ΑΡΙΣΤΟΤΕΛΕΙΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΟΝΙΚΗΣ

Στρατηγική Συμμόρφωσης NIS2

Cybersecurity Seminar by Google

Αναφορά 3ης Εργασίας

Νίκος Τουλκερίδης

Ιανουάριος 2026

Περιεχόμενα

1 Εισαγωγή και Σκοπός

Η παρούσα αναφορά συντάχθηκε στο πλαίσιο των αρμοδιοτήτων του Υπεύθυνου Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ), με στόχο την αξιολόγηση και τη διασφάλιση της συμμόρφωσης του Ακτινοδιαγνωστικού Τμήματος του Νοσοκομείου με την Ευρωπαϊκή Οδηγία **NIS 2 (Directive 2022/2555)**, όπως ενσωματώθηκε στην Ελληνική νομοθεσία με τον **Νόμο 5160/2024**. Ως «Βασική Οντότητα» (Essential Entity) στον τομέα της Υγείας, ο οργανισμός οφείλει να λάβει κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διαχείριση κινδύνων (Άρθρο 21 της Οδηγίας / Άρθρο 15 Ν. 5160/2024) και την αποτροπή περιστατικών που θα μπορούσαν να διαταράξουν την παροχή κρίσιμων υπηρεσιών υγείας.

2 Αναγνώριση Υπηρεσιών & Συστημάτων (Asset Inventory)

Η διαδικασία αναγνώρισης περιουσιακών στοιχείων (Asset Inventory) αποτελεί το θεμέλιο για τη Διαχείριση Κινδύνων κατά το Άρθρο 21 της Οδηγίας NIS 2. Στο Ακτινοδιαγνωστικό Τμήμα, εντοπίστηκαν και κατηγοριοποιήθηκαν τα παρακάτω κρίσιμα στοιχεία που υποστηρίζουν την επιχειρησιακή ροή (MRI Examination Workflow).

2.1 Πληροφοριακά Δεδομένα (Data)

Τα δεδομένα αποτελούν το σημαντικότερο περιουσιακό στοιχείο, καθώς εμπίπτουν τόσο στο NIS 2 όσο και στον GDPR (Ευαίσθητα Προσωπικά Δεδομένα Υγείας).

- **Δεδομένα Απεικόνισης (Medical Imaging Data):** Αρχεία τύπου DICOM που παράγονται από τον Μαγνητικό Τομογράφο (MRI). Είναι κρίσιμα για τη διάγνωση (Availability Integrity).
- **Ιατρικό Ιστορικό Δημογραφικά Στοιχεία (PHI/PII):** Ονοματεπώνυμο, ΑΜΚΑ, ιστορικό ασθενούς που λαμβάνονται από το MyHealth/ΗΔΙΚΑ και το Πληροφοριακό Σύστημα Νοσοκομείου (HIS).
- **Ιατρικές Γνωματεύσεις (Medical Reports):** Τα αποτελέσματα της διάγνωσης που συντάσσουν οι ιατροί (Internal/External Physicians).
- **Δεδομένα Διαπίστευσης (Credentials):** Κωδικοί πρόσβασης ιατρών και τεχνικών για είσοδο στα συστήματα (PACS, Workstations).
- **Αρχεία Καταγραφής (Logs):** Δεδομένα κίνησης δικτύου και προσβάσεων (Audit Trails) για λόγους ιχνηλασιμότητας.

2.2 Υλισμικοτεχνικά (Hardware)

Περιλαμβάνει τον φυσικό εξοπλισμό που φιλοξενεί ή επεξεργάζεται τα δεδομένα. Βάσει του δικτυακού σχεδιασμού (Subnet 10.10.20.0/24), διακρίνουμε:

- **MRI Scanner (Μαγνητικός Τομογράφος):** Η κύρια ιατροτεχνολογική συσκευή λήψης δεδομένων.
- **MRI Console/Workstation:** Ο σταθμός εργασίας ελέγχου του τομογράφου (συνδεδεμένος άμεσα με τον Scanner).
- **PACS Server (Picture Archiving and Communication System):** Κεντρικός εξυπηρετητής αποθήκευσης και διαχείρισης εικόνων.
- **Ιατρικοί Σταθμοί Εργασίας (Physician Workstations):** Υπολογιστές που χρησιμοποιούν οι εσωτερικοί ιατροί για επισκόπηση και γνωμάτευση.

