



## **IZAZOVI I REŠENJA U UNAPREĐENJU BEZBEDNOSTI OPERATIVNIH TEHNOLOGIJA I INDUSTRIJSKIH KONTROLNIH SISTEMA**

---

Slavko DUBAČKIĆ, ODS „Elektrodistribucija Srbije“, Novi Sad, Srbija  
Aleksandar BOŠKOVIĆ, „Fakultet tehničkih nauka“ Novi Sad, Srbija  
Đorđe VLADISAVLJEVIĆ, ODS „Elektrodistribucija Srbije“, Novi Sad, Srbija

# Uvod

- Izgradnja IKT bezbednosti u OT mrežama
  - Za izgradnju efikasne i efektivne IKT bezbednosti u industrijskim sistemima (ICS – Industrial Control System) i/ili sistemima zasnovanim na operativnim tehnologijama (OT – Operational Technology) potrebno je razvijati mehanizme za IKT bezbednost.
  - Ovaj rad identifikuje te mere i razloge koji stoje iza njihove primene, kako bi organizacije mogle da prilagode ove mere tako da odgovaraju njihovom okruženju i rizicima.
  - Mere su namenjene da budu usmerene na rezultate umesto da budu samo propisane.

# Razlike između IT i OT sistema

- Fokus na tehnologijama:
  - Najčešće razlike između IT i OT sistema se ogledaju u nameni sistema, starosti OT sistema, specifičnim komunikacionim rešenjima i mrežnim protokolima u OT mrežama, (ne)sposobnosti OT sistema da usvoji određene bezbednosne mere.
- Misija ili poslovna svrha sistema:
  - IT je fokusiran ka poslovnim procesima, dok je OT namenjen uglavnom na primarne delatnosti kompanija.
- Kod napada na IT sisteme najčešće je cilj da se pristupi samom sistemu i podacima koji se tu nalaze.
- Tipovi napada u OT sistemima koji najviše zabrinjavaju su oni koji nastoje da poremete funkcionalnost sistema, izazovu fizičku štetu ili čak izazovu incidente vezane za bezbednost koji dostižu nivo oštećenja opreme ili gubitka života.

# Mere za unapređenje IKT bezbednosti u industrijskim (OT) sistemima

- Sedam preporuka koje bi trebalo primeniti da bi OT sistemi bili spremni za bezbednosne izazove:
  1. Uložite u nadogradnju OT mreža
    - „Dobra vest“ je ta da su OT mreže vrlo često tehnološki stare i da minimalnim ulaganjima može se dosta poboljšati bezbednost ovih sistema.
  2. Postavite teška pitanja i definišite odgovornost
    - Vrlo je važno identifikovati ko je odgovoran za nadgledanje OT mreža. Bez odgovornosti nema ni bezbednosti.
  3. Priznajte svoje nedostatke
    - Odsustvo dokaza nije isto što i dokaz o odsustvu zlonamernih aktera u OT mreži, to što neko ne vidi neke alarme ne znači da problema nema.
  4. Proverite da li postoji segmentacija između vaših IT i OT mreža
    - Dobro razgraničavanje IT i OT mreža, postavljanje „crvenih linija“, su od suštinskog značaja.
  5. Učinite OT mrežu vidljivom
    - Ne može se pravilno braniti OT mreža ako nema pristupa opremi i uređajima.
  6. Zaštita OT mreža nije jednokratna vežba
    - Kako se i koliko često ažuriraju i revidiraju bezbednosni mehanizmi.
  7. Edukujte rukovodioce o uticaju napada na OT mreže
    - Rukovodioci moraju da razumeju rizike poslovanja ako su OT mreže narušene i kako ovakvi napadi mogu da se propagiraju i kroz IT i kroz OT mreže.



