METODE ZAŠTITE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA OD ŠTETNIH UTJECAJA IZ MREŽNE OKOLINE U KONTEKSTU SIGURNOSTI I ZAŠTITE

Jandrok, Karlo

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite
Specijalistički diplomski stručni studij sigurnosti i zaštite

Karlo Jandrok

METODE ZAŠTITE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA OD ŠTETNIH UTJECAJA IZ MREŽNE OKOLINE U KONTEKSTU SIGURNOSTI I ZAŠTITE

ZAVRŠNI RAD

Karlovac, 2021.

Karlovac University of Applied Sciences
Safety and Protection Department
Professional graduate study of Safety and Protection

Karlo Jandrok

METHODS OF PROTECTION OF INFORMATION AND COMUNICATION SYSTEMS FROM HARMFUL IMPACTS FROM THE NETWORK ENVIRONMENT IN THE CONTEXT OF SECURITY AND PROTECTION

FINAL PAPER

Karlovac, 2021.

Veleučilište u Karlovcu
Odjel Sigurnosti i zaštite
Specijalistički diplomski stručni studij sigurnosti i zaštite

Karlo Jandrok

METODE ZAŠTITE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA OD ŠTETNIH UTJECAJA IZ MREŽNE OKOLINE U KONTEKSTU SIGURNOSTI I ZAŠTITE

ZAVRŠNI RAD

Mentor:
dr. sc. Damir Kralj, prof. v. š.

Karlovac, 2021

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J. J. Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički diplomski stručni studij sigurnosti i zaštite
(označiti)
Usmjerenje: Zaštita od požara Karlovac, 12.02.2020.

ZADATAK ZAVRŠNOG RADA

Student: Karlo Jandrok Matični broj: 0420417004

Naslov: METODE ZAŠTITE INFORMACIJSKO-KOMUNIKACIJSKIH SUSTAVA OD ŠTETNIH UTJECAJA IZ MREŽNE OKOLINE U KONTEKSTU SIGURNOSTI I ZAŠTITE

Opis zadatka:

- na osnovi dostupnih izvora te vlastitih iskustava i saznanja, analizirati aktualne vrste štetnih utjecaja koje prijete sa strane globalne mreže (interneta) poslovnim i osobnim informacijsko-komunikacijskim sustavima;
- analizirati dostupne metode i sredstva zaštite od prodora utjecaja, kao i neke od dostupnih oblika sigurnosne politike, koji obuhvaćaju metode u sredstva za prevenciju ugroze, kao i scenarij sanacije već nastale štete, te analizirati u kojoj mjeri su ove aktivnosti obuhvaćene aktualnom zakonskom regulativom;
- kako u kontekstu sigurnosti i zaštite ovakvi utjecaji mogu ugroziti život, zdravlje i materijalne vrijednosti u raznim područjima ljudske djelatnosti, na osnovi prethodnih analiza, dati procjenu postojećeg stanja i predložiti mogućnosti poboljšanja.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
12.02.2020.	10.09.2021.	17.09.2021.

Mentor: Predsjednik ispitnog povjerenstva:

dr. sc. Damir Kralj, prof. v.š. dr. sc. Vladimir Tudić, prof. v.š.

PREDGOVOR

Izjavljujem da sam rad izradio samostalno korištenjem navedenih pisanih i mrežnih izvora te vlastitih iskustava.

Zahvaljujem se profesorima Veleučilišta u Karlovcu, naročito mom mentoru dr.sc. Damiru Kralju, prof.v.š. na suradnji, pomoći, stručnim savjetima i smjernicama koje su mi puno pomogle u izradi ovog završnog rada.

Također se zahvaljujem svojoj obitelji i prijateljima koji su me cijelo vrijeme ohrabrivali i poticali te bili uz mene tijekom cijelog školovanja i u svakom novom izazovu.

SAŽETAK

Informacijsko komunikacijski sustavi sastoje se od više različitih elemenata koji imaju za cilj funkcioniranje cjeline na najbolji mogući način i za svrhu koja je unaprijed određena, a bavi se prikupljanjem, obradom i distribucijom podatka. Visoka tehnologija u mnogočemu donosi velike prednosti u pogledu lake dostupnosti, smanjivanja geografskih prepreka i slično, ali također se može iskoristiti u svrhu ostvarivanja koristi kroz metode koje nisu dopuštene poput krađe ili promjene podataka s ciljem nanošenja štete, smanjivanja dostupnosti usluge kroz zagušenje mreže i slično. Zbog toga je važno usmjeriti pažnju na metode zaštite s kojima se rizik može smanjiti na neku prihvatljivu razinu. U Hrvatskome vatrogastvu su razvijeni sljedeći informacijski sustavi, servisi i alati: VATROnet, Interaktivan baza opasnih tvari, Sustav za praćenje vozila i GIS alati, Sustav za uzbunjivanje, Upravljanje vatrogasnim intervencijama i Središnji portal internet stranica.

Ključne riječi:

Informacijsko komunikacijski sustav, metode zaštite, štetni utjecaj, informacijski sustavi u vatrogastvu

SUMMARY

Information and communication systems consists of many different elements that need to ensure functioning in the most efficient possible way and for the purpose that is already predetermined. High tech brings a lot of advantages in the area of easy access and decreasing geographical obstacles. However, it can still be used in taking advantage in a negative way through theft or altering information with an aim to inflict damage, limit accessibility or network congestion. That is the reason why it is important to focus on protection methods in order to minimize the risk level to an acceptable rate. The following information systems, services and tools have been developed in the Croatian Fire Brigade: VATROnet, Interactive database of hazardous substances, Vehicle tracking system and GIS tools, Alarm system, Fire intervention management and the website of the Middle Portal.

Keywords:

Information communication system, protection methods, harmful impact, information system at fire service

SADRŽAJ

1. UVOD

Nagli i brz razvoj tehnologije omogućio nam je mnogo prednosti, a jedna od njih je i svakodnevno korištenje interneta za različite svrhe, od razonode i zabave pa sve do posla. Jedan od potencijalnih nedostataka su i tzv. mrežno temeljene prijetnje. Stil života se prije nije toliko temeljio na internetu, pa takve prijetnje nisu dolazile do izražaja. Ali sada kada su se vremena i navike promijenile, promijenili su se i načini i metode preko kojih nas neka osoba može ugroziti. Neke od potencijalnih prijetnji se tiču korištenja tuđih osobnih podataka zbog stjecanja koristi. Hrvatska vatrogasna zajednica je razvila informacijske sustave, servise i alate, a to su: Središnji portal internet stranica , VATROnet, Interaktivan baza opasnih tvari, Sustav za praćenje vozila i GIS alati, Upravljanje vatrogasnim intervencijama i Sustav za uzbunjivanje. Razvojem informacijskih sustava i alata koji su prvenstveno namijenjeni vatrogascima da bi im se olakšao rad prilikom intervencija, prikupljanja i obrade podataka dolazi do opasnosti da se takve aplikacije iskoriste u zlonamjerne svrhe. U svrhu zaštite potrebno je koristiti sva dostupna sredstva zaštite i prevencije koja su raspoloživa.

1.1. Predmet i cilj rada

Cilj ovog rada je prikazati i analizirati opasnosti koje prijete prilikom korištenja informacijsko komunikacijskih sustava, prijetnje i posljedice koje se mogu dogoditi. Pošto se u radu osvrćemo na vatrogasni sustav i njegove aplikacije, kroz rad ću pokušati objasniti kakve se posljedice mogu dogoditi ukoliko dođe do neželjenih situacija kod korištenja informacijsko komunikacijskih sustava.

1.2. Izvori podataka

Podaci za izradu ovoga rada prikupljani su iz više vrsta izvora: pregledavani su zakoni u domeni informacijske sigurnosti, podaci dostupni na web stranicama Hrvatske kao i na stranim web stranicama.

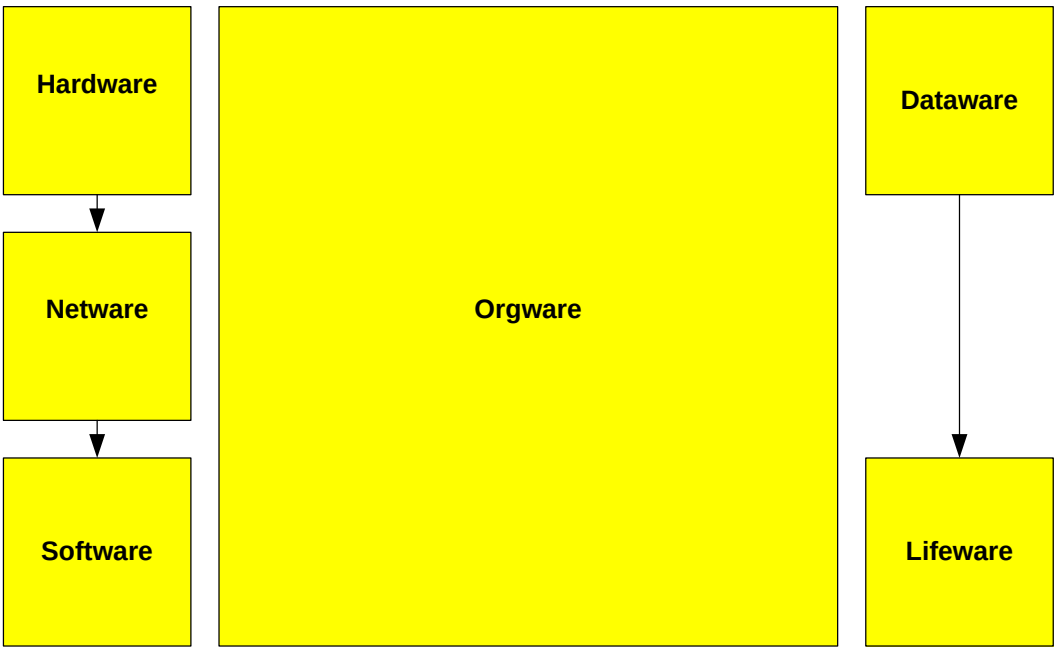
2. OSNOVE INFORMACIJSKIH SUSTAVA

Kako bi se što bolje objasnili sigurnosni aspekti i mjere zaštite informacijskih sustava, te općenito informacijskih sustava, potrebno je pobliže objasniti neke osnovne pojmove, kao što su:

- Informacija je podatak koji njegovom primatelju posreduje neku relevantnu novost. [1] To je zapravo skup podataka (obično u obliku slova, znakova, zvukova ili simbola) koji imaju neko zajedničko značenje.
- Sustav – općenito se opisuje kao skup određenih elemenata koji su međusobno povezani te tako tvore svrsishodnu cjelinu odnosno sam sustav. Svaki promatrani sustav može se opisati i kao podsustav određenog šireg, odnosno većeg sustava. Kao primjer nekog sustava mogli bi navesti jednu poslovnicu određene banke u nekome gradu, koja je ujedno i podsustav centralne banke koja može biti u nekom drugom gradu. Svaki sustav okružen je svojom okolinom, s kojom je u međudjelovanju.
- Informacijski sustav – je dio nekog tehnološkog i/ili organizacijskog stvarnog sustava čija je svrha permanentno opskrbljivanje potrebnim informacijama svih razina njegovog upravljanja i odlučivanja. Informacijski sustav je uvijek podsustav nekog organizacijskog sustava, koji kroz svoje temeljne aktivnosti tj. prikupljanje, obradu, pohranjivanje i distribuiranje informacija, omogućuje upravljanje tim organizacijskim sustavom ili nekim njegovim podsustavom. [1]

2.1. Elementi informacijsko komunikacijskog sustava

Informacijsko – komunikacijski (IK) sustav je spoj više različitih elemenata koji zajednički čine cjelinu. Svaki dio sustava ima svoju ulogu i bez njega sustav ne bi mogao funkcionirati na zadovoljavajući način.



Slika 1. Prikaz elemenata Informacijsko – komunikacijskog sustava (izvor: autor)

Slika 1. prikazuje prikaz elemenata IK sustava napravljen preko MS Visia. MS Visio je program za izradu i modeliranje različitih sustava, dijagrama i grafikona. Cjelokupni sustav je zamišljen kao jedan veliki pravokutnik koji se sastoji od više manjih pravokutnika. Svi manji dijelovi su sadržani unutar organizacijskog dijela informacijskog sustava. Može se vidjeti kako mrežni dio informacijskog sustava služi kao most između sklopovskog i programskog dijela sustava. Na drugoj strani nalaze se podatkovni dio sustava i ljudski faktor kao dio istog sustava.

U nastavku će svaki pojedinačni dio informacijskog sustava biti opisan počevši sa sklopovskim dijelom, a završivši sa ljudskim čimbenikom.

2.2. Sklopovski dio informacijsko komunikacijskog sustava

Materijalno-tehničku (engl. *hardware*) komponentu informacijskih sustava čine svi strojevi, uređaji i sredstva namijenjena isključivo ili pretežito obradi (procesiranju) podataka, odnosno informacija. [2]

Sklopovlje zapravo čini onaj dio sustava koji se može neposredno opipati. Bez njega se uspješno ne bi mogla koristiti ni komponenta softvera, jer je sama računalna

komponenta nezamisliva bez sklopovske potpore. U okviru jednog sustava, sklopovski dio čine:

- tipkovnica (žična ili bežična),
- monitor,
- miš (žični ili bežični),
- slušalice / mikrofon (odvojeni ili zajednički),
- skener,
- pisač i
- kućište.

