Sigurnost podataka kao čimbenik zaštite života i zdravlja

Varga, Željko

VELEUČILIŠTE U KARLOVCU

SPECIJALISTIČKI STUDIJ SIGURNOSTI I ZAŠTITE

Željko Varga

SIGURNOST PODATAKA KAO ČIMBENIK ZAŠTITE ŽIVOTA I ZDRAVLJA

ZAVRŠNI RAD

Karlovac, 2015.

VELEUČILIŠTE U KARLOVCU

SPECIJALISTIČKI STUDIJ SIGURNOSTI I ZAŠTITE

Smjer: Zaštita na radu

SIGURNOST PODATAKA KAO ČIMBENIK ZAŠTITE ŽIVOTA I ZDRAVLJA

ZAVRŠNI RAD

Mentor:
dr.sc. Damir Kralj

Student:
Željko Varga

Karlovac, 2015.

Sažetak

Područje interesa ovog završnog rada usmjereno je na rizične ljudske djelatnosti, kao što su oružane snage (vojska, policija) te neke druge organizacije s delikatnim područjem djelovanja npr. procesna i kemijska industrija te istraživački instituti u kojima se rukuje opasnim materijalima i elementima koji su im potrebni u području njihovog istraživanja. Isto tako ovim radom bi željeli skrenuti pozornost na značaj sigurnosti informacija i podataka kao ključnog čimbenika prevencije od opasnih događaja do kojih bi moglo doći u slučaju da povjerljivi podaci i informacije dođu u posjed raznim nepoželjnim skupinama i pojedincima koje bi navedeno mogli iskoristiti i upotrijebiti za nanošenje materijalne štete ili ugrožavanje života i zdravlja ljudi. Takvi podaci ne smiju biti javno dostupni (moraju biti tajni). Dakle, cilj je postizanje visokog stupnja sigurnosti i zaštite podataka i informacija, a definiranje sigurnosne politike zasigurno je jedan od najboljih programa.

Ključne riječi: informacijski sustavi, zaštita podataka, zaštita života i zdravlja, visoko rizične djelatnosti, sigurnosni rizici i prijetnje, terorizam, sigurnosna politika, kriptologija.

Summary

The scope of this final thesis covers different areas of risky human activities e.g. various forms of armed forces (army, police) and other organizations with delicate operation areas, such as process and chemical industry and various research institutes which are handling with hazardous materials and elements needed in their area of research. With this thesis we would also like to draw attention on importance of the information and data security as a key-factor for prevention of the hazardous events that might occur in cases such as when confidential data and information get in possession by undesirable groups and individuals, which may use it to commit great material damage or threat to public life and health. Such data should be publicly unavailable (restricted or secret). So, the goal is to achieve a sufficiently high level of data and information security and protection, and defining the security policy is definitely one of the best programs.

Keywords: information systems, data protection, protection of life and health, high-risk activities, security risks and threats, terrorism, security policy, cryptology.

ZAHVALA

Posebno bih se zahvalio mentoru dr.sc. Damiru Kralju na ukazanom povjerenju, pruženoj pomoći i stručnim savjetima prilikom izrade Završnog rada.

Isto tako zahvalio bi svojoj obitelji na razumijevanju i velikoj podršci tijekom studiranja uz rad i završetku specijalističkog diplomskog studija.

Sadržaj

1. Uvod

Informacija *(eng.-information)* je podatak o nekoj činjenici ili izvještaj o čemu [1]. Informacije se javljaju u više oblika a mogu biti zapisane na papiru, pohranjene u elektroničkom obliku, sačuvane na filmu, mogu se prenositi poštom ili elektroničkim putem. Bez obzira u kojem je obliku pohranjena, informacija mora biti uvijek prikladno zaštićena. Zbog distribuiranosti poslovne okoline, informacije su izložene većem broju prijetnji i ranjivosti. Da bi informacija bila zaštićena nužno je poduzeti velik broj radnji u smislu implementacije kontrola sigurnosti u informacijski sustav i osigurati suradnju i prihvaćanje sigurnosnih pravila od strane korisnika.

Informacijski sustav (*eng.-information system*) je organizacijski adekvatno i funkcionalno usmjeren sustav djelovanja sa zadatkom da prikuplja, memorira, obrađuje i distribuira podatke i informacije korisnicima. Sigurnost informacijskih sustava vrlo je kompleksna i široka tema u kojoj je jasna jedino činjenica da bez kvalitetnog programa sigurnosti, sustav nije moguće u cijelosti zaštititi. Kvalitetni programi omogućavaju uspostavu sigurnosti na svim kritičnim točkama sustava, kao i u bilo kojem segmentu sigurnosti. Za kvalitetan rad potrebno je zaštiti informacije od:

- neovlaštenih izmjena - osigurati **integritet,**
- objavljivanja tajnih informacija - osigurati **tajnost,**
- uskraćivanja dostupnosti informacija ovlaštenim korisnicima - osigurati **dostupnost.**

Sigurnosni rizici za računalo i sadržane podatke korisnika postaje u više oblika:

- *krađa podataka,*
- *neovlašten pristup podacima,*
- *gubitak podataka zbog kvara sustava ili prekida napajanja,*
- *gubitak podataka zbog napada virusa [2]* .

