Κυβερνοασφάλεια (Cybersecurity)

Εκδ. 1

Κυβερνοχώρος (Cybespace) και Κυβερνοασφάλεια (Cybersecurity)

- Κυβερνοχώρος
  - Αποτελείται από Ηλεκτρονικούς Υπολογιστές (Η/Υ) και δίκτυα, μέσω των οποίων οι Η/Υ είναι συνδεδεμένοι μεταξύ τους προκειμένου να εξυπηρετείται η ροή των πληροφοριών, να κατανέμεται η επεξεργασία και να διευκολύνονται οι επικοινωνίες
  - Σε αυτόν αποθηκεύονται ψηφιακά δεδομένα
- Κυβερνοασφάλεια: αφορά στην ασφάλεια του κυβερνοχώρου σε θέματα σχετικά με την πρόσβαση, τον έλεγχο και την αποθήκευση δεδομένων

Στρατηγικές στον τομέα της ασφάλειας στον κυβερνοχώρο

- Δημιουργία αντιγράφων ασφαλείας
- Ενημέρωση των πληροφοριακών συστημάτων
- Εκπαίδευση στελεχών
- Παρακολούθηση του περιβάλλοντος πληροφοριών, προκειμένου να αναγνωρίζουν οι επιχειρήσεις πότε επιχειρείται επίθεση
- Πολλαπλά επίπεδα ασφαλείας (έλεγχος πρόσβασης, προστασία από κακόβουλο λογισμικό κλπ)
- Προετοιμασία για την παραβίαση

Παράδειγμα επίθεσης στη ναυτιλία

- Στις 27 Ιουνίου 2017, έγινε επίθεση στην εταιρεία A.P. Moller Mayersk, από το κακόβουλο λογισμικό NotPetya (ή ExPetr) (ransomware).
- Το κακόβουλο λογισμικό διέκοψε την online κράτηση και διαχείριση του φορτίου, υποχρεώνοντας το προσωπικό να χρησιμοποιεί προσωπικούς λογαριασμούς για να απαντήσει σε κρίσιμα ζητήματα
- Χρειάστηκε σχεδόν μια εβδομάδα ώστε να αποκατασταθεί το ζήτημα
- Κατά την επίθεση προκλήθηκε πρόβλημα σε περίπου 80 λιμάνια που λειτουργούσαν με το σύστημα της APM και το κόστος έφτασε στα 300 εκ δολάρια.

Ψήφισμα IMO MSC.428(98) - 16 Ιουν 2017

- Από έρευνα της SeaIntel (αρχές 2017), προκύπτει ότι το 44% των 50 κορυφαίων μεταφορέων έχουν ανεπαρκείς πολιτικές και αδυναμίες στις διαδικασίες για την ασφάλεια στον κυβερνοχώρο (π.χ. ασθενείς κωδικοί πρόσβασης, ελλιπής εφαρμογή updates)
- Προτρέπει τη δημιουργία ενός εγκεκριμένου συστήματος διαχείρισης της ασφάλειας του κυβερνοχώρου από όλους τους εμπλεκόμενους φορείς, σύμφωνα με τους στόχους και τις λειτουργικές απαιτήσεις του ISM
- Αναπτύσσει τις κατευθυντήριες γραμμές στην εγκύκλιο MSC-FAL.1/Circ.3 Guidelines on Maritime Cyber Risk Management, που περιέχει συστάσεις για τη διαχείριση του θαλάσσιου κυβερνοχώρου και τη διασφάλιση της ναυτιλίας από απειλές και αδυναμίες. Σύμφωνα με το βιβλίο πληροφορικής, αυτή η εγκύκλιος παραμένει ακόμη μη υποχρεωτική για τους πλοιοκτήτες

Κυβερνοασφάλεια - Κυβερνοπροστασία

Η κυβερνοασφάλεια ασχολείται με την προστασία των συστημάτων του πλοίου από:

- μη εξουσιοδοτημένη πρόσβαση πληροφοριών και δεδομένων
- σφάλματα χειρισμών
- άρνηση πρόσβασης

Η κυβερνοπροστασία καλύπτει τον κίνδυνο από απώλεια:

- διαθεσιμότητας των συστημάτων
- ακεραιότητας των κρίσιμων δεδομένων
- των κρίσιμων λειτουργικών συστημάτων

Σχέδιο διαχείρισης κινδύνου στον κυβερνοχώρο

Θα πρέπει να μπορεί να:

- προσδιορίσει και να διαχειριστεί τους ρόλους και τις ευθύνες των χρηστών (στο σκάφος και στη ξηρά)