2.3. Mrežni dio informacijsko komunikacijskog sustava

Mrežna podrška (engl. *netware*) služi za povezivanja svih elemenata sustava u cjelinu. [3]

Mrežni dio IK sustava je spona ili premosnica koja povezuje sustav sa okolinom, ali i sa drugim različitim dijelovima sustava. Drugim riječima radi se o prijenosnom mediju između sustava i okoline. Tu bi se mogli svrstati različiti mrežni i optički kabeli, ruteri, koncentratori, premosnici i prospojnici čija je zadaća ostvariti komunikaciju. U pravilu se mrežna oprema može podijeliti na aktivnu i pasivnu mrežnu opremu.

Aktivna oprema su svi elektronički uređaji koji prihvaćaju i distribuiraju promet unutar računalnih mreža tj. imaju memoriju i procesor (mrežna kartica, prospojnik, ruter), a pasivna oprema je sustav vodova (optika i bakar) koji služi za povezivanje aktivne mrežne opreme. [4]

2.4. Programski dio informacijsko komunikacijskog sustava

Software ili nematerijalna komponenta informacijskih sustava predstavlja ukupnost ljudskoga znanja ugrađenog u strojeve, opremu i uređaje, koje je samo po sebi predmet obrade ili pak diktira način obrade u sustavu. Predmet obrade su

relevantni podaci kao manifestacija činjeničnog znanja raspoloživoga u informacijskom sustavu, dok se metodološka znanja u taj sustav ugrađuju u obliku računalnih programa. [2]

Bez programske podrške ili bez *softwarea* ne može se zamisliti rad računala, a samim time i rad sustava, jer računala danas predstavljaju integralne dijelove sustava. *Software* može doći u različitim oblicima poput operativnih sustava, programa i aplikacija.

Kada se govori o operativnom sustavu tu su nezaobilazna tri operativna sustava:

- MS Windows
- Linux
- MacOS.

Operativni sustav predstavlja skup svih operacija i zadataka koji su potrebni za uspješan i automatiziran rad na računalu. Od tri navedena operativna sustava, dva su proizvodi velikih tvrtki poput Microsoft-a i Apple-a. Komercijalni proizvodi tih sustava se najčešće povezuju uz računala koje Microsoft i Apple prodaju krajnjim korisnicima. U odnosu na njih, Linux predstavlja besplatan operacijski sustav koji dolazi u različitim varijantama poput Minta ili Ubuntua.

Programi koji se koriste su raznovrsni i imaju različite funkcije, od računanja i korištenja jednostavnih računskih operacija poput zbrajanja, množenja, oduzimanja i dijeljenja, pa sve do programa poput Excela u kojima se podaci mogu spremiti, obraditi i prikazati u tablicama korištenjem različitih naprednih funkcija. Temeljna zadaća programa iz gledišta sustava je riješiti problem uz što manji utrošak vremena i sredstava. Iz današnje perspektive, klasični programi koji se izvode na računalu se mogu zamijeniti sa aplikacijama koje se također vrlo efikasno mogu koristiti na mobilnom telefonu ili tabletu. Na taj način se dobiva i mobilnost u odnosu na klasična stolna računala koja su fiksirana i lokacijski određena, a pritom se ne koristi prijenosno računalo.

2.5. Organizacijski dio informacijsko komunikacijskog sustava

Organizacijski dio IK sustava prikazuje se kao rezultat dostignuća organizacijskih znanosti te dostignuća informatike koja ima znatan utjecaj na način i tehnologiju poslovanja, te samu organizaciju.

Orgware se sastoji od organizacijskih postupaka, metoda i načina vezivanja programske podrške (eng. *Software*), sklopovlja (eng. *Hardware*) i ljudske podrške (eng. *Lifeware*) u jednu funkcionalnu cjelinu.

Svi planovi, postupci i procedure koje opisuju rad jednog sustava od najniže do najviše razine su sadržani u *orgware*-u. Detaljan opis svih aktivnosti, radnih zadaća i odgovornosti osoba koje se nalaze unutar nekog sustava također čine organizacijski dio jednog sustava.

Primjer koji najbolje može opisati organizacijski dio sustava je opis radnih zadaća vezan za trgovinu koja prodaje telekomunikacijsku opremu. Opisane radne zadaće su: davanja informacija i prodaja proizvoda, promjena tarifa, tarifnih modela i rješavanje reklamacija, prihvat proizvoda i slanje proizvoda na servis, te rad na obračunu na završetku radnog dana. Svaka opisana radna zadaća sadrži određene procedure koje trebaju osigurati uspješno izvršavanje zadaća i izbjegavanje potencijalnih problema.

2.6. Podatkovni dio informacijsko komunikacijskog sustava

Podatkovni dio sustava (eng. *Datawere*) je vezan za organizaciju baze podataka i informacijskih resursa. *Dataware* se više koristi kod velikih sustava gdje je potrebno izvršiti projektiranje baza podataka tako da ih mogu koristiti razni korisnici.[5] Tu se javljaju i problemi zaštite sustava od neovlaštenog korištenja, kao i različiti stupnjevi u ovlaštenosti u pristupu podacima i informacijama.

Podaci o svim radnim procesima, zadaćama, planovima i poslovima su neizostavan dio svakog sustava. Podatkovni dio uglavnom sadrži podatke o aktualnim i prethodnim projektima, statističke podatke vezane za uspješnost zaposlenika, kupovinu ili prodaju proizvoda i usluga, podatke o inventaru i imovini tvrtke, podatke o istraživanjima i slično.

Uloge podatkovnog i organizacijskog dijela su slične, ali i različite. U oba slučaja radi se o podacima, međutim u organizacijskom dijelu su obuhvaćeni podaci na razini cijelog sustava i svih njegovih dijelova, dok podatkovni dio sadrži sve podatkovne podatke vezane samo za taj dio sustava.

2.7. Ljudski faktor informacijsko komunikacijskog sustava

Ljudski faktor informacijskog sustava čine svi ljudi koji u bilo kojoj funkciji i s bilo kakvom namjerom sudjeluju u radu sustava i koriste rezultate njegova rada. S jedne strane, to je skupina profesionalnih informatičara koji djeluju u sustavu i njihov je brojčani udio u ukupnom ljudskom potencijalu sustava daleko manji u odnosu na drugu skupinu – skupinu korisnika rezultata rada sustava. [2]

Unutar jedne tvrtke (jednog sustava) može postojati više različitih odjela (ljudski potencijali, tajništvo, informatički odjel, uprava), a svaki od njih ima različitu zadaću za koju je netko unutar sustava zadužen. Korištenjem određenog dijela sustava ta zadaća se izvršava. Svaka osoba koja se nalazi unutar sustava ima svoju ulogu, sve uloge nisu jednako važne, međutim u danom trenutku se situacija može promijeniti, pa tako i sama važnost uloge unutar sustava.

Lifeware predstavlja stalan problem, jer odlaskom uhodanog osoblja i dolaskom novog osoblja, koje još nije sasvim upoznato sa sustavom, nastaju poteškoće u organizaciji, komunikaciji i korištenju sustava. Stoga, uvođenju novih ljudi u sustav valja posvetiti pozornost, tj. novi se djelatnici moraju upoznati sa sustavom, proći odgovarajuće tečajeve, odnosno školovanje, te mora proći stanovito razdoblje njihova prilagođavanja. To isto vrijedi i za osoblje prilikom postavljanja novog sustava, odnosno kod uvođenja nekih promjena u sustavu. [6]

3. MREŽNO TEMELJENE PRIJETNJE

Postoji puno različitih prijetnji koje su dosta raznolike i usmjerene na komuniciranja preko interneta (e-mail, društvene mreže, nagradne igre i slično) i svakodnevnih aktivnosti poput surfanja, igranja igara, internetske kupovine i slično.

U prethodnom poglavlju je opisan informacijsko – komunikacijski sustav s obzirom na sve njegove dijelove. Svaki od njegovih dijelova je ranjiv na različite prijetnje, a to se ne smije zanemariti. U nastavku će biti opisane neke od mrežno temeljenih prijetnji.

3.1. Zlonamjerni programi

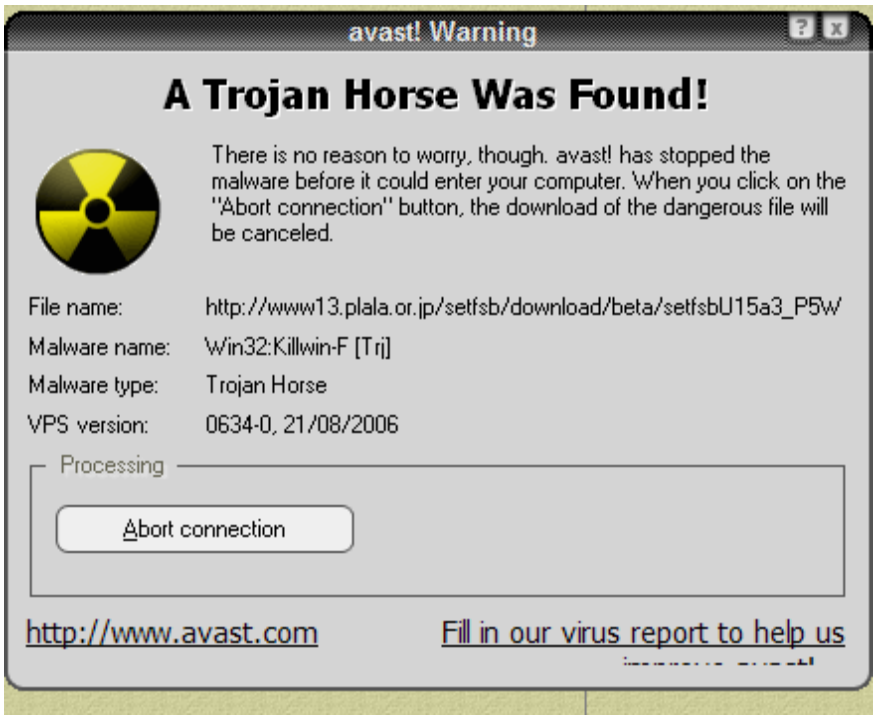
Malware je zajednički naziv za štetne ili maliciozne programe koje zlonamjerne osobe koriste kako bi pristupili podacima sa drugih računalima. Takvi su programi obično skriveni u privicima ili besplatnom sadržaju. Koriste se za niz nezakonitih radnji kao što su zaobilaženje sigurnosnih programa, krađu osobnih podataka, brisanje ili oštećivanje podataka. Postoji cijeli niz različitih štetnih programa, uključujući računalne viruse, tzv. trojanske konje, špijunske programe (engl. *spyware*) i programe za ucjenu (engl. *ransomware*). [7]

Osim manipulacijom korisnika, *malware* se ugrađuje u računalo i korištenjem sigurnosnih propusta softvera koji koristite. To znači da takav *malware* s jednog zaraženog računala na drugo može putem mreže prijeći bez ikakve interakcije s korisnikom i bez ikakve vidljive reakcije računala, ali pod uvjetom da je ciljno računalo ranjivo. [8]

Računalni virus je mali dio softvera koji se može proširiti sa jednog zaraženog računala na drugo. To je program koji može dalje mijenjati, krasti i brisati podatke sa računala ili čak sa cijelog računalnog diska. Računalni virus također može koristiti druge programe poput e-maila kako bi se lakše širio dalje.

Trojanski konj je štetni program koji je skriven unutar nekog drugog programa sa svrhom činjenja štete. Obično radi u pozadini i može uzrokovati različite oblike štete:

- izbrisati ili presnimiti podatke na zaraženom računalu,
- deaktivirati vatrozid i antivirusni program
- instalirati druge viruse.



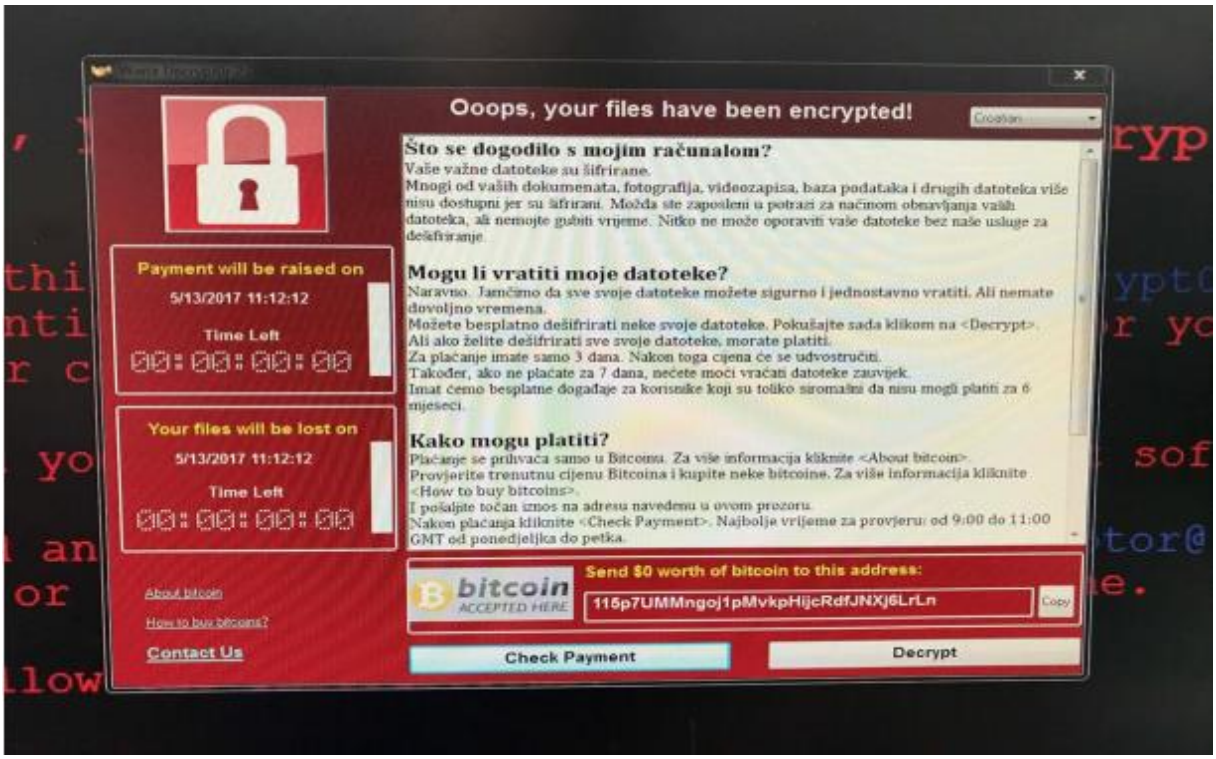
Slika 2. Upozorenje o pronalasku trojanskog konja na računalu [9]

Na slici 2. je prikazana poruka koja se može pojaviti u slučaju pronalaska trojanskog konja na računalu preko antivirusnog programa. Antivirusni programi mogu predstavljati vrlo važan alat u pronalasku i eliminaciji potencijalno sumnjivih programa.

