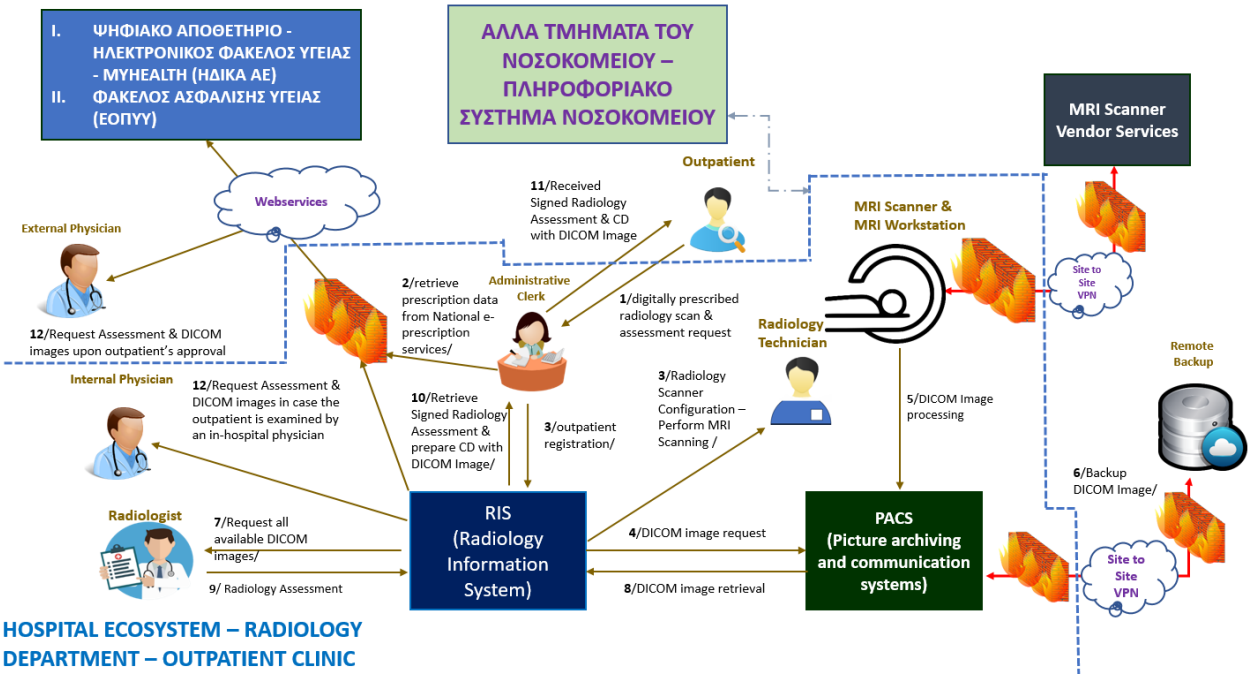
GOOGLE.ORG CYBERSECURITY SEMINARS

ARISTOTLE UNIVERSITY OF THESSALONIKI

ΣΥΜΜΟΡΦΩΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΑΚΤΙΝΟΔΙΑΓΝΩΣΤΙΚΟΥ ΤΜΗΜΑΤΟΣ ΝΟΣΟΚΟΜΕΙΟΥ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ NIS 2

Σας δίδεται στο ακόλουθο σχήμα η επιχειρησιακή διαδικασία (ροή εργασιών) του Ακτινοδιαγνωστικού Τμήματος ενός Νοσοκομείου έχοντας οριστεί **Υπεύθυνος Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών** (ΥΑΣΠΕ).



Αφού μελετήστε το διάγραμμα ροής εργασιών που σας δίνεται παρακαλείστε να εντοπίσετε (μερικά δεν υπάρχουν στο σχήμα) και να εκτελέσετε τις εξής εργασίες:

1. **Αναγνώριση Υπηρεσιών & Συστημάτων:** Ποια είναι τα περιουσιακά στοιχεία (asset inventory) του συστήματος, διαχωρίζοντάς τα σε:
   i. Πληροφοριακά δεδομένα (π.χ. δεδομένα ιατρικά, Εικόνες DICOM, Γνωματεύσεις κτλ).
   ii. Υλισμικοτεχνικά (π.χ. servers, firewalls, τερματικά)
   iii. Λογισμικότεχνικά (π.χ. Πληροφοριακά Συστήματα Βάσεις Δεδομένων κτλ)
   iv. Ανθρώπινοι πόροι (π.χ. υπάλληλοι, διαχειριστές συστήματος)

2. **Αναγνωρίστε τα κρίσιμα σημεία κινδύνου** (risk points) στο διάγραμμα: (Πιθανά σημεία διαρροής ή αλλοίωσης δεδομένων, Σημεία που απαιτούν έλεγχο πρόσβασης ή καταγραφή ενεργειών, Διασυνδέσεις με τρίτους) και **σημεία τρωτότητας**