- εντοπίσει τις ευπάθειες (αδύναμα σημεία) και να εκτιμήσει τον κίνδυνο
- εφαρμόσει τεχνικά μέτρα και διαδικασίες για την προστασία από περιστατικό και τη συνέχιση της ομαλής λειτουργίας
- υλοποιήσει δραστηριότητες για την προετοιμασία και την αντιμετώπιση περιστατικών

Η διαχείριση των πιθανών απειλών στον κυβερνοχώρο πρέπει να περιλαμβάνεται στον κώδικα ISPS

Ιός στο σύστημα ECDIS καθυστερεί τον απόπλου

Ένα νεότευκτο πλοίο μεταφοράς χύδην φορτίου (dry bulk), το οποίο σχεδιάστηκε, ώστε να στηρίζεται στα ηλεκτρονικά συστήματα και στους ηλεκτρονικούς χάρτες, χωρίς να έχει καθόλου έντυπους χάρτες, καθυστέρησε τον απόπλου του εξαιτίας ιού στο σύστημα ηλεκτρονικών χαρτών ECDIS. Οι αξιωματικοί του πλοίου δεν κατάφεραν να αναγνωρίσουν ότι επρόκειτο για ιό και θεώρησαν ότι υπάρχει τεχνικό σφάλμα στο ECDIS. Ένας τεχνικός από την κατασκευάστρια εταιρία χρειάστηκε να επισκεφθεί το πλοίο και, μετά από μεγάλο διάστημα προσπαθειών, ανακάλυψε ότι και τα δύο δίκτυα ECDIS είχαν μολυνθεί από ιό. Ο ιός τέθηκε σε καραντίνα και τα συστήματα αποκαταστάθηκαν. Η πηγή και τα μέσα μόλυνσης σε αυτήν την περίπτωση είναι άγνωστα. Η καθυστέρηση στον απόπλου του πλοίου και το κόστος επισκευών ανήλθαν σε εκατοντάδες χιλιάδες δολάρια (ΗΠΑ).

Προσδιορισμός των απειλών

- Οι απειλές στον κυβερνοχώρο δεν έχουν εμφανή αντίκτυπο και δεν υπάρχουν αναφορές, καθώς οι περισσότερες εταιρείες δεν ανακοινώνουν τα αντίστοιχα προβλήματα
- Υπάρχουν διάφορα κίνητρα των επιτιθέμενων όπως δυσαρεστημένο προσωπικό, ανταγωνισμός, αναζήτηση κέρδους (π.χ. από εκβιασμό).
- ΠΡοβλήματα ασφαλείας μπορεί να προκύψουν και κατά λάθος, π. χ. από ανθρώπινο σφάλμα (όπως διαγραφή αρχείων)

Πίνακας 4.1
Κίνητρα και στόχοι

Ποιος μπορεί να το κάνει	*Κίνητρα*	*Στόχοι – Τρόποι επίτευξης των στόχων τους*
Ακτιβιστές (ακόμα και δυσαρεστημένοι υπάλληλοι)	▸ Προσβολή της φήμης της εταιρίας ▸ Διακοπή των λειτουργιών της εταιρίας	▸ Καταστροφή δεδομένων ▸ Δημοσίευση ευαίσθητων δεδομένων ▸ Πρόκληση της προσοχής των ΜΜΕ ▸ Άρνηση πρόσβασης στην υπηρεσία ή στο τελικό σύστημα
Εγκληματίες	▸ Οικονομικό κέρδος ▸ Εμπορική κατασκοπεία ▸ Βιομηχανική κατασκοπεία	▸ Πώληση κλεμμένων δεδομένων ▸ Επιδίωξη λύτρων για τα κλεμμένα δεδομένα ▸ Επιδίωξη λύτρων για να επιτραπεί η συνέχιση λειτουργίας των συστημάτων ▸ Πραγματοποίηση δόλιων μεταφορών φορτίων ▸ Συγκέντρωση πληροφοριών ακριβούς τοποθεσίας φορτίου, σχεδίων μεταφοράς και διαχείρισης, για πιο εξεζητημένες εγκληματικές ενέργειες όπως κλοπή φορτίου
Καιροσκόποι	▸ Πρόκληση, κομπασμός	▸ Διείσδυση στις άμυνες του συστήματος ασφάλειας ▸ Οικονομικό κέρδος
Κράτη Χρηματοδοτούμενοι Οργανισμοί από κράτη Τρομοκράτες	▸ Πολιτικό όφελος ▸ Κατασκοπεία	▸ Απόκτηση πρόσβασης σε σημαντικές πληροφορίες ▸ Αποδιοργάνωση οικονομιών και κρίσιμων εθνικών υποδομών

Τύποι κυβερνοεπίθεσης

- Μη στοχευμένες επιθέσεις
  Η εταιρεία αποτελεί έναν από τους πολλούς πιθανούς στόχους
- Στοχευμένες επιθέσεις
  Το σύστημα και τα δεδομένα μιας εταιρείας αποτελούν τον επιδιωκόμενο στόχο

