Εισαγωγή στη Διαχείριση Κινδύνων στην Κυβερνοασφάλεια στη Ναυτιλία

CSP001_S_M

ΠΑΡΟΥΣΙΑΣΗ:
ΠΗΝΕΛΟΠΗ ΚΥΡΑΝΟΥΔΗ, ΕΡΕΥΝΗΤΡΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
ΝΙΝΕΤΑ ΠΟΛΕΜΗ, ΚΑΘΗΓΗΤΡΙΑ, ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

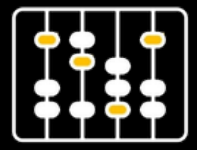
Project Agreement no. 101083594

Στόχοι: Ποιος-Τι-Γιατί πρέπει να παρακολουθήσουν αυτή την εκπαίδευση

ΠΟΙΟΣ

Επαγγελματίες στον τομέα των ναυτιλιακών και λιμενικών δραστηριοτήτων, της κυβερνοασφάλειας και της διαχείρισης σε περιβάλλοντα IT, OT, IoT και εφοδιαστικής αλυσίδας

ΤΙ



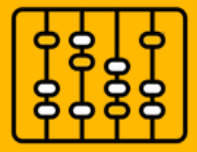
Σεμινάριο σχετικά με τη διαχείριση κινδύνων στον τομέα της κυβερνοασφάλειας και την πιστοποίηση σε ναυτιλιακά συστήματα, το οποίο καλύπτει πρότυπα, ελέγχους και ασφάλεια της εφοδιαστικής αλυσίδας

ΓΙΑΤΙ

Να δώσει τη δυνατότητα στους συμμετέχοντες να αξιολογούν τους κινδύνους, να υποστηρίζουν την πιστοποίηση και να διασφαλίζουν ασφαλείς και ανθεκτικές ναυτιλιακές δραστηριότητες

CSP Εκπαίδευση Υλικοτεχνική υποστήριξη:

ΠΟΤΕ



Χρονοδιάγραμμα (θα αναρτηθεί στην πλατφόρμα DCM)

ΠΟΥ

Φυσικά, εικονικά ή και τα δύο (θα αναρτηθεί στην πλατφόρμα DCM)

ΠΩΣ

Σεμινάριο με εκπαιδευτή

Προσφορά αξίας

Οφέλη για τους συμμετέχοντες

- Επίπεδο εκπαίδευσης: Προχωρημένο
- Επαγγελματική εκπαίδευση στον τομέα της κυβερνοασφάλειας
- Βασισμένο στο Ευρωπαϊκό Πλαίσιο Δεξιοτήτων για την Κυβερνοασφάλεια (ECSF)
- Πρωτοποριακές γνώσεις από εμπειρογνώμονες του κλάδου και του ακαδημαϊκού χώρου
- Πιστοποιητικό ολοκλήρωσης
- Βοηθά στην ανάπτυξη δεξιοτήτων και στην επαγγελματική εξέλιξη

TI

Θέματα εκπαίδευσης

- Εισαγωγή στην Κυβερνοασφάλεια στη Ναυτιλία
- Κατανόηση των Κυβερνοκινδύνων στη Ναυτιλία
- Πρότυπα και Βέλτιστες Πρακτικές στον Τομέα της Κυβερνοασφάλειας
- Πιστοποίηση στην Κυβερνοασφάλεια στη Ναυτιλία

ΓΙΑΤΙ

Μαθησιακά αποτελέσματα

Γνώσεις:

- Κατανόηση των απειλών για την ασφάλεια στον κυβερνοχώρο που αφορούν ειδικά τον ναυτιλιακό τομέα.
- Εξοικείωση με τα σχετικά πλαίσια, τους κανονισμούς και τα πρότυπα που διέπουν την κυβερνοασφάλεια στον ναυτιλιακό τομέα.
- Γνώση των κυβερνοκινδύνων που επικρατούν στις ναυτιλιακές δραστηριότητες.
- Ενημέρωση σχετικά με μελέτες περιπτώσεων και πραγματικά παραδείγματα συμβάντων κυβερνοασφάλειας στη ναυτιλιακή βιομηχανία.
- Κατανόηση των μεθοδολογιών και των εργαλείων αξιολόγησης κινδύνου που είναι προσαρμοσμένα στον ναυτιλιακό τομέα.
- Κατανόηση της ασφάλειας των πληροφοριών και των ναυτιλιακών εννοιών.
- Κατανόηση των βέλτιστων πρακτικών για την ασφάλεια των συστημάτων IT και OT στον ναυτιλιακό τομέα.
- Γνώση των προτύπων και των συστημάτων πιστοποίησης στον τομέα της κυβερνοασφάλειας που αφορούν ειδικά τον ναυτιλιακό κλάδο.
- Εξοικείωση με βασικές έννοιες που σχετίζονται με την πιστοποίηση στον τομέα της κυβερνοασφάλειας.

Κατανόηση των βέλτιστων πρακτικών για την απόκτηση και τη διατήρηση πιστοποίησης στον τομέα της ναυτιλιακής κυβερνοασφάλειας.

ΠΟΙΟΣ

Προφίλ των εκπαιδευτών

- Η Πηνελόπη Κυρανούδη έχει αποκτήσει μεταπτυχιακό τίτλο σπουδών στην Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων από το Πανεπιστήμιο του Αιγαίου (Τμήμα Μηχανικών Συστημάτων Πληροφοριών και Επικοινωνιών). Διετέλεσε Υπεύθυνη Ασφάλειας Δικτύων και Πληροφοριών στον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), συμβάλλοντας: σε πέντε δημοσιεύσεις στους τομείς της Κυβερνοασφάλειας στη Ναυτιλία, της Ψηφιακής Υγείας και των Εθνικών Στρατηγικών Κυβερνοασφάλειας, στη δημιουργία διαδικτυακών εργαλείων και στην οργάνωση εκδηλώσεων της ΕΕ για την Κυβερνοασφάλεια. Κατά τη διάρκεια της 10ετούς καριέρας της, εργάστηκε επίσης σε διάφορες θέσεις και ρόλους, όπως Προγραμματίστρια Ιστού και Εφαρμογών, Μηχανικός Ασφάλειας Πληροφορικής, Ερευνήτρια Κυβερνοασφάλειας και Λέκτορας σε εταιρείες και οργανισμούς όπως η Express Publishing SA, η Cosmote SA, η Maggioli SpA και το Aegean College, μεταξύ άλλων. Σήμερα πραγματοποιεί τις διδακτορικές της σπουδές στον τομέα της Κυβερνοασφάλειας στο Πανεπιστήμιο Πειραιά (Τμήμα Πληροφορικής). Κατέχει τη θέση της Ερευνήτριας Κυβερνοασφάλειας στο Πολυτεχνείο Κρήτης (Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών), συμβάλλοντας σε ερευνητικά προγράμματα της ΕΕ. Τα ερευνητικά της ενδιαφέροντα εστιάζουν στον τομέα της Κυβερνοφυσικής Ασφάλειας, ιδίως στους τομείς της Ναυτιλίας, του OT/IoT και της Ανάλυσης Απειλών.

- Η Νινέτα Πολέμη είναι καθηγήτρια κυβερνοασφάλειας στο Πανεπιστήμιο Πειραιά-UNIPI- (Εργαστήριο Κυβερνοασφάλειας, Τμήμα Πληροφορικής) και CTO/Συνιδρύτρια της Trustilio. Διετέλεσε (2017-2020) Διευθύντρια Προγράμματος και Υπεύθυνη Πολιτικής στη Γενική Διεύθυνση της Ευρωπαϊκής Επιτροπής (Μονάδα CONNECT H1 με τίτλο «Τεχνολογίες και Δυνατότητες Κυβερνοασφάλειας»). Απέκτησε το Διδακτορικό της στα Εφαρμοσμένα Μαθηματικά (Θεωρία Κωδικοποίησης) από το Πανεπιστήμιο City της Νέας Υόρκης (Μεταπτυχιακό Κέντρο). Διετέλεσε διδάσκουσα και ερευνήτρια στο Πανεπιστήμιο City της Νέας Υόρκης (Κολλέγια Queens & Baruch), στο Κρατικό Πανεπιστήμιο της Νέας Υόρκης (Farmingdale), στο Ελεύθερο Πανεπιστήμιο των Βρυξελλών (ULB)-Solvay Brussels School-. Έχει πάνω από 150 δημοσιεύσεις στον τομέα της ασφάλειας (π.χ. ασφάλεια λιμένων, ασφάλεια στη θάλασσα, ασφάλεια της εφοδιαστικής αλυσίδας στη θάλασσα) και έχει οργανώσει πολυάριθμες επιστημονικές και πολιτικές διεθνείς επιστημονικές εκδηλώσεις κυβερνοασφάλειας. Έχει λάβει πολλές ερευνητικές επιχορηγήσεις (NATO, IEEE) και βραβεία (NSA, MSI Army Research Office IEEE, CYNY, Ελληνικό Υπουργείο Ναυτιλίας, Γενικό Γραφείο Εθνικής Άμυνας) και έχει συμμετάσχει ως Υπεύθυνη Έργου και Τεχνική Διευθύντρια σε περισσότερα από 60 διεθνή, ευρωπαϊκά και εθνικά έργα έρευνας και ανάπτυξης και εμπορικά έργα στον τομέα της κυβερνοασφάλειας. Εργάζεται ως εξωτερική εμπειρογνώμονας/κριτής/σύμβουλος στον ENISA, την Ευρωπαϊκή Επιτροπή (DG CNECT, DG HOME), το ITE, Focal Point.

