STRATEGIJE ZA RAZVOJ ČVRSTIH OKVIRA ZAŠTITE OD PRIJETNJI

Ana Balaško, dipl.ing.el.
Ivan Periša, dipl.ing.el.

HEP-Operator distribucijskog sustava d.o.o.

Pregled prezentacije

- Zablude oko kibernetičke zaštite
- Kibernetička sigurnost vs kibernetička otpornost
- Zašto je važna kibernetička sigurnost i otpornost u EES-u?
- Izazovi dionika EES-a
- Definiranje okvira zaštite od prijetnji
- Politika sigurnosti informacijskih sustava
- Korisni „alati” za razvoj čvrstih okvira od prijetnji
- Zaključak

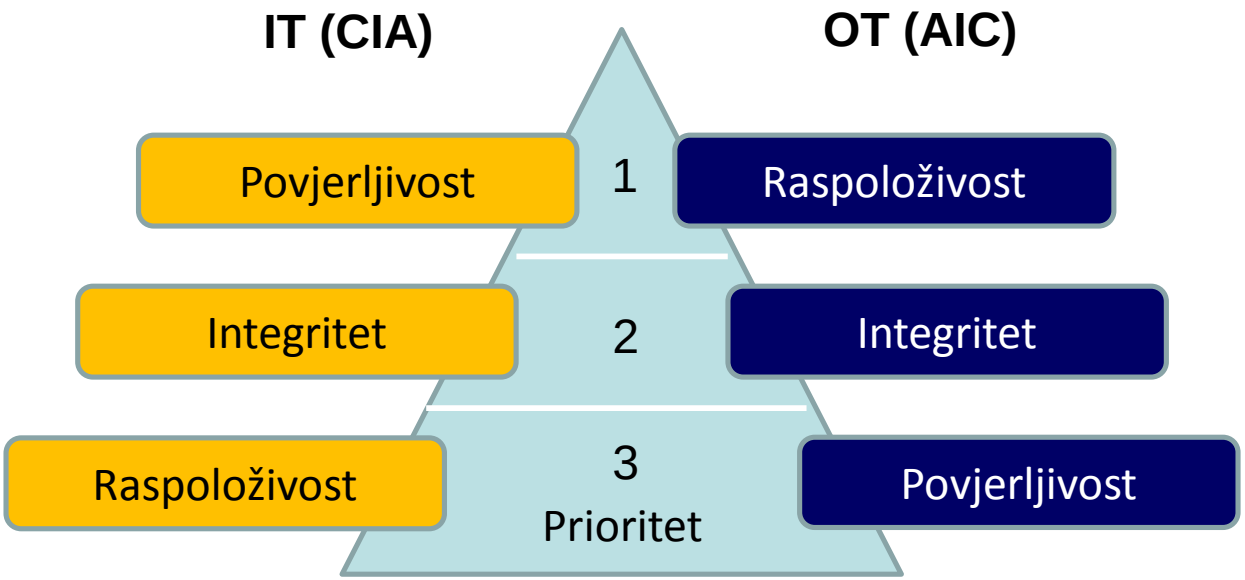
Zablude oko kibernetičke zaštite

- Obveznici smo NIS2 Direktive
- NIS2 pruža jasne smjernice i mjere upravljanja kibernetičkim rizicima
- Već se kasni sa usklađenjem sa NIS2
  - ZKS stupio na snagu 15.02.2024. (NN 14/2024)
  - rok za donošenje pripadajuće uredbe: 9 mjeseci
  - rok za usklađenje: 1 godina od dana dostave obavijesti
  - ocjena sukladnosti – najmanje jednom u 2 godine
  - stručni nadzor – jednom u roku 3 do 5 godina
- CER Direktiva (EU) 2022/2557 o otpornosti kritičnih subjekata?
- ….