Εργαλεία/τεχνικές επιτιθέμενων

- Malware. Κακόβουλο λογισμικό που έχει σχεδιαστεί για να προκαλέσει βλάβη. Υπάρχουν διάφοροι τύποι, όπως:
  - ιός (virus). Όταν εκτελείται, αναπαράγεται προσκολώμενος σε άλλα προγράμματα
  - σκουλήκι (worm). Αυτόνομο πρόγραμμα, που αναπαράγεται για να μολύνει άλλα μηχανήματα
  - Δούρειος ίππος (trojan horse). Λογισμικό που παραπλανά τους χρήστες για την πραγματική του πρόθεση
  - Ransomware. Κρυπτογραφεί τα δεδομένα του θύματος και απειλεί να αποκλείσει την πρόσβαση σε αυτά, εκτός αν καταβληθούν λύτρα
-

Ομηρία εταιρίας και πλοίου για λύτρα (ransomware)

Υπήρξε αναφορά εταιρίας ότι τα εταιρικά δίκτυα μολύνθηκαν από ιό που ζητούσε λύτρα για να τα αποκαταστήσει. Η πηγή από την οποία προήλθε ο ιός φαινόταν να είναι ένα επισυναπτόμενο αρχείο ηλεκτρονικού ταχυδρομείου από δύο πράκτορες πλοίων. Οι πράκτορες, όμως, δεν είχαν αποστείλει οι ίδιοι το email. Αυτό συνέβη σε δύο διαφορετικές περιπτώσεις, σε ξεχωριστά λιμάνια. Τα δίκτυα των πλοίων επηρεάστηκαν και αυτά, αλλά δεν υπήρξε επίδραση στην αξιοπλοΐα τους. Στη συγκεκριμένη περίπτωση πληρώθηκαν τα λύτρα, αν και αυτό δεν συστήνεται.

Η σημασία αυτού του περιστατικού είναι ότι όχι μόνο η εταιρία, αλλά και οι έμπιστοι επιχειρηματικοί εταίροι της, πρέπει να καταβάλλουν προσπάθειες για την ασφάλεια του κυβερνοχώρου. Όλοι στην αλυσίδα εφοδιασμού θα πρέπει να συνεργάζονται για να μετριάζουν τους κινδύνους στον κυβερνοχώρο.

Εργαλεία/τεχνικές επιτιθέμενων

- Spyware. Λογισμικό υποκλοπής, που συλλέγει πληροφορίες και τις αποστέλλει σε άλλη οντότητα, εν αγνοία μας
- Adware. εισάγει αυτόματα διαφημίσεις στα προγράμματά μας, δημιουργώντας έσοδα για το δημιουργό του
- Scareware. κακόβουλο λογισμικό που χρησιμοποιεί την κοινωνική μηχανική για να προκαλέσει σοκ, άγχος ή να απειλήσει, έτσι ώστε να χειραγωγήσει τους χρήστες