3. **Καταγράψτε σε ενιαίο πίνακα τα ανωτέρα ευρήματα με τις εξής στήλες**:
   i. Περιγραφή asset (Υπηρεσία/Σύστημα)
   ii. Κατηγορία asset (**Κατηγορία Υπηρεσίας**)
   iii. Περιγραφή
   iv. Κρίσιμη Υπηρεσία (Ναι/Όχι)

v. Πιθανή Ευπάθεια/Απειλή
vi. Τεχνολογία/Πλατφόρμα (Ελεύθερη επιλογή από τη μεριά σας να συμπληρώστε αυτή τη στήλη)
vii. Αξιολόγηση Ασφάλειας (Περίοδος)
viii. Πολιτική Αναφορών Ασφαλείας
ix. Αξιολόγηση Κρίσιμου Κινδύνου (Περιγραφή)
x. Προτεινόμενη Πολιτική Ασφαλείας & Τεχνικό Μέτρο
xi. Συσχέτιση με απαίτηση της NIS2 (να αναφέρετε αντιστοίχηση σε άρθρο της)

Το Παραδοτέο της άσκησης είναι 1 Αρχείο (pdf ή word) με τον ενιαίο πίνακα του παραπάνω ερωτήματος.

Υποδείξεις για την εκτέλεση της άσκησης:

1. Θα πρέπει να δείτε τα βήματα 1 έως 12 του παραπάνω σχήματος που δείχνουν τη ροή των εργασιών στο ακτινοδιαγνωστικό τμήμα για καταγράψετε τα asset. Μελετώντας τη ροή ανιχνεύετε τους ρόλους και τους χρήστες (π.χ. ιατρός, γραμματεία), επίσης ανιχνεύετε τα πληροφοριακά συστήματα (π.χ. RIS, PACS), επίσης ανιχνεύετε τα ακτινοδιαγνωστικά μηχανήματα (π.χ. MRI Scanner, MRI Workstation) τα οποία έχουν εγκατεστημένο firmware (ειδικό λειτουργικό σύστημα) για να λειτουργήσει, επίσης ανιχνεύετε την εφοδιαστική αλυσίδα – επικοινωνία με προμηθευτές (π.χ. MRI Scanner vendors), επίσης ανιχνεύετε εκτός από τα firewall, τις υποδομές των πληροφοριακών συστημάτων (π.χ. Server για RIS κτλ.), τα switch τα οποία δεν είναι ορατά στο διάγραμμα αλλά είναι βασική υποδομή για την δικτυακή επικοινωνία των Η/Υ των Ιατρών, γραμματέων κτλ. (επίσης οι Η/Υ δεν είναι ορατοί στο διάγραμμα). **Προσοχή:** αν και στο σχήμα βλέπετε 5 firewall να θεωρήσετε **1 firewall** εντός τον διακεκομμένων μπλε γραμμών. Το σχήμα είναι εποπτικό και δείχνει όλες τις διασυνδέσεις με τον έξω κόσμο (επικοινωνία με δομές ή ιατρούς εκτός των διακεκομμένων μπλε γραμμών). Η χρήση 1 μόνο firewall μπορεί να επιτελέσει όλες τις εργασίες. **Προσοχή:** δεν καταγράφετε τις υποδομές εκτός των διακεκομμένων μπλε γραμμών.