# Mere za unapređenje IKT bezbednosti u industrijskim (OT) sistemima

- Pet preporuka koje bi trebalo primeniti da bi OT sistemi bili spremni za bezbednosne izazove:
  1. Odgovori na incident
    - Operativni plan reakcije na incidente sa fokusom na integritet sistema i mogućnostima oporavka i tokom napada. Ovo predstavlja skup predviđenih incidenata i scenarija za reagovanje u tim slučajevima.
  2. Odbranjiva arhitektura
    - Arhitekture koje obezbeđuju tražene funkcionalnosti (vidljivost, prikupljanje podataka, identifikaciju sredstava i sl.) ali tako izgrađene da minimizuju negativne posledice eventualnih incidenata (segmentacija, industrijski DMZ i sl.).
  3. Nadzor mreže
    - Kontinuirano praćenje bezbednosti OT mreže. Koriste se alati koji poznaju i industrijske protokole i mehanizmi za detekciju potencijalni slabih tačaka u sistemu.
  4. Bezbedan daljinski pristup
    - Identifikacija i kontrola svih tačaka gde se omogućuje udaljeni pristup.
  5. Upravljanje ranjivostima zasnovano na proceni rizika
    - Razumevanje postojećih bezbednosnih mera i mehanizama i poznavanja rada uređaja u OT sistemima, koje pomažu u donošenju odluka o upravljanju rizicima po IKT bezbednost OT sistema.

# Mera br. 1 – Odgovori na incident

- Mera br. 1: Operativni plan reakcije na incidente
  1. Odrediti koji scenariji predstavljaju najveći rizik i od kojih se treba braniti
    - Planiranje scenarija treba da počne sa incidentima u stvarnom svetu i da bude zasnovano na realnim podacima.
    - Kompanije bi trebalo da utvrde koji su se incidenti dogodili u njihovoj industriji i da tu počnu. Neki scenariji će biti prikladni za više industrija, dok neki mogu biti prikladni samo za specifična okruženja.
  2. Razmotriti scenarije zasnovane na posledicama
    - Analiza scenarija sa aspekta posledica po OT sistem, uzimajući u obzir najgori mogući scenario, tj. najveću moguću štetu.
    - Scenariji zasnovani na realnim podacima treba da budu prioritet, jer je velika verovatnoća da će se oni ponoviti.
  3. Izvršiti vežbu „na stolu“
    - Kada se scenariji odaberu i dogovore potrebno ih je provežbati ali tako da se tačno odrede ciljevi koje u ovakvim simulacijama je potrebno ostvariti.
- Ključni aspekt Mere br. 1 u u OT sistemima jeste uspostavljanje zajedničkog pogleda na moguće rizike u radu/poslovanju kompanije i određivanje nivoa funkcionalnosti OT sistema u slučajevima napada.

# Mera br. 1 – Odgovori na incident

- Prvi koraci

1. Definisati role i odgovornosti

- Definisane odgovornosti predstavlja sastavni deo svake uloge (role). Svaki deo sistema se procenjuje sa stanovišta važnosti, definišu se pravila bezbednog ponašanja i uloge svakog pojedinca kome je data nadležnost nad istim.
- Uloge se definišu od najvišeg vrha kompanije: top menadžment, IKT menadžment, vlasnici poslovnih procesa, sistem dizajneri, vođe projekata, rukovodioci, krajnji korisnici, revizori.

2. Klasifikacija informacija i procesa

- Klasifikacija na osnovu raspoloživosti.
- Klasifikacija na osnovu osetljivosti.

3. Identifikacija i klasifikacija bezbednosnih pretnji

- Potencijalne mete ugrožavanja sigurnosti u mreži: OT oprema, serveri, mreža, serveri, radne stanice.
- Bezbednosna granica – perimetar.

- Bezbednosna politika neke kompanije se sastoji od bezbedonosnih procesa koji se sprovode i ljudi (organizacije) koji ih sprovode u skladu sa poslovnim procesima.