ΤΜΗΜΑ ΑΣΦΑΛΕΙΑΣ ΑΤΤΙΚΗΣ
Διωξης Ηλεκτρονικού Εγκλήματος
Προσοχή!
Αυτό το λειτουργικό σύστημα μπλοκάρεται λόγω παραβίασης των νόμων της Ελλάδας! Σημειώθηκαν οι ακόλουθες παραβιάσεις:
IP διεύθυνσή σας είναι "
". Από αυτή την IP διεύθυνση επισκέφτηκαν ιστοσελίδες που περιέχουν πορνογραφία, την παιδική πορνογραφία, κτηνοβασία, και τη βία κατά των παιδιών. Ο
ολογιστής σας επίσης περιείχε βίντεο που περιλαμβάνει πορνογραφία, βία και παιδική πορνογραφία! Επιπλέον, από το ηλεκτρονικό ταχυδρομείο σας αποστελλόταν μηνύματα με τη μορφή spam, που
περιείχαν τρομοκρατική πρόθεση.
Αυτό το μπλοκάρισμα του υπολογιστή έγινε για να σταματήσουν οι παράνομες δραστηριότητές σας.
Τα στοιχεία σας:
Τοποθεσία: Greece, Athens
ISP: Tellas S.A.
ια να ξεκλειδώσετε τον υπολογιστή, πρέπει να πληρώσετε
ρόστιμο 100 ευρώ.
πορείτε να πληρώσετε ποινή με δύο τρόπους:
) Μέσω του συστήματος Ukash:
α να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής
9-ψήφιο κωδικό και να πατήσετε ΟΚ (αν έχετε πολλαπλούς κωδικούς, πρέπει να
σάγετε ένα προς ένα, και στη συνέχεια κάντε κλικ στο ΟΚ).
ν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους
δικούς στη διεύθυνση economic-crime@hellenicpolice.gr
) Πληρωμή μέσω Paysafecard:
α να πληρώσετε με αυτό το τρόπο πρέπει να εισάγετε στη μορφή της καταβολής
να 16-ψήφιο κωδικό (αν είναι αναγκαίο, με έναν κωδικό πρόσβασης), και στη
υνέχεια κάντε κλικ στο ΟΚ (εάν έχετε πολλαπλούς κωδικούς, πρέπει να εισάγετε
να προς ένα, και στη συνέχεια κάντε κλικ στο ΟΚ).
ν στη διαδικασία πληρωμής θα γίνει σφάλμα, θα πρέπει να στείλετε τους
δικούς στη διεύθυνση economic-crime@hellenicpolice.gr
Ukash Πού μπορώ να αγοράσω Ukash?
Μπορείτε να προμηθευτείτε Ukash σε εκατοντάδες σημεία παγκοσμίως, online, από πορτοφόλια, καταστήματα ψιλικών και μηχανήματα αυτόματης ανάληψης.
KKT - ΚΚΤ Αγοραστέ την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & ψιλικών
kapa change
Kapa - Αγοραστέ την Ukash σε επιλεγμένα σημεία λιανικής στην Ελλάδα όπως περίπτερα και καταστήματα τροφίμων & ψιλικών
OK
paysafecard Πού μπορώ να αγοράσω Paysafecard?
Payzone Hellas είναι η μεγαλύτερη εταιρεία κινητής τηλεφωνίας top-up δικτύου στην Ελλάδα με εγκατεστημένη πάνω από 11.000 τερματικά POS. Payzone Hellas πρωταγωνιστεί, επίσης, πληρωμή λογαριασμών και υπηρεσιών κοινής ωφελείας για την προκαταβολή και τους παρόχους υπηρεσιών στην Ελλάδα.

Εργαλεία/τεχνικές επιτιθέμενων

- phishing: ενέργεια εξαπάτησης των θυμάτων, κατά την οποία ο επιτιθέμενος υποδύεται μια αξιόπιστη οντότητα, με σκοπό να αποκτήσει προσωπικούς κωδικούς
- water holing. επίθεση σε μηχάνημα ενός ατόμου που ανήκει σε μια ομάδα, οργάνωση κλπ. Ο επιτιθέμενος παρατηρεί τη δραστηριότητα του ατόμου π.χ. ποιούς ιστοτόπους παρακολουθεί και τους μολύνει
- scanning. Τυχαία επίθεση σε μεγάλο μέρος του δικτύου
- Social engineering. Κακόβουλες δραστηριότητες που πραγματοποιούνται μέσω κοινωνικών αλληλεπιδράσεων. Χρησιμοποιεί τη ψυχολογική χειραγώγηση (π.χ. για να αποσπάσει κωδικούς)

Social engineering - Κέβιν Μίτνικ

- Ένας από τους πιο διάσημους Αμερικάνους χάκερς
- Χρησιμοποίησε τεχνικές social engineering π.χ. πήρε τηλέφωνο το διαχειριστή ενός συστήματος προσποιούμενος ότι είχε χάσει τον κωδικό του και τον έπεισε να του φτιάξει καινούριο.
- Φυλακίστηκε. Όταν αποφυλακίστηκε, του απαγόρευσαν τη χρήση συσκευών με πληκτρολόγιο. Σήμερα έχει δική του εταιρεία ασφαλείας και κάνει σεμινάρια σχετικά με το θέμα


WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

Εργαλεία/τεχνικές επιτιθέμενων

- Brute Force. Εξαντλητική δοκιμή κωδικών, με την ελπίδα να βρεθεί ο σωστός
- Denial of Service (DoS). Επίθεση εναντίον ενός υπολογιστή ή υπηρεσίας, έτσι ώστε να τον/την καταστήσει ανίκανη να εξυπηρετήσει τους χρήστες.
- Spear-phishing. Μοιάζει με το phishing, αλλά το άτομο στοχοποιείται π.χ. με email

Στάδια κυβερνοεπίθεσης

- Παρακολούθηση/αναγνώριση: ο επιτιθέμενος αποκτά πληροφορίες για το στόχο του μέσω π.χ. social media, τεχνικών forums, χρήσης ειδικών εργαλείων
- Εγκατάσταση του κακόβουλου προγράμματος, με διάφορους τρόπους όπως email, μολυσμένες συσκευές usb
- Παραβίαση συστήματος, που μπορεί να οδηγήσει σε αλλαγές στο σύστημα από τον επιτιθέμενο, πρόσβαση σε ευαίσθητα δεδομένα
- Pivot. Χρήση του παραβιασμένου συστήματος, για να επιτεθεί σε άλλα συστήματα π.χ. εντός του πλοίου

