ALPHA MARINE CONSULTING P.C.

MARINE CONSULTANTS & SURVEYORS
T: +30 211 888 1000, F: +30 211 8881039
mail@alphamrn.com | www.alphamrn.com

DIAPLOUS Cyber

MARITIME CYBER RISK REDUCER
T: +30 216 600 7557, F: +30 210 410 1070
info@diaplous-cyber.com | www.diaplous-ms.com

WEBINAR - 21.12.2020

CYBER SECURITY IN THE MARITIME ENVIRONMENT

Questions & Answers (Q&A)

1. Πόσο χρήσιμο και απαραίτητο είναι το penetration test;

Το penetration test είναι απαραίτητο εργαλείο για κάθε εταιρεία, προκειμένου να εντοπιστούν τα τρωτά σημεία των IT και OT συστημάτων της αφού προσφέρει τη δυνατότητα να εντοπιστούν όλες οι επιπτώσεις από μια κυβερνοεπίθεση. Είναι επίσης το πλέον χρήσιμο εργαλείο εκτίμησης κινδύνου (risk assessment) καθώς, από τεχνικής απόψεως, θα μας δώσει πληρέστερη πληροφόρηση από οποιαδήποτε άλλη μέθοδο προσέγγισης και εκτίμησης αδυναμιών.

Το penetration test πρέπει να γίνεται στην εταιρεία και τουλάχιστον σε ένα ποσοστό του στόλου της. Για να γίνει σωστή εκτίμηση κινδύνου, πρέπει να επικεντρώνεται ξεχωριστά στο κάθε σύστημα, ώστε να υποδεικνύει τα κενά ασφαλείας που μπορεί να έχει το συγκεκριμένο σύστημα σε επίπεδο input/output data, χωρίς να κινδυνεύει η ομαλή και απρόσκοπτη λειτουργία της εταιρείας ή του πλοίου.

Με βάση τα αποτελέσματά του, η εταιρεία πρέπει να υιοθετήσει τις απαραίτητες διορθωτικές ενέργειες, ώστε να αντιμετωπίσει με επιτυχία τα κενά που εντοπίστηκαν.

Το penetration test πρέπει να επαναλαμβάνεται σε τακτά χρονικά διαστήματα για να επιβεβαιώνεται κάθε φορά η αποτελεσματικότητα των διορθωτικών ενεργειών που υιοθετούνται.

Πρέπει να σημειωθεί ότι οι ναυλωτές και, κυρίως, οι εταιρείες πετρελαιοειδών, απαιτούν πλέον κατά τη διάρκεια των TMSA Office Audits τη διενέργεια penetration test τόσο στην εταιρεία όσο και στα πλοία.

2. Ποια είναι η κατάσταση με τις ασφαλιστικές εταιρείες και τους underwriters; Το cyber security καλύπτεται από τα υπάρχονται ασφαλιστικά συμβόλαια;

Αυτή τη στιγμή, σε σχέση με το cyber security, η ασφαλιστική αγορά είναι υπό διαμόρφωση. Το βέβαιο είναι ότι θα προκύψουν νέα προϊόντα για την ασφάλιση έναντι μιάς κυβερνοεπίθεσης.

Κάθε ναυτιλιακή εταιρεία θα πρέπει να αποδείξει ότι έχει διενεργήσει «due diligence» προκειμένου να μπορεί να ασφαλιστεί. Η ασφαλιστική εταιρεία πρέπει να γνωρίζει πώς ενεργεί η εταιρεία, προκειμένου να διασφαλίσει την κυβερνοασφάλεια, τα μέτρα προστασίας που έχει υιοθετήσει και εάν διαθέτει επαρκείς διαδικασίες και μηχανισμούς αντιμετώπισης πιθανού περιστατικού κυβερνοεπίθεσης.

Εκτιμάται ότι το ύψος του σχετικού ασφαλίστρου θα διαμορφώνεται με βάση τα παραπάνω.

