REPUBLIKA SLOVENIJA
MINISTRSTVO ZA ZDRAVJE

NAČRT ZA OKREVANJE IN ODPORNOST

Financira Evropska unija
NextGenerationEU

Stanje in izzivi kibernetske varnosti v praksi

Milan Gabor, Viris

Konferenca NOO eZdravje 2026
Brdo, 3. marec 2026

/Milan Gabor

- etični heker
- direktor
- predavatelj
- trener
- OWASP Maribor vodja
- še vedno heka!

Trenutno stanje kibernetske varnosti v zdravstvu

- **Globalni trendi:**
  - Zdravstvo med najbolj napadanimi sektorji
  - Ransomware kot prevladujoča grožnja
  - Povečanje napadov na dobavitelje IT rešitev
  - Napadi na verige dobav (supply chain)
- **Zakaj je zdravstvo privlačna tarča?**
  - Visoka vrednost zdravstvenih podatkov na črnem trgu
  - Pogosto zastarela IT infrastruktura
  - Pomanjkanje kadrov za kibernetsko varnost
  - Veliko zunanjih izvajalcev

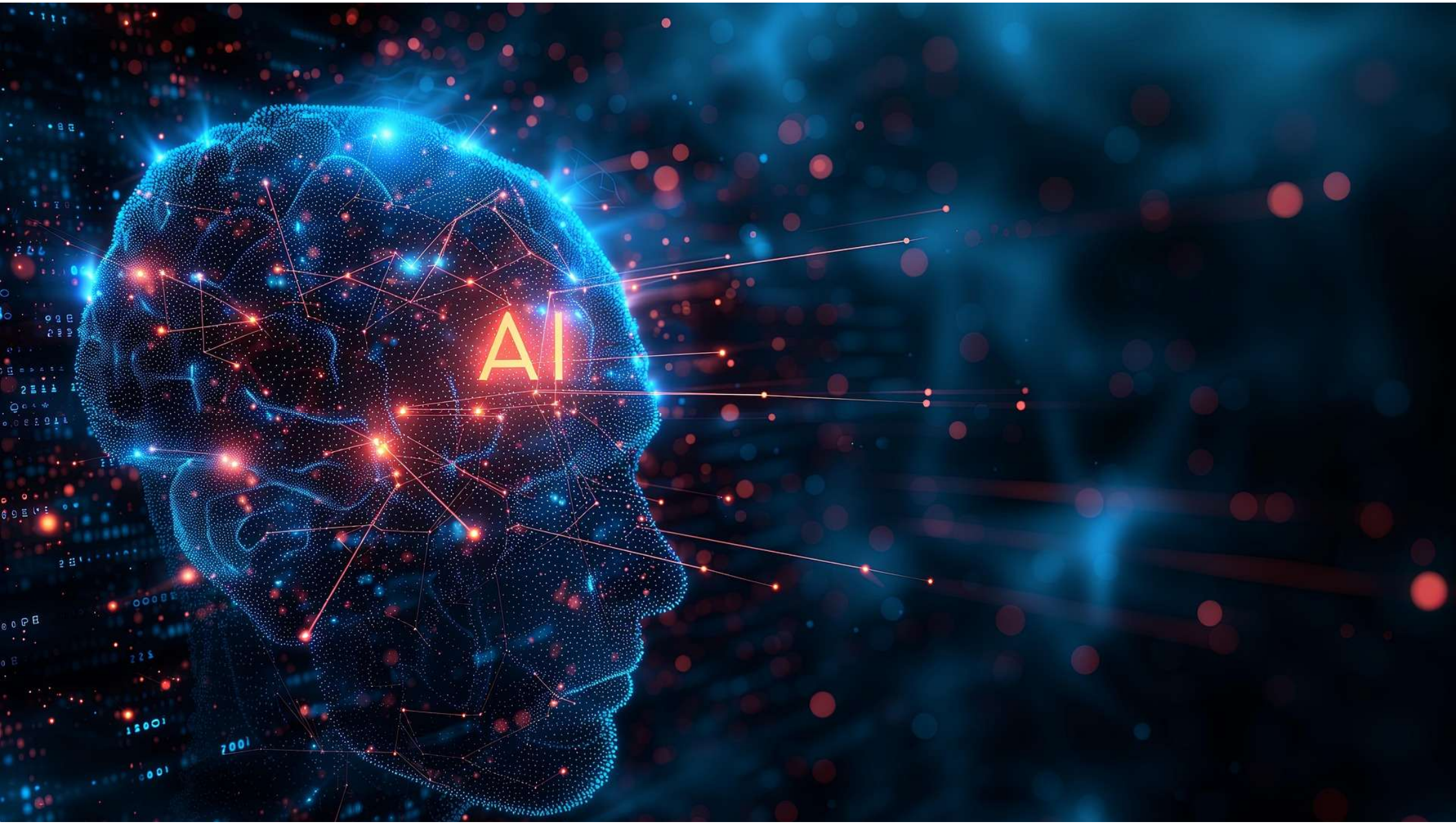
309 incidents
affecting cybersecurity in the health sector were reported in 2023

