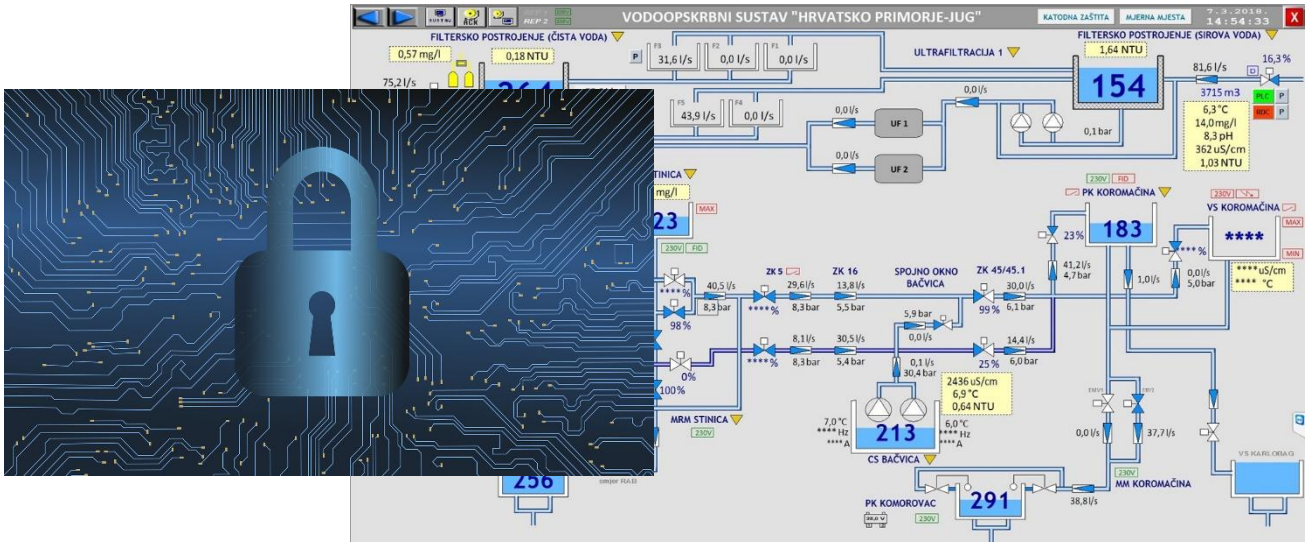
Kibernetička sigurnost i sustavi daljinskog nadzora i upravljanja

Zagrel Rittmeyer d.o.o.



Sigurnost i pouzdanost Nadzorno upravljačkih sustava

U suvremenoj vodoopskrbi i odvodnji, daljinski nadzor i upravljanje postali su neizostavni dijelovi tehnoloških sustava. Prikupljanje i obrada velikih količina procesnih podataka omogućuju efikasniji nadzor i upravljanje, analizu gubitaka, preciznije modeliranje i predviđanje ponašanja sustava. Međutim, sve veća povezanost OT (operativne tehnologije) s IT (informatičko tehničkim) sustavima povećava izloženost sigurnosnim prijetnjama.

Što su OT sustavi?

OT sustavi omogućuju izravnu interakciju s fizičkim svijetom, za razliku od IT sustava koji se bave obradom podataka. Oni uključuju:

- **SCADA** – sustavi za daljinski nadzor i upravljanje industrijskim procesima
- **PLC** – programabilni logički kontroleri za upravljanje strojevima i procesima
- **DCS** – distribuirani upravljački sustavi za automatizaciju proizvodnje

Povezivanje OT i IT sustava putem raznih komunikacijskih kanala donosi mnoge prednosti, ali i nove sigurnosne izazove.

Kibernetička sigurnost – ključni izazovi

Sigurnost podataka tema je današnjice – svakodnevno smo svjedoci problema s kojima se bore tvrtke nedovoljno pripremljene za kibernetičke izazove današnjice.

Nepouzdani rad OT sustava može uzrokovati ozbiljne posljedice. Najčešći uzroci su:

- Nenamjerne ljudske pogreške i proceduralni propusti
- Zastarjela, nefunkcionalna oprema i neodgovarajuće sigurnosne mjere
- Nekvalitetno održavanje, nemogućnost dobave zamjenskih dijelova
- Maliciozni napadi (interni i eksterni)

- Nedostatak odgovora na sigurnosne incidente
- Prirodne katastrofe

Kako bi se spriječili ovi rizici, zakonski i normativni okviri postaju sve stroži, osobito za kritične sustave.

