OT i IT kibernetička sigurnost

Tintor, Danijel

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Stručni studij

OT I IT KIBERNETIČKA SIGURNOST

Završni rad

Danijel Tintor

Osijek, 2020.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Osijek, 22.09.2020.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Ime i prezime studenta:	Danijel Tintor
Studij, smjer:	Preddiplomski stručni studij Elektrotehnika, smjer Automatika
Mat. br. studenta, godina upisa:	A 4476, 17.09.2019.
OIB studenta:	76285055951
Mentor:	Mr.sc. Dražen Dorić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Dr. sc. Krešimir Miklošević
Član Povjerenstva 1:	Mr.sc. Dražen Dorić
Član Povjerenstva 2:	Dr.sc. Venco Ćorluka
Naslov završnog rada:	OT i IT kibernetička sigurnost
Znanstvena grana rada:	**Automatizacija i robotika (zn. polje elektrotehnika)**
Zadatak završnog rada	Problematika kibernetičke sigurnosti industrijskih upravljačkih sustava (OT) je potpuno različita od informatičke (IT) kibernetičke sigurnosti zbog različitih prioriteta (povjerljivost podataka, integritet, autentičnost i očuvanje privatnosti) ta dva svijeta i podrazumijeva potpuno različit profil stručnjaka. U konačnici obje navedene grupe stručnjaka nakon obavljanja aktivnosti na procjeni, smanjenju rizika i održavanju sustava kibernetičke sigurnosti objedinjuju rezultate svoga rada u jednu cjelinu u svrhu učinkovite zaštite tvrtke od potencijalne ugroze iz kibernetičkog svijeta, te sposobnosti brzog i sigurnog oporavka sustava u slučaju incidenta. U okviru završnog rada treba prikazati postupke kod analize rizika pri OT i IT kibernetičkoj sigurnosti, ukazati na razlike u ta dva svijeta, te navesti korake u sveobuhvatnoj
Prijedlog ocjene pismenog dijela ispita (završnog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	22.09.2020.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum: 29.09.2020.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 22.09.2020.

Ime i prezime studenta:	Danijel Tintor
Studij:	Preddiplomski stručni studij Elektrotehnika, smjer Automatika
Mat. br. studenta, godina upisa:	A 4476, 17.09.2019.
Turnitin podudaranje [%]:	3

Ovom izjavom izjavljujem da je rad pod nazivom: **OT i IT kibernetička sigurnost**

izrađen pod vodstvom mentora Mr.sc. Dražen Dorić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

Tintor Danijel

SADRŽAJ

1. UVOD

Kibernetička sigurnost veže se uz razvoj tehnologija koje se toliko brzo mijenjaju u području komunikacijske i informacijske tehnologije (ICT/IT) te u industrijskim upravljačkim sustavima (ICS). Cilj je velikom brzinom razvijati nove usluge i proizvode, dok je sigurnost tih usluga bila u sjeni i vrlo malo je mogla utjecati na nove tehnologije.

„Kibernetika“ se pojavila sredinom prošlog stoljeća te predstavlja znanost o raznim sustavima upravljanja. Pojam „kibernetički“ uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu1 još 2002. godine. „Kibernetički“ se u hrvatskom jeziku koristi kao značenje kakvo ima i prefiks „cyber-“ u engleskom jeziku.

Problematika kibernetičke sigurnosti industrijskih upravljačkih sustava (ICS - Industrial Control Systems) ili OT (Operational Technology) je potpuno različita od informatičke (ICT ili IT-Information and Communications Technology) kibernetičke sigurnosti zbog različitih prioriteta (povjerljivost podataka, integritet, autentičnost i očuvanje privatnosti) ta dva svijeta i podrazumijeva potpuno različit profil stručnjaka. U konačnici obje navedene grupe stručnjaka nakon obavljanja aktivnosti na procjeni, smanjenju rizika u održavanju sustava kibernetičke sigurnosti, objedinjuju rezultate svoga rada u jednu cjelinu u svrhu učinkovite zaštite tvrtke od potencijalne ugroze iz kibernetičkog svijeta, te sposobnosti brzog i sigurnog oporavka sustava u slučaju incidenta.

Ovdje se usmjerava na IT i OT sektore društva i njihove ranjivosti kao i prijetnje i napade koji mogu nanijeti ozbiljnu štetu sustavima. Prikazuju se različite poveznice i različiti načini upravljanja u IT i OT sektorima. Pokušava se probuditi svijest o načinima obrane i o sigurnosti od kibernetičkih zlonamjernih napadana. Stručnjaci za kibernetičku sigurnost u ovim sektorima imaju različite odgovornosti i zadaće. Kao i svuda u svijetu tako i stručnjaci u RH susreću se sa kibernetičkim prijetnjama i napadima koji se često pojavljuju.

Glavna tema ovoga rada jeste prikazati razlike među OT i IT sustava. Na početku potrebno je upoznati se sa kibernetičkom sigurnosti u cijelosti, od njenog nastanka do danas. U drugom poglavlju „Pojava kibernetičke sigurnosti, prijetnje i napadi“ opisan je način na koji je nastala kibernetička sigurnost. Nastankom kibernetičke sigurnosti javljaju se i mnoge prijetnje i napadi koji su vidljivi u istom poglavlju. U poglavlju „Industrijski upravljački sustavi (ICS ili OT) i njihova sigurnost“ približava se djelovanju i funkcijama ICS-a. Prikazuje se upravljanje i način rada u industriji. Najvažnije je u ovom djelu govoriti o SCADA sustavu koji je najbitniji za

kontrolu i prikupljanje informacija u ICS-u. Zlonamjerni napadi su uglavnom usmjereni na SCADA sustave te je potrebno objasniti moguće prijetnje i načine na koje treba osigurati takav sustav. Nadalje, u poglavlju „ Informacijsko-komunikacijski sustavi (ICT ili IT) i njihova sigurnost“ pobliže se opisuje IT sustav i njegove funkcije. Također sustav prema kome se upućuje mnogo prijetnji, stoga je potrebno razviti i različite sigurnosne mjere. Poglavlje koje objedinjuje ova dva sustava jeste „Usporedba sigurnosti u ICS/OT-u i ICT/IT-u“. Potrebno je navesti i objasniti osnovne i najznačajnije razlike i prioritete spomenuta dva sustava. Usporedba funkcija i mjera zaštite se obrađuje jer su se OT sustavi napretkom tehnologije povezali sa IT sustavima. Tako su postali OT sustavi mnogo ranjiviji. Ranjivosti ova dva sustava privlače napadače i nanose se ozbiljne štete. Povodom toga uspoređeni su poslovi i zadaće kibernetičkih stručnjaka, kao i same njihove vještine i certifikati. Kibernetička sigurnost postala je aktuelna tema u cijelom svijetu pa tako i u RH. Tomu je posvećeno poglavlje „Kibernetička sigurnost u RH“. Statistički podaci najbolje govore o osviještenosti i poznavanju društva o kibernetičkoj sigurnosti.

Iako su u današnje vrijeme napadi na nečiju imovinu zabranjeni raznim pravnim regulativama i moralnim preprekama, napadi se događaju na dnevnoj bazi i opasnosti za korisnike dolaze sa svih strana. Po nekim statistikama, potrebno je 256 dana da bi se otkrio napadač koji je prisutan u poslovnom sustavu.

Od razvoja ICT-a i ICS-a mnogo je odstupanja u radu nastalo zbog ljudskih grešaka, zlonamjernih postupaka i tehnoloških ili organizacijskih grešaka.

2. POJAVA KIBERNETIČKE SIGURNOSTI, PRIJETNJE I NAPADI

Kibernetička sigurnost postaje sve aktuelnija tema u IT i OT sektorima. Uvođenjem interneta u većinu sustava i uređaja (tzv. Internet of Things, skraćeno IoT) postaju ICT sustavi sve napredniji i zastupljeniji. Napretkom informacijskih i komunikacijskih tehnologija i ostvarivanjem veza između IT i OT računalnih mreža, te korištenjem komercijalnih PC tehnologija u OT svijetu je dovelo do ugroze do tada sigurnih OT sustava.

Putem interneta odnosno IoT, moguća su dva načina komunikacije u IT i OT sustavima:

- Uređaj - čovjek
- Uređaj - uređaj

Internet stvari (engl. Internet of Things) su sustavi koji su odvojeni od poslovnih procesa, ali utječu i daju potporu na različitim nivoima poslovanja.
Razine u integraciji i komunikaciji cjelovitog sustava proizvodne tvrtke su :

- ERP - Enterprise resource planning; = planiranje resursa poduzeća u IT sektoru.
- MES - Manufacturing execution system; = sustavi izvršenja proizvodnje, sloj između IT i OT sektora
- SCADA - Supervisory control and data acquisition**.** = računalni sustav za nadzor, mjerenje i upravljanje industrijskim sustavima u OT sektoru.

Povezivanjem IT i OT sektora pojavljuje se veliki kibernetički prostor u kome je međusobno povezana infrastruktura, mnogo raspoloživih podataka te sve veći broj korisnika koji međusobno komuniciraju. Neispravnim upravljanjem i radom na sustavu može doći do tehničkih smetnji, ali i opasnosti globalnih sigurnosnih razmjera. Društvo i stručnjaci se takvim opasnostima suprotstavljaju na razne načine koje jednim imenom nazivamo „kibernetička sigurnost“.

Kibernetička sigurnost se tiče osiguravanja ranjivih stvari putem IT-a. To se odnosi na podatke koji se pohranjuju i tehnologije koje se koriste za njihovo osiguranje. Dio kibernetičke sigurnosti u vezi s zaštitom informacijskih i komunikacijskih tehnologija - tj. hardver i softver poznat je pod nazivom ICT sigurnost.

Sektori industrije ICS/OT i ICT/IT danas predstavljaju tehnološke grane koje sve više funkcioniraju u simbiozi, određene IT tehnologije imaju značajnu primjenu u industriji, a industrija pruža podršku IT sektoru tako što pruža potrebne energije putem primarnih i rezervnih izvora. Ovakvi integracijski procesi su neizbježni i predstavljaju evoluciju poslovanja. Aktivni pristup praćenju IT trendova, novi poslovni modeli i industrijske tehnologije preduvjet su za održivi razvoj i dugoročnu konkurentnost energetskih tvrtki.