Περίγραμμα εκπαίδευσης

Θέμα-1: Εισαγωγή στην κυβερνοασφάλεια στον ναυτιλιακό τομέα

Επισκόπηση των απειλών για την κυβερνοασφάλεια στον ναυτιλιακό τομέα

Σημασία της κυβερνοασφάλειας στον ναυτιλιακό τομέα

Εισαγωγή στα σχετικά πλαίσια και κανονισμούς για την κυβερνοασφάλεια (π.χ. κατευθυντήριες γραμμές του ΔΝΟ για τη διαχείριση των κυβερνοκινδύνων)

Θέμα-2: Κατανόηση των κυβερνοκινδύνων στον ναυτιλιακό τομέα

Προσδιορισμός των κυβερνοκινδύνων στις ναυτιλιακές δραστηριότητες

Μελέτες περιπτώσεων και πραγματικά παραδείγματα περιστατικών κυβερνοασφάλειας στη ναυτιλιακή βιομηχανία

Αξιολόγηση κινδύνων έναντι διαχείρισης κινδύνων

Περίγραμμα εκπαίδευσης

Θέμα-3: Πρότυπα και βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας

Επισκόπηση των προτύπων κυβερνοασφάλειας που ισχύουν για τον ναυτιλιακό κλάδο (π.χ. ISO 27001, Πλαίσιο Κυβερνοασφάλειας NIST)

Επισκόπηση των βασικών εννοιών της ασφάλειας πληροφοριών και του ναυτιλιακού τομέα

Βέλτιστες πρακτικές για την ασφάλεια των συστημάτων IT και OT στον ναυτιλιακό τομέα (π.χ. Κατευθυντήριες γραμμές ENISA - Διαχείριση Κυβερνοκινδύνων για Λιμένες, Μεθοδολογία Διαχείρισης Κινδύνων CYSMET)

Θέμα 4: Πιστοποίηση στον τομέα της κυβερνοασφάλειας στη ναυτιλία

Πρότυπα και συστήματα πιστοποίησης στον τομέα της κυβερνοασφάλειας που ισχύουν για τη ναυτιλιακή βιομηχανία (π.χ. Κοινά Κριτήρια, EUCC)

Επισκόπηση των βασικών εννοιών της πιστοποίησης στον τομέα της κυβερνοασφάλειας

Βέλτιστες πρακτικές για την πιστοποίηση της ναυτιλιακής κυβερνοασφάλειας (π.χ. Μεθοδολογία αξιολόγησης κινδύνου και συμμόρφωσης CYRENE)

Βασικές γνώσεις και προαπαιτούμενα

Βασικές γνώσεις:

Βασική κατανόηση των υπολογιστών και των δικτύων

Εξοικείωση με τις συνήθεις απειλές και ευπάθειες ασφάλειας στο διαδίκτυο

Ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια

Προαπαιτούμενα:

Κανένα

Πηγές:

Υλικό αναφορών

1. ISO/IEC 27001:2022, Συστήματαδιαχείρισης ασφάλειας πληροφοριών — Απαιτήσεις
2. ISO/IEC 27005:2018, Διαχείριση κινδύνωνασφάλειας πληροφοριών
3. ISO/IEC 15408, Κοινά Κριτήρια γιατην Αξιολόγηση της Ασφάλειας της Τεχνολογίας Πληροφοριών
4. ISO/IEC 18045, Κοινή μεθοδολογία αξιολόγησης για την αξιολόγηση της ασφάλειας της τεχνολογίας πληροφοριών
5. NIST SP 800-30 Rev. 1, Οδηγός για τη διεξαγωγή αξιολογήσεων κινδύνου
6. NIST SP 800-37 Rev. 2, Πλαίσιο διαχείρισης κινδύνων για συστήματα πληροφοριών και οργανισμούς
7. NIST SP 800-82 Rev. 2, Οδηγός για την ασφάλεια των βιομηχανικών συστημάτων ελέγχου (ICS)
8. NIST, Πλαίσιο Κυβερνοασφάλειας (CSF) 2.0
9. Σειρά IEC 62443, Ασφάλεια για συστήματα βιομηχανικού αυτοματισμού και ελέγχου
10. Διεθνής Ναυτιλιακός Οργανισμός (IMO), Κατευθυντήριες γραμμές για τη διαχείριση των κυβερνοκινδύνων στη ναυτιλία
11. ENISA, Βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο στον ναυτιλιακό τομέα
12. ENISA, Κατευθυντήριες γραμμές για τη διαχείριση των κυβερνοκινδύνων στους λιμένες
13. ENISA, Το τοπίο των απειλών στις μεταφορές
14. Ευρωπαϊκή Ένωση, EUCC (Ευρωπαϊκό Σύστημα Πιστοποίησης Κυβερνοασφάλειας)
15. Έργο CYRENE, Μεθοδολογία αξιολόγησης κινδύνων και συμμόρφωσης για τις ναυτιλιακές αλυσίδες εφοδιασμού
16. Frontiers in Computer Science, Μεθοδολογία διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας για συστήματα εφοδιαστικής αλυσίδας (CYSMET), 2023

Πρόοδος μαθήματος

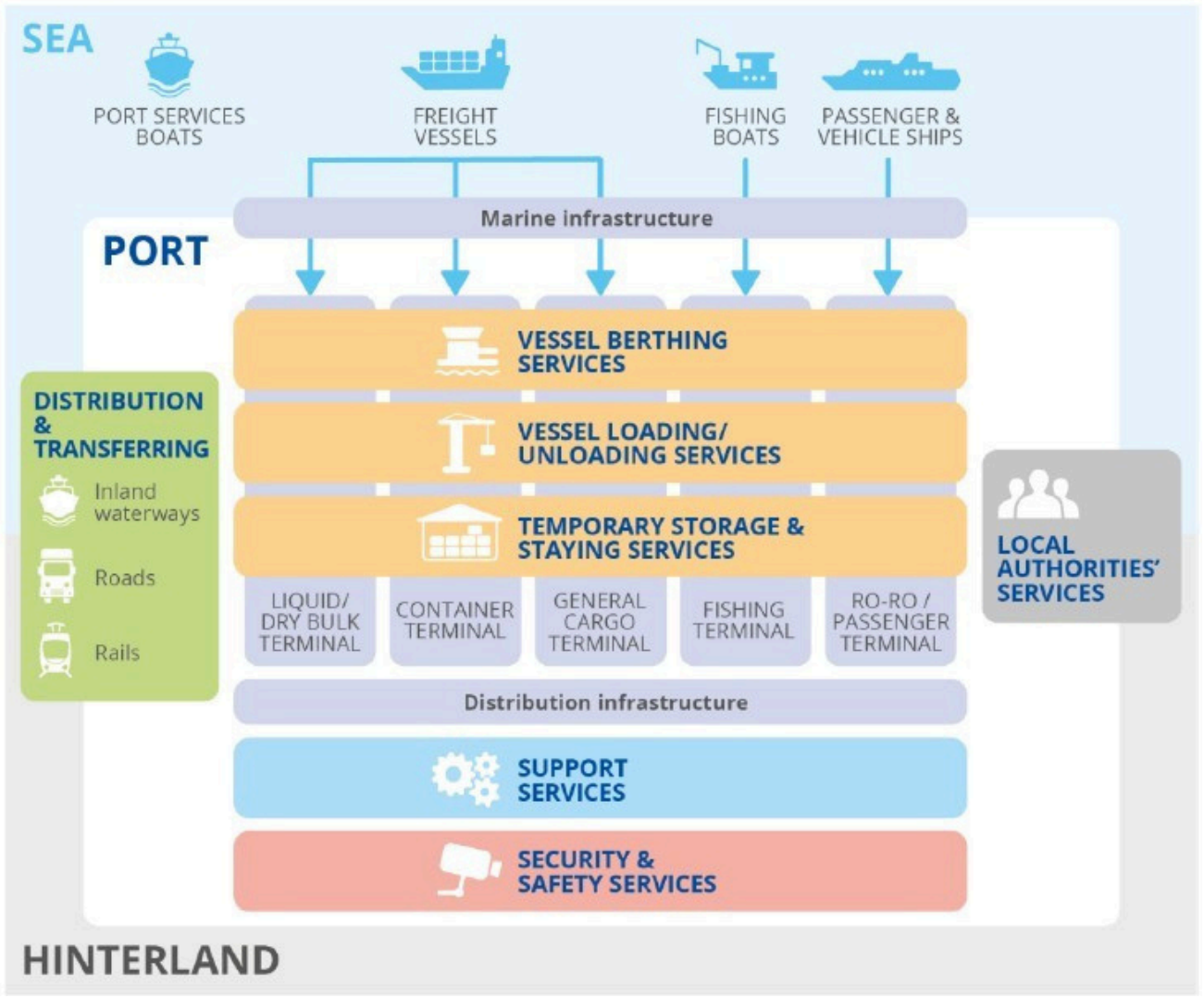
o1. Εισαγωγή στην Κυβερνοασφάλεια στη Ναυτιλία

o2. Κατανόηση των Κυβερνοκινδύνων στη Ναυτιλία

o3. Πρότυπα και Βέλτιστες Πρακτικές στον Τομέα της Κυβερνοασφάλειας

o4. Πιστοποίηση στην Κυβερνοασφάλεια στη Ναυτιλία

Υπηρεσίες & Υποδομές Λιμένων



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2=1

Τι είναι η Κυβερνοασφάλεια στη Ναυτιλία

Προστασία των **διασυνδεδεμένων συστημάτων πληροφορικής,τεχνολογίας λειτουργίας και διαδικτύου των πραγμάτων στον τομέα της ναυτιλίας** σε λιμένες, πλοία και δίκτυα εφοδιασμού

