω.

ΑΠΑΙΤΟΥΜΕΝΕΣ ΕΝΕΡΓΕΙΕΣ

Η εφαρμογή της κατάλληλης άμυνας περιλαμβάνει διεξοδικούς ελέγχους, όπως:

- Εγκατάσταση antivirus λογισμικών.
- Πολιτική για την ασφαλή λειτουργία και συντήρηση του συστήματος.
- Ασφαλής σχεδιασμός και ανάπτυξη εφαρμογών και συστημάτων.

- Ευαισθητοποίηση των υπαλλήλων που εργάζονται στη ναυτιλιακή βιομηχανία.
- Διασφάλιση των λιμένων που χρησιμοποιούν κατά κύριο λόγο αυτοματοποιημένα συστήματα για τη διακίνηση φορτίων.

Η ναυτιλιακή βιομηχανία θα πρέπει να ακολουθήσει κανόνες και πρότυπα ασφαλείας σε όλα τα επίπεδα της οργάνωσης.

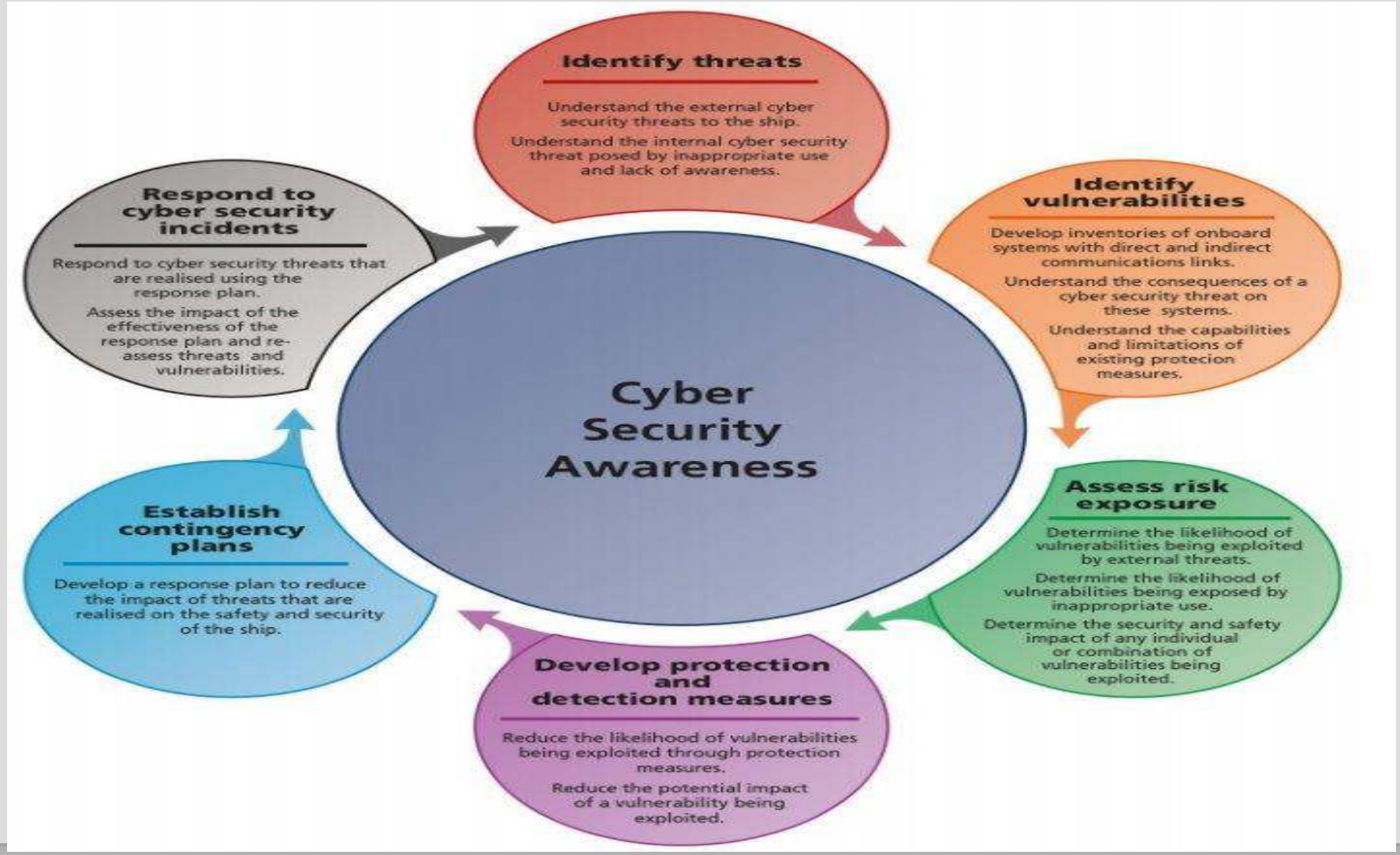
Τι μπορώ να κάνω; Χρήση του ηλεκτρονικού ταχυδρομείου

Σκέψου διπλά πριν το στείλεις!

