Cyber security-zaštita kritičnih infrastruktura

Mataić, Ira

Sveučilište Sjever

Završni rad br. 334/PIM/2022

CYBER SECURITY – ZAŠTITA KRITIČNIH INFRASTRUKTURA

Ira Mataić, 0336041639

Koprivnica, rujan 2022. godine

Sveučilište Sjever

Odjel za Poslovanje i menadžment

Završni rad br. 334/PIM/2022

CYBER SECURITY – ZAŠTITA KRITIČNIH INFRASTRUKTURA

Studentica:

Ira Mataić, 0336041639

Mentor:

doc. dr. sc. Ernest Vlačić

Koprivnica, rujan 2022. godine

Sveučilište Sjever
Sveučilišni centar Koprivnica
Trg dr. Žarka Dolinara 1, HR–48000 Koprivnica

UNIVERSITY NORTH

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL Odjel za ekonomiju

STUDIJ preddiplomski stručni studij Poslovanje i menadžment

PRISTUPNIK Ira Matić | MATIČNI BROJ 5838/336

DATUM 20.9.2022 | KOLEGIJ Menadžment inovacija

NASLOV RADA CYBER SECURITY – ZAŠTITA KRITIČNIH INFRASTRUKTURA

NASLOV RADA NA ENGL. JEZIKU CYBER SECURITY - CRITICAL INFRASTRUCTURE PROTECTION

MENTOR dr. sc. Ernest Vlačić | ZVANJE doc.

ČLANOVI POVJERENSTVA

1. doc. dr. sc. Mirko Smoljić, predsjednik
2. doc. dr. sc. Joško Lozić, član
3. doc. dr. sc. Ernest Vlačić, mentor
4. Jospi Vuković, pred., zamj. član
5.

Zadatak završnog rada

BROJ 334/PIM/2022

OPIS

U okviru ovog završnog rada zadatak je u okviru teme razraditi slijedeće:

- definirati kibernetičke napade
- dati jasnu sliku o osnovnim metodama prevencije za zaštitu od kibernetičkih napada
- objasniti koje su ranjivosti i prijetnje s kojima se susreću moderne kritične infrastrukture te njihova zaštita
- zaključno se osvrnuti na SCADA sustave te koja je njihova uloga u kritičnim infrasturkturama

ZADATAK URUČEN 21.9.2022 | POTPIS MENTORA

SVEUČILIŠTE SJEVER

VŽ KC

MMI

SAŽETAK

Posljednjih godina pojam "kibernetička sigurnost" postao je široko korišten pojam. Međutim, kao i kod mnogih žargona, čini se da postoji vrlo malo razumijevanja što taj pojam zapravo podrazumijeva. Iako to možda nije problem kada se pojam koristi u neformalnom kontekstu, potencijalno može uzrokovati značajne probleme u kontekstu organizacijske strategije, poslovnih ciljeva ili međunarodnih sporazuma. Područje kibernetičke sigurnosti postaje sve važnije zbog sve veće ovisnosti o računalnim sustavima, uključujući pametne telefone, televizore i razne uređaje koji čine Internet of Things. Kritične infrastrukture igraju vitalnu ulogu u pružanju potpore modernog društva. Pouzdanost, izvedba, kontinuirani rad, sigurnost, održavanje i zaštita kritičnih infrastruktura nacionalni su prioriteti za zemlje diljem svijeta. Europska unija poduzela je prvi konkretan korak u obrani od kibernetičkih prijetnji 2016. godine s „Direktivom o sigurnosti mrežnih i informacijskih sustava“ (NIS direktiva) propisivanjem državama članicama da usvoje strože standarde kibernetičke sigurnosti. Pretpostavlja se da će u budućnosti glavna meta napada biti kritična infrastruktura te je vrlo važno razumjeti i ulagati u zaštitu kritične infrastrukture.

Cilj ovog završnog rada je pokušati dati jasnu sliku o kibernetičkim napadima i osnovnim metodama prevencije koje će pomoći unutarnjim revizorima da procijene ima li organizacija odgovarajuću zaštitu od napada. Također, ovaj rad istražuje ranjivosti i prijetnje s kojima se susreću moderne kritične infrastrukture te njihova zaštita. Za ljude razumijevanje kibernetičkog kriminala pomaže da ne postanu žrtve određenih zločina, poput krađe identiteta.

Ključne riječi: kibernetička sigurnost, kritična infrastruktura, kibernetička prijetnja, zaštita kritične infrastrukture, SCADA sustavi

ABSTRACT

In recent years, the term “cyber security” has become a widely used term. However, when there’s many jargons, there’s very little understanding as to what that term exactly means. While this may not be a problem when the term is used in an informal context, it can potentially cause significant problems in the context of organizational strategy, business objectives or international agreements. The field of Cyber security is becoming really important due to the increasing dependence on computer systems, including televisions, smartphones and various devices that make up the Internet of Things. Critical infrastructures play a vital role in supporting modern society. Reliability, overall performance, continuous work, security,

preservation protection of critical infrastructures are national prime concern for all countries around the world. The European Union took the first step in defense against cyber threats in 2016. with "Directive on the Security of Network and Information Systems" (NIS Directive) by requiring member states to adopt much stricter cyber security standards. It is estimated the main target of attacks will be critical infrastructure, and it is very important to understand and invest in the protection of them.

The goal of this final paper is to try to give a clear picture of cyber attacks and basic prevention methods that could help internal auditors to estimate whether their organization has adequate protection against cyber attacks. Also, this work investigates vulnerabilities and threats faced by modern critical infrastructures and their protection. Understanding cybercrime helps people avoid becoming future victims of certain cybercrimes, such as identity theft and many other cybercrimes.

Keywords: cyber security, critical infrastructure, cyber threat, protection of critical infrastructure, SCADA system

POPIS KORIŠTENIH KRATICA

Apple DOS	Apple Disk Operating Systems
APT	Advanced Package Tool
ARPANET	Advanced Research Projects Agency Network
BCaaS	Blockchain-as-a-Service
C&C	Command and Control
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CRYPTaaS	Cryptography-as-a-Service
DCS	Distributed Control System
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DOJ	Department of Justice
EPES	Electrical Power Energy Systems
FMaaS	Flow Modeling As A Service
HMI	Human-Machine Interface
HSM	Hardware Security Module
HVAC	Heating, ventilation, and air conditioning
I/O	input/output
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IED	Improvised Explosive Devise
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centers
MitM	Man in the Middle
NGN	Next-Generation Network
NIPP	National Infrastructure Protection Plan
NIS direktiva	Network And Information Systems directive

NIST	National Institute of Standards and Technology
OSTP	The Office of Science and Technology Policy
OT	Operational Technologies
PLC	Programmable Logic Controller
PNNL	Pacific Northwest National Laboratory
PSTN	A public switched telephone network
RAS	Remote Access Service
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition
SQL	Structured Query Language
WMD	Weapons of Mass Destruction

SADRŽAJ

UVOD

U današnjem automatiziranom svijetu posebnu pozornost treba posvetiti kibernetičkoj sigurnosti podataka i mrežnih aktivnosti. Prošli su dani kada je mrežna sigurnost bila povezana isključivo s velikim tvrtkama i institucijama. Trenutno, svatko može biti moguća žrtva kibernetičkog napada, bez obzira na status i novce na bankovnom računu. Kako je sigurnost rasla, hakerski svijet je rastao brže. Sve zemlje u razvoju i razvijenog svijeta usvojila su i provela rješenja digitalne kritične infrastrukture. U skladu s Direktivom EU-a (2008/114/EC) ključna infrastruktura je alat ili sustav koji se nalazi u svakoj državi i konačan je za održavanje važnih funkcija, zdravstvenih, sigurnosnih, financijskih ili socijalnih kriterija pojedinaca, a prestanak njegovog učinkovitog djelovanja ili njegovo uništenje može imati značajan utjecaj na države.

Tijekom godina potreba za zaštitom kritične infrastrukture postaje sve hitnija. Kritična infrastruktura mora biti dobro zaštićena od napada i mora kontinuirano poboljšavati metode detekcije i eliminacije. Suvremeni sustavi za kontrolu i prikupljanje podataka (SCADA) potrebni su za praćenje i upravljanje proizvodnjom, prijenosom i distribucijom električne energije. U doba IoT-a, SCADA je prerastao u velike, složene i distribuirane sustave koji su podložni uobičajenim i novim prijetnjama.

Industrijski sustav upravljanja (ICS) glavni je pojam koji se odnosi na skupinu tehnologija automatizacije procesa, kao što su sustavi za kontrolu i prikupljanje podataka (SCADA) i distribuirani sustavi upravljanja (DCS), koji su nažalost posljednjih godina izloženi sve većem broju napada. Budući da pružaju vitalne usluge kritičnoj infrastrukturi kao što su komunikacija, proizvodnja i energija, napadači predstavljaju ozbiljnu prijetnju svakodnevnom radu država. Društva sve više ovise o javnim ICT mrežama i njihovim uslugama. Stabilnost, sigurnost i otpornost kibernetičkog prostora pitanje je nacionalne sigurnosti jer se ranjivosti može iskoristiti za uništavanje kritičnih infrastruktura države, koja se oslanja na ICT mreže i usluge. Napadi na kritične infrastrukture uglavnom utječu na sektore financijskih, informacijskih i komunikacijskih tehnologija i energetike.

U radu je korištena znanstvena metoda. Tema se proučavala na temelju postojeće znanstvene literature o temi rada. Jedna od metoda koja je korištena je metoda indukcije. Tu je tema razmotrena od pojedinačnog do općenitog. Na temelju analize pojedinačnih činjenica došlo se do zaključka i zapažanja konkretnih slučajeva te se dolazi do općeg zaključka. Također je korištena metoda dedukcije; od općeg prema pojedinačnom da bi se što bolje tema shvatila. Još

jedna od metoda koja je korištena je komparativna metoda. Tu su se uspoređivali odnosi, sličnosti i razlike između više država i način njihove zaštite kritične infrastrukture da bi se izveli određeni zaključci. Korištena je i metoda analize gdje se znanstveno istraživalo i gdje su se raščlanili složeni pojmovi i sudovi na jednostavnije elemente. Završni rad je pisan objektivno te su korišteni pouzdani izvori.

Hipotezu koji ovaj rad donosi je koliko je važan SCADA sustav za kritične infrastrukture. Kroz istraživanja i proučavanja dati će se jasna slika o tome te će se objasniti zašto je SCADA sustav bitan kod kritične infrastrukture.

Cilj završnog rada je pokušati dati jasnu sliku o kibernetičkim napadima i metodama prevencije. Također, ovaj rad istražuje ranjivosti i prijetnje s kojima se susreću kritične infrastrukture te njihova zaštita. Dati će se slika o tome koje su to sve kritične infrastrukture, koje opasnosti ih okružuju te kako se zaštiti od njih.

Ovaj završni rad je podijeljen na sedam dijelova koji su međusobno povezani. U uvodnom djelu su objašnjeni ciljevi te korištene znanstvene metode, a također se postepeno ulazi u temu samoga rada. Prvi dio govori o povijesti u računalnoj industriji te koje su najstarije i najčešće prijetnje računalne industrije. Drugi dio govori o kibernetičkoj sigurnosti, zašto nam je potrebna kibernetička sigurnost te koje su njene vrste; također dotičemo se i kibernetičke sigurnosti u sadašnjem vremenu i koje su sve nove prijetnje te kako se možemo zaštititi. U trećem poglavlju govorimo o kritičnoj infrastrukuturi. Tu će se dotaknuti pitanje tko je odgovoran za kritičnu infrastrukturu, međuovisnost kritičnih infrastruktura i koliko je ona važna, koje su prijetnje i opasnosti. Također će se spomenuti i podrška za kritičnu infrastrukturu te će se nabrojati i objasniti koji su to sve sektori kritične infrastrukture. U četvrtom poglavlju govorimo o zaštiti kritične infrastrukture. Tu će se spomenuti zašto nam je potrebna zaštita, strateška zaštita i nekoliko programa za zaštitu te inovacije i rješenja. U petom poglavlju se spominje SCADA sustavi te se kroz ovo poglavlje i obrazlaže hipoteza. Na kraju rada je iznesen zaključak te se ukratko opisuje sve što je u radu bitno i daje se još jednom obrazloženje hipoteze. U zaključku su također iznesene glavne spoznaje i stavovi.

1. POVIJEST U RAČUNALNOJ INDUSTRIJI I CYBER SECURITY

1.1. Tamna strana računala

Računalni virus je računalni kod koji je osmišljen tako da se ubaci u drugi softver i, kada je izvršen, može se replicirati i propagirati pomoću softvera ili datoteke domaćina. Virusi se mogu dizajnirati tako da oštećuju zaraženog domaćina krađom prostora na tvrdom disku, zapisivanjem pritisaka tipki za krađu lozinki, stvaranjem neugodnih poruka i drugih aktivnosti koje se obavljaju bez odobrenja ili znanja korisnika računala. Rani virusi bili su virusi u pogonskom sektoru i širili su se od strane korisnika računala koji su dijelili zaražene diskove. Drugi virusi vezani su uz e-poštu; to je bila poruka s ugrađenim virusima poslana korisnicima. Neki virusi dizajnirani su za pričvršćivanje na datoteke kao što su dokumenti Word-a ili proračunske tablice. To je osnovni kod koji se može izvršiti kada se datoteka učitava, a kada se virus spoji na dokument, kod u virusu će se pokrenuti svaki put kada se dokument pokrene. Eugene H. Spafford napominje da je prvu upotrebu termina Virus koji se odnosi na neželjene računalne kodove ponudio Gregory Benford, istraživački fizičar u Lawrence Livermore Radiation Laboratory, koji je primijetio da se „loš kod" može reproducirati među laboratorijskim računalima i ući u ARPANET. Fred Cohen je 1983. formalno definirao termin računalni virus, i stvorio je primjer koda za samo-reprodukciju i nazvao ga računalnim virusom kako bi opisao program koji se stvara tako da utječe na druge računalne programe modificirajući ih tako da u program uključi vlastitu kopiju.

Razvoj računalnih virusa kroz godine:

- 1981. - Elk Cloner virus - napisan za Apple DOS 3.3 i širio se diskovima; prikazivao je kratku pjesmu i aktivirao se na svojoj 50. upotrebi. Elk Cloner virus je bio prvi PC virus;
- 1986. - The Brain virus - prvi svjetski virus koji se također proširio diskovima, dva brata u Pakistanu koja su napisali virus nisu namjeravala da to bude destruktivan virus, ali unatoč njihovim namjerama, pretvorio se u jedan;
- 1999. - Melissa virus - baziran je na Microsoft Word Macro i osmišljen je za zarazu poruka e-pošte slanjem zaraženih dokumenata na prvih 50 osoba na korisnikovoj listi. Virus Melissa prouzročio je više od 50 milijuna dolara štete drugim korisnicima računala i tvrtkama;
- 2000. - I Love You virus - zarazio je milijune računala u jednom danu samo zato što je u privitku pisalo „Volim te", a radoznalost ljudi navela ih je da otvore zaraženi privitak

koji se je kopirao u različite datoteke na hard disku korisnika i također koristio za krađu lozinki od žrtve;

- 2001. - Code Red virus - bio je usmjeren za napad na Bijelu kuću SAD-a kao distribuirani napad uskraćivanja usluga, ali je zaustavljen prije nego što je uspio napasti. Međutim, virus je zarazio tisuće drugih računala i prouzročio štetu od preko 1 milijarde dolara. Druga verzija, Code Red II, napala je sustave Windows 2000 i Windows NT;
- 2002. - Nimda virus - bio je jedan od najbržih virusa koji se širio internetom, a meta su mu bili internet serveri te je prouzročio znatnu štetu brojnim korisnicima;
- 2003. - Slammer virus - bio je virus web poslužitelja koji je također putovao internetom nevjerojatnom brzinom. Mnoge korporacije u financijskom i zračnom sektoru pretrpjele su značajne gubitke procijenjene u rasponu od nekoliko milijardi dolara.