Κατάρρευση εν πλω των λειτουργιών πλοήγησης σε σύστημα ολοκληρωμένης Γέφυρας

Ένα πλοίο που έπλεε σε περιοχή με μεγάλη κυκλοφορία και μειωμένη ορατότητα, υπέστη κατάρρευση των συστημάτων πλοήγησης. Μέχρι να φτάσει στο λιμάνι για επισκευές, το πλοίο έπρεπε, για δύο ημέρες, να πλοηγηθεί με ένα μόνο ραντάρ και απλούς χάρτες. Η αιτία της αποτυχίας όλων των υπολογιστών ECDIS αποδόθηκε στα ξεπερασμένα λειτουργικά συστήματα. Βρέθηκε ότι στο προηγούμενο λιμάνι που βρισκόταν το πλοίο, ένας τεχνικός προχώρησε σε αναβάθμιση του λογισμικού πλοήγησης. Το ξεπερασμένο λειτουργικό σύστημα του υπολογιστή δεν ήταν σε θέση να λειτουργήσει με το καινούργιο λογισμικό και κατέρρευσε. Το πλοίο έμεινε στο λιμάνι μέχρις ότου εγκατασταθούν σε αυτό καινούργιοι υπολογιστές για το σύστημα ECDIS, με την έγκριση των επιθεωρητών. Παράλληλα, εκδόθηκε αναφορά γεγο-

επιθεωρητών. Παράλληλα, εκδόθηκε αναφορά γεγονότος που δεν είχε αποτέλεσμα τον τραυματισμό, την ασθένεια ή την καταστροφή, αλλά υπήρχε περίπτωση να συμβεί. Το κόστος των καθυστερήσεων ήταν μεγάλο και το ανέλαβε η ιδιοκτήτρια εταιρία. Αυτό το περιστατικό τονίζει ότι δεν είναι όλες οι αποτυχίες των υπολογιστών αποτέλεσμα μιας σκόπιμης επίθεσης και ότι το ξεπερασμένο λογισμικό είναι επιρρεπές σε αποτυχία. Η προληπτική συντήρηση του λειτουργικού συστήματος θα είχε αποτρέψει αυτό το περιστατικό. Επίσης η διαδικασία των ενημερώσεων πρέπει να είναι αντιστρεπτή και να περιλαμβάνει και στοιχειώδεις δοκιμές λειτουργικότητας.

Συστήματα με τρωτά σημεία

Συστήματα στα οποία συνήθως παρουσιάζονται τρωτά σημεία:

- συστήματα διαχείρισης φορτίου
- συστήματα γέφυρας
- συστήματα πρόωσης και ελέγχου μηχανών
- συστήματα ελέγχου πρόσβασης
- συστήματα εξυπηρέτησης και διαχείρισης επιβατών
- συστήματα διαχείρισης δημόσιων σταθερών ή ασύρματων δίκτυων
- διοικητικά συστήματα και συστήματα διαχείρισης ελεύθερου χρόνου
- συστήματα επικοινωνιών

Συνηθισμένα τρωτά σημεία σε συστήματα πλοίου

- παρωχημένα και μη υποστηριζόμενα επιχειρησιακά συστήματα
- παρωχημένο λογισμικό προστασίας από ιούς
- Ανεπαρκείς διαμορφώσεις ασφαλείας π.χ. χρήση default κωδικών διαχειριστή
- δίκτυα, χωρίς μέτρα προστασίας
- εξοπλισμός ή συστήματα που συνδέονται συνεχώς με τη στεριά
- ανεπαρκείς έλεγχοι πρόσβασης για τρίτους π.χ. εργολάβους

Κατάρρευση υπολογιστή πλοήγησης κατά τη διάρκεια πλοήγησης από πιλότο

Στην περίπτωση αυτή το πλοίο κινούνταν υπό την καθοδήγηση πιλότου. Ένας πιλότος ήταν πάνω στο πλοίο όταν το σύστημα ECDIS και ο υπολογιστής απόδοσης ταξιδιού κατέρρευσαν. Η κατάρρευση οδήγησε σε αμηχανία των αξιωματικών επί του πλοίου. Αλλά ο Πλοίαρχος και ο πιλότος βοήθησαν να πλοηγηθεί με ασφάλεια το πλοίο, με οπτική επαφή και χρησιμοποιώντας το ραντάρ. Όταν οι υπολογιστές προχώρησαν σε επανεκκίνηση, αποδείχτηκε ότι το λειτουργικό σύστημα ήταν ξεπερασμένο και δεν υποστηριζόταν πλέον από την κατασκευάστρια εταιρία. Ο Πλοίαρχος ανέφερε ότι αυτά τα προβλήματα ήταν συχνά (αποκαλούνται «gremlins») και ότι υπήρχαν συχνές αναφορές στην εταιρία, οι οποίες δεν εισακούστηκαν. Στο περιστατικό αυτό γίνεται φανερό ότι η έγκαιρη επίλυση των προβλημάτων του πλοίου από την εταιρία, μπορεί να αποτρέψει ατυχήματα.