PREBACITI FOKUS NA KIBERNETIČKU SIGURNOST I OTPORNOST

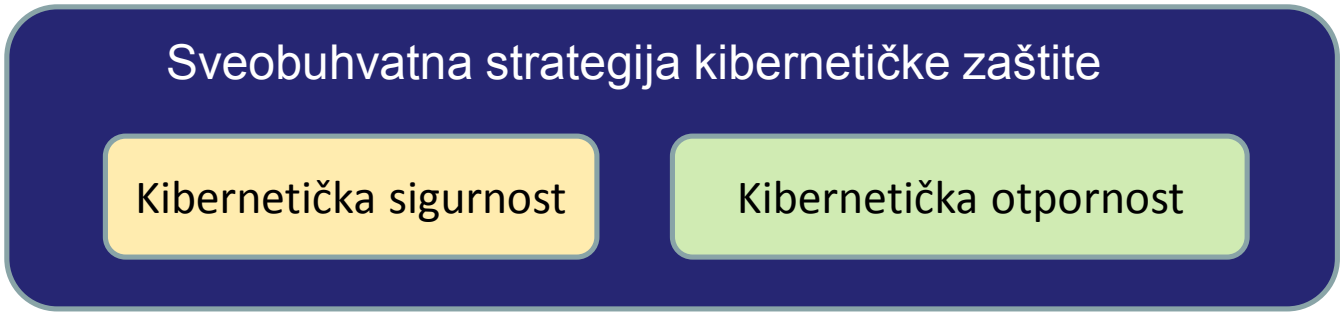
Kibernetička sigurnost vs kibernetička otpornost (1)

- Kibernetička sigurnost
  - zaštita sustava od prijetnji, napada i neovlaštenog pristupa
  - Cilj: očuvati raspoloživost, integritet i povjerljivost

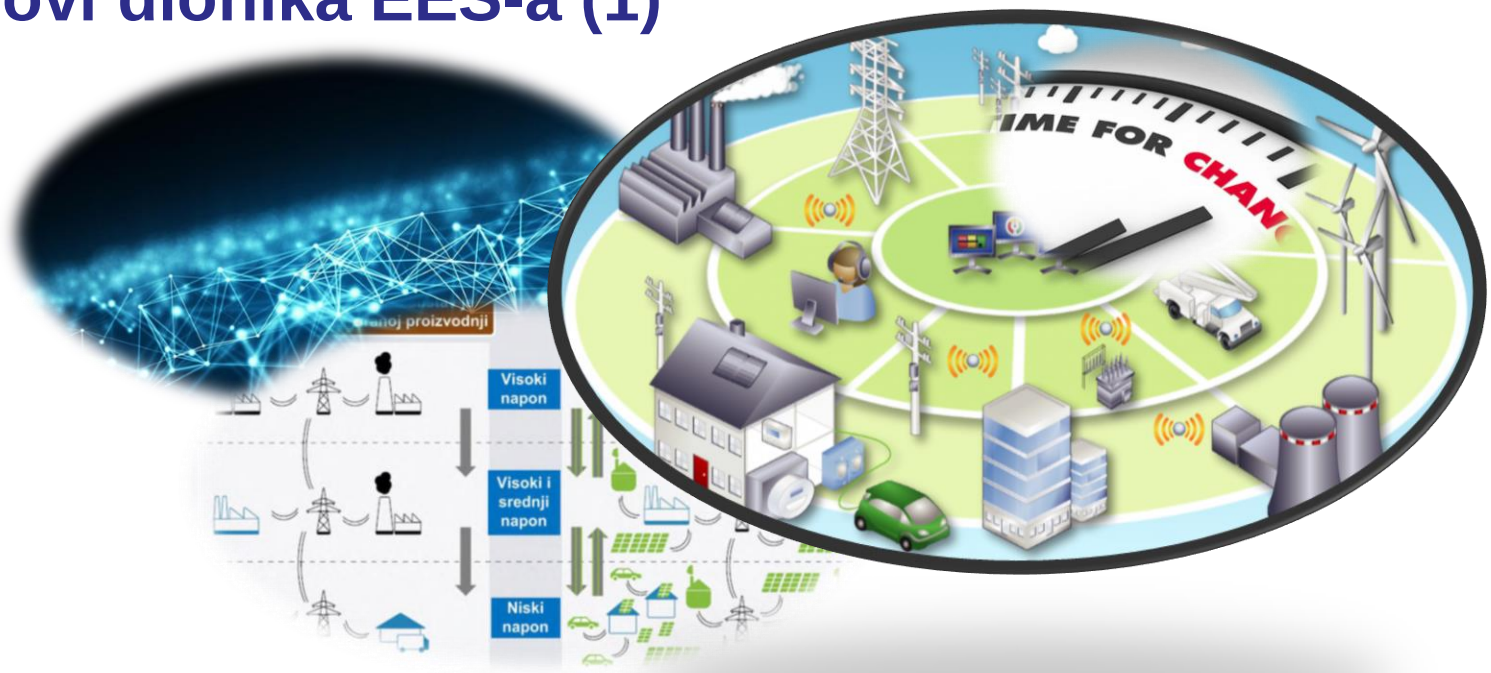


Kibernetička sigurnost vs kibernetička otpornost (2)