Računalni crvi ne mijenjaju druge programe, već je on računalni program koji se može replicirati s računala na računalo i prijeći na mrežne veze. Važno je naglasiti da, iako crvi ne mijenjaju druge programe, mogu nositi druge šifre koje mijenjaju programe. Trojanski konj je program koji se maskira kao legitimna aplikacija, a istovremeno obavlja tajnu funkciju. Kod Trojanskog konja programi se ne šire sami, pa se oslanjaju na korisnike da prihvate programe iz nepouzdanih izvora.

Prethodno spomenuti virusi u pogonskom sektoru, virusi datoteka i makro virusi bili su neke od najranijih meta za dizajnere virusa. Međutim, kako prelazimo na suvremene prijetnje, trebali bismo također uključiti multipartitne viruse, stealth viruse i polimorfne viruse. Multipartitni virusi su hibrid koji može zaraziti datoteke u sektoru za pokretanje kao i programske datoteke. Nakon što je pogonski sektor zaražen i kada se sustav digne, multipartitni virusi se učitavaju u memoriju i započinju proces zaraze drugih datoteka. Kao rezultat njihovog kretanja, takve viruse je teško ukloniti. Stealth viruse je još teže identificirati i ukloniti jer su dizajnirani da koriste posebne metode da se sakriju od otkrivanja. Njihova metoda se može opisati na idući način: ponekad se privremeno uklanjaju iz memorije kako bi izbjegli otkrivanje i sakrili se od skenera virusa. Neki također mogu preusmjeriti disk da čita drugi sektor umjesto sektora u kojem se nalaze. Polimorfne viruse najteže je identificirati jer su dizajnirani da mutiraju ili mijenjaju virusni kod poznat kao potpis svaki put kada se šire ili zaraze datoteke. Budući da se antivirusni softver stvara na temelju potpisa virusa, postaje gotovo nemoguće zaštititi se od polimorfnog virusa osim ako dobavljač antivirusnog softvera nije osigurao novu "zakrpu" za zaštitu od njega.

1.2. Botnet

Botnet nije nužno zlonamjeran jer postoje legitimne svrhe i upotrebe za automatizirane programe koji izvršavaju zadatke bez intervencije korisnika. Međutim, botnetovi su nedavno postali poznati po tome što su postali značajna prijetnja internetu zbog sve veće zlonamjerne upotrebe od strane kibernetičkih kriminalaca. Botnet je mreža računala kojima kibernetički kriminalac ili napadač može na daljinu koordinirati kako bi se postigla namjeravana i zlonamjerna svrha. Zlonamjerni cilj može varirati od pokretanja distribuiranog napada uskraćivanja usluge, neželjene pošte, napada prijevarom klika ili jednostavnog iznajmljivanja usluge napada pojedincima koji možda žele da neka druga osoba ili entitet budu napadnuti. Dakle, botnet je mreža računala koja su već pod kontrolom pojedinca koji funkcioniraju kao središnji entitet za kontrolu i komunikaciju sa svakim strojem.

Zlonamjerni agent koji omogućuje da računalo daljinski kontrolira Bot Master naziva se Bot Agent. Glavna funkcija Bot Agenta je komunikacijska veza s botnet mrežom. To dopušta Bot Agentu da prima i tumači naredbe od Bot Mastera i šalje podatke natrag Bot Masteru ili da izvršava napade. Command and Control kanal ključan je online resurs Bot Mastera koji dopušta kontrolu nad botovima. Bez C&C kanala, Bot Master ne može usmjeravati zlonamjernu aktivnost bota. Budući da snaga bota leži u broju kompromitiranih računala pod kontrolom Bot Mastera, može se shvatiti koliko je važna računalna sigurnost, tako da oni koji djeluju kao Bot Masters ne mogu dodati još kompromitiranih strojeva u svoju kolekciju. Primjeri zlonamjerne upotrebe botneta nalaze se u distribuiranim napadima uskraćivanja usluge gdje su svi strojevi usmjereni da napadnu unaprijed određenu žrtvu, korporaciju ili vladin entitet u određeno vrijeme i na određeni datum. Rezultat tako masivnog napada na simultani način stvorit će problem prekoračenja za poslužitelje ciljane stranice i onesposobiti njihovu stranicu i uslugu. Ova vrsta napada također se može koristiti za slanje velike količine neželjene pošte na označenu metu.

Prijevara klikom još je jedan primjer kako Bot Master može usmjeriti svoje botove na određene web stranice u svrhu prikupljanja prihoda od oglašivača koji plaćaju da potencijalni korisnici kliknu na njihovu web stranicu. Budući da mrežni oglašivači plaćaju za svaki klik na oglase koje imaju na web mjestima, ovo pruža priliku kibernetičkom kriminalcu da zaradi na tome. Slijedi primjer kako se izvodi prijevara klikom. Prvo, napadač postavlja web stranicu koja sadrži samo oglase. Napadač se zatim prijavljuje na jedan ili više programa za oglašavanje kao što su Google, Ad Sense ili Yahoo. Nakon što se sklope dogovori između oglasnih podružnica

i napadača, Bot Master daje upute botnet mrežama pod njegovom kontrolom da kliknu oglase na njegovoj web stranici s oglasima. Ova će akcija potaknuti plaćanje od strane online oglašivača. Druga varijanta ove iste teme je kada vlasnik web stranice koja ima legitiman softver na svojoj web stranici kontaktira Bot Mastera i zatraži od Bot Mastera da uputi botove da preuzmu reklamirani softverski proizvod. Budući da će softverska tvrtka platiti vlasniku web stranice za svaku preuzetu instalaciju njihovog proizvoda, to može rezultirati velikim profitom za vlasnika web stranice, posebno ako Bot Master ima tisuće računala pod svojom kontrolom. Bot Master također može uputiti botove da koriste zlonamjerni softver za napad na entitet koji bi mogao zatražiti drugi pojedinac koji se želi osvetiti. Bot Master koji služi kao davatelj usluga može iznajmiti svoje usluge zainteresiranim korisnicima, a takve stranice postoje na internetu, "Deep Webu" i "Silk Roadu". Druge kibernetičke ofenzivne operacije mogu uključivati kibernetičku špijunažu i napade na kritičnu infrastrukturu nacije.

2. CYBER SECURITY

Cyber security je praksa obrane podataka, mreža, mobilnih uređaja, računala, poslužitelja i elektroničkih sustava od zlonamjernih napada. Također je poznata kao sigurnost informacijske tehnologije ili elektronička informacijska sigurnost. Pojam se primjenjuje u različitim kontekstima, od poslovanja do mobilnog računalstva, i može se podijeliti u nekoliko uobičajenih kategorija:

- Mrežna sigurnost - praksa osiguravanja računalne mreže od uljeza, bilo da su ciljani napadači ili oportunistički malware-i;
- Sigurnost aplikacija - usmjerena na zaštitu softvera i uređaja od prijetnji;
- Informacijska sigurnost - štiti privatnost podataka i integritet, kako u pohrani tako i u prijenosu;
- Operativna sigurnost - uključuje procese zaštite podataka i odluke za rukovanje. Uključuje dopuštenja koja korisnici imaju kada pristupaju mreži i postupci koji određuju kako i gdje se podaci mogu pohraniti ili dijeliti;
- Oporavak od katastrofe - definiraju kako organizacija reagira na kibernetičku sigurnost ili bilo koji drugi događaj koji uzrokuje gubitak podataka. Politike oporavka od katastrofe diktiraju kako organizacija obnavlja svoje informacije kako bi se vratila na isti radni kapacitet kao prije događaja;
- Edukacija krajnjih korisnika - bavi se najnepredvidljivijim faktorom kibernetičke sigurnosti: ljudima. Svatko može slučajno unijeti virus u inače siguran sustav ako ne slijedi dobre sigurnosne prakse. Podučavanje korisnika da izbrišu sumnjive privitke e-pošte, da ne priključuju neidentificirane USB stikove i razne druge važne lekcije od ključne su važnosti za sigurnost svake organizacije.

Globalna kibernetička prijetnja nastavlja se razvijati velikom brzinom, sa sve većim brojem povreda podataka svake godine. Izvješće RiskBased Security-a otkrilo je da je 7,9 milijardi zapisa bilo izloženo povredama podataka u prvih devet mjeseci 2019. godine. Ova brojka je više nego dvostruko veća (112%) od broja izloženih zapisa u istom razdoblju 2018. godine. Medicinske usluge, trgovci na malo i javni subjekti doživjeli su najviše napada. Neki od tih sektora privlačniji su kibernetičkim kriminalcima jer prikupljaju financijske i medicinske podatke, ali sve tvrtke koje koriste mreže mogu biti meta podataka o klijentima, korporativne špijunaže ili napada na klijente.

Kibernetička sigurnost je važna jer uz sve veći broj korisnika, uređaja i programa, u kombinaciji s povećanom količinom podataka, od kojih je većina osjetljiva ili povjerljiva, važnost kibernetičke sigurnosti nastavlja rasti. Sve veći obujam i sofisticiranost kibernetičkih napadača i tehnika napada dodatno kompliciraju problem. Održavanje kibernetičke sigurnosti u „moru" prijetnji koji se stalno razvija izazov je za sve organizacije. Tradicionalni reaktivni pristupi, u kojima su resursi usmjereni na zaštitu sustava od najvećih poznatih prijetnji, više nije dovoljna taktika. Kako bismo išli u korak s promjenjivim sigurnosnim rizicima, potreban je prilagodljiviji pristup. Nekoliko ključnih savjetodavnih organizacija za kibernetičku sigurnost nudi smjernice. Na primjer, Nacionalni institut za standarde i tehnologiju (NIST) preporučuje usvajanje kontinuiranog praćenja i procjena u stvarnom vremenu kao dio procjene rizika za obranu od poznatih i nepoznatih prijetnji. Prednosti kibernetičke sigurnosti su: zaštita poslovanja od kibernetičkih napada i povreda podataka, zaštita podataka i mreža, sprječavanje neovlaštenog pristupa korisnika, poboljšano vrijeme oporavka nakon napada, zaštita za krajnje korisnike i uređaje, kontinuitet poslovanja, poboljšano povjerenje u ugled tvrtke i povjerenje programera, partnera, kupaca, dionika i zaposlenika.

Neki od glavnih izazova kibernetičke sigurnosti je taj što ju neprestano ugrožavaju hakeri, gubitak podataka, privatnost, upravljanje rizicima i promjena strategija kibernetičke sigurnosti. Ne previđa se da će broj kibernetičkih napada biti manji u bliskoj budućnosti. Štoviše, povećane ulazne točke za napade, kao što je dolazak Internet of Things-a, povećavaju potrebu za sigurnošću mreža i uređaja. Kako se pojavljuju nove tehnologije i kako se tehnologija koristi na nove ili drugačije načine, razvijaju se novi načini napada. Pratiti te česte promjene i napredak u napadima, kao i ažurirati prakse za zaštitu od njih, može biti izazov. Problemi uključuju osiguravanje stalnog ažuriranja svih elemenata kibernetičke sigurnosti radi zaštite od potencijalnih ranjivosti. Osim toga, organizacije mogu prikupiti mnogo potencijalnih podataka o pojedincima koji koriste jednu ili više njihovih usluga. Uz sve više podataka koji se prikupljaju, vjerojatnost da kibernetički kriminalac želi ukrasti podatke koji otkrivaju identitet je još jedna briga. Na primjer, organizacija koja pohranjuje podatke koji otkrivaju identitet u oblaku može biti izložena napadu ransomwarea. Organizacije bi trebale učiniti sve što mogu kako bi spriječile proboj oblaka. Još jedan izazov za kibernetičku sigurnost uključuje nedostatak kvalificiranog osoblja za kibernetičku sigurnost. Kako raste količina podataka koje tvrtke prikupljaju i koriste, raste i potreba za osobljem zaduženim za kibernetičku sigurnost koje analizira, upravlja i reagira na incidente.

2.1. Važnost Cyber security

Opseg djelovanja kibernetičke sigurnosti uključuje zaštitu informacija i sustava od velikih kibernetičkih prijetnji. Te prijetnje imaju mnoge oblike. Kao rezultat toga, držanje koraka sa strategijom kibernetičke sigurnosti može biti izazov, osobito u vladinim i poduzetničkim mrežama gdje, u svom najinovativnijem obliku, kibernetičke prijetnje često ciljaju na tajnu, političku i vojnu imovinu nacije ili njezinog stanovništva. Neke od uobičajenih prijetnji su:

- Cyber terorizam - inovativna upotreba informacijske tehnologije od strane terorističkih skupina kako bi unaprijedile svoj politički cilj. Ima oblik napada na mreže, računalne sustave i telekomunikacijske infrastrukture.
- Cyber ratovanje - uključuje nacionalne države koje koriste informacijsku tehnologiju da prođu kroz mreže druge nacije kako bi nanijele štetu. Napade prvenstveno izvode hakeri koji su dobro uvježbani u korištenju računalnih mreža.
- Cyber špijunaža - praksa korištenja informacijske tehnologije za dobivanje tajnih podataka bez dopuštenja njihovih vlasnika ili posjednika. Najčešće se koristi za postizanje strateške, ekonomske i vojne prednosti.

2.1.1. Cyber kriminalci

Uključuje aktivnosti kao što su prijevara s kreditnom karticom, uhođenje, klevetanje na internetu, dobivanje neovlaštenog pristupa računalnim sustavima, ignoriranje autorskih prava, licenciranja softvera, nadjačavanje enkripcije za izradu ilegalnih kopija, softversko piratstvo i krađu tuđeg identiteta radi izvršenja kriminalnih radnji. Sve to provode kibernetički kriminalci. Mogu se kategorizirati u tri skupine koje odražavaju njihovu motivaciju.

- Tip 1: kibernetički kriminalci – željni priznanja:
  - hakeri iz hobija;
  - IT stručnjacima (socijalni inženjering je jedna od najvećih prijetnji);
  - politički motivirani hakeri;
  - terorističke organizacije.
- Tip 2: kibernetički kriminalci – ne zanimaju ih priznanje:
  - psihološke prevencije;
  - financijski motivirani hakeri (korporativna špijunaža);
  - državno - sponzorirano hakiranje (nacionalna špijunaža, sabotaža);
  - organizirani kriminalci.
- Tip 3: kibernetički kriminalci – insajderi:

- bivši zaposlenici traže osvetu;
- konkurentska poduzeća koriste zaposlenike za stjecanje ekonomske prednosti kroz štetu i/ili krađu.