# Mera br. 2 – Odbranjiva arhitektura

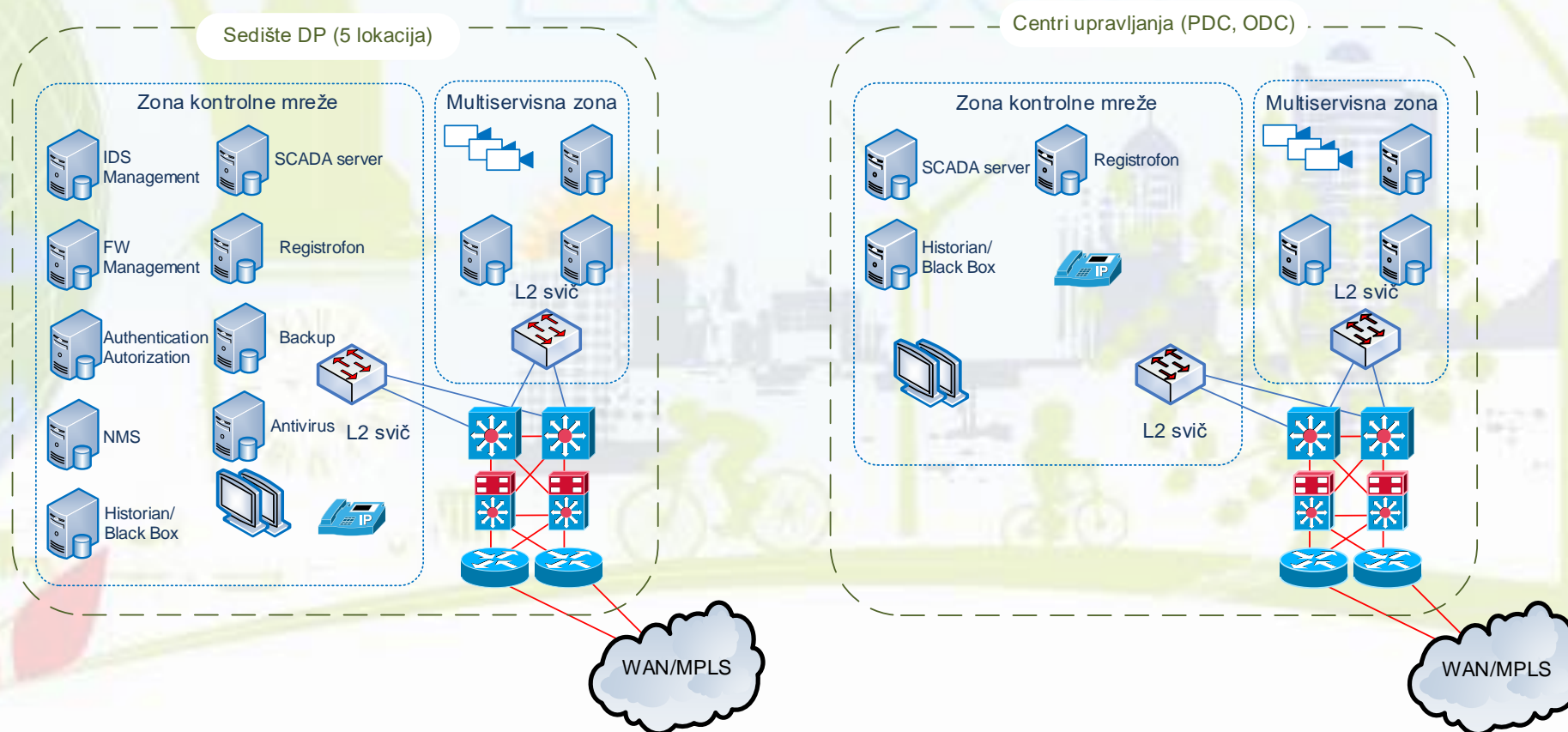
- Mera br. 2: Odbranjiva arhitektura

1. Odbranjiva arhitektura je arhitektura koja smanjuje što je moguće više rizik kroz dizajn i implementaciju sistema, a istovremeno olakšava odbranu.
2. Ne postoji takva stvar kao što je siguran sistem ili arhitektura – ljudski element je taj koji omogućava da odbranjiva arhitektura postane zaštićena arhitektura.
3. Planiranje scenarija treba da počne sa incidentima u stvarnom svetu i da bude zasnovano na realnim podacima.
4. Pri izgradnji odbranjve IKT arhitekture u OT sistemima preporučuju se sledeće mere:
  - Identifikacija imovine i inventar (barem ključnih lokacija).
  - Segmentirana IKT mreža.
  - Razmisliti gde je moguće primeniti „read only“ princip.
  - Nadzor mrežnog saobraćaja i sistemske komunikacije.
  - Prikupljanje komunikacionih logova.
  - Sposobnost prelaska u „odbranjivu poziciju“, tj. stanje povećane pripravnosti sa ograničenim funkcionalnostima sistema u slučajevima sumnje na napad.
  - Definisati role i odgovornosti