Razvoj sigurnosti energetskog sustava predstavlja novi izazov za koji se očekuje da će porasti u skorijoj budućnosti. Radi se analiza trenutnog stanja i osnovno pojašnjenje kibernetičke sigurnosti industrije u skladu s novim propisima. S obzirom na brzi porast kibernetičkih napada na ICS.

Sl.2.1. Položaj i poveznice kibernetičke sigurnosti

Sigurnost podataka - za zaštitu privatnosti i integriteta podataka u stanju mirovanja ili u pokretu.

Mrežna sigurnost - za zaštitu računalne mreže od loših aktera koji bi mogli biti ciljani napad ili zlonamjerni softver.

Operativna sigurnost - za stvaranje i održavanje procesa, postupaka i donošenja odluka za obradu i zaštitu podataka.

Sigurnost aplikacije - koncentrirati se na održavanje sigurnosti softvera i uređaja bez prijetnji.

Kontinuitet poslovanja i oporavak od katastrofe - politike i postupci koji nalažu kako organizacija ponovno uspostavlja kontrolu nad svojim radom.

Upravljanje rizikom - upravljanje organizacijskim rizikom u samom programu tvrtke za informacijsku sigurnost.

Trening o svjesnosti sigurnosti - baviti se obrazovanjem ljudi koji često uzrokuju sigurnosne ranjivosti na temelju svojih radnji ili njihovog nedostatka. Ljudi mogu nenamjerno uvesti virus ili zlonamjerni softver u inače siguran sustav ako nisu upoznati sa najboljim sigurnosnim praksama, poput brisanja sumnjivih privitaka u e-porukama, do umetanja neidentificiranih USB-ova itd. (Sl.2.1.)

2.1. Vrste kibernetičkih prijetnji

Krađa identiteta

Lažno predstavljanje je praksa slanja lažnih e-poruka koje nalikuju e-porukama iz uglednih izvora. Cilj je ukrasti osjetljive podatke poput brojeva kreditnih kartica i podataka o prijavi. To je najčešća vrsta kibernetičkih napada. Možete se zaštititi obrazovanjem ili tehnološkim rješenjem koje filtrira zlonamjerne e-poruke.

Ransomware

Ransomware je vrsta zloćudnog softvera. Dizajniran je za iznuđivanje novca blokiranjem pristupa datotekama ili računalnom sustavu dok otkupnina ne bude plaćena. Plaćanje otkupnine ne jamči vraćanje datoteka ili vraćanje sustava.

Malware

Zlonamjerni softver je vrsta softvera namijenjena za neovlašteni pristup ili oštećivanje računala.

Malware na mobilnim aplikacijama

Mobilni uređaji ranjivi su na napade malware-a baš kao i ostali računalni hardver. Napadači mogu ugraditi zlonamjerni softver u preuzimanja aplikacija, mobilne web stranice ili e-poštu i tekstualne poruke. Jednom kad je kompromitiran, mobilni uređaj zlonamjernom lopovu može omogućiti pristup osobnim podacima, podacima o lokaciji, financijskim računima i još mnogo toga.

Socijalni inženjering

Socijalni inženjering je taktika koju protivnici koriste kako bi vas naveli na otkrivanje osjetljivih podataka. Oni mogu tražiti novčano plaćanje ili dobiti pristup vašim povjerljivim podacima. Društveni inženjering može se kombinirati s bilo kojom od gore navedenih prijetnji da biste imali veću vjerojatnost da ćete kliknuti na veze, preuzeti zlonamjerni softver ili vjerovati zlonamjernom izvoru.

Prijetnje kroz IoT uređaje

IoT uređaji poput industrijskih senzora ranjivi su na više vrsta kibernetičkih prijetnji. Uključuju hakere koji preuzimaju uređaj kako bi ga učinio dijelom DoS napada i neovlašteni pristup podacima koje uređaj prikuplja. S obzirom na njihov broj, geografsku distribuciju i često zastarjele operativne sustave, IoT uređaji glavna su meta zlonamjernih aktera.

Trojanci

Nazvan po trojanskom konju drevne grčke povijesti, trojanac je vrsta zlonamjernog softvera koji ulazi u ciljni sustav izgledajući poput jedne stvari, npr. standardni dio softvera, ali zatim izdaje zlonamjerni kôd unutar glavnog sustava.

"Čovjek u sredini" (engl. Man-in-the-middle [MitM])

Kada napadač uspostavi položaj između pošiljatelja i primatelja elektroničkih poruka i presretne ih, može ih mijenjati u tranzitu. Pošiljatelj i primatelj vjeruju da izravno komuniciraju jedni s drugima. Ovakav napad može se koristiti u vojsci da zbuni neprijatelja.

Distribuirani napadi uskraćivanja usluge (engl. Distributed Denial-of-Service [DDoS])

Distribuirani napadi uskraćivanja usluge imaju za cilj narušiti računalnu mrežu preplavivši mrežu suvišnim zahtjevima za preopterećenje sustava i sprječavanje ispunjavanja legitimnih zahtjeva.

Malvertising

Zlonamjerno oglašavanje upotreba je mrežnog oglašavanja za širenje zlonamjernog softvera. (Sl.2.2.)

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

Sl.2.2. Lista najvećih kibernetičkih prijetnji

2.2. Vrste kibernetičkih napada

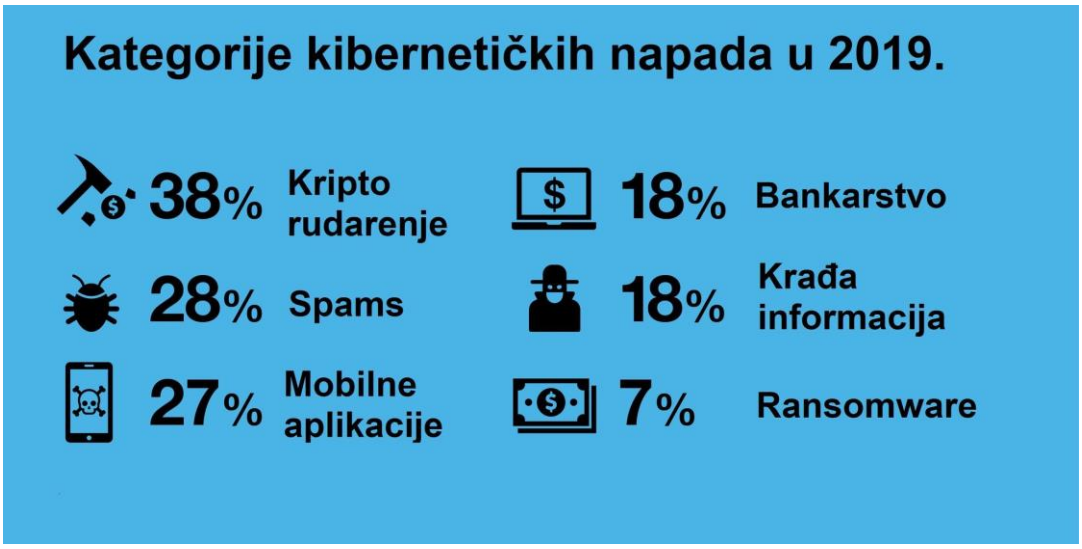
Kibernetički napadi se dijele u 4 kategorije koje će zasebno biti objašnjene u narednim odlomcima.

Kibernetički kriminal je kriminal koji je izveden uz pomoć računala ili računalne tehnologije. Najčešće se ova kategorija povezuje s prijevarama koje uključuju internet bankarstvo i razne prijevare na web trgovinama upotrebom tuđih, nelegalno stečenih, kreditnih kartica. Smatra se da je kibernetički kriminal najbrže rastući sektor globalno organiziranog kriminala, ali pretpostavka je da će u budućnosti još više rasti. Razlog za to je što za bilo kakav napad tog oblika nije potrebna fizička prisutnost napadača. U današnje vrijeme moguće je ispaliti projektil, kupiti oružje, upasti u informacijske sustave raznih državnih i nedržavnih institucija samo jednim klikom sa računala koje se ni ne nalazi u blizini mete.

Kibernetička špijunaža je akcija pomoću koje se stječu tajne informacije bez dopuštenja oštećene osobe. Najčešće se koristi u industriji kako bi se stekla prednost nad konkurencijom tako da se istraži proizvod koji će plasirati na tržište i pokuša napraviti jednak ili bolji proizvod prije negoli ga konkurencija stigne plasirati. Također, još jedna od najčešćih primjena kibernetičke špijunaže je u vojne svrhe. Razlog za to je što svaka zemlja želi biti najjača i želi znati čime raspolažu druge zemlje jer vojna nadmoć, nažalost, znači i nadmoć u svemu ostalom. Kibernetička špijunaža se izvodi pomoću špijunskih programa, računalnih virusa, trojanskih konja i raznim drugim načinima.

Kibernetički terorizam su planirani i politički motivirani napadi koje najčešće izvode nacionalne skupine, rjeđe pojedinci. Jedna od stvari koje se svrstavaju u kibernetički terorizam je regrutiranje sljedbenika ISIL-a preko društvenih mreža na kojima dogovaraju i koordiniraju napadima. Za očekivati je da će i takav oblik terorizma evoluirati na način da će svaka od tih akcija putem računala imati ljudske žrtve kao posljedicu. Ako ne direktno, onda će kombinacija kibernetičkog i fizičkog terorizma uskoro biti vrlo ozbiljna tema rasprava zaštite nacionalne sigurnosti. Jedan primjer takve kombinacije je da se uslijed fizičkog čina terorizma, npr. autobombe, onemoguće komunikacijski sustavi kako pomoć ne bi stigla na vrijeme i to bi rezultiralo puno većim brojem ljudskih žrtava.

Kibernetički rat je rat koji se vodi uz pomoć računala i računalnih mreža. Najčešće je barem jedan od sudionika država. Najjednostavnije objašnjenje kibernetičkog rata je da je to informacijski rat kojim se pokušava steći informacijska prednost nad protivnikom u ratu. Jedan od načina da se to postigne je krađa i izmjena protivničkih informacija. Kibernetički rat je zapravo događaj ili aktivnost u kojoj se kontinuirano i učestalo koristi kibernetički terorizam, kibernetičku špijunaži i kibernetički kriminal u svrhu napada na protivnika.



Sl.2.3. Vrste kibernetičkih napada u 2019.godini

Sl.2.4. Zemlje koje su pretrpjele najviše kibernetičkih napada u razdoblju od 2006.-2020.