2.2. Vrste prijetnji

Prijetnje kojima se kibernetička sigurnost suprotstavlja su trostruke. To su kibernetički kriminal, napad i terorizam. Kibernetički kriminal uključuje pojedinačne aktere ili grupe koji ciljaju sustave radi izazivanja poremećaja ili financijske dobiti. Kibernetički napadi uključuje politički motivirano pribavljanje informacija, dok kibernetički terorizam ima cilj potkopavanje elektroničkih sustava kako bi se izazvala panika ili strah.

Proces praćenja novih tehnologija, sigurnosnih trendova i obavještajnih podataka o prijetnjama izazovan je zadatak. Kontrolu nad računalnim sustavima se stječu kroz neke od uobičajenih metoda koje se koriste za ugrožavanje kibernetičke sigurnosti:

- Malware

Malware je oblik zlonamjernog softvera u kojem se bilo koja datoteka ili program može koristiti za nanošenje štete korisniku računala. Jedna od najčešćih kibernetičkih prijetnji je zlonamjerni softver. To je softver koji je haker napravio da ometa ili ošteti računalo nekog korisnika. Često se širi neželjenim privitkom e-pošte ili preuzimanjem koje izgleda legitimno. Kibernetički kriminalci mogu koristiti zlonamjerni softver za zarađivanje novca ili politički motivirane napade. Postoji niz različitih vrsta zlonamjernog softvera:

- Virus - samoumnožavajući program koji se pričvršćuje na datoteku i proširuje se računalnim sustavom te tako zarazi datoteke;
- Trojanci - zlonamjerni softver prerušen u legitimni softver;
- Spyware - program koji tajno zapisuje što radi korisnik, tako da hakeri mogu te informacije iskoristit;
- Ransomware - zlonamjerni softver koji zaključava korisničke podatke i datoteke, uz prijetnju da će ih izbrisati osim ako se ne plati;
- Adware - softver za oglašavanje koji širi zlonamjerni softver;
- Botneti - mreže računala zaraženih zlonamjernim softverom koje kibernetički kriminalci upotrebljavaju za obavljanje zadataka na mreži bez dopuštenja korisnika.

- SQL

Ubacivanje SQL (Structured Query Language) vrsta je napada koji se upotrebljava za krađu podataka iz baze podataka te preuzimanje kontrole. To im daje pristup osjetljivim informacijama sadržanim u bazi podataka.

- Krađa identiteta (phishing)

Phishing je kada se ciljaju žrtve e-poštom koja izgleda kao da je od legitimne tvrtke i traži osjetljive informacije. Phishing napadi često se koriste za navođenje ljudi na predaju podataka o kreditnoj kartici i drugih osobnih podataka.

- Man in the middle (MitM)

Man in the middle vrsta je prijetnje u kojoj se presreće komunikaciju između dvije osobe kako bi se ukrali podatci. Na primjer, na nesigurnoj WiFi mreži, napadač bi mogao presresti podatke koji se prenose sa žrtvinog uređaja i mreže.

- Distributed denial of service (DDoS)

Napad uskraćivanjem usluge je slučaj kada napadači sprječavaju računalni sustav da ispuni legitimne zahtjeve preplavljujući mreže i poslužitelje prometom. To čini sustav neupotrebljivim, sprječavajući organizaciju u obavljanju vitalnih funkcija.

- Advanced package tool (APT)

APT su dugotrajni ciljani napadi u kojima se napadač infiltrira u mrežu i ostaje neotkriven dulje vrijeme s ciljem krađe podataka.

2.3. Novo polje Cyber security-a

Od samog početka računala nije se razmišljalo o potrebi stvaranja računalnih sigurnosnih programa za njega. Na kraju krajeva, razvoj ovog područja odvijali su znanstvenici, inženjeri, fizičari i matematičari. Njihov je rad osmišljen kako bi se na nove načine stvorilo i poboljšalo povjerenje istraživačkih i znanstvenih zajednica. Nikada im nije palo na pamet da će jednog dana ljudi biti skloni zlorabiti njihova otkrića ili ih čak koristiti u nemoralne, nezakonite ili kriminalne svrhe. Međutim, nakon kasnih 1980-ih, nekima je postalo jasno da će računala morati imati sigurnosne mogućnosti. Zanimljivo je da je sigurnost na većini uređaja postavljena u zadani način rada, a kada je postalo očitije da je sigurnost nužna za ovo područje, promjene

u hardveru su polako evoluirale. Hardver nije bio jedina sigurnosna ranjivost, jer je i softver imao sigurnosnih problema. Na kraju se enkripcija pojavila kao tehnika koja može zaštititi informacijske podatke pohranjene u našim bazama podataka.

Budući da su se pojavili virusi, crvi i zlonamjerni softveri, stvorena je industrija koja nudi softverska rješenja za zaštitu računala od tih virusa i zlonamjernih programa. Kako su dizajneri virusa i zlonamjernog softvera postajali sve sofisticiraniji u proizvodima koje su izrađivali, industrija je uvijek bila u poziciji reakcije i pokušavala uhvatiti korak s dizajnom zlonamjernog softvera. Ironija je usredotočena na to koliko malo košta dizajn virusa i koliko je nevjerojatno skup razvoj antivirusnih alata za zaštitu od tih virusa.

Budući da su računalne prijevare, zlouporaba i krađa intelektualnog vlasništva sada dosegli razinu koja može uništiti cijele tvrtke, postoji nacionalni interes za zaštitu informacijske imovine. Od 1984. godine savezna vlada potiče industrije i korporacije da se pozabave pitanjem osiguranja svoje imovine, podataka i intelektualnog vlasništva. Korporacijski sektor povijesno je odstupao od ovih vladinih preporuka i poticaja jer su na informacijske sustave gledali kao na troškovne centre, a budući da su se rukovoditelji američkih korporacija više usredotočili na tromjesečne račune dobiti i gubitka, bili su više zainteresirani za profitne centre, a ne za troškovne centre.

2.3.1. Najnovije prijetnje

- Dridex malware

U prosincu 2019. Ministarstvo pravosuđa Sjedinjenih Američkih Država (DOJ) optužilo je vođu organizirane kibernetičke kriminalne skupine za njihovu ulogu u globalnom napadu zlonamjernim softverom Dridex. Ova zlonamjerna kampanja utjecala je na javnost, vladu, infrastrukturu i poslovanje diljem svijeta. Dridex je financijski trojanac s nizom mogućnosti, a pogađa žrtve od 2014. godine. Zarazi računala putem phishing e-pošte ili postojećeg zlonamjernog softvera. Nakon toga sposoban je za krađu lozinki, bankovnih podataka i osobnih podataka koji se koriste u lažnim transakcijama. Dridex je prouzročio ogromne financijske gubitke koji se mjere stotinama milijuna dolara. Kao odgovor na napade Dridex-a, National Cyber Security Centre Ujedinjenog Kraljevstva savjetovao je javnosti da "osiguraju da su uređaji zakrpani, da je antivirusni program uključen i ažuran te da imaju sigurnosne kopije datoteka".

- Romantične prevare

U veljači 2020. FBI je upozorio građane SAD-a da budu svjesni prijevare povjerenja koju čine napadači koristeći stranice za upoznavanje i sobe za chat. Počinitelji iskorištavaju ljude koji traže nove partnere, navodeći žrtve da im daju osobne podatke. FBI izvješćuje da su romantične prijetnje utjecale na 114 žrtava u Novom Meksiku 2019., s financijskim gubicima u iznosu od 1,6 milijuna dolara.

- Emotet malware

Krajem 2019. The Australian Cyber Security Centre upozorio je nacionalne organizacije na raširenu globalnu kibernetičku prijetnju zlonamjernog softvera Emotet. Emotet je sofisticirani trojanac koji može ukrasti podatke i učitati drugi zlonamjerni softver.

2.4. Zaštita od napada

Zaštita krajnjeg korisnika ključni je aspekt kibernetičke sigurnosti. Uostalom, često je pojedinac (krajnji korisnik) taj koji slučajno učita zlonamjerni softver ili neki drugi oblik prijetnje na svoje stolno računalo, prijenosno računalo ili mobilni uređaj. Kako mjere kibernetičke sigurnosti štite krajnje korisnike i sustave? Prvo, kibernetička sigurnost oslanja se na kriptografske protokole za šifriranje e-pošte, datoteka i drugih kritičnih podataka. To ne samo da štiti informacije u prijenosu, već i štiti od gubitka ili krađe. Osim toga, sigurnosni softver krajnjeg korisnika skenira računalo u potrazi za dijelovima zlonamjernog koda, stavlja ovaj kod u karantenu i zatim ga uklanja s računala. Sigurnosni programi mogu čak otkriti i ukloniti zlonamjerni kod skriven u primarnom zapisu za pokretanje. Elektronički sigurnosni protokoli također su usmjereni na otkrivanje zlonamjernog softvera u stvarnom vremenu. Mnogi koriste heurističku i bihevioristička analizu za praćenje ponašanja programa i njegovog koda za obranu od virusa ili trojanaca koji mijenjaju svoj oblik sa svakim izvođenjem (polimorfni i metamorfni malware). Sigurnosni programi nastavljaju razvijati nove obrane dok stručnjaci za kibernetičku sigurnost identificiraju nove prijetnje i nove načine za borbu protiv njih. Da biste maksimalno iskoristili sigurnosni softver za krajnjeg korisnika, zaposlenici moraju biti educirani o tome kako ga koristiti. Nekoliko koraka za zaštitu od napada su:

1. Ažurirajte svoj softver i operativni sustav - to znači da imate koristi od najnovijih sigurnosnih zakrpa;
2. Koristite antivirusni softver - sigurnosna rješenja kao što je Kaspersky Total Security će otkriti i ukloniti prijetnje;
3. Koristite jake lozinke - pobrinite se da vaše lozinke nije lako pogoditi;

4. Ne otvarajte privitke e-pošte nepoznatih pošiljatelja, mogli bi biti zaraženi zlonamjernim softverom;
5. Ne klikajte na poveznice u e-porukama od nepoznatih web stranica ili pošiljatelja; ovo je uobičajeni način na koji se širi zlonamjerni softver;
6. Izbjegavajte korištenje WiFi mreža na javnim mjestima - nesigurne mreže čine vas ranjivima na napade man-in-the-middle.

3. KRITIČNE INFRASTUKTURE

Kritična infrastruktura uključuje imovinu, sustave, objekte, mreže i druge elemente na koje se društvo oslanja kako bi održalo nacionalnu sigurnost, ekonomsku vitalnost te javno zdravlje i sigurnost. Kritičnu infrastrukturu poznajemo kao struju koju koristimo u domovima, vodu koju pijemo, prijevoz koji nas pokreće, trgovine u kojima kupujemo te internet i komunikacije na koje se oslonimo kako bismo održali kontakta s prijateljima, obitelji i kolegama. Nije sva infrastruktura unutar industrijskog sektora ključna za naciju ili regiju. Potrebno je utvrditi koja je infrastruktura kritična za održavanje stalnih usluga ili funkcija i ranjiva na neku vrstu prijetnje ili opasnosti.

Postoje četiri određene životne funkcije – transport, voda, energija i komunikacije, što znači da su njihovi poslovi toliko kritični da će prekid ili gubitak jedne od ovih funkcija izravno utjecati na sigurnost i otpornost kritične infrastrukture unutar i između brojnih sektora. Ove veze i međuovisnosti između infrastrukturnih elemenata i sektora znače da gubitak jedne ili više funkcija obično ima neposredan učinak na misiju u više sektora. Kao rezultat toga, s vremenom može doći do gubitka drugih funkcija. Identificiranje i službeno priznavanje industrijskih sektora koji su ključni sektori i/ili imaju međusektorsku međuovisnost olakšava suradnju i razmjenu informacija koja promiče kontinuitet poslovanja i usluga.

3.1. Tko je odgovoran?

Jačanje sigurnosti i otpornosti kritične infrastrukture zajednička je odgovornost dionika - vlasnika i operatera kritične infrastrukture te raznih vladinih tijela i nevladinih organizacija (uključujući industrijska udruženja).

Uloge i odgovornosti za održavanje ili poboljšanje sigurnosti i otpornosti infrastrukture uvelike variraju i na njih utječu mnogi čimbenici kao što su: javno naspram privatnog vlasništva; uredbe unutar sektora; predviđene prijetnje i opasnosti za određeni sektor; i odluke o tome hoće li se sektor ili regija odlučiti usredotočiti na poduzimanje radnji za zaštitu infrastrukture, smanjenje posljedica ili brz odgovor i oporavak od nepovoljnih događaja.

3.2. Međuovisnosti kritične infrastrukture

Važno istraživanje Pedersona, Dudenhoeffera, Hartleya i Permanna o međuovisnosti kritične infrastrukture sugerira da većina kritičnih infrastrukturnih sustava međusobno djeluje kroz povezanost koja se može pojaviti kao rezultat politika, procedura ili izravne blizine. Njihovo

istraživanje u Nacionalnom laboratoriju Idaho otkrilo je da te interakcije stvaraju složene odnose, ovisnosti i međuovisnosti koje prelaze granice infrastrukture. Ovo važno istraživanje zaključilo je da sposobnost pružanja zaštite kritičnim infrastrukturama ovisi o temeljitijem i dobrom razumijevanju načina na koji postoje međuovisnosti između infrastruktura. Njihovo istraživanje usredotočilo se na to što su zapravo infrastrukturne međuovisnosti i kako se one modeliraju. Njihovo istraživanje o modeliranju učinka koji jedna infrastruktura može imati na drugu infrastrukturu može se ocijeniti njihovom međuovisnošću. Pojedinačna strategija zaštite osmišljena za jednu kritičnu infrastrukturu potpuno zanemaruje utjecaj toga koliko je svih 16 kritičnih infrastruktura postalo međuovisno. Usredotočenost na posljedice prisiljava sigurnosnu strategiju da prihvati mnogo detaljniju analizu od prethodnog pristupa zaštite jedne kritične infrastrukture, što je prije bila prevladavajuća praksa.

3.3. Primjena modela optimizacije na kritične infrastrukture

Istraživački projekt Browna, Carlylea, Salmerona i Wooda na Odjelu za operacijska istraživanja primijenio je modele optimizacije na razine kako bi kritične infrastrukture učinili otpornijima na terorističke napade. Njihovo istraživanje nastojalo je analizirati ranjivosti bilo koje kritične infrastrukture kroz niz koordiniranih terorističkih napada u kojima su ponudili utemeljene prijedloge za smanjenje ranjivosti. Primjenom modela visoke vjernosti uspjeli su formulirati i pronaći podatke za rješavanje modela visoke vjernosti kritičnih infrastrukturnih sustava. Istraživanje koje su citirali Brown, Carlyle, Salmeron i Wood temeljilo se na stvaranju tri modela za analizu četiri komponente napada protiv: strateške rezerve nafte, granične patrole i električne mreže.