Računalni crvi su zlonamjerni programi koji se bez sudjelovanja korisnika šire putem računalnih mreža na druga računala. Za razliku od računalnih virusa, računalni crvi na ciljanom računalu ne inficiraju datoteke te imaju sposobnost samostalnog širenja i umnožavanja samih sebe. Najčešće iskorištavaju propuste u operacijskim sustavima i programima, svojim djelovanjem uzrokuju probleme s performansama i stabilnošću računala te računalnih mreža. [10]

Špijunski program je program koji daljinski prati internetske aktivnosti koje se izvode na računalu. Te aktivnosti mogu biti različite:

- prikupljanje informacija o navikama surfanja,
- prikazivanje oglasa prema sadržaju koji zanima korisnika i
- skeniranje tvrdog diska u potrazi za bankovnim podacima ili lozinkama



Slika 3. Primjer obavijesti *ransomwarea* [11]

Na slici 3. se može vidjeti jedan primjer *ransomwarea*. Mogu se uočiti tri dijela. Prvi sadrži poruku sa objašnjenjem nastale situacije. Drugi dio je vezan za upute za ispunjavanje zahtjeva i vraćanja kontrole nad računalom, a treći i posljednji dio sadrži podatke o načinu plaćanja. U slučaju neisplate navedene svote novca u određenom vremenu spominje se sankcija u obliku brisanja podataka sa računala, trajnog zaključavanja pristupa računalu i sličnog.

3.2. Krađa podataka i identiteta preko interneta

U današnje moderno doba kada su mnoge tradicionalne stvari prenesene i u virtualni oblik (komuniciranje, obavljanje kupovine, bankarske transakcije), važno je paziti na podatke koji se koriste u tim pratećim aktivnostima. To može biti korisničko ime sa pratećom lozinkom, ali i osobni podaci potrebni za provođenje neke transakcije kao što je plaćanje računa ili kupovina (adresa, ime i prezime, broj bankovnog računa).

Ponekad se čini da za gotovo svaku aktivnost na internetu moramo smisliti lozinku i korisničko ime, te dati određene osobne podatke. To je postalo nužno jer internetske stranice žele zaštititi korisnike i njihov identitet, a neke od njih također nude i usluge društvenog umrežavanja. No, potrebno je biti na oprezu jer sa otkrivanjem prevelikog broja osobnih podataka i informacija može se postati podložan napadima zlonamjernih ljudi [12].

Pitanje se aktualizira i na društvenim mrežama, gdje se često može dogoditi pokušaj preuzimanja tuđeg identiteta kroz krađu profila sa popularne društvene mreže Facebook. Tu do izražaja u punom smislu može doći i tzv. socijalni inženjering. To je zapravo skup postupaka kojim se na različite načine želi doći do povjerljivih informacija u svrhu ispunjavanja nekog cilja.

Socijalni inženjering obuhvaća i niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći. [13]

Napadači uvijek žele ostaviti dojam legitimnosti, odnosno uvjerljivosti. Tako npr. u porukama elektroničke pošte često navedu neki poznati podatak o korisniku (najčešće njegovo ime koje može biti vidljivo iz adrese elektroničke pošte), datum rođenja itd. Napadači se najčešće pouzdaju u zakon velikih brojeva i šire velike količine poruka kako bi, koristeći socijalni inženjering, iskoristili povjerenje dijela ciljanih korisnika i na taj način ih natjerali da ispune njihov cilj. Mora se napomenuti kako se napadači mogu usmjeriti prema prikupljanju detaljnih informacija vezanih uz zasebnog korisnika umjesto prikupljanja osnovnih informacija o velikom broju korisnika čime otvaraju sebi mogućnost slanja mnogo osobnije poruke elektroničke

pošte koja može biti vezana uz specifične interese korisnika, privatne informacije te bliske ljude iz okoline. Tako umanjuju broj poslanih poruka, ali povećavaju dojam legitimnosti poruke čime uvećavaju šansu uspješnog ostvarivanja kontakta sa žrtvom.[13]

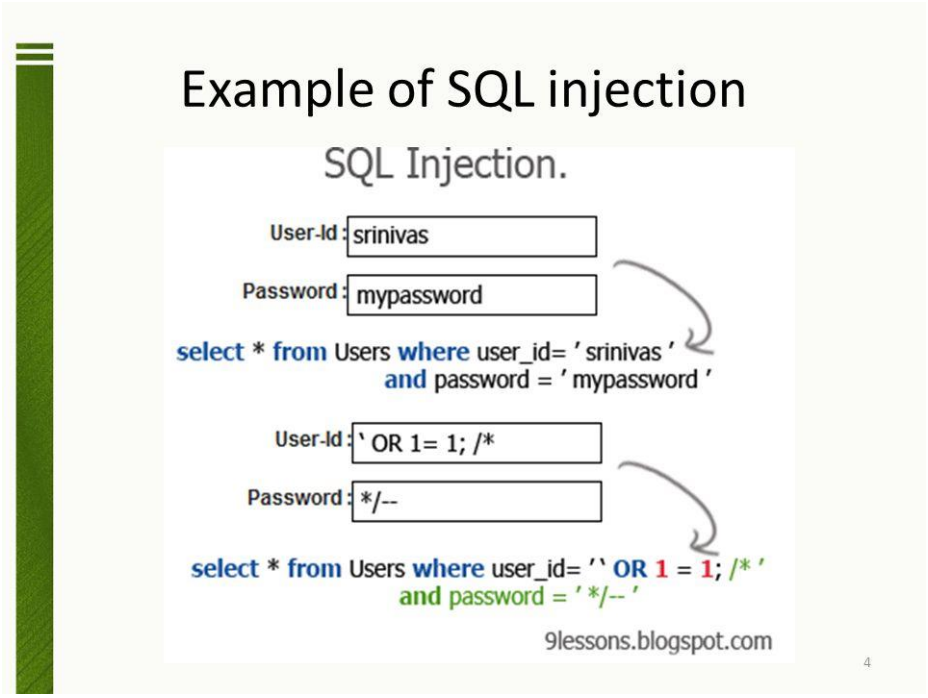
3.3. Hakiranje

Riječ hakiranje dolazi od engleske riječi *hacker*, koja označava osobu koja ima za cilj stvoriti štetu, ukrasti povjerljive informacije ili novac korištenjem neke vrste malicioznog softvera, umetanjem malicioznog sadržaja ili nekom drugom metodom. [14]

Haker može djelovati kako bi ostvario neki cilj, ali može i predstavljati plaćenika koji je unajmljen kako bi obavio neki točno određeni posao. Među hakerima postoji podjela na one koje izazivaju štetu, ali i na one koji rade na prevenciji i spriječavanju štete. Oni svoje znanje koriste kako bi otkrili potencijalne ranjivosti u programima i web stranicama, tako da bi se u konačnici takve stvari mogle sanirati i prestale predstavljati sigurnosni rizik.

Postoji više različitih metoda kojima hakeri mogu ugroziti neki sustav, ali u radu će biti predstavljene samo dvije metode: SQL (*Structured Query Language* - SQL) umetanje i DoS (*Denial of Service* – DoS) napadi ili napadi uskraćivanjem resursa.

Napad umetanjem SQL koda je jedan od 10 najopasnijih napada na web stranice. Sve web stranice koje za svoj rad koriste bazu podataka mogu biti potencijalna meta. Ovi napadi utječu na povjerljivost, autentikaciju, autorizaciju i integritet podataka baze podataka. Različite web stranice mogu postati potenijalno ranjive na ovaj oblik napada, a najčešći cilj napada je krađa korisničkih podataka zapisanih u bazi podataka, poput podataka o kreditnim karticama ili adresama elektroničke pošte. Napad je moguć zbog nedovoljnih provjera korisničkih podataka, poput podatka o korisničkom imenu kojeg korisnik upisuje prilikom prijave. Napadač može iskoristiti polje za unos kako bi umetnuo posebno oblikovani SQL kod i tako izveo napad. [15]



Slika 4. Primjer umetanjem SQL koda [16]

Najpoznatiji SQL kod čije umetanje može izazvati napad je oblika „' OR 1=1“, a koji je prikazan na slici 4, a koristi se za ispitivanje ranjivosti *web* stranice na napad umetanjem SQL koda ili za zaobilaženje prijave. Napadi često nižu nekoliko SQL naredbi pomoću znaka točka-zarez, koriste znak dvostrukih crtica koje označavaju komentar u SQL kodu. [17]

Napadač pokušava zaobići polje za prijavu. SQL upit uz poznato ime korisnika i lozinku (kod korisnika "srinivas" uz lozinku "mypassword") bi imao ovaj oblik: Koristi se SQL naredba za odabir SELECT kojom se iz tablice korisnici ispisuju sva korisnička imena i lozinke koji odgovaraju gore navedenom uvjetu srinivas i mypassword. Kada su korisnički podaci nepoznati, napadač se koristi sa sljedećim upitom: Select * iz tablice korisnika u kojima je korisničko ime OR 1=1;/* uz lozinku */--. Na taj način prikazati će se svi podaci o korisnicima, jer se polje lozinke preskače znakovima --, a tvrdnja 1=1 je uvijek točna.

Napadi uskraćivanjem resursa (eng. denial of service, DoS) su aktivnosti poduzete od strane zlonamjernih korisnika sa ciljem onemogućavanja ispravnog funkcioniranja različitih računalnih i mrežnih resursa čime određene usluge postaju nedostupne. Često korišten izraz u hrvatskoj literaturi je i DoS stanje, a odnosi se na vremenske trenutke nepravilnog rada ili potpune onemogućenosti funkcioniranja

aplikacija i računalnih ili mrežnih usluga. Činjenica da je internet izgrađen od konačnog broja mrežnih komponenata te da računalni sustavi ne raspolažu s neograničenim količinama procesne moći, pridonosi ishodima ovakvih napada. [18]

Najbolji primjer DoS napada je pokušaj istovremenog otvaranja određene web stranice sa jako velikog broja računala. Kao rezultat napada stranica postane nedostupna, čime je učinjena šteta svima koji su u tom trenutku željeli pristupiti stranici. Ponekad web stranice nemaju na raspolaganju dovoljno resursa za primanje jako velikog zahtjeva korisnika (prodaja ulaznica za velike događaje poput koncerata ili nogometnih utakmica) u jako kratkom vremenu. Tada se ipak ne radi o napadu uskraćivanjem resursa, već su jednostavno osigurani resursi nedovoljni za primanje tako velikog broja zahtjeva.

3.4. Iskorištavanje ranjivosti programa

Izrada programa je prilično složen i nerijetko dugotrajan proces u kojemu do konačne verzije programa mora proći jako puno krugova testiranja. Tek nakon što je sve u najboljem redu, program se izdaje na tržište i može se koristiti. Međutim, neke greške koje nastaju unutar programa nisu odmah vidljive, već se pojavljuju nakon točno odgovarajućih događaja. Njihov ishod može često biti poguban i izrazito štetan ako se brzo ne otkrije. Hakeri nastoje iskoristiti sve poznate i nepoznate ranjivosti programa kako bi ostvarili svoj cilj. Nepoznate ranjivosti su pritom vrijednije zato što su one nepoznate za veliki broj korisnika, a posebno ako se radi o programu koji je jako raširen.