Α/Α	Υπηρεσία/ Σύστημα	Κατηγορία Υπηρεσίας	Περιγραφή	Κρίσιμη Υπηρεσία (Ναι/Όχι)	Owner	Ευπάθειες ή Απειλές	Τεχνολογία/ Πλατφόρμα	Αξιολόγηση Ασφάλειας (Περίοδος)	Πολιτική Αναφορών Ασφαλείας	Αξιολόγηση Κρίσιμου Κινδύνου (Περιγραφή)	Δικτυακές Πληροφορίες (IP/ Υποδίκτυο)	Πολιτική Ασφάλειας
1	Διακομιστής Ιστοσελίδας	Web Server	Φιλοξενία ιστοσελίδας e-commerce	Ναι	Α.Α.	DDoS, SQL Injection	Apache, Nginx, Linux	Ετήσια Αξιολόγηση	Αναφορά εντός 24 ωρών	Κίνδυνος παραβίασης δεδομένων χρηστών.	**IP:** 192.168.1.10 **Υποδίκτυο:** 192.168.1.0/24	**Πολιτική Συστήματος:** Χρήση ισχυρών κωδικών, εγκατάσταση WAF, περιορισμός πρόσβασης ανά IP. **Αντίδραση σε Επιθέσεις:** Μόνιμο logging, ενεργοποίηση του DDoS protection
2	Βάση Δεδομένων Πελατών	Database Server	Αποθήκευση προσωπικών δεδομένων	Ναι	Α.Α.	SQL Injection,	MySQL, MariaDB	Ετήσια Αξιολόγηση	Αναφορά εντός 48 ωρών	Κίνδυνος διαρροής προσωπικών δεδομένων.	**IP:** 192.168.1.20 **Υποδίκτυο:** 192.168.1.0/24	**Πολιτική Συστήματος:** Ενίσχυση κρυπτογράφησης, περιορισμός πρόσβασης με βάση ρόλους, τακτική αναβάθμιση. **Αντίδραση σε Επιθέσεις:** Ενεργοποίηση αναφορών για μη εξουσιοδοτημένη πρόσβαση, άμεσως αποκατάσταση.
3	FIREWALL	Δίκτυο	Προστασία από μη εξουσιοδοτημένη πρόσβαση	Ναι	Α.Α.	TCP Flood, DoS	Fortinet, Palo Alto	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών	Κίνδυνος παρακάμψης του firewall.	**IP:** 192.168.100.1 **Υποδίκτυο:** 192.168.100.0/24	**Πολιτική Συστήματος:** Διαχείριση κανόνων πρόσβασης, ενεργοποίηση logging, περιορισμός συνδέσεων από άγνωστες IP. **Αντίδραση σε Επιθέσεις:** Ενεργοποίηση αναφορών και άμεση ανάλυση για οποιαδήποτε παραβίαση των κανόνων.
4	Υπηρεσία Παροχής Ενέργειας	Κρίσιμη Υποδομή	Παροχή ενέργειας για λειτουργία οργανισμού	Ναι	Α.Α.	Στατική Διακοπή, Cyber-Physical Attacks	SCADA, PLCs, IoT	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών	Κίνδυνος διακοπής ενεργειακής τροφοδοσίας ή υποδομών.	**IP:** 192.168.10.10 **Υποδίκτυο:** 192.168.10.0/24	**Πολιτική Συστήματος:** Χρήση προστασίας από επιθέσεις σε SCADA, κρυπτογράφηση των επικοινωνιών, παρακολούθηση συνεχώς των ενεργειακών συστημάτων για πιθανές αδυναμίες. **Αντίδραση σε Επιθέσεις:** Άμεση αποσύνδεση από το δίκτυο σε περίπτωση αναγνωρισμένων επιθέσεων. Εφαρμογή στρατηγικής "Air Gap (φυσική ή λογική απομόνωση)" για κρίσιμα συστήματα ενέργειας.

2. Αφού καταγράψετε όλα τα παραπάνω δημιουργήσετε τον πίνακα με τις στήλες που φαίνονται στο παρακάτω πίνακα, ο οποίος σας δίνεται ως παράδειγμα. Τα assets που ανιχνεύσατε τα εισάγετε σε κάθε γραμμή του πίνακα κάτω από τη στήλη **Υπηρεσία/Σύστημα** και συμπληρώστε στη συνέχεια τα στοιχεία των διπλανών στηλών κατά τη δική σας προτίμηση (π.χ. Η/Υ Ιατρού, ανατρέξατε στο διαδίκτυο για να βρείτε 1 ευπάθεια Windows και συμπληρώστε την αντίστοιχη στήλη **ευπάθειες/απειλές).** Στη στήλη **τεχνολογία πλατφόρμα** αναγράψτε π.χ. MS WINDOWS 10 Professional. Στη στήλη Δικτυακές πληροφορίες θέσατε διεύθυνση IP από διευθύνσεις IP:10.10.20.1 έως 10.10.20.250.
3. Για το firewall να θέσετε 2 Διευθύνσεις IP την εσωτερική IP:10.10.20.254 και εξωτερική IP: 173.82.147.219. Θεωρείστε ότι το firewall είναι firmware v.2.5 έτους 2023 στη στήλη **τεχνολογία πλατφόρμα**. Αναζητήσετε στο διαδίκτυο για ευπάθειες από outdated firmware σε firewall και καταγράψτε 1 από αυτές.
4. Για το MRI SCANNER καταγράψτε στη στήλη **τεχνολογία πλατφόρμα** firmware v.0.15 έτους 2021 Αναζητήσετε στο διαδίκτυο για ευπάθειες από outdated firmware σε MRI SCANNER
5. Στη στήλη πολιτική ασφαλείας αναγράψτε τι πρέπει να γίνει για να αντιμετωπιστεί η κάθε ευπάθεια.
6. **Παραδοτέο είναι ο πίνακας με excel.**