Četiri komponente analize bile su (1) kritičnost, odnosno koliko je bitna imovina; (2) ranjivost i koliko je imovina osjetljiva na nadzor ili napad; (3) rekonstitutivnost i koliko će teško biti oporavak od nanesene štete; i (4) prijetnja i koliko je vjerojatan napad na ovu imovinu. Modeli su se temeljili na usporedbi vojnih i civilnih planera i zahtijevali su donošenje odluka. Istraživanje je koristilo prilično elegantna matematička izračunavanja kako bi došli do svojih zaključaka, a autori navode da se njihovo istraživanje temeljilo na korištenju modela visoke vjernosti. Međutim, važno je napraviti razliku između modela i simulacije, i dok je ova studija koristila modeliranje, pravo pitanje je usredotočeno na to je li to više pristup naprednog modeliranja procesa, budući da ovaj pristup uključuje detaljne i matematičke modele za pružanje informacija za podršku odlučivanju i sposobnost predviđanja. S druge strane, vjernost u simulaciji tradicionalno se definirala kao stupanj do kojeg simulator replicira stvarnost.

Simulacija se, baš kao i modeliranje, također može definirati kao "niska" ili "visoka" vjernost, a u slučaju simulacije, odnosi se na to koliko blisko istraživanje predstavlja "stvarni" život. Matematičko modeliranje visoke vjernosti sugerira da su njihovi modeli optimizacije primijenjeni na elemente kritične infrastrukture zemlje unaprijedili znanje i da će bolje pripremiti donositelje odluka da donose važne prosudbe dok obavljaju svoje dužnosti.

3.4. Prijetnje i opasnosti za kritičnu infrastrukturu

I prirodni i umjetni (namjerni ili slučajni) incidenti mogu nanijeti štetu, onesposobiti ili uništiti kritičnu infrastrukturu. Umjesto da se fokusiraju na jednu vrstu prijetnje ili opasnosti odjednom, kao što su uragani ili terorizam, države bi trebale identificirati sve prijetnje i opasnosti koje predstavljaju najveći rizik za kritičnu infrastrukturu, što omogućuje učinkovitije planiranje i raspodjelu resursa. Kritična infrastruktura dugo je bila izložena rizicima povezanim s fizičkim prijetnjama i prirodnim katastrofama, a sada je sve više izložena kibernetičkim rizicima. Ti rizici proizlaze iz rastuće integracije informacijskih i komunikacijskih tehnologija s kritičnom infrastrukturom i protivnicima koji su usredotočeni na iskorištavanje potencijalnih kibernetičkih ranjivosti.

Veze i međuovisnosti između infrastrukturnih elemenata i sektora znače da oštećenje, prekid ili uništenje jednog infrastrukturnog elementa može uzrokovati kaskadne učinke, utječući na nastavak rada drugog. Utvrđivanjem i razumijevanje međuovisnosti ili ovisnosti između infrastrukturnih elemenata i sektora važni su za procjenu rizika i ranjivosti te za određivanje koraka koji se mogu poduzeti za povećanje sigurnosti i otpornosti. Na primjer, električna mreža se oslanja na integrirane informacijske i komunikacijske sustave iz drugih sektora kritične infrastrukture kako bi funkcionirala. Jedan primjer neposredne potrebe za energijom su oporavak nakon prirodne katastrofe. Sve dok se energetski sustav ne obnovi, sustavi vode i otpadnih voda ne mogu osigurati čistu vodu, prirodni plin ne može teći za opskrbu toplinom, a proizvodni i telekomunikacijski sustavi brzo postaju neoperativni nakon što rezervni izvori energije počnu kvariti.

Živimo u svijetu u kojem se teroristička aktivnost povećava i postaje sve rasprostranjenija, gdje napadi mogu biti jednostavni i oportunistički po prirodi ili složeni i organizirani. Rastući broj napada na lake mete/mjesta s velikim brojem ljudi u više gradova diljem svijeta pokazuje da se priroda prijetnje razvija i pojačava potrebu za globalnom budnošću, pripravnošću i suradnjom.

Prijetnje i opasnosti mogu biti specifične za zemljopisne regije ili za cijelu zemlju, a mogu čak imati i globalne posljedice; kao što su:

- Klimatološki događaji (ekstremne temperature, suša, šumski požari);
- Hidrološki događaji (poplave);
- Meteorološki događaji (tropski cikloni, jake oluje, jake zimske oluje);
- Geofizički događaji (potresi, tsunamiji, vulkanske erupcije);
- Pandemije (globalno izbijanje bolesti);
- Svemirski vremenski događaji (geomagnetske oluje);
- Tehnološke i industrijske nesreće (strukturalne nepogode, industrijski požari, ispuštanje opasnih tvari, izlijevanje kemikalija);
- Neplanirani poremećaji (zastarjela infrastruktura, kvar opreme, veliki prekid napajanja);
- Kriminalni incidenti i terorizam napadi (vandalizam, krađa, kinetički napadi);
- Cyber incidenti (napadi uskraćivanjem usluge, zlonamjerni softver, krađa identiteta);
- Napadi na lanac opskrbe (iskorištavanje ranjivosti radi izazivanja sistemskih ili mrežnih neuspjeha);
- Operacije stranog utjecaja (širenje dezinformacija ili potkopavanje demokratskih procesa).

3.5. Internet, društveni mediji i kibernetički napadi na kritične infrastrukture

Rast interneta i društvenih medija bio je fenomenalan u smislu ogromnog broja ljudi koji sada žive i rade u ovom globalnom međusobno povezanom svijetu. Procijenjeno je da je u 2014. više od 2,5 milijarde ljudi bilo spojeno na svjetsku mrežu. Kako bismo dodatno demonstrirali prilike, izazove i rizike koji čekaju sve nas, sada doživljavamo "Internet of Things", gdje će ovoj složenosti biti dodano još doslovno nekoliko milijardi strojeva i uređaja koji će također biti dostupni i međusobno će komunicirati, voditi i u mnogim slučajevima donositi odluke bez ljudske kontrole i prosudbe.

Sve veći broj ljudi i uređaja koji se povezuju u kibernetičkom prostoru uvelike će utjecati na određene dijelove kritične infrastrukture. Infrastrukture koje će biti neposredno pogođene bit će sljedeće: sustav električne mreže, transport i telekomunikacije. Ostali infrastrukturni sektori također će biti pogođeni, kao što su sustavi hrane, vode, hitne službe te bankarske i financijske usluge, ali utjecaj na njihovu izvedbu i kontinuitet usluge neće biti tako dubok kao prethodni. Kako društva postaju toliko međusobno povezana sa svojim uređajima i uslugama, ova sve veća ovisnost može povećati ranjivost na poremećaje kritičnih infrastruktura. Sada se pojavila globalna trgovina digitalnim oružjem koja prodaje sofisticirani zlonamjerni softver ponuđačima

koji najviše ponude, uključujući hakerske alate i napade "Zero-Day Exploits" koji iskorištavaju dosad nepoznate ranjivosti.

Bankarske i financijske zajednice doživjele su prilično sofisticirane napade, jer su u ožujku 2013. kibernetički napadi prekinuli bankarske usluge Wells Fargo, J.P. Morgan Chase, Citi Group, U.S. Bancorp, PNC Financial Services, American Express i Bank of America. Symantec Corporation procjenjuje trošak za potrošače na 110 milijardi dolara na globalnoj razini. Drugi oblik poremećaja i ranjivosti koji utječe na naše velike korporacije je "kibernetička ekonomska špijunaža". Bivši ministar obrane Leon Panetta upozorio je na "cyber Pearl Harbor", u kojem bi napadi usmjereni na kritičnu infrastrukturu mogli prouzročiti značajna i rasprostranjena razaranja budući da se napadi mogu daljinski pokrenuti protiv industrijskih kontrolnih sustava (ICS-ova) dizajniranih da modificiraju ili reprogramiraju one ICS-ove koji kontroliraju cjevovode, željezničke pruge, brane i električne mreže, uzrokujući tako gubitak kritičnih usluga i također oštećujući važne i skupe dijelove infrastrukturnog sustava.

U 2011. Ministarstvo domovinske sigurnosti izvijestilo je o porastu napada na kritičnu infrastrukturu od 383%. Izvješće navodi da bi s vremenom budući napadi mogli postati još destruktivniji kako se kibernetičko oružje i kapaciteti šire i kako infrastrukture za električnu energiju, transport i komunikaciju sve više ovise o internetu. Za razliku od nuklearnog oružja, barijere za ulazak su male za kibernetičke napade, a pojedinci s ograničenim iskustvom mogu brzo postati sposobni za provođenje razornih radnji u kibernetičkom prostoru.

3.6. Pokretači otpornosti i sigurnosti kritične infrastrukture

Sigurnost se može definirati kao smanjenje rizika za kritičnu infrastrukturu od upada, napada ili posljedica prirodnih katastrofa ili katastrofa izazvanih ljudskim djelovanjem, primjenom fizičkih sredstava ili obrambenih kibernetičkih mjera. Otpornost je sposobnost prilagodbe i pripreme promjenjivim uvjetima. To znači biti u stanju izdržati i brzo se oporaviti od poremećaja, namjernih napada, nesreća ili prirodnih prijetnji ili incidenata. Otporna infrastruktura također mora biti robusna, agilna i prilagodljiva.

Snažan program sigurnosti i otpornosti kritične infrastrukture temelji se na suradnji i dijeljenju informacija. Suradnja se olakšava uspostavom procesa potrebnih za slobodnu komunikaciju vlade(a) i privatnog sektora bez objavljivanja zaštićenih informacija; podržati pouzdano okruženje za razmjenu informacija u kojem dionici razmjenjuju informacije radi jačanja sigurnosti i otpornosti; osigurati da su relevantni dionici pošteno zastupljeni i angažirani, sa svih razina vlasti, industrije, upravljanja u hitnim slučajevima i sigurnosti. Uspješna razmjena

informacija zahtijeva uspostavljene mehanizme ili kanale za redovito dopiranje do dionika prije, tijekom i nakon incidenta. Dijeljenje informacija može imati mnoge oblike, uključujući treninge, brifinge, upozorenja e-poštom, konferencijske pozive ili sastanke na sigurnim lokacijama za raspravu o povjerljivim materijalima o specifičnim prijetnjama ili opasnostima te dokumente i forume koji potiču razmjenu naučenih lekcija.

Kako bi se olakšala dobrovoljna suradnja i razmjena informacija unutar i između sektora kritične infrastrukture i vladinih agencija (saveznih, državnih, lokalnih, plemenskih i teritorijalnih), uspostavio se službeni okvir partnerstva koji se sastoji od koordinacijskih vijeća vlade i privatnog sektora koji se također sastaju odvojeno kako bi zajedno poboljšali sigurnost i otpornost kritične infrastrukture. Razmjena informacija privatnog sektora provodi se putem Centra za razmjenu i analizu informacija (ISAC). ISAC prvenstveno djeluju kroz sektorski model, što znači da se organizacije unutar određenog sektora kritične infrastrukture (ili specifičnog segmenta unutar sektora) udružuju radi razmjene informacija. Iako su mnoge od ovih skupina već bitni pokretači učinkovite razmjene informacija, neke se organizacije ne uklapaju uredno u uspostavljeni sektor ili imaju jedinstvene potrebe. SAD također ima industrijske suradničke organizacije za razmjenu informacija i analizu (ICAO). Stvoreni za prikupljanje, analizu i širenje informacija o kibernetičkoj prijetnji, ICAO-i nude fleksibilniji pristup samoorganiziranim aktivnostima dijeljenja informacija među određenim interesnim zajednicama.

3.7. Istraživanje i razvoj za podršku kritičnim infrastrukturama

Na temelju vladine identifikacije kritične infrastrukture, Izvršni ured predsjednika i OSTP razvili su plan istraživanja strukturiran oko devet znanstvenih, inženjerskih i tehnoloških tema koje bi podržale cjelokupne sektore kritične infrastrukture. Devet usmjerenih područja za poticanje istraživanja i razvoja za sektore kritične infrastrukture su: detekcija i senzorski sustavi, zaštita i prevencija, ulazni i pristupni portali, insajderske prijetnje, analiza i sustavi za podršku odlučivanju, odgovor, oporavak i rekonstitucija, nove prijetnje i ranjivosti, napredne infrastrukturne arhitekture i dizajn sustava, ljudska i društvena pitanja.

Preslikavanjem dugoročnih sveobuhvatnih ciljeva na pet znanstvenih, inženjerskih i tehnoloških tema, stvoreni su sljedeći prioriteti istraživanja i razvoja:

1. Poboljšati performansi senzora, razvoj tehnologije za otkrivanje neeksplodiranih ubojnih sredstava, razviti sustav globalnog pozicioniranja u stvarnom vremenu sinkroniziran za praćenje električne mreže, poboljšati senzorske nizove i poboljšati detekciju eksploziva i

radiologije, poboljšati senzore za otkrivanje neovlaštenog miješanja u sustave vode, grijanja, ventilacije i klimatizacije (HVAC), poboljšati SCADA i HVAC sustave.

2. Unaprijediti modeliranja rizika, simulacije i analize za podršku odlučivanju, standardizirati analizu ranjivosti i analizu rizika kritičnih infrastrukturnih sektora, provesti kvantitativne procjene rizika kako bi se bolje kvantificirali rizici od terorizma za sektore kritične infrastrukture.

3. Poboljšati kibernetičku sigurnost, razviti nove metode za zaštitu od automatizirane detekcije, odgovora i oporavka od napada na kritične informacijske infrastrukture, poticati migraciju na sigurniju internetsku infrastrukturu.

4. Bavite se insajderskom prijetnjom, poboljšati tehnologije kao što su određivanje namjere i praćenje nenormalnog ponašanja za otkrivanje insajderske prijetnje, pokrivajući fizičku i kibernetičku infrastrukturu.

5. Poboljšati situacijsku svijest velikih razmjera za kritičnu infrastrukturu, definirati arhitekturu komunikacijskog i računalnog sustava potrebnu za stvaranje nacionalne zajedničke operativne slike kritičnih infrastruktura.

3.8. Sektori kritične infrastrukture

Globalno gledano, živimo u digitalnom krajoliku punom kibernetičkih prijetnji i ranjivosti. Idemo u budućnost u kojoj stručnjaci za sigurnost u javnom i privatnom sektoru moraju koristiti visoko suradničku i međusobno povezanu platformu za kibernetičku sigurnost kritične infrastrukture.

Kao što Ministarstvo domovinske sigurnosti (DHS) ističe "osiguranje kritične infrastrukture zajednička je odgovornost - koju dijele savezne, državne, lokalne, plemenske i teritorijalne vlade; privatne tvrtke; i pojedini građani." Dakle, čak i na makroekonomskoj razini, kibernetička sigurnost ponovno je zajednička odgovornost u našim svakodnevnim životima. Ministarstvo domovinske sigurnosti trenutačno surađuje s mnogim industrijskim sektorima, saveznim agencijama i organizacijama privatnog sektora na distribuciji informacija o novim prijetnjama i ranjivostima kritične infrastrukture. DHS poslušno nadzire, analizira i reagira na sigurnosne incidente koji utječu na ključne sektore industrije. Kibernetički napadi na bilo koji od ovih kritičnih sektora mogao bi dovesti do katastrofalnih učinaka na sigurnost nacije, kao i na javno zdravlje i sigurnost građana.