Najčešće se ranjivosti pojavljuju zbog nedovoljne kvalitete programskog koda. Proizvođač softvera ne radi dovoljno testova kojim bi otkrio pogreške u softveru prije njegove distribucije. Osim nedovoljne kvalitete programskog koda ranjivosti se mogu pojaviti i zbog neprikladnog korištenja softvera. Ako korisnik neispravno podesi softver ili ne slijedi sigurnosne smjernice za njegovu uporabu, može potencijalnim napadačima otvoriti cijeli niz ranjivosti bez obzira na to koliko je softver kvalitetan. Postoji mnoštvo različitih vrsta ranjivosti. Iskorištavajući pojedine ranjivosti napadač može dobiti kontrolu nad sustavom, s njega ukrasti podatke ili ga jednostavno učiniti nedostupnim. Posebno su opasne ranjivosti koje napadaču omogućuju izravnu

kontrolu nad računalnim sustavom. Napadač ih može iskoristiti kako bi na računalo postavio neki oblik zlonamjernih programa i proširio se na druga računala. [19]

4. INFORMACIJSKI SUSTAV U VATROGASTVU U REPUBLICI HRVATSKOJ

Razvojem informacijskih tehnologija i vatrogastva pojavila se potreba za uvođenjem informatizacije u procese vatrogasne djelatnosti. Uvjeti za uspješno korištenje informacijsko-komunikacijskih sustava i alata su osim aplikacija i odgovarajuće infrastrukture, standardizacija poslovnih procesa u vatrogastvu, dobra educiranost korisnika, te kvalitetna korisnička podrška. Hrvatska vatrogasna zajednica ulaže velike napore kako bi se ovi uvjeti osigurali vatrogasnim organizacijama diljem Republike Hrvatske, a razvoj ovih alata pokazao se kao prilika za uređivanje nekih vatrogasnih procesa, te omogućio suradnju s drugim državnim i znanstveno-istraživačkim institucijama. [20]

Do danas su razvijeni sljedeći informacijski sustavi i alati:

- VATROnet - središnja baza podataka koja sadrži informacije o svim vatrogasnim postrojbama, članovima, vozilima i opremi
- Sustav za praćenje vozila i GIS alati - skup alata koji omogućuju praćenje i navođenje vatrogasaca tijekom vatrogasnih intervencija
- Interaktivna baza opasnih tvari - baza koja sadrži podatke o opasnim tvarima, uključujući i opise na koji način njima sigurno postupati
- Sustav za uzbunjivanje - aplikacija koja omogućuje uzbunjivanje vatrogasaca na vatrogasne intervencije
- Upravljanje vatrogasnim intervencijama - glavni operativni alat u kojeg su integrirani svi ostali sustavi i koji pruža podršku tijekom vođenja vatrogasnih intervencija na svim razinama upravljanja
- Središnji portal internet stranica - sustav putem kojeg bilo koja vatrogasna postrojba ili zajednica u Hrvatskoj može besplatno dobiti vlastitu internet stranicu i administracijske ovlasti za njezino uređivanje [20]

4.1. VATROnet

VATROnet je središnja baza podataka Hrvatske vatrogasne zajednice u koju se pohranjuju podaci o vatrogasnim organizacijama, njihovim članovima, zaposlenicima, opremi, vozilima i aktivnostima. VATROnet se koristi primarno kao alat za evidenciju podataka i generiranje različitih vrsta izvještaja i statistike. Uz to, aplikacija se koristi u procesu dodjele odlikovanja, izradi vatrogasnih iskaznica, te administraciji vatrogasnih osposobljavanja i vatrogasnih natjecanja. . Podaci uneseni u VATROnet koriste se u ostalim aplikacijama Hrvatske vatrogasne zajednice, zbog čega je izrazito je važno da su podaci uneseni u VATROnet ispravni. Velika pažnja je posvećena zaštiti podatka unutar sustava VATROnet, gdje svi korisnici zavisno o svojim pravima mogu hijerarhijski pristupati podacima. Sustav je usklađen s zakonskim propisima koji reguliraju zaštitu osobnih podataka. [21]

4.2. Sustav za praćenje vatrogasnih vozila i GIS alati

Sustav omogućuje operaterima uvid u trenutne pozicije vatrogasnih vozila i osoba na GIS podlozi. Osim toga, moguće je navoditi i slati poruke na vozila te generirati izvještaje, povijest kretanja i rekonstrukciju intervencija. GIS podloge moguće je uređivati alatima "Map Editor" i "Mobile Data Collection" Korisnički račun definiran je skupom vozila, odnosno uređaja za praćenje čije kretanje se može pratiti kroz aplikaciju. Korisnici mogu pratiti samo vozila unutar vlastite vatrogasne organizacije te vozila hijerarhijski podređenih vatrogasnih organizacija. Vatrogasne organizacije mogu sukladno svojim potrebama zatražiti bilo koji broj korisničkih računa za praćenje vozila u njihovoj ovlasti. Karte i slojevi mogu se uređivati kroz zasebne aplikacije "Map Editor" i "Mobile Data Collection" čiji vlasnik je GIS Cloud d.o.o., a Hrvatska vatrogasna zajednica nabavlja po 21 licencu koje dodjeljuje vatrogasnim zajednicama županija/Grada Zagreba. Vatrogasne zajednice i druge organizacije mogu po potrebi iz vlastitih sredstava nabavljati i dodatne licence za aplikacije "Map Editor" i "Mobile Data Collection". Korisničke račune dodjeljuje i ukida Hrvatska vatrogasna zajednica, na zahtjev vatrogasne organizacije koja u svoja vozila ima ugrađene odgovarajuće uređaje za praćenje i navođenje vozila. [22]

4.3. Interaktivna baza opasnih tvari

Aplikacija je rađena kao web portal koji služi javnosti/građanstvu kao izvor općih informacija o opasnim tvarima (osnovne opasnosti, koliko koje tvari smiju skladištiti itd.) i hitnim službama kao pomoć pri rukovanju opasnim tvarima na intervencijama. Ideja aplikacije je da na jednom mjestu budu objedinjene sve informacije, pravilnici, zakoni i iskustva o opasnim tvarima i njihovim sigurnim rukovanjem, sigurnosno-tehnički listovi, ERI kartice, evidencija opreme za opasne tvari. [23]

4.4. Upravljanje vatrogasnim intervencijama

Upravljanje vatrogasnim intervencijama, odnosno UVI, zajednički je projekt Hrvatske vatrogasne zajednice i Državne uprave za zaštitu i spašavanje kojim se za vatrogasne intervencije želi postići standardizacija radnih procesa, izrada jedinstvenog sustava pohrane, obrade i distribucije informacija, veća efikasnost izvješćivanja, te ekonomičnost u održavanju programskih rješenja, uređaja i opreme. Glavni rezultat projekta je istoimena aplikacija koja se daje besplatno na korištenje vatrogasnim postrojbama i operativnim centrima. Aplikacija je operativni alat i kao takva koristi se primarno kao podrška radnim procesima koji se odvijaju tijekom vatrogasne intervencije, no omogućuje i retroaktivan unos podataka o intervencijama, te naprednu analizu prikupljenih podataka.

Sustav UVI možemo gledati kroz tri segmenta:

- Standardizacija poslovnih procesa (propisivanje radnih procesa: priprema za vatrogasnu intervenciju, upravljanje intervencijom, analitička i izvještajna obrada)
- Aplikacija UVI (Softversko rješenje koja pokriva radne procese, te integracija sa svim ostalim sustavima)
- ICT infrastruktura (Podrška radu informacijskog sustava, vlastita infrastruktura, koncept „*black box*”) [24]

4.5. Sustav za uzbunjivanje

Aplikacija je namijenjena za uzbunjivanje vatrogasaca za vatrogasne intervencije, te obavještavanja vatrogasaca za razne druge aktivnosti. Uzbunjivanje se radi putem glasovne poruke ili SMS-a. Grupe za uzbunjivanje, zajedno s ostalim podacima, uređuju se u aplikaciji VATROnet. Aplikacija je zamišljena da se koristi preko internet preglednika računala na adresi http://uvi.193.hr/evatrogasci/web, no samo uzbunjivanje može se vršiti i putem telefonskih uređaja. Tijekom uzbunjivanja, operater odmah dobiva povratnu informaciju od uzbunjenih osoba koje su potvrdile dolazak, a nakon intervencije moguće je generirati razne izvještaje i statističke podatke. Aplikacija je integrirana u sustav Upravljanje vatrogasnim intervencijama i preporuka je da se aplikacija koristi kao dio tog sustava, no aplikaciju je moguće koristiti i zasebno. Korisnički računi vatrogasnim organizacijama daju se besplatno, a plaća se korištenje uzbunjivanja. Trošak korištenja ovisi o količini poslanih SMS-ova i potrošenih minuta razgovora. Za mobilne brojeve unutar VPN-a cijena korištenja je 0 kn/min. Velika je pažnja posvećena telekomunikacijskog infrastrukturi, kako bi sustav nesmetano radio. [25]

4.6. Održavanje programskih komponenti

Održavanje programskih komponenti odnosi se na ispravljanje pogrešaka u programu, nadogradnje aplikacija, gašenje i stavljanje novih verzija aplikacija u produkciju, te osiguravanje sigurnosnih kopija baze podataka i programskog koda. [22]

4.6.1. Plan gašenja aplikacije radi održavanja

Ukoliko se planira privremeno gašenje aplikacije, korisnici se o tome obavješćuju, u pravilu, najmanje 7 dana prije samog gašenja ukoliko se radi o redovitom održavanju, odnosno 1 dan ukoliko se radi o ispravljanju pogrešaka visokog prioriteta (pogreške zbog kojih je rad bitno otežan). Obavijest sadrži predviđeno vrijeme do kada aplikacija neće biti dostupna. Ukoliko se ispravlja pogreška visokog prioriteta, koja potpuno onemogućuje rad, korisnici neće nužno biti obavješteni prije gašenja aplikacije. Nakon završetka održavanja, korisnici se obavješćuju o

nadogradnjama, ispravcima, te ostalim radovima provedenim nad aplikacijom, bazom ili serverom, a koji utječu na daljnji rad korisnika s aplikacijom. [22]

4.6.2. Sigurnosne kopije

Kopije izvornog i izvršnog koda rade se nakon svake nadogradnje aplikacije i čuvaju do sljedeće nadogradnje. Sigurnosne kopije baze podataka rade se svaka 24 h i čuvaju se najmanje 7 dana. Kopije se čuvaju na lokaciji fizički udaljenoj od poslužitelja na kojem se nalazi sama aplikacija. [22]

4.6.3. Održavanje fizičkih komponenti infrastrukture

Održavanje fizičkih komponenti infrastrukture odnosi se na održavanje računalne i mrežne opreme, te osiguravanje međusobne povezanosti sustava i dostupnosti krajnjim korisnicima. Infrastruktura se može podijeliti na centralnu infrastrukturu i infrastrukturu krajnjih korisnika. Zbog specifičnosti u održavanju, infrastruktura sustava Upravljanje vatrogasnim intervencijama može se podijeliti i na infrastrukturu u vatrogasnim operativnim centrima (VOC/ŽVOC). [22]

4.6.4. Održavanje centralne infrastrukture

Centralna infrastruktura nalazi se na središnjoj lokaciji koju osigurava Hrvatska vatrogasna zajednica. Centralna infrastruktura uključuje poslužitelje na kojima su pokrenute aplikacije, te mrežnu i ostalu opremu kojom se osigurava neprekidan rad i dostupnost aplikacija korisnicima. Održavanje centralne infrastrukture osigurava Hrvatska vatrogasna zajednica. [22]

5. VRSTE PRIJETNJI INFORMACIJSKO–KOMUNIKACIJSKOM SUSTAVU NA PRIMJERU IZ VATROGASTVA

Vatrogasni informacijski sustavi svakodnevno se susreću s raznovrsnim vrstama prijetnji i sigurnosnih ugroza.

Prema raznim istraživanjima, ustanovljeno je da je najčešća vrsta prijetnje prema informacijskim sustavima ljudski faktor, odnosno ljudska nenamjerna pogreška (Tablica 1).

Tablica 1. Vrste prijetnji IK sustavu u vatrogastvu [26]

Prirodne prijetnje	Namjerne prijetnje ljudi	Nenamjerne prijetnje ljudi	Oprema
meteorološke nepogode, geofizičke nepogode, sezonski fenomeni, astrofizički fenomeni, biološke prijetnje	gomilanje prometa, neautorizirani pristup, prisluškivanje, otkrivanje podataka, sabotaža, maliciozni programi , namjerno oštećivanje imovine, zlouporaba ovlasti	nedovoljna educiranost, nepravilno rukovanje, nemar i nepažnja, nedisciplina, nenamjerno oštećenje fizičke imovine, nenamjerno brisanje podataka, neadekvatna organizacija	električni kvarovi i neispravnosti, tvorničke greške, prestanak napajanja, ispadi opreme, prekid komunikacije, zračenja

S obzirom na izvor prijetnje, ljudski faktor koji se manifestira kao namjerna ili nenamjerna prijetnja pokazao se kao najučestaliji. Prijetnje uzrokovane kvarom opreme nalaze se na drugom mjestu po učestalosti kao vrsta prijetnji informacijskom sustavu, te prirodne prijetnje na trećem. [27]

Računalni informacijski sustavi često su ranjivi na tzv DoS napade (eng. *Denial of Service*) u kojima je cilj sustav zagušiti sa što više zahtjeva u kraćem vremenu kako bi se zagušenjem privremeno onesposobio sustav. Zamislimo sljedeći scenarij u kojem osoba s atribucijom namjernosti želi nanijeti veliku štetu ili privremeno onesposobiti vatrogasni informacijski sustav zbog nekih svojih motiva koji su pojednostavljeno terorističke naravi. U jednom od potencijalnih scenarija može se odlučiti za podmetanje većeg broja malih požara uz pomoć svojih suradnika. Požari su podmetnuti na lokacijama koje su međusobno dosta udaljene, nalaze se na nepristupačnom terenu i samim time dolazi do DoS napada požarima kojima se resursi u obliku dostupnih vatrogasaca i dobrovoljaca zaokupljaju. Dok gotovo sve dostupno ljudstvo gasi mnoštvo većih ili manjih požara, podmeće se požar na nekom od objekata koji su posebno važni poput (spremište goriva, telekomunikacijska centrala, dalekovod ili slično). Drugi pristup bi se mogao sastojati u kombinaciji podmetanja požara i prijavljivanjem većeg broja lažnih dojava o požarima.

