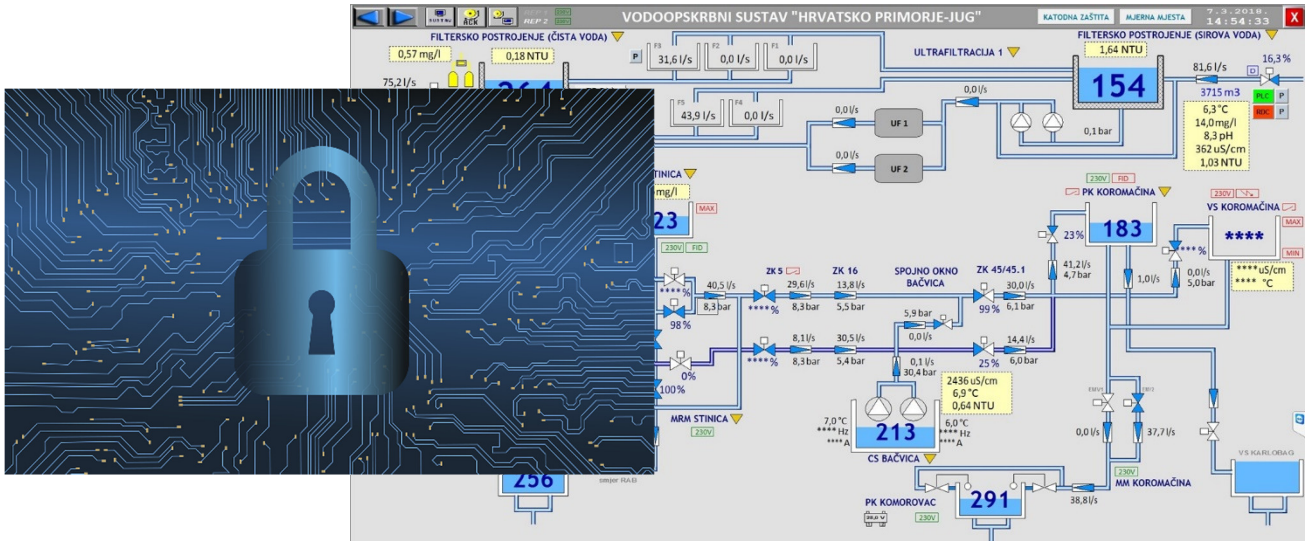
Kibernetička sigurnost i sustavi daljinskog nadzora i upravljanja

Zagrel Rittmeyer d.o.o.



Sustav daljinskog nadzora i upravljanja u vodoopskrbi i odvodnji

Danas nema vodoopskrbne komunalne organizacije koja u svom radnom procesu ne koristi daljinski nadzor i upravljanje, te obradu velikog broja prikupljenih procesnih podataka. Temeljem ovih podataka izrađuju se izvještaji, modelira se i prognozira ponašanje vodoopskrbnog sustava.

Nadzorno upravljački sustav se integrira sa sustavima za nadzor gubitaka, GIS-om, matematičkim modelima i poslovnim računalnim sustavima.

Kibernetička sigurnost

Sigurnost podataka tema je današnjice. Zbog kompleksnosti nadzorno upravljačkih sustava i ovisnosti poslovanja o njihovom pouzdanom radu, sve je veća uloga sigurnosti podataka te informatičke ili kibernetičke sigurnosti. Osnovni uzročnici nepouzdanog rada sustava su:

- Pogreške u postupcima rukovanja, upravljanja i nenamjerne ljudske pogreške,
- Nekvalitetno održavanje programske i sklopovske opreme,
- Maliciozni napadi (vanjski),
- Interni napadi,
- Prirodne katastrofe.