Regulativa i standardi

Europska unija, kao i propisi Republike Hrvatske nameće stroge zahtjeve kroz:

- **NIS2 Direktivu** – propisuje sigurnosne obveze i izvještavanje ključnih subjekata
- **Zakon o kibernetičkoj sigurnosti i pripadnu Uredbu** – određuje operatere kritičnih usluga i njihove obveze
- **Cyber Resilience Act** – postavlja obvezne sigurnosne zahtjeve za digitalne proizvode (primjena od 2027.),

a između mnogobrojnih standarda ističu se:

- **ISO/IEC 27001** – standard za upravljanje informacijskom sigurnošću
- **IEC 62443** – standard za sigurnost industrijskih automatizacijskih i kontrolnih proizvoda, kao i sustava

Kako osigurati kibernetičku otpornost?

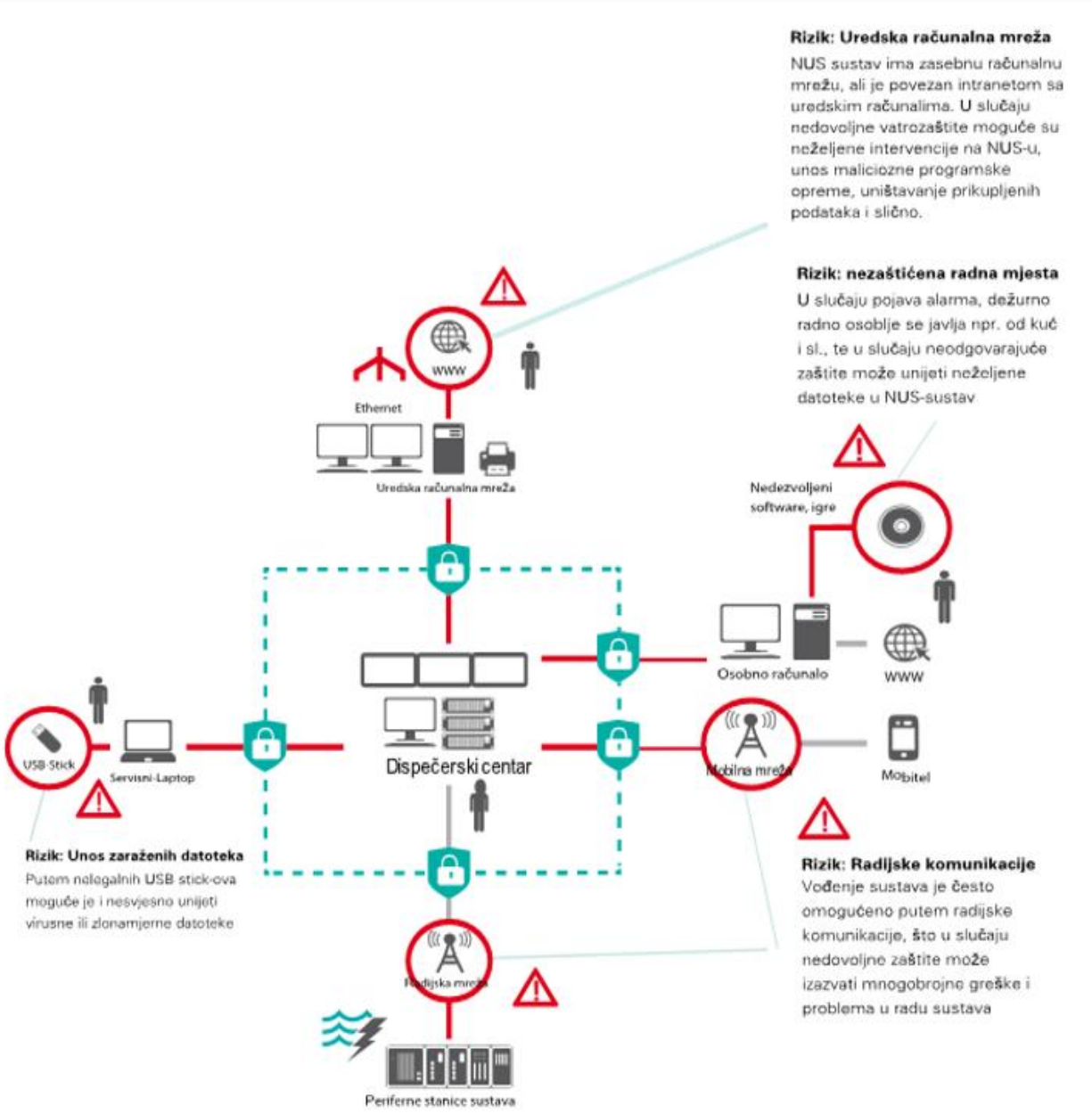
Temeljem nastojanja za pouzdan i efikasan rad Operatera kritičnih usluga, ali i zakonskih propisa, tvrtke su obvezne implementirati mjere kibernetičke sigurnosti (uskladiti organizaciju i akte, popisati imovinu, analizirati rizike, poduzimati mjere za uklanjanje neprihvatljivih rizika, predvidjeti upravljanje incidentima, izvještavati o incidentima, osigurati kontinuitet poslovanja, biti podložni reviziji nadležnih tijela i sl.).