Rizične djelatnosti u Republici Hrvatskoj su oružane snage i neke druge organizacije s delikatnim područjem djelovanja kao što su npr. procesna i kemijska industrija te istraživački instituti u kojima se rukuje opasnim materijalima i elementima koji su im potrebni u području njihovog istraživanja. Informacije i podaci koji se pohranjuju ili prenose u navedenim djelatnostima o opasnim robama, materijalima i elementima su imovina te jedan od najvažnijih i najskupljih resursa u poslovanju i korištenju i kao takvu ju je potrebno prikladno zaštiti. Njihovo pravovremeno posjedovanje, njena ispravnost i tajnost često je od odlučujuće važnosti u poslovanju bilo koje institucije.

Kada bi neke nepoželjne skupine i organizacije mogle doći u posjed značajnim informacijama a kasnije i u posjed opasnih roba, materijala i elemenata s njima bi mogli ugroziti život i zdravlje ljudi.

Za čovječanstvo velika su prijetnja teroristi koji su organizirani u razne terorističke skupine i organizacije. Iz dana u dan su sve stručniji i sve nepredvidivi. Jako im se teško suprotstaviti pa je uz osiguranje sigurnosnih mjera i vrhunske tehnologije potrebno razvijati znanstvene resurse kojima bi se ugrožene države mogle oduprijeti i pružiti odgovarajuća rješenja. U današnjem svijetu mala je vjerojatnost uporabe velikih količina radioloških, bioloških, nuklearnih i kemijskih agenasa isto tako ni ratovanje oružjem za masovno uništenje već je veća mogućnost djelovanja neke terorističke skupine uporabom manjih količina agensa. Kako bi se što učinkovitije moglo oduprijeti današnjim terorističkim prijetnjama, treba uspostaviti obrambeni model po kojem je potrebno djelovati.

Obrambeni model bi trebao biti povezan u suradnji znanosti, obrane i sigurnosti. U suvremenim zemljama model po kojem se provodi nadzor je povezani međuresorni sustav ministarstava te ustanova i smatra se najučinkovitijim i najracionalnijim. U Republici Hrvatskoj Vlada kao izvršna vlast trebala bi upravljati neposredno ili posredno s takvim sustavom jer se u njemu obavljaju poslovi od nacionalnog interesa. Za razvoj sustava jedino Vlada raspolaže ljudskim i materijalnim resursima. Sustav treba neprestano i učinkovito funkcionirati, posebno kod terorizma ili akcidenta. Posebno mjesto u sustavu imaju laboratoriji koji se bave problematikom nuklearno-biološko-kemijske obrane. Sastavni i najvažniji dio sustava su metode detekcije i identifikacije radioloških, bioloških i kemijskih *noksi [1]*. *Noksa* (*lat. Noxa*) je nešto što štetno djeluje na zdravlje, naziv za bilo kakvog uzročnika bolesti. Sustav može omogućiti cjelovito i kvalitetno provođenje svih mjera sigurnosti u obrani od najvećih sigurnosnih ugroza.

Osim opasnosti od radioloških, bioloških, nuklearnih i kemijskih agenasa postoje opasnosti od gomilanja malog i lakog oružja te pripadajućeg streljiva. Poznato je da smanjenje, nezakonitog posjedovanja i korištenja oružja je jedan od ključnih preduvjeta sigurnosti i stabilnosti svake države, pa tako i Republike Hrvatske. Do sad u Republici Hrvatskoj uz poticaj stranih institucija npr. (*eng. Small Arms and Light Weapons (SALW)*) organizirale su se u nekoliko navrata akcije prikupljanja raznog oružja i pripadajućeg streljiva zaostalog iz domovinskog rata. Akcije pod nazivom: "Zbogom oružje", "Manje oružja – manje tragedija ", pridonijele su smanjenju oružja, međutim još ne u dovoljnoj mjeri.

Hipoteza na koju ćemo pokušati odgovoriti u ovom radu je: "Važnost zaštite podataka i informacija u specifičnim i rizičnim ljudskim djelatnostima bitan je čimbenik života i zdravlja ljudi".

2. Specifične i rizične djelatnosti

2.1. Oružane snage

Oružane snage u Republici Hrvatskoj sačinjavaju vojska i policija. Sredstva i materijali kojima oružane snage rukuju mogle bi predstavljati određenu opasnost za sigurnost života i zdravlja ljudi.

Za sada u oružanim snagama nema opasnosti od nuklearnog goriva jer se ne posjeduju podmornice na nuklearni pogon, međutim radioaktivni element nastaje u reaktoru nuklearne elektrane "Krško" (opširnije u poglavlju 2.4. Nuklearna elektrana "Krško") pa bi mogao biti na meti neželjenih skupina. U svijetu postoji ova vrsta rizika i opasnosti i to u lukama na zapadnoj obali poluotoka Krima u središtu Crnog mora koji je bio izdvojen iz Autonomne pokrajine Krim i bio je pod upravom Kijeva i predsjednika Ukrajine (Slika 1). Međutim početkom Ukrajinske krize na Krim je 18. ožujka 2014. godine izvršena ruska invazija, nakon čega je poluotok priključen Ruskoj federaciji. U lukama Crnog mora prema Harkivskom sporazumu trebala bi boraviti do 2042. godine ruska Crnomorska flota [3].

Slika 1- Nuklearna podmornica u luci Sevastopolj u Crnom moru [3].

Kod opasnosti i zlouporabe (visoko) radioaktivnog otpada (istrošeno nuklearno gorivo), postoje dva gledišta [4]:

- tehnički,
- politički.