3. INDUSTRIJSKI UPRAVLJAČKI SUSTAVI (ICS ili OT) I NJIHOVA SIGURNOST

Industrijski upravljački sustav (ICS) općeniti je pojam koji obuhvaća nekoliko vrsta kontrolnih sustava, uključujući nadzornu kontrolu i prikupljanje podataka (SCADA), distribuirane upravljačke sustave (DCS) i druge konfiguracije upravljačkog sustava, kao što su programibilni logički kontroleri (PLC), koji se nalaze u industrijskim sektorima i infrastrukturama. ICS se sastoji od kombinacija kontrolnih komponenti (npr. električnih, mehaničkih, hidrauličkih, pneumatskih) koje djeluju zajedno u postizanju industrijskog cilja (npr. proizvodnja, transport tvari ili energije). Dio sustava koji se prije svega odnosi na proizvodnju rezultata naziva se procesom. Upravljački dio sustava uključuje specifikaciju željenog izlaza ili performansi. Kontrola se može u potpunosti automatizirati ili može uključivati čovjeka u petlju. Sustavi se mogu konfigurirati za rad s otvorenom petljom, zatvorenom petljom i ručnim načinom rada. U upravljačkim sustavima s otvorenom petljom izlaz se kontrolira prema utvrđenim postavkama. U sustavima za upravljanje zatvorenom petljom izlaz ima učinak na ulaz na takav način da održava željeni cilj. U ručnom načinu rada sustavom potpuno upravljaju ljudi. Dio sustava koji se prije svega odnosi na održavanje usklađenosti s specifikacijama naziva se regulator (ili kontrola). Tipični ICS može sadržavati brojne kontrolne petlje, (HMI), alate za daljinsku dijagnostiku i održavanje, izgrađene pomoću mreže i mrežnih protokola.

Industrijski procesi nadzora ICS-a obično se koriste u industriji električne energije, vode i otpadnih voda, nafte i prirodnog plina, kemijskoj, prometnoj, farmaceutskoj, papirnoj, prehrambenoj i pećima te u diskretnoj proizvodnji.

Industrijski upravljački sustavi (ICS) izvorno su bili analogni sustavi koji su bili izolirani od svih ostalih sustava. Sigurnost, stabilnost i pouzdanost bili su najvažniji. Analogna priroda sustava bila je prikladna za davanje podataka, ali ne i za pružanje informacija. Tehnološki napredak i regulatorni zahtjevi transformirali su ICS-ove iz analognog u digitalni i povezali ih vanjskim okruženjima. Industrija se prebacila na komercijalne, neočekivane (COTS) operativne sustave poput Microsoft Windows. To je osiguralo zajednički izgled i osjećaj između ICT organizacije i organizacije ICS okruženja. Supermikroračunalu je omogućeno upravljanje glavnom stanicom bez potrebe za glavnim računalom. Mikroprocesori su pružili inteligenciju kontrolerima i instrumentima, omogućujući ovim sustavima prikupljanje i pružanje diskretnih analognih točaka, kao i opisne informacije, pa čak i lokalnu kontrolu. Ovi podaci pokazali su se od velike vrijednosti

organizacijama izvan postrojenja ili trafostanice, što je stvorilo potrebu za tim daljinskim pristupom podacima, što je značilo da je potrebno umrežavanje.

Poboljšanja u troškovnim performansama potaknula su taj razvoj, što je rezultiralo mnogim današnjim „pametnim“ tehnologijama poput pametne električne mreže, pametnog prijevoza, pametnih zgrada i pametne proizvodnje. Iako to povećava povezanost i kritičnost ovih sustava, to također stvara veću potrebu za njihovom prilagodljivošću, otpornošću, te sigurnošću.

Upotreba okruženja glavnih operativnih sustava kao što su Windows i Linux pokretanje ICS aplikacija ostavlja ih jednako osjetljive kao ICT sustavi. U isto vrijeme primjena tehničkih rješenja i metoda glavnih IT zaštita pomoći će osigurati više suvremena ICS računala i upravljačke konzole (tj. osobna računala). IT tehnologije koriste virtualne privatne mreže (VPN) za osiguranje komunikacija do i sa ICS mreža. Sigurnost ICT-a usredotočena je na snagu algoritma enkripcije, dok se sigurnost ICS-a usredotočuje na ono što prelazi u VPN.

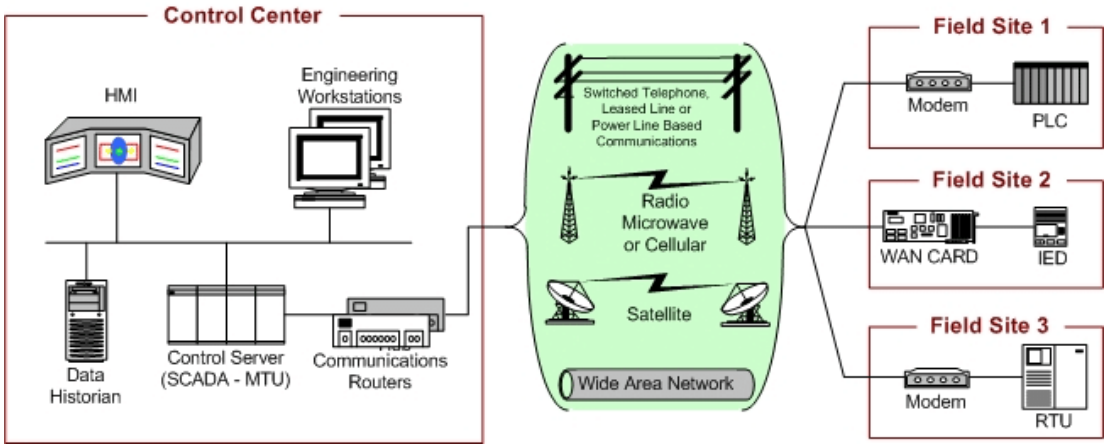
Inženjering ICS-a nastavlja se razvijati kako bi pružio nove mogućnosti uz održavanje tipičnih dugačkih životnih ciklusa ovih sustava. Inženjerski modeli i analize razvijaju se u svrhu rješavanja ovih novonastalih svojstava, uključujući sigurnost, privatnost i ovisnosti o utjecaju na okoliš.

3.1. SCADA sustav

SCADA sustavi koriste se za kontrolu raspršene imovine gdje je centralizirano prikupljanje podataka jednako važno kao i kontrola. Ti se sustavi koriste u distribuciji kao što su sustavi za distribuciju vode i odvodnju otpadnih voda, plinovodi za naftu i prirodni plin, sustavi za prijenos i distribuciju električne mreže te željeznički i drugi javni prometni sustavi. SCADA sustavi integriraju sustave za prikupljanje podataka sa sustavima za prijenos podataka i HMI softverom kako bi osigurali centralizirani sustav praćenja i upravljanja za brojne procesne ulaze i izlaze. SCADA sustavi dizajnirani su za prikupljanje informacija na terenu, prijenos u središnje računalno postrojenje i prikaz podataka operateru grafički ili tekstualno, omogućujući tako operateru da nadzire ili kontrolira cijeli sustav s središnjeg mjesta u skoro stvarnom vremenu. Na temelju sofisticiranosti i postavljanja pojedinog sustava, kontrola bilo kojeg pojedinačnog sustava, rada ili zadatka može biti automatska ili se može obavljati naredbama operatora.

Tipični hardver uključuje kontrolni poslužitelj smješten u kontrolnom centru, komunikacijsku opremu (npr. radio, telefonsku liniju, kabel ili satelit) i jedno ili više raspodijeljenih polja koja se sastoje od udaljenih terminalnih jedinica (RTU-a) ili PLC-a, koji upravlja aktuatorima i nadgleda

senzore. (Sl.3.1.). Upravljački poslužitelj pohranjuje i obrađuje informacije s RTU ulaza i izlaza, dok RTU ili PLC kontroliraju lokalni proces. Komunikacijski hardver omogućava prijenos informacija i podataka između upravljačkog poslužitelja i RTU-a ili PLC-a. Softver je programiran da kaže sustavu što i kada treba nadzirati, koji su rasponi parametara prihvatljivi i što pokrenuti kada se parametri mijenjaju izvan prihvatljivih vrijednosti. Inteligentni elektronički uređaj (IED), poput zaštitnog releja, može komunicirati izravno na upravljačkom poslužitelju ili lokalni RTU može ispitati IED-ove da bi prikupili podatke i proslijedili ga na upravljački poslužitelj. IED-ovi pružaju izravno sučelje za kontrolu i nadzor opreme i senzora. IED-ovi se mogu izravno ispitivati i kontrolirati od strane upravljačkog poslužitelja te u većini slučajeva imaju lokalno programiranje koje omogućuje da IED djeluje bez izravnih uputa kontrolnog centra. SCADA sustavi obično su dizajnirani tako da budu otporni na oštećenja sa značajnom redundancijom ugrađenom u sustav. Što možda nije dovoljna mjera zaštite od zlonamjernog napada [3].



Sl.3.1. Kontrolni centar ICS-a

3.2. Kibernetička sigurnost SCADA sustava u ICS-u

Infrastruktura koja se nalazi u energetskim sektorima upravlja se i kontrolira SCADA sustavima (nadzorno upravljanje i prikupljanje podataka). SCADA sustav u početku je bio izolirani sustav, a danas ima otvorenu arhitekturu i koristi standardne tehnologije koje su povezane s drugim korporativnim mrežama. Pri ovoj transformaciji SCADA sustavi počinju biti ranjiviji prema vanjskim napadima. Ovakav problem ranjivosti rješava se pomoću zakrpa u SCADA sustavu. Dva su ključna problema sa korištenjem zakrpa: nedostatak zakrpi i stopa neuspjeha. Korištenjem zakrpa koje nisu temeljito testirane, može dovesti do nepoželjnih članova u sustavu, što nije prihvatljivo za okolinu sustava. Zakrpe su važne za korekciju sigurnosnih i funkcionalnih problema softvera. Važne su također jer ublažavaju ranjivost softvera. Primjenom zakrpa smanjuje se mogućnost incidenata.