5.1. Mjere zaštite informacijsko – komunikacijskog sustava u vatrogastvu

Kako bi se postigla maksimalna sigurnost vatrogasnog informacijskog sustava potrebno je obratiti pažnju na [28]:

· fizičke metode zaštite,

· organizacijske metode zaštite.

5.1.1. Fizičke metode zaštite

Fizička sigurnost vatrogasnog informacijskog sustava jedna je od ključnih komponenti cjelokupne zaštite informacijskog sustava.

Fizičku sigurnost podrazumijevaju tri osnovna aspekta kako bi se osigurala adekvatna zaštita, a to su:

· zaštita informacijske opreme i uređaja

· zaštita okoline

· kontrola fizičkog pristupa

Zaštita informacijske opreme i uređaja

Najvažniji aspekt kod fizičke zaštite informacijskog sustava predstavlja pravilna zaštita opreme i uređaja. Svakom uređaju treba definirati posebne mjere zaštite s obzirom na njegovu namjenu i vrijednost. Takve mjere trebaju spriječiti sve prijetnje, uključujući prijetnje od prirodnih nepogoda ili ljudske prijetnje. Većina organizacija provodi samo osnovne mjere zaštite opreme koje često nisu dovoljne, a odnose se na zaštitu poslužitelja i osobnih računala. Razlog tome je što navedeni elementi sadrže najviše osjetljivih podataka pa njihovo oštećenje može dovesti do ozbiljnih posljedica. Ipak, potrebno je provesti dodatne sigurnosne mjere pri rukovanju s opremom, kao što su [29]:

- zaključavanje uređaja nakon uporabe (npr. fax uređaja),
- smještaj uređaja na osigurana mjesta,
- pohrana prijenosnih medija na sigurna mjesta te
- adekvatno uništavanje starih prijenosnih medija.

5.1.2. Organizacijske mjere zaštite

Organizacijske mjere podrazumijevaju osiguranje ažurnosti, točnosti i pravilnosti obavljanja poslova, kao i sprječavanje neovlaštene izmjene dokumentacije i podataka te neovlaštenog korištenja informatičke opreme i mreže.

Organizacijskim mjerama zaštite određuje se:

· Organizacija prostora

· Odgovorna osoba za provedbu sigurnosti

· Program edukacije zaposlenika

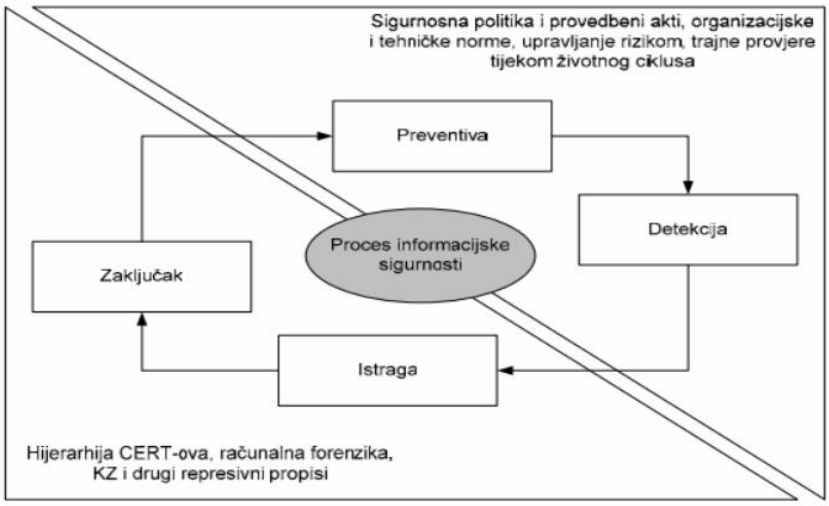
5.2. Načini zaštite informacijsko – komunikacijskih sustava od mrežno temeljenih prijetnji

U prethodnom poglavlju su opisane moguće prijetnje koje se mogu susresti na mreži. Puno prostora nije ostavljeno za načine sprječavanja i prevencije, zbog toga što se četvrto poglavlje bavi načinima zaštite i prevencije i unutar njega će biti spomenute konkretne mjere koje su potrebne za sigurno surfanje i korištenje računala na internetu.

Informacijska sigurnost definira se kao očuvanje [30]:

- povjerljivosti – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj,
- integriteta – zaštita postojanja, točnosti i kompletnosti informacije kao i procesnih metoda,
- raspoloživosti – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva.

Pojednostavljeno informacijska sigurnost treba osigurati da sve informacije budu dostupne svima, uzimajući u obzir ovlasti i hijerarhiju. Tako da se ne može dogoditi situacija u kojoj i direktor i obični radnik imaju iste ovlasti i pristup podacima. Potrebno je sačuvati integritet informacijama, kako bi se osigurala točnost informacija bez opasnosti od slučajnih ili namjernih promjena. Na taj način se mogu izbjeći sve potencijalno neugodne situacije koje mogu nastati zbog pogrešnog tumačenja informacija. Sve informacije moraju biti dostupne autoriziranim korisnicima u točno određenom trenutku kada oni upute zahtjev za uslugom.



Slika 5. Prikaz procesnog pogleda na informacijsku sigurnost [30]

Na slici 5. je prikazan proces informacijske sigurnosti. Proces ima četiri koraka, a to su preventiva, detekcija, istraga i zaključak. Svaki korak je povezan s određenim aktivnostima.

Prvi korak je preventiva, što znači da se rizik i potencijalna šteta moraju smanjiti na najmanju moguću mjeru. Određuju se sigurnosne mjere, ograničava se pristup informacijama prema unaprijed utvrđenoj hijerahiji, prate se iskustva tvrtki koje rade u sličnom području. Drugi korak je detekcija. Detekcija ima za cilj detektirati potencijalne sigurnosne ranjivosti i propusti, prije nego što se oni dogode. Isprobavaju se različite kombinacije kako bi se mogli simulirati potencijalno štetni događaji i njihov utjecaj na sami sustav. Treći korak je istraga. Onog trenutka kada se dogodi neki sigurnosni propust mora se obaviti istraga kako bi se utvrdila točna razina na kojoj se dogodio sigurnosni propust ili kako bi se utvrdilo o kojem odjelu se radi. Zadnji i četvrti korak je zaključak. Kod zaključka se uzima u obzir koje su mjere prevencije korištene prije nastanka propusta, pokušava se utvrditi potencijalne greške u procesu detekcije i jesu li se slijedili svi sigurnosni protokoli u cilju smanjivanja štete.

U Hrvatskoj se sa pitanjem informacijske sigurnosti bavi nacionalni CERT (eng. *Computer Emergency Response Team*). Nacionalni CERT osnovan je u skladu sa Zakonom o informacijskoj sigurnosti u Republici Hrvatskoj.

5.3. Zakoni propisi i norme informacijske sigurnosti

U nastavku slijedi popis zakonskih i podzakonskih akata iz područja informacijske sigurnosti u Republici Hrvatskoj

- Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu (NN – MU 9/02)
- Zakon o tajnosti podataka (NN 79/07)
- Zakon o izmjenama i dopunama Zakona o tajnosti podataka (NN 86/12)
- Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima (NN 102/07)
- Zakon o informacijskoj sigurnosti (NN 79/07)
- Zakon o elektroničkom potpisu (NN 10/02, 80/08)
- Zakon o sigurnosnim provjerama (NN 85/08)
- Zakon o izmjenama i dopunama Zakona o sigurnosnim provjerama (NN 86/12)
- Uredba o sadržaju, izgledu, načinu ispunjavanja i postupanja s upitnikom za sigurnosnu provjeru (NN 114/08)
- Naputak o sigurnosnoj edukaciji o mjerama i standardima informacijske sigurnosti (prosinac 2008., UVNS, Neklasificirano)
- Naputak o provedbi sigurnosne akreditacije Sustava registara (veljača 2009., UVNS, Neklasificirano) o Naputak o sadržaju i izgledu NATO i EU Certifikata (travanj 2009., UVNS, Neklasificirano)
- Zakonu o pravu na pristup informacijama (NN 25/13, NN 85/15)
- Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga o Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN109/12, 33/13-ispravak, 126/13, 67/16 i 66/19)
- Pravilnik o izmjenama i dopunama Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN 126/13)
- Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga - neslužbeni pročišćeni tekst
- Pravilnik o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevara u pružanju usluga elektroničke pošte (NN 42/09)
- Pravilnik o izvršavanju sigurnosne mjere zabrane pristupa Internetu NN 34/13

- Pravilnik o tehničkim pravilima i uvjetima povezivanja sustava certificiranja elektroničkih potpisa (NN 89/02)
- Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata (NN 107/10)
- Uredba o mjerama informacijske sigurnosti (NN 46/08)
- Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost (NN 30/2011)
- Pravilnik o standardima sigurnosne provjere (ožujak 2011., UVNS, Neklasificirano)
- Pravilnik o standardima fizičke sigurnosti (ožujak 2011., UVNS, Neklasificirano)
- Pravilnik o standardima sigurnosti podataka (svibanj 2011., UVNS, Neklasificirano)
- Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava (svibanj 2008., UVNS, Neklasificirano)
- Pravilnik o standardima sigurnosti poslovne suradnje (svibanj 2008., UVNS, Neklasificirano)
- Uredba o djelokrugu, sadržaju i nositelju poslova certificiranja elektroničkih potpisa za tijela državne uprave (NN 146/04)

5.3.1. Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti (ZOIS) definira terminologiju informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti, informacijski sustav, sigurnosnu akreditaciju te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. Zakon o informacijskoj sigurnosti primjenjuje se na državna tijela, tijela jedinica lokalne i regionalne samouprave kao i na pravne osobe s javnim ovlastima koje u svom radu koriste klasificirane i neklasificirane podatke. Također, primjenjuje se na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima. [31]

Poseban naglasak stavljen je na definiciju i opis sljedećih područja informacijske sigurnosti

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podataka,
- sigurnost informacijskog sustava i
- sigurnost poslovne suradnje

5.3.2. Zakon o tajnosti podataka

Zakon o tajnosti podataka Zakonom o tajnosti podataka (ZOTP) utvrđuju se pojmovi podatak, klasificirani i neklasificirani podaci, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom zakona. Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima te pravne i fizičke osobe koje, u skladu s ovim zakonom, ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima. Jasno je određeno da se klasificiranim podatkom ne može proglasiti podatak radi prikrivanja kaznenog djela, prekoračenja ili zlouporabe ovlasti te drugih oblika nezakonitog postupanja u državnim tijelima. [32]

Prema članku 4. ZOTP, definiraju se sljedeći stupnjevi klasificiranih podataka:

- Vrlo tajno,
- Tajno,
- Povjerljivo,
- Ograničeno

5.3.3. Zakon o zaštiti osobnih podataka

Zakonom o zaštiti osobnih podataka (ZOZOP) uređuje se zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem, obradom i korištenjem

osobnih podataka u Republici Hrvatskoj. Svrha zaštite osobnih podataka je zaštita života kao i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama. [33]

Ovaj zakon je bio na snazi do 25.05.2018., nakon ovoga zakona na snazi je Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

5.3.4. Institucije za upravljanje informacijskom sigurnošću RH

Temeljne institucije upravljanja informacijskom sigurnošću u RH su Nacionalni CERT, CARNet CERT, Zavod za sigurnost informacijskih sustava (ZSIS), Ured vijeća za nacionalnu sigurnost (UVNS), Agencija za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT d.o.o.), Agencija za zaštitu osobnih podataka (AZOP) te Ministarstvo uprave Republike Hrvatske.Nacionalni CERT Nacionalni CERT (eng. Computer Emergency Response Team) osnovan je 2008. godine kada je Carnet prema obvezama Zakona o informacijskoj sigurnosti osnovao Odjel za Nacionalni CERT. Tim putem Nacionalni CERT preuzeo je sve poslove koje je obavljao CARNet CERT kao jedini CERT u RH od 1996. godine. [35]

Na ovaj način CARNet je omogućio bolju brigu o sigurnosti javnih informacijskih sustava kroz djelatnost Nacionalnog CERT-a te pružio kvalitetniju uslugu korisnicima u sustavu znanosti i obrazovanja kroz aktivnosti CARNet-ovog Odjela za računalnu sigurnost. Nakon ustrojstva Nacionalnog CERT-a započinje uspostava hijerarhijski ustrojene infrastrukture CERT timova koja je nužna za preventivno djelovanje i učinkovitu koordinaciju pri rješavanju sigurnosnih incidenata vezanih uz informacijsko komunikacijske sustave. Slikom je prikazan hijerarhijski ustroj CERT-ova zajedno sa vršnim koordinirajućim tijelom, Nacionalnim CERT-om i prema tom zakonu jedna od zadaća je obrada incidenata na Internetu, tj. očuvanje informacijske sigurnosti u RH. Prema Pravilniku o radu Nacionalnog CERT-a, on se bavi incidentom, ako se jedna

od strana u incidentu nalazi u RH (odnosno, ako je u .hr domeni ili u hrvatskom adresnom prostoru). [34]

Nacionalni se CERT sa svojim resursima uključuje u pomoć pri rješavanju značajnih incidenata koji su definirani prema sljedećim prioritetima:

1) incidenti koji su potencijalna ugroza za živote ljudi,

2) incidenti koji uključuju infrastrukturu Interneta u Republici Hrvatskoj,

3) incidenti značajnog opsega,

4) nove vrste ugrožavanja računalne sigurnosti te

5) ostali incidenti.