Tehničko gledište su nuklearni reaktori u pogonu projektirani tako da su količine Pu[1] (moguće iskoristiti za vojnu uporabu) zanemarive i nemoguće primijeniti bez prethodne prerade goriva. Proces prerade istrošenog nuklearnog goriva, skup je i opasan proces tako nekoliko zemalja u svijetu posjeduje tehnologiju za ekstrakciju plutonija.

Političko gledište je zanimljivije, naime mnoge države potpisale su ugovore (konvencije i različite aranžmane) kojim se sprječava moguća zlouporaba. Na globalnoj razini, za potrebe praćenja provedbe ugovora „nuklearno oružje“ i osiguranje razvoja nuklearne energije u miroljubive svrhe osnovana je 1957. godine od strane Ujedinjenih naroda (UN-a) International Atomic Energy Agency (IAEA), (hrv. Međunarodna agencija za atomsku energiju). IAEA provodi redovne inspekcije civilnih nuklearnih postrojenja te prati inventar i transport radioaktivnih materijala.

U Hrvatskoj bi veći rizik i opasnosti mogle biti velike količine malog i lakog oružja (Slika 2, 3 i 4) i pripadajuće streljivo te minsko-eksplozivnih sredstava, obzirom da su akumulirane tijekom Domovinskog rata. Po završetku rata najveći dio oružja, pripadajućeg streljiva i eksplozivnih sredstava stavljen je pod nadzor oružanih snaga. Ako bi u posjed terorističkim skupinama i organizacijama stigle veće količine navedenih sredstava, iste bi se mogle iskoristiti za terorističke napade.

Slika 2 - Razno vojno naoružanje [5].

1 Pu- plutonij – radioaktivni element, nastaje u nuklearnom reaktoru djelovanjem neutrona, služi kao nuklearno gorivo i kao eksploziv u nuklearnim bombama;

Slika 3 – Inačice automatske puške [6].

Slika 4 - Razne strojnice [7].

2.1.1. Analiza stanja

Jedan od ključnih elemenata i preduvjeta za sigurnost Republike Hrvatske je suzbijanje nezakonitog posjedovanja i učinkovita kontrola malog i lakog oružja. Područje Republike Hrvatske pogodno je za krijumčarenje oružja u zapadnu Europu zbog svog specifičnog geostrateškog položaja te kao tranzitno područje presijeca ju tzv. "Balkanska ruta". Republika Hrvatska je u proteklom razdoblju sustavno smanjivala nezakonito posjedovanje oružja te poduzela niz mjera i aktivnosti. Akcija Ministarstva unutarnjih poslova pod nazivom "Zbogom oružje" tijekom 2002. godine, omogućila je predaju neregistriranog oružja bez sankcija ili ga je bilo potrebno legalizirati. Isto tako bila je uspješna kampanja "Manje oružja – manje tragedija" koja se od 2007. godine provodila u suradnji s Programom UN-a za razvoj, skraćeno (UNDP od *eng. United Nations Development Programme).* UNDP-i predstavlja najveći multilateralni izvor razvojne pomoći u svijetu.

2.1.2. Nacionalna strategija i Akcijski plana za kontrolu malog i lakog oružja

U svrhu kontrole i smanjenja Vlada Republike Hrvatske donijela je Nacionalnu strategiju za kontrolu malog i lakog oružja s pripadajućim Akcijskim planom. Akcijski plan sadrži jasno definirane mjere za unapređenje dosadašnjih aktivnosti u ovom području, a s ciljem stvaranja što sigurnijeg okruženja za hrvatske građane [8].

Cilj nacionalne strategije.

Opći cilj Nacionalne strategije je izgradnja učinkovitijeg sustava kontrole malog i lakog oružja u svim njegovim segmentima, a prvenstveno u vezi sa:

- suzbijanjem nezakonite proizvodnje i trgovine oružjem,
- usklađivanjem nacionalnog zakonodavstva sa standardima EU, UN i OESS-a,
- osiguranjem dosljedne primjene zakona i propisa, te provođenjem jedinstvene i učinkovitije kaznene politike,
- sigurnijim i učinkovitijim upravljanjem zalihama oružja,
- provođenjem programa povećanja opće sigurnosti smanjenjem količine oružja u zakonitom i nezakonitom posjedu, uključujući medijske kampanje, te akcije prikupljanja i uništavanja oružja.

Operativni ciljevi nacionalne strategije.

Radi ostvarenja općeg cilja, Nacionalna strategija postavlja jedanaest operativnih ciljeva koji su detaljnije razrađeni kroz tekst Nacionalne strategije i pripadajućeg Akcijskog plana.

"Operativni ciljevi su sljedeći:

OC1–Smanjenje količine oružja dostupnog za nezakonite aktivnosti,

OC2–Smanjenje broja nesreća prouzrokovanih upotrebom oružja i streljiva,

OC3–Smanjenje vidljive prisutnosti oružja u zajednici, te borba protiv kulture naoružanja,

OC4–Podizanje svijesti javnosti o problemu velikog broja komada malog oružja,

OC5–Provođenje aktivnosti u cilju suzbijanja nezakonite trgovine oružjem,

OC6–Djelotvornija provedba međunarodnih mjera radi prevencije, borbe protiv i iskorjenjivanja nezakonite trgovine malim i lakim oružjem,

OC7–Uspostava učinkovitijeg informacijskog sustava,

OC8–Poduzimanje odgovarajućih mjera radi sprječavanja kršenja embarga na oružje Vijeća sigurnosti Ujedinjenih naroda, Europske unije i drugih embarga koji proizlaze iz međunarodnih obveza Republike Hrvatske,

OC9–Poboljšanje pravnih propisa kojima će se utvrditi standardi i procedure u vezi sa skladištenjem, upravljanjem i sigurnošću oružja u posjedu oružanih snaga Republike Hrvatske,

OC10–Nastavak aktivnosti pojačanog uništavanja malog i lakog oružja i streljiva određenog za uništavanje,

OC11–Ostvarivanje suradnje s drugim državama i međunarodnim i regionalnim organizacijama na razvijanju i jačanju partnerstva u cilju razmjene informacijama i suzbijanju organiziranog kriminala."[8].