3. Χρειάζεται οι εταιρείες να διαθέτουν IT/OT inventory;

Η ύπαρξη και τήρηση λεπτομερών IT/OT inventory είναι σημαντική απαίτηση, σύμφωνα με τις οδηγίες που έχουν εκδοθεί τόσο από τους Νηογνώμονες όσο και από τους διάφορους φορείς της ναυτιλιακής βιομηχανίας.

Σύμφωνα με το σχετικό IMO Resolution: «*Information technology and operational technology systems should be considered The protection of information and data exchange within the IT/OT systems should also be considered.... Every Company must* ***identify*** *the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.*

Τα IT/OT inventories πρέπει όχι μόνο να υπάρχουν, αλλά και να ανανεώνονται συνεχώς, ώστε να καταγράφονται σε αυτά όλες οι αλλαγές που μπορεί να έχουν προκύψει εν τω μεταξύ στο πλοίο ή την εταιρεία.

Η αξιοπλοϊα του πλοίου είναι πλέον συνυφασμένη με την προστασία των συστημάτων του που συνδέονται με την ασφάλεια, ναυσιπλοία, κλπ.

4. Έχουν ξεκινήσει οι ναυλωτές να απαιτούν την εισαγωγή συγκεκριμένων όρων στα ναυλοσύμφωνα;

Τα τελευταία χρόνια, γίνονται πολλές συζητήσεις στην BIMCO αναφορικά με τον καθορισμό των απαιτήσεων που θα περιλαμβάνονται στα ναυλοσύμφωνα. Πρόσφατα, οι μεγάλες εταιρείες πετρελαιοειδών άρχισαν να προβλέπουν ειδικό όρο στα ναυλοσύμφωνα, σχετικό με την κυβερνοασφάλεια. Απαιτούν, δηλαδή, την αναγραφή στα ναυλοσύμφωνα όρων σχετικά με τη διενέργεια penetration test στο γραφείο και το πλοίο, την ύπαρξη συγκεκριμένων διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας και την αντιμετώπιση περιστατικών κυβερνοεπίθεσης, καθώς και την υποχρέωση άμεσης ενημέρωσης του ναυλωτή και των αρμόδιων αρχών, της σημαίας κλπ.

Η άποψή μας είναι ότι σύντομα όλα τα ναυλοσύμφωνα θα περιλαμβάνουν αυτή την απαίτηση.

5. Ποιός είναι ο ρόλος που διαμορφώνεται για το τμήμα IT Department, είτε είναι in house είτε όχι και ποιά είναι η διασύνδεσή του με τα υπόλοιπα τμήματα της εταιρείας;

Συνήθως σε μια ναυτιλιακή εταιρεία ο ρόλος του IT Department δεν είναι κομβικός, αφού δεν έχει (ακόμη) κεντρική θέση στη διασφάλιση του business continuity της εταιρείας και δεν συμμετέχει ενεργά στα κέντρα λήψης αποφάσεων.

Με τις νέες απαιτήσεις, ο ρόλος του συγκεκριμένου τμήματος γίνεται κεντρικός και αποκτά στενή διασύνδεση με όλα τα υπόλοιπα τμήματα της εταιρείας και τα πλοία. Κατά τη γνώμη μας, η διοίκηση της κάθε εταιρείας πρέπει να αντιληφθεί το νέο τοπίο που διαμορφώνεται σε θέματα κυβερνοάμυνας και να αναβαθμίσει το ρόλο του IT Department.

Απο την άλλη πλευρά, και οι εργαζόμενοι του τμήματος οφείλουν να αντιληφθούν τις νέες προκλήσεις του ρόλου τους, που υπερβαίνουν τον αποκλειστικά τεχνικό/υποστηρικτικό ρόλο και απαιτούν «ολιστική» προσέγγιση και ικανότητα. Πρέπει να διαμορφώσουν μιά νέα κουλτούρα μέσα από πρακτικές και διαδικασίες, που θα πρέπει να εμπεδωθούν σε όλα τα επίπεδα της εταιρείας, να γίνουν αποδεκτές από όλο το προσωπικό και να διασυνδεθούν με όλες τις υπολοιπες διαδικασίες που ακολουθεί η εταιρεία.