Njegova je misija prevencija i zaštita javnih IK sustava u Republici Hrvatskoj od ugroza njihove sigurnosti te pružanje pomoći u suzbijanju posljedica nastalih sigurnosnih incidenata.

5.4. Mjere zaštite

Mjere zaštite informacijskih sustava dijelimo na proaktivne i reaktivne mjere zaštite.

5.4.1. Proaktivne mjere

Proaktivne mjere su one mjere koje se provode prije nego što se neki sigurnosni propust ili incident dogodi. Na taj način se želi utjecati na mogući nastanak štete i spriječiti ga prije nego što se on zapravo dogodi.

Proaktivne mjere podrazumijevaju [34]:

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti u svrhu priprema za sprečavanje šteta,
- kontinuirano praćenje računalno-sigurnosnih tehnologija te se sva nova saznanja prikupljaju i diseminiraju,
- javno objavljivanje novih informacija u svrhu edukacije najšire javnosti i unapređenju svijesti o značaju računalne sigurnosti i

- provođenje detaljne edukativne obuke za specifične grupe korisnika.

U kontekstu ranije spomenutih mrežno temeljenih prijetnji, njihov štetni utjecaj se može umanjiti kroz mjere prevencije. Dobra osnova za početak je odgovorno ponašanje na internetu. Ponekad treba malo sporije reagirati i dobro promisliti prije otvaranja sumnjivih web stranica, e-mailova i slično. Potreban je oprez pri korištenju osobnih podataka na internetu, jer neke web stranice mogu biti jako vješto iskopirane i omogućiti kopiranje podataka prema napadaču. Zbog toga se provjeravaju sigurnosni certifikati web stranica. Nužan uvjet prevencije je i korištenje najnovije ažurirane verziju antivirusnog programa ili vatrozida. Posljednja ažurirana verzija sadrži sve prijetnje koje su dosad zabilježene, a kako se prijetnje stalno razvijaju, isto vrijedi i za ažuriranje antivirusnih programa. Preporuča se i redovito skeniranje računala kako bi se pronašli i izbrisali potencijalni zlonamjerni programi.

Navedene preventivne mjere se mogu koristiti kod:

- različitih zlonamjernih programa
- krađe podataka i identiteta.

Uvođenjem jednostavnih provjera moguće je obraniti web stranicu od većine napada umetanjem SQL koda. Preporuča se na poseban način obraditi sve primljene podatke koji: sadrže sumnjive znakove poput znaka točke-zareza, dvostrukih crtica ili navodnika, sadrže SQL ključne riječi, ne odgovaraju očekivanom tipu podataka ili sadrže preveliki broj znakova. Još jedan način borbe protiv napada je korištenje neuobičajenih imena za tablice i atribute u bazi podataka te minimiziranje informacija koje su dostupne u porukama greške. Time se napadaču otežava prikupljanje informacija o bazi podataka što je prvi korak u izvođenju napada. Ako napadač ne zna strukturu baze podatka te imena tablica i atributa ne može izvesti napad. [35]

Važno je zapamtiti da ne postoji niti jedan računalni sustav koji je u potpunosti siguran i nema niti jednu ranjivost. Isto vrijedi i za softver. Zbog toga je važno redovito ažurirati sav softver koji se na sustavu koristi i pratiti upozorenja proizvođača softvera. [36]

Posljednje dvije preventivne mjere koje se preporučuju su edukacija i enkripcija. Edukacija je iznimno važna zato što je to proces koji se stalno ponavlja zbog već ranije spomenutih razloga konstantnog razvoja prijetnji, ali i metoda zaštite. Poznavanjem potencijalnih prijetnji i ranjivosti može se izbjeći šteta koja se može dogoditi prilikom njihovog nastanka. Enkripcija omogućava korisniku zaštitu podataka kroz korištenje određenog ključa koji je poznat samo pošiljatelju i primatelju. Na taj način se može ograničiti pristup podacima, a u slučaju gubitka podataka postoji manja opasnost. Podaci bez ključa ili šifre su neupotrebljivi.

Ovisno o preferencijama mogu se koristiti i određeni programi za enkripciju koji su dostupni na tržištu poput PGP-a (*Pretty Good Privacy* – PGP). Program koristi kombinaciju javnog i privatnog ključa. Svaka osoba ima javni i privatni ključ: javni se ključ dijeli sa svima, a privatni se ključ sigurno pohranjuje i ne dijeli. Javni ključ koristi se za šifriranje, a privatni za dešifriranje. [37]

5.4.2. Reaktivne mjere

Onoga trenutka kada se otkrije sigurnosni propust koji je uzrokovao određenu štetu, tada se više ne mogu poduzeti preventivne mjere ili proaktivne mjere. Potrebno je prihvatiti činjenica da je šteta nastala i da se nastala šteta treba pokušati smanjiti na najmanju moguću mjeru.

Reaktivne mjere podrazumijevaju [34]:

- na osnovu prikupljenih saznanja izrađuju se i distribuiraju sigurnosna upozorenja, javno ili ciljano
- nacionalni CERT prikuplja, obrađuje i priprema sigurnosne preporuke o slabostima u informacijskim sustavima te ih javno distribuira i arhivira u svom informacijskom sustavu
- koordinacija rješavanja značajnijih incidenata u koje je uključena barem jedna strana iz Republike Hrvatske.

Kroz praćenje CERT-ovih upozorenja možemo saznati koje su prijetnje trenutno aktualne, a u slučaju da se prijetnja već dogodila tada je potrebno reagirati u skladu sa sigurnosnim preporukama kako bi se šteta smanjila.

Kako bi se organizacijama javnog i privatnog poslovnog sektora pomoglo pri uvođenju sustava informacijske sigurnosti u svrhu prevencije od zlouporabe, gubitka ili oštećenja podataka i informacija, u Velikoj Britaniji razvijena je norma BS 7799 pod nazivom *Industry Code of Practice*. Iz norme BS 7799 proizašle su ISO/IEC 17799, odnosno ISO/IEC 27002 te ISO/IEC 27001 kao međunarodne norme. Razlog usvajanja norme BS 7799 kao međunarodne norme je taj što osigurava fleksibilnost, definira upravljački okvir, a ne zadire u konkretnu tehničku implementaciju što je čini primjenjivom u organizacijama različitih tehničkih sustava bez obzira na njihovu veličinu. Uspostava kvalitetnog sustava upravljanja informacijskom sigurnošću zahtjeva primjenu oba standarda. Navedene norme nisu tehničke, nego norme upravljanja, a sadrže strukturirani skup smjernica i specifikacija za pomoć organizacijama u razvoju sustava upravljanja informacijskom sigurnošću (eng. *Information Security Management System*, ISMS). [38]

ISO 27001 je međunarodna norma objavljena od strane Međunarodne organizacije za standardizaciju (ISO) i opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Najnovija inačica ovog standarda je objavljena 2017. godine, te je sadašnji puni naziv ISO/IEC 27001:2017. Norma je razvijena na temelju britanskog standarda BS 7799-2, a prva revizija objavljena je 2005. godine. ISO 27001 može biti implementiran u bilo kojoj organizaciji, neovisno o njenoj veličini ili namjeni. Razvijen je od strane stručnjaka iz područja informacijske sigurnosti i propisuje metodologiju za primjenu upravljanja informacijskom sigurnošću u organizaciji. Također, omogućava tvrtkama dobivanje certifikata, što znači da neovisno certifikacijsko tijelo daje potvrdu da je organizacija implementirala informacijsku sigurnost sukladno ISO 27001. [38]

Norma opisuje sustav upravljanja informacijskom sigurnošću i daje specifikacije za primjenu prvog dijela norme i izgradnje ISMS-a, a sastoji se od četiri osnovna poglavlja: [38]

- sustavi za upravljanje informacijskom sigurnošću (eng. *Information Security Management System – ISMS*);
- odgovornost uprave (eng. *Management Responsibility*);
- ispitivanje sustava upravljanja (eng. *Management Review*);

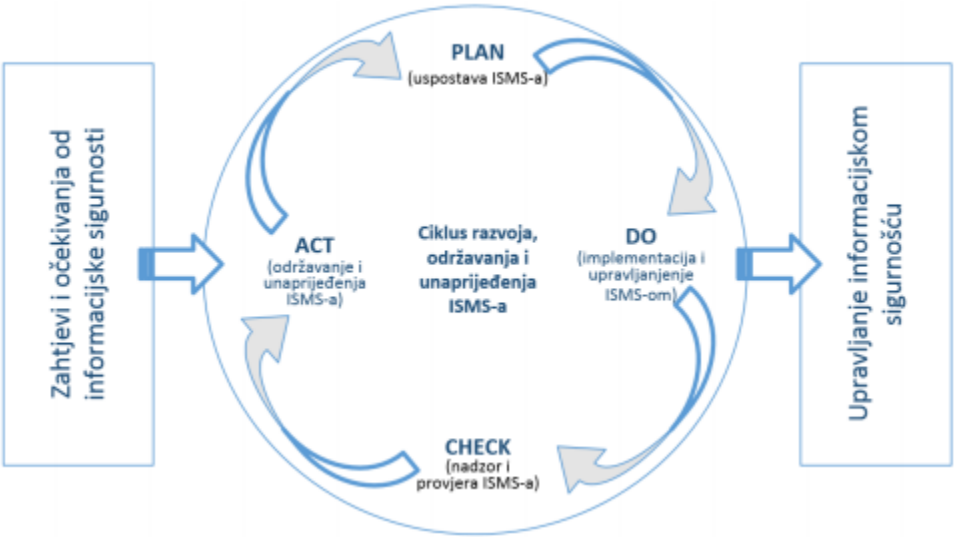
- poboljšanje sustava za upravljanje informacijskom sigurnošću (eng. *ISMS Improvement*).

Iz perspektive upravljanja prethodna, osnovna, poglavlja moguće je sažeti u dva skupa:

- sustav za upravljanje sigurnošću koji obuhvaća dokumentiranje, pregled, ispitivanje, odgovornost uprava, korektivne i preventivne mjere te stalno poboljšanje sustava i
- upravljanje informacijskom sigurnošću koji je ciklus uspostave, implementacije, rukovanja, pregledavanja, ispitivanja i poboljšanja sustava za upravljanje informacijskom sigurnošću (ISMS), a koji je opisan modelom PDCA (eng. Plan-Do-Check-Act).

PDCA ciklus prikazan slikom sastoji se od sljedećih faza:

- PLAN: Planiranje i uspostava sustava za upravljanje informacijskom sigurnošću;
- DO: Implementacija i upravljanje sustavom informacijske sigurnosti;
- CHECK: Nadzor i ispitivanje sustava informacijske sigurnosti;
- ACT: Unaprjeđenje sustava informacijske sigurnosti;



Slika 6. Shema PDCA ciklusa [38]

Shema PDCA ciklusa kao što je vidljivo iz slike 6., faze PDCA ciklusa se ponavljaju s ciljem osiguranja ažurnosti upravljanja sigurnošću IK sustava. Norma ISO 27001 sastoji se od 11 područja, 39 kontrolnih ciljeva i ukupno 133 kontrole koje koriste kao pomoć prilikom identifikacije, upravljanja i smanjenja niza prijetnji kojima je IK sustav izložen. Također, osigurava se usklađenost s važećom zakonskom regulativom, aktivnostima unutar organizacije kao i pouzdanost sustava u slučaju nesreće, ali i edukacija zaposlenika. [38]

6. PRIMJER NAPADA NA 911 SUSTAV U SVIJETU

Sljedeća generacija 9-1-1 (NG 9-1-1) sustava, koji djeluje na platformi Internet Protocol (IP), omogućuje međusobnu povezanost sa širokim rasponom javnih i privatnih mreža, kao što su bežične mreže, Internet i redovne telefonske mreže. Unaprijedit će se sustavi NG 9-1-1 i mogućnosti današnjih mreža 9-1-1, omogućujući kompatibilnost s više vrsta komunikacije, pružanje veće situacijske svijesti dispečerima i hitnim pomoćima, te uspostavljanje razine otpornost koja prethodno nije moguća. NG9-1-1 će dopustiti javne točke za javnu sigurnost PSAP (engl. *public-safety answering point*) koje treba prihvatiti i prihvatiti obradu niza informacija, uključujući tekstualne, slikovne, video i glasovne pozive. [39]

Uz sve prednosti koje novi način modernijih funkcioniranja sustava za hitne službe donosi, otvara se tu i dosta prostora za potencijalne prijetnje, koje će biti spomenute kasnije.