2.1.3. Prijedlog poboljšanja

S obzirom na smanjivanje brojnog stanja pripadnika oružanih snaga Republike Hrvatske potrebna je reorganizacija i smanjenje broja skladišnih objekata u kojima se skladišti oružje i streljivo. To se posebno odnosi na skladišta streljiva zbog čega se iz neperspektivnih skladišnih objekata streljivo postupno premješta u perspektivna (bolje tehnički uređena skladišta). Dinamika premještanja ovisi o raspoloživim financijskim sredstvima, kao i dinamici kojom se smanjuje ukupno raspoloživa količina streljiva temeljem uništavanja, prodaje ili donacije. Prijedlog poboljšanja je da se iz fondova EU kroz projekte ubrza preseljenje u sigurnija skladišta koja treba tehnički opremiti odgovarajućom opremom kako bi se sigurnije skladištilo. Isto tako potrebno je poboljšanje evidencija službenog uskladištenog oružja, streljiva te eksplozivnih sredstava u cilju što boljeg uvida i praćenja navedenog.

2.3. Institut "Ruđer Bošković"

Institut “Ruđer Bošković” (IRB) je institucija koja je smještena u samom središtu Zagreba, okružena je gradskim naseljima sa velikim brojem stanovnika. Već 30 godina na Institutu se skladišti nisko radioaktivni otpad u manjim količinama. U razmišljanju dosadašnjih vlasti, tamo bi se ubuduće skladištile kompletne količine radioaktivnog otpada koji nastaje u medicinskim, istraživačkim te gospodarskim subjektima diljem Hrvatske [9]. Obzirom da se u IRB-u otpad prvo kategorizira, potom odlaže u bačve od nehrđajućeg čelika, smješta na plastificiranu površinu i pod konstantnim je sigurnosnim nadzorom, odlučilo se da središnje mjesto za sav hrvatski radioaktivni otpad bude IRB. Tamo se za sada skladišti sav hrvatski radioaktivni otpad koji nastaje u Hrvatskoj na dnevnoj bazi manje od jednoga kubičnog metra radioaktivnog otpada iz sve tri grane, medicine, istraživačke djelatnosti i industrije. Dosad se taj otpad deponirao na običnim odlagalištima, što je neprimjereno. Međutim i dalje je činjenica da Hrvatska ima dva gotovo 50 godina stara skladišta radioaktivnog materijala iz medicinskih izvora, koja se nalaze u centru metropole, koja je, uzgred rečeno, na vrlo trusnom području pa su sva naklapanja o riziku kojeg svi žele izbjeći posve apsurdna. U Zagrebu na dvije lokacije danas je pohranjeno oko 7,5 kubika radionuklida nastalih kroz korištenje ionizirajućeg zračenja u raznim vrstama medicinskih, građevinskih i elektronskih uređaja. Danas se taj materijal skladišti u IRB-u i Institutu za medicinska istraživanja i medicinu rada, no ista su dugoročno neadekvatna za tu namjenu, te trajno rješenje za ovaj otpad mora biti pronađeno. Republika Hrvatska je prema EU regulativi, trebala već napraviti plan za izgradnju trajnih odlagališta otpada.

2.4. Nuklearna elektrana "Krško"

Krajem prošle godine Hrvatska i Slovenija usuglasile su se o produljenju rada nuklearne elektrane Krško (NE Krško) nakon 2023. Dakle, NE Krško radit će do 2043. godine. Duži rad elektrane implicira i veću količinu iskorištenog nuklearnog goriva koje će trebati zbrinuti. Privremeno skladište elektrane napunjeno je do čak 95% nisko i srednje radioaktivnim otpadom, pa su u elektrani primorani kreativno rješavati problem skladištenja do izgradnje skladišta. Prema procjenama 2023. bit će potrebno zbrinuti oko devet tisuća tona radioaktivnog otpada i 870 tona istrošenog goriva. Bude li elektrana doista radila do 2043. godine te količine rastu na 10.200 tona radioaktivnog otpada i 1.000 tona istrošenog goriva.

2.5. Radioaktivni otpad

Radioaktivni je otpad posebna kategorija industrijskog ili opasnog otpada koji u posljednje vrijeme dobiva sve veće značenje. Nastaje prilikom rudarenja, pripreme goriva, reprocesinga, a otpad su i otpaci nastali u postrojenjima. Radioaktivni se otpad ne proizvodi samo u onim zemljama koje imaju nuklearne elektrane za proizvodnju električne energije, već nastaje u mnogim drugim djelatnostima poput radioterapije ili industrijskih testiranja. Dakle, osim u nuklearnoj energetici radioaktivni otpaci nastaju i u medicini, pri istraživanjima, ali i u industriji. Njegovo sigurno odlaganje i upravljanje njime (Slika 5) izazov je za sve zemlje bez obzira na njihov stav o nuklearnoj energiji [10].

Slika 5 - Prijevoz istrošenog goriva u spremnicima [10].