Godine 2013. izrađen je Nacionalni plan zaštite infrastrukture (NIPP 2013: Partnerstvo za sigurnost i otpornost kritične infrastrukture) gdje bi se opisalo kako će subjekti privatnog i

javnog sektora surađivati na zaštiti kritične infrastrukture u SAD-u. Jeste li znali da postoji 16 sektora u kojima je vlada Sjedinjenih Država postavila kritičnu infrastrukturu kibernetičke sigurnosti? Neki znaju, ali drugi ne shvaćaju opseg industrija koje kritična infrastruktura pokriva i koliko se oslanjamo na svaku od njih. Od ključne je važnosti da imamo te programe za zaštitu naše kritične infrastrukture. Već smo vidjeli vijesti o kibernetičkim napadima na ove vodeće industrije. Ove nam priče pokazuju koliko je važno zaštititi i očuvati te sektore.

1. Sektor energetskih usluga

Energetski sektor pokreće gospodarstvo 21. stoljeća. Bez stalne opskrbe energijom, dobrobit građana su potkopani, a gospodarstvo ne može funkcionirati.

Kibernetički napad 2015. uništio je energetsku mrežu u Ukrajini za više od 225 000 ljudi korištenjem spear phishing e-pošte. Prema vladinim dužnosnicima Sjedinjenih Država, niti jedna industrijska električna mreža ne može se spojiti na internet kako bi se spriječio kibernetički napad. Jedini način na koji bi električne mreže bile poremećene je putem netehnološkog hakiranja ili fizičke sigurnosne povrede. Međutim, neke sigurnosne tvrtke izvješćuju da je određena hakerska skupina pod nazivom Dragonfly 2.0 ciljala na američke energetske tvrtke i uspješno dobila pristup mapiranju za industrijske sustave upravljanja koji pokreću električne mreže iz zapisa poslovnih podataka.

2. Sektor brana

Sektor brana osigurava osnovno održavanje vode i kontrolira usluge vode, uključujući hidroelektranu, gradsku i industrijsku opskrbu vodom, sustave za poljoprivrednu vodu, kontrolu mulja i valova, rutu toka za unutarnji masovni transport, modernu administraciju otpada i rekreacijske usluge.

Godine 2016. iranska nacionalna država počinila je kibernetički napad na Sjedinjene Države na branu Rye Brook u New Yorku. Hakeri su pristupili industrijskim kontrolnim sustavima unutar brane, ali srećom nisu mogli ispustiti vodu. Međutim, ovo je mogla biti katastrofa koja je čekala da se dogodi uz samo nekoliko klikova.

3. Sektor financijskih usluga

Sektor financijskih usluga ima cilj zaštititi najvitalniji izvor ekonomije. Široko rasprostranjena, nestanak električne energije, nedavne prirodne katastrofe te povećanje broja i napredovanja

kibernetičkih napada pokazuju veliku raznolikost potencijalnih opasnosti s kojima se ovaj sektor suočava. Ovo je očito jedan od najnapadanijih sektora. Kibernetički kriminalci redovito napadaju financijski sektor koristeći sve vrste prijetnji za iznudu i financijsku dobit.

Najnovija provala kreditnog ureda Equifax s više od 143 milijuna ukradenih zapisa smatra se kritičnom provalom infrastrukture. Ova povreda je bila toliko dalekosežna da je pogodila gotovo polovicu američke populacije od 44% populacije SAD-a.

4. Nuklearni reaktori i sektor otpada

Ovaj sektor uključuje nuklearnu infrastrukturu i energetske reaktore koji opskrbljuju električnom energijom, kao i medicinske izotope koji se koriste za liječenje raka. Nuklearne elektrane velika su briga za kibernetičke napade.

Nedavno je probijena poslovna evidencija nuklearnog postrojenja u Sjedinjenim Državama, ali kritična infrastruktura nije bila pogođena. Stručnjaci sugeriraju da, iako hakeri ne mogu pristupiti kritičnoj infrastrukturi, oni još uvijek dobivaju informacije koje se kasnije mogu koristiti za hakiranje sustava radi pune kontrole. To bi moglo dovesti do još ozbiljnijih napada.

5. Sektor prehrane i poljoprivrede

Prehrambeni i poljoprivredni sektor gotovo je potpuno u privatnom vlasništvu i sastoji se od milijuna farmi, restorana i registriranih objekata za proizvodnju, preradu i skladištenje hrane. Ova podjela predstavlja otprilike jednu petinu ekonomske aktivnosti. Poljoprivrednici i vlasnici poljoprivrednih tvrtki zabrinuti su zbog novih ranjivosti poljoprivredne opreme. Prehrambena i poljoprivredna industrija sada se oslanja na više podataka s povezanim uređajima, ali to dolazi s ozbiljnim rizikom od novih ranjivosti. Ono što više zabrinjava je anketa Farm Bureaua koja je izjavila da 87% farmera nema plan odgovora ako dođe do povrede sigurnosti u tvrtki koja drži njihove podatke.

6. Sektor vodoopskrbe i kanalizacije

Pitka voda za piće ključna je za osiguranje opće dobrobiti cijelog čovječanstva. Pročišćena otpadna voda neophodna je za izbjegavanje bolesti. Na taj način, osiguranje opskrbe pitkom vodom i pročišćavanje otpadnih voda ključni su za gospodarstvo.

7. Sektor zdravstva

Sektor zdravstva osigurava zdravlje i sigurnost za sve. Koristi od ovog sektora uglavnom su privatne, što zahtijeva koordinirane napore i razmjenu podataka između opće populacije i privatnih odjela. Ovaj sektor ima obilje osjetljivih podataka i osobnih podataka koje mogu iskoristiti hakeri unutar zdravstvenih organizacija.

8. Sektor hitne službe

Sektor hitnih službi zajednica je milijuna visokokvalificiranog, obučenog osoblja za hitne slučajeve, zajedno s fizičkim i kibernetičkim sigurnosnim resursima, pružajući širok raspon usluga pripravnosti i oporavka tijekom svakodnevnih operacija i odgovora na incidente.

Ovaj sektor ima pet različitih sektora prikazanih na donjoj slici:

Slika 1. Pet sektora hitnih službi

Izvor: https://medium.com/@esaylors/fire-departments-are-not-businesses-they-are-critical-infrastructure-39d4647b3746

Američka policija i vatrogasna i spasilačka služba postaju žrtve najnovijih kibernetičkih napada ransomwarea poput WannaCryja. Ove kritične usluge mogu se potpuno isključiti, što je zabrinjavajuće jer se građani oslanjaju na te usluge svaki dan.

9. Sektor prometnih sustava

Odjel domovinske sigurnosti i Odjel prometa dodijeljeni su kao ko-sektorske agencije za sektor prometnih sustava. Transportni okvir zemlje brzo i sigurno premješta pojedince i proizvode

kroz zemlju i inozemstvo. Sektor transportnih sustava također bilježi porast kibernetičkih napada.

Nedavno je sustav željeznice u San Franciscu zaražen zlonamjernim virusima koji su njegove sustave isključili iz mreže. Naši "pametni" povezani gradovi sve će više postajati meta kibernetičkih kriminalaca.

10. Kemijski sektor

Kemijski sektor bitan je segment gospodarstva koji proizvodi, koristi, skladišti i transportira opasne kemikalije. Veliki izbor drugih temeljnih sektora također ovisi o ovom sektoru.

Značajan napad, 'Nitro', dogodio se 2011. pri čemu su hakeri upotrijebili malware pod nazivom PoisonIvy kako bi ukrali osjetljive podatke i informacije iz nekoliko kemijskih tvrtki u SAD-u.

11. Sektor komunikacija

Komunikacijski sektor temeljni je dio gospodarstva i skrivenih operacija svih organizacija, udruga za javnu sigurnost i vlade. S porastom prihvaćanja mobilnih uređaja i tableta, sektor komunikacija jedna je od najvećih meta kibernetičkih napada. Žice i preklopnici koji povezuju mreže koje napajaju ove uređaje često su meta napada. Komunikacijski sektor je okosnica povezivanja za sve što koristimo uključujući glas, podatke, internet i video.

12. Sektor informacijskih tehnologija

Ovaj je sektor ključan za sigurnost, gospodarstvo i opću dobrobit zemlje budući da se organizacije, vlade, znanstvena zajednica i privatni stanovnici progresivno oslanjaju na kapacitete Sektora informacijske tehnologije. Ovi virtualni i cirkulirani kapaciteti stvaraju i daju opremu, programiranje i okvire za inovacije podataka i administracije, te - u zajedničkom naporu sa Sektorom komunikacija - internet.

13. Bazni sektor obrambene industrije

Sektor obrambene industrijske baze (DIB) cjelokupni je moderni kompleks koji osnažuje inovativan rad i održavanje okvira vojnog oružja, podsustava i segmenata ili dijelova, kako bi se zadovoljili zahtjevi vojske. Hakeri i nacionalne države neprestano napadaju sektor DIB-a zbog vrlo povjerljivih podataka i intelektualnog vlasništva koje posjeduje.

14. Kritični proizvodni sektor

Kritični proizvodni sektor ključan je za uspješno gospodarstvo. Trenutačni kibernetički napad ili poremećaj određenih komponenti proizvodnog sektora mogao bi poremetiti temeljne kapacitete na nacionalnoj razini i drugim osnovnim sektorskim područjima. Ovaj sektor uključuje proizvođače metala, strojeva, automobilske i transportne opreme te proizvođače električne opreme.

Za kritičnu proizvodnju, kibernetički napadi gotovo su se udvostručili do rujna 2016., prema američkom DHS-u. Slično kao u DIB sektoru, kibernetički kriminalci pokušavaju ukrasti osjetljivo intelektualno vlasništvo i podatke kako bi ih prodali radi zarade. Proizvođači automobila jedna su od glavnih meta kibernetičkih kriminalaca u proizvodnoj industriji, na njih otpada gotovo 30% kibernetičkih napada.

15. Sektor državnih ustanova

Ovaj sektor uključuje široku lepezu zgrada, smještenih u SAD-u i inozemstvu, koje su iznajmljeni ili u vlasništvu vlada. Objekti američke vlade često mogu biti meta kibernetičkih kriminalaca.

Godine 2011. dva su istraživačka laboratorija, Pacific Northwest Laboratory (PNNL) i Thomas Jefferson National Laboratory u Newport Newsu u Virginiji, bili žrtve kibernetičkog napada. Napadi su na kraju uzrokovali da ti laboratoriji na nekoliko dana zatvore sav pristup internetu i pristup web stranicama.

16. Sektor gospodarskih objekata

Sektor gospodarskih objekata uključuje mnoge različite organizacije koje privlače pojedince za kupovinu, posao, zabavu ili ugostiteljstvo. Većina tih organizacija je u privatnom vlasništvu, uz minimalno uplitanje vlade ili drugih regulatornih tijela. U ovom sektoru najčešće čujemo o kibernetičkim napadima u vijestima. Male do velike korporacije postaju žrtve povreda podataka, napada zlonamjernim softverom i krađe identiteta.

3.8.1. Tri kritične infrastrukture

Tri najkritičnije infrastrukture zemlje odabrane su na temelju utjecaja međuovisnosti na svih preostalih 13 kritičnih infrastruktura. Tri kritične infrastrukture odabrane za detaljniju analizu su: energija i sustav električne mreže, transport i telekomunikacije. Svaka od ove tri kritične

infrastrukture može duboko utjecati na sve preostale kritične infrastrukture, stoga je važno razumjeti njihove ranjivosti i rizicima.

3.8.1.1. Energija i sustav električne mreže

Energija predstavlja najkritičniju infrastrukturu nacije, jer je neophodna za svaki aspekt života. Cijelo naše gospodarstvo ovisi o energiji koja se uglavnom proizvodi u sustavu električne mreže te naftnom i plinskom sustavu. Sama kvaliteta života koju uživamo izravno je povezana s učinkovitim funkcioniranjem energetskog sustava. Zdravstveni sustavi, svi aspekti zapošljavanja ljudi, kao i obrazovni sustavi oslanjaju se na proizvodnju i korištenje energije. Vitalni nacionalni sigurnosni i obrambeni sustavi u potpunosti se oslanjaju na energetsku infrastrukturu. Energetska infrastruktura temeljno je organizirana oko dva glavna sektora, električne energije te nafte i prirodnog plina.

Električnu energiju koju proizvodi prvi sektor sadrži tri glavne komponente: prijenosa, proizvodnje i distribucije. Proizvodnja električne energije odvija se korištenjem brana hidroelektrana, nuklearnih elektrana i postrojenja na fosilna goriva. Prijenosni i distribucijski sustavi povezuju se s područjima sustava električne mreže. Distribucijski sustavi upravljaju, kontroliraju i distribuiraju proizvedenu električnu energiju u tvrtke, vladine organizacije i individualne domove. Činjenica da se električna energija ne može pohraniti i da se može koristiti samo u trenutku kada je proizvedena ukazuje na to koliko mora biti otporna na teroristički napad. Ciljanje ovog sektora stoga se može usredotočiti na tri glavne komponente proizvodnih postrojenja, dalekovoda i distribucijskih centara. Napad na bilo koju od ove tri komponente može stvoriti velike probleme. Stoga nisu ranjive samo nuklearne elektrane i hidroelektrane, već i sami prijenosni vodovi i trafostanice.

Većina električne energije proizvedene su na ugljen na fosilna goriva, zatim slijede nuklearne elektrane, nafta i plin te hidroenergija i ostali obnovljivi izvori. Prijenosni sustav uključuje visokonaponske vodove, stupove, podzemne kablove i transformatore, prekidače i releje, dok se distribucijski sustav sastoji od niskonaponskih razvodnih vodova i kablova te trafostanica. Sve zajedno, najveće vrste terorističkih prijetnji električnom sustavu usredotočene su na fizičke napade terorista i kibernetičke napade. Fizički napadi mogu se usredotočiti na bilo koju od proizvodnih stanica ili komponenata prijenosa i distribucije i mogu uzrokovati lokalne poremećaje ili, ako se koriste na koordiniran način s kibernetičkim napadom, mogu rezultirati ozbiljnim nestankom struje koji bi mogao izazvati ozbiljnu destabilizaciju mreže. Teoretski,

moguće je uzrokovati kolaps električne mreže, s kaskadnim kvarovima na opremi daleko od točke napada, što dovodi do još dužih i ozbiljnijih nestanka struje.

U zaštiti sustava električne mreže od kibernetičkog napada, mora se pratiti i biti svjestan novih napretka u kibernetičkom oružju. Također moraju se bolje zaštititi sustavi nadzorne kontrole i prikupljanja podataka (SCADA) s poboljšanom sigurnošću kao što su firewalls, korištenje enkripcije i preciznije mjere za otkrivanje kibernetičkih napada. Inteligentne mreže dizajnirane za nadzor i odgovor na kibernetičke prijetnje također će biti potrebne ako se žele bolje zaštititi sustavi. Područje u kojem je potrebno dodatno istraživanje i razvoj usredotočuje se na načine otkrivanja kibernetički napada iz internih izvora kao što su nezadovoljni zaposlenici. Možda je ironija naših nastojanja da se nosimo s najvažnijom infrastrukturom nacije, našim sustavom električne mreže, koji se pokazao ranjivijim prema onima kojima je taj sustav povjeren nego samim teroristima od kojih tražimo zaštitu. Stoga smo naučili da naše kritične infrastrukture moraju biti zaštićene ne samo od terorista, već i od samih ljudi kojima smo povjerili da reguliraju i štite vrijedne resurse.