Αξιολόγηση κινδύνου - Αντικείμενο διερεύνησης

Κατά την αξιολόγηση, διερευνώνται τα εξής:

- Ποιά στοιχεία βρίσκονται σε κίνδυνο;
- ποιά είναι η πιθανή συνέπεια από ένα περιστατικό;
- ποιός είναι υπεύθυνος για τη διαχείριση του κινδύνου;
- είναι τα συστήματα προστατευμένα από το ίντερνετ;
- υπάρχει δυνατότητα απομακρυσμένης πρόσβασης (remote access);
- ποιές καλές πρακτικές (π.χ. συχνή αλλαγή κωδικών) εφαρμόζονται για την εξάλειψη του κινδύνου;
- ποιό είναι το επίπεδο εκπαίδευσης του προσωπικού

Στην αξιολόγηση, είναι αναγκαίο να συμμετέχει και η διευθυντική ομάδα της εταιρείας, για διάφορους λόγους όπως την ανάδειξη της σπουδαιότητας του ζητήματος και τη διερεύνηση των αλλαγών που θα γίνουν σε επιχειρησιακό επίπεδο κλπ (όχι μόνο τεχνικά μέτρα)

Παράμετροι που αναλύονται κατά την αξιολόγηση

1. Πρόσβαση από τρίτους (π.χ. απομακρυσμένη πρόσβαση, τεχνικοί που ανεβαίνουν στο πλοίο, συστήματα τρίτων τα οποία επικοινωνούν με τα συστήματα του καραβιού)
2. Αξιολόγηση των επιπτώσεων από μια πιθανή επίθεση
3. Ατομικές συσκευές των εργαζομένων (Bring Your Own Device - BYOD)

Επίθεση ιού (Worm attack) στα ναυτιλιακά πληροφοριακά και επιχειρησιακά συστήματα

Το πλοίο ήταν εφοδιασμένο με σύστημα διαχείρισης ενέργειας, το οποίο μπορούσε να συνδεθεί στο Διαδίκτυο για αναβάθμιση λογισμικού, απομακρυσμένη διάγνωση, συλλογή δεδομένων και απομακρυσμένη λειτουργία. Στο πλοίο, αν και είχε φτιαχτεί πρόσφατα, το σύστημα δεν ήταν συνδεδεμένο στο Διαδίκτυο από τον σχεδιασμό, αλλά η σύνδεση θα γινόταν εκ των υστέρων. Μετά από έλεγχο που αποφάσισε να κάνει το τμήμα πληροφορικής της εταιρίας για να βρει αν υπάρχουν ευπάθειες του συστήματος και αν μπορεί να συνδεθεί με το δίκτυο, ανακάλυψε έναν αδρανή ιό, ο οποίος θα ενεργοποιούνταν μόλις συνδεόταν το σύστημα στον υπολογιστή. Οι συνέπειες θα ήταν σοβαρές, αν είχε συνδεθεί το σύστημα στο δίκτυο.

Περιστατικό Πέμπτ

Το περιστατικό αποδεικνύει ότι ακόμα και τα συστήματα που δεν είναι συνδεδεμένα σε δίκτυο μπορούν να εκτεθούν σε κίνδυνο, και δείχνει πόσο σημαντική είναι η προληπτική διαχείριση του κυβερνοχώρου.

Η πλοιοκτήτρια εταιρία ενημέρωσε την κατασκευάστρια για την ανακάλυψη και ζήτησε την κατάλληλη διαδικασία, ώστε να διαγραφεί ο ιός. Στα αρχεία της πλοιοκτήτριας εταιρίας είχε καταγραφεί επίσκεψη τεχνικού στο πλοίο και πιστεύεται ότι η μόλυνση μπορεί να προήλθε από τον τεχνικό και μια μολυσμένη συσκευή αφαιρούμενων μέσων (USB). Ο ιός αυτός είχε σχεδιαστεί για να επικοινωνεί με τον εξυπηρετητή εντολών και ελέγχου του, ώστε να λαμβάνει το επόμενο σύνολο οδηγιών. Θα μπορούσε ακόμη και να δημιουργήσει αρχεία και φακέλους.