Za način odlaganja osobito je važno o kojoj je vrsti radioaktivnog otpada riječ i kakva su mu obilježja. Postupci klasifikacije radioaktivnog otpada razvrstavaju otpade prema fizikalnim, kemijskim i radiološkim svojstvima koja su važna za određeni skup operativnih zahtjeva s kojima se susreće onaj koji o otpadu skrbi.

Klasifikacija radioaktivnog otpada kojom se koristi Međunarodna agencija za atomsku energiju (IAEA) kombinira skrb o dugoročnoj sigurnosti s onoj dnevnoj ili operativnoj sigurnosti.

Klasifikacija je usvojena od više međunarodnih organizacija te uobličena u Temeljne standarde sigurnosti pri zaštiti od ionizirajućih zračenja i za sigurnost izvora zračenja. Radioaktivni otpad je karakteriziran trajnošću (kratkotrajni, dugotrajni) i rastućim intenzitetom zračenja (niskoradioaktivni, srednjeradioaktivni i visokoradioaktivni). Vrsta i debljina operativnih štitova važno je klasifikacijsko obilježje intenziteta zračenja otpada kao bi se s otpadom moglo sigurno rukovati ili ga sigurno izolirati. Količina topline koju oslobađa otpad sljedeće je važno obilježje za dugoročnu i za operativnu sigurnost.

Visokoradioaktivni otpad nastaje kada se iz istrošenog goriva izdvoje fisibilni i oplodni nuklidi. Da bi se zaštitilo zdravlje ljudi i okoliš, sada i u budućnosti, bez prenošenja nepotrebnog tereta na nove naraštaje, razvijen je niz strategija i koncepata skrbi o kratkotrajnim i dugotrajnim radioaktivnim otpadima [11]. Neke se strategije primjenjuju, neke se još razvijaju. Od svih razmatranih ili ispitivanih načina odlaganja samo se odlaganje u tlo danas smatra prihvatljivim Ostale mogućnosti nemaju dostatnu razinu nadzora, osjetljive su na međunarodne prigovore, ili znače neprihvatljivo velik rizik. Štoviše, još uvijek ni jedan način odlaganja ne otklanja potrebu za odlaganjem u tlu. Otpad koji sadrži pretežno kratkoživuće radionuklide ugrožava ljude, ali to je opasnost koja se zbog raspada umanjuje; poslije dovoljno dugog vremena, koje može biti i nekoliko stotina godina, opasnost pada na razinu kod koje više nema rizika za ljudsko zdravlje ili okoliš.

2.6. Postrojenja za proizvodnju kemijskih proizvoda

Postrojenja za proizvodnju kemijskih tvari koje se sastoje od funkcionalno povezanih jedinica:

- proizvodnja temeljnih organskih kemikalija,
- proizvodnja temeljnih anorganskih kemikalija,
- proizvodnja temeljnih proizvoda za zaštitu bilja i biocida,
- proizvodnja umjetnih gnojiva na bazi fosfora, dušika, kalija,
- proizvodnja osnovnih farmaceutskih proizvoda uporabom kemijskih ili bioloških postupaka,
- proizvodnja eksploziva.

3. Sustav Bionadzora

Kako bi vlada RH mogla objedinjeno i centralizirano pratila gore navedeno stanje u specifičnim i rizičnim ljudskim djelatnostima te u sprezi znanosti, obrane i sigurnosti i međuresornim sustavom ministarstva i ustanovama, organizira se model sustava Bionadzora s obzirom na to da ista raspolaže s resursima (ljudski i materijalni) [12].

Sustav Bionadzora je cjelina od sastavnica koja djeluje objedinjeno i centralizirano kao da je sve na jednom mjestu, iako su lokacije na različitim mjestima.

Navedena cjelina sustava Bionadzora operativno je uvezana preko tzv. Središnjeg zapovjedništva.

3.1. Sastavnice sustava Bionadzora

Glavne sastavnice sustava Bionadzora su sljedeće:

- oružane snage (vojska i policija);
- obavještajne službe;
- civilna zaštita,
- javno zdravstvo,
- toksikološke ustanove i
- meteorološke ustanove (jedinice).

Svaka od sastavnica sustava u navedenim područjima pridonosi svojim radom kojim se bavi. Informacije i podaci skupljaju se u kompletnu sliku situacije ili prostora. Ove resurse mora razvijati svaka država pa tako i Republika Hrvatska. U najvećem opsegu vojska obavlja i provodi obrambeno-sigurnosnu sastavnicu sustava Bionadzora zbog svojih ljudskih i materijalnih resursa.

3.2. Aktivnosti sustava Bionadzora

Sustav Bionadzora provodi sljedeće aktivnosti prilikom obrane od terorizma *noksama*:

- Preventivno:
  - obavještajni,
  - stručni i znanstveni rad,
  - edukacija i komunikacija.

- Pravovremeno otkrivanje:
  - nuklearni, biološki i kemijski detektori i senzori.
- Identifikacija (karakterizacija) *noksi* (bojni otrovi, biološki agensi, zračenja):
  - vojni laboratoriji,
  - sredstva sanacije, dekontaminacije i zbrinjavanje žrtava.

U učinkovitom sprječavanju posljedica od kemijskog ili biološkog oružja, kako u vojnim operacijama tako i u slučajevima terorizma, važan i neizostavan element je brza detekcija i precizna identifikacija *noksi*.