54%
of cyberattacks in the health sector involve ransomware

https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en

Posledice kibernetskih incidentov

- Prekinitev zdravstvenih storitev
- Odpoved operacij
- Izguba podatkov
- Globe (GDPR, NIS2)
- Škoda na ugledu
- Tožbe pacientov


AI

kakšna je varnost na področju kibernetske varnosti v slovenskem zdravstvu? podkrepi s primeri

Thought for 35s >

Varnost na področju kibernetske varnosti v slovenskem zdravstvu je **neizenačena**: na nacionalni ravni imamo precej centralizirane in standardizirane storitve (npr. eZdravje), hkrati pa je veliko **lokalnih informacijskih okolij (bolnišnice, zdravstveni domovi, lekarne, dobavitelji)**, ki so zaradi kadrovskih, finančnih in tehnoloških omejitev bolj izpostavljena. Splošna slika groženj v Sloveniji se tudi **zaostruje** (več incidentov, več socialnega inženiringa, več izsiljevanja). SI CERT +1

Konkretni primeri iz Slovenije

1. **UKC Maribor (januar 2026): poskus vdora zaznan in prekinjen**
   UKC Maribor je javno navedel, da so varovalni sistemi zaznali vdor in so aktivnosti napadalca omejili; napad je bil prekinjen, preden bi ogrozil delovanje IT sistema. 24ur
2. **Lekarna Ljubljana (avgust 2019): ransomware Ryuk, velike motnje in milijonska škoda**
   SI-CERT in dokumenti navajajo napad z izsiljevalskim virusom Ryuk, ki je povzročil resne motnje v delovanju poslovalnic; škoda je bila ocenjena na **več kot 2 milijona EUR**. SI CERT +2
3. **Zloraba zaupanja v zdravstvo (junij 2020): lažna sporočila v imenu NIJZ**
   V letnem poročilu SI-CERT je opisan primer kampanje, kjer so napadalci pošiljali lažna e-sporočila "v imenu NIJZ" z zlonamerno priponko (LokiBot) za krajo podatkov – tipičen primer, kako je zdravstvo pogosto uporabljeno kot prepričljiva krinka za napade na zaposlene in organizacije. SI CERT

kakšna je varnost na področju kibernetske varnosti v slovenskem zdravstvu? podkrepi s primeri

Varnost v slovenskem zdravstvu je trenutno v fazi intenzivnega prilagajanja in nadgradenj. Čeprav se digitalizacija (eZdravje, eNaročanje, telemedicine) hitro širi, varnostna infrastruktura v preteklosti ni vedno sledila temu tempu, kar je zdravstvene ustanove postavilo v vlogo "mehkih tarč".

Danes je stanje mešanica **visoke stopnje ogroženosti** in **močnega sistemskega odziva**, ki ga narekujejo nove evropske direktive (NIS2).