- Kibernetička otpornost:
  - kontinuitet poslovanja
  - redovito testiranje planova oporavka
  - obuka osoblja za postupanje u kriznim situacijama
  - implementacija sustava i procesa koji omogućuju brzi oporavak
  - cilj: brza reakcija i oporavak od kibernetičkih napada, kako bi se minimizirala štete i održala operativna sposobnost



Izazovi dionika EES-a (1)



- Kako osigurati visoku razinu kibernetičke zaštite, a pri tome omogućiti snažnu digitalizaciju elektroenergetskog sustava i korištenje naprednih mreža

Izazovi dionika EES-a (2)

- Dekarbonizacijska strategija -> energetska tranzicija
- Krajnji pasivni korisnici -> aktivni sudionici na tržištu
- Pasivna mreža -> aktivna mreža (distribucijska fleksibilnost, pomoćne usluge, ...)
- Usložnjavanje poslovnih procesa u svim segmentima EES-a i za sve dionike EES-a
  - povećanje stupnja digitalizacije
  - „otvaranje” sustava
- **veća ranjivost na kibernetičke prijetnje**

Izazovi dionika EES-a (3)

- „Izolirani" sustavi - sigurni (*safety*), ali nezaštićeni (*security*)
- Uređaji s dugim vijekom trajanja i ciklusima zamjene - podrška
- Otežana nadogradnja opreme – fokus funkcionalnost
- Prividna odvojenost sustava – VPN, razmjena podataka,…
- Upravljački komunikacijski protokoli- legacy protokoli, sada IP based
- Geografska distribuiranost - sigurnost kom. mreže i podataka
- ….
- Podrška regulatora

Zašto je važna kibernetička zaštita u EES-u?

- Napad na OT:
  - Narušen / značajno otežan / zaustavljen poslovni proces
  - Ugroženo pružanje usluga
  - Kaskadni učinak na druge važne sektore
  - Ekonomska šteta
  - Ugrožavanje života i sigurnosti
  - …

Definiranje okvira zaštite od prijetnji

- Kontekst organizacije
- Poslovna strategija
- Što branimo i od koga branimo
- Modeliranje prijetnji
- Procjena rizika
- Mjere za smanjenje kibernetičkih rizika
- **Politika sigurnosti informacijskih sustava**

Politika sigurnosti informacijskih sustava

- Uloga - temeljni okvir za upravljanje sigurnošću IS-a
- Međunarodni standardi i smjernice (ISO 27001, ISO 27002, IEC 62443, NIST,…)
- Ključne sastavnice : svrha, korisnici, ciljevi, pravila pristupa i autorizacije, klasifikacija podataka, operacija nad podacima, pravila izrade sigurnosne kopije podataka, sigurnosna svijest i edukacija, odgovornosti, prava i dužnosti zaposlenika…
- Pravna snaga: disciplinske mjere, tužbe, kaznene prijave, gubitak povjerenja i ugleda, …

Korisni „alati” za razvoj čvrstih okvira od prijetnji

- ISO 27001 - okvir za uspostavu, implementaciju, održavanje i poboljšanje upravljanja IS-om u organizacijama.
- ISO 27002 - smjernice i preporuke za impl. kontrola i mjera koje pomažu organizacijama u zaštiti njihovih informacija i sustava.
- IEC 62443 - smjernice i zahtjevi za zaštitu industrijskih kontrolnih sustava od kibernetičkih prijetnji.
- ISO 22301 - okvir za sigurnost i otpornost te sustav upravljanja kontinuitetom poslovanja organizacije.
- MITRE ATT&CK ICS - smjernice o taktikama, tehnikama i procedurama koje se koriste u napadima na ICS okruženja, kao i preporuke za detekciju, obranu i odgovor na takve napade.

Zaključak

- Ranjivost na kibernetičke napade proporcionalna je stupnju digitalizacije
- Podizanje stupnja kibernetičke sigurnosti često ide na štetu jednostavnosti korištenja informacijskih sustava -> edukacija
- Brinuti o kibernetičkoj sigurnosti trebamo zbog doba i okolnosti u kojima živimo i mogućih posljedica, a ne isključivo da zadovoljimo zakonsku obavezu
- Usvajanje Secure by Design principa
- Briga o kibernetičkoj sigurnosti je kontinuiran proces

Hvala na pažnji!

ana.balasko@hep.hr
ivan.periša@hep.hr