U obrani od terorizma, trebao bi biti uspostavljen sustav detekcije i identifikacije bioloških i kemijskih agensa, a zatim i uzbunjivanja, može imati presudnu važnost u razvoju situacije, broju žrtava i ostalim posljedicama. U okviru problematike kemijskog terorizma zasnovanog na primjeni noksi, na prvom mjestu su bojni otrovi.

Bojni otrovi i njihovi prekursori definirani su Zakonom o potvrđivanju Konvencije o zabrani razvijanja, proizvodnje, gomilanja i korištenja kemijskog oružja i o njegovom uništenju ("Narodne Novine", Međunarodni ugovori, br. 4 od 13. travnja 1995. godine). Mora se naglasiti da su u Članku 2. Konvencije, definirane svrhe koje nisu zabranjene po ovoj Konvenciji (između ostalog, tu su i istraživačke svrhe), jer je nemoguće odvojiti istraživanja i identifikaciju bojnih otrova od rada s njima. U poglavlju vezanom za inspekcije i verifikacije, Konvencija nalaže količinu kemikalija (masu) dopuštenu po pojedinim skupinama i popisima. Za identifikaciju bojnih otrova danas se koriste instrumentalne odnosno fizikalne metode koje se temelje na fizikalnim promjenama tvari ili fizikalnih svojstava. Najraširenija i veoma pouzdana metoda je plinsko-masena spektrometrija (GC/MS). Osim toga, postoje kombinacije dva spektrometra masa (MS-MS) gdje se smjesa spojeva razdvoji na sastavne spojeve, a zatim na fragmente, te kombinacija GC-MS-MS koja je pogodna za identifikaciju smjesa bioloških komponenti i bojnih otrova. Analize identifikacije bojnih otrova potrebno je provoditi pod zaštitnom opremom. Metodologija mjera sigurnosti u području obrane od bioloških *noksi* ne provodi se samo Bionadzorom, već i mjerama biozaštite *(eng. biosafety)* i biosigurnosti *(eng. biosecurity)*.

Države članice Konvencije o zabrani razvoja, proizvodnje i skladištenja biološkog i toksičnog oružja (BTCW) definiraju dva pojma: biozaštite i biosigurnosti.

- Biozaštita uključuje načela, tehnologije, praksu te mjere implementirane u prevenciji akcidenata (otpuštanje i širenje agensa) ili nenamjernih izlaganja biološkim agensima, toksinima i zaštitu ljudi te okoliša od širenja i izlaganja agensima kao i toksinima.
- Biosigurnost uključuje mjere zaštite i nadzora "Biohazard" prostora implementirane u prevenciju neovlaštenog ulaska i zadržavanja, krađe, prijenosa, diverzije ili namjernog otpuštanja bioloških agensa ili toksina.

Dakle, Biozaštita u cilju sprječavanja oslobađanja opasnih patogena i toksina uključuje mehanizme i načela fizičke zaštite laboratorija i tehnologije, a Biosigurnost uključuje zaštitu i kontrolu opasnih patogena i toksina i njihovo moguće oslobađanje izvan laboratorija i korištenje u ne miroljubive svrhe. U idealnim sustavima zaštite, uzorci zraka, vode i tla se bez obzira na prijetnju napada svakodnevno prikupljaju s određenih, strateški važnih lokacija te se nakon toga obrađuju metodama molekularne biologije u posebno opremljenim laboratorijima. Takvo kontinuirano, "preventivno" praćenje stanja na terenu omogućava pravodobnu i učinkovitu obrambenu aktivnost. Jedna od učinkovitih mjera sigurnosti je krajnji korisnik sustava zaštitne opreme, sustava, instrumentarija, kemikalija, bioloških materijala itd. Tako se preventivno onemogućuju radnje koje bi imale štetne posljedice za društva (npr. priprema i provedba terorističkog akta).

4.Terorizam i ciljevi terorističkih napada

4.1. Terorizam

Terorizam je smišljena, planirana, pažljivo pripremljena, tajno organizirana i provedena nasilna djelatnost (uglavnom ilegalnih, ali u javnosti poznatih) organizacija ili skupina usmjerena na nedemokratsko, nasilno ostvarivanje javno proklamiranih političkih ili drugih ciljeva, a obavljana pod notom "cilj opravdano sredstvo". Danas je terorizam ozbiljan čimbenik destabilizacije nacionalne i međunarodne sigurnosti, s negativnim utjecajem na globalni sustav.

Skupine nositelja terorizma:

1.) krajnje lijevo usmjerenje,

2.) krajnje desno usmjerenje,

3.) radikalno islamske,

4.) nacionalističke i

5.) ostale (organizirani kriminal).

Slika 6 - Napadi na WTC trgovački centar 11. rujna 2001, godine u New Yorku[13].

Slika 7 - Ostaci trgovačkog centra WTC u New Yorku nakon terorističkog napada[13].

Mete terorističkih napada danas su usmjerene na određene pozicije i ciljeve a to su kritična nacionalna infrastruktura : vojska, policija, financije, vanjska politika i pravosuđe.
U velikim gradovima napadi mogu biti na:

- trgovačke centre (Slika 6 i 7),
- sportske priredbe,
- željezničke i autobusne postaje,
- parkove, trgove,
- dostupna javna mjesta gdje se okupljaju veći broj ljudi,
- komunikacijsku i ostalu infrastrukturu.

Obzirom na to da je Republika Hrvatska članica Europske unije, NATO-a te sudjeluje u mirovnim misijama, teritorijalno graniči sa BiH, (neki građani bili su povezani sa terorističkim skupinama), zato postoji određeni rizik od terorizma i u Hrvatskoj.

