Mere za unapređenje bezbednosti savremenih OT mreža

* ***Slavko DUBAČKIĆ[1], Aleksandar BOŠKOVIĆ[2], Đorđe VLADISAVLJEVIĆ[1]***

[1]Centar za IKT, Elektrodistribucija Srbije doo Beograd, Srbija
[2] Fakultet tehničkih nauka, Univerzitet u Novom Sadu, Srbija

Za stvaranje efikasne i efektivne IKT bezbednosti u industrijskim upravljačkim sistemima i bezbednosti sistema zasnovanih na operativnim tehnologijama (OT) 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.

Ključne reči: *OT mreže, industrijski upravljački sistemi, IKT bezbednost.*

1. Uvod

Za stvaranje efikasne i efektivne IKT bezbednosti u industrijskim sistemima i bezbednosti sistema zasnovanih na operativnim tehnologijama (OT) potrebno je razvijati mehanizme za IKT bezbednost.
Mere o kojima se govori u ovom radu su:

- **Odgovor na incident** – Operativni plan reagovanja na incidente sa fokusom na očuvanje integriteta sistema i sposobnost oporavka čak i tokom napada. Ovo uključuje niz predviđenih incidenata i scenarija za reagovanje u tim situacijama.
- **Odbranjiva arhitektura** – Arhitekture koje pružaju potrebne funkcionalnosti (vidljivost, prikupljanje događaja, identifikaciju resursa, itd.), ali su konstruisane tako da minimizuju negativne posledice potencijalnih incidenata (segmentacija, industrijski DMZ, itd.).
- **Nadzor mreže** – Kontinuirano praćenje sigurnosti OT mreže. Koriste se alati koji su upoznati sa industrijskim protokolima i mehanizmima za otkrivanje potencijalno ranjivih tačaka u sistemu.
- **Bezbedan daljinski pristup** – Identifikacija i kontrola svih tačaka gde je omogućen udaljeni pristup.
- **Upravljanje ranjivostima putem procene rizika** – Razumevanje postojećih bezbednosnih mera, mehanizama i poznavanje rada uređaja u OT sistemima kako bi se pomoglo u donošenju odluka o upravljanju rizicima u vezi sa IKT bezbednošću OT sistema.

Pored zaštite sopstvenih resursa, kompanije imaju obavezu da štite i svoje korisnike i zajednicu u kojoj rade, mada je tu jako teško definisati granice i obime odgovornosti. Očekuje se da će kompanije pristupiti zaštiti svojih IKT resursa, uključujući i IT i OT aspekte, izvršiti procene rizika i uložiti u mehanizme zaštite. U većini kompanija postoji razumevanje za ovakve poslovne odluke. Međutim, često se dešava da su pretnje i aktivnosti napadača mnogo dinamičnije nego što kompanije mogu da ih prate i prilagode se tim promenama.
Na osnovu do sada dokumentovanih napada, autori ovog rada izdvojili su i prezentovali ključne IKT bezbednosne mere u OT sistemima. Ove mere smatraju kritičnim i procenjuju ih kao osnovni

minimum za očuvanje sigurnosti kako same kompanije, tako i bezbednosti korisnika, partnera i šire zajednice. U nekim slučajevima, ove mere su od suštinskog značaja i za nacionalnu bezbednost. Naravno, uz ove mere, mogu se primeniti i dodatne mere kako bi se dalje smanjio rizik, u skladu sa ciljevima organizacije i procenama rizika.

2. Razlike između OT i IT sistema

U kontekstu ovog rada, važno je razmotriti nekoliko ključnih razlika između OT i IT sistema. Ove razlike se obično ogledaju u sledećim aspektima: svrha sistema, starost OT sistema, specifična komunikaciona rešenja i mrežni protokoli u OT mrežama, kao i sposobnost ili nesposobnost OT sistema da prihvate određene bezbednosne mere. Međutim, važno je napomenuti da se ova razmatranja često usredsređuju na tehnološke aspekte.