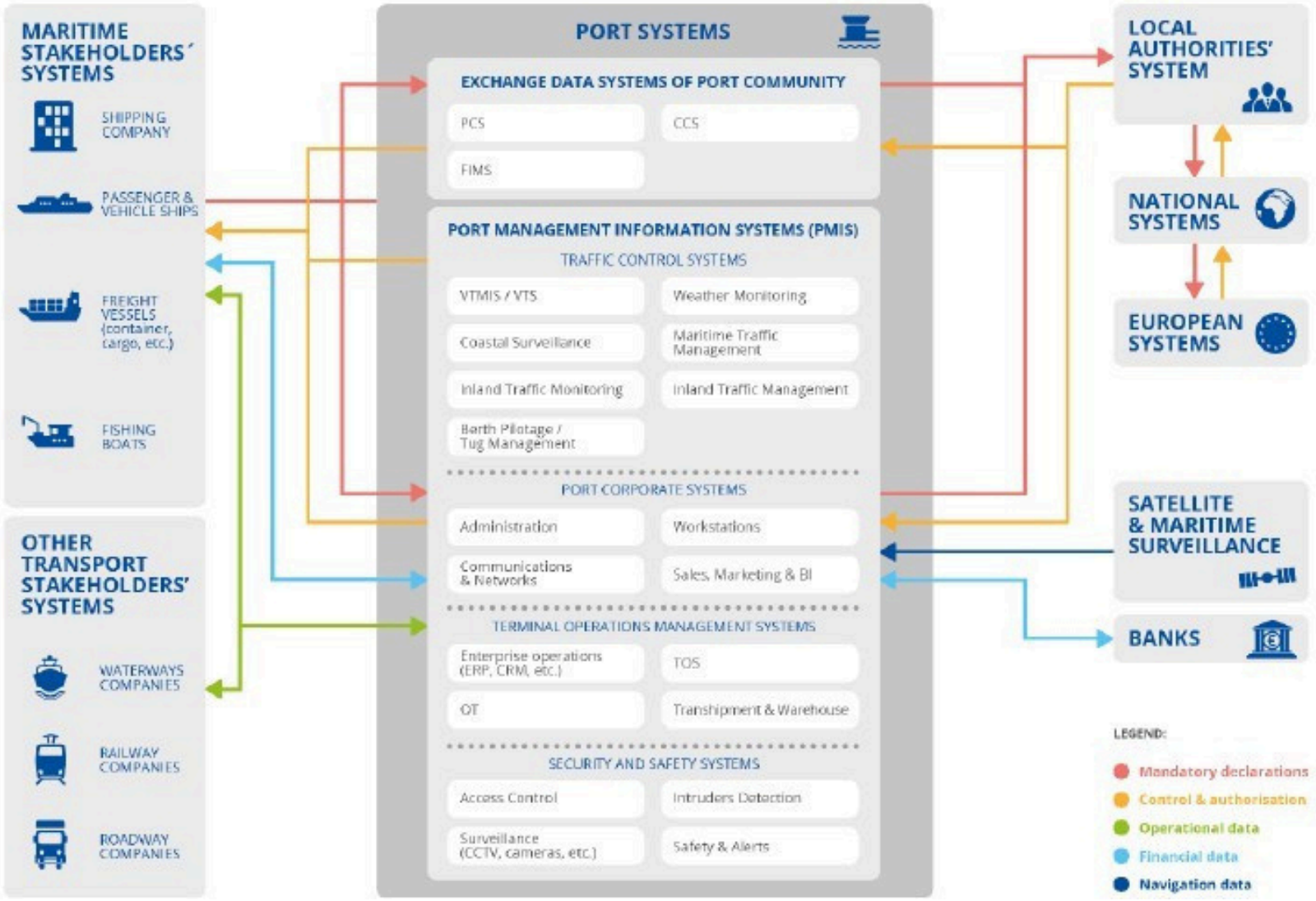
Έμφαση στην εξασφάλιση:

- **Ασφάλε**ια πλοίων, πληρώματος και λειτουργιών
- **Ακεραιότητα** συστημάτων πλοήγησης και κρίσιμων συστημάτων αποστολής
- **Διαθεσιμότητα και συνέχεια** λιμενικών και λειτουργιών αλυσίδας εφοδιασμού

Αντιμετωπίζει τις μοναδικές προκλήσεις των:

- Περιβάλλοντα με υψηλό βαθμό **διασύνδεσης και κατανεμημένα**
- Ενσωμάτωση **συστημάτων IT, OT και IoT**
- Έκθεση τόσο σε **κυβερνοκινδύνους όσο και** σε **φυσικούς κινδύνους**

Περιληπτικό Μοντέλο Αναφοράς Λιμενικών Συστημάτων



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2= 1

Συστήματα IT, OT & IoT σε Ναυτιλιακά Περιβάλλοντα

Συστήματα IT:

- Πλατφόρμες κρατήσεων
- Συστήματα ERP
- Συστήματα λιμενικής κοινότητας

Συστήματα IoT / IIoT:

- Αισθητήρες (φορτίου, περιβάλλοντος, εξοπλισμού)
- Έξυπνες συσκευές και συστήματα παρακολούθησης
- Συνδεδεμένα περιουσιακά στοιχεία σε λιμένες και πλοία

Συστήματα OT:

- Συστήματα πλοήγησης
- Λιμενικός εξοπλισμός (γερανοί, συστήματα ελέγχου)
- Συστήματα ελέγχου πλοίων

Αυξανόμενη ενοποίηση μεταξύ συστημάτων IT, OT και IoT

Το IoT διευρύνει σημαντικά την επιφάνεια επίθεσης

Τι είναι μια Απειλή;

Απειλή: Μια πιθανή αιτία ενός ανεπιθύμητου συμβάντος, το οποίο μπορεί να προκαλέσει βλάβη σε ένα σύστημα ή έναν οργανισμό.
[ISO/IEC 27000:2018]

Σε αυτό το πλαίσιο, μια απειλή είναι ένας εξωτερικός παράγοντας που θα μπορούσε να εκμεταλλευτεί μια ευπάθεια σε ένα σύστημα.
Οι απειλές μπορεί να είναι ανθρωπογενείς (όπως επιτιθέμενοι ή εσωτερικές απειλές), περιβαλλοντικές (όπως φυσικές καταστροφές) ή τεχνικές (όπως κακόβουλο λογισμικό ή ευπάθειες σε λογισμικό).
Το τοπίο των απειλών στην κυβερνοασφάλεια στη θάλασσα θα περιλαμβάνει κινδύνους τόσο από σκόπιμες επιθέσεις (π.χ. ransomware) όσο και από ακούσια περιστατικά (π.χ. ανθρώπινα λάθη).

https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Τύποι Απειλών στον Κυβερνοχώρο στη Ναυτιλία

Απειλές που σχετίζονται με την πληροφορική:

- Κυβερνοεπιθέσεις (ransomware, phishing, malware)
- Επιθέσεις σε διαδικτυακές εφαρμογές
- Παραβίαση διαπιστευτηρίων

Απειλές που σχετίζονται με την OT:

- Επιθέσεις πλοήγησης (π.χ. πλαστογράφηση GPS)
- Επιθέσεις σε ICS / συστήματα ελέγχου
- Φυσικές-κυβερνοεπιθέσεις

Απειλές σχετικές με το IoT / IIoT:

- Παραβιασμένοι αισθητήρες και συσκευές
- Αδύναμοι μηχανισμοί ελέγχου ταυτότητας
- Εκμετάλλευση συσκευών μεγάλης κλίμακας

Απειλές που σχετίζονται με τον άνθρωπο:

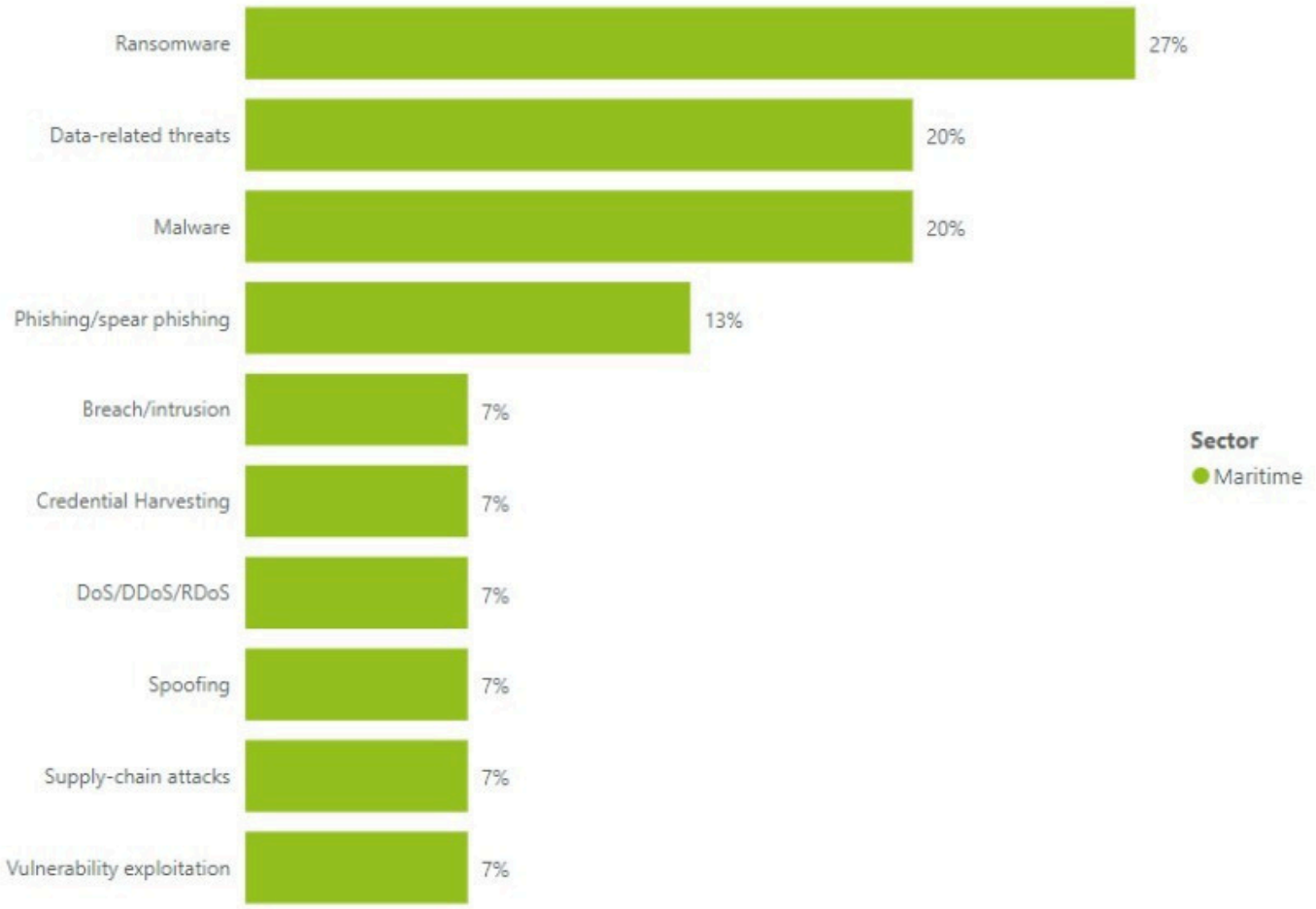
- Απειλές από εσωτερικούς
- Κοινωνική μηχανική ( )
- Ανθρώπινο λάθος και εσφαλμένη διαμόρφωση