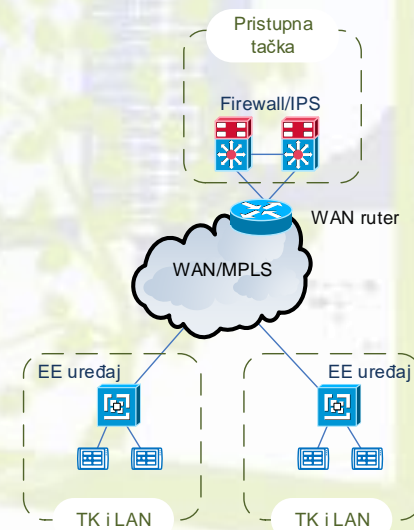
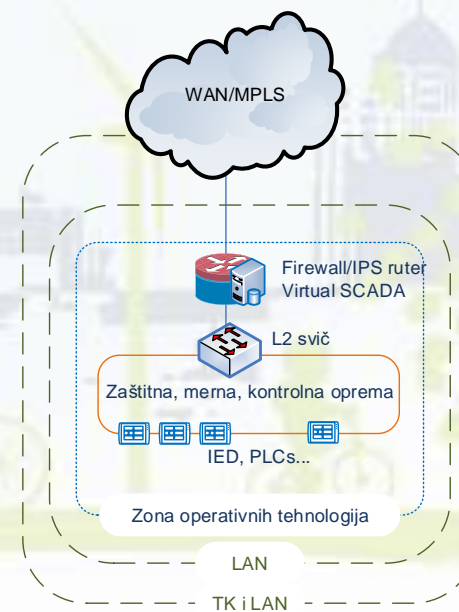
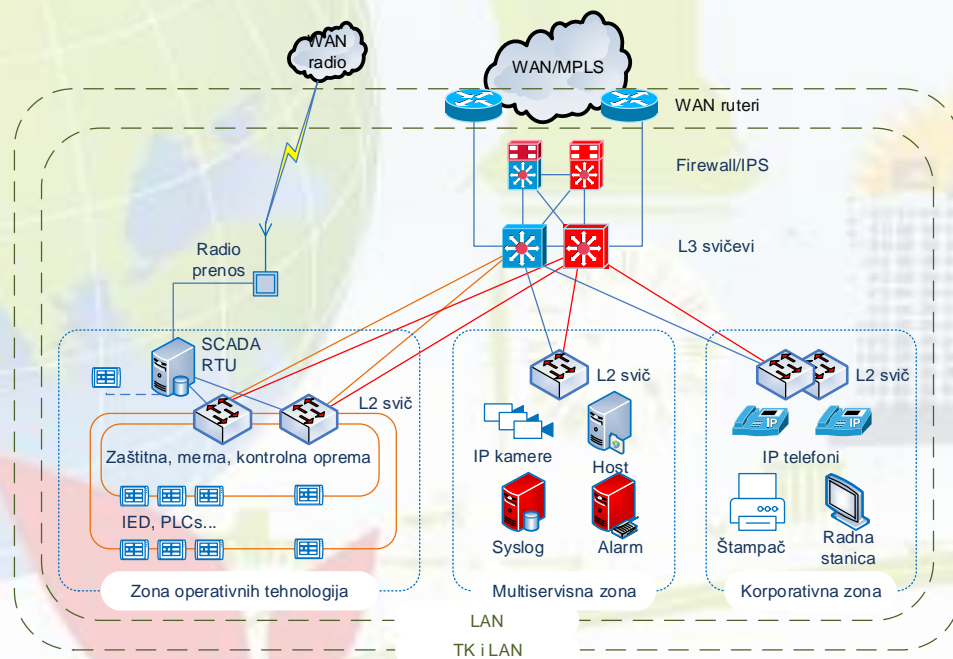
# Mera br. 2 – Odbranjiva arhitektura