Zakrpe kako pomažu tako mogu u softveru predstavljati rizik. Mogu slučajno promijeniti ponašanje komponente i srušiti stabilnost procesa. Prije svakog uvođenja zakrpe u rad sustava, potrebno je testirati zakrpu i provjeriti ranjivost iste. Zakrpa se ne smije smatrati jedinom metodom obrane u ICS-u. Potrebno je povećati obranu u dubini (engl. DiD - Defense in Depth) pomoću kompenzacijskih kontrola. Izraz „obrana u dubini“ odnosi se na strategiju u kojoj se koriste višestruki slojevi obrane kako bi se spriječili napadi.

Obrambene strategije za SCADA sustave su [2]:

a) Razumjeti što SCADA sustav značiti za rad organizacije, kako se najbolje upravlja zakrpama i kako steći sigurnost. Potrebno je stručno osposobljavanje zaposlenih i upoznavanje sa informacijama o poslovanju.
   Kako održavati sigurnost i kako se postaviti u situacijama koje ugrožavaju sigurnost.
b) Očvrsnuti SCADA sustav što znači ukloniti ili onemogućiti funkcionalnost nepotrebnih komponenti u sustavu.
c) Vatrozid koji omogućuje povezivanje između pouzdanih portova i računala. Vatrozid također treba sadržavati mehanizme za alarmiranje kako bi se otkrilo ponašanje izvan zadanih parametara.
d) Povećati obranu u dubinu, odnosno identificirati komunikaciju između opreme. Na mjestima gdje oprema komunicira postavljaju se kontrole u vidu vatrozida.
e) Redovnim procjenama i kontrolama sigurnosti smanjuje se mogućnost rizika.

Na ICS terenskim uređajima ugrađuju se kibernetički-osjetljive tehnologije poput Bluetooth i bežičnih modema. To znači da je to moguće doći do SCADA mreže iz daleka. Mnoge vjetroelektrane koriste komunikacijske funkcije s ugrađenom Wi-Fi (Wireless Fidelity), općom paketnom radio uslugom (GPRS) s karticama modula identiteta pretplatnika (SIM) i RS-232 uređajima za vanjske RTU-ove. U mnogim slučajevima nije moguće zaobići ranjivi udaljeni pristup bez onemogućivanja ICS uređaja. Shodno tome, potrebno je definirati specifikacije proizvoda koje uključuju odgovarajuće sigurnosne politike i arhitekture u kojima su ICS „dizajnirani“ ranjivi.

Nenamjerne posljedice nespojivog softvera ili neprikladne komunikacije prouzročile su značajne kibernetičke incidente. To je podmukli problem jer pojedini sustavi rade onako kako je dizajnirano, dok je ranjivost međusobno povezivanje pojedinačno sigurnih sustava. U jednom slučaju, ponovno pokretanje radne stanice upravljačkog sustava koja nije bila ni u mreži upravljačkog sustava, izravno je dovelo do automatskog isključivanja nuklearne elektrane. U ovom su slučaju i radna stanica i PLC radili točno onako kako su zamišljeni. U drugom slučaju, nespojivi softver pretvorio je termo elektranu u 'yo-yo' (yo-yo je igračka načinjena od dva diska povezana osovinom na koju je zavezana uzica s petljom), uzrokujući da se prebaci s maksimalnog opterećenja na minimalno opterećenje i natrag, unutar konfiguriranih parametara, tijekom 3 sata, uzrokujući ekstremni stres na rotoru parne turbine.

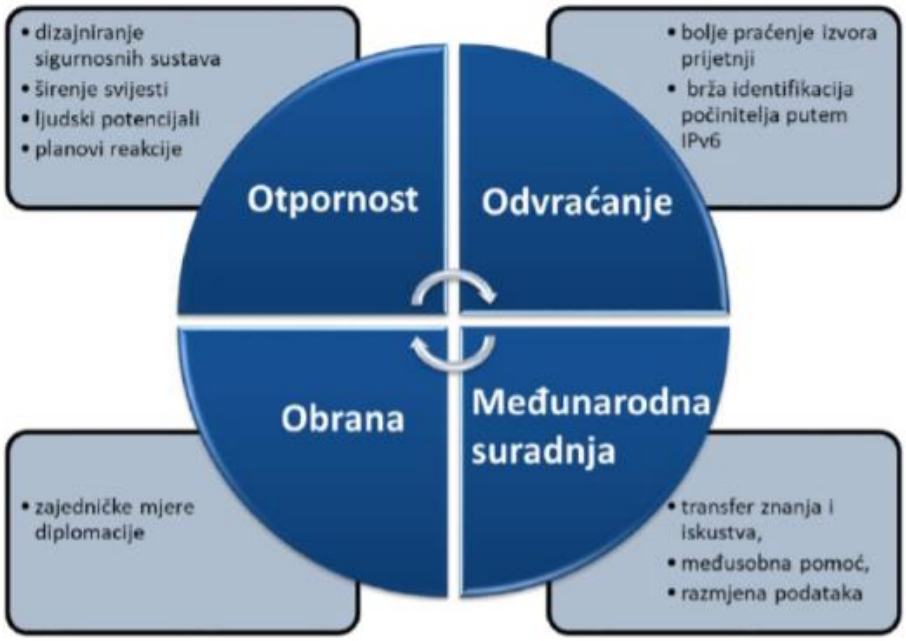
Top 10 prijetnji i napada u ICS-u
Infiltracija zlonamjernog softvera putem prijenosnih medija i vanjskog hardvera
Infekcija zlonamjernim softverom putem interneta
Ljudska pogreška i sabotaža
Kompromitiranje ekstraneta i komponenata u oblaku
Socijalni inženjering i krađa identiteta
DDoS napadi
Upravljačke komponente povezane na Internet
Upad putem daljinskog pristupa
Tehnički kvarovi i viša sila
Kompromitiranje pametnih telefona u proizvodnom okruženju

Tablica 3.1. Najčešći napadi i prijetnje na ICS

3.3. Obrambene strategije u ICS-u

Obrambene strategije SCADA sustava dio su strategija za obranu cjelokupnog ICS-a. Nakon povezivanja OT sektora sa IT sektorom nastali su veliki problemi i ranjivosti u ICS-u. Stručnjaci za sigurnost ICS-a imaju zadatak razviti strategije za obranu od napada na industriju:

- Razvoj sigurnosnih politika, postupaka, treninga i obrazovnog materijala koji se posebno odnosi na ICS.
- Bavljenje sigurnošću tijekom životnog ciklusa ICS-a od dizajna arhitekture do nabave, instalacije, održavanja do stavljanja izvan pogona.
- Implementacija mrežne topologije za ICS koji ima više slojeva, a najkritičnija komunikacija odvija se u najsigurnijem i najpouzdanijem sloju.
- Pružanje logičkog odvajanja između korporativne i ICS mreže (npr. izvanredni vatrozid za inspekciju između mreža).
- Korištenje DMZ mrežne arhitekture (tj. sprječavanje izravnog prometa između korporativne i ICS mreže).
- Dizajniranje kritičnih sustava (otpornost na pogreške) kako bi se spriječili katastrofalni kaskadni događaji.
- Onemogućavanje neiskorištenih portova i usluga na ICS uređajima nakon testiranja kako bi se osiguralo da to neće utjecati na ICS rad.
- Ograničivanje fizičkog pristupa ICS mreži i uređajima.
- Korištenjem suvremene tehnologije, poput pametnih kartica za provjeru osobnog identiteta (PIV).
- Primjena sigurnosnih kontrola poput softvera za otkrivanje provale, antivirusnog softvera i softvera za provjeru integriteta datoteka, gdje je to tehnički izvedivo, radi sprječavanja, odvraćanja, otkrivanja i ublažavanja unošenja, izlaganja i širenja zlonamjernog softvera izvan i unutar ICS-a.
- Primjena sigurnosnih tehnika poput šifriranja na ICS pohranu podataka i komunikaciju, gdje je to prikladno određeno.
- Brzo aktiviranje sigurnosnih zakrpa nakon testiranja svih zakrpa u terenskim uvjetima, ako je moguće, prije instalacije na ICS.
- Praćenje i nadzor kritičnih područja ICS-u. (Sl.3.2.)



Sl.3.2. Zajedničko jačanje otpora prema prijetnjama i napadima

3.4. Nedostaci sigurnosti pri dizajnu današnjih ICS-a

Zlonamjerni napadači traže „rupe“ u sigurnosti ICS-a kako bi došli do mogućnosti upravljanja sustavima. Napadači moraju vrlo dobro biti upućeni u nedostatke pri dizajnu sigurnosnih mehanizama. Pri dizajnu ICS-a ostali su ranjivi nedostaci [1]:

- Većina TCS protokola nema rudimentarnu provjeru autentičnosti ili mogućnosti šifriranja, pa čak i one koje se teoretski mogu sigurno konfigurirati (npr. DNP3 [Distributed Network Protocol 3], Modbus i ICCP [Inter-control Center Communications Protocol]) zahtijevaju znatni napor da se osiguraju.
- Ponovno podizanje sustava i zaustavljanja nisu zaštićena. Rudimentarni TCP / IP (Transmission Control Protocol/Internet Protocol) napadi pretjerani su u okruženju upravljačkog sustava. DDoS se može postići jednostavnim slanjem naredbi za resetiranje i ponovno pokretanje ili zaustavljanje.
- Softver nije zaštićen.
- Alat za firmware nije zaštićen. Zapravo je lakše gurnuti firmware preko Etherneta u OT okruženju nego u tradicionalnom IT okruženju. To znači da bi jednostavni firmware

mogao stvoriti sat ili čak nekoliko dana štete na razini cijele industrije. Složeniji napadi firmware mogli bi postavljati logičke bombe to bi bilo gotovo neprimjetno i moglo bi se zasaditi godinama ili desetljećima unaprijed pokrećući se. U OT domeni, logičke bombe mogu jednostavno biti promjena zadanih vrijednosti.

- Osnovna kontrola pristupa nije dostupna. Čak i osnovni pristup jezgri ili problemski način rada upravljačkih modela ne postoji na većini uređaja.
- Ethernet-serijska povezanost je sveprisutna. Postoje tri prevladavajuća Ethernet-serijska vektora napada. Mnoge osnovne funkcije nisu moguće bez serijske povezanosti, a sve češće su svi sustavi centralno upravljani putem Etherneta. Neminovno je da osobna računala (omogućena Ethernet-om) omogućuju serijski pristup. Posebno kada se radi o električnom prijenosu, komunikacijski koncentratori olakšavaju slanje Ethernet naredbi na uređaje koji naredbe prosljeđuju kao serijske naredbe. IEC 61850 može omogućiti releje za otvaranje s Etherneta krajnjim uređajem, bilo prijenosom naredbe preko serijskih linija.