Απειλές μεταξύ τομέων:

- Επιθέσεις στην αλυσίδα εφοδιασμού

Οι απειλές μπορούν να επηρεάσουν συστήματα σε πλοία, λιμένες και θαλάσσιες υποδομές

Κύριες Απειλές στη Ναυτιλία



https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Γιατί τα Ναυτιλιακά Συστήματα είναι ιδιαίτερα εκτεθειμένα σε Απειλές στον Κυβερνοχώρο

Πολύπλοκο οικοσύστημα: Λιμένες, πλοία, εφοδιαστική και αρχές

Σύγκλιση IT/OT: Διασύνδεση λειτουργικών και επιχειρηματικών συστημάτων

Υψηλή συνδεσιμότητα: Δορυφορικές επικοινωνίες, απομακρυσμένη πρόσβαση, ενσωμάτωση τρίτων

Παλαιά συστήματα: Δύσκολα στην ασφάλεια και τη συντήρηση, συχνά στερούνται σύγχρονων μέτρων ασφαλείας

Περιβάλλον κρίσιμης σημασίας για την ασφάλεια: Τα συμβάντα στον κυβερνοχώρο μπορούν να έχουν άμεσο φυσικό αντίκτυπο

Αυτοί οι παράγοντες αυξάνουν σημαντικά την επιφάνεια επίθεσης και την έκθεση σε κινδύνους

Η σημασία της Κυβερνοασφάλειας στη Ναυτιλία

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Η σημασία της Κυβερνοασφάλειας στη Ναυτιλία

- **Προστασία κρίσιμων υποδομών:** Οι ναυτιλιακές δραστηριότητες αποτελούν αναπόσπαστο μέρος του παγκόσμιου εμπορίου, μεταφέρονταςπάνωαπότο 80%τωνεμπορευμάτωνπαγκοσμίως.Ηκυβερνοασφάλειαδιασφαλίζειτηνπροστασίατωνλιμένων, τωνναυτιλιακώνεταιρειών καιτωνδικτύωνlogisticsαπό κυβερνοαπειλές.

- **Πρόληψη διαταραχών:** Οι κυβερνοεπιθέσεις μπορούν να οδηγήσουν σε σημαντικές διαταραχές στις ναυτιλιακές και λιμενικές δραστηριότητες. Για παράδειγμα, περιστατικά όπως η κυβερνοεπίθεση κατά της Maersk το 2017 είχαν ως αποτέλεσμα σημαντικές λειτουργικές καθυστερήσεις και απώλειες που ξεπέρασαν τα 300 εκατομμύρια δολάρια.

- **Διασφάλιση της ακεραιότητας των δεδομένων:** Η διασφάλιση της ακεραιότητας και της εμπιστευτικότητας ευαίσθητων δεδομένων, όπως τα συστήματα πλοήγησης και τα δηλωτικά φορτίου, είναι ζωτικής σημασίας. Οι παραβιάσεις μπορούν να θέσουν σε κίνδυνο την ασφάλεια και να οδηγήσουν σε οικονομικές απώλειες.

- **Συμμόρφωση με τους κανονισμούς:** Οι αυξανόμενοι κανονισμοί, όπως οι κατευθυντήριες γραμμές του Διεθνούς Ναυτιλιακού Οργανισμού (IMO), επιβάλλουν την εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας για την προστασία των πλοίων και των λιμένων, ενώ η διασφάλιση της συμμόρφωσης μπορεί να αποτρέψει νομικές επιπτώσεις.

- **Ενίσχυση της ασφάλειας:** Η κυβερνοασφάλεια προστατεύει από απειλές που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια του πληρώματος και των πλοίων. Τα συμβάντα στον κυβερνοχώρο μπορούν να επηρεάσουν τα συστήματα πλοήγησης, θέτοντας σε κίνδυνο τη ναυτική ασφάλεια.

- **Οικοδόμηση εμπιστοσύνης:** Μια ισχυρή στάση στον τομέα της κυβερνοασφάλειας ενισχύει την εμπιστοσύνη μεταξύ των ενδιαφερόμενων μερών, συμπεριλαμβανομένων κυβερνήσεων, πελατών και συνεργατών. Αυτή η εμπιστοσύνη είναι απαραίτητη για την ομαλή λειτουργία των ναυτιλιακών εφοδιαστικών αλυσίδων.

Κανονιστικοί Παράγοντες για την Κυβερνοασφάλεια στη Ναυτιλία

Κανονισμοί: Υποχρεωτικές νομικές απαιτήσεις που πρέπει να τηρούν οι οργανισμοί

- Απαιτήσεις του Διεθνούς Ναυτιλιακού Οργανισμού (IMO)
- Κανονισμοί της ΕΕ (π.χ. GDPR, NIS2)

Πρότυπα: Τυποποιημένες απαιτήσεις για την εφαρμογή και τη διαχείριση της ασφάλειας

- ISO/IEC 27001

Πλαίσια: Δομημένες προσεγγίσεις για τη διαχείριση των κινδύνων στον τομέα της κυβερνοασφάλειας

- Πλαίσιο Κυβερνοασφάλειας του NIST

Κατευθυντήριες γραμμές: Συνιστώμενες βέλτιστες πρακτικές και μη δεσμευτικές οδηγίες

- Κατευθυντήριες γραμμές της ENISA
- Κατευθυντήριες γραμμές του ΔΝΟ για τη διαχείριση των κινδύνων στον κυβερνοχώρο

Οι κανονισμοί απαιτούν από τους οργανισμούς να εφαρμόζουν μέτρα κυβερνοασφάλειας

Χρησιμοποιούνται πρότυπα και πλαίσια για την επίτευξη συμμόρφωσης και την απόδειξη της ασφάλειας

Πρόοδος μαθήματος

o1. Εισαγωγή στην Κυβερνοασφάλεια στη Ναυτιλία

o2. Κατανόηση των Ναυτιλιακών Κυβερνοκινδύνων

o3. Πρότυπα και Βέλτιστες Πρακτικές στον Τομέα της Κυβερνοασφάλειας

o4. Πιστοποίηση στην Κυβερνοασφάλεια στη Ναυτιλία

Τι είναι ο Κίνδυνος;

Κίνδυνος: Η επίδραση της αβεβαιότητας στους στόχους (ISO 31000:2018; ISO/IEC 27000:2018). Ο κίνδυνος χαρακτηρίζεται συχνά με αναφορά σε πιθανά γεγονότα και συνέπειες ή σε συνδυασμό αυτών (συμπεριλαμβανομένων των αλλαγών στις συνθήκες) και τη σχετική «πιθανότητα» εμφάνισης. [ISO/IEC 27000:2018, ISO 31000:2018]

Ευπάθεια έναντι Απειλής έναντι Κινδύνου

Ορισμοί:

- **Ευπάθεια:** μια αδυναμία που μπορεί να αξιοποιηθεί
- **Απειλή:** μια πιθανή αιτία βλάβης
- **Κίνδυνος:** η πιθανότητα και ο αντίκτυπος μιας απειλής που εκμεταλλεύεται μια ευπάθεια

Παράδειγμα:

- **Ευπάθεια:** Ανεπαρκώς ασφαλής απομακρυσμένη πρόσβαση σε συστήματα λιμένων
- **Απειλή:** Προσπάθεια μη εξουσιοδοτημένης πρόσβασης
- **Κίνδυνος:** Παραβίαση λογαριασμού

