ΠΑΝΕΛΛΗΝΙΟΣ ΕΝΩΣΙΣ ΠΛΟΙΑΡΧΩΝ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ ΠΑΣΗΣ ΤΑΞΕΩΣ

ΕΤΟΣ ΙΔΡΥΣΕΩΣ 1916

ΑΡ.ΠΡΩΤ. ΠΕΙΡΑΙΑΣ 30-7-2019

Προς τα
Αξιότιμα Μέλη της
Πανελλήνιας Ένωσης Πλοιάρχων Ε.Ν.

Θέμα: USCG / Νεότερη Ναυτιλιακή Αγγελία σχετικά με κυβερνο-επιθέσεις σε εμπορικά πλοία

Εφαρμογή: Αφορά ποντοπόρα εμπορικά πλοία.

Σχετικά: Εγκύκλιος ΕΕΕ υπ' αρ. 8134/1.6.2019

Περίληψη: Η εγκύκλιος παρέχει ενημέρωση για την έκδοση νεότερης ναυτιλιακής αγγελίας από την Αμερικανική Ακτοφυλακή (USCG), που εστιάζει σε πρόσφατη κυβερνο-επίθεση με χρήση κακόβουλου λογισμικού σε ποντοπόρο πλοίο και παρέχει συστάσεις βασικών μέτρων για τη βελτίωση της κυβερνο-ασφάλειας των πλοίων.

Σε συνέχεια της ανωτέρω σχετικής εγκυκλίου μας, έχουμε την τιμή να σας γνωρίσουμε ότι η Αμερικανική Ακτοφυλακή (USCG) εξέδωσε τη Ναυτιλιακή Αγγελία (Marine Safety Alert) **06/19** που αφορά σε πρόσφατη κυβερνο-επίθεση με χρήση κακόβουλου λογισμικού σε ποντοπόρο πλοίο που επηρέασε σημαντικά το δίκτυο του πλοίου (shipboard network).

Από έρευνα που διετέλεσε ομάδα ειδικών στην κυβερνο-ασφάλεια της USCG διαπιστώθηκε ότι παρόλο που δεν επηρεάστηκαν σημαντικά συστήματα ελέγχου του πλοίου, ήταν ελλιπής η εφαρμογή αποτελεσματικών μέτρων ασφάλειας του κυβερνοχώρου. Επιπρόσθετα, βρέθηκε ότι το δίκτυο του πλοίου που χρησιμοποιείτο από το πλήρωμα, χρησιμοποιείτο και για υπηρεσιακούς λόγους, όπως επικαιροποίηση ηλεκτρονικών χαρτών, στοιχεία φορτίου και επικοινωνία με την ξηρά.

Με αφορμή το περιστατικό αυτό, από την USCG συνιστάται ανεπιφύλακτα οι διαχειρίστριες εταιρείες και οι εμπλεκόμενοι χειριστές να ακολουθούν τα κάτωθι βασικά μέτρα:

- Να γίνει τμηματικός διαχωρισμός δικτύων (Segment Networks). Προτείνεται διαχωρισμός των δικτύων σε "υποδίκτυα" (subnetworks) προκειμένου να επαυξάνεται ο βαθμός δυσκολίας κάποιου επιτήδειου χάκερ να αποκτήσει πρόσβαση σε βασικά συστήματα και εξοπλισμό του πλοίου.
- Να δημιουργηθούν προφίλ και κωδικοί πρόσβασης ανά χρήστη. Προτείνεται η εξάλειψη χρήσης γενικών διαπιστευτηρίων σύνδεσης για πολλαπλούς χρήστες και η δημιουργία προφίλ δικτύου για κάθε εργαζόμενο με χρήση μοναδικού κωδικού πρόσβασης και/ή κάρτας ταυτοπροσωπίας (ID card). Προτείνεται επίσης περιορισμός της πρόσβασης μόνο στα επίπεδα (levels) που είναι απαραίτητα σε κάθε χρήστη για υπηρεσιακούς λόγους.

Οι λογαριασμοί του διαχειριστή του δικτύου θα πρέπει να χρησιμοποιούνται μόνο όταν είναι απαραίτητο.

- Να δίδεται προσοχή στη χρήση εξωτερικών μέσων (External Media). Το περιστατικό αυτό αποκάλυψε ότι είναι κοινή πρακτική τα δεδομένα/στοιχεία φορτίου να μεταφέρονται στην αποβάθρα μέσω φορητού δίσκου USB. Είναι κρίσιμο για οποιοδήποτε εξωτερικό μέσο, να προηγείται σάρωση, πριν τη σύνδεσή του σε οποιοδήποτε δίκτυο του πλοίου, για τυχόν κακόβουλα λογισμικά σε αυτόνομο σύστημα.
- Να γίνει εγκατάσταση και τακτική επικαιροποίηση βασικού λογισμικού προστασίας από ιούς.
- Να εκτελούνται επιδιορθώσεις των λογισμικών προγραμμάτων (patch computing).

Πρόσθετη πληροφόρηση σχετικά με παροχή πληροφοριακού υλικού προς βελτίωση των δικτύων που χρησιμοποιούν τα πλοία μπορεί να αναζητηθεί στην ναυτιλιακή αγγελία της USCG που διατίθεται στον ηλεκτρονικό σύνδεσμο:

https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG5PC/INV/Alerts/0619.pdf

Παρακαλούμε για την ενημέρωσή σας.

Μετά τιμής
Ο Πρόεδρος

Εμμανουήλ Τσικαλάκης