- **Δικτυακός Εξοπλισμός (Network Devices):**
  - Perimeter Firewall (Πύλη ασφαλείας προς το δίκτυο του Νοσοκομείου/Internet).
  - Network Switch (για τη διασύνδεση του Subnet 10.10.20.x).

2.3 Λογισμικότεχνικά (Software)

Οι εφαρμογές και τα λειτουργικά συστήματα που εκτελούνται στο hardware.

- **Λειτουργικά Συστήματα (OS):**
  - Windows 10/11 Pro (σταθμοί εργασίας ιατρών).
  - Proprietary OS / Embedded Windows (MRI Console).
  - Windows Server / Linux (PACS Server).
- **Εφαρμογές Υγείας:**
  - PACS Software (Server Client Viewer).
  - RIS Client (Radiology Information System) για διαχείριση ραντεβού/ασθενών.
- **Υπηρεσίες Ιστού (Webservices):** Διασύνδεση με ΗΔΙΚΑ (MyHealth) και ΕΟΠΥΥ (API calls).
- **Λογισμικό Ασφαλείας:** Antivirus/EDR agents, VPN Client (για την απομακρυσμένη υποστήριξη του Vendor).

2.4 Ανθρώπινοι Πόροι (People)

Οι χρήστες που αλληλεπιδρούν με το σύστημα, οι οποίοι αποτελούν συχνά τον ”αδύναμο κρίκο” (Phishing, Social Engineering).

- **Εσωτερικοί Ιατροί (Internal Physicians):** Ακτινολόγοι του νοσοκομείου που κάνουν διάγνωση.
- **Εξωτερικοί Ιατροί (External Physicians):** Συνεργάτες που ενδέχεται να έχουν απομακρυσμένη πρόσβαση ή να λαμβάνουν γνωματεύσεις.
- **Τεχνολόγοι Ακτινολογικού (Technologists):** Χειριστές του MRI Scanner και της Κονσόλας.
- **Διοικητικό Προσωπικό (Secretariat):** Υπάλληλοι γραφείου για την εγγραφή ασθενών.
- **Τεχνική Υποστήριξη Κατασκευαστή (Vendor Support):** Εξωτερικοί τεχνικοί με δικαιώματα διαχειριστή για συντήρηση (μέσω VPN).
- **Διαχειριστής Συστημάτων / ΥΑΣΠΕ (IT Admin / CISO):** Υπεύθυνοι για τη λειτουργία και την ασφάλεια της υποδομής.

3 Αναγνώριση Κρίσιμων Σημείων Κινδύνου

Με βάση την ανάλυση της ροής εργασιών (Workflow) και της αρχιτεκτονικής του συστήματος, εντοπίστηκαν τα ακόλουθα κρίσιμα σημεία κινδύνου που απαιτούν άμεση αντιμετώπιση κατά το Ν. 5160/2024:

3.1 Ασφάλεια Εφοδιαστικής Αλυσίδας (Vendor Remote Access)

Η δυνατότητα απομακρυσμένης πρόσβασης του κατασκευαστή (Vendor Support) στον MRI Scanner για συντήρηση αποτελεί σοβαρό κίνδυνο. Εάν ο λογαριασμός του προμηθευτή παραβιαστεί, επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο (Supply Chain Attack).

- **Σχετική Απαίτηση NIS 2:** Άρθρο 21, παρ. 2δ (Ασφάλεια εφοδιαστικής αλυσίδας).

3.2 Παλαιότητα Λογισμικού (Legacy Systems)

Ο Μαγνητικός Τομογράφος (MRI Scanner) και η Κονσόλα Ελέγχου συχνά λειτουργούν με παλαιότερες εκδόσεις λειτουργικών συστημάτων (π.χ. Windows 7 Embedded ή παλαιότερα), τα οποία δεν λαμβάνουν πλέον ενημερώσεις ασφαλείας, καθιστώντας τα ευάλωτα σε γνωστές επιθέσεις (π.χ. WannaCry/Ransomware).