U kritičnim sistemima, najveća razlika između IT i OT sistema leži u misiji ili poslovnoj svrsi sistema. IT sistemi obično su fokusirani na upravljanje poslovnim procesima, dok su OT sistemi uglavnom namenjeni osnovnim operacijama kompanije. Iz tog razloga, rizici i pretnje za ova dva tipa sistema takođe se značajno razlikuju.

Kod napada na IT sisteme, najčešći cilj je pristup samom sistemu i podacima koji se u njemu nalaze. Napadači često ne nastoje da izazovu fizičke promene u IT sistemima; njihovi ciljevi često uključuju krađu podataka ili ometanje rada sistema. Sa druge strane, tipovi napada na OT sisteme koji najviše izazivaju zabrinutost su oni koji teže da poremete funkcionalnost sistema, izazovu fizičku štetu ili čak izazovu bezbednosne incidente koji mogu dovesti do oštećenja opreme ili gubitka života. Malo je verovatno da će napadač postići takve efekte ciljajući samo jedan deo sistema. Da bi postigli razorni efekat, napadač mora da kompromituje inženjersku radnu stanicu, nauči kako da manipuliše logikom kontrolera putem nje, i sa razumevanjem te logike, utiče na proizvodni proces. Drugim rečima, napadač može da cilja jedan sistem, kako bi manipulisao drugim sistemom i izazvao fizički uticaj na trećem sistemu.

Preterano usmeravanje pažnje samo na pojedinačni OT sistem ili njegove komponente obično nije dovoljno za uspešan napad. Dizajn OT sistema omogućava komunikaciju između njegovih delova, i uspešan napadač na ovakvom sistemu sigurno će iskoristiti ove veze kako bi postigao svoj cilj - narušavanje osnovne funkcionalnosti tih sistema. Ovakav pristup predstavlja radikalno drugačiji način razmišljanja o bezbednosti informacionih tehnologija u poređenju sa većinom IT okruženja.

3. Operativni plan reakcije na incidente

Kompanije moraju imati specifičan plan reagovanja na incidente za svoje OT sisteme. Česta greška je razmišljati o reagovanju na incidente kao o poslednjem koraku u sopstvenoj strategiji bezbednosti. Ovaj pristup često rezultira neskladom između primenjenih bezbednosnih mera i potreba za reagovanjem na incidente. Na primer, kompanije mogu otkriti da njihova strategija otkrivanja pretnji, izbor arhitekture ili prikupljanje podataka više nisu adekvatni. Takođe, s obzirom na sve veće regulatorne zahteve širom sveta za prijavljivanje incidenata, kompanije moraju prepoznati koje specifične probleme i zahteve trebaju rešiti kako bi obezbedile efikasan odgovor na incidente mnogo pre nego što se incident zaista dogodi.

Ključni deo odgovora na incidente u OT sistemima je sposobnost analize osnovnih uzroka samog incidenta. Analiza osnovnih uzroka omogućava povratak u siguran režim rada, ali sve veća složenost

industrijske automatizacije čini ovu analizu izuzetno izazovnom. Planovi odgovora na IT incidente često se usredsređuju na identifikaciju napadača, njihovo obuzdavanje i otklanjanje. S druge strane, OT planovi odgovora na incidente daju prioritet akcijama koje se baziraju na potencijalu za operativni uticaj i razmatraju kako sistem može delovati tokom napada na način koji smanjuje uticaj i štetu na sam tehnički sistem. Reagovanje na incidente i ulaganje u IKT bezbednost OT sistema ne samo da smanjuje rizik, već i poboljšava operativnu otpornost omogućavajući analizu uzroka problema, bez obzira na to da li je problem nastao zbog napadača ili drugih faktora.