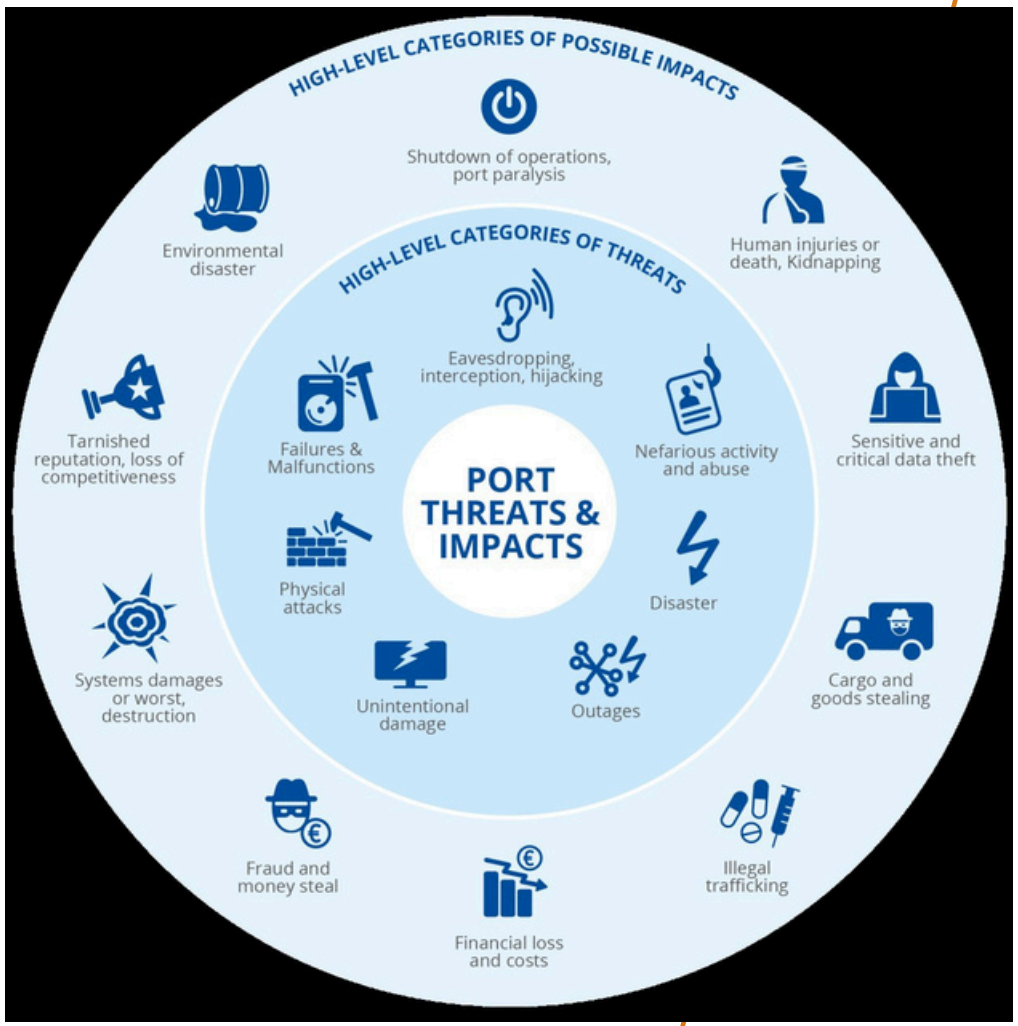
Ο κίνδυνος υφίσταται μόνο όταν υπάρχει απειλή που μπορεί να εκμεταλλευτεί μια ευπάθεια

Σενάρια Ναυτιλιακών Κυβερνοκινδύνων και ο Αντίκτυπός τους

Σενάριο συμβάντος κινδύνου	Πιθανές επιπτώσεις
Παραποίηση συστήματος πλοήγησης (π.χ. πλαστογράφηση GPS)	Λανθασμένη θέση και πιθανές επιπτώσεις στην ασφάλεια του σκάφους
Παραβίαση δεδομένων φορτίου	Διαρροή ευαίσθητων δεδομένων και επιπτώσεις σε οικονομικό επίπεδο και στη φήμη
Διακοπή των λιμενικών δραστηριοτήτων	Καθυστερήσεις, συμφόρηση και επιπτώσεις στην εφοδιαστική αλυσίδα
Λογισμικό εκβιασμού (ransomware) στα συστήματα των τερματικών σταθμών	Μη διαθεσιμότητα συστημάτων, διακοπή λειτουργίας και οικονομικές απώλειες

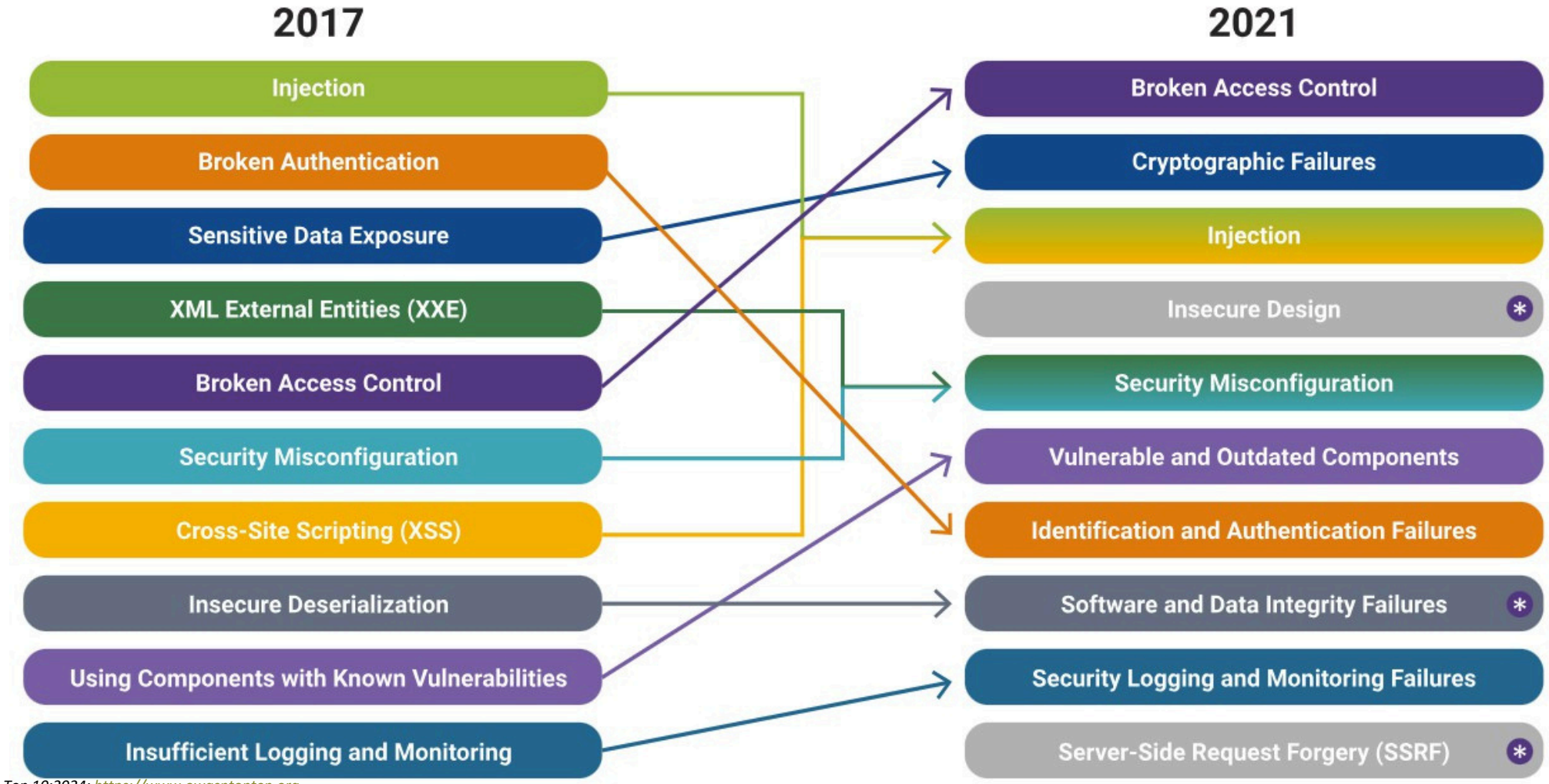
Οι κυβερνοκίνδυνοι στο ναυτιλιακό περιβάλλον μπορούν να επηρεάσουν την ασφάλεια, τις λειτουργίες και τη συνέχεια των επιχειρήσεων

Προσδιορισμός των Κυβερνοκινδύνων στις Ναυτιλιακές Λειτουργίες



https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

OWASP Οι 10 Κρισιμότεροι Κίνδυνοι Ασφάλειας σε Εφαρμογές Web



OWASP Top 10:2024: https://www.owasptopten.org

Περιστατικά Κυβερνοασφάλειας στη Ναυτιλία

Police warning after drug traffickers' cyber-attack

16 October 2013

Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

«Σεαυτή τηνπερίπτωση, προσέλαβανχάκερ[πουήταν] πολύ υψηλού επιπέδου,έξυπνοιτύποι,πουέκανανπολλήδουλειά στον τομέα του λογισμικού», προσθέτει.

Λέει ότι η επιχείρηση για την παραβίαση των εταιρειών του λιμανιού πραγματοποιήθηκε σε διάφορες φάσεις, ξεκινώντας με την αποστολή κακόβουλου λογισμικού μέσω ηλεκτρονικού ταχυδρομείου στο προσωπικό, επιτρέποντας στην οργανωμένη εγκληματική ομάδα να έχει απομακρυσμένη πρόσβαση στα δεδομένα.