- **Σχετική Απαίτηση NIS 2:** Άρθρο 21, παρ. 2α (Πολιτικές για την ανάλυση κινδύνου και την ασφάλεια πληροφοριακών συστημάτων).

3.3 Διασύνδεση με Εξωτερικές Υπηρεσίες (Cloud/Webservices)

Η ανταλλαγή δεδομένων με την ΗΔΙΚΑ (MyHealth) και τον ΕΟΠΥΥ μέσω Webservices, καθώς και η αποστολή εικόνων σε Εξωτερικούς Ιατρούς (External Physicians), αυξάνει την επιφάνεια επίθεσης (Man-in-the-Middle attacks) και τον κίνδυνο διαρροής δεδομένων αν δεν χρησιμοποιηθεί ισχυρή κρυπτογράφηση.

3.4 Φυσική Ασφάλεια Ανθρώπινος Παράγοντας

Η χρήση φορητών μέσων (USB/DVD) για την εγγραφή εξετάσεων στους ασθενείς και η φυσική πρόσβαση στα Workstations αποτελούν σημεία εισόδου για κακόβουλο λογισμικό.

4 Μητρώο Συμμόρφωσης & Τεχνικών Μέτρων

Στον πίνακα που ακολουθεί καταγράφονται τα αναγνωρισμένα συστήματα βάσει των απαιτήσεων καταγραφής της Οδηγίας NIS 2.

#	Υπηρεσία / Σύστημα	Κατηγορία	Περιγραφή	Crit.	Own.	Ευπάθειες / Απειλές	Τεχνολογία	Αξιολ. Ασφ.	Report Pol.	Αξιολ. Κινδύνου	Δίκτυο (IP)	Πολιτική Ασφαλείας (NIS 2)
1	MRI Scanner	Hardware (Ιατροτεχνολογικό)	Μονάδα Μαγνητικής Τομογραφίας	Ναι	Head Rad.	• Outdated Firmware • No Security Patching • Physical Access	Firmware v.0.15 (2021)	Ετήσια	24 ώρες	Διακοπή λειτουργίας, Ransomware	10.10.20.10 /24	**Άρθρο 21:** Network Segmentation (VLAN), USB Lock, Απαγόρευση Internet (Air-gapped αν εφικτό).
2	MRI Console	Hardware / Workstation	Σταθμός Ελέγχου MRI	Ναι	Tech.	• SMBv1 exploit • Legacy OS	Windows Emb. Std 7	Ετήσια	24 ώρες	Lateral Movement σε δίκτυο	10.10.20.11 /24	**Άρθρο 21:** Απενεργοποίηση SMBv1, Application Whitelisting, VPN για Vendor.
3	PACS Server	Software / Database	Αποθήκευση Εικόνων (DICOM)	Ναι	IT Admin	• SQL Injection • Unauth. Access	Win Srv 2019, SQL DB	Ετήσια	24 ώρες	Διαρροή PHI (GDPR), Αλλοίωση Δεδομένων	10.10.20.50 Port: 104, 443	**Άρθρο 23:** Κρυπτογράφηση Βάσης (At rest), Backup Policy, Access Logs.
4	Perimeter Firewall	Δίκτυο	Προστασία περιμέτρου	Ναι	CISO	• Outdated Firmware • DDoS • Misconfig	Firmware v.2.5 (2023)	Εξαμη- νιαία	12 ώρες (Σημαντικό)	Παράκαμψη ασφάλειας, Είσβολή στο δίκτυο	Int: 10.10.20.254 Ext: 192.168.100.1	**Άρθρο 21:** Τακτικά Updates, Geo-blocking, IPS/IDS, MFA για VPN.
5	PC Ιατρών	Hardware	Σταθμοί Γνωμάτευσης	Ναι	IT Admin	• Phishing • Weak Passwords	Windows 10/11 Pro	Ετήσια	24 ώρες	Είσοδος Malware, Κλοπή Credentials	10.10.20.101 έως .200	**Άρθρο 21:** Εκπαίδευση χρηστών, MFA, Endpoint Protection (EDR).
6	Webservices (ΗΔΙΚΑ)	Software / Cloud	Διασύνδεση ΕΟΠΥΥ/MyHealth	Ναι	Ext. Provider	• API Key Theft • MITM Attack	REST API / HTTPS	Ετήσια	24 ώρες	Υποκλοπή δεδομένων κατά τη μεταφορά	Outbound Port 443	**Άρθρο 21 (Crypto):** TLS 1.3, Certificate Pinning, IP Whitelisting.