Pregled procesa planiranja odgovora na incidente specifičan za OT sisteme je sledeći:

- **Identifikacija scenarija koji predstavljaju najveći rizik od kojih se treba štititi** – Planiranje scenarija treba da krene od stvarnih incidenata i da se bazira na stvarnim podacima. Kompanije treba da utvrde koji su se incidenti dogodili u njihovoj oblasti i da krenu od tih podataka. Neki scenariji mogu biti relevantni za više oblasti privrede, dok se drugi mogu odnositi samo na određene vrste okruženja unutar oblasti. Na primer, naftne kompanije mogu razmatrati TRISIS napad, dok energetske kompanije mogu imati u vidu IKT napade u Ukrajini 2015. i 2016. godine. Međutim, fokus ne bi trebalo da bude samo na tome kako je napad izvršen, već pre svega na tome šta je postignuto, jer će napadači sigurno menjati svoje metode kako bi ostvarili svoje ciljeve.
- **Razmatranje scenarija zasnovanih na posledicama –** Drugi korak uključuje analizu scenarija sa aspekta njihovog uticaja na OT sistem, uzimajući u obzir najgori mogući scenario, tj. najveću moguću štetu. Scenariji zasnovani na stvarnim podacima trebaju biti prioritet, jer postoji visoka verovatnoća da će se ponoviti. Osim toga, to su scenariji iz stvarnog sveta koji su već zabeleženi, a budući da ih ima relativno malo, mogu poslužiti kao posebno korisne tačke fokusa. Scenariji zasnovani na posledicama predstavljaju „umetnost mogućeg“. Kako bi se sprečilo gubljenje u detaljima i strahu, treba razmotriti ove scenarije u okviru konteksta konkretne kompanije. Potrebno je iskoristiti stručnost i znanje interne ekipe, koja ima informacije koje napadači možda nemaju. Bez obzira na to da li se napad dogodio u stvarnom svetu, treba identifikovati uticaje sa visokim posledicama koji brinu operativce, inženjere ili rukovodstvo i utvrditi da li ih je moguće postići putem IKT napada. Potrebno je analizirati šta bi napadač morao da uradi da bi izveo takav napad i uključiti i taj scenario.
- **Simulacije** – Nakon što su scenariji izabrani i usaglašeni, važno je sprovesti testiranje koje jasno definiše ciljeve koje treba postići tokom ovih simulacija. Ovo se odnosi na svaku organizacionu jedinicu i svaki simulirani incident posebno. Ove simulacije treba ponavljati sve dok se ne postigne željeni nivo reagovanja. Ključni element ove mere u OT sistemima je uspostavljanje zajedničkog razumevanja potencijalnih rizika u poslovanju kompanije i određivanje nivoa funkcionalnosti OT sistema u slučaju napada.

4. Odbranjiva arhitektura

Odbranjiva arhitektura je dizajn sistema koji ima za cilj smanjiti rizike kroz svoj dizajn i implementaciju, istovremeno olakšavajući odbranu od potencijalnih pretnji. Važno je napomenuti da ne postoji apsolutno siguran sistem ili arhitektura – ljudski faktor igra ključnu ulogu u transformaciji odbranjive arhitekture u zaštićenu arhitekturu. Postoje različiti modeli za postizanje ovog cilja, kao što su Purdue model ili ISA/IEC 62443 arhitektura. Iako su ovi modeli važni smernice, ključna je pravilna implementacija kako bi se postigao odgovarajući nivo bezbednosti.

S obzirom na različite sisteme koji se koriste na različitim lokacijama kompanije, često dolazi do varijacija u implementaciji bezbednosnih sistema. Stvaranje potpuno standardizovanog pristupa za implementaciju bezbednosnih sistema širom kompanije obično nije izvodljivo, posebno u velikim i kompleksnim organizacijama. Međutim, cilj bi trebao biti smanjenje broja različitih rešenja na minimum.

Pri izgradnji odbranjive IKT arhitekture u OT sistemima, preporučuju se sledeće mere:

- Identifikacija imovine i inventar, barem za najvrednije objekte na ključnim lokacijama;
- Segmentacija IKT mreža radi izolacije sistema;
- Razmatranje primene principa „samo za čitanje“ gde je to moguće;
- Nadzor mrežnog saobraćaja i komunikacije sistema;
- Prihvat komunikacionih logova za praćenje aktivnosti;
- Razvoj sposobnosti za prelazak u „odbranjivu poziciju“, što znači prelazak u stanje povećane pripravnosti sa ograničenim funkcionalnostima sistema u slučajevima sumnje na napad.