Odgovornost na odabiru organizacije, imenovanju odgovornih osoba za kibernetičku sigurnost te izradi normativnih akata leži na samoj tvrtki. Prilikom analiziranja rizika, predlaganja mjera za uklanjanje neprihvatljivih rizika, izrade protokola kod pojave incidenata i sl. tema, predstavnici Zagrel Rittmeyer d.o.o. pružaju svojim naručiteljima tehničke i funkcijske preporuke o svojstvima OT sustava.

Identifikacija, analiza i upravljanje rizicima

U prvom koraku kod rada na povećanju kibernetičke sigurnosti, neminovno je popisati imovinu, te napraviti detaljnu funkcionalnu shemu sustava, a potom analizirati identificirati ranjivost i prijetnje takve konfiguracije i primijenjenih postupaka. Navest ćemo neke primjere:

- rade li se redovito kopije programske opreme i baze prikupljenih podataka?
- postoje li u sustavu alternativni komunikacijski putevi?
- može li se sustavu pristupiti neovlašteno?
- postoji li antivirusna /antimalware zaštita?
- postoji li plan oporavka sustava u slučaju katastrofalnih događaja?
- da li se registriraju i analiziraju greške i ispadi u radu sustava
- …….



Svaki sustav je drugačije konfiguracije, drugačijih zahtjeva i drugačijih funkcija, tako da nije moguće napraviti standardni obrazac s popisom svih rizika u sustavu nego je potrebno svaki sustav analizirati zasebno.

Umanjenje rizika

Idući korak u razradi kibernetičke sigurnosti je vrednovanje pronađenih rizika koji bi mogli ugroziti rad nadzorno upravljačkog sustava, a potom prijedlog mjera za njihovo otklanjanje ili umanjivanje. Odluku o ovim aktivnostima donosi korisnik – vlasnik sustava.

Neki od prijedloga za povećanje kibernetičke sigurnosti i pouzdanosti rada nadzorno upravljačkog sustava su:

- korištenje certificirane i dobavljive opreme, osigurani lanci opskrbe
- osigurano održavanje i mogućnosti širenja te modernizacije sustava od strane ovlaštenih dobavljača
- sigurnost ljudskih resursa, politike kontrole pristupa i upravljanja imovinom
- redundantne konfiguracije,

- izdvojene lokalne računalne mreže OT sustava,
- vatrozidovi novijih generacija,
- legalizirana programska oprema i propisano obnavljanje verzija operacijskih sustava te programske opreme,
- osigurane sigurnosne kopije programske opreme,
- antivirusni programi,
- zaštićeni komunikacijski kanali,
- propisana ovlaštenja i postupci upravljačkog i servisnog osoblja u redovitom radu i izvanrednim situacijama,
- sustav ovlaštenja za rad operativnog osoblja (lozinke, višefaktorska autentifikacije i dr.),
- osiguran neometan rad osoblja,
- propisan postupak nakon pojave incidenta, te obnavljanja sustava u slučaju značajnijih incidenata,
- arhiviranje i analiza događaja kod pojave incidenata,
- osigurana kontinuirana edukacija operativnog i rukovodećeg osoblja o kibernetičkoj sigurnosti,
- osiguran kontinuitet poslovanja
- ……..

Zagrel Rittmeyer d.o.o. – Vaš partner za kvalitetu i kibernetičku sigurnost

Naš tim certificiranih stručnjaka pruža usluge analize, savjetovanja i implementacije kibernetičkih sigurnosnih mjera. Posjedujemo ISO 27001 certifikat i koristimo CE certificiranu opremu usklađenu s IEC 62443 standardima. Cilj nam je optimizirati sigurnost vašeg sustava, osigurati usklađenost s regulativom i omogućiti neometan rad vaših kritičnih operacija.

Obratite nam se za analizu i unapređenje kibernetičke sigurnosti vaših OT – Nadzorno upravljačkih sustava!

Zagrel Rittmeyer d.o.o.

Ljudevita Posavskog 29

10360 Sesvete

OIB 00100837674

tel: 01 4550 817

email: zagrel@zagrel-rittmeyer.hr

web: www.zagrel-rittmeyer.com