- Primena u EDS: Dispečerski centri (DDC, PDC, ODC)



# Mera br. 2 – Odbranjiva arhitektura

Primena u EDS: Elektroenergetski objekti



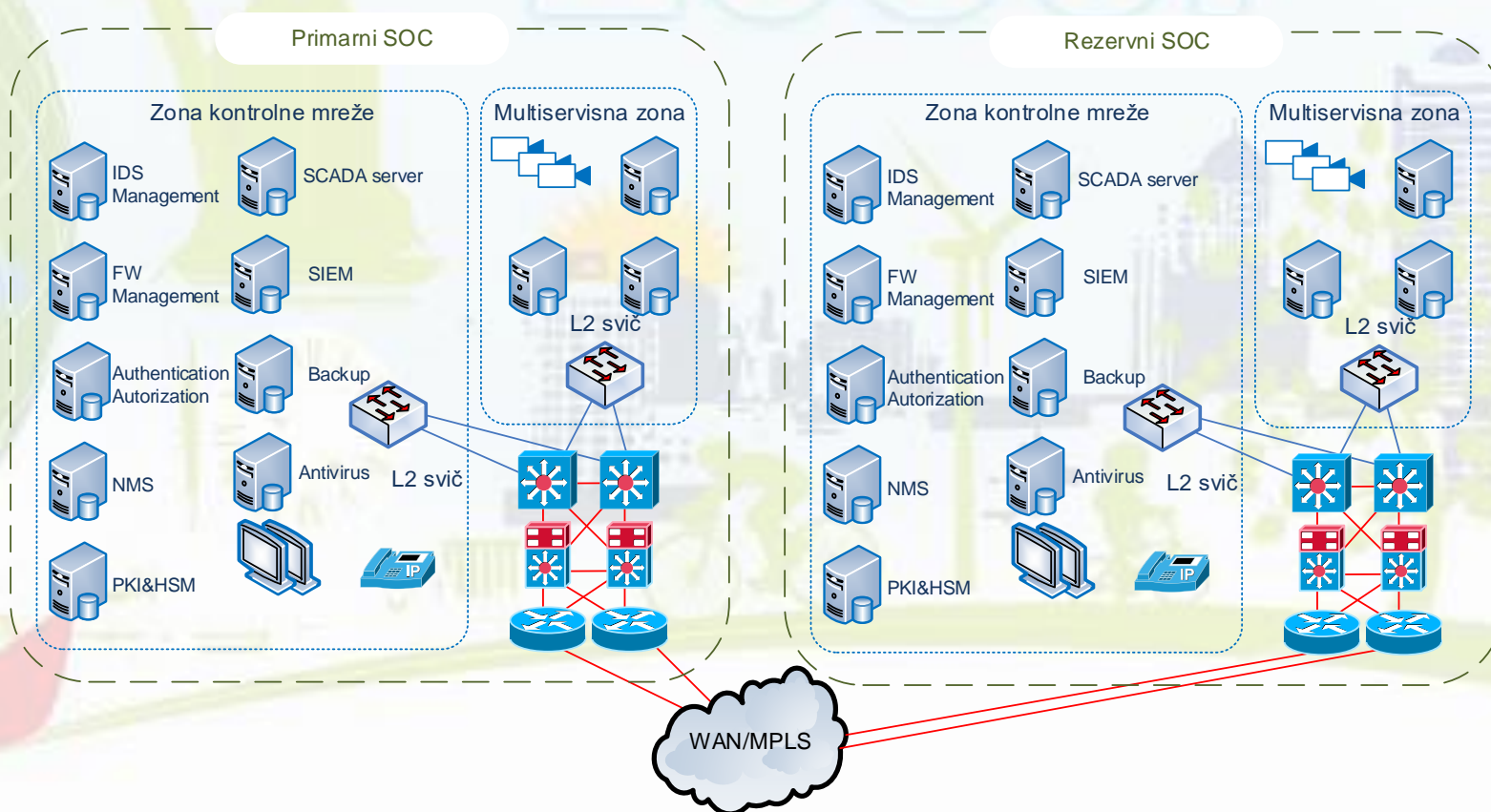
# Mera br. 3 – Nadzor mreže

- Mera br. 3: Vidljivost i nadzor IKT mreže
  1. Priroda IKT sistema pokreće potrebu za praćenjem mreže da bi se razumele interakcije u sistemu.
  2. Nadgledanje specifično za IKT sisteme u OT mrežama uključuje inspekciju paketa IKT protokola koji su specifični za to okruženje.
  3. Vidljivost i nadzor IKT mreže u OT sistemima nije samo tehnološki problem.
  4. Postavlja se pitanje izbora alata za nadzor. Ne postoji rešenje koje se može jednostavno kupiti.



# Mera br. 3 – Nadzor mreže

Primena u EDS: Security Operations Center (SOC)