Industrija prirodnog plina ogromna je mreža plinskih bušotina, cjevovoda prirodnog plina i distribucijskih vodova prirodnog plina. Ovaj je sustav stvoren kako bi se zadovoljila potražnja na tržištu i kako bi se održala sigurnost, a iako je vandalizam uzet u obzir, sustav, kao i mnogi drugi dijelovi infrastrukture, nije dizajniran da izdrži teroristički napad. Budući da prirodni plin osigurava veliki postotak stambenih i industrijskih energetskih potreba, kritičan je dio energetske infrastrukture.

Sve u svemu, sustav električne mreže te sustavi nafte i prirodnog plina ključni su za potpuno funkcioniranje gotovo svakog aspekta gospodarstva, a svaki prekid u tim uslugama čak i na nekoliko dana mogao bi imati ogromne posljedice. Potencijalni raspon ciljeva za ove sustave je ogroman, kako u smislu geografskih problema tako i složenih međuovisnosti koje zahtijevaju koordinirano sučelje između njih. Još jedan važan aspekt koji treba uzeti u obzir u zaštiti ovih sustava od terorista je priznati koliko svaka od ovih industrija potpuno ovisi o kibernetičkim računalnim sustavima. Budući da te industrije još nisu iskusile sofisticirane kibernetičke napade, nisu u potpunosti integrirale računalnu sigurnost i programe za analizu napada kako bi se spriječile i zaštitile od ove vrste terorističkih napada.

3.8.1.2. Prijevoz

Višestruki oblici prijevoznih sustava pružili su ne samo veliku pogodnost građanima, već i važnu i nezamjenjivu uslugu gospodarskom sustavu. Gotovo sve komponente nacionalne

infrastrukture oslanjaju se na transportne sustave kako bi osigurali isporuku resursa koji su im potrebni ili resursa koje proizvode. Sustav autocesta izgrađen je u obliku međusobno povezanih državnih i lokalnih cesta, cestarina, mostova. Osim sustava autocesta, nacija također ovisi o željezničkoj mreži. Druga važna značajka transportnog sustava je zračna luka, a sustav unutarnjih plovnih putova također je ključan za kretanje. Svi ti sustavi pružaju komercijalne usluge mnogim komponentama infrastrukturnog sustava zemlje.

Željeznički sustav, koji prevozi i teret i putnike, također utječe na probleme javne sigurnosti. Željeznički teretni sustav prevozi veliku količinu kemikalija poput plinovitog klora i drugih materijala, koji mogu biti vrlo opasni u slučaju nesreće ili ako postanu meta terorista. Kad uzmemo u obzir kretanje putnika koji godišnje koriste željeznički sustav, doživljavamo različite sigurnosne ranjivosti. Budući da se ovaj obujam putničkog prometa ne može provjeriti na potencijalno oružje kao što se provjeravaju putnici zrakoplova, mora se shvatiti kompromis u sigurnosti u odnosu na nužnost upravljanja sustavom koji mora premjestiti veliki obujam putničkog prometa, a istovremeno minimizirati prekid ukrcaja i iskrcaja željezničkih sustava.

Pomorska infrastruktura, koja uključuje morske luke, sustav obalnih i unutarnjih plovnih putova te brojne prevodnice, brane i kanale, pruža vrlo složen sustav za zaštitu, s obzirom na opseg teretnih brodova i nevjerojatnu količinu tereta koja prolazi kroz luke. Sigurnost luka posebno je ranjiv dio infrastrukture s dolaskom modernih kontejnerskih praksi, koje su sposobne za vrlo sofisticiran utovar kontejnera na brodove pri čemu brzina kojom se kontejneri utovaruju i istovaruju ostavlja malo vremena za inspekciju tereta utovaren unutar svakog kontejnera. U stvari, broj kontejnera koji su ušli u Sjedinjene Države 2004. premašio je 9 milijuna kontejnera, a 95% tih kontejnera nije bilo pregledano. Ovi kontejneri od 40 stopa mogu postati naš "trojanski konj 21. stoljeća", budući da bi mogli biti natovareni oružjem za masovno uništenje (WMD) ili eksplozivima koji bi lako mogli proći kroz lučki inspekcijski sustav. Vladina Inicijativa za sigurnost kontejnera, prema kojoj teret treba biti pregledan u stranim lukama prije polaska, idealan je plan i program; međutim, zahtijeva bliski i vrlo kooperativni program sa stranim zemljama kako bi se osigurali spremnici zaštićeni od neovlaštenog otvaranja. Također će zahtijevati da pošiljatelji naprave odgovarajuće tehničke izmjene kako bi njihovi kontejneri bili zaštićeni od neovlaštenog otvaranja. Sasvim je očito koliko je prometni sustav važan za gospodarstvo i sigurnost. Izazov zaštite građana i ovih prometnih sustava zahtijevat će goleme napore u istraživanju kako bi se razvile nove metode zaštite.

3.8.1.3. Telekomunikacija

Telekomunikacijska industrija je tijekom godina dosljedno pružala pouzdane, robusne i sigurne komunikacije koje su rezultirale gospodarskim prosperitetom i nacionalnom sigurnošću. Ministarstvo obrane, kao i savezne, državne i lokalne pravosudne agencije, ovise o komunikacijskim mogućnostima koje pružaju brojne telekomunikacijske tvrtke. Štoviše, ekonomska snaga izgrađena je na čvrstoj osnovi koju pruža telekomunikacijski sektor, budući da se sva poduzeća i komercijalna poduzeća oslanjaju na sposobnost komuniciranja sa svojim korisnicima.

Telekomunikacijska infrastruktura slična je energetskoj i električnoj mrežnoj infrastrukturi, po tome što bi bilo kakva njena šteta stvorila kaskadni utjecaj na druge višestruke infrastrukture jer su zahtjevi za brzim, sigurnim komunikacijskim kanalima i mogućnostima implicitni u većini drugih infrastruktura. Kao posljedica toga, vlada i telekomunikacijska industrija često moraju surađivati kako bi izgradili i održavali otpornu i sigurnu industriju, sposobnu zaštititi svoju široko raspršenu kritičnu imovinu. Telekomunikacijski sektor pruža glasovne i podatkovne usluge javnim i privatnim korisnicima kroz složenu i raznoliku infrastrukturu javne mreže koja obuhvaća javnu komutiranu telekomunikacijsku mrežu (PSTN), internet i privatne poslovne mreže. PSTN pruža komutirane sklopove za telefon, podatke i iznajmljene usluge.

Napredak tehnologije podatkovnih mreža popraćen nevjerojatnom potražnjom za podatkovnim uslugama rezultirao je svjetskim širenjem i korištenjem interneta. Iako PSTN ostaje okosnica ove važne infrastrukture, sve mobilne i satelitske tehnologije pružaju pristupnike ovom vrlo složenom sustavu. Zbog konvergencije tradicionalnih mreža s komutiranim krugovima i mreža širokopojasnog internetskog protokola, telekomunikacijska infrastruktura prolazi kroz prilično značajnu transformaciju, koja će u konačnici dovesti do mreže sljedeće generacije (NGN). Ova konvergencija, zajedno s rastom NGN-a i pojavom bežičnih mogućnosti, nastavlja predstavljati izazove telekomunikacijskoj industriji i vladi. Nova infrastruktura koja se razvija mora ostati pouzdana, robusna i sigurna.

Telekomunikacijska infrastruktura vrlo je jasna meta terorističkih organizacija. Kao takva, vlada ima jasnu odgovornost surađivati s industrijom kako bi osigurala njezinu zaštitu. U isto vrijeme, vlada ovisi o suradnji industrije u dobivanju elektroničkih dokaza o terorističkim aktivnostima. Delikatna priroda legalnog prikupljanja takvih dokaza važna je i za industriju, koja traži zaštitu od pravnih tužbi i odgovornosti, i za vladu, koja traži pravno opravdanje za nastavak elektroničkog pretraživanja, kao i za korištenje takvog materijala u kasnijim

parnicama protiv članova terorista i organizacije. Zbog stvarnosti kibernetičkih i fizičkih prijetnji zemlji i telekomunikacijskoj industriji, vlada mora surađivati s industrijom kako bi razumjela ranjivosti i razvila protumjere te uspostavila politike, planove i postupke koji će rezultirati ublažavanjem ovih rizika.

U budućnosti je sasvim očito da bi teroristički napad usmjeren na telekomunikacijsku infrastrukturu, kao i na drugu infrastrukturu ili cilj istovremeno, imao najdublji utjecaj na naciju. Stoga možemo očekivati da će telekomunikacijska infrastruktura biti fokusiranija meta terorista u budućim pokušajima napada.

4. ZAŠTITA KRITIČNE INFRASTRUKTURE

4.1. Zašto je potrebna kibernetička sigurnost kritične infrastrukture?

Naša nacija ovisi o otpornosti implementacije kibernetičke sigurnosti kritične infrastrukture. Prijetnje koje se razvijaju nastavit će nadahnjivati zajedničke napore među partnerima iz privatnog i javnog sektora. Podizanje svijesti i obuka korisnika temelj je kibernetičke sigurnosti kritične infrastrukture. Korisnici moraju naučiti o najboljim sigurnosnim praksama kako bi osigurali otpornost kritične infrastrukture u budućnosti.

Postoji nekoliko sigurnosnih strategija za sprječavanje kibernetičkih napada za ovih 16 kritičnih infrastrukturnih sektora. Preporuke uključuju odgovarajuću konfiguraciju i upravljanje zakrpama, smanjenje područja napada, popis dopuštenih aplikacija, izgradnju slojevite mreže, odgovarajuće upravljanje autentifikacijom, implementaciju sigurnog daljinskog pristupa za korisnike, aktivno praćenje prodora napada i izvršavanje pripremljenog odgovora.

4.2. Strateška zaštita kritične infrastrukture

Strateška zaštita kritične infrastrukture odnosi se na sveukupnu dugoročnu zaštitu cjelokupne kritične infrastrukture i čovječanstva u cjelini. Kao takav, radi se manje o zaštiti bilo kojeg elementa infrastrukture, a više o zaštiti sveukupne zajednice sustava podrške koji podržavaju ljudski život i društvo na Zemlji i, na kraju, kako se čovječanstvo širi svemirom, na druga mjesta.

Za početak, mora se priznati da su svi resursi ograničeni i da ideja da je “the solution to pollution is dilution” ne može opstati. Pojam održivosti neko vrijeme mora biti uravnotežen s pojmom napretka, jer ako čovječanstvo želi preživjeti morat će poboljšati tehnologiju. To onda znači da moramo mudro trošiti naše ograničene neobnovljive (barem dugo vremena oni nisu obnovljivi) resurse kako bismo napredovali do razine na kojoj možemo živjeti samo na obnovljivim resursima. Ugljena će uskoro nestati, ali nafte će nestati prije, barem ovdje na Zemlji. U vremenskom okviru infrastrukture, ugljen još nije ozbiljan problem, ali nafta jest jer je sada na ili otprilike na vrhuncu proizvodnje za sva vremena. Prelazak na ugljen znači više zagađenja i ima mnoge druge implikacije, a to znači da zaštita električne i energetske infrastrukture podrazumijeva istraživanje i razvoj u toj areni s planovima za prijelaz i upravljanje promjenama koji moraju početi sada, a ne u zadnji čas.

U kraćim vremenskim okvirima, postoji ideja da se zaštita proteže izvan neposredne. Dok su u većini poduzeća vremenski okviri od mjeseci do nekoliko godina uobičajeni pristup optimizaciji, u kritičnim infrastrukturama realniji su vremenski okviri od najmanje desetaka godina, a češće i do stotina godina. Time se mijenja priroda ulaganja i, posljedično, ulaganja u zaštitu.

Ako se želi postići održivost tijekom vremena, moraju se primjenjivati standardi, a ti standardi moraju izdržati test vremena jer evolucijska priroda infrastrukture implicira da će oni biti prisutni još dugo vremena. Snaga u Europi i velikom dijelu ostatka svijeta razlikuje se u smislu napona od one u Sjedinjenim Državama. To znači da je oprema često nekompatibilna te kao takva ne može dobro funkcionirati za informacije i telekomunikacije, koje moraju međusobno djelovati na globalnoj osnovi. Standardi su također ključni unutar infrastrukture. Na primjer, ako se koriste različite frekvencije, radio uređaji ne mogu komunicirati, a ako se koriste različite veličine cijevi i tlakovi, cijevi mogu puknuti ili se moraju ponovno montirati. Mehanizmi zaštite i troškovi zaštite mogu biti prilično različiti za različite tehnologije. Vlakna su manje osjetljiva na eksploataciju na mnoge načine, ali su osjetljivija na lomove pri savijanju i pomicanju Zemlje. Kad se vlakna uklone, ona nemaju nikakvu vrijednost, ali starim bakrenim žicama materijalna vrijednost s vremenom raste i mogu se reciklirati za ponovnu upotrebu.

Kritične infrastrukture strateška su imovina koja ima duboke implikacije na ekonomiju, kvalitetu života i opstanak stanovništva i kao takve ih treba zaštititi za dobrobit ljudi čija ih vlada, industrija i napor stvaraju i održavaju. U vrijeme rata, kritične infrastrukture su vitalne za vojne operacije i prve su mete neprijateljskih operacija. U vremenima konkurencije te su infrastrukture ključ zdravlja, bogatstva i prosperiteta. Strateška vrijednost kritičnih infrastruktura temeljna je za životne cikluse društava, a zaštita tih društava u velikoj je mjeri jednaka zaštiti te kritične infrastrukture.

Razumijevanje strateške vrijednosti infrastrukture također pomaže u razumijevanju prave prirode upravljanja rizikom koje ih okružuje. Kako bi se razumjele posljedice kvarova infrastrukture, modeliranje mora ići dalje od pojedinačnog poslovanja koje se sastoji od svakog elementa infrastrukture do vrijednosti te infrastrukture za društvo u cjelini i implikacija njezinog kvara za to društvo. Nadalje, pojedinačni infrastrukturni elementi mogu imati relativno male izravne učinke, ali u cjelini, kada mnogi od njih zakažu zbog zajedničkih načina neuspjeha ili međuovisnosti, može se dogoditi domino efekt, urušavajući cijelo društvo. Dakle, cjelokupnu kritičnu infrastrukturu društva mora rješavati društvo u cjelini ili će društvo u cjelini trpjeti posljedice lokalne optimizacije.

4.3. Inovacije i rješenja

1. Critical-chains

Critical-chains je trogodišnji istraživački i inovacijski program financiran uz potporu programa Europske komisije Horizont 2020 s fokusom na sigurnosni okvir omogućen IoT & Blockchain za Fintech integrirane kibernetičke fizičke sustave nove generacije za podršku financijskom sektoru. Konzorcij Critical-Chains predstavlja snažnu kemiju relevantne stručnosti i inkluzivan skup dionika koji čine krajnji korisnici (kupci), financijski sektor (banke i središnje druge ugovorne strane) i sektor osiguranja. Projekt ima za cilj razviti novi trokutasti model odgovornosti i integrirani okvir koji podržava odgovorne, učinkovite, pristupačne, brze, sigurne financijske ugovore i transakcije koji čuvaju privatnost radi zaštite od nedopuštenih transakcija, nezakonite trgovine novcem i prijevara u FinTech e-operacijama. Ovo je inovativni skup rješenja temeljen na oblaku "X-as-a Service" koji uključuje nekoliko kibernetičko-fizičkih sigurnosnih slojeva koji su već potvrđeni kroz prve pilot programe, kako slijedi:

- Višefaktorska hardverski potpomognuta autentifikacija (Auth-as-a-Service);
- Sloj integriteta temeljnih podataka lanca blokova (Blockchain-as-a-Service (BCaaS));
- Kriptografija kao usluga (CRYPTaaS);
- Sigurnost podataka i informacija te očuvanje privatnosti na svim slojevima oblaka putem hardverskog sigurnosnog modula (HSM) i učinkovite IoT povezivosti poboljšane preko Bluetooth Low Energy 5.0 čipa s transakcijama Modeliranje protoka kao usluga (FMaaS).