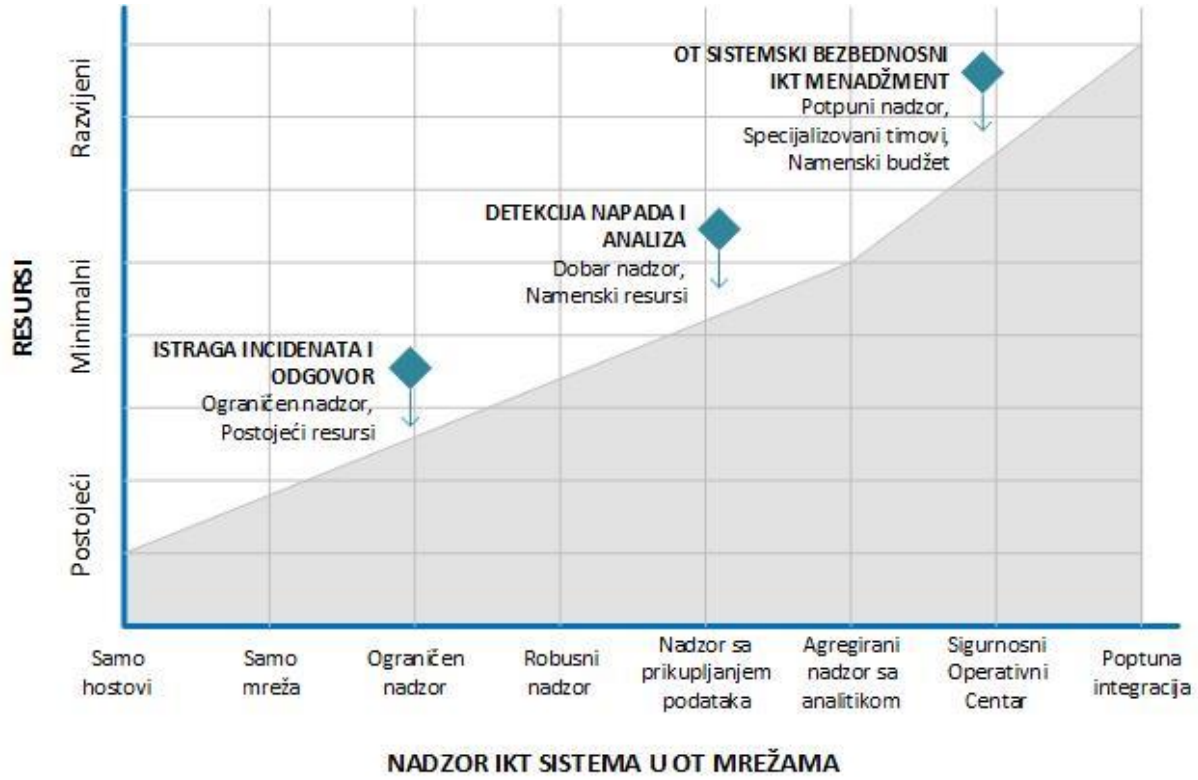
5. Vidljivost i nadzor IKT mreže

Sistemski karakter IKT sistema nameće potrebu za nadzorom mreže kako bi se razumeli međusobni uticaji unutar sistema. Nadzor specifičan za IKT sisteme u OT mrežama obuhvata inspekciju paketa IKT protokola koji su specifični za to okruženje. Dobar pristup nadzoru IKT mreže u OT sistemima pomaže u prikupljanju podataka, definisanju scenarija rizika, validaciji arhitekture i postavljanju, unapređenju i primeni mera koje će biti opisane. Osim toga, u sve složenijem okruženju industrijske automatizacije, postaje sve teže doći do analize osnovnog uzroka incidenta, čak i kod događaja koji nisu IKT napadi. Nadzor mreže specifičan za OT sisteme može doprineti opštoj otpornosti i oporavku kako bi se izbegli skupi scenariji zastoja i istraživanja.