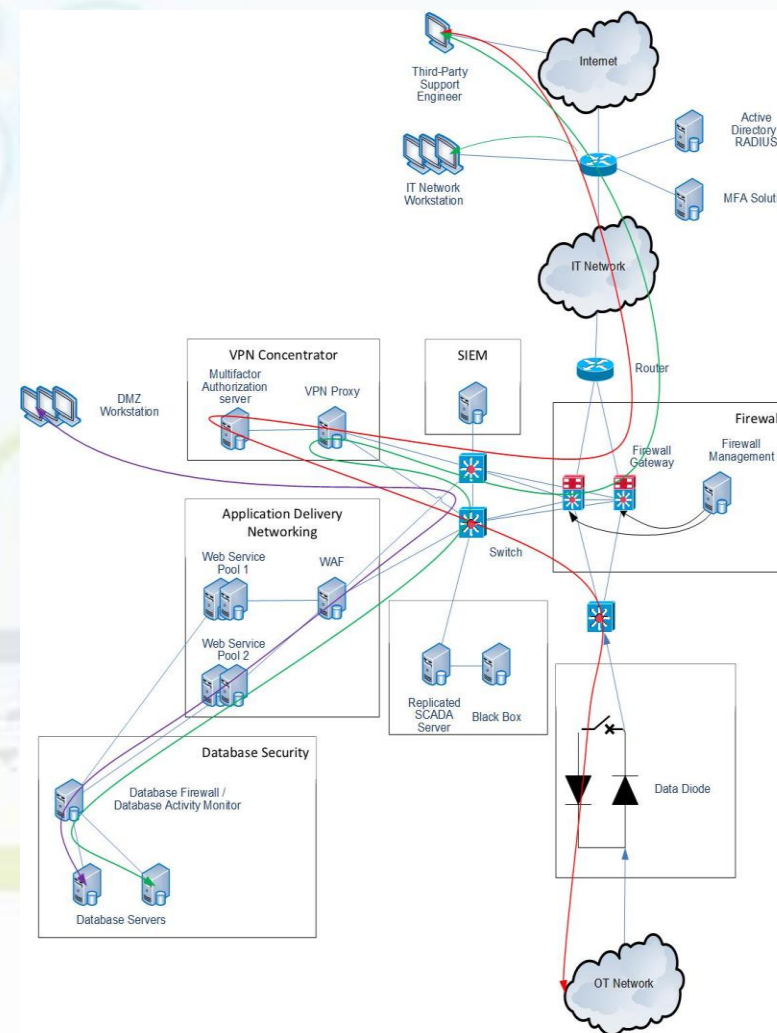


# Mera br. 4 – Bezbedan daljinski pristup

- Mera br. 4: Bezbedan daljinski pristup
  1. Daljinsko povezivanje je neizbežno a ima i značajnu poslovnu i operativnu korist.
    - Pristup iz IT mreže,
    - Pristup van kompanije.
  2. Iako su prednosti udaljenog pristupa ogromne, veliki su i rizici, čak se u poslednje vreme (pandemija COVID 19) sve više ovi rizici tolerišu.
  3. U većini kompanija više nije neophodno ciljati IT mreže da bi se došlo do OT mreža. Čak i kada napadači ciljaju IT mreže, to nisu uvek kompanijske IT mreže, već IT mreže njihovih dobavljača, osoblja za održavanje, integratora ili proizvođača opreme.

