iT SECURITYPRO

CYBERSECURITY & BUSINESS IT, IN-DEPTH ANALYSIS

06/07/08.2024 • Τεύχος 85 WWW.ITSECURITYPRO.GR Τιμή 5€

MARITIME CYBER SECURITY

- ΣΥΝΕΝΤΕΥΞΗ: ΘΕΜΙΣΤΟΚΛΗΣ ΣΑΡΔΗΣ - ΠΡΟΕΔΡΟΣ Δ.Σ. ΤΗΣ ΑΜΜΙΤΕΣ
- ΕΚΠΑΙΔΕΥΣΗ: ΤΟ ΒΑΣΙΚΟ ΣΤΟΙΧΕΙΟ ΚΑΘΕ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
- Ο ΑΝΘΡΩΠΙΝΟΣ ΠΑΡΑΓΟΝΤΑΣ: ΕΝΑΣ ΜΕΓΑΛΟΣ ΚΙΝΔΥΝΟΣ

CYBER INSURANCE - ΜΕΡΟΣ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ CYBER SECURITY ΤΩΝ ΝΑΥΤΙΛΙΑΚΩΝ ΕΤΑΙΡΕΙΩΝ

Σε έναν ολοένα και πιο διασυνδεδεμένο κόσμο, οι ναυτιλιακές εταιρείες αντιμετωπίζουν ένα μοναδικό σύνολο προκλήσεων όσον αφορά την ασφάλεια στον κυβερνοχώρο. Καθώς τα πλοία ψηφιοποιούνται όλο και περισσότερο και εξαρτώνται από την τεχνολογία, ο **κίνδυνος απειλών στον κυβερνοχώρο είναι μεγάλος και η επένδυση στην κυβερνοασφάλεια είναι αναγκαία.** Η ασφάλιση Cyber Insurance, ένα κρίσιμο εργαλείο για την αύξηση του ποσοστού διαχείρισης του κινδύνου και την οικονομική προστασία των ναυτιλιακών επιχειρήσεων έναντι των ψηφιακών κινδύνων.

Οι ναυτιλιακές εταιρείες λειτουργούν σε ένα πολύπλοκο οικοσύστημα που περιλαμβάνει ναυτιλιακές γραμμές, λιμάνια, παρόχους φορτίων & υπηρεσιών και φορείς εκμετάλλευσης πλοίων. Τα τρωτά σημεία αυτής της διασύνδεσης μπορούν να εκμεταλευθούν οι εγκληματίες του κυβερνοχώρου.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΒΑΣΙΚΟΙ ΚΙΝΔΥΝΟΙ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΠΟΥ ΑΝΤΙΜΕΤΩΠΙΖΕΙ Η ΝΑΥΤΙΛΙΑΚΗ ΒΙΟΜΗΧΑΝΙΑ

Ευπάθειες των συστημάτων των πλοίων: Τα σύγχρονα πλοία βασίζονται σε ολοκληρωμένα συστήματα πλοήγησης, επικοινωνίας και διαχείρισης φορτίου. Μια κυβερνοεπίθεση με στόχο αυτά τα συστήματα θα μπορούσε να διαταράξει τις λειτουργίες, να θέσει σε κίνδυνο την ασφάλεια ή ακόμη και να οδη-


ΝΙΚΟΣ ΓΕΩΡΓΟΠΟΥΛΟΣ
Digital Risks Insurance Broker – **Cromar** Insurance Brokers SA, Co- Founder
The DPO Academy LinkedIn Profile: https://www.linkedin.com/in/nikos-georgopoulos/

γήσει σε περιβαλλοντικές καταστροφές.
Κίνδυνοι στην εφοδιαστική αλυσίδα: Στα θαλάσσια logistics εμπλέκονται πολλά μέρη, από τους προμηθευτές έως τις τελωνειακές υπηρεσίες. Ενα περιστατικό παραβίασης ασφάλειας σε οποιοδήποτε τμήμα αυτής της αλυσίδας όχι μόνο μπορεί να διαταράξει τη ροή του φορτίου, να καθυστερήσει τις αποστολές και να επηρεάσει τα έσοδα αλλά να προκαλέσει και λειτουργικές ανωμαλίες σε όλο το εύρος της αλυσίδας εφοδιασμού.
Παραβιάσεις δεδομένων: Οι ναυτιλιακές εταιρείες διαχειρίζονται ευαίσθητα δεδομένα, όπως πληροφορίες για το πλήρωμα, δηλωτικά φορτίου και οικονομικά αρχεία. Μια παραβίαση δεδομένων μπορεί να οδηγήσει σε οικονομικές απώλειες, νομικές ευθύνες και ζημία στη φήμη.