Vidljivost i nadzor IKT mreža u OT sistemima nisu samo tehnički izazovi. Često se postavlja pitanje izbora alata za nadzor, iako ne postoji gotovo rešenje. Prilikom izbora sistema za nadzor, kompanije treba da razmotre sledeće faktore:

- Tehničke mogućnosti za nadzor i prikupljanje podataka unutar sistema;
- Korišćena oprema i protokoli u svim sistemima od interesa;
- Stručnost i obuka osoblja u kompaniji za obavljanje ovih zadataka;
- Postojeći ili očekivani procesi koji su povezani sa planovima za reagovanje na moguće incidente.

Sa realnim razumevanjem unutarnje organizacije i zrelosti tehničkih i kadrovskih IKT resursa u kompaniji, moguće je izabrati odgovarajuće rešenje koje bi trebalo da bude u skladu sa sledećom slikom.



Slika 1. Analiza spremnosti i kapaciteta za IKT nadzor

Za ocenu tehnološke platforme za nadzor IKT mreža u OT sistemima korisno je analizirati sledeće karakteristike:

- Pasivni nadzor koji ne ometa industrijske operacije;
- Inventar opreme i topologija;
- Identifikacija i analiza specifičnih OT protokola;
- Identifikacija ranjivosti;
- Otkrivanje pretnji na osnovu prethodnih scenarija i upravljanje odgovorima na incidente;
- Prikupljanje i agregacija podataka za podršku;
- Podrška za analizu osnovnih uzroka operativnih problema i prekida rada.

6. Bezbedan daljinski pristup

IT i OT digitalizacija su značajno povećale daljinsku povezanost. Ponekad je ova daljinska povezanost nepotrebna i može se smanjiti ili eliminisati. Međutim, u većini industrijskih organizacija, daljinska povezanost je neizbežna i može imati značajne poslovne i operativne koristi.

Iako su prednosti udaljenog pristupa ogromne, takođe postoje i značajni rizici, a ovih dana se, zbog pandemije COVID-19, ti rizici sve više tolerišu. Udaljeni pristup i rad od kuće postali su uobičajeni način rada. Kao rezultat toga, napadači sve više ciljaju sisteme za daljinski pristup. U većini kompanija više nije potrebno ciljati IT mreže kako bi se došlo do OT mreža. Čak i kada napadači ciljaju te mreže, to možda nisu IT mreže same kompanije, već IT mreže njenih dobavljača, osoblja za održavanje, integratora i proizvođača opreme ili čak OT mreže same kompanije.

Uspostavljanje sigurnog udaljenog pristupa je neophodno u savremenim industrijskim sistemima. Jedan od mehanizama je i višefaktorska autentifikacija (MFA), i trebalo bi je primenjivati gde god je to moguće. Tamo gde MFA nije moguća, potrebno je razviti kompenzacione mere. Ovo može uključivati pristup preko više posredničkih servera, jednosmerni pristup i slične mere.

7. Upravljanje ranjivostima putem procene rizika

Program upravljanja ranjivostima zasnovan na proceni rizika usredsređuje se na ranjivosti koje predstavljaju stvarnu pretnju kompaniji. Prioritet su ranjivosti, odnosno mehanizmi, koji bi mogli pomoći napadaču da pristupi OT mrežama ili uvede novu funkcionalnost koju bi mogao iskoristiti da izazove operativne probleme, kao što su gubitak kontrole ili bezbednosni propusti.
Cilj programa upravljanja ranjivostima nije samo potpuno otklanjanje ovih ranjivosti, već i, u mnogim slučajevima, umanjivanje njihovog uticaja ili praćenje njihove potencijalne eksploatacije. Nije uvek neophodno momentalno reagovati na određene ranjivosti (oko 4%). Oko 10% napada su potpuno bezopasni u smislu ometanja funkcionalnosti OT sistema, ali ipak ukazuju na ranjivost sistema. Preostale ranjivosti moraju se nadgledati zbog moguće eksploatacije ili ih potpuno onemogućiti.
Često se fokusiranje na ranjivosti dovodi do sukoba između IT i OT osoblja jer pronalaženje i otklanjanje svake ranjivosti u OT okruženju može imati direktan uticaj na primarnu funkcionalnost sistema. To može zahtevati ponovno pokretanje sistema ili čak potpuno razumevanje tačnih uticaja na određeni industrijski sistem. Neophodno je proceniti rizik u odnosu na potrebne aktivnosti za smanjenje tog rizika i doneti konačnu odluku o tome da li i u kojoj meri (koliko često, gde, na kojem delu OT sistema itd.) primeniti određenu preventivnu meru. Iz ovih razloga, potreban je način da se testiraju primenljivi sigurnosni zakrpi i donesu operativne odluke o riziku u vezi sa identifikovanim ranjivostima.
Izveštaji su pokazali da je za 77% dokumentovanih ranjivosti bilo potrebno direktno pristupiti uređajima unutar OT sistema. Ovaj pristup se može kontrolisati putem nadzora udaljenog pristupa (na firewall uređajima ili VPN koncentratorima) i takođe putem jednostavne kontrole fizičkog pristupa objektima i instalacijama.