Slika 8 - Teroristički napad u urede časopisa Charlieja Habdoa u Parizu [14].

Suradnja terorista s organiziranim kriminalom velika je prijetnja sigurnosti europskih zemalja. Suradnja se proširila i na ilegalnu trgovinu oružjem i eksplozivom, a moguće da se i takvom suradnjom teroristi domognu nuklearnih materijala koji mogu poslužiti za izradu opasnih oružja od onih koje su dosad koristili u svojim napadima. Prema stranim izvorima samo u Rusiji organiziranom kriminalu dostupno je oko 1350 tona plutonija, 40 000 komada nuklearnog oružja velike i nepoznate količine materijala koji se može iskoristiti za izradu takozvanih prljavih atomskih bombi [15].

Nadalje, kao drsku ideju naveli bi primjer iz New Yorka gdje su uhićene dvije žene. Kriminalističkom obradom utvrđeno je da su pristaše džihadističke skupine Islamske države (IS). Optužene su da su planirale izraditi bombe te izvesti napad u Sjedinjenim Državama . Ideja je bila da izrade bombe od gnojiva i kalijevog glukonata. U daljnjoj kriminalističkoj obradi pretragom stanova " *pronađeno je velik broj plinskih boca i uputa o njihovoj preinaci u eksplozivne naprave*" [16].

Navedeni primjeri potvrđuju da se terorističke skupine opskrbljuju materijalima te elementima, koji bi se mogli u određenim situacijama upotrijebiti za terorističke napade. Kako bi terorističke skupine ostvarile svoje planirane ciljeve bave se krijumčarenjem raznih kemikalija, biološki patogenim te nuklearnim otpadom. Navedeni materijali i elementi mogu stvoriti teške posljedice za sigurnost i zdravlje ljudi te za okoliš u određenim područjima. Do sada je međunarodna zajednica postigla dogovor o uništenju kemijskog oružja na temelju Konvencije o zabrani kemijskog oružja (OPCW) sa sjedištem u Haagu u Nizozemskoj. Biološko i nuklearno oružje je pod određenim stupnjem međunarodnog nadzora koji vodi BTWC-a te IAEA-a. Cilj ovih institucija je smanjenje ove vrste oružja, kako ne bi došlo u ruke raznim terorističkim skupinama diljem svijeta kao i u ruke diktatorskim režimima. Prema informacijama mnogi diktatorski režimi i razne terorističke skupine domogli su se vrlo opasnog oružja.

4.2. Postojeće stanje nadzora

Problemi su odgovarajući nadzor, roba ljudi, kopnom a i morem. Ovaj problem generira povećan i odgovarajući nadzor svih roba, tehnologije, i ljudi unutarnjem u međunarodnom planu (na unutarnjoj, bilateralnoj, multiratelarnoj razini). Isto tako postoje problemi u stručnom osoblju koje obavlja nadzor roba, ljudi kao i koliko je djelotvorna oprema. Bitni su i postupci te standardi koji se koriste pri nadzoru. Kako bi se sve što smo do sad naveli, sačuvali i osigurali od upada u sustave i krađe podataka, informacija i konačno roba, materijala i elemenata potrebno je definirati sigurnosnu politiku u svakoj instituciji.

4.3. Prijedlog poboljšanja nadzora

Ciljevi međunarodne zajednice a samim tim i Republike Hrvatske je veća kontrola i smanjenje širenja oružja za masovno uništenje na zemlje s nestabilnim režimima i koji mogu svojom nestabilnošću prouzročiti nekontrolirano širenje opasnih tvari te oružja. Posebni naglasak je u području kemijskog, biološkog i nuklearnog (KBM) oružja. Već smo naveli da je Republika Hrvatska članica EU, uskoro će postati članica Schengena, tranzitna je zemlja sa visokim rizikom navedenih transporta, stoga je potreban veliki i djelotvorni globalni nadzor prometa roba i ljudi.

Transport raznih roba je sve složena djelatnost kao i krijumčarenje opasnih i zabranjenih tvari. Često je krijumčarenje unosan posao kojim se bave pojedinci, skupine, organizacije a i ponekad cijele države ili organizacije koje imaju državnu potporu. Za sprječavanje krijumčarenja te provođenje ove djelatnosti, potrebna su velika materijalna sredstva kako bi se nabavila suvremena tehnika i uređaji za otkrivanje. Slijedom navedenih činjenica, podaci i informacije o materijalima, resursima i sredstvima koji se upotrebljavaju i skladište u specifičnim i rizičnim ljudskim djelatnostima trebali bi se zaštiti od upada nepoželjnih grupa i organizacija te u konačnici otuđivanja. U tu svrhu potrebno je definirati sigurnosnu politiku zaštite podataka.