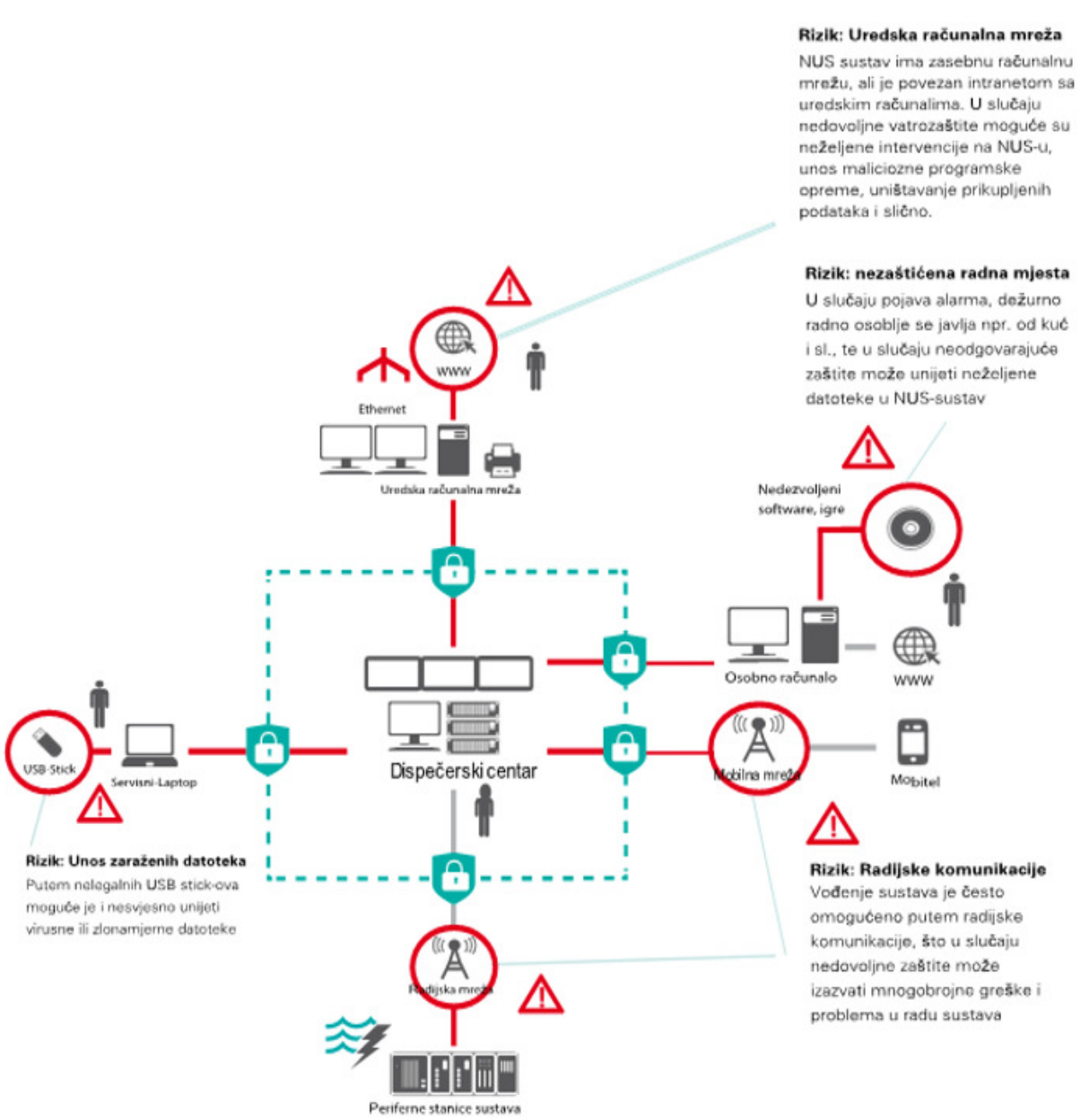
U cilju izbjegavanja navedenih uzroka nepouzdanog rada sve se više korisnika odlučuje na značajne korake u uvođenju kibernetičke sigurnosti nadzorno upravljačkih sustava.

Analiza rizika

U prvom koraku neminovno je napraviti detaljnu funkcionalnu shemu sustava, a potom analizirati slabe točke takve konfiguracije. Navest ćemo neke od primjera:

- 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?
- mogu li neovlaštene osobe pristupiti pojedinim dijelovima vašeg sustava?
- postoji li plan oporavka sustava u slučaju katastrofalnih događaja?



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 mora donijeti korisnik – vlasnik sustava.

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

- redundantne sklopovske konfiguracije,
- izdvojene lokalne računalne mreže nadzorno upravljačkog sustava,
- vatrozidovi,
- legalizirana programska oprema i propisano obnavljanje verzija operacijskih sustava te 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 i dr.)
- osiguran neometan rad osoblja, itd.

Zagrel Rittmeyer d.o.o. i ISO 27001

Sve navedene aktivnosti oko povećanja pouzdanosti rada na visoko stručnoj i profesionalnoj razini pružaju specijalisti Zagrel Rittmeyer d.o.o., u skladu sa standardom ISO 27001, čiji certifikat posjedujemo.

Obratite nam se s povjerenjem oko analize i izrade prijedloga povećanja kibernetičke sigurnosti, odnosno povećanja kvalitete i pouzdanosti vaših nadzorno upravljačkih sustava.

Zagrel Rittmeyer d.o.o.

Kraljice Jelene 6

10000 Zagreb

OIB 00100837674

tel: 01 4550 817

email: zagrel@zagrel-rittmeyer.hr

web: www.zagrel-rittmeyer.com