2. CyberSANE

CyberSANE ima za cilj doprinijeti rastućoj potrebi za poboljšanjem razine prevencije, spremnosti, reakcije i otpornosti na kibernetičke incidente i prijetnje CII-ja.

- Napredan, konfigurabilan i prilagodljiv sustav za rukovanje incidentima sigurnosti i privatnosti;
- Temeljit za procjenu ranjivosti;
- Procjenjuje vjerojatnost kibernetičkih napada;
- Identificira odnose između pokazatelja kompromisa, prijetnji i protivnika;
- Procjenjuje kaskadne učinke napada;
- Pruža tehničku pomoć i smjernice za istraživanje i rukovanje složenim, međusobno povezanim kibernetičkim sigurnosnim incidentima i povredama podataka;

• Kombinira i analizira sve informacije povezane sa sigurnosnim incidentima na učinkovit i točan način;

• Dijeli informacije i upozorenja sa svim dionicima.

3. CYBERWISER

CYBERWISER.eu obrazovna je, suradnička platforma za civilni kibernetički poligon u stvarnom vremenu na kojoj će se održavati natjecanja u kibernetičkoj sigurnosti, što je čini referentnom, autoritativnom, neovisnom platformom za kibernetičku sigurnost u EU za profesionalnu obuku. Korisnici mogu igrati ulogu napadača i/ili branitelja u različitim skalabilnim i konfigurabilnim scenarijima, sastavljenim od skupa virtualnih resursa koji predstavljaju ICT infrastrukturu tvrtke. Trenutačno nude 4 tečaja s različitim razinama učenja od osnovnih do naprednih i potvrđuju projekt s 3 sveobuhvatna pilot projekta: Proizvodnja i distribucija energije, Željeznički promet i Stručno i akademsko osposobljavanje.

Oni također nude uslugu procjene kibernetičke sigurnosti za mala i srednja poduzeća i Stručni registar kibernetičke sigurnosti, gdje profesionalci bilo koje dobi mogu promovirati svoje specifične skupove vještina i iskustva na tečajevima kibernetičke sigurnosti koje su pohađali i kvalifikacijama.

4. FINSEC

Razvija, demonstrira i na tržište donosi integrirani, inteligentni, suradnički i prediktivni pristup sigurnosti kritičnih infrastruktura u financijskom sektoru. U tu svrhu, FINSEC će uvesti, implementirati i potvrditi novu referentnu arhitekturu za integriranu fizičku i kibernetičku sigurnost kritičnih infrastruktura, koja će omogućiti rukovanje dinamičkim, naprednim i asimetričnim napadima, dok će u isto vrijeme povećati usklađenost financijskih organizacija sa sigurnosnim standardima i propisima.

5. InfraStress

Rješavajući trenutnu fragmentaciju dostupnih sigurnosnih rješenja i tehnologije, InfraStress pruža integrirani okvir uključujući detekciju kibernetičkih i fizičkih prijetnji, inteligenciju prijetnji i inovativnu metodologiju za procjenu otpornosti – sve prilagođeno svakom mjestu. Njihova rješenja uključuju:

• Sustavi detekcije i zaštite fizičkih prijetnji i opasnosti;

• Sustavi za otkrivanje i zaštitu kibernetičkih prijetnji;

• Ljudski senzori i senzori gužve;

• Integracija postojećih i novih -fizičkih detekcijskih sustava i senzora;

• Situacijska slika za integriranu kibernetičko-fizičku zaštitu industrijski osjetljivih lokacija i postrojenja;

• Obavještavanje i predviđanje kibernetičkih i fizičkih prijetnji;

• Usluge podrške odlučivanju u prevenciji i pripravnosti;

• CIIP usluge praćenja i ranog upozoravanja;

• Usluge podrške pri donošenju odgovora, ublažavanja i oporavka;

• Usluge analize nakon događaja;

• Dijeljenje informacija i distribucija relevantnim dionicima.

6. PANACEA

Projekt PANACEA razvio je, s tri europska zdravstvena centra, alat od devet alata usmjeren na ljude za procjenu i poboljšanje kibernetičke sigurnosti sociotehničkih sustava zdravstvene skrbi (ICT, umreženi medicinski uređaji, osoblje) i medicinskih uređaja/životnih ciklusa sustava. Uključuje inovativne alate temeljene na softveru:

• Dinamička procjena rizika, temeljena na višeslojnom modelu grafa napada uključujući "ljudske" i "poslovne" slojeve, i automatsko generiranje preporuka za ublažavanje;

• Međuorganizacijske sigurne informacije;

• Sigurnost prema dizajnu i certifikacija sustava/medicinskih uređaja usklađena s propisima;

• Identifikacija lica od stroja do stroja i putem pametnog telefona (također s maskama).

Također uključuje netehničke alate koji utječu na ponašanje osoblja i podržavaju menadžment:

• Kontekstualizirani modeli upravljanja rizikom;

• Obrazovni videozapisi bez glasa;

• Metodologija za stvaranje bihevioralnih "poticaja";

• Metodologija za maksimiziranje povrata ulaganja u kibernetičku sigurnost;

• Smjernice za kontekstualiziranu implementaciju prethodnih alata.

Potencijalna integrirana upotreba devet alata daljnja je inovativna značajka, koja podržava puni plan-uradi-provjeri-djeluj i multidisciplinarne pristupe spremnosti za kibernetičku sigurnost.

7. ReAct

ReAct ima za cilj poboljšati otpornost računalnih sustava i kritičnih infrastruktura putem dvosmjernog pristupa:

• Otkrivanje ranjivosti: nekoliko naših računalnih sustava ima ranjivosti, koje se šarenim jezikom računala obično nazivaju "greške". Kibernetički napadači iskorištavaju te bugove kako bi dobili pristup udaljenim računalnim sustavima i izveli sve vrste nezakonitih poslova. Razvijanjem sofisticiranih pristupa fuzzingu, istraživači ReActa mogu pronaći (i zakrpati) ranjivosti vrlo rano u procesu implementacije sustava i tako stvoriti robusnije i otpornije operativne računalne sustave.

• Predviđanje: iako je teško predvidjeti kada i kako će računala biti ugrožena, ReAct istraživači su razvili vrlo precizan pristup predviđanja koji može predvidjeti koja računala imaju veću šansu da će biti ugrožena. Ovo se predviđanje može koristiti za precizno određivanje, izolaciju i eventualno jačanje posebno ranjivih računala.

8. RESISTO

RESISTO platforma inovativno je rješenje za holističku svijest o situaciji komunikacijskih CI-ja i poboljšanu otpornost. RESISTO implementira inovativni sustav podrške odlučivanju za zaštitu komunikacijskih infrastruktura od kombiniranih kibernetičko-fizičkih prijetnji iskorištavanjem modela softverski definirane sigurnosti na skupu najsuvremenijih komponenti kibernetičko/fizičke sigurnosti (Blockchain, strojno učenje, IoT sigurnost, otkrivanje prijetnji u zraku, holistička audio-video analitika) i usluge (Responsible Disclosure Framework) za detekciju i reakciju u slučaju napada ili prirodnih katastrofa. Putem RESISTO-a, komunikacijski operateri moći će implementirati skup akcija ublažavanja i protumjera koje značajno smanjuju utjecaj negativnih događaja u smislu gubitka performansi, društvenih posljedica i kaskadnih učinaka.

9. SDN-microSENSE

Projekt SDN-microSENSE pridonijet će:

• Sprječavanje i rješavanje poremećaja temeljnih infrastruktura EPES mikromreža;

• Postizanje otpornih i sigurnih operacija suočenih s raznim kibernetičkim prijetnjama, povredama podataka i kvarovima;

• Ostvarivanje sigurnog i fleksibilnog upravljanja trgovanjem;

• Distribuirani i učinkoviti IT kibernetički obrambeni sustavi za velike EPES-ove;

• Razmjena informacija između energetskih operatera i aktera koja štiti privatnost;

• Formuliranje preporuka za standardizaciju i certifikaciju EPES-ova.

10. STOP-IT

Razvio je okvir za upravljanje rizikom od svih opasnosti (temeljen na EU ISO okviru za upravljanje rizikom (ISO 31000:2009), za fizičku i kibernetičku zaštitu kritičnih infrastruktura za vodu. Prevencija, otkrivanje, odgovor i ublažavanje relevantnih rizika uzeti su u obzir za generiranje modularnih rješenja (tehnologija, alata i smjernica) ugrađenih u integriranu, skalabilnu, prilagodljivu i modularnu softversku platformu. STOP-IT platforma strukturirana je u devet modula koji grupiraju tehnološka rješenja i alate za analizu koji se dalje mogu razlikovati u strateškim/taktičkim alatima i operativni alati:

• Strateški i taktički alati su simulacijski alati razvijeni za podršku menadžerima rizika i donositeljima odluka u povećanju spremnosti protiv utjecaja kibernetičkih prijetnji na uslugu koja se pruža. Omogućuju generiranje prilagođenih scenarija napada, procjenu njihovog povezanog rizika u smislu prekida usluge i izračunavanje učinkovitosti za smanjivanje rizika da se poveća otpornost sustava.

• Operativni alati podržavaju rad kibernetičko-fizičkog integriranog sustava gotovo u stvarnom vremenu ili u stvarnom vremenu pružajući opsežan popis tehnologija za otkrivanje anomalija različite prirode, kao što su napadi ometanja, IT i fizički upadi, abnormalna ponašanja, gubitak dostupnost i cjelovitost podataka.

Nadalje, projekt STOP-IT unapređuje praktična znanja o kibernetičkoj zaštiti kritične vodne infrastrukture kroz napredne, interaktivne i modularne aktivnosti obuke.

5. SCADA SUSTAVI

U ovom poglavlju dotaknut ćemo se ICS i SCADA sustava koji su međusobno povezani te ćemo odgovoriti na hipotezu. Kroz znanstveno istraživanje približit ćemo sliku i pokazati zašto je SCADA sustav važan za zaštitu kritične infrastrukture.

5.1. Sigurnost ICS-a (Industrial control system)

Sigurnost ICS-a je područje koje zabrinjava i uključuje zaštitu industrijskih kontrolnih sustava, integriranog hardvera i softvera dizajniranog za nadzor i kontrolu rada strojeva i povezanih uređaja u industrijskim okruženjima. Unatoč očitom riziku za kritičnu infrastrukturu, sigurnost ICS-a ne smatra se značajnim područjem ulaganja. Neki tvrde da su troškovi uključeni u sigurnost ICS-a previsoki, posebno unutar kritičnih sustava. To često dovodi do nerazvijene sposobnosti odgovora na incidente u postavljenom operativnom ICS-u. Veće infrastrukture pate od nedovoljnog razumijevanja postavljenih komponenti kao što su programabilni logički kontroleri (PLC) ili slični inteligentni elektronički uređaji (IED), udaljene terminalne jedinice (RTU) i ulazno/izlazni (I/O) uređaji.

Povijesno gledano, ti sustavi nisu bili umreženi i nedostajale su im računalne i komunikacijske tehnologije. Glavni fokus rastućeg interneta stvari (IoT) je umrežavanje ne-računalnih uređaja i omogućavanje njihove razmjene podataka putem interneta. Iako industrijski kontrolni sustavi sami možda nisu povezani na internet, human-machine interfaces (HMI) preko kojih se njima upravlja obično jesu.

Industrijski sustavi, uključujući kritičnu infrastrukturu, sve su više umreženi i opremljeni računalnim i komunikacijskim tehnologijama. Budući da ICS često podržavaju kritičnu infrastrukturu, ne mogu se lako skinuti radi sigurnosnih ažuriranja i tako često ostaju nezakrpani i ranjivi. Budući da sustavi imaju vrlo ograničene računalne resurse, često nemaju kapacitet za pokretanje antimalware softvera. Zbog sadašnjih ICS sustava, tek su nedavno preuzeli IP komunikaciju i povezane uređaje, gdje tradicionalna IT sigurnost, komunikacijska sigurnost i zaštita kontrolnih sustava imaju svoje granice i stoga njihovu učinkovitost tek treba dokazati.

5.2. SCADA sustavi

Sustavi industrijske kontrole (ICS) i sustavi nadzorne kontrole i prikupljanja podataka (SCADA) kritične su komponente za rad industrijskih postrojenja i kritične infrastrukture. Uspješni kibernetički napadi mogli bi paralizirati unutarnje procese, uzrokovati financijske

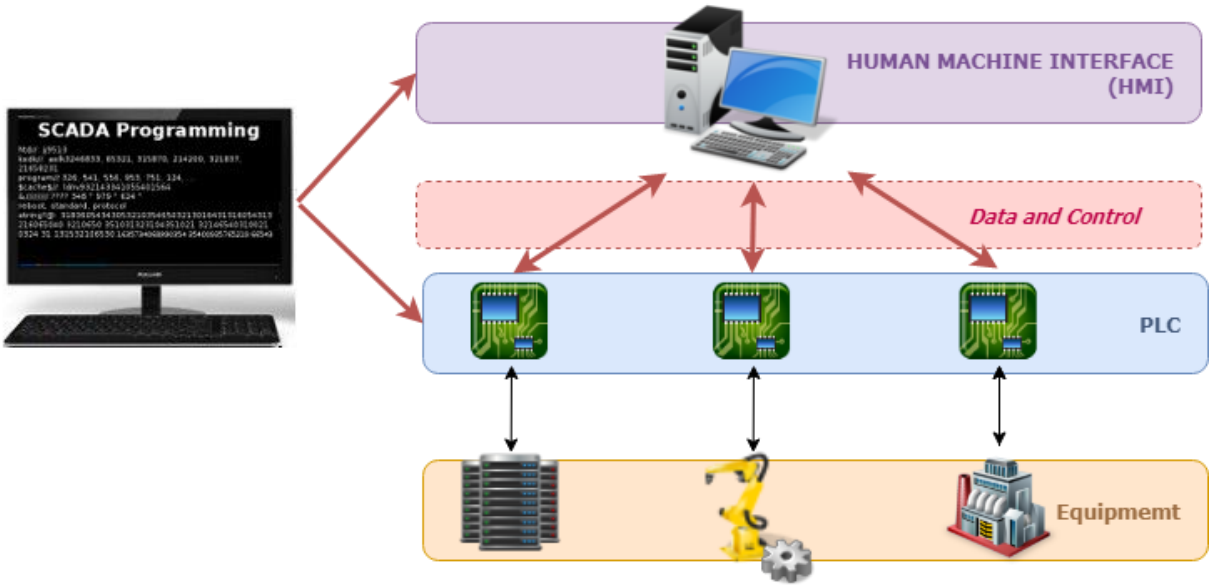
gubitke i potencijalno dovesti do gubitka ljudskih života. SCADA sustav je kombinacija hardvera i softvera koji omogućava automatizaciju industrijskih procesa prikupljanjem podataka operativne tehnologije (OT). SCADA povezuje senzore koji nadziru opremu kao što su motori, pumpe i ventili s poslužiteljem na licu mjesta ili udaljenim poslužiteljem. Od pročišćavanja otpadnih voda do upravljanja električnom mrežom, pametni gradovi se sve više oslanjaju na SCADA sustave upravljanja kako bi pomogli u praćenju i optimizaciji svega, od uzoraka semafora do javne potrošnje energije.