Η εταιρία ζήτησε από εξειδικευμένο προσωπικό να διεξάγει έρευνα και αποκατάσταση. Η έρευνα έδειξε ότι όλοι οι διακομιστές που σχετίζονταν με το σύστημα ήταν μολυσμένοι με τον ιό, ο οποίος βρισκόνταν στο σύστημα για 875 μέρες. Εργαλεία σάρωσης απομάκρυναν τον ιό και η ανάλυση έδειξε ότι η μόλυνση τελικά προήλθε από μολυσμένη συσκευή αφαιρούμενων μέσων κατά την εγκατάσταση λογισμικού. Ο ιός ήταν αποθηκευμένος στη μνήμη του συστήματος και θα ενεργοποιούνταν μόλις θα συνδεόταν στον διακομιστή, επηρεάζοντας την απόδοση.

Αξιολόγηση επιπτώσεων

Χρησιμοποιείται το μοντέλο C.I.A. του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST)

- Confidentiality (Εμπιστευτικότητα)
- Integrity (Ακεραιότητα)
- Availability (Διαθεσιμότητα)

Εμπιστευτικότητα (Confidentiality)

Είναι η μη αποκάλυψη ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένα άτομα.

Έλλειψη εμπιστευτικότητας μπορεί να προκύψει π.χ. αν ένας χρήστης έχει πρόσβαση στα προσωπικά δεδομένα ενός άλλου χρήστη

Ακεραιότητα (Integrity)

Διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση, χωρίς ανεπιθύμητες τροποποιήσεις από μη εξουσιοδοτημένα άτομα.

Απώλεια ακεραιότητας μπορει να προκύψει αν π.χ. κάποιος χρήστης αλλάξει (αλλοιώσει) τα δεδομένα των τραπεζικών λογαριασμών που είναι αποθηκευμένα μέσα σε ένα πληροφοριακό σύστημα

Διαθεσιμότητα (Availability)

Διαθεσιμότητα σημαίνει να είναι τα συστήματα, δίκτυα, δεδομένα κλπ διαθέσιμα όταν τα χρειάζεται κάποιος χρήστης.

Απώλεια διαθεσιμότητας μπορεί να προκύψει π.χ. αν υποστεί ζημιά κάποιος server και οι χρήστες δε μπορούν να χρησιμοποιήσουν τις εφαρμογές που βρίσκονται εγκατεστημένες σε αυτόν

Κατηγορίες Επιπτώσεων

- Χαμηλή. Η απώλεια της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας έχει μόνο περιορισμένο αντίκτυπο στην εταιρεία ή το πλοίο π.χ. υποβάθμιση της επιχειρησιακής ικανότητας του πλοίου για μικρό χρονικό διάστημα, απουσία τραυματισμών
- Μέτρια. Η απώλεια της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας έχει σημαντική αρνητική επίπτωση στην εταιρεία ή το πλοίο, στα περιουσιακά στοιχεία ή τα άτομα π.χ. υποβάθμιση της επιχειρησιακής ικανότητας του πλοίου για μεγάλο χρονικό διάστημα, μικροτραυματισμοί
- Υψηλή. Η απώλεια της εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας έχει σοβαρές καταστροφικές συνέπειες στην εταιρεία ή το πλοίο στα περιουσιακά στοιχεία ή τα άτομα π.χ. ολοκληρωτική απώλεια της λειτουργίας του πλοίου, σοβαροί τραυματισμοί απειλητικοί για τη ζωή

Ποιοί κάνουν την αξιολόγηση

- Η εταιρεία
- Τρίτοι. Αυτοί μπορεί να αξιολογήσουν τους κινδύνους αφού τελειώσει την αξιολόγησή της η εταιρεία. Συνήθως είναι εξειδικευμένες εταιρείες, με ιδιαίτερη τεχνογνωσία

Διαδικασία αξιολόγησης

- Φάση 1. Δραστηριότητες προ-αξιολογησης (καταγραφή υφιστάμενης κατάστασης, μελέτη εγχειριδίων κλπ).
- Φάση 2. Αξιολόγηση πλοίου (χρήση του μοντέλου CIA για εντοπισμό ευπαθειών)
- Φάση 3. Αναθεώρηση και αναφορά/καταγραφή ευπάθειας (σύνοψη βασικών σημείων, λίστα ενεργειών που πρέπει να γίνουν)
- Φάση 4. Αναφορά κατασκευαστών (γνωστοποίηση τρωτών σημείων σε κατασκευάστες συστημάτων, ώστε να γίνουν οι απαραίτητες διορθώσεις)

Ανάπτυξη μέτρων προστασίας και ανίχνευσης

- Πρέπει να υπάρχει προστασία σε πολλαπλά επίπεδα (φυσική ασφάλεια πλοίου, προστασία δικτύων, δημιουργία λίστας εγκεκριμένων προγραμμάτων και εφαρμογών, δικαιώματα χρηστών, έλεγχος πρόσβασης κλπ)
- Τα μέτρα προστασίας χωρίζονται σε
  - τεχνικά
  - διαδικαστικά

Τεχνικά μέτρα προστασίας

- περιορισμός και έλεγχος θυρών δικτύου, πρωτοκόλλων και υπηρεσιών π.χ. απαγόρευση χρήσης torrents
- διαμόρφωση/ρύθμιση συσκευών δικτύου όπως routers, τείχος προστασίας
- φυσική ασφάλεια π.χ. κάρτες ασφαλείας για πρόσβαση σε αίθουσες με servers
- προστασία επικοινωνιών με διάφορους τρόπους όπως VPN
- Διαχείριση/συστηματική εφαρμογή updates
- .....