2. Ključni primeri in incidenti

V zadnjih letih smo bili v Sloveniji priča več dogodkom, ki so razgalili ranljivosti:

- **Napad na zdravstveni dom (marec 2024):** Zabeležen je bil primer napada z izsiljevalsko programsko opremo na enega izmed zdravstvenih domov, kar je povzročilo začasne motnje pri dostopu do kartotek in naročanju pacientov.
- **Phishing kampanje pod krinko uradnih institucij:** Napadalci pogosto uporabljajo lažna e-poštna sporočila, ki izgledajo, kot da jih pošilja Ministrstvo za zdravje ali ZZZS, da bi od zaposlenih pridobili gesla za dostop do centralnih sistemov.
- **Incidenti v lekarnah in specializiranih zavodih:** SI-CERT je v letih 2024 in 2025 zabeležil porast incidentov v širšem zdravstvenem sektorju, kjer so tarče predvsem informacijski sistemi za upravljanje z zalogami zdravil in recepti.

Zakaj je kibernetska varnost v zdravstvu kritična?

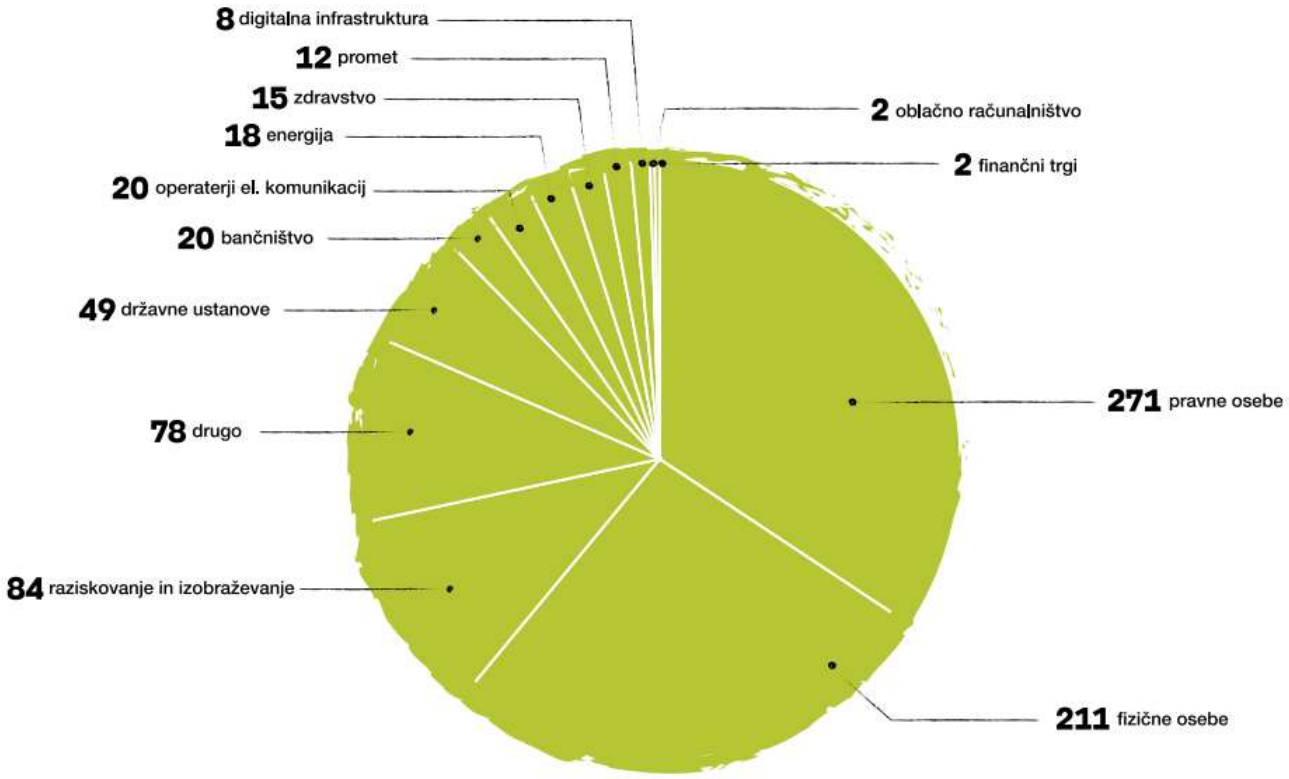
- **Ključne značilnosti zdravstvenega sektorja:**
- Visoka občutljivost podatkov (osebni in zdravstveni podatki)
- Neprekinjeno delovanje (24/7 sistemi)
- Veliko število povezanih naprav (IoT, medicinska oprema)
- Nizka toleranca na izpade sistemov
- Kompleksno regulativno okolje (GDPR, nacionalna zakonodaja)