Osnovna SCADA arhitektura počinje programabilnim logičkim kontrolerima (PLC) ili udaljenim terminalnim jedinicama (RTU). PLC-ovi i RTU-ovi su mikroračunala koja komuniciraju s nizom objekata kao što su tvornički strojevi, HMI-ovi, senzori i krajnji uređaji, a zatim usmjeravaju informacije od tih objekata do računala sa SCADA softverom. SCADA softver obrađuje, distribuira i prikazuje podatke, pomažući operaterima i drugim zaposlenicima da analiziraju podatke i donose važne odluke.

SCADA sustavi tradicionalno su povezani s podskupom ICS-a koji se nazivaju sustavi kontrole širokog područja. Sigurnost u SCADA sustavima je istaknutija nego kod većine drugih računalnih sustava zbog potencijalne ozbiljnosti ishoda degradacije usluge, kao i poremećaja u svakodnevnom životu. Kod starijih računalnih sustava pouzdanost je bila ključna briga, a sigurnost je bila mnogo niže na popisu. Danas, uz veću povezanost, sigurnost je sada visoko na dnevnom redu. Štoviše, SCADA sustavi ne samo da postaju povezaniji s internetom već komunikacije unutar njih funkcioniraju kroz zajedničku infrastrukturu internetskog protokola (IP). U postojećim istraživanjima iznesena su brojna pitanja u vezi s implementacijom sigurnosti u SCADA:

- Pouzdanost sustava redovito ima prednost nad prijetnjama sigurnosti i može rezultirati visokom sigurnosnom ranjivošću.
- Rad SCADA mora biti u tijeku, što jako otežava primjenu ažuriranja, izvođenje krpanja ili modificiranje komponenti sustava.
- Korištenje sustava za otkrivanje upada (IDS) kao prve linije obrane. IDS se ponaša kao protuprovalni alarm za računalnu mrežu otkrivajući pokušaje neovlaštenog pristupa.
- Usluga daljinskog pristupa (RAS), koja omogućuje legitimnim korisnicima pristup SCADA sustavu s lokacije izvan lokacije. RAS bi se trebao koristiti samo u načinu povratnog poziva.

Prethodno navedene specifične karakteristike u vezi sa SCADA-om znače da je nužan pristup specifičan za domenu. In-line sigurnosni mehanizmi (npr. tradicionalno korištenje mrežnog IDS-a) ili sigurnosni alati na razini glavnog računala (npr. antivirusni) ne preporučuju se zbog mogućeg utjecaja kašnjenja ili pojave pojedinačnih točaka kvara duž vitalnog komunikacijskog puta. S obzirom na sve veću sofisticiranost napada, kibernetička sigurnost više ne može ovisiti o nadziranim algoritmima za otkrivanje koji se temelje na obrascima kako bi se zajamčio kontinuirani sigurnosni nadzor. Trebaju postojati pristupi koji rješavaju lažne prijetnje, koji osiguravaju odgovarajuću ravnotežu između snage održavanja i detekcije.



Slika 2. SCADA system

Izvor: https://www.dpstele.com/scada/how-systems-work.php

Napadi iz stvarnog svijeta poput infekcija crvom STUXNET savršeno predstavlja slabost regulatornih sustava posvećenih kontroli kritičnih infrastruktura. Prvi put izoliran sredinom lipnja 2010., STUXNET je bio računalni virus posebno dizajniran za napad na industrijska računala temeljena na sustavu Windows i preuzimanje kontrole nad programabilnim logičkim kontrolerom (PLC), utječući na ponašanje udaljenih aktuatora i dovodeći do fenomena nestabilnosti. Paradoks je da se kritične infrastrukture u velikoj mjeri oslanjaju na najnovije međusobno povezane (i ranjive) tehnologije informacijske i komunikacijske tehnologije (ICT), dok je oprema za upravljanje stari softver/hardver. Takva kombinacija čimbenika može dovesti do vrlo opasnih situacija, izlažući sustave širokom spektru napada. Lekcija koju je zajednica CIIP (Critical Information Infrastructure Protection) naučila iz širenja crva STUXNET je da, kako bi se učinkovito reagiralo na određenu prijetnju niske razine, postoji potreba da se uzmu u obzir i globalne i lokalne perspektive. Osim dobivanja šire perspektive o stanju sustava,

postoji potreba za povećanjem inteligencije opreme i uređaja koji se koriste za utjecaj na ponašanje sustava, kao što su RTU-ovi.

U procjeni infekcije botneta Mariposa u ICS organizaciji, Ministarstvo domovinske sigurnosti SAD-a objasnilo je da su otkrili da je do infekcije došlo kada je zaposlenik koristio USB pogon za preuzimanje prezentacijskih materijala na prijenosno računalo. Kada je korisnik spojio prijenosno računalo na korporativnu mrežu po povratku na posao, virus se proširio na preko 100 hostova.

Sigurnost SCADA komunikacija postaje sve kompliciranija jer je donesena odluka da se SCADA mreže povežu s IT mrežama kako bi se omogućila bolja i brža komunikacija. Ali su nove značajke povećale prijetnje i rizike za SCADA komunikacije. Ideja da se polju doda inteligencija nije nova. Brojni projekti EU (Europske unije) kao što su FP6 SAFEGUARD i FP7 CRUTIAL (CRitical UTility InfrastructurAL Resilience) istraživali su tehničku izvedivost poboljšanja kibernetičke sigurnosti SCADA sustava poboljšanjem inteligencije terenskih uređaja.

Važnost SCADA sustava je automatizacija. Omogućuje organizaciji pažljivo proučavanje i predviđanje optimalnog odgovora na izmjerene uvjete i automatsko izvršavanje tih odgovora svaki put. Oslanjanje na preciznu kontrolu stroja za nadzor opreme i procesa gotovo eliminira ljudske pogreške.

6. ZAKLJUČAK

Na temelju onoga što je napisano u ovom završnom radu mogu se izvući sljedeći zaključci: Čak ni snažan sustav kibernetičke sigurnosti više nije dovoljan. To je radi toga što su kibernetički napadi neizbježni. Dilema nije da li nego kada. Organizacije odgovorne za kibernetičku sigurnost ne mogu se zaštititi od svake pojedine kibernetičke prijetnje. Ove organizacije moraju promijeniti pristup koji su preuzeli s kibernetičke sigurnosti na kibernetičku otpornost. Napadači će se sve više oslanjati na tehnološka sredstva za izvođenje svojih operacija, koristeći kibernetičke sposobnosti za kontrolu. Ovo područje postalo je vrlo važno za rad sigurnosnih službi u smislu definiranja mogućih prijetnji koje dolaze s ovog područja. Ovisnost o informacijsko-komunikacijskoj tehnologiji zahtijeva da mjere kibernetičke sigurnosti budu propisane i regulirane nacionalnim zakonodavstvom – kako bi sustavi, mreže i objekti kritične infrastrukture mogli pravovremeno otkriti, spriječiti i učinkovito odgovoriti na sigurnosne prijetnje. Bitan element je i međusektorska usklađenost koja zahtijeva dobro koordinirane upravljačke i sigurnosne mehanizme.

Iako nisu svi pojedinci žrtve kibernetičkog kriminala, još uvijek su u opasnosti. Zločini počinjeni iza računala loša su strana 21. stoljeća. Uz razvoj tehnologije, kriminalci ne moraju pljačkati banke, niti moraju biti vani da bi počinili bilo kakav zločin. Kibernetički kriminalci imaju sve što im je potrebno nadohvat ruke. Njihovo oružje više nije oružje; napadaju pokazivačima miša i lozinkama.

Kritična infrastruktura je temelj o kojem ovise svakodnevne vitalne društvene i ekonomske funkcije, a poremećaj ili gubitak bilo kojeg elementa kritične infrastrukture ima potencijal ozbiljno utjecati na naše živote. Zajednički rad i razmjena dobrih praksi, pristupa i iskustava pomoći će u promicanju i poboljšanju sigurnosti i otpornosti kritične infrastrukture. Industrije uvijek traže rješenja za poboljšanje performansi i stabilnosti svojih sustava, tolerancije grešaka, sigurnosti i isplativosti. Suvremeno društvo ne uspijeva nastaviti svoju funkcionalnost ako njegove kritične infrastrukture ne funkcioniraju. Kibernetička sigurnost važna je briga u kritičnim infrastrukturama temeljenim na SCADA sustavima i ti su sustavi stalno pod prijetnjama. Osim prijetnji okolišu, sigurnosne mjere kritične infrastrukture moraju se nositi sa sofisticiranim kibernetičkim napadima.

SCADA se koristi za upravljanje i kontrolu kritičnih infrastruktura koje pružaju osnovne usluge građanima zemlje. Većinu kritičnih infrastruktura kontroliraju sustavi upravljanja kao što je SCADA. Kritične infrastrukture vitalne su i vrlo važne za društvo. Ako je SCADA sigurnosno

ugrožena, doći će do katastrofalnih posljedica na život društva. Ekonomija će biti pogođena. To će utjecati na okoliš i naposljetku na život. Ranjivosti ili prijetnje potrebno je identificirati i popraviti jer inače može doći do napada koji će imati katastrofalne učinke na društvo. Važnost SCADA sustava je automatizacija. To omogućuje organizaciji predviđanje optimalnog odgovora na izmjerene uvjete i automatsko izvršavanje tih odgovora svaki put te se time gotovo eliminiraju ljudske pogreške.

Sveučilište
Sjever

SVEUČILIŠTE
SJEVER

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, IRA MATAIĆ pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog rada pod naslovom CYBER SECURITY – ZAŠTITA KRITIČNE INFRASTRUKTURE te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
Ira Mataić

Mataić

(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, IRA MATAIĆ neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog rada pod naslovom CYBER SECURITY – ZAŠTITA KRITIČNE INFRASTRUKTURE čiji sam autor/ica.

Student/ica:
Ira Mataić

Mataić

(vlastoručni potpis)

7. LITERATURA

Knjige:

1. Božinović, D. (2016) Globalna sigurnost : sigurnosni izazovi u 21. stoljeću. Zagreb: Narodne novine.
2. Christen, M., Gordijn, B., Loi, M. (2019) The Ethics of Cybersecurity. Njemačka: Springer.
3. Colbert, J. M. E. (2016) Cyber-security of SCADA and Other Industrial Control Systems. 1sr ed. Njemačka: Springer
4. Datt, S. (2016) Mrežna forenzika : zaštitite mrežu od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera. Zagreb: Dobar plan.
5. Johnson, A. T. (2015) Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. USA: Webster University.
6. Maglaras, L., Kantzavelou, I., Ferrag, A. M. (2021) Cyber Security of Critical Infrastructures. Švicarska: MDPI.
7. Marcus, M. K. (2020) The Security of Critical Infrastructures: Risk, Resilience and Defense. Njemačka: Springer.
8. Mihaljević, B. (2019) Koncepti kriznog upravljanja i kritične infrastrukture. Zagreb: Hrvatska udruga menadžera sigurnosti.
9. Mihaljević, B., Ostojić, A. (2019) Koncepti kriznog upravljanja i kritične infrastrukture. Zagreb: uhms.
10. Mikac, R., Cesarec, I., Larkin, R. (2018) Kritična infrastruktura: Platforma uspješnog razvoja sigurnosti nacija. Zagreb: Jesenski i Turk.
11. Mitrevske, M., Mileski, T., Larkin, R., Vatter, M., Mikac, R. (2019) Kritične infrastrukture. Skopje: Friedrich Ebert.
12. Muftić, S. (1979) Sigurnost kompjutorskih sistema. Sarajevo: Zavod za ekonomsko planiranje.
13. Rass, S., Schauer, S., Konig, S., Zhu, Q. (2020) Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach. 1st ed. Njemačka: Springer.
14. Ross, A. (2019) Industrije budućnosti. Zagreb: Mate.
15. Thomas, S. M., McDonald, D. J. (2020) Power System SCADA and Smart Grids. CRC Press

E knjige:

1. CISA (2019) Critical Infrastructure Security and Resilience. Dostupno na: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf (9. kolovoz 2022.)
2. Klaić, A., Perešin, A. (2011) Koncept regulativnog okvira informacijske sigurnosti. Velika Gorica: University of Applied Sciences Velika Gorica. https://bib.irb.hr/datoteka/521742.AK_AP_Koncept_regulativnog_okvira_inf_sig_DKU_032011.pdf (10. kolovoza 2022.)
3. Matika, D., Poljanec-Borić, S. (2009) Kritična infrastruktura u Hrvatskoj: Prema novom sustavu sigurnosti i zaštite. Zagreb: Institut društvenih znanosti Ivo Pilar. Dostupno na: https://www.pilar.hr/wp-content/images/stories/dokumenti/kriticna_infrastruktura/eski_knjiga_cd_003.pdf (8. kolovoza 2022.)
4. Tatalović, S. (2009) Energetska sigurnost i zaštita kritične infrastrukture: utjecaj na politike nacionalne sigurnosti. Zagreb: Institut za istraživanje i razvoj obrambenih sustava MORH-a i Institut društvenih znanosti Ivo Pilar. Dostupno na: https://www.pilar.hr/wp-content/images/stories/dokumenti/kriticna_infrastruktura/eski_knjiga_cd_027.pdf (9. kolovoza 2022.)

Internet:

1. cisa.gov Dostupno na: https://www.cisa.gov/water-and-wastewater-systems-sector (10. kolovoza 2022.)
2. cyberwatching.eu (2022) Dostupno na: https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/critical-infrastructure (10. kolovoza 2022.)
3. energy.eu (2018) Dostupno na: https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en (9. kolovoza 2022.)
4. federaltimes.com (2016) Dostupno na: https://www.federaltimes.com/smr/critical-infrastructure/2016/07/11/communications-a-rapidly-evolving-threat-environment/ (10. kolovoza 2022.)
5. itgovernance (2020) Dostupno na: https://www.itgovernance.co.uk/what-is-cybersecurity (8. kolovoza 2022.)
6. kaspersky (2022) Dostupno na: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (8. kolovoza 2022.)

7. techtarget (2019) Dostupno na: https://www.techtarget.com/searchsecurity/definition/cybersecurity (8. kolovoza 2022.)
8. waterworld.com (2005) Dostupno na: https://www.waterworld.com/home/article/16190328/role-of-scada-in-securing-critical-infrastructure (11. kolovoza 2022.)
9. weforum.org (2022) Dostupno na: https://www.weforum.org/agenda/2022/05/securing-systemically-important-critical-infrastructure/ (9. kolovoza 2022.)
10. zakon.hr (2013) Dostupno na: https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama (8. kolovoza 2022.)

SLIKE