4. INFORMACIJSKO-KOMUNIKACIJSKI SUSTAVI (ICT ILI IT) I NJIHOVA SIGURNOST

Informacijska i komunikacijska tehnologija (ICT) ili informacijska tehnologiju (IT) objedinjene komunikaciju, integraciju telekomunikacija i računala, također i integraciju softvera koji korisnicima omogućavaju pristup, pohranu, prijenos i obradu informacijama.

Izraz ICT koristi se i za označavanje konvergencije audiovizualne i telefonske mreže s računalnim mrežama putem jedinstvenog kablovskog sustava. Postoje veliki ekonomski poticaji za spajanje telefonske mreže s računalnim mrežnim sustavom koristeći jedinstveni sustav kabliranja, distribucije signala i upravljanja. ICT je ključni pojam koji uključuje bilo koji komunikacijski uređaj, koji obuhvaća radio, televiziju, mobitele, računalni i mrežni hardver, satelitske sustave itd. Kao i različite usluge i uređaje s njima, poput video konferencija i učenja na daljinu.

ICT je široka tema i koncepti se razvijaju. Obuhvaća svaki proizvod koji će pohranjivati, dohvaćati, obrađivati, prenositi ili primati informacije u digitalnom obliku (npr. Osobna računala, digitalna televizija, e-pošta ili roboti).

ICT sustavi koriste se u mnogim okruženjima, kao što su: uredi, trgovine, tvornice, zrakoplovi, brodovi..

ICT sustavi su svakodnevni i uobičajeni, a opet izvanredni u tome što mogu dodati dodatnu snagu onome što mi radimo i želimo raditi.

Važnost ICT sustava:

Korištenjem ICT sustava čovjek je:

- produktivniji - veći broj zadataka možemo obaviti u isto vrijeme uz smanjene troškove pomoću računala nego što smo mogli prije njihovog izuma
- u mogućnosti se nositi s ogromnim količinama informacija i brzo ih obraditi
- u mogućnosti brzog prijenosa i primanja informacija

4.1. Sigurnost u ICT sustavima

Sigurnost mreže

Mrežna sigurnost koristi se za sprečavanje neovlaštenih ili zlonamjernih korisnika da uđu u vašu mrežu. To osigurava beskompromisnost upotrebljivosti, pouzdanosti i integriteta. Ova vrsta sigurnosti je neophodna kako bi se spriječilo da haker pristupi podacima unutar mreže. Također ih sprječava da negativno utječu na mogućnost vaših korisnika da pristupe mreži ili koriste istu.

Sigurnost mreže postaje sve izazovnija jer tvrtke povećavaju broj krajnjih točaka i prelaze usluge na javni oblak.

Sigurnost na internetu

Internet sigurnost uključuje zaštitu informacija koje se šalju i primaju u preglednicima, kao i mrežnu sigurnost koja uključuje web-bazirane aplikacije. Ove su zaštite dizajnirane za nadziranje dolaznog internetskog prometa zbog zlonamjernog softvera i neželjenog prometa. Ova zaštita može biti u obliku vatrozida, antimalwarea i antispywarea.

Sigurnost krajnje točke

Sigurnost krajnje točke pruža zaštitu na razini uređaja. Uređaji koji se mogu zaštititi krajnjom točkom uključuju mobitele, tablete, prijenosna računala i stolna računala. Sigurnost krajnje točke spriječit će uređaje da pristupaju zlonamjernim mrežama koje mogu biti prijetnja vašoj organizaciji. Unaprijed zaštita od zlonamjernog softvera i softver za upravljanje uređajima su primjeri sigurnosti krajnje točke.

Sigurnost u oblaku

Aplikacije, podaci i identiteti premještaju se u oblak, što znači da se korisnici izravno povezuju s Internetom i nisu zaštićeni tradicionalnim sigurnosnim snopom. Sigurnost u oblaku može pomoći u sigurnom korištenju softverske aplikacije kao usluge (SaaS) i javnom oblaku. Sigurnosni posrednik za pristup oblaku (CASB), siguran internetski pristupnik (SIG) i jedinstveno upravljanje prijetnjama na temelju oblaka (UTM) mogu se koristiti za sigurnost oblaka.

Sigurnost aplikacije

Uz sigurnost aplikacija, aplikacije se posebno kodiraju u vrijeme njihova stvaranja kako bi bile što sigurnije, kako bi se osiguralo da nisu ranjive na napade. Ovaj dodani sloj sigurnosti uključuje procjenu koda aplikacije i identificiranje ranjivosti koje mogu postojati unutar softvera.

Sl.4.1. ICT/IT sustav

Top 10 prijetnji i napada u ICT-u
Malware
Web napad
Malware na mobilnim aplikacijama
Krađa identiteta
Spam
DDoS napadi
Trojanci
Ransomware
Manipulacija podacima
Curenje informacija

Tablica 4.1. Najčešći napadi i prijetnje na ICT sustave

5. USPOREDBA SIGURNOSTI U ICS/OT-u I ICT/IT-u

Prije svega, razlog ove usporedbe je razlika kibernetičkog sustava industrijskog nadzora (ICS) i kibernetičkog sustava ICT nadzora. Drugo, ako su politike informacijske tehnologije (IT) procedure, tehnologije i ispitivanja bili dovoljni za osiguravanje ICS-a, ne bi bilo potrebe za sustavima za nadzornu kontrolu i sigurnost prikupljanja podataka (SCADA), ali oni nisu. Temeljni problem je gledati na tehnologije kibernetičke sigurnosti i prijetnje kao jednako primjenjive na ICT i ICS. Određene glavne ICT sigurnosne tehnologije negativno utječu na rad ICS-ova.

Primjeri uključuju upotrebu alata za skeniranje portova, što rezultira zamrzavanjem komponenata i blokiraju enkripciju, što usporava rad upravljačkog sustava. To rezultira uskraćivanjem usluge (DDoS). ICT sustavi pružaju najbolji trud u ispunjavanju zadatka. ICS su "deterministički" jer to moraju učiniti sada i ne mogu čekati kasnije, jer to može imati značajne posljedice za djelovanje ICS-a.

U početku su ICS imali malo sličnosti s ICT sustavima po tome što su ICS bili izolirani sustavi koji pokreću protokole upravljanja koristeći specijalizirani hardver i softver. Široko dostupni, jeftini uređaji Ethernet i internetskog protokola (IP) sada zamjenjuju starije vlasničke tehnologije, što povećava mogućnost kibernetičke ranjivosti i incidenata. Budući da ICS prihvaća informatička rješenja za promicanje korporativne povezanosti i mogućnosti udaljenog pristupa, a dizajnira se i implementira pomoću standardnih računala, operativnih sustava (OS) i mrežnih protokola, počinju nalikovati ICT sustavima. Ova integracija podržava nove ICT mogućnosti, ali pruža značajno manju izolaciju ICS-a od vanjskog svijeta od prethodnih sustava, stvarajući veću potrebu za osiguravanjem tih sustava. Iako su sigurnosna rješenja dizajnirana za rješavanje ovih sigurnosnih problema u tipičnim ICT sustavima, moraju se poduzeti posebne mjere opreza prilikom uvođenja istih tih rješenja u ICS okruženja. U nekim su slučajevima potrebna nova sigurnosna rješenja prilagođena ICS okruženju.

ICS ima mnogo karakteristika koje se razlikuju od tradicionalnih ICT sustava, uključujući različite rizike i prioritete. Neki od njih uključuju značajan rizik za zdravlje i sigurnost ljudskih života, ozbiljnu štetu okolišu i financijska pitanja poput gubitaka u proizvodnji i negativan utjecaj na nacionalnu ekonomiju. ICS imaju različite zahtjeve za performansama i pouzdanošću, a također koriste operativne sustave i aplikacije koje se mogu smatrati nekonvencionalnima za tipično ICT osoblje.

5.1. Operativne razlike između ICS/OT-a i ICT/IT-a

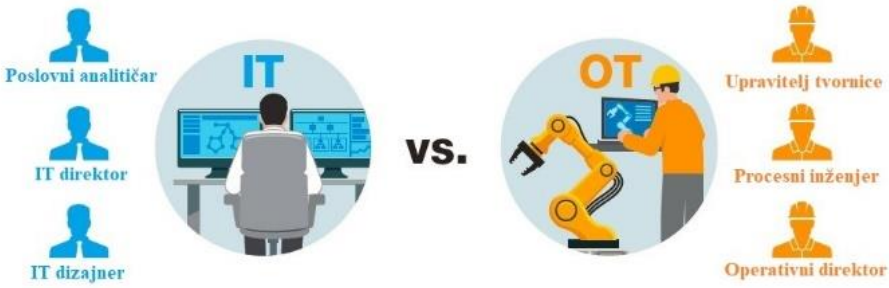
Kao i svi sustavi, za osiguravanje učinkovitog rada potrebno je periodično održavanje i podešavanje koje je potrebno unaprijed zakazati kako ne bi došlo do utjecaja na sustav. To također mora uključivati sigurnosne zakrpe. Mnogi se procesi ne mogu zaustaviti bez uzrokovanja značajnih ekonomskih, a možda čak i sigurnosnih učinaka. Bilo je mnogo slučajeva gdje je ICS utjecao jer su korporativni ICT zahtijevali brzu zakrpu, što je rezultiralo time da je "lijek gori od bolesti." Gašenje velikog industrijskog postrojenja može koštati i nekoliko stotina tisuća dolara u minuti.

Trenutno stanje u svijetu ICT-a osigurava visoki stupanj inteligencije i mogućnosti obrade raznih uređaja unutar ICT sustava. Standardna implementacija pruža centralizirane kontrolne točke za autentifikaciju i autorizaciju ICT aktivnosti. Oprema i softveri u ICT-u mijenjaju se generacijski svakih 5-7 godina, dok su u ICS-u oprema i softveri dugotrajniji, puno sporije se mijenjaju. Po samoj prirodi ICS-a i njihovim predviđenim funkcijama, ICS-ovi mogu biti stari od 15 do 20 godina, možda i stariji, prije predviđene zamjene. Kao što se može vidjeti, očekivanja uređaja različita su za ICS i ICT sustave, a ta razlika stvara dva nevjerojatno složena problema: kako autentificirati pristup i kako zakrpati ili nadograditi softver.