Διαδικαστικά μέτρα προστασίας

- Εκπαίδευση και ενημέρωση των χρηστών (προσωπικό του πλοίου, προσωπικό της στεριάς)
- Έλεγχος της πρόσβασης των επισκεπτών π.χ. πρακτόρων, τεχνικών
- καθορισμός διαφόρων διαδικασιών που σχετίζονται με θέματα ασφάλειας π.χ. να γίνεται έλεγχος σε αφαιρούμενες συσκευές USB, προτού χρησιμοποιηθούν
- ….

Περιστατικό Έκτο

Πρόσβαση επιθεωρητή δεξαμενών καυσίμων στο διοικητικό δίκτυο του πλοίου

Σε πλοίο μεταφοράς χύδην φορτίου, αφού τελείωσε ο ανεφοδιασμός, επιβιβάστηκε ο επιθεωρητής δεξαμενών καυσίμων και ζήτησε πρόσβαση σε υπολογιστή για να εκτυπώσει το έγγραφο προς υπογραφή. Ο επιθεωρητής χρησιμοποίησε ένα φορητό μέσο αποθήκευσης και, χωρίς να το γνωρίζει, εισήγαγε ένα κακόβουλο λογισμικό στο δίκτυο διαχείρισης του πλοίου. Το κακόβουλο λογισμικό δεν εντοπίστηκε, μέχρι που το πλήρωμα ανέφερε προβλήματα στα επιχειρησιακά δίκτυα. Τότε ακολουθήθηκε η διαδικασία εκτίμησης κινδύνου του πλοίου και ανιχνεύτηκε ο ιός.

Το περιστατικό αυτό αναδεικνύει την ανάγκη ύπαρξης διαδικασιών που απαγορεύουν ή περιορίζουν τη χρήση φορητών μέσων αποθήκευσης ακόμα και στους επισκέπτες.

Διακομιστής κύριας εφαρμογής μολυσμένος με ιό καταβολής λύτρων (ransomware)

Ο ιός μόλυνε τον διακομιστή και προκάλεσε διακοπή των πληροφοριακών συστημάτων. Ο ιός κρυπτογράφησε κάθε αρχείο, με αποτέλεσμα να χαθούν κρίσιμα δεδομένα, και έτσι δεν μπορούσαν να χρησιμοποιηθούν από τα συστήματα του πλοίου. Το περιστατικό επαναλήφθηκε ακόμα και μετά την αποκατάσταση του διακομιστή. Η αιτία της μόλυνσης ήταν ο πολύ αδύναμος κωδικός εισόδου ως συνέπεια μιας αδύναμης πολιτικής, που επέτρεψε στους επιτιθέμενους να εγκαταστήσουν υπηρεσίες απομακρυσμένης πρόσβασης. Το τμήμα πληροφορικής της εταιρίας απενεργοποίησε τον μην πιστοποιημένο χρήστη και επέβαλε μια πιο αυστηρή πολιτική για τους κωδικούς εισόδου στα συστήματα του πλοίου.

Σχέδιο έκτακτης ανάγκης

Ενεργοποιείται όταν συμβεί κάποιο περιστατικό. Δίνει προτεραιότητα σε επείγουσες ενέργειες. Μπορεί να περιλαμβάνει:

- Αποσύνδεση επιχειρησιακών συστημάτων πλοίου από συστήματα στη στεριά, για προστασία του πλοίου από επιθέσεις
- Σενάρια για το τί πρέπει να γίνει π.χ. σε περίπτωση επίθεσης με ransomware - αν πρέπει να πληρωθούν τα λύτρα
- αναφορές που θα πρέπει να γίνουν σε περίπτωση επίθεσης
- ενέργειες για ανάκτηση της λειτουργίας των συστημάτων
- διάφορα άλλα…

Το σχέδιο έκτακτης ανάγκης πρέπει να υπάρχει σε έντυπη μορφή, ώστε να μην υπάρχει εξάρτηση από τυχόν μολυσμένα συστήματα. Επίσης, πρέπει να βρίσκεται τόσο πάνω στο πλοίο όσο και στην εταιρεία