Ο ΡΟΛΟΣ ΤΗΣ ΑΣΦΑΛΙΣΗΣ CYBER INSURANCE

Η ασφάλιση στον κυβερνοχώρο παρέχει οικονομική προστασία στις ναυτιλιακές εταιρείες, καλύπτοντας μια σειρά κινδύνων που σχετίζονται με τις ψηφιακές απειλές. Ας δούμε τι κυρίως προσφέρει η ασφάλιση Cyber Insurance
Οικονομική προστασία: Η ασφάλιση στον κυβερνοχώρο συμβάλλει στον μετριασμό των οικονομικών απωλειών που προκύπτουν από περιστατικά παραβίασης ασφάλειας στον κυβερνοχώρο. Καλύπτει δαπάνες , νομικά έξοδα και απώλεια εσόδων λόγω διακοπής εργασιών που οφείλονται σε περιστατικά παραβίασης ασφάλειας.**Επίσης καλύπτει την μεταφορά χρημάτων σε κυβερνοεγκληματίες μετα από περιστατικό παραπλάνησης social engineering.**
Αντιμετώπιση περιστατικών: Όταν συμβαίνει ένα περιστατικό στον κυβερνοχώρο, η ταχεία ανταπόκριση είναι κρίσιμη. Τα ασφαλιστήρια συμβόλαια cyber insurance παρέχουν πρόσβαση σε εμπειρογνώμονες που μπορούν να βοηθήσουν τις ναυτιλικές εταιρίες να αντιμετωπίσουν ενα περιστατικό μειώνοντας τις συνέπειες και επιταχύνοντας την ανάκαμψη.
Ευθύνη έναντι τρίτων: Εάν τα συστήματα μιας ναυτιλιακής εταιρείας παραβιαστούν και προκαλέσουν ζημία σε άλλα μέρη (π.χ. λιμενικές αρχές, ιδιοκτήτες φορτίων), η ασφάλιση cyber insurance μπορεί να καλύψει τα νομικά έξοδα και τις ζημίες.

Η ΠΕΡΙΠΤΩΣΗ ΤΗΣ MAERSK

Ο δανέζικος ναυτιλιακός κολοσσός Maersk το 2017 έπεσε θύμα ενός περιστατικού **ransomware NotPetya**, και υπέστη σημαντικές απώλειες λόγω της διακοπής της λειτουργίας και της καταστροφής δεδομένων. Το περιστατικό ανέδειξε τις συνέπειες που μπορεί να έχει στις ναυτιλιακές εταιρείες ενα περιστατικό παραβίασης ασφάλειας.
"**Θυμάμαι εκείνο το πρωί – οι φορητοί υπολογιστές έκαναν επανεκκίνηση και δεν φαινόταν να πρόκειται για κυβερνοεπίθεση εκείνη τη στιγμή, αλλά πολύ γρήγορα ο πραγματικός αντίκτυπος έγινε εμφανής"**, δήλωσε ο Lewis Woodcock, επικεφαλής κυβερνοασφάλειας στην Maersk. Στο youtube μπορείτε να δείτε την περιγραφή της επίπτωσης του συμβάντος στην Maersk από τον Jim Hageman Snabe πρόεδρο της Maersk οταν συνέβει το περιστατικό. Ας δούμε τον αντίκτυπο του περιστατικού ransomware NotPetya στις επιχειρηματικές δραστηριότητες της Maersk:
Διαταραχή εταιρικών λειτουργιών: Η επίθεση είχε σοβαρό λειτουργικό αντίκτυπο, 49.000 φορητοί υπολογιστές και συσκευές ηλεκτρονικών υπολογιστών τέθηκαν εκτός λειτουργίας, 1.200 κρίσιμες επιχειρηματικές εφαρμογές που χρησιμοποιεί η Maersk και servers σε 600 τοποθεσίες σε 130 χώρες κατέστησαν μη προσβάσιμες.
Οικονομικές απώλειες: Οι οικονομικές επιπτώσεις ήταν σημαντικές. Η Maersk εκτίμησε ότι η κυβερνοεπίθεση θα επηρέαζε αρνητικά τα αποτελέσματά της κατά 200-300 εκατ. δολάρια. Αυτό το ποσό αντικατοπτρίζει το κόστος που σχετίζεται με την ανάκαμψη, τον χρόνο διακοπής λειτουργίας και τις χαμένες επιχειρηματικές ευκαιρίες.
Προβλήματα στην εφοδιαστική αλυσίδα: Η επίθεση επηρέασε την εφοδιαστική αλυσίδα. Τα λιμάνια αντιμετώπισαν προβλήματα στη διαχείριση των πλοίων και καθυστερήσεις. Η απώλεια χωρητικότητας σε επίπεδο κλάδου στη διαδρομή από την Άπω Ανατολή προς τη Βόρεια Ευρώπη και τη Μεσόγειο κατά τη διάρκεια του β' τριμήνου εκτιμήθηκε σε 15-20% και επηρέασε το παγκόσμιο εμπόριο.
Μη δυνατότητα πρόσβασης σε δεδομένα: Η μεγάλη εξάρτηση της Maersk από τα δεδομένα επιδείνωσε την κατάσταση. Για την διαχείριση κάθε εμπορευματοκιβωτίου απαιτούνταν περίπου 300 σελίδες πληροφοριών για τελωνειακά, υποστηρικτικά και εισαγωγικά/εξαγωγικά έγγραφα. Η μη διαθεσιμότητα αυτών των δεδομένων δημιούργησε μεγάλο πρόβλημα στις εργασίες της Maersk.
Η επίθεση NotPetya στη Maersk ήταν το περιστατικό αφύπνισης της ναυτιλιακής βιομηχανίας, υπογραμμίζοντας την αναγκαιότητα αύξησης των επενδύσεων στην κυβερνοασφάλεια και στην ασφάλιση Cyber Insurance για την διαχείριση του κινδύνου.
Καθώς οι ναυτιλιακές εταιρείες πλέουν στην ψηφιακή εποχή, η ασφάλιση στον κυβερνοχώρο καθίσταται απαραίτητο μέρος της στρατηγικής τους για τη διαχείριση κινδύνων. Περισσότερα στοιχεία για την ασφάλιση Cyber Insurance των ναυτιλιακών εταιριών μπορείται να βρείτε στην εκπαιδευτική μηχανή www.maritimecyberinsurance.com.