5. Primjena Norme ISO/IEC 17799 za sigurnosnu politiku zaštite podataka

Primjena norme u sigurnosnoj politici ISO[2] 17799:2005 organizirana je u petnaestak poglavlja. Dio dokumenta tematizira upoznavanje s problemom upravljanja informacijskom sigurnošću. Uz prijedlog ustroja zaštite informacija obrazlaže se i sustav provjera koji se može primijeniti na gotovo sve poslovne subjekte i javne organizacije. ISO 17799:2005 norma razlikuje provjeru sigurnosne politike, ljudskih resursa, komunikacija i operativnog sustava, nabavu, organizaciju i održavanje IT sustava, odgovor na incidente te općenito pridržavanje uobičajenih poslovnih običaja. Najveći dio dokumenta odnosi se na provjeru sustava komunikacija i ostalih informacijskih tehnologija koje se koriste u poslovnim procesima. Provjera pristupa posebna je cjelina. Kako bi tehnička sredstva koja su danas na raspolaganju polučila najbolje rezultate, smatraju tvorci norme, potrebno je naglasiti važnost donošenja jasnih pravila o tome tko ima pristup kojim resursima. Sigurnosna politika komunikacijske i informatičke zaštite je definirana sukladno normi ISO/IEC 17799:2005 koja se sastoji se od 11 domena:

1.) Sigurnosna politika,
2.) Organiziranje informacijske sigurnosti,
3.) Upravljanje imovinom,
4.) Sigurnost i ljudski resursi,
5.) Fizička zaštita i zaštita od okoline,
6.) Upravljanje komunikacijama i operacijama,
7.) Kontrola pristupa,
8.) Obogaćivanje, razvoj i održavanje informacijskog sustava,
9.) Upravljanje incidentima informacijskog sustava,
10.) Upravljanje poslovnim kontinuitetom,
11.) Usklađivanje.

2 ISO- *eng. International Standardization Organization,* Međunarodna organizacija za norme

Primjena norme u sigurnosnoj politici.

- Želimo zaštititi:
  - podatke,
  - ostale korisnike Interneta.

6. Uloga sigurnosne politike

Sigurnosna politika je skup pravila, smjernica i postupaka koja definiraju na koji način informacijski sustav učiniti sigurnim i kako zaštititi njegove tehnološke i informacijske vrijednosti. Sigurnosnom politikom definirana su pravila koja se odnose na:

- svu računalnu opremu institucije (računalna sklopovska podrška (eng. *hardware* i programska potpora *(eng. software*)),
- osobe odgovorne za administraciju informacijskog sustava,
- sve zaposlenike i korisnike sustava, odnosno osobe koje imaju pravo pristupa,
- vanjske suradnike (npr. ovlaštene djelatnike zadužene za održavanje sustava).

6.1. Ciljeve sigurnosne politike

Ciljeve sigurnosne politike možemo razmatrati na dva načina:

- Prvi način definira sigurnosnu politiku kao potrebu zaštite:
  - informacijske vrijednosti,
  - širenje virusa,
  - napade na druge sustave i sl.
- Drugi način definicije sigurnosne politike možemo opisati kao skup sigurnosnih mjera i kontrola nad:
  - korisnicima sustava,
  - poslužiteljima:
    1. elektronička pošta,
    2. web stranice i usluge,
    3. mrežne aplikacije.
  - mrežnom infrastrukturom:
    1. mrežni uređaji,
    2. kabliranje,
    3. IP adrese.

- računalima klijenta (stolna i prijenosna računala i dodatna oprema),
- programska podrška ,
- podacima,
- korištenjem interneta,
- komunikacijama.

Provjera sigurnosne politike obavljati će se periodično svakih godinu dana, a po potrebi je nužno provjeru provesti i ranije.

Prijevremenu provjeru sigurnosne politike potrebno je napraviti:

- ako se dogode sigurnosni incidenti,
- ako se otkriju potencijalne ranjivosti sustava,
- ako se implementiraju novi servisi, sklopovska podrška (*eng. hardware*), programska potpora (*eng, software*),
- ako se dogode promjene u strukturi zaposlenika itd.

6.2. Identifikacija resursa

Jedan od uvjeta za uspješno upravljanje sigurnošću informacijskog sustava jest identifikacija resursa koji su dio tog sustava. Bez precizne identifikacije resursa nije moguće provesti njihovu kvalitetnu zaštitu. Kroz proces identifikacije resursa potrebno je prebrojati sve resurse unutar informacijskog sustava te procijeniti njihovu relativnu vrijednost za organizaciju.

Kvalitetnom identifikacijom resursa nužno je postići sljedeće zahtjeve:

- ustanoviti vlasnike poslovnih procesa, odnosno odgovorne osobe,
- identificirati pojedine resurse bitne za funkcioniranje poslovnih procesa,
- procijeniti vrijednost resursa,
- ustanoviti njihovo fizičko ili logičko mjesto u sustavu,
- napraviti odgovarajuću dokumentaciju.

Odgovarajuća implementacija sigurnosti za ovakve informacije je od kritične važnosti.

- ugrađivanje odgovarajućih kontrola koje smanjuju rizik,
- svjesno i objektivno prihvaćanje rizika, udovoljavajući sigurnosnoj politici organizacije i kriterijima prihvatljivog rizika,
- izbjegavanje rizika zabranama,
- za rizike čiji postupci uključuju implementiranje odgovarajućih kontrola, te kontrole moraju biti odabrane i implementirane zadovoljavajući zahtjeve definirane procjenom rizika.

Kontrole moraju osiguravati da su rizici reducirani na prihvatljiv nivo uzimajući u obzir.

- ciljeve organizacije,
- operativne potrebe i ograničenja,

Smještanjem opreme na kojima se čuvaju podaci u posebnu prostoriju, propisima kojima se određuje tko joj smije pristupiti, kontroliranjem uvjeta u takvoj prostoriji kao što su temperatura i vlaga, postižemo duži radni vijek opreme a time i pouzdaniji rad sustava. Uvođenjem kontrole pristupa podacima i definiranjem sankcija onima koji se ne pridržavaju propