ΚΥΒΕΡΝΟΧΩΡΟΣ

ΚΑΘΗΓΗΤΗΣ: ΕΜΜΑΝΟΥΗΛ ΒΟΛΟΣ

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η κυβερνοασφάλεια προστατεύει τα συστήματα σχετικά με τη λειτουργία του πλοίου και των πληροφοριακών συστημάτων από:

- Μη εξουσιοδοτημένη πρόσβαση πληροφοριών και δεδομένων
- Σφάλματα χειριστών
- Άρνηση πρόσβασης

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Η κυβερνοπροστασία καλύπτει τον κίνδυνο από απώλεια:

- Διαθεσιμότητας των συστημάτων
- Ακεραιότητας των κρίσιμων για την ασφάλεια δεδομένων
- Των λειτουργικών συστημάτων

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Θέματα κυβερνοασφάλειας που μπορεί να προκύψουν:

- Επιρροή διαθεσιμότητας και ακεραιότητας των λειτουργικών συστημάτων
- Σφάλμα κατά τη συντήρηση του λογισμικού
- Απώλεια ή αλλοίωση δεδομένων εξωτερικών αισθητήρων (πχ GNSS)

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Σχέδιο διαχείρισης κινδύνου στον κυβερνοχώρο:

- Προσδιορίζει και διαχειρίζεται ρόλους και ευθύνες χρηστών προσωπικού ξηράς και επί του σκάφους
- Εντοπίζει σημεία (στα συστήματα, δεδομένα και εφαρμογές) που αν αλλοιωθούν δημιουργούν κινδύνους

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

- Εφαρμόζει διαδικασίες για προστασία από περιστατικό και εξασφαλίζει συνέχεια των εργασιών
- Υλοποιεί δραστηριότητες για προετοιμασία και αντιμετώπιση των περιστατικών στον κυβερνοχώρο

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

- Απειλές μπορεί να προκύψουν και αποτο εσωτερικό της εταιρείας
- Ζημιά μπορεί να προκληθεί και από ανθρώπινο σφάλμα

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Τύποι κυβερνοεπίθεσης

- **Στοχευμένες επιθέσεις** (σύστημα και δεδομένα εταιρείας αποτελούν τον στόχο)
- **Μη στοχευμένες επιθέσεις** (σύστημα και δεδομένα εταιρείας είναι ένας από τους πολλούς στόχους)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Παραδείγματα εργαλείων για μη στοχευμένες επιθέσεις:

- **Malware** (λογισμικό με στόχο την πρόκληση βλάβης):
  - **Ιός** (πρόγραμμα που μολύνει υπολογιστές)
  - **Σκουλήκι** (αναπαράγεται και μειώνει επιδόσεις)
  - **Δούρειος Ίππος** (χρησιμοποιεί θύματα για να επιτεθεί σε άλλους στόχους)
  - **Ransomware** (κρυπτογράφηση δεδομένων θύματος και αποκλεισμός πρόσβασης)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

- **Spyware** (συλλογή δεδομένων και αποστολή τους σε τρίτους)
- **Adware** (εισαγωγή αυτόματων διαφημίσεων κατά την διάρκεια εγκατάστασης)
- **Scareware** (προώθηση ανεπιθύμητων λογισμικών μέσω απειλών)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Παραδείγματα εργαλείων για μη στοχευμένες επιθέσεις:

- **Phishing** (εξαπάτηση με την προβολή αξιόπιστου αποστολέα)
- **Water Holing** (μόλυνση ιστοσελιδών που επισκέπτεται το στοχευμένο θύμα)
- **Scanning** (τυχαία επίθεση σε μεγάλο μέρος του Διαδικτύου)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Παραδείγματα εργαλείων για στοχευμένες επιθέσεις:

- **Social Engineering** (χειραγώγηση μέσω ανθρώπινων αλληλεπιδράσεων για αποκάλυψη ευαίσθητων πληροφοριών)
- **Brute Force** (εξαντλητική δοκιμή πιθανών κωδικών)
- **Denial of Service** (πρόκληση ανικανότητας θύματος να δεχτεί άλλες συνδέσεις)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Παραδείγματα εργαλείων για στοχευμένες επιθέσεις:

- **Spear-phising** (αποστολή προσωπικών μηνυμάτων ηλεκτρονικού ταχυδρομείου με κακόβουλο λογισμικό)
- **Subverting the supply chain** (επίθεση σε θύμα εκθέτοντας σε κίνδυνο εξοπλισμό και λογισμικά που του παραδίδονται)

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Στάδια κυβερνοεπίθεσης:

1. **Παρακολούθηση-αναγνώριση** (social media, forums, ιστοσελίδα θύματος)
2. **Εγκατάσταση κακόβουλου προγράμματος**, μέσω:
   - **Ηλεκτρονικών υπηρεσιών θύματος**
   - **Αποστολής email με κακόβουλο λογισμικό στο προσωπικό της εταιρείας**
   - **Παροχής μολυσμένων αφαιρετικών μέσων**
   - **Δημιουργίας ψευδών ιστότοπων με ενθάρρυνση εισαγωγής κωδικών προσωπικού**

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Στάδια κυβερνοεπίθεσης:

3. **Παραβίαση συστήματος**, με τον επιτιθέμενο:
   - Να πραγματοποιεί αλλαγές για επιρροή λειτουργίας συστήματος
   - Να αποκτά πρόσβαση σε εμπορικά ευαίσθητα δεδομένα
   - Να επιτυγχάνει πλήρη έλεγχο ενός συστήματος

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΑΠΕΙΛΩΝ

Στάδια κυβερνοεπίθεσης:

4. **Pivot** με τον επιτιθέμενο να προσπαθεί:
   - Να εγκαταστήσει εργαλεία στο σύστημα
   - Να αποκτήσει πλήρη εικόνα του δικτύου
   - Να εγκαταστήσει εργαλεία ή καταγραφέα κωδικών
   - Να εκτελέσει νέες επιθέσεις στο σύστημα

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Τρωτά σημεία χωρίζονται σε:

- Συστήματα επί του πλοίου
- Συστήματα επικοινωνίας και διασύνδεσης πλοίου με στεριά

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Συστήματα επί του πλοίου

- Συστήματα Διαχείρισης Φορτίου
- Συστήματα Γέφυρας
- Συστήματα Πρόωσης και Ελέγχου Μηχανών
- Συστήματα Ελέγχου Πρόσβασης
- Συστήματα Εξυπηρέτησης και Διαχείρισης Επιβατών

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Συστήματα επί του πλοίου

- Συστήματα Διαχείρισης Δημόσιων Σταθέρων ή Ασύρματων Δικτύων
- Διοικητικά Συστήματα και Συστήματα Διαχείρισης Ελεύθερου Χρόνου
- Συστήματα Επικοινωνιών

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Συστήματα Επικοινωνίας και Διασύνδεσης Πλοίου με Στεριά

- Τοπικές Εφαρμογές
- Διαβαθμισμένη Πρόσβαση
- Ιδιαίτερη Προσοχή στους Όρους Αποδοχής των Υπηρεσιών

ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ

Συνηθισμένα τρωτά σημεία στα συστήματα πλοίων

- Παρωχημένα μη υποστηριζόμενα επιχειρησιακά συστήματα
- Παρωχημένο λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό
- Ανεπαρκείς διαμορφώσεις ασφάλειας
- Δίκτυα υπολογιστών πλοίων χωρίς μέτρα προστασίας
- Εξοπλισμός που συνδέεται με την στεριά
- Ανεπαρκείς έλεγχοι πρόσβασης από τρίτους

Αξιολόγηση κινδύνου

Ερωτήματα:

- Ποια στοιχεία βρίσκονται σε κίνδυνο
- Ποιες οι συνέπειες από περιστατικό στον κυβερνοχώρο
- Ποιος είναι ο υπεύθυνος διαχείρισης κινδύνου
- Υπάρχει προστασία των συστημάτων από το Internet
- Υπάρχει δυνατότητα απομακρυσμένης χρήσης των συστημάτων
- Υπάρχουν καλές πρακτικές εξάλειψης του κινδύνου
- Ποιο το επίπεδο εκπαίδευσης του εμπλεκόμενου προσωπικού

Αξιολόγηση κινδύνου

Αύξηση διαθέσιμων πληροφοριών λόγω:

- Αυξανόμενης χρήσης των Big Data
- Έξυπνων πλοίων
- Internet of Things

Αξιολόγηση κινδύνου

Κατηγορία Επίπτωσης	Ορισμός	Επεξήγηση
Χαμηλή	Περιορισμένο αρνητικό αντίκτυπο σε εταιρεία και πλοίο	- Μικρές οικονομικές ζημιές - Απουσία τραυματισμών - Μείωση αποτελεσματικότητας λειτουργιών του πλοίου
Μέτρια	Σημαντική αρνητική επίπτωση σε εταιρεία και πλοίο	- Σημαντικές οικονομικές ζημιές - Πιθανά ατυχήματα - Προβλήματα λειτουργιών του πλοίου
Υψηλή	Σοβαρές αρνητικές επιπτώσεις σε εταιρεία και πλοίο	- Σημαντικές οικονομικές ζημιές - Σοβαρή βλάβη σε άτομα - Ζημιές στο περιβάλλον - Αδυναμία εκτέλεσης μιας/πολλών λειτουργιών πλοίου

Αξιολόγηση κινδύνου

Διαδικασία Αξιολόγησης Κινδύνου

Φάση 1: Δραστηριότητες προ-αξιολόγησης

– Καταγραφή βασικών λειτουργιών και έλεγχος βάσει μοντέλου CIA

– Εντοπισμός κατασκευαστών πληροφοριακών συστημάτων

– Μελέτη εγχειριδίων κρίσιμων συστημάτων

– Εντοπισμός σημείων επικοινωνίας με κατασκευαστές

–Μελέτη εγχειριδίων συντήρησης συστημάτων

–Καθορισμός συμβατικών απαιτήσεων

– Υποστήριξη εκτίμησης κινδύνου με εξωτερικό εμπειρογνώμονα

Αξιολόγηση κινδύνου

Διαδικασία Αξιολόγησης Κινδύνου

Φάση 2: Αξιολόγηση πλοίου

Τρωτά σημεία και ευπάθειες κατηγοριοποιούνται σε:

-Τεχνικά θέματα
- Τρόπος πρόσβασης
- Σφάλματα υλοποίησης
- Σφάλματα χρήστη

Αξιολόγηση κινδύνου

Διαδικασία Αξιολόγησης Κινδύνου

Φάση 3: Αναθεώρηση και καταγραφή ευπάθειας

- Σύνοψη κυριότερων σημείων
- Τεχνικά ευρήματα
- Λίστα ενεργειών με προτεραιότητα
- Συμπληρωματικά δεδομένα (τεχνικές λεπτομέρειες)
- Παράρτημα (σύνολο διεργασιών και εργαλείων)

Φάση 4: Αναφορά κατασκευαστών