5 Δικτυακή Αρχιτεκτονική & Κανόνες Firewall

Για την προστασία του Ακτινοδιαγνωστικού Τμήματος, σχεδιάστηκε μια αρχιτεκτονική ασφαλείας που διαχωρίζει τα κρίσιμα ιατρικά συστήματα από το γενικό δίκτυο του Νοσοκομείου και το Διαδίκτυο. Η κίνηση ελέγχεται από ένα Περιμετρικό Firewall (Next-Generation Firewall - NGFW).

5.1 Σχήμα Διευθυνσιοδότησης (IP Addressing Scheme)

Το εσωτερικό δίκτυο του τμήματος ορίζεται ως ένα απομονωμένο υποδίκτυο (Subnet) με τα εξής χαρακτηριστικά:

- **Network Address:** 10.10.20.0/24 (Subnet Mask: 255.255.255.0)
- **Firewall Internal Interface (Gateway):** 10.10.20.254
- **Firewall External Interface (WAN/Hospital LAN):** 192.168.100.1 (Στατική IP για επικοινωνία με το υπόλοιπο νοσοκομείο)

Κατανομή Διευθύνσεων IP (IP Allocation):

Εύρος IP	Περιγραφή Χρήσης	Παραδείγματα
10.10.20.2 - .19	Δικτυακός Εξοπλισμός (Switches, APs)	Switch Mgmt IP
10.10.20.20 - .50	**Ιατρικά Μηχανήματα (Critical)**	MRI Scanner, Console
10.10.20.51 - .100	Servers	PACS Server, RIS DB
10.10.20.101 - .200	Σταθμοί Εργασίας (Clients)	PC Ιατρών, Γραμματεία

5.2 Πολιτική Κανόνων Firewall (Firewall Policy)

Η πολιτική ασφαλείας βασίζεται στην αρχή της «Ελάχιστης Πρόσβασης» (Least Privilege). Όλη η κίνηση απαγορεύεται εκτός αν επιτραπεί ρητά.

5.2.1 Κανόνες Εισερχόμενης Κίνησης (Inbound Rules)

Κίνηση από το Εξωτερικό Δίκτυο (WAN/Hospital LAN) προς το Εσωτερικό Δίκτυο (10.10.20.0/24).

Rule ID	Source	Destination	Service/Port	Action
IN-01	**VPN Vendor Pool** (Authenticated)	MRI Console (10.10.20.20)	**RDP (TCP 3389)**	**ALLOW**
Σημείωση: Η πρόσβαση επιτρέπεται μόνο μέσω κρυπτογραφημένου τούνελ (VPN) και όχι απευθείας από το Internet. Ο Vendor λαμβάνει IP από το VPN Pool κατά τη σύνδεση.				
IN-02	Hospital HIS Server	PACS Server (10.10.20.50)	DICOM (104), HL7 (2575)	**ALLOW**
Σημείωση: Για την αποστολή εντολών εξέτασης από τους θαλάμους νοσηλείας.				
IN-DEF	Any	Any	Any	**DENY**

5.2.2 Κανόνες Εξερχόμενης Κίνησης (Outbound Rules)

Κίνηση από το Εσωτερικό Δίκτυο προς το Διαδίκτυο ή το Δίκτυο Νοσοκομείου.

Rule ID	Source	Destination	Service/Port	Action
OUT-01	PACS Server	External Cloud (Disaster Recovery)	HTTPS (443) / SFTP (22)	**ALLOW**
OUT-02	Physician PCs	EOPYY / IDIKA (MyHealth)	HTTPS (443)	**ALLOW**
OUT-03	MRI Scanner	Any Internet	Any	**BLOCK**
Σημείωση: Ο τομογράφος δεν πρέπει να έχει ποτέ πρόσβαση στο Web για αποφυγή malware.				
OUT-DEFAULT	Any	Any	Any	**DENY**