Tradicionalne usluge 9-1-1 obično rade preko standardnih govornih telefonskih mreža i koriste softver, poput računalnih sustava dispečiranja, koji djeluju na zatvorenim, unutarnjim mrežama s malo ili nikakvim međusobno povezanostima s drugim sustavima. Relativno ograničena sredstva za ulazak u naslijeđene sustave 9-1-1 smanjuju potencijalni vektori napada. Međutim, cyber rizik i dalje predstavlja problem i s njim se mora aktivno upravljati, čak i zajedno naslijeđeni sustavi. Potencijalni cyber rizici za NG 9-1-1 sustave ne umanjuju koristi od NG 9-1-1. Ipak, cyber rizici predstavljaju novu razinu izloženosti koju administratori PSAP (engl. *public-safety answering point*) moraju razumjeti i aktivno upravljati kao dio sveobuhvatnog rizika za program upravljanja. Sustavi su već pod napadom. Kako cyber prijetnje rastu u složenosti i sofisticiranosti, napadi bi mogli biti ozbiljniji protiv NG 9-1-1 sustava jer napadači mogu pokretati više distribuiranih napada s većom automatizacijom, pokrivajući šire geografsko područje i protiv više različitih ciljeva. [39]

Tablica 2. Javna sigurnost u stvarnom svijetu i 9-1-1 cyber napada [39]

VRSTA PRIJETNJE	OPIS	STVARNI PRIMJER
TELEFONIJA DENIAL OF SERVICE ATTACK (TDoS)	Upotreba protokola glasa putem Interneta(VoIP) sustavi za preplavljivanje telefonasustavi koji ih čine nesposobnima upućivanje ili primanje poziva.	U listopadu 2016. optužen je tinejdžer u Arizoni za slanje tisuća poziva u centre za hitne slučajeve 9-1-1i agencije za provođenje zakona u više država putem kompromitiranih mobilnih telefona.
NEOVLAŠTENI PODATKOVNI PRISTUP	Napadači mogu pristupiti osjetljivim bazama podataka (npr. provođenje zakona,zdravstvene evidencije) krasti, mijenjati ilioštetiti podatke.	U kolovozu 2017., okrug Schuyler u New Yorku doživio je cyber napad u kojem su hakeri dobili pristup komunikacijskom sustavu okruga. Napad je izvršen korištenjem metode grube sile (eng. *brute force*) u kojem se isprobavaju sve moguće kombinacije lozinki. Napad je imao za posljedicu privremeno onesposobljavanje sposobnosti otpreme policijskih zamjenika na teren.
NEOVLAŠTEN MREŽNI PRISTUP	Napadači dobivaju pristup mreži koristeći ukradene vjerodajnice i / ili uređaje.	U 2016. godini dvoje tinejdžera dobilo je neovlašteni pristup službenom Twitter računu policijske uprave Manitowoc korištenjem ukradenih vjerodajnica.
RANSOMWARE	Upotreba softvera za blokiranje računala s ciljem iznude ili traženja otkupnine	U ožujku 2018. Otet je cjelokupni sustav hitne službe 9-1-1 grada Baltimora korištenjem softvera za otmicu (tzv. *ransomware*). Napad je kompromitirao gradski računalno podržan dispečerski poslužitelj, što je imalo za posljedicu privremeno gašenje digitalnih sustava slanja i snimanja.

Rizici nastaju kada prijetnja iskoristi ranjivost sustava, što dovodi do neželjenog događaja koji ima negativne posljedice na željeno stanje mreže. Kibernetska sigurnost riskira da NG 9-1-1 sustavi imaju ozbiljne potencijalne utjecaje, uključujući gubitak života ili imovine, prekid posla za pogođene korisnike mreže, financijske troškove zbog neovlaštene uporabe podataka i naknadno rješavanje. Postoji mnoštvo potencijalnih aktera, svaki s različitim namjerama i mogućnostima za izvođenje programa napada. Razumijevajući motive i sposobnosti odgovornih za pokretanje napada, sustav se može lakše obraniti. Administratori mogu bolje predvidjeti vrste napada s kojima bi se mogli suočiti i bolje zaštititi podatke i imovinu koji su vjerojatne mete. [39]

Svaka od navedenih prijetnji u tablici 2. poput napada preplavljivanjem telefonskih sustava ili onemogućavanjem usluge, davanje pristupa neovlaštenim podacima ili pristupanje podacima s kojima ne bi trebali raspolagati uz korištenje softvera za ucjenu može imati štetne posljedice na informacijski sustav. Sve navedeno vrlo lako se može preslikati i na informacijski sustav u vatrogastvu. U prvom primjeru navodi se postupak jednog američkog tinejdžera iz 2016. koji je optužen za slanje tisuće poziva u određenom vremenskom razdoblju u centar 9-1-1. S obzirom kako se pozivi u taj centar šalju samo onda kada je to od velike važnosti za život jedne ili više osoba koja se nalazi u opasnosti to znači kako je tim postupkom ugrožen život mnogih osoba. Nije isključeno kako je moguće i kako je netko tragično nastradao čekajući pomoć hitne službe koja nije došla ili je došla kasnije zbog gomile lažnih poziva koje su preplavile cijeli sustav i učinile ga beskorisnim.

Druga tematika i druga vrsta prijetnji je scenarij u kojem osoba s atribucijom namjernosti raspolaže s podacima i koristi ih za stjecanje koristi ili nanošenje štete. 2017. godine u New Yorku jedan od okruga je bio privremeno onesposobljen zbog podataka koji su neovlašteno prikupljeni. Hakeri su korištenjem metode grube sile isprobali sve moguće kombinacije za lozinku i uspjeli pristupiti komunikacijskom sustavu okruga Schuyler. To je imalo za posljedicu onesposobljavanje slanja policijskih zamjenika na intervencije.

Treći primjer je dobivanje pristupa korištenjem ukradenih vjerodajnica. U 2016. godini dvoje tinejdžera koji su uspjeli dobiti neovlašteni pristup službenom Twitter računu policijske uprave okruga Manitowoc u državi Wisconsin. Na sreću veća šteta nije počinjena, međutim korištenjem društvenih mreža mogu se postići velike štete

potencijalnim objavljivanjem štetnih, nepotpunih ili lažnih informacija koje mogu imati za cilj obmanu, potencijalnu optužbu protiv nekoga ili nešto slično.

Četvrti primjer koji je naveden u tablici 2. je upotreba softvera za blokiranje računala s ciljem iznude ili traženja otkupnine. U ožujku 2018. godine je otet cjelokupni sustav hitne službe 911 grada Baltimora u državi Maryland. Taj napad je pokazao što se sve može dogoditi onoga trenutka kada osoba s atribucijom namjernosti neovlašteno preuzme pristup nad jednim od sustava koji je od velike važnosti za funkcioniranje svih hitnih službu u višemilijunskom gradu. Dispečerski poslužitelj koji se nalazio na računalu je kompromitiran što je dovelo do privremenog prestanka rada digitalnih sustava slanja i snimanja.

S obzirom kako svaki nepoželjni događaj u nekom sustavu predstavlja rizik, u nastavku se donosi nekoliko informacija o modelu procjene rizika.

Pitanje sigurnosti oduvijek je bilo predmet ljudskog interesa. Općenito bismo mogli definirati sigurnost kao sposobnost izbjegavanja događaja koji bi imali negativne posljedice za određeni objekt. Predmet sigurnosti može biti ljudski život ili imovina koja ima određenu važnost za čovjeka. Procjena rizika (eng. *risk assessment*) je dio jednog većeg procesa kojeg nazivamo upravljanje rizikom (eng. *risk management*). Procjena rizika je proces prepoznavanja, kvantificiranja i razvrstavanja rizika po prioritetima prema kriterijima za prihvaćanje rizika i ciljevima važnim za organizaciju. Procjena rizika sastoji se od dva potprocesa, a to su analiza rizika i vrednovanje rizika prema standardu ISO 27002. [40]

7. RIZICI I OPASNOSTI INFORMACIJSKOGA SUSTAVA

U tablici 3. prikazan je model procjena štetnih događaja usko vezanih uz informacijsko komunikacijski sustav u vatrogastvu. Na okomitoj osi je prikazana vjerojatnost da se određeni događaj dogodi od 1 do 5 opisno (vrlo malo vjerojatno, malo vjerojatno, vjerojatno, vrlo vjerojatno, gotovo sigurno). Mala vjerojatnost označava događaj koji se ne događa često, dok gotovo sigurno prikazuje događaj koji će se dogoditi s vrlo velikom sigurnošću.

Tablica 3. Procjena rizika za štetne događaje usko vezane uz informacijsko komunikacijski sustav u vatrogastvu (izvor: autor)

Vjerojatnost	Neznatan	Beznačajan	Značajan	Veliki	Katastrofalan
Gotovo sigurno	Lažni poziv	Loša komunikacija	Manjkava zaštita sustava	DDOS napad	Potres
Vrlo vjerojatno	Pad WEB stranice	Neovlašteni pristup	Ljudska greška	Sabotaža	Požar
Vjerojatno	Nepažnja	Gomilanje prometa	Pogrešna informacija	Ispad opreme	Poplava
Malo	Nedovoljna edukacija	Linija u kvaru	Prekid komunikacije	Tehnička pogreška opreme	PAD IK sustava
Vrlo malo	Neiskustvo	Nenamjerno brisanje podataka	Nenamjerno oštećenje opreme	Zauzeta linija	Prestanak napajanja

Utjecaj

Događaji su poredani od onih koji su manje vjerojatni i koji će se rijeđe dogoditi prema onima koji su vrlo vjerojatni i koji će se češće dogoditi (od dolje prema gore). Na vodoravnoj osi je prikazan utjecaj određenih događaja (neznatan, zanemariv, značajan, veliki i katastrofalan). Što je utjecaj događaja veći, veće su i njegove posljedice. Sretna okolnost u samom procesu procjene rizika je u tome da je mala vjerojatnost za događanje događaja koji mogu uzrokovati katastrofalne posljedice. Događaji su također označeni i sa različitim bojama, tako da zelena boja predstavlja malu razinu opasnosti, žuta boja srednju razinu opasnosti i crvena boja predstavlja najveću razinu opasnosti.

Neznatan utjecaj na nastanak štetnog događaja u informacijskom sustavu imaju sljedeći događaji:

- neiskustvo
- nedovoljna edukacija
- nepažnja
- pad web stranice
- lažni poziv

Iako navedeni događaji imaju mali utjecaj za potencijalno štetan događaj, uvijek se može dogoditi kombinacija nekoliko događaja koji zajednički mogu uzrokovati nesreću iako to samo po sebi nije izgledno. Primjerice jedan lažni poziv sam ne bi imao veliko značenje, ali u kombinaciji sa padom web stranice i neiskustvom u ključnom trenutku može uzrokovati štetne posljedice.

Beznačajan utjecaj na nastanak štetnog događaja u informacijskom sustavu imaju sljedeći događaji:

- nenamjerno brisanje podataka
- linija u kvaru
- gomilanje prometa
- neovlašteni pristup
- loša komunikacija

Loša komunikacija može biti česta i relativno bezazlena pojava, međutim u kombinacijii sa drugim događajma može biti opasna. Sljedeća najveća opasnost je gomilanje poziva i preopterećenje mreže.

Značajan utjecaj na nastanak štetnog događaja u informacijskom sustavu imaju sljedeći događaji:

- nenamjerno oštećenje opreme
- prekid komunikacije
- pogrešna informacija
- ljudska greška
- manjkava zaštita sustava

Prekid komunikacije je značajan problem, primjerice ukoliko dođe do prekida komunikacije između vatrogasnog operativnog centra, dežurni u centru nezna šta se odvija na terenu i kakvi su uvjeti, dali je vatrogascima potrebna ispomoć. Ako nema komunikacije nezna se tijek intervencije. Primjerice pogrešna informacija kod primanja poziva odnosno kod javljanja nesretnog događaja može imati za posljedicu da se na teren pošalje vozilo sa neadekvatnom opremom.

Veliki utjecaj na nastanak štetnog događaja u informacijskom sustavu imaju sljedeći događaji:

- zauzeta linija
- tehnička pogreška opreme
- ispad opreme
- sabotaža
- DDOS napad

Konkretno ovdje mogu napisati događaj koji se odvio u stvarnome životu, Vatrogasni opertivni centar je uputio sirenu za uzbunjivanje Dobrovoljnog vatrogasnog

društva, kada su dobrovoljni vatrogasci stigli u vatrogasni dom i htjeli se javiti dežurnome u VOC putem fixne linije nisu mogli stupiti u kontakt jer fixne telefonske linije nisu radile. U kontakt je stupljeno preko mobilne mreže. Intervenciji je prethodio potres. Primjerice u Hrvatskoj se 29. rujna 2020. godine dogodio pad telekomunikacijske mreže, te je time bila onemogućena komunikacija sa hitnim i žurnim službama. Padu telekomunikacijske mreže se pripisuje tehnički kvar. Najveći problem kod ovog događaja je to da ljudi nisu mogli dobiti broj 112, policiju, vatrogasce i Hitnu pomoć što ima za posljedicu da službe ne mogu reagirati te odgovoriti na svoje zadatke i pomoći unesrećenima. Ravnateljstvo CZ MUP-RH je objavilo obavjest putem Twitter-a.

Slika 7. MUP obavijest o nedostupnosti [41]

Katastrofalan utjecaj na nastanak štetnog događaja u informacijskom sustavu imaju sljedeći događaji :

- prestanak napajanja
- pad (IK) sustava
- poplava
- požar
- potres.

Događaji koji su nabrojani mogu imati katastrofalan utjecaj i teške posljedice na sve sudionike. Na sreću oni se ne događaju često. Neka od velikih elementarnih nepogoda poput potresa jake snage u kombinaciji sa nestankom struje ili padom informacijsko komunikacijskih sustava može uzrokovati nemjerljivu štetu.