Od značajne važnosti je unutarnja i intersistemska komunikacija kako u ICT-u tako i u ICS-u oblasti. ICS-ovi su namijenjeni za rad u bilo kojem trenutku, bez obzira na to jesu li povezani s drugim sustavima ili ne. Ta neovisnost čini ICS vrlo fleksibilnim. Starost opreme otežava pravilno provjeru komunikacije, i to ne samo između poslužitelja, već i između poslužitelja i uređaja, uređaja i uređaja, radnih stanica i uređaja te uređaja i ljudi. Starije tehnologije zbog nedostatka odgovarajućih operativnih sustava nemaju mogućnost pristupa centraliziranim procesima provjere autentičnosti. Mnogi ICS-ovi dizajnirani su tako da inženjer ICS-a bude administrator sustava. Stoga je primjena centralizirane provjere autentičnosti neprimjerena današnjim tehnologijama. U ICT mreži pravila provjere autentičnosti odvijaju se u pozadini i većinom su skrivena od krajnjeg korisnika. U ICS mreži filtar za provjeru autentičnosti nalazi se u prvom planu i zahtijeva interakciju s krajnjim korisnikom, što uzrokuje kašnjenje i frustraciju. Zakrpa ili nadogradnja ICS-a ima mnogo zamki. Za utvrđivanje zakrpa treba provjeriti da li je zakrpa zaista jednaka onoj koja je poslana i da biste utvrdili da zakrpa stvarno popravlja grešku i neće negativno utjecati na performanse sustava. To nije tako lako kao što se čini.

Važno je pitanje kako zaštititi nezamislive, nesigurne radne stanice poput onih koje i dalje postoje?

Ukratko, operativne i rizične razlike između ICS i ICT sustava stvaraju potrebu za povećanom sofisticiranošću u primjeni kibernetičke sigurnosti i operativnih strategija. Višefunkcijski tim kontrolnih inženjera, operatora upravljačkih sustava i IT sigurnosnih stručnjaka treba usko surađivati kako bi razumio moguće komplikacije instalacije, rada i održavanja sigurnosnih rješenja u kombinaciji s radom upravljačkog sustava. IT stručnjaci koji rade s ICS-om moraju razumjeti utjecaj pouzdanosti tehnologija informacijske sigurnosti prije implementacije. Neki od OS-ova i aplikacija koji rade na ICS-u možda neće raditi ispravno s računalnim rješenjima za kibernetičku-sigurnost (COTS) zbog specijaliziranih arhitektura ICS okruženja.



Prioritet br.1	Povjerljivost	Dostupnost
Fokus	Cjelovitost podataka je ključna	Kontrolni proces ne tolerira zastoje
Cilj zaštite	Windows računala, serveri	Industrijski uređaji, čitači bar kodova
Utjecaj okoline	Klimatizacija	Ekstremne temperature, vibracije i udari

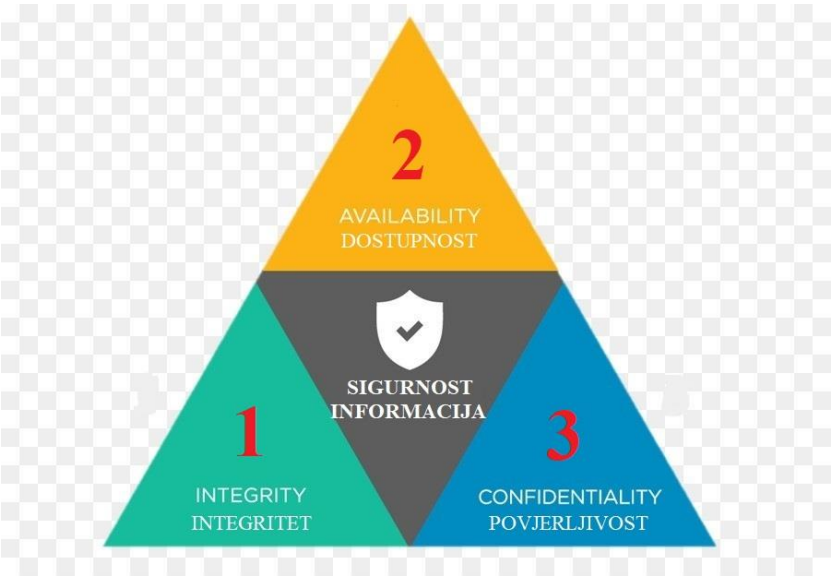
Sl.5.1. Osnovne razlike između ICS/OT-a i ICT/IT-a

U ICT domeni kibernetički napadi često su usredotočeni na stjecanje vlasničkih podataka. Shodno tome, trojka povjerljivosti, integriteta i dostupnosti (CIA) (Sl.5.2) (Sl.5.3.) rezultira povjerljivošću najvažnijim atributom koji diktira potrebu šifriranja. Međutim, u domeni ICS kibernetički-napadi uglavnom su usredotočeni na destabilizaciju imovine. Posljedično, luk integriteta i dostupnosti mnogo je važniji od povjerljivosti, činjenica koja smanjuje važnost šifriranja i značajno povećava važnost provjere autentičnosti i integriteta poruke. ICS sigurnost trebala bi se usredotočiti na tehnologije koje se bave cjelovitošću i dostupnošću. (Sl.5.1.)

ICS sigurnost je inženjerski problem koji zahtijeva inženjerska rješenja. Otpornost i robusnost su kritični čimbenici održivosti kompromitiranih ICS-ova, ICS sigurnost zahtijeva uravnoteženi pristup dizajnu tehnologije, razvoju i testiranju proizvoda, razvoju i primjeni odgovarajućih ICS

politika i postupaka, analiziranju namjernih i nenamjernih sigurnosnih prijetnji i proaktivnog upravljanja komunikacija preko pogleda, zapovjedništva i upravljanja, nadgledanja i sigurnosti.

Sl.5.2. Trokut prioriteta u ICT sustavima (CIA- confidentiality, integrity, availability/ povjerljivost, integritet, dostupnost)



Sl.5.3. Trokut prioriteta u ICS-u (integritet, dostupnost, povjerljivost)

5.2. Stručnjaci za kibernetičku sigurnost u ICS/OT-u i ICT/IT-u te njihove odgovornosti

Inženjer za kibernetičku sigurnost je profesionalac koji stvara i izvršava sigurna mrežna rješenja koja pružaju sigurnost od kibernetičkih napada, hakera itd. Oni također redovito prate i testiraju te sustave kako bi osigurali da su sustavi i mreže ispravno ažurirani i rade. Inženjer za kibernetičku sigurnost može biti poznat po nekoliko drugih imena poput IT inženjera zaštite podataka, inženjera zaštite podataka ili čak inženjera za web sigurnost. Također, uloga inženjera za kibernetičku sigurnost često se integrira s ostalim IT ulogama jer nedostaje raspoloživa radna snaga.

Stručnjak za kibernetičku sigurnost brine se o svakodnevnim operacijama i strukturama podataka nadgledajući operativne performanse. Konfiguriraju antivirusne sustave i konzole. Profesionalci moraju imati dubinsko razumijevanje sustava upravljanja ranjivima i zajedničkih sigurnosnih aplikacija. Oni provode nadogradnju softvera i objašnjavaju kriterije rada, konfiguraciju dokumenata i specifikacije sustava. Oni upravljaju sustavom PPC-a od prijetnji i identificiraju i upravljaju incidentima i ublažavaju rizike.

Provodi analizu prijetnji i rizika i daje bitne prijedloge. Stručna pomoć u provođenju istraživanja, testiranja, procjene i uvođenja sigurnosnih postupaka. Specijalist dizajnira materijale za obuku o sigurnosti i organizira treninge za ostale odjele. Profesionalci će ispitati i procijeniti tehnologije povezane sa sigurnošću. Rješavaju sigurnosne probleme i druge probleme koji se tiču podataka. Oni vode računa o podacima mrežnog prometa i internetske povezanosti i izvješćima o rizicima.

Stvara vlastite alate i aktivno sudjeluje u pregledu sigurnosne arhitekture klijentskih tehnologija. Profesionalci provode procjenu rizika i analizu utjecaja poslovanja na nove sustave i tehnologije. Održavaju srdačan odnos s ključnim partnerima.

Stručnjak za kibernetičku sigurnost nudi integraciju i implementaciju sigurnosnog rješenja računalnog sustava. Moraju ispitati tehničke probleme i pružiti osnovni inženjering i dodatnu podršku u rješavanju problema. Odgovornost je stručnjaka za kibernetičku sigurnost da osigura da su svi informacijski sustavi funkcionalni i sigurni. Profesionalci se moraju držati u različitim fazama životnog ciklusa razvoja sustava kako bi obavili analizu rizika.

Odgovoran je za brigu o ugrađenim sigurnosnim sustavima softvera, hardvera i komponenti. Oni moraju razviti jedinstvene strategije za softverske sustave, mreže, podatkovne centre i hardver. Profesionalci moraju razumjeti QA softver i hardver za sigurnosne ranjivosti i rizike. Moraju razviti vatrozid kako bi osigurali mrežnu infrastrukturu. Upravo je on taj koji mora prepoznati

kibernetičke napadače i prijaviti se višem rukovodstvu. Moraju paziti na vanjske upada, napade i hakere. Profesionalci bi trebali zatvoriti sigurnosnu ranjivost u slučaju napada.

5.2.1. Usporedba inženjera za kibernetičku sigurnost u ICS/OT-u i ICT/IT-u

Spomenute dvije grupe stručnjaka moraju razviti različite vještine i posjedovati određene certifikate.