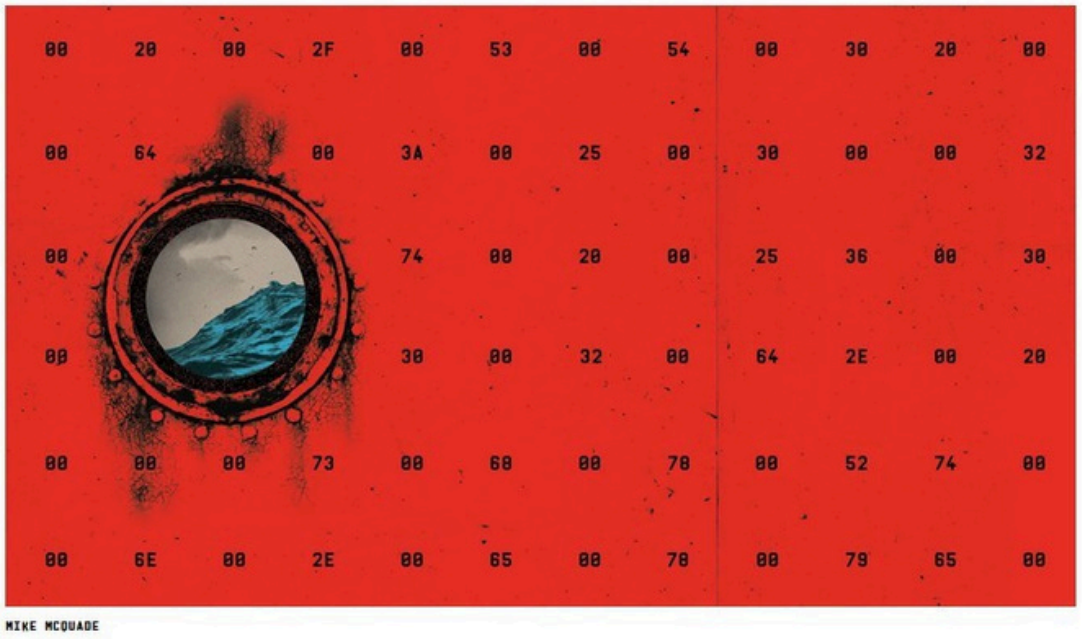
Όταν ανακαλύφθηκε η αρχική παραβίαση και εγκαταστάθηκε τείχος προστασίας για την αποτροπή περαιτέρω επιθέσεων, οι χάκερς εισέβαλαν στις εγκαταστάσεις και εγκατέστησαν συσκευές καταγραφής πληκτρολογίων στους υπολογιστές.

Αυτό τους επέτρεψε να αποκτήσουν ασύρματη πρόσβαση στα πληκτρολόγια που πληκτρολογούσε το προσωπικό, καθώς και σε στιγμιότυπα οθόνης από τις οθόνες τους.

Περιστατικά Κυβερνοασφάλειας στη Ναυτιλία

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.



Ο Τζένσεν σήκωσε το βλέμμα του για να ρωτήσει αν κάποιος άλλος στο ανοιχτό γραφείο του, όπου εργάζονταν οι υπάλληλοι του τμήματος πληροφορικής, είχε διακοπεί τόσο απότομα. Και καθώς έστρεψε το κεφάλι του, είδε όλες τις άλλες οθόνες υπολογιστών στο δωμάτιο να σβήνουν η μία μετά την άλλη με ταχύ ρυθμό.

«Είδα ένα κύμα οθονών να γίνονται μαύρες. Μαύρες, μαύρες, μαύρες. Μαύρες, μαύρες, μαύρες, μαύρες», λέει. Οι υπολογιστές, όπως ανακάλυψαν γρήγορα ο Jensen και οι γείτονές του, είχαν κλειδωθεί ανεπανόρθωτα. Η επανεκκίνηση τους επέστρεφε μόνο στην ίδια μαύρη οθόνη.

[...] Οι δημιουργοί του NotPetya συνδύασαν αυτό το ψηφιακό «κλειδί-πασπαρτού» με μια παλαιότερη εφεύρεση γνωστή ως Mimikatz, η οποία δημιουργήθηκε ως απόδειξη της εφικτότητας της ιδέας από τον Γάλλο ερευνητή ασφάλειας Benjamin Delpy το 2011. Ο Delpy είχε αρχικά κυκλοφορήσει το Mimikatz για να αποδείξει ότι τα Windows άφηναν τους κωδικούς πρόσβασης των χρηστών να παραμένουν στη μνήμη των υπολογιστών. Μόλις οι χάκερ αποκτούσαν αρχική πρόσβαση σε έναν υπολογιστή, το Mimikatz μπορούσε να αντλήσει αυτούς τους κωδικούς πρόσβασης από τη μνήμη RAM και να τους χρησιμοποιήσει για να εισβάλει σε άλλους υπολογιστές στους οποίους είχε πρόσβαση με τα ίδια διαπιστευτήρια. Σε δίκτυα με υπολογιστές πολλαπλών χρηστών, μπορούσε ακόμη και να επιτρέψει μια αυτοματοποιημένη επίθεση να μεταπηδά από τον έναν υπολογιστή στον άλλο.

Περιστατικά Κυβερνοασφάλειας στη Ναυτιλία

Troubled waters: Cyber-attacks on San Diego and Barcelona's ports

03 Oct 2018

Our AI is actively defending ports across the world – such as Harwich Haven Authority and Belfast Harbour.

Last summer's wave of ransomware attacks compromised port terminals and disrupted global shipping. Since then, cyber security has quickly risen to the top of the agenda for the maritime sector. Earlier this year, another port was hit with ransomware, and then, last week, the ports of Barcelona and San Diego revealed that they had been the victims of further ransomware attacks.

Ωστόσο, η αυξανόμενη σύγκλιση των συστημάτων IT και OT δεν δείχνει σημάδια επιβράδυνσης. Οι υπερσυνδεδεμένοι «έξυπνοι» λιμένες προσφέρουν αποδοτικότητα και ακρίβεια, μειώνοντας παράλληλα το κόστος. Ωστόσο, η αλληλεπίδραση του φυσικού και του ψηφιακού περιβάλλοντος στους λιμένες παραμένει μια σημαντική πρόκληση για τις ομάδες κυβερνοασφάλειας που είναι επιφορτισμένες με την προστασία τους. Χωρίς να βιαζόμαστε να βγάλουμε συμπεράσματα, ίσως δεν αποτελεί έκπληξη το γεγονός ότι ο Λιμένας της Βαρκελώνης βρίσκεται στη διαδικασία υλοποίησης ενός «έργου Ψηφιακού Λιμανιού», το οποίο ξεκίνησε πέρυσι με σκοπό την προώθηση της ψηφιοποίησης του λιμενικού περιβάλλοντος.

Ο Ανθρώπινος Παράγοντας στην Κυβερνοασφάλεια στη Ναυτιλία

Σε πολλά ναυτιλιακά περιστατικά, ο **άνθρωπος αποτελεί το πιο αδύναμο σημείο** και όχι το σύστημα

Το phishing και η κοινωνική μηχανική αποτελούν συνηθισμένα σημεία εισόδου για κυβερνοεπιθέσεις

Οι εσωτερικές απειλές περιλαμβάνουν τόσο κακόβουλες ενέργειες όσο και ακούσια λάθη από υπαλλήλους ή εξωτερικούς συνεργάτες

Το ανθρώπινο λάθος, όπως η λανθασμένη διαμόρφωση ή τα αδύναμα διαπιστευτήρια, δημιουργεί ευπάθειες στα συστήματα

Η έλλειψη ευαισθητοποίησης και εκπαίδευσης στον τομέα της κυβερνοασφάλειας αυξάνει την έκθεση σε επιθέσεις και μειώνει την ικανότητα αντίδρασης

Οι ανθρώπινες ενέργειες μπορούν να επηρεάσουν **τα συστήματα IT, OT και IoT** σε όλα τα ναυτιλιακά περιβάλλοντα

Από το IT στο OT: Πώς κλιμακώνονται οι Επιθέσεις στον Ναυτιλιακό Τομέα

Βήμα1:Αρχικήπρόσβαση (επίπεδοπληροφορικής)

- Ηλεκτρονικό μήνυμα phishing
- Παραβίαση διαπιστευτηρίων
- Ευπάθειες εφαρμογών ιστού

Βήμα 2: Πλευρική κίνηση (δίκτυο IT)

- Πρόσβαση σε εσωτερικά συστήματα
- Αύξηση προνομίων
- Κίνηση στο εταιρικό δίκτυο

Βήμα3:Μετάβαση σε συστήματα OT/IoT

- Σύνδεση με λειτουργικά συστήματα
- Αδύναμη τμηματοποίηση δικτύου
- Κοινόχρηστα διαπιστευτήρια ή διεπαφές

Βήμα 4: Επιπτώσεις στη λειτουργία

- Διακοπή λειτουργίας των λιμένων
- Παρεμβολές στο σύστημα πλοήγησης
- Δυσλειτουργία εξοπλισμού

Τα συμβάντα στον κυβερνοχώρο συχνά ξεκινούν στον τομέα της πληροφορικής, αλλά επηρεάζουν τις λειτουργίες της τεχνολογίας λειτουργίας

Ανάλυση Συμβάντων με Χρήση Εννοιών Κινδύνου

Ποιο περιουσιακό στοιχείο επηρεάστηκε;

Ποια ευπάθεια εκμεταλλεύτηκε;

Ποια απειλή προκάλεσε το περιστατικό;

Ποια ήταν η επίδραση στις λειτουργίες, την ασφάλεια ή την επιχείρηση;

Ποιοι έλεγχοι θα μπορούσαν να είχαν αποτρέψει ή να είχαν μετριάσει το περιστατικό;

Αξιολόγηση και Διαχείρισης Κινδύνου

Πεδίο εφαρμογής: Η αξιολόγηση κινδύνου εστιάζει στον εντοπισμό και την αξιολόγηση των κινδύνων, ενώ η διαχείριση κινδύνου περιλαμβάνει ολόκληρη τη διαδικασία, συμπεριλαμβανομένης της αντίδρασης και της παρακολούθησης.