8. Zaključak

Primena mera za unapređenje IKT bezbednosti u OT sistemima, o kojima se govori u ovom radu, predstavlja dobar pristup za obezbeđenje kontinuiteta poslovnih procesa, kako kroz investicione projekte tako i kroz programe održavanja sistema. Ove mere mogu biti sprovedene u sinhronizaciji sa drugim aktivnostima kako bi se stvorio dobar program IKT bezbednosti u OT sistemima koji je prilagođen rizicima sa kojima se kompanije suočavaju. Ove kritične mere prioriteta mogu pomoći kompanijama koje traže preporuke i smernice o tome šta dalje da rade, a da se to ne svodi samo na prekomerno ili nedovoljno ulaganje. Elementi podrške ovim kritičnim merama moraju uključivati:

- Identifikaciju ključnih lokacija (zdravstvo, bezbednost, poslovanje, životna sredina, nacionalna bezbednost, itd.);
- Definisanje prioritetnih taktičkih i strateških planova usklađenih sa poslovnim procesima;
- Usklađivanje sa scenarijima rizika i pretnji koji mogu uticati na poslovanje;
- Identifikaciju sopstvenih potreba i zahteva dobavljača (što je od suštinskog značaja za IKT okruženje);

- Obuku zaposlenih za upotrebu alata i tehnologija.

Iako će mere istaknute u ovom radu delovati kao vredan resurs i za stručnjake i za rukovodioce, one su manje efikasne i teže ih je primeniti bez odgovarajuće podrške unutar organizacije, što uključuje:

- Identifikaciju kritičnih objekata.
- Operativno usklađene planove odgovora na incidente.
- Organizacijsku koordinaciju u scenarijima zasnovanim na riziku.

Literatura

[1] Dubačkić S, Bošković A, Vladisavljević Đ, „Predlog mera IKT zaštite sistema upravljanja elektroenergetskim objektima“, CIGRE Srbija, 36. Savetovanje CIGRE Srbija 2023, 22.-26.5.2023, Zlatibor.

[2] Dubačkić S, Bošković A, Vladisavljević Đ, „Predlozi tipskih modela za realizaciju visoko pouzdanih lokalnih komunikacionih mreža u elektroenergetskim okruženjima“, Nacionalni komitet CIRED Srbija, 12. Savetovanje o elektrodistributivnim mrežama Srbije sa regionalnim učešćem – CIRED, 30.8.-3.9.2021, Vrnjačka Banja.

[3] Telegroup d.o.o. Beograd, „Projekat IT bezbednosti SCADA sistema ODS“, 2019, Beograd.

[4] Telegroup d.o.o. Beograd, „Projekat IT bezbednosti SCADA sistema ODS – Faza 2 – Predlog tehničkog rešenja Projekta IT bezbednosti SCADA sistema“, 2019, Beograd.

[5] Telegroup d.o.o. Beograd, „Projekat IT bezbednosti SCADA sistema ODS – Faza 3 – Tehničko rešenje IT bezbednosti SCADA sistema Naručioca po tipskim trafo stanicama i vezama (idejni projekat)“, 2019, Beograd.