# Mera br. 4 – Bezbedan daljinski pristup

- Primena u EDS: VPN pristup OT mreži (DMZ firewall)
  - Dozvoljavanje i blokiranje saobraćaja između zone (WAN, IT mreža, OT mreža).
  - Rutiranje između mreža/zona.
  - Napredni inspekcijski mehanizmi.
  - Antivirus.
  - Anti-bot funkcionalnost.
  - Funkcionalnost inspekcije HTTPS saobraćaja.
  - Logovanje saobraćaja.
  - Sistem za analitiku i alarmiranje.



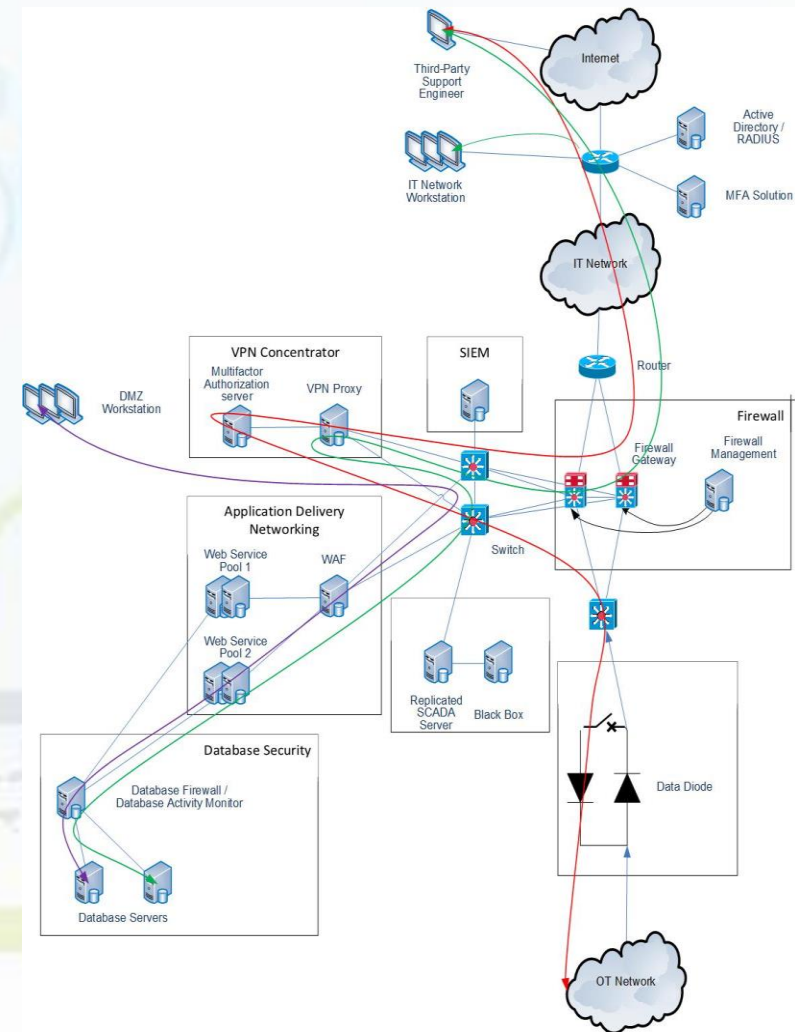


# Mera br. 5 – Upravljanje ranjivostima na bazi procene rizika

- Mera br. 5: Upravljanje ranjivostima bazirano na proceni rizika
  1. Pristup OT mrežama.
    - Pristup iz IT mreže,
    - Pristup van kompanije.
  2. Nove funkcionalnosti koje se mogu iskoristiti da izazovu operativne probleme (gubitak kontrole ili bezbednosti).
- Fokus programa upravljanja ranjivostima ne mora biti da se u potpunosti zakrpe te ranjivosti, već, u mnogim slučajevima, da se ublaži njihov uticaj ili da se nadgleda njihova aktivnost.
- IT i OT pogled na ranjivosti. Sanacija svake ranjivosti u OT okruženju može da ima direktan uticaj na primarnu funkcionalnost sistema.
- Procena rizika u odnosu na potrebne aktivnosti na smanjenje istog rizika. Da li i u kojoj meri (i koliko često i na koliko mesta i na kojem deli OT sistema i sl.) treba primeniti datu preventivnu meru.