Najznačajniji certifikati i vještine IT stručnjaka [8]:

- Ovjereni etički haker (CEH) – stručnjak (haker) koji razumije slabosti i ranjivosti u sustavima te koristi isto znanje i alate kao i zlonamjerni haker, ali na zakonit i legitiman način.
- Certifikat za kontrolu rizika i informacijskih sustava (CRISC) - CRISC je jedini certifikat koji IT stručnjak priprema za jedinstvene izazove upravljanja informacijama i rizikom u poduzeću.
- Ovlašteni kontroler informacijske sigurnosti (CISM) - CISM znači veći potencijal zarade i napredovanje u karijeri.
- Ovlašteni revizor informacijskih sustava (CISA) - svjetski poznat kao standard postignuća za one koji vrše reviziju, kontrolu, nadzor i procjenu informacijske tehnologije i poslovnih sustava.
- Ovlašteni stručnjak za sigurnost informacijskih sustava (CISSP) - dokaz da se posjeduju vještine potrebne za učinkovito osmišljavanje, primjenu i upravljanje programom za kibernetičku sigurnost.
- CompTIA Security + - prvo je sigurnosno certificiranje koje bi IT profesionalci trebali zaraditi. Utvrđuje osnovno znanje potrebno za bilo koju ulogu kibernetičke sigurnosti i pruža odskočnu dasku za poslove na kibernetskoj sigurnosti srednje razine.

Odgovornosti IT stručnjaka za kibernetičku sigurnost su:

- Stvoriti, izvršiti, implementirati, nadgledati i nadograditi sve sigurnosne mreže i sustave kako bi zaštitili kompletne podatke organizacije.
- Provesti procjenu sigurnosnih zahtjeva organizacije i uspostavite najbolje prakse i standarde.
- Odgovoriti na bilo kakva kršenja sigurnosti unutar mreža i sustava organizacije.
- Obavljati redovita ispitivanja prodora.
- Redovito provoditi razne testove kako bi se otkrila bilo kakva ranjivost u sustavu i mreži.
- Otkriti bilo kakve slučajeve sigurnosnih i mrežnih problema.
- Poduzeti relevantne mjere za zaštitu postojećih podataka i infrastrukture organizacije.
- Aktivno sudjelovati u istragama za bilo kakve povrede sigurnosti.
- Svakodnevno se baviti poslovima poput komunikacije i koordinacije s različitim odjelima organizacije.
- Aktivno sudjelovati u procesu upravljanja promjenama.
- Uloge i odgovornosti inženjera za kibernetičku sigurnost vrlo su slične ulogama sigurnosnog analitičara. Sigurnosni analitičar provest će sustav kroz svoje korake, dok će inženjer za kibernetičku sigurnost izgraditi rješenja za osiguranje sustava i mreža. U mnogim će organizacijama posao inženjera za kibernetičku sigurnost i sigurnosnog analitičara biti vrlo sličan.

Najznačajniji certifikati i vještine OT stručnjaka:

Za TÜV certifikat stručnjaka za kibernetičku sigurnost u operativnoj tehnologiji potrebno je:

- Kombinirati opće i specijalno operativno tehnološko znanje (OT) i razumijevanje o kibernetičkoj sigurnosti.
- Primjena teorijskih i praktičnih metoda kibernetičke sigurnosti na analizu i rješavanje problema kibernetičke sigurnosti.
- Pružanje tehničkog i komercijalnog vodstva u domeni kibernetičke sigurnosti OT-a.
- Dokaz učinkovitih međuljudskih vještina.
- Demonstracija osobne predanosti profesionalnim standardima, prepoznavanje obveza prema društvu, profesiji i sigurnosti.

Odgovornosti OT stručnjaka za kibernetičku sigurnost su:

- Razviti sigurnosne inženjerske zahtjeve, postupke i politike za nadogradnju, industrijski nadzorni sustav (ICS) i nadzornu kontrolu.
- Primijeniti znanje o industrijskoj opremi i procesima za razvoj sigurnih dizajna mrežne arhitekture.
- Identificirati iskoristive ranjivosti koje bi mogle utjecati na operacije.
- Ocijeniti sustave za kibernetičke rizike i aktivnosti sanacije te dizajnirati i implementirati industrijska rješenja za praćenje kibernetičke sigurnosti.
- Identificirati probleme integracije COTS / GOTS sustava, nedostatke u implementaciji sigurnosne kontrole i preporučiti poboljšanja za jačanje sigurnosnog položaja.
- Steći potpuno razumijevanje klijentove tehnologije i informacijskih sustava.
- Obavite testiranje ranjivosti, procjenu rizika i sigurnosti koristeći način razmišljanja penetracijskih testera.
- Osigurati tehnički nadzor (i smjernice) sigurnosnom timu.
- Nadgledati programe svjesnosti o sigurnosti.
- Dostavljati tehnička izvješća i službene papire o nalazima ispitivanja.
- Razviti ili ažurirati politike i vodiče za upravljanje sigurnošću.

5.3. Ranjivosti u ICS/OT-u i ICT/IT-u

Načini ugrožavanja ICS-a uključuju: gubitak vida (LOV), manipuliranje vidom (MOV), odbijanje kontrole (DOC) i gubitak kontrole (LOC) [1]:

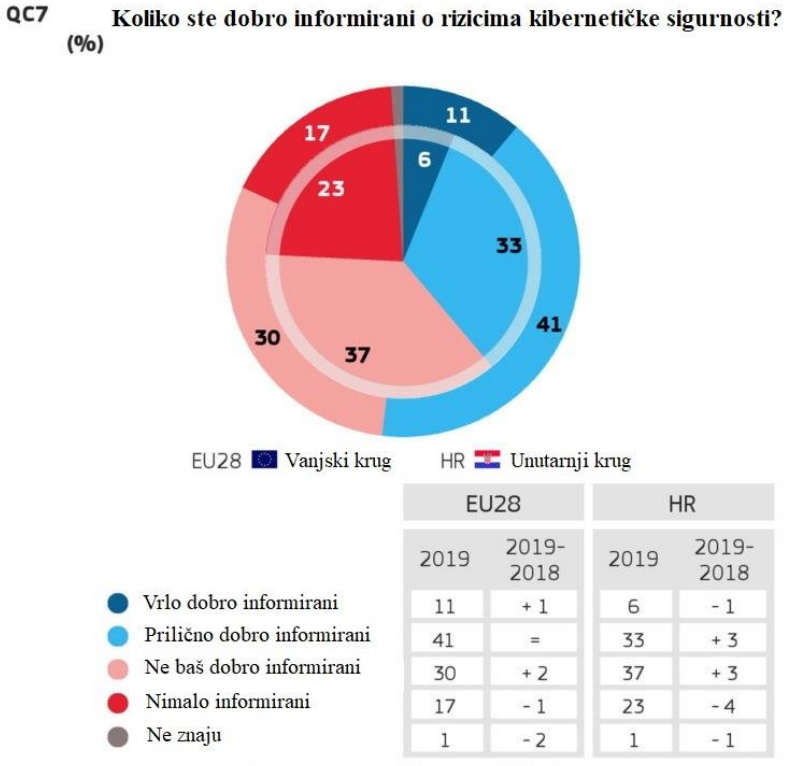
- LOV „zaslijepi“ operatere i stvara rizik poduzimanja neprimjerenih ili štetnih radnji zbog netočnih saznanja o stanju sustava. Zbog toga će mnogi operateri postrojenja ručno zatvoriti svoje objekte na LOV. Primjer je kada crvi ili virusi koji ciljaju Windows isključuju HMI, a operatori ručno isključuju turbine za izgaranje i proizvodnju. LOV s posljedičnim gašenjem elektrane se dogodio s crvima.
- MOV je uzrokovan namjerno, manipuliranjem upravljačkih zaslona kako bi rukovodio zaposlenikom. Kao primjer, promijenjene su nacionalne laboratorijske demonstracije. Prikazano stanje IED-a od zatvorenih do otvorenih, čime operater može raditi potencijalno opasne operacije, učinkovito postaje napadač.
- DOC je mjesto gdje, nenamjernim ili namjernim radnjama, operaterima se uskraćuje mogućnost za interakcijom s kontrolnim točkama procesa. Nenamjerni DOC uključuje nezgode operatera, kvarove hardvera, kvarove na mreži ili nepravilni mrežni kapacitet. Emisija nuklearne elektrane Browns Ferry bila je slučaj DOC-a.
- LOC je stalni gubitak kontrole ili stvaranje nestabilnih uvjeta u kojima operateri ne mogu poduzimati alternativne mjere prije nego što dođe do potencijalnog katastrofalnog stanja. Pucanje plinovoda Bellingham, Washington, slučaj je LOC-a.

Budući da postoji toliko mnogo načina pristupa ICS uređajima, imovina zaštićena provjerom identiteta može se ugroziti ako se iskoristi ranjivost koja zaobilazi provjeru autentičnosti, koristi se neautorizirana pouzdana veza (npr., SQL napadi ubrizgavanja) ili se vrši DDoS napad protiv otvorenih portova.
Obično napadači u ICT zajednici zahtijevaju vrlo malo ranjivosti baze podataka za dobivanje povjerljivih podataka. Trenutačne se ICT sigurnosne discipline jako usredotočuju na ranjivost u jednoj točki, ali to je rijetko slučaj za ICS.

U ICT zajednici često se raspravlja o sigurnosti softvera. Osiguranje softvera uključuje dodatne discipline sigurnosti i pouzdanosti softvera. Cilj jamstva softvera je pružiti opravdano pouzdanje da softver nema ranjivosti, da funkcionira na predviđen način i da na predviđen način ne ugrožava sigurnost, okruženje ili informacije s kojima rukuje.

6. KIBERNETIČKA SIGURNOST U RH

Prema najnovijem istraživanju Europola [6] „ Za 2019. godinu o stavovima Europljana prema kibernetičkim prijetnjama svijest o kibernetičkom kriminalu raste, 52% ispitanika izjavili su da su prilično dobro ili vrlo dobro informirani o kibernetičkim prijetnjama, u odnosu na 46% u 2017. godini. Međutim, Europljani postaju manje sigurni u svoju sposobnost zaštite Interneta: 59% korisnika interneta smatra da se mogu dovoljno zaštititi od kibernetičkog kriminala, što je značajan pad jer je taj postotak u 2017. godini bio 71%“. (Sl. 6.1.)



	EU28		HR	
	2019	2019-2018	2019	2019-2018
Vrlo dobro informirani	11	+ 1	6	- 1
Prilično dobro informirani	41	=	33	+ 3
Ne baš dobro informirani	30	+ 2	37	+ 3
Nimalo informirani	17	- 1	23	- 4
Ne znaju	1	- 2	1	- 1

Sl.6.1.Razina svijesti o sigurnosti na internetu, vanjski krug je informiranost Europljana, unutarnji krug informiranost u Hrvatskoj

Dokaz da napadači ne biraju žrtvu i da su kibernetičke prijetnje „pred vratima“ Hrvatske je napad na Ministarstvo vanjskih i europskih poslova, prema podacima CERT-a, 2015. godine. Iako napadači nisu došli do bilo kakvih povjerljivih podataka, sam čin napada se smatra ozbiljnim ugrožavanjem nacionalne sigurnosti.