Διαδικασία: Η εκτίμηση κινδύνου αποτελεί υποκατηγορία της διαχείρισης κινδύνου. Η αποτελεσματική διαχείριση κινδύνου δεν μπορεί να πραγματοποιηθεί χωρίς μια διεξοδική εκτίμηση κινδύνου.

Τελικοί στόχοι: Στόχος της εκτίμησης κινδύνων είναι η κατανόηση των κινδύνων, ενώ στόχος της διαχείρισης κινδύνων είναι η διαχείριση αυτών των κινδύνων με τρόπο που προστατεύει τον οργανισμό και υποστηρίζει τους στόχους του.

Διαδικασία Αξιολόγησης Κινδύνων

Φάση	Βήμα	Ενέργειες
Αξιολόγηση κινδύνου	1. Ορισμός πεδίου εφαρμογής	Ορισμόςτουπεδίου εφαρμογής σε λιμένες,πλοία και ναυτιλιακά συστήματα (IT, OT, IoT)
	2. Κατανόηση περιουσιακών στοιχείων και συστημάτων	Προσδιορισμός κρίσιμων περιουσιακών στοιχείων, ρόλων και εξαρτήσεων
	3. Προσδιορισμός κινδύνων	Προσδιορισμός απειλών, ανακάλυψη τρωτών σημείων, σημεία έκθεσης
	4. Ανάλυση κινδύνων	Αξιολόγηση της πιθανότητας και του αντίκτυπου στην ασφάλεια, τις λειτουργίες και την επιχείρηση
	5. Αξιολόγηση κινδύνων	Προτεραιοποίηση των κινδύνων με βάση καθορισμένα κριτήρια
Αντιμετώπιση κινδύνων	6. Επιλογή μέτρων ελέγχου	Επιλέξτε τα κατάλληλα μέτρα ασφαλείας
	7. Καθορισμός στρατηγικής αντιμετώπισης	Καθορισμός στρατηγικής (μετριασμός, αποδοχή, μεταφορά, αποφυγή)
	8. Εφαρμογή μέτρων ελέγχου	Εφαρμογή ελέγχων σε περιβάλλοντα IT, OT και IoT
Παρακολούθηση και επανεξέταση	9. Παρακολούθηση και αναθεώρηση	Συνεχής παρακολούθηση των κινδύνων, αξιολόγηση των ελέγχων και προσαρμογή

Περιληπτικό Παράδειγμα Μεθοδολογίας Διαχείρισης Ναυτιλιακών Κυβερνοκινδύνων (ENISA)

https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

Παράδειγμα Μεθοδολογίας Διαχείρισης Κινδύνων

Main axes of risk analysis	CYSMET methodology
1. Perimeter/boundaries setting	Step 0: Scope of SCS risk assessment Step 1: Analysis of SCS *1.1 Scope and objectives of SCS* *1.2 Identification of SCS-BPs* *1.3 SCS modeling*
2. Threat analysis	Step 2: SCS threat analysis *2.1 Identification of cyber and/or physical individual threats linked to an SCS asset* *2.2 SCS threat assessment*
3. Vulnerability analysis	Step 3: SCS vulnerability and impact analysis *3.1 Determination of attacker profile* *3.2 Identification of confirmed individual vulnerabilities* *3.3 Identification of confirmed/zero-day vulnerabilities* *3.4 Creation of vulnerability chains in SCS* *3.5 Identification of attack methods and graphs* *3.6 Assessment of individual vulnerability severity level*
4. Impact analysis	
5. Risk assessment	Step 4: Risk assessment *4.1 Assessment of risk level of individual assets* *4.2 Vulnerability chain risk level assessment*
6. Risk mitigation strategy	Step 5: Risk mitigation—Selection of security controls

https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2023.1156726/full

Πρόοδος μαθήματος

o1. Εισαγωγή στην Κυβερνοασφάλεια στη Ναυτιλία

o2. Κατανόηση των Κυβερνοκινδύνων στη Ναυτιλία

o3. Πρότυπα και Βέλτιστες Πρακτικές στον Τομέα της Κυβερνοασφάλειας

o4. Πιστοποίηση στην Κυβερνοασφάλεια στη Ναυτιλία

Γιατί τα Πρότυπα & τα Πλαίσια Κυβερνοασφάλειας έχουν Σημασία

Η κυβερνοασφάλεια δεν μπορεί να βασίζεται σε ad hoc μέτρα ή μεμονωμένες λύσεις

Οι οργανισμοί χρειάζονται μια **δομημένη προσέγγιση** για τη συνεπή διαχείριση των κινδύνων

Τα πρότυπα εξασφαλίζουν **συνεπή προστασία σε όλα τα συστήματα IT, OT και IoT**, καθορίζουν σαφείς και μετρήσιμους **ελέγχους ασφάλειας** και επιτρέπουν **την ευθυγράμμιση με τις κανονιστικές και λειτουργικές απαιτήσεις**

Επιτρέπουν στους οργανισμούς να λαμβάνουν **αποφάσεις με βάση τον κίνδυνο**, να αποδεικνύουν την ασφάλεια μέσω **ελέγχων** και να προετοιμάζονται για **πιστοποίηση και συμμόρφωση**

Βασικά Πρότυπα & Πλαίσια για την Κυβερνοασφάλεια στη Ναυτιλία

ISO/IEC 27001:2022:Διεθνέςπρότυπο για τηδημιουργίακαι τη διατήρησηενός συστήματοςδιαχείρισης ασφάλειας πληροφοριών (ISMS), που διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών μέσω μιας συστηματικής προσέγγισης.

Πλαίσιο Κυβερνοασφάλειας NIST: Πλαίσιο βασισμένο στον κίνδυνο που βοηθά τους οργανισμούς να εντοπίζουν, να προστατεύουν, να ανιχνεύουν, να ανταποκρίνονται και να ανακάμπτουν από απειλές κυβερνοασφάλειας.

GDPR (Γενικός Κανονισμός για την Προστασία Δεδομένων): Κανονισμός της ΕΕ που καθορίζει τις απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, ο οποίος ισχύει και για τους ναυτιλιακούς οργανισμούς που επεξεργάζονται δεδομένα πολιτών της ΕΕ.

Διαχείριση Κυβερνοκινδύνων του ΔΝΟ: Κατευθυντήριες γραμμές για την ενσωμάτωση της κυβερνοασφάλειας στις ναυτιλιακές δραστηριότητες και στα συστήματα διαχείρισης της ασφάλειας, με σκοπό την προστασία των ναυτιλιακών και λιμενικών δραστηριοτήτων.

Κατευθυντήριες οδηγίες ENISA (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια): Συστάσεις και βέλτιστες πρακτικές στον τομέα της κυβερνοασφάλειας για ναυτιλιακά και λιμενικά περιβάλλοντα, που υποστηρίζουν την προστασία βάσει κινδύνου και την ανθεκτικότητα των κρίσιμων υποδομών.

Προκλήσεις στην Εφαρμογή Προτύπων Κυβερνοασφάλειας στη Ναυτιλία

Τα **παλαιά συστήματα OT είναι δύσκολο να ενημερωθούν ή να ασφαλιστούν**, καθώς δε σχεδιάστηκαν με γνώμονα την κυβερνοασφάλεια και συχνά δεν μπορούν να υποστηρίξουν σύγχρονους ελέγχους

Συχνά, **τα συστήματα δεν μπορούν να τεθούν εκτός λειτουργίας**, καθώς απαιτείται συνεχής λειτουργία, γεγονός που περιορίζει τη δυνατότητα εφαρμογής ενημερώσεων ή εκτέλεσης εργασιών συντήρησης

Τα μέτρα ασφάλειας δεν πρέπει να παρεμποδίζουν την ασφάλεια και τη λειτουργία, γεγονός που απαιτεί προσεκτική ισορροπία μεταξύ προστασίας και επιχειρησιακής συνέχειας

Πολλαπλοί ενδιαφερόμενοι (λιμένες, φορείς εκμετάλλευσης, προμηθευτές) μοιράζονται συστήματα και ευθύνες, καθιστώντας πιο περίπλοκη τη συνεπή εφαρμογή των ελέγχων

Βασικοί Έλεγχοι Ασφάλειας στα Ναυτιλιακά Συστήματα

Οέλεγχος πρόσβασηςκαιηδιαχείρισηταυτότηταςδιασφαλίζουνότιμόνοεξουσιοδοτημένοιχρήστες και συστήματα μπορούνναέχουνπρόσβασησεκρίσιμαναυτιλιακάσυστήματα

Η τμηματοποίηση του δικτύου περιορίζει την εξάπλωση των επιθέσεων μεταξύ εταιρικών και λειτουργικών περιβαλλόντων

Η παρακολούθηση και η ανίχνευση συμβάντων επιτρέπουν την έγκαιρη ανίχνευση ύποπτων δραστηριοτήτων σε όλα τα συστήματα

Η ενίσχυση της ασφάλειας του συστήματος και η διαχείριση ενημερώσεων μειώνουν τα τρωτά σημεία, λαμβάνοντας παράλληλα υπόψη τους λειτουργικούς περιορισμούς

Η δημιουργία αντιγράφων ασφαλείας και η ανάκτηση διασφαλίζουν ότι τα συστήματα και τα δεδομένα μπορούν να αποκατασταθούν μετά από διακοπή λειτουργίας ή συμβάντα στον κυβερνοχώρο

