KAKO NIS2 GRADI OTPORNIJE GRADOVE

Od propisa do prakse

Pomoćnik pročelnika za informatiku i informacijsku sigurnost

Danijel Antonić, GRAD RIJEKA

28. STUDENI 2025.

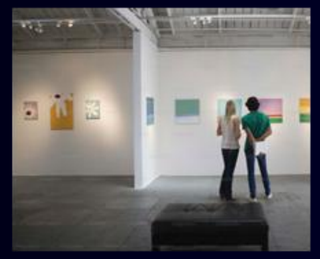
OČITE UGROZE

UGROZE?

EleMENTI SUVREMENOG KIBERNETIČKOG NAPADA

- Vrlo **sofisticirani protivnici**: državno sponzorirane skupine ili elitni kibernetički kriminalci
- Korištenje **najnovije tehnologije i alata**: napredni eksploati, zero-day ranjivosti
- **Specijalizirana umjetna inteligencija:** automatizirani alati za penetraciju i detekciju slabosti
- **Financijska superiornost:** napadači raspolažu s višestruko većim proračunima od IT odjela ciljanih organizacija
- Dovoljna je **samo jedna greška**: kompromitacija sustava često počinje s jednim nezaštićenim ulazom

ŠTO MOŽE BITI KOMPROMITIRANO ?



REALNOST 2025.: GRADOVI SU METE!

70% kIBERNETIČKIH NAPADA U EUROPI POGAĐA **JAVNE INSTITUCIJE (ENISA).**
REALNA PROCJENA VREMENA **OPORAVKA OD 120 DANA NA VIŠE**)

Država	Grad	Vrsta napada / incidenta
Rumunjska	Bukurešt – Sektor 5 (City Hall)	Ransomware
Rumunjska	Timișoara (City Hall, DFMT, policija)	Ransomware
BiH	Sarajevo – općina Centar	Ransomware
Nizozemska	Eindhoven	Datalek
Italija	Palermo	Ransomware
Španjolska	Badajoz	Ransomware
Španjolska	La Vila Joiosa (Villajoyosa)	Ransomware
Španjolska	Elche	Ransomware
Švedska	~200 općina i regija	Ransomware (dobavljač)
Belgija	Antwerpen	Ransomware
Grčka	Solun (Thessaloniki)	Cyber-napad


City of Antwerp hit by cyber attack

Tuesday, 6 December 2022

By The Brussels Times Newsroom

Nije pitanje hoće li se dogoditi, nego kad.

Gradovi koji su morali ugasiti sustave

TROŠAK RAČUNALNOG NAPADA

Koliko kriminalci traže? (Ransom zahtjevi)
Prema ENISA-i i europskim slučajevima:

Tipični zahtjevi za gradske uprave:
200.000 € – 3.000.000 €

U većini slučajeva i nakon plaćanja — podaci nisu u potpunosti vraćeni!

Efektivni trošak napada:

Trošak oporavka sustava (forenzika, reinstalacija, vraćanje servisa). Trošak vanjskih stručnjaka (CSIRT, konzultanti, sigurnosne tvrtke). Gubitak podataka,gubitak prihoda i potreba za rekonstrukcijom dokumenata.

80% mogućnost ponovnog napada!

NAJVEĆE SLABOSTI GRADOVA DANAS

- IT sustavi često ovise o entuzijazmu pojedinaca, bez institucionalne podrške
- Rukovodstvo ne percipira stvarne sigurnosne prijetnje i ne alocira adekvatna sredstva
- Nedostatak stručnog kadra — preopterećeni i malobrojni IT timovi
- Zastarjela infrastruktura i aplikacije — hardver, OS, baze, servisi
- Nepostojanje ili zastarjelost sigurnosnih alata (npr. EDR, SIEM, segmentacija mreže)

Najveća slabost nije tehnologija, nije ni IT.
Najveća slabost je percepcija rizika i posljedica kibernetičkog napada na grad

ŠTO JE NIS2 I ZAŠTO NAS SE TIČE

01 DIREKTIVA

Direktiva koja traži da organizacije značajno podignu razinu kibernetičke sigurnosti, uvedu strože kontrole i prijavljuju incidente u roku 24 sata.

02 Lokalna transpozicija NIS2 Direktive

• ZAKON O KIBERNETIČKOJ SIGURNOSTI
•UREDBA O KIBERNETIČKOJ SIGURNOSTI
Uredba definira 13 mjera iz Priloga II: upravljanje rizicima, mrežna sigurnost, incident management, kontinuitet, fizička sigurnost, identiteti

Kazne do 7 milijuna € ili maksimalno 1,4% prihoda. Reputacijska i kaznena odgovornost leži na čelniku. Čelnik može biti kažnjen od 500 do 3000€.

ŠTO OVO ZNAČI U PRAKSI ZA GRADONAČELNIKE

Gradonačelnik je odgovorna osoba za kibernetičku sigurnost

Uprava ima obavezu:

- aktivno nadzirati sigurnost
- usvajati politike i strateške planove
- osigurati budžet za zaštitu
- imenovati odgovorne osobe (CISO / koordinator)
- provoditi nadzor i kontrole dobavljača
- redovito procjenjivati rizike
- Implementirati tehničke mjere zaštite
- Implementirati sustav sigurnosnih kopija i testirati funkcionalnost istih

PrePORUKE ZA GRADONAČELNIKE U KONTEKSTU NIS2

- Osigurajte punu potporu za implementaciju kibernetičke sigurnosti u gradu.
- Uključite se u radnu skupinu za ICT i kibernetičku sigurnost Udruge gradova
- Koristite besplatne resurse CDU RH za jačanje sigurnosne infrastrukture
- Uključite se u SKAUT – državni sustav ranog upozoravanja SOA-e

Kazne do 7 milijuna € ili maksimalno 1,4% prihoda. Reputacijska i kaznena odgovornost leži na čelniku. Čelnik može biti kažnjen od 500 do 3000€.

HVALA
NA PAŽNJI!

daniel.antonic@rijeka.hr