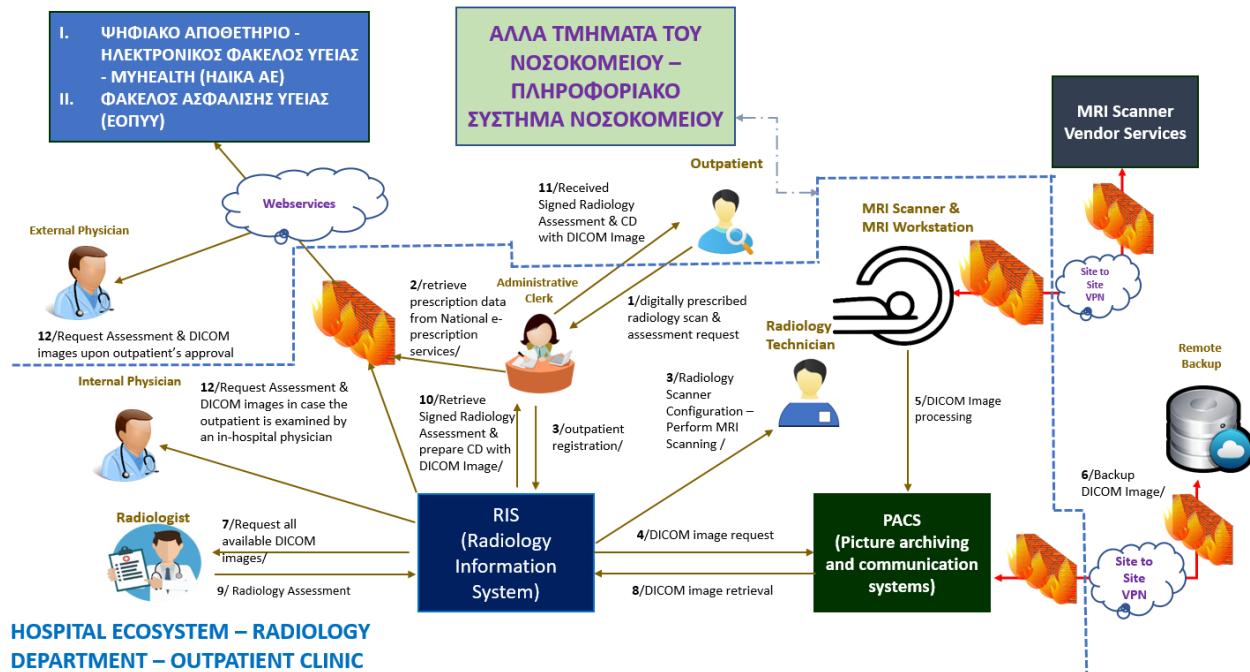


ΣΥΜΜΟΡΦΩΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΑΚΤΙΝΟΔΙΑΓΝΩΣΤΙΚΟΥ ΤΜΗΜΑΤΟΣ ΝΟΣΟΚΟΜΕΙΟΥ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ NIS 2

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:
 - Πληροφοριακά δεδομένα (π.χ. δεδομένα ιατρικά, Εικόνες DICOM, Γνωματεύσεις κτλ).
 - Υλισμικοτεχνικά (π.χ. servers, firewalls, τερματικά)
 - Λογισμικότεχνικά (π.χ. Πληροφοριακά Συστήματα Βάσεις Δεδομένων κτλ)
 - Ανθρώπινοι πόροι (π.χ. υπάλληλοι, διαχειριστές συστήματος)
- 2. Αναγνωρίστε τα κρίσιμα σημεία κινδύνου (risk points) στο διάγραμμα:** (Πιθανά σημεία διαρροής ή αλλοιώσης 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:**
 - Περιγραφή asset (Υπηρεσία/Σύστημα)
 - Κατηγορία asset (Κατηγορία Υπηρεσίας)
 - Περιγραφή
 - 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:

- 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.