- Το εταιρικό e-mail είναι ένα εργαλείο προγραμματισμένο για δουλειές σχετικές με την εταιρεία. Η προσωπική χρήση πρέπει να είναι περιορισμένη.
- Η εταιρική υποδομή δεν πρέπει να χρησιμοποιείται για προσωπικούς σκοπούς.
- Διπλός έλεγχος ότι το e-mail θα σταλεί μόνο στους επιθυμητούς παραλήπτες, μην ξεχάσετε να ελέγξετε τις ηλεκτρονικές διευθύνσεις που έχουν απαντήσει.

- Μην προωθείτε επαγγελματικά e-mail σε προσωπικό λογαριασμό.
- Μην ανοίγετε e-mail ή επισυναπτόμενα αρχεία από άγνωστους αποστολείς.
- Θυμηθείτε ότι κάθε e-mail που στέλνετε θα αποθηκευτεί σε ένα server ΄σε ένα άλλο υπολογιστή κάπου, ακόμη και αν το σβήσετε από τον υπολογιστή ή από οποιαδήποτε άλλη συσκευή.

- Προστατέψτε τα μέσα μεταφοράς των δεδομένων (USB flash drivers- memory sticks, εξωτερικούς σκληρούς δίσκους, DVD- CD) χρησιμοποιώντας μόνο μέσα μεταφοράς εγκεκριμένα από την εταιρεία και ελέγχοντας τα για κακόβουλο λογισμικό.
- Χρήση της τεχνικής social engineering.
- Συνεργασία με έμπιστους ανθρώπους.
- Προσοχή στην χρήση των μέσων κοινωνικής δικτύωσης.


Identify threats
Understand the external cyber security threats to the ship.
Understand the internal cyber security threat posed by inappropriate use and lack of awareness.
Identify vulnerabilities
Develop inventories of onboard systems with direct and indirect communications links.
Understand the consequences of a cyber security threat on these systems.
Understand the capabilities and limitations of existing protecion measures.
Assess risk exposure
Determine the likelihood of vulnerabilities being exploited by external threats.
Determine the likelihood of vulnerabilities being exposed by inappropriate use.
Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.
Develop protection and detection measures
Reduce the likelihood of vulnerabilities being exploited through protection measures.
Reduce the potential impact of a vulnerability being exploited.
Establish contingency plans
Develop a response plan to reduce the impact of threats that are realised on the safety and security of the ship.
Respond to cyber security incidents
Respond to cyber security threats that are realised using the response plan.
Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
Cyber Security Awareness

Οι 6 παρακάτω βασικοί πυλώνες καθοδήγησης των **BIMCO/ CLIA / ICS/ INTERTANKO/INTERCARGO** ως προς την ενημέρωση της κυβερνο- ασφάλειας.

1. Αναγνωρίστε τον κίνδυνο.
2. Αναγνωρίστε την τρωτότητα
3. Αποτιμήστε την επικινδυνότητα.
4. Αναπτύξτε προστατευτικά και ανιχνευτικά μέτρα.
5. Δημιουργήστε σχέδιο εκτάκτου ανάγκης.
6. Ανταποκριθείτε σε περιστατικό κυβερνο- ασφάλειας.

ΠΗΓΕΣ – ΒΙΒΛΙΟΓΡΑΦΙΑ

USCG : MCB 001- 16 και MCB 002-16

BIMCO, CLIA, ICS, INTERTANKO και INTERCARGO :

“THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS”

SAFETY4SEA

Άδωνης Βιολάρης (Κυπριακό ναυτικό επιμελητήριο)

ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ!

Capt. Παναγιώτης Γιγής μέλος Δ.Σ. ΠΕΠΕΝ

Instructor at Delphic Maritime training center of Angelicoussis Group.

ΤΕΛΟΣ