Može se reći da je u vatrogastvu te ostalim hitnim i dežurnim službama komunikacija najvažnija stvar. Dojava a drintervencija i štetnih događaja obavlja se putem telekomunikacijskih usluga u vatrogasni operativni centar, potom dežurni u operativnome centru uzbunjuje profesionalnu postrojbu koja se nalazi u sklopu operativnog centra ili dobrovoljna vatrogasnuštva koja se uzbunjuju sirenom na vatrogasnim domovima i sms porukama. Ovdje vidimo da opet postoji problem kod uzbunjivanja dobrovoljnih vatrogasnih društava jer se uzbunjuju daljinski preko sirene i sms-ova a za oboje se upotrebljavaju telekomunikacijske usluge. Za većinu aplikacija i programa u vatrogasnome dispečerskome centru potreban je internet, te ukoliko dođe do pada mobilne mreže programi su neupotrebljivi. Aplikacije koje je napravila Hrvatska vatrogasna zajednica, korisnici im pristupaju putem interneta što nam govori da vatrogasni centri ovise o internetu i telekomunikacijama. Komunikacija na vatrogasnim intervencijama se odvija putem radioveza.

8. ZAKLJUČAK

Napredak tehnologije je donio mnoge mogućnosti koje su prije bile nezamislive, a to su mogućnosti komuniciranja sa svim osobama bez obzira na njihovu trenutnu udaljenost, kupovina bez potrebe za odlaskom iz kuće, izbjegavanje repova u banci i slično. Međutim napredak je donio sa sobom i neke negativne stvari, a to su mrežno temeljene prijetnje.

Sve visoko tehnološke mogućnosti ostavljaju prostor za ranjivost u obliku neovlaštenog i nezakonitog pristupa raznovrsnim podatcima koje upisujemo pri registraciji za e-mail, pretplate, društvene mreže, za kupovinu i slično. Zlonamjerne osobe žele prikupiti te podatke kako bi sebi donijeli korist, a drugome nanijeli štetu.

Najznačajnije mrežno temeljene prijetnje su:

- računalni virusi
- zlonamjerni programi
- krađa podataka i identiteta
- SQL umetanje i napadi uskraćivanjem resursa, DoS
- računalna ranjivost.

S obzirom na pitanje rizika koje je vrlo bitno i koje se ne može u potpunosti ukloniti, važno ga je svesti na najmanju moguću mjeru, odnosno na što manju štetu za sve uključene strane. Nekoliko događaja manjeg značenja ili jedan događaj većeg rizika nemaju isti utjecaj na konačni ishod. Primjeri iz SAD-a u kojima su pojedinci uspjeli u potpunosti zagušiti sustav 911 kroz napad uskraćivanjem resursa ili kroz korištenje zlonamjernog softvera pokazali su koliko je zapravo veliki značaj mrežno temeljenih prijetnji.

Zlonamjerni hakeri ciljaju na osobe ispred ekrana, a ne na tehnologiju. Upotrebom prevara kao što su krađa identiteta, *phishing* i drugih sličnih trikova društvenog inženjeringa, oni mogu zaobići sigurnosnu infrastrukturu u potpunosti.
Ne postoji sustav koji je savršen i koji nema niti jedan nedostatak, ali zato postoje proaktivne i reaktivne metode zaštite koje se mogu koristiti u različitim trenucima. Eliminiranjem potencijalno nepoželjnih događaja, poštivanjem najvažnijih normi i sigurnosnih standarda neće se rizik u potpunosti izbaciti, međutim može ga se smanjiti

na zanemarivu i prihvatljivu mjeru. Informacije predstavljaju važan alat kojim se može pomoći i olakšati razumijevanje, a mogu se neželjeno iskoristiti kako bi se nekome nanijeti šteta. Većinom osobe koje su napadnute nisu svjesne toga sve do trenutka pada sustava ili uskraćivanja usluge. U kontekstu samog informacijskog sustava važno je podijeliti informacije prema prioritetima odnosno prema potrebi. Svi zaposlenici unutar sustava ne trebaju imati isti pristup prema svim informacijama ako nisu usko vezana uz njihova zaduženja, jer to može predstavljati potencijalni sigurnosni rizik. U nekim slučajevima pristup informacijama je važan, kao primjerice raspored radnog vremena na poslu koji mora biti dostupan svim zaposlenicima kako bi osigurao nesmetano odvijanje.

Jedan od važnih dijelova informacijske sigurnosti se odnosi također i na odgovorno ponašanje na internetu, koje uključuje izbjegavanje sumnjivih stranica, mailova koji su pristigli od nepoznatih pošiljatelja i odgovornost u radu s podacima tijekom internetskih transakcija. Svijest o mogućnosti da dođe do gubitka podataka ili druge štete korištenjem interneta je prvi i najvažniji preduvjet da korisnik ostane siguran privatno i na poslu, jer ako padne sustav zbog nesavjesnog korištenja i nepridržavanja uputa može doći do katastrofalnih posljedica, gdje su u pitanju spašavanje i sigurnost ljudi.

LITERATURA

[1] Fakultet prometnih znanosti, „Uvod u informacijske sustave“ dostupno na: https://www.fpz.unizg.hr/ztos/iszp/a2.pdf (14.08.2020.)

[2] Element, „Poslovni informacijski sustavi“, dostupno na: https://element.hr/wp-content/uploads/2020/06/unutra-13646.pdf (14.08.2020.)

[3] Sveučilište u Zadru, „Informacijski sustavi“, dostupno na: http://www.unizd.hr/portals/4/nastavni_mat/1_godina/info/predavanje_2.pdf (14.08.2020.)

[4] Mujarić E.,“Računalne mreže“, dostupno na:

http://mreze.layer-x.com/s010400-0.html (14.08.2020.)

[5] Markov P., „Analiza značaja ICT za poslovanje turoperatera“, završni rad, Sveučilište u Splitu, 2017., dostupno na: https://core.ac.uk/download/pdf/198107663.pdf (15.08.2020.)

[6] Čuljak I., „Erp sustavi u poslovanju poduzeća“, diplomski rad, Veleučilište u Požegi, Požega 2018 (preuzeto, 15.08.2020.)

[7] Hrvatska udruga banaka, dostupno na: https://www.hub.hr/sigurnost-na-internetu/vrste-prijevara/malware (15.08.2020.)

[8] CERT, „Sigurnije na internetu“, dostupno na: https://www.cert.hr/wp-content/uploads/2018/02/Sigurnije_na_internetu.pdf (15.08.2020.)

[9] Slika „Trojan Horse“, dostupno na: http://1.bp.blogspot.com/-QcQxputrMaI/Twst429MOPI/AAAAAAAADiU/tl6yP-0D46s/s1600/trojan-horse-virus.png

[10] CERT, „Conficker“,dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-03-294.pdf (15.08.2020.)

[11] Kralj D., „Primjena računala“,dostupno na: http://www.vuka.hr/fileadmin/user_upload/knjiznica/on_line_izdanja/Damir_Kralj-Primjena_racunala.pdf

[12] Hrvatska udruga banaka, „Vrste prijevara“ dostupno na: https://www.hub.hr/hr/sigurnost-na-internetu/vrste-prijevara/drustvene-mreze-i-krada-identiteta (15.08.2020.)

[13] CERT, „O socijalnom inženjeringu“, dostupno na: http://www.cert.hr/socijalni_inzenjering (15.08.2020)

[14] ClickSSL, „Types Of Internet Security Threats“, dostupno na: https://www.clickssl.net/blog/types-of-internet-security-threats-and-preventions/2 (15.08.2020)

[15] Centar informacijske sigurnosti, „Napadi umetanjem SQL koda“, dostupno na: https://www.cis.hr/dokumenti/2608-napadiumetanjemsqlkoda.html (15.08.2020)

[16] Slika, “Example of SQL injection“, dostupno na: http://slideplayer.com/slide/6836897/23/images/4/Example+of+SQL+injection.jpg

[17] CERT, „Napadi uskraćivanjem resursa“, dostupno na: https://www.cert.hr/wp-content/uploads/2006/08/CCERT-PUBDOC-2006-07-162.pdf (16.08.2020)

[18] Centar informacijske sigurnosti, „Napadi uskraćivanjem resursa“, dostupno na: https://www.cis.hr/www.edicija/Napadiuskraivanjemresursa.html (16.08.2020)

[19] CERT, „Ranjivost“, dostupno na: https://www.cert.hr/ranjivosti/ (16.08.2020)

[20] Hrvatska vatrogasna zajednica, „Informatizacija“, dostupno na: https://hvz.gov.hr/informatizacija/81 (16.08.2020)

[21] Hrvatska vatrogasna zajednica, „VATROnet“, dostupno na: https://hvz.gov.hr/istaknute-teme/informatizacija/vatronet/97

(16.08.2020)

[22] Hrvatska vatrogasna zajednica, „Održavanje i korištenje informacisjkih sustava HVZ“, dostupno na: https://hvz.gov.hr/UserDocsImages//Informatizacija//Odr%C5%BEavanje%20i%20kori%C5%A1tenje%20IS%20HVZ.pdf (16.08.2020)

[23] Hrvatska vatrogasna zajednica, „ Interaktivna baza opasnih tvari“, dostupno na: https://hvz.gov.hr/istaknute-teme/informatizacija/interaktivna-baza-opasnih-tvari/99 (17.08.2020)

[24] Hrvatska vatrogasna zajednica, „ Sustav upravljanje vatrogasnim intervencijama“, dostupno na: https://hvz.gov.hr/istaknute-teme/informatizacija/sustav-upravljanje-vatrogasnim-intervencijama/101 (17.08.2020)

[25] Hrvatska vatrogasna zajednica, „Sustav za uzbunjivanje“, dostupno na: https://hvz.gov.hr/istaknute-teme/informatizacija/sustav-za-uzbunjivanje/100 (17.08.2020)

[26] Hadljina N. prof. Dr. Sc., „Zaštita i sigurnost informacijskih sustava“, Fakultet elektrotehnike i računarstva, dostupno na: https://www.academia.edu/40437665/ZA%C5%A0TITA_I_SIGURNOST_INFORMACIONIH_SISTEMA (18.08.2020)

[27] Bukovac T, Sigurnost informacijskih sustava, Diplomski rad, Sveučilište u Zagrebu, Filozofski fakultet, Zagreb, 2016., dostupno na: http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf (18.08.2020)

[28] CERT, „Sigurnosna politika“, dostupno na: https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf (18.08.2020)

[29] CERT, „Fizička zaštita informacijskih sustava“, dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf (18.08.2020)

[30] CERT, „Nacionalni program informacijske sigurnosti u Republici Hrvatskoj“, dostupno na: https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2005-04-110.pdf (18.08.2020)

[31] Zakon o informacijskoj sigurnosti, dostupno na: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti

[32] Zakon o tajnosti podataka, dostupno na: https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka

[33] Zakon o zaštitit osobnih podataka, dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html

[34] CERT, „O nacionalnom CERT-u“, dostupno na: http://www.cert.hr/onama (19.08.2020.)

[35] Centar informacijske sigurnosti , „Napadi umetanjem SQL koda“, dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2011-09-025.pdf (19.08.2020.)

[36] CERT, „Ranjivost“, dostupno na: https://www.cert.hr/ranjivosti/ (20.08.2020.)

[37] Kangeronline, „PGP šifriranje“, dostupno na: https://kangeronline.com/page-4/pgp-ifriranje-vodi-za-poetnike/

[38] Peraković D. dr.sc., „Sigurnost i zaštita informacijsko komunikacijskog sustava“,nastavni materijali, Fakultet prometnih znanosti, dostupno na: http://e-student.fpz.hr/Predmeti/S/Sigurnost_i_zastita_informacijsko_komunikacijskog_sustava/Materijali/SZIKS_-_P01-P02-S01-P03-P4-P5-S02-P06-P07-S03-P08-P9-S04.pdf (19.08.2020.)

[39] 911.gov, „Cyber risks to Next Generation 9-1-1“, dostupno na: https://www.911.gov/pdf/OEC_NG911_Cybersecurity_Primer_May_2018.pdf (21.08.2020)

[40] Otvoreni sustavi i sigurnost, „Procjena rizika“, dostupno na:

https://security.foi.hr/wiki/index.php/Procjena_rizika.html (21.04.2021.)

[41] Jutarnji list, „ Velike poteškoće s HT-ovom mrežom“, dostupno na: https://www.jutarnji.hr/life/tehnologija/velike-poteskoce-s-ht-ovom-mrezom-objavljeni-zamjenski-brojevi-hitne-vatrogasaca-i-centra-112-15021888 (10.06.2021.)

PRILOZI

POPIS SKRAĆENICA

CERT (*Computer Emergency Response Team*) – specijalizirana ustanova za provođenje prevencije i zaštite protiv računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj

DoS (*Denial of Service*) - napadi uskraćivanjem resursa

DoS stanje – stanje u kojem je usluga uskraćena

IK - Informacijsko – komunikacijski

PGP (Pretty Good Privacy) – besplatan kriptografski alat za šifriranje komunikacije preko maila

SQL umetanje – metoda ubacivanja SQL koda sa ciljem

SQL (*Structured Query Language* – strukturirani jezik za upite

NG 9-1-1(next generation) sljedeća generacija 911

PSAP (engl. *public-safety answering point*) Call centar u koji dolaze svi pozivi prema hitnim službama

POPIS SLIKA

POPIS TABLICA