Πρόοδος μαθήματος

o1. Εισαγωγή στην Κυβερνοασφάλεια στη Ναυτιλία

o2. Κατανόηση των Κυβερνοκινδύνων στη Ναυτιλία

o3. Πρότυπα και Βέλτιστες Πρακτικές στον Τομέα της Κυβερνοασφάλειας

o4. Πιστοποίηση στην Κυβερνοασφάλεια στη Ναυτιλία

Τι είναι η Πιστοποίηση στον Τομέα της Κυβερνοασφάλειας

Μια επίσημη διαδικασία για την αξιολόγηση και την επαλήθευση της ασφάλειας συστημάτων ή προϊόντων

Βασίζεται σε συστήματα πιστοποίησης και πρότυπα αξιολόγησης (π.χ. Κοινά Κριτήρια, EUCC)

Διεξάγεται από **ανεξάρτητους και διαπιστευμένους φορείς αξιολόγησης**

Απαιτεί **καθορισμένες απαιτήσεις ασφάλειας, δοκιμές και επίπεδα διασφάλισης**

Οδηγεί σε πιστοποιημένο επίπεδο εμπιστοσύνης στην ασφάλεια του συστήματος ή του προϊόντος

Συμμόρφωση έναντι Πιστοποίησης

Πτυχή	Συμμόρφωση	Πιστοποίηση
Ορισμός	Τήρηση κανονιστικών ή νομικών απαιτήσεων	Επίσημη αξιολόγηση βάσει καθορισμένων κριτηρίων ασφάλειας
Αξιολόγηση	Αυτοδηλωμένη ή εσωτερική	Ανεξάρτητη αξιολόγηση από τρίτους
Πεδίο εφαρμογής	Νόμοι, κανονισμοί, πολιτικές	Πρότυπα και συστήματα πιστοποίησης (π.χ. Κοινά Κριτήρια, EUCC)
Αποτέλεσμα	Αποδεικνύει τη συμμόρφωση	Παρέχει επαληθευμένη διαβεβαίωση και εμπιστοσύνη

Γιατί η Πιστοποίηση Κυβερνοασφάλειας στη Ναυτιλία έχει Σημασία

Κανονιστικέςαπαιτήσειςκαιαπαιτήσειςσυμμόρφωσης:Ηπιστοποίησηβοηθάτουςοργανισμούςνασυμμορφωθούν με τις κανονιστικές απαιτήσεις

Επιχειρηματικές και συμβατικές απαιτήσεις: Συχνά απαιτείται από συνεργάτες, πελάτες και ενδιαφερόμενα μέρη της εφοδιαστικής αλυσίδας

Μείωση του κινδύνου σε διασυνδεδεμένα συστήματα: Παρέχει διασφάλιση σε σύνθετα ναυτιλιακά οικοσυστήματα

Εμπιστοσύνη και αξιοπιστία: Ενισχύει την εμπιστοσύνη μεταξύ λιμένων, φορέων εκμετάλλευσης και τρίτων

Ανταγωνιστικό πλεονέκτημα: Αποδεικνύει την ωριμότητα και διαφοροποιεί τους οργανισμούς στην αγορά

Κοινά Πρότυπα & Συστήματα Πιστοποίησης στην Κυβερνοασφάλεια

Κοινά Κριτήρια (ISO/IEC 15408) – Πιστοποίηση προϊόντων και συστημάτων πληροφορικής με βάση την αξιολόγηση της ασφάλειας

Κοινή Μεθοδολογία Αξιολόγησης (ISO/IEC 18045) – Καθορίζει τη μεθοδολογία για την αξιολόγηση προϊόντων σύμφωνα με τα Κοινά Κριτήρια

EUCC (Ευρωπαϊκό Σύστημα Πιστοποίησης Κυβερνοασφάλειας) – Πλαίσιο της ΕΕ για την πιστοποίηση προϊόντων και υπηρεσιών ΤΠΕ

Επισκόπηση της Διαδικασίας Πιστοποίησης

Καθορισμόςτουαντικειμένουαξιολόγησης(ΤΟΕ)(σύστημαήπροϊόνεντόςτουπεδίου εφαρμογής)

Επιλογή ενός εφαρμοστέου Προφίλ Προστασίας (PP) ή καθορισμός απαιτήσεων για την αξιολόγηση

Καθορισμός του Στόχου Ασφάλειας (ST) που περιγράφει τον τρόπο με τον οποίο το ΤΟΕ πληροί τους απαιτούμενους στόχους ασφάλειας

Διεξαγωγή ανεξάρτητης αξιολόγησης και δοκιμών ασφάλειας με βάση καθιερωμένη μεθοδολογία αξιολόγησης

Αξιολόγηση που διενεργείται από διαπιστευμένα εργαστήρια αξιολόγησης και φορείς πιστοποίησης

Πιστοποίηση που εκδίδεται με καθορισμένο επίπεδο διασφάλισης, το οποίο υποδεικνύει το επίπεδο εμπιστοσύνης στην ασφάλεια του συστήματος

Διατήρηση της πιστοποίησης μέσω ενημερώσεων, επιτήρησης και επαναξιολόγησης

Προκλήσεις στην Πιστοποίηση στη Ναυτιλία

Καθορισμός του πεδίου εφαρμογής της πιστοποίησης σε πλοία και λιμένες: Τα συστήματα καλύπτουν πλοία, λιμενική υποδομή και δίκτυα logistics, καθιστώντας δύσκολη την απομόνωση του αντικειμένου αξιολόγησης

Αξιολόγηση συστημάτων σε περιβάλλοντα λειτουργίας: Περιορισμένη δυνατότητα διεξαγωγής δοκιμών σε συστήματα που βρίσκονται σε λειτουργία, λόγω της συνεχούς λειτουργίας και των περιορισμών ασφαλείας

Ετερογενή και παλαιά ναυτιλιακά συστήματα: Οι διαφορετικές τεχνολογίες και ο παλαιότερος εξοπλισμός περιπλέκουν την προσαρμογή στις σύγχρονες απαιτήσεις αξιολόγησης

Εξαρτήσεις της ναυτιλιακής εφοδιαστικής αλυσίδας: Η πιστοποίηση πρέπει να λαμβάνει υπόψη τα διασυνδεδεμένα συστήματα μεταξύ φορέων εκμετάλλευσης, λιμένων, προμηθευτών και παρόχων logistics

Αξιολόγηση Κινδύνου & Συμμόρφωσης στις Ναυτιλιακές Αλυσίδες Εφοδιασμού

Η πιστοποίηση εκτείνεται πέρα από τα μεμονωμένα συστήματα **και καλύπτει τις διασυνδεδεμένες υπηρεσίες της ναυτιλιακής εφοδιαστικής αλυσίδας** (λιμένες, πλοία, logistics, πάροχοι υπηρεσιών)

Η αξιολόγηση βασίζεται σε:

- **Ανάλυση κινδύνων σε αλληλοσυνδεόμενες επιχειρηματικές διαδικασίες, περιουσιακά στοιχεία και επιχειρηματικούς εταίρους (BPs)**, συμπεριλαμβανομένων των αλληλεξαρτήσεων και των αλυσιδωτών επιπτώσεων που προκαλούνται από το φαινόμενο του καταρράκτη
- **Εφαρμογή ελέγχων** πέρα από οργανωτικά και τεχνικά όρια
- **Συλλογή αποδεικτικών στοιχείων** από πολλαπλούς ενδιαφερόμενους (συστήματα, διαδικασίες, λειτουργίες)

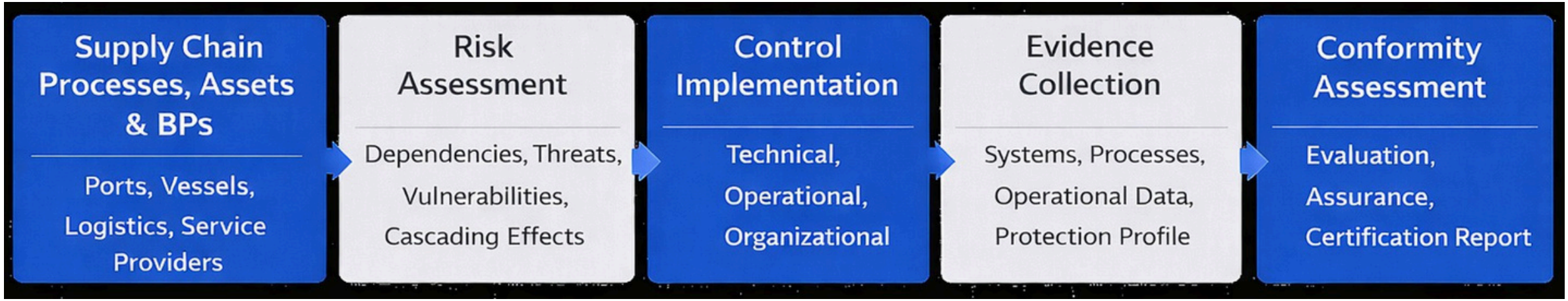
Η μεθοδολογία αξιολόγησης κινδύνου και συμμόρφωσης CYRENE εισάγει μια προσέγγιση προσανατολισμένη στην εφοδιαστική αλυσίδα του ναυτιλιακού τομέα, η οποία υποστηρίζει τόσο τους υπεύθυνους υλοποίησης όσο και τους αξιολογητές

Έμφαση και στα δύο:

- Την ασφάλεια **με βάση τον κίνδυνο** σε επίπεδο οικοσυστήματος
- Συμμόρφωση **βάσει αποδεικτικών στοιχείων** και συνεχής αξιολόγηση

Μεθοδολογία Αξιολόγησης Κινδύνου & Συμμόρφωσης CYRENE

Περιληπτική απεικόνιση της μεθοδολογίας CYRENE



Ευχαριστούμε

Αποστολή ερωτήσεων στις ηλ. διευθύνσεις:
pkyranoudi@tuc.gr
dpolemi@unipi.gr