Το cyber security πρέπει να γίνει μέρος της καθημερινής λειτουργίας της εταιρείας και να ενσωματωθεί στο Σύστημα Ασφαλούς Διαχείρισης. Αυτό απαιτεί το «commitment» της Διοίκησης της εταιρείας.

Με βάση τα παραπάνω, πιστεύουμε ότι πρέπει να ενδυναμωθεί ο ρόλος του IT Department και του Information Security Officer της κάθε εταιρείας, που δεν είναι απαραίτητο να έχει σχέση με τον ρόλο του Company Security Officer. Τα καθήκοντα και οι αρμοδιότητες των εργαζομένων πρέπει να είναι καταγεγραμμένα λεπτομερώς, με έμφαση στην αντιμετώπιση κινδύνων και τη διαχείρηση κρίσεων.

Για να είναι αποτελεσματικός ο ρόλος αυτός, απαιτείται η συνεργασία του IT Department με τα υπόλοιπα τμήματα της εταιρείας. Αυτό σημαίνει ότι αντίστοιχα καθήκοντα πρέπει να ανατεθούν σε όλους τους εργαζομένους (ομάδα αντιμετώπισης περιστατικών έκτακτης ανάγκης, κλπ), ώστε όλοι οι συμμετέχοντες να ασκήσουν με επιτυχία τα καθηκοντά τους, έχοντας ως στόχο την αντιμετώπιση κάθε σχετικού περιστατικού με τις κατά το δυνατόν μικρότερες συνέπειες και την γρήγορη επιστροφή στην κανονικότητα.

6. Ποιές είναι οι απαιτήσεις των διαφόρων Port State Control Authorities και της US Coast Guard αναφορικά με την εφαρμογή των διαδικασιών κυβερνοασφάλειας;

Η USCG πρόσφατα υιοθέτησε σχετικές απαιτήσεις βάσει των οποίων θα ελέγχει τις σχετικές διαδικασίες κυβερνοασφάλειας καθώς και αν αυτές εφαρμόζονται σε κάθε πλοίο κατά τη διάρκεια των επιθεωρήσεων που διεξάγει. Είναι δεδομένο ότι όλα τα Port State Control Authorities θα εκδώσουν αντίστοιχες οδηγίες προς τους επιθεωρητές τους αναφορικά με τους ελέγχους που πρέπει να διενεργούν.

Τονίζουμε ιδιαίτερα τη σύνδεση του cyber security με την αξιοπλοϊα του πλοίου (seaworthiness).
Ένα πλοίο που δεν τηρεί τους κανονισμούς κυβεροασφάλειας, δεν θα θεωρείται seaworthy.
Αυτό σημαίνει ότι για τους σκοπούς του Port State Control, το cyber security αναδεικνύεται σε βασική και υποχρεωτική παράμετρο, ισοδύναμη με την SOLAS, MARPOL, κλπ.

7. Πώς πρέπει να αντιμετωπίζεται ένα cyber incident; Υπάρχει αναλογία με το τυπικό "marine incident";

Το cyber incident πρέπει να αντιμετωπιστεί ως ένα marine incident, τα δε μέτρα που πρέπει να λαμβάνονται για την αντιμετώπισή του θα είναι ανάλογα με τη σοβαρότητά του.

Πρακτικά, σε κάθε Σύστημα Διαχείρισης πρέπει να υπάρχει κατηγοριοποίηση των συμβάντων βάσει των πραγματικών ή των δυνητικών επιπτώσεων τους. Κάθε κατηγορία συμβάντων θα σηματοδοτεί καθορισμένες ενέργειες και χρόνους αντίδρασης, την επάνδρωση της ομάδας αντιμετώπισης της κρίσης και άλλες δράσεις από πλευράς εταιρείας και πλοίου. Έτσι απαιτείται η κοινοποιηση π.χ. περιστατικών που ανήκουν στην υψηλότερη κατηγορία, στους ναυλωτές, τη Σημαία του πλοίου και σε άλλες αρμόδιες αρχές, που θεωρείται ότι πρέπει να ενημερωθούν για το συγκεκριμένο περιστατικό.

Προκύπτει, επομένως, η υποχρέωση κάθε εταιρείας να οργανώσει ένα Σχέδιο Αντιμετώπισης Κρίσεων και Περισταστικών Κυβερνοεπιθέσεων (Response Plan), το οποίο θα πρέπει να συνδυαστεί με το ήδη υπάρχον Σύστημα Αντιμετώπισης Κρίσεων (Emergency Response Plan).

Παράλληλα πρέπει να αναφέρουμε τα υποχρεωτικά ετήσια γυμνάσια και ασκήσεις ετοιμότητας τα οποία μπορούν να συνδυάζονται με τα penetration test που προαναφέραμε.

Γίνεται, λοιπόν, προφανές ότι η επιτυχία της αντιμετώπισης μιας κυβερνοεπίθεσης εξαρτάται από την εκπαίδευση και την ετοιμότητα των συμμετεχόντων και την εξοικείωση με τις διαδικσίες και τις υποχρεώσείς τους.

8. Μπορεί να υπάρξει κάποια καθυστέρηση στην ημερομηνία εφαρμογής της νέας νομοθεσίας αναφορικά με το cyber security;

Δεν υπάρχει καμμία πληροφορία για κάποια παράταση του κανονισμού του IMO που είναι σε ισχύ από 1/1/2021.

9. Ποιά είναι τα πλεονεκτήματα που παρέχει η συνεργασία της DIAPLOUS-CYBER με την ALPHA MARINE CONSULTING;

Η συνεργασία μας στοχεύει στην ολιστική λύση θεμάτων κυβερνοασφάλειας στη ναυτιλία.
Παρέχουμε υψηλού επιπέδου πρωτοπόρες υπηρεσίες και μεθοδολογίες, που έχουν σκοπό όχι μόνον την απλή «συμμόρφωση» αλλά και τη συνεχή (24x7) υποστήριξη των ναυτιλιακών εταιρειών σε κάθε επίπεδο. Η συνεργασία μας συνδυάζει την βαθειά και πολυτετή γνώση και εμπειρία που έχει η κάθε μία εταιρεία στους τομείς δραστηριότητάς της.

Οι υπηρεσίες που παρέχουμε μπορούν να συνδυαστούν με τους περισσότερους επίσημους προμηθευτές συστημάτων IT/OT. Βεβαίως, σημαντικό ρόλο παίζουν τα χαρακτηριστικά των ήδη

εγκατεστημένων συστημάτων (π.χ. το μοντέλο, κατασκευαστής, κτλ.). Η συνεργασία των εταιρειών μας μάς επιτρέπει να καλύψουμε το πεδίο της κυβερνοασφάλειας, χρησιμοποιώντας όλα τα εγκατεστημένα συστήματα.

10. Περιμένουμε από τα Flag States οδηγίες για την εφαρμογή των cyber regulations;

Θεωρούμε βέβαιο ότι οι περισσότερες ναυτιλιακές σημαίες θα εκδώσουν ή έχουν ήδη εκδώσει επιμέρους οδηγίες. Οι οδηγίες αυτές στοχεύουν σε αυτό που ονομάζουμε «compliance». Ωστόσο, οι πιο σημαντικές απαιτήσεις θα προέλθουν από τους ναυλωτές/Oil Majors και την ασφαλιστική αγορά.

Τέλος, δεν πρέπει να ξεχνάμε ότι αυξημένες απαιτήσεις έχουν ήδη περιληφθεί όχι μόνον στα TMSA αλλά και στα DBMS για τα Φορτηγά πλοία.

Contact

For more information about DIAPLOUS-CYBER, please:

- Visit our website and subscribe our newsletter at https://diaplous-ms.com/index.php/cyber-security/
- E-mail us at info@diaplous-cyber.com
- Call us at +30 216 600 7500 (standard working hours, UTC+2)

For more information about ALPHA MARINE CONSULTING, please:

- Visit our website: https://alphamrn.com/
- Email us at: mail@alphamrn.com
- Call us at: Tel: +30 211 888 1000 (standard working hours, UTC+2)