- Kibernetski napad v zdravstvu ni samo finančno tveganje – je neposredno tveganje za življenje in zdravje pacientov.

Realna slika, ki jo vidimo v letih 2025 in 2026

- **Vzpon izsiljevalskih virusov (Ransomware 2.0):** Ne gre več le za zaklepanje podatkov, temveč za grožnjo z javno objavo občutljivih zdravstvenih kartotek (dvojna izsiljevanja)
- **Napad na oskrbovalne verige:** Napadalci ne napadajo le bolnišnic, ampak njihove ponudnike programske opreme za e-naročanje ali diagnostiko
- **Internet medicinskih stvari (IoMT):** Več tisoč povezanih naprav (infuzijske črpalke, srčni spodbujevalniki), ki pogosto nimajo ustrezne zaščite

PRIJAVITELJI PO SEKTORJIH



https://www.cert.si/wp-content/uploads/2025/08/Porocilo-o-kibernetski-varnosti_SI-CERT_2024.pdf

Ključni izzivi v eZdravju

Zastarela oprema (Legacy systems)	Medicinske naprave (npr. MRI), ki tečejo na sistemih Windows 7, XP ali 10, ker certifikacija nove programske opreme traja leta
Interoperabilnost	Potreba po hitri izmenjavi podatkov med ustanovami odpira "luknje" v varnostnih zidovih
Uporabniška izkušnja vs. Varnost	Zdravnik v nujnem primeru nima časa za 3-stopenjsko avtentikacijo; varnost ne sme ovirati hitrosti oskrbe
Pomanjkanje kadra	Kronično pomanjkanje IT strokovnjakov, ki bi razumeli specifike kliničnih procesov