# Mera br. 5 – Upravljanje ranjivostima na bazi procene rizika

- Primena u EDS: VPN pristup OT mreži (DMZ firewall)
  - Za 77% dokumentovanih ranjivosti, izveštaji su pokazali, potreban je direktan pristup uređajima unutar OT sistema.



# Zaključak

- Kontinuitet poslovanja

1. Primena pet mera za povećanje IKT bezbednosti u OT sistemima predstavlja dobar pristup za obezbeđenje kontinuiteta poslovnih procesa kroz investicione projekte i kroz programe održavanja sistema.
2. Mere se mogu sprovoditi u sinhronizaciji sa drugim aktivnostima kako bi se stvorio dobar program IKT bezbednosti u OT sistemima prilagođen rizicima sa kojima se kompanije suočavaju.
3. Elementi podrške kritičnim merama moraju uključiti sledeće:
  - Identifikacija najvažnijih lokacija.
  - Upoznajte sebe.
  - Prioritetni taktički i strateški plan usklađen sa poslovnim procesima.
  - Šta je potrebno i kada delovati tokom napada?
  - Usklađivanje sa scenarijima rizika i pretnjama koji mogu uticati na vaše poslovanje.
  - Kako će izgledati napad na vas?
  - Partnerstva sa dobavljačima su od suštinskog značaja za IKT okruženja.
  - Identifikujte svoje potrebe i zahteve dobavljača.
  - Obučenosť zaposlenih za korišćenje alata, tehnologija.
  - Ljudi će spasiti dan.



# Zaključak 2

- Pet mera IKT bezbednosti

1. Odgovori na incident
2. Odbranjiva arhitektura
3. Nadzor mreže
4. Bezbedan daljinski pristup
5. Upravljanje ranjivostima zasnovano na proceni rizika

- British Standards Institution: Ključne kontrolne tačke

1. Izrada dokumenata o bezbednosnim polisama IKT Sistema
2. Definisane odgovornosti po pitanju bezbednosti
3. Edukacija o bezbednosti IKT Sistema
4. Izveštavanje o bezbednosnim incidentima
5. Kontrola virusa
6. Planiranje kontinuiteta poslovanja
7. Kontrola prava umnožavanja podataka
8. Obezbeđivanje kompanijskih podataka
9. Saglasnost sa zakonskom regulativom
10. Saglasnost sa opštom bezbednosnom politikom

# Zaključak 3

- Operativni odgovor

1. Priprema: Vežbajte.
2. Identifikacija: Pribavite i analizirajte dokaza.  
Interna i eksterna razmena informacija.
3. Ograničavanje: Odredite gde bi napadač trebao biti da bi se postigao efekat.  
Izolujte sistem ili izolujte upravljanje.
4. Iskorenjivanje: Identifikujte osnovni uzrok ili početne tačke napada.
5. Oporavak: Vratite integritet sistema upravljanja.  
Odredite kada treba vratiti mogućnosti upravljanja sistemom.
6. Naučene lekcije: Koje su radnje preduzete da bi se sprečio sličan napad?  
Da li su informacije efikasno deljene?

# HVALA NA PAŽNJI!

Kontakt podaci autora:

- Slavko DUBAČKIĆ, Elektrodistribucija Srbije, [slavko.dubackic@es.rs](mailto:slavko.dubackic@es.rs)
- Aleksandar BOŠKOVIĆ, Fakultet tehničkih nauka, [aboskov@uns.ac.rs](mailto:aboskov@uns.ac.rs)
- Đorđe VLADISAVLJEVIĆ, Elektrodistribucija Srbije, [djordje.vladisavljevic@es.rs](mailto:djordje.vladisavljevic@es.rs)