Αυξημένα κρούσματα ψηφιακών επιθέσεων σε ελληνικές ναυτιλιακές

2020/07/07 13:10 στην κατηγορία ΝΑΥΤΙΛΙΑ

Ευάλωτες σε ψηφιακές επιθέσεις αποδεικνύονται οι ναυτιλιακές εταιρείες, παγκοσμίως, μεταξύ αυτών και οι ελληνικές, όπως μετέδωσε ο ΣΕΠΕ.

Όσο προχωρά ο ψηφιακός μετασχηματισμός του τομέα και όσο αυξάνεται η συνδεσιμότητα, ο ναυτιλιακός κλάδος μπαίνει στο στόχαστρο του κυβερνο-εγκλήματος.

Το σύνολο των ελληνικών ναυτιλιακών επιχειρήσεων, που συμμετείχαν στην έρευνα, διαπιστώνει αύξηση των καταστροφικών κυβερνοεπιθέσεων κατά το τελευταίο δωδεκάμηνο.

Οι μισές από τις αυτές εκτιμούν ότι η αύξηση των περιστατικών ήταν μικρότερη από 10%, με το 25% να αναφέρει ότι τα περιστατικά κυβερνοεπιθέσεων αυξήθηκαν κατά 25% ή και περισσότερο.

Πάντως, παρά την αύξηση των κρουσμάτων, σύμφωνα με τη μελέτη “Global Information Security Survey 2020” της EY, για τις ελληνικές ναυτιλιακές το ζήτημα της κυβερνοασφάλειας αποτελεί χαμηλότερη προτεραιότητα, σε σύγκριση με το σύνολο των επιχειρήσεων, που συμμετείχαν στην παγκόσμια έρευνα.

Για την ακρίβεια, το θέμα των ψηφιακών επιθέσεων βρίσκεται χαμηλά στη λίστα των προτεραιοτήτων των διοικήσεων των εταιρειών.

Το 57% των στελεχών του ελληνικού ναυτιλιακού κλάδου απαντά ότι τα Διοικητικά Συμβούλια των επιχειρήσεών τους δεν αντιμετωπίζουν τις κυβερνοαπειλές, ως κρίσιμο κίνδυνο. Επιπλέον, το 71% των στελεχών αναφέρει ότι τα Διοικητικά Συμβούλια ασχολούνται με ζητήματα κυβερνοασφάλειας σε ad hoc βάση.

Σύμφωνα πάντα με την έρευνα, το 71% των ελληνικών ναυτιλιακών επιχειρήσεων δαπανά λιγότερο από $100.000 ετησίως για την κυβερνοασφάλεια.

Μάλιστα, παράλληλα, καμία ελληνική ναυτιλιακή επιχείρηση δεν δαπανά πάνω από $1 εκατ. για αυτόν τον σκοπό.

Ρυθμιστικό πλαίσιο

Ενδιαφέρον παρουσιάζει το εύρημα της έρευνας ότι ένας στους δύο ερωτώμενους στην Ελλάδα (50%) εκτιμά ότι το ρυθμιστικό καθεστώς για την κυβερνοασφάλεια είναι ανεπαρκές.

Παρά το ανεπαρκές ρυθμιστικό περιβάλλον και τις χαμηλότερες δαπάνες, ένα στα τέσσερα στελέχη (25%), θεωρεί ότι είναι πολύ πιθανό να αντιληφθεί μια κυβερνοεπίθεση με κακόβουλο λογισμικό (malware), που χρησιμοποιεί αρχεία, προγράμματα και βιβλιοθήκες, τα οποία προσφέρονται από το λειτουργικό σύστημα και όχι προσαρμοσμένα, customized malware (“living off the land” attacks).

“Η ολοένα και μεγαλύτερη εξάρτηση της ναυτιλίας από ψηφιακά συστήματα και ο αυξανόμενος ρυθμός υιοθέτησης νέων τεχνολογιών, καθιστούν την κυβερνοασφάλεια άμεση προτεραιότητα για τις ναυτιλιακές επιχειρήσεις. Ο αυξημένος βαθμός έκθεσης σε κινδύνους στον κυβερνοχώρο, συναρτάται άμεσα με την αύξηση στη συνδεσιμότητα”, διαπιστώνει η ΕΥ Ελλάδος.

Πλαίσιο κυβερνοασφάλειας

Με στόχο τη θωράκιση από τα περιστατικά, η ΕΥ συνιστά στις επιχειρήσεις του κλάδου μερικές βασικές αρχές, όπως η εκπαίδευση και ενημέρωση του πληρώματος, η κατάτμηση των δικτύων, το ενημερωμένο λογισμικό, η ασφαλής παραμετροποίηση και η τήρηση αντιγράφων ασφαλείας.

Βασικό εργαλείο για τις ναυτιλιακές εταιρείες παγκοσμίως θα αποτελέσει το πλαίσιο κυβερνοασφάλειας του Διεθνούς Ναυτιλιακού Οργανισμού (International Maritime Organization – IMO), το οποίο θα τεθεί σε ισχύ την 1η Ιανουαρίου 2021. Το πλαίσιο βασίζεται σε πέντε πυλώνες: αναγνώριση, ανταπόκριση, προστασία, ανάκαμψη και εντοπισμός.