Nacionalni CERT navodi „ U prvih devet mjeseci 2019. godine Nacionalni CERT je obradio 804 incidenta, odnosno 17,5% više u odnosu na cijelu 2018. godinu, kada su zabilježena 684 incidenta.

To se može pripisati povećanoj razini svijesti korisnika o informatičkoj sigurnosti te saznanja da u Hrvatskoj postoji tijelo koje se bavi kibernetičkim incidentima [5].

Vodeći tipovi incidenata u Hrvatskoj u prvih devet mjeseci 2019. godine su bili krađa identiteta i web defacement (kompromitirano web sjedište s izmijenjenim izgledom ili sadržajem web stranice).“

Početak prošle godine obilježile su prijevare starijih osoba preko lažnih profila na Facebooku, a preko kojih ih se tražilo novac. S tim se slučajem bavila i policija. Nakon toga je trajala e-mail phishing kampanja prema korisnicima jedne banke koji je vodio na lažnu stranicu dotične i zavaravao klijente da se prijave. Uslijedile su lažni mailovi s CEO porukama, a CERT je tražio stopiranje daljnjeg slanja takvih mailova od kolega iz inozemstva.
Drugi kvartal započeo je e-mail phishing napadom na korisnike Hrvatske pošte. Potom je CERT spriječio širenje MikroTika koji je širio maliciozne softvere za rudarenje kriptovaluta, kao i lažna stranica za alat za čuvanje lozinki.
Najveći udio žrtava su iz područja industrije, a drugi najveći udio žrtava su iz područja financija. Najnoviji veliki napad se dogodio 14. veljače 2020. kada je INA bila meta velikog kibernetičkog napada ucjenjivačkim zloćudnim programom (malware) koji je interno značajno utjecao na poslovanje. INA je imala problema s izdavanjem bonova za mobitele i elektroničkih vinjeta te naplate komunalnih računa. Nešto više od mjesec dana nakon napada, situacija je stavljena pod kontrolu, barem kada je riječ o uslugama usmjerenima prema krajnjim korisnicima. Dok je opskrba tržišta bila sigurna. Prodaja goriva na maloprodajnim mjestima se odvijala neometano. Neslužbena informacija je da su kibernetički kriminalci ucjenjivali naftnu kompaniju za 1500 Bitcoina što preračunato u domaću valutu iznosi oko 100 milijuna kuna. U hrvatskim okvirima 100 milijuna kuna je rekordan iznos za neku korporativnu ucjenu i dovoljno velik da zabrine domaće kompanije.

Tvrtke u Hrvatskoj, kao i u svijetu, imaju tehnologiju na zavidnoj razini. Ulažu i sadrže najnoviju opremu, sustave i programe. Tvrtke najčešće zanemare brigu o sigurnosti, odnosno tvrtke najčešće nemaju pravila o sigurnom korištenju računala, ne ugrožavajući informacije i podatke na njima.

Republika Hrvatska donosi „ Uredbu o kibernetičkoj sigurnosti operatera ključnih usluga i davatelja digitalnih usluga“ koja preuzima direktivu Europskog parlamenta o mjerama visoke razine sigurnosti. Uredba je ključni dokument i njeno postojanje je značajno za sve vlasnike IT i OT sustava. Uredba sa zakonima dostupna je u literaturi [7].

7. ZAKLJUČAK

Tema ovog završnog rada je usporedba sigurnosti u OT i IT sustavima, te sličnosti i razlike u sigurnosti ta dva sustava. Naziv operativne tehnologije (OT) odnosi se na industriju, a to uključuje hardver i softver koji otkriva ili uzrokuje promjene izravnim praćenjem i kontrolom industrijske opreme, imovine i procesa. Pod pojmom Informacijske Tehnologije (IT) smatra se upotreba računala za pohranu, dohvaćanje, prijenos i obradu podataka ili informacija. Dok se u IT sustavima najveći prioritet daje povjerljivosti podatka u OT sustavima to je dostupnost, odnosno pouzdanost. Ova razlika u prioritetima IT i OT sustava je glavni razlog zašto se metodologije ispitivanja IT sigurnosti, uobičajeni nalazi i zajedničke preporuke ne mogu jednostavno prilagoditi i ponovno upotrijebiti u OT sustavima.

Ovaj završni rad na početku obrađuje vrste kibernetičkih napada i prijetnji, te zatim glavne značajke industrijskih upravljačkih sustava i informacijsko komunikacijskih sustava. Poslije toga navedena je usporedba sigurnosti u ta dva sustava, te stanje kibernetičke sigurnosti u Republici Hrvatskoj. Sama tema sigurnosti u OT i IT sustavima je dosta opširna, pri istraživanju teme kroz navedenu literaturu stekao sam osnovni uvid u samu problematiku, te se bolje upoznao sa mogućim prijetnjama i posljedicama kibernetičkih napada na takve sustave.

Godinama su se industrijski sustavi oslanjali na zaštićene protokole i softver, ljudi su ručno njima upravljali i nadzirali ih te nisu imali veze s vanjskim svijetom. Iz tog su razloga bili prilično beznačajna meta za napadače, jer nije bilo umreženog sučelja za napad. OT i IT bili su slabo povezani i nisu se bavili istim vrstama ranjivosti. Promatrajući razvoj tehnologija, vjerojatno će razlike između OT i IT nestajati sve dok se potencijalno ova dva sustava ne spoje u jedan zajednički. U međuvremenu je neophodno da obje strane uzmu u obzir stručnost i gledište druge strane i zajednički rade na konačnom cilju – sigurnosti i produktivnosti.

LITERATURA

[1] J.Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, New York, 2010.

[2] A. Bolanča, D. Pavlović, S. Šijanović-Pavlović, Razvoj sustava kibernetičke sigurnosti i nacionalne taksonomije u svrhu zaštite operatora ključnih usluga energetskog sektora, Nafta i Plin, No. 155., Vol. 38., str. 23-38, 2018.

[3] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST- National Institute of Standards and Technology, Gaithersburg, Svibanj 2014.

[4] Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, Zagreb, 7. listopada 2015. (NN108/2015)

[5] Stavovi o kibernetičkoj sigurnosti u Hrvatskoj u usporedbi s ostalim članicama EU, 25. listopada 2018., dostupno na : https://www.cert.hr/NCEUrep [08.07.2020. 16:29]

[6] G. Knezović, 59% korisnika Interneta smatra da nisu dovoljno zaštićeni, Mreža za IT profesionalce, 29. siječnja 2020., dostupno na: https://mreza.bug.hr/59-korisnika-interneta-smatra-da-nisu-dovoljno-zasticeni/ [16.09.2020. 08:42]

[7] Vlada Republike Hrvatske, Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, 26. srpnja 2018. (NN 68/18), dostupno na: https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Uredba%20o%20kiberneti%C4%8Dkoj%20sigurnost%20operatora%20klju%C4%8Dnih%20usluga.pdf

[8] S. Morgan, Cybercrime magazine, 10 Hot Cybersecurity Certifications For IT Professionals To Pursue In 2020, 18. kolovoza 2020., dostupno na: https://cybersecurityventures.com/10-hot-cybersecurity-certifications-for-it-professionals-to-pursue-in-2019/

SAŽETAK

Problematika kibernetičke sigurnosti industrijskih upravljačkih sustava (ICS ili OT-Operativna tehnologija) je različita od informatičke (ICT ili IT-Informacijska i komunikacijska tehnologija) kibernetičke sigurnosti zbog različitih prioriteta (povjerljivost podataka, integritet, autentičnost i očuvanje privatnosti). Različite vrste prijetnji i napada na sustave kao i metode obrane od zlonamjernih napadača. Ta dva svijeta i podrazumijevaju potpuno različit profil stručnjaka.

Budući da ICS prihvaća informatička rješenja za povezivanjem i mogućnosti udaljenog pristupa, a dizajnira se i implementira pomoću standardnih računala, u konačnici ICS i ICT imaju i svoje međusobne veze. U ovim sustavima stručnjaci nakon obavljanja aktivnosti na procjeni, smanjenju rizika u održavanju sustava kibernetičke sigurnosti, objedinjuju rezultate svoga rada u jednu cjelinu u svrhu učinkovite zaštite tvrtke od potencijalne ugroze iz kibernetičkog svijeta, te sposobnosti brzog i sigurnog oporavka sustava u slučaju incidenta.

Ključne riječi: kibernetička sigurnost, industrijski upravljački sustav (ICS), operativna tehnologija (OT), informacijska i komunikacijska tehnologija (ICT/IT), sustav, razlika, prijetnje, napadi, obrana.

ABSTRACT

Cyber security of Operational Technology (OT) and Information Technology (IT)

The issue of cyber security of Industrial Control Systems (ICS or OT-Operating Technology) is different from information (ICT or IT-Information and Communication Technology) cyber security due to different priorities (data confidentiality, integrity, authenticity and privacy). Different types of threats and attacks on systems as well as methods of defense against malicious attackers. These two worlds imply a completely different profile of experts.

Because ICS accepts IT connectivity solutions and remote access capabilities, and is designed and implemented using standard computers, ultimately ICS and ICT have their interconnections as well. In these systems, experts, after performing assessment activities, reducing the risk of maintaining a cyber security system, combine the results of their work into one whole in order to effectively protect the company from potential threats from the cyber world, and the ability to quickly and safely recover from incidents.

Keywords: cyber security, Industrial Control System (ICS), Operational Technology (OT), Information and Communication Technology (ICT/IT), system, difference, threats, attacks, defense.

ŽIVOTOPIS

Danijel Tintor, rođen 07. srpnja 1997. u Vukovaru. Završio Srednju Tehničku školu Nikola Tesla u Vukovaru u razdoblju od 2011.- 2015. godine. Upisuje se 2017. godine na Preddiplomski stručni studij Elektrotehnike, smjer Automatika na FERIT-u u Osijeku. Stručnu praksu obavljao je u Danieli Systec-u 2020. godine u Osijeku.