A/A	Υπηρεσία/ Σύστημα	Κατηγορία Υπηρεσίας	Περιγραφή Υπηρεσία (Ναι/Οχι)	Owner	Ευπάθειες ή Απειλές	Τεχνολογία/ Πλατφόρμα	Αξιολόγηση Ασφάλειας (Περίοδος)	Πολιτική Αναφορών Κινδύνου Ασφαλείας (Περιγραφή Υποδίκτυου)	Αξιολόγηση Κρίσιμου Υποδίκτυου εις (IP/ Πληροφορί ^η Υποδίκτυου)	Δικτυακές Πληροφορί ^η	Πολιτική Ασφάλειας	
1	Διακομιστής Ιστοσελίδας	Web Server	Φιλοξενία ιστοσελίδας e-Nai commerce	A.A.	DDoS, SQL Injection	Apache, Nginx, Linux	Ετήσια Αξιολόγηση	Αναφορά εντός 24 ωρών παραβίασης χρηστών.	Kινδύνος παραβίασης διαφορούς	IP: 192.168.1.10 Υποδίκτυο: 192.168.1.0/24 ^η ενεργοποίηση του DDoS	Πολιτική Συστήματος: Χρήση ιαυλιών κυβικών, εγκατάσταση WAF περιφερειακώς πρόσβασης ανά IP. Αντίδραση σε Επιθέσεις: Μόνιμη αποστολή ενημέρωσης σε Επιθέσεις.	
2	Βάση Δεδομένων Πελατών	Database Server	Αποθήκευση προσωπικών δεδομένων	Nαι	A.A.	SQL Injection,	MySQL, MariaDB	Ετήσια Αξιολόγηση	Αναφορά εντός 48 ωρών προσωπικών δεδομένων.	Kινδύνος διαφορούς	IP: 192.168.1.20 Υποδίκτυο: 192.168.1.0/24 ^η ενημέρωση πρόσβασης, αποστολή πολιτικής αποστολής.	Πολιτική Συστήματος: Ενίσχυση κρυπτογράφησης περιφερειακώς πρόσβασης με βάση ρόλους, τακτική αναθεώρηση. Αντίδραση σε Επιθέσεις: αποστολή ενημέρωσης σε Επιθέσεις για μετά ενημέρωση πρόσβασης αποστολή πολιτικής αποστολής.
3	FIREWALL	Δίκτυο	Προστασία από μη εξουσιοδοτη- μένη πρόσβαση	Nαι	A.A.	TCP Flood, DoS	Fortinet, Palo Alto	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών	Kινδύνος παρακάμψης tou firewall.	IP: 192.168.100.1 Υποδίκτυο: 192.168.100.0/24 ^η ενημέρωση αποστολής και άμεση απόσπαση για οποιαδήποτε παραβίαση των κανονιών.	Πολιτική Συστήματος: Διαφέρον κανονών πρόσβασης, ενεργοποίηση ενημέρωσης σε Επιθέσεις από την πλευρά εμπορευμάτων. Αντίδραση σε Επιθέσεις: άμεση απόσπαση από το δίκτυο σε τροφοδοτικά ή 192.168.10.0/24 ^η ενημέρωση αποστολής εφαρμογής παραπομπής "Air Gap (φυσική ή λογική απομόνωση)" για κρίσιμα συστήματα ενέργειας.
4	Υπηρεσία Παροχής Ενέργειας	Κρίσιμη Υποδομή	Παροχή ενέργειας για λειτουργία οργανισμού	Nαι	A.A.	Στατική Διακοπή, Cyber-Physical Attacks	SCADA, PLCs, IoT	Ετήσια Αξιολόγηση	Αναφορά εντός 12 ωρών υποδομών.	Kινδύνος διακοπής ενεργειακής τροφοδοτικής	IP: 192.168.10.10 Υποδίκτυο: 192.168.10.0/24 ^η ενημέρωση σε Επιθέσεις Εφαρμογή παραπομπής "Air Gap (φυσική ή λογική απομόνωση)" για κρίσιμα συστήματα ενέργειας.	Πολιτική Συστήματος: Χρήση προστασίας επιθέσεων σε SCADA κρυπτοπρόσθιτης πλατφόρμας αυστηρώς των ενεργειακών συστημάτων για πιθανές αδιναίμες. Αντίδραση σε Επιθέσεις: άμεση απόσπαση από το δίκτυο σε τροφοδοτικά ή 192.168.10.0/24 ^η ενημέρωση αποστολής εφαρμογής παραπομπής "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.**