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024

Dobavna veriga: najpogostejša vstopna točka

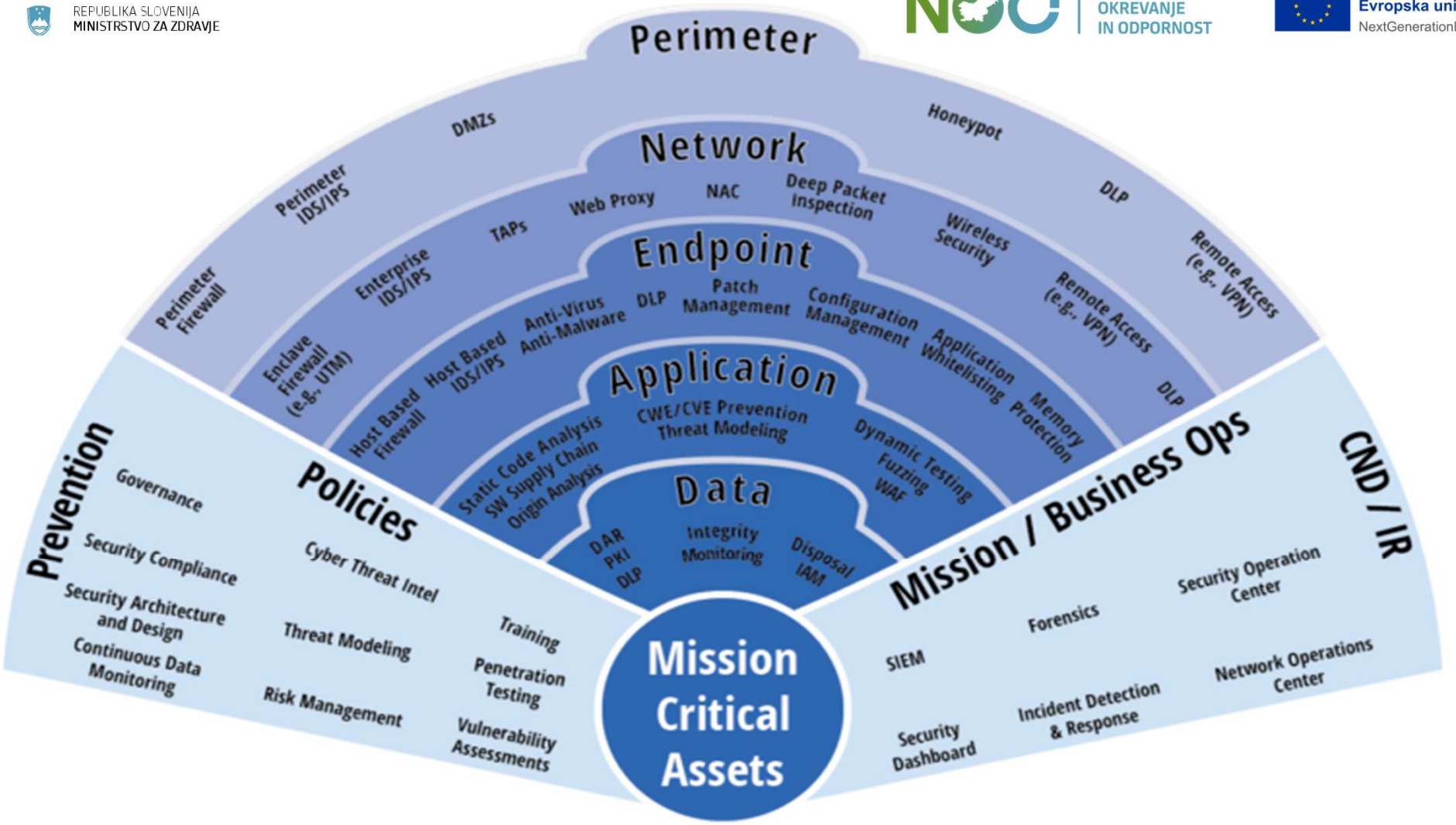
- Zdravstvo je ekosistem, ne zaprt sistem
- Dobavitelji, zunanji vzdrževalci, integracije
- Tipičen vzorec iz testiranj:
  - zaupanja preveč, nadzora premalo
- Sporočilo:
  - varnost organizacije je enaka varnosti njenega najslabšega dobavitelja

Infrastruktura: ko osnovna higiena odpove

- Klasični problemi, ki jih še vedno srečujemo:
  - identitete, dostopi, segmentacija
- Zakaj napadalec po vstopu hitro napreduje
- Razlika med “imamo varnost” in “varnost dejansko deluje”
- Sporočilo:
  - večina resnih incidentov se začne zelo banalno

Aplikacije: podatki so tam, kjer so aplikacije

- Aplikacije kot neposreden dostop do zdravstvenih podatkov
- Najpogostejše težave:
  - kdo lahko vidi kaj
  - kako se preverja identiteta
- Integracije in API-ji kot nova šibka točka
- Sporočilo:
  - ena logična napaka lahko pomeni masovno izpostavljenost podatkov


Perimeter
DMZs
Honeypot
Network
Perimeter IDS/IPS
Web Proxy
NAC
Deep Packet Inspection
DLP
TAPs
Wireless Security
Endpoint
Perimeter Firewall
Enterprise IDS/IPS
Remote Access (e.g., VPN)
Enclave Firewall (e.g., UTM)
Anti-Virus Anti-Malware
DLP
Patch Management
Configuration Management
Application Whitelisting
Remote Access (e.g., VPN)
Host Based IDS/IPS
Application
Host Based Firewall
CWE/CVE Prevention Threat Modeling
Memory Protection
DLP
Static Code Analysis SW Supply Chain Origin Analysis
Dynamic Testing Fuzzing WAF
Data
DAR PKI DLP
Integrity Monitoring
Disposal IAM
Prevention
Policies
Mission / Business Ops
CND / IR
Governance
Security Compliance
Security Architecture and Design
Continuous Data Monitoring
Cyber Threat Intel
Threat Modeling
Risk Management
Training
Penetration Testing
Vulnerability Assessments
Mission Critical Assets
Forensics
Security Operation Center
SIEM
Network Operations Center
Incident Detection & Response
Security Dashboard

Primer dobre prakse

- **Tehnični ukrepi:**
  - Večfaktorska avtentikacija (MFA)
  - Segmentacija omrežij
  - Redne varnostne kopije (offline backup)
  - EDR/XDR rešitve
  - Redne posodobitve
- **Organizacijski ukrepi:**
  - Izobraževanje zaposlenih
  - Simulacije phishing napadov
  - Načrti odziva na incidente (IRP)
  - Redni varnostni pregledi

Varnostno testiranje

- Pred produkcijo:
  - Penetracijski testi
  - Code review
  - SAST / DAST analiza
  - Testiranje avtorizacijskih mehanizmov
- Po uvedbi:
  - Redni varnostni pregledi
  - Redno spremljanje logov
  - SIEM/SOC

Upravljanje identitet in dostopov (IAM)

- Močna in unikatna gesla
- Uporaba upravljalnikov gesel
- Večfaktorska avtentikacija (MFA)
- Načelo najmanjših privilegijev (Least Privilege)
- Redni pregledi pravic dostopa
- Takojšnja deaktivacija računov ob odhodu zaposlenih

- Posebnost v zdravstvu:
  - Veliko rotacij kadra (študenti, specializanti, zunanji izvajalci)
  - Dostopi do posebej občutljivih podatkov (diagnostika, psihiatrija)

Obseg testiranja: zakaj “kljukica” ne deluje

- Penetracijsko testiranje ≠ avtomatski sken
- Preozek obseg daje lažen občutek varnosti
- Pravo vprašanje:
  - *kaj bi napadalec res napadel?*
- Sporočilo:
  - slab test je pogosto bolj nevaren kot noben test

Kako se lotiti pravilno?

- Varnost kot proces, ne enkratni dogodek
- Fokus na tveganja, ne na število ranljivosti
- Sodelovanje: IT, varnost, vodstvo, dobavitelji
- Penetracijsko testiranje kot orodje za učenje, ne kaznovanje


“Just keep vibe coding.
We can always fix it later.”

Izbira dobaviteljev in pogodbeni vidik

- Ključna vprašanja:
  - Kje se hranijo podatki?
  - Ali je omogočena enkripcija v mirovanju in prenosu?
  - Kako je urejen odziv na incidente?
  - Kakšni so SLA časi?
- V pogodbah morajo biti opredeljeni:
  - Izbira dobaviteljev in pogodbeni vidik


CONTROL
DISASTER
RECOVERY
IMT
SLA
INCIDENT
MANAGEMENT
DIAGNOSIS
RESPONSE
EVENT
SECURITY
PROTOCOL
OPERATIONS
POLICY
PLANNING
ANALYSIS
DETECTION

Odzivanje na incidente

- Ker 100% varnost ne obstaja, mora vsaka organizacija v eZdravju vedeti, kaj storiti, ko gre nekaj narobe
- **Detekcija:** Kako hitro sploh opazimo vdor?
- **Omejitev (Containment):** Takojšnja izolacija okuženega dela omrežja, da virus ne preskoči na medicinske naprave
- **Obnova:** Preverjanje integritete varnostnih kopij (Backupov) – so kopije sploh delujoče in neokužene?
- **Komunikacija:** Obveščanje pacientov (če so bili podatki odtujeni) in poročanje organom v skladu z NIS 2

Na koncu

- V zdravstvu ni vprašanje *če*, ampak *kdaj*
- Največje težave so znane – a še vedno prisotne
- Pravi pristop bistveno zmanjša vpliv incidentov
- Kibernetska varnost je del varnosti pacientov
- Tehnologija sama ni dovolj – ključni so ljudje in procesi
- Varnost mora biti vključena že v fazi načrtovanja

- Cilj: odpornost in zaupanje, ne iluzija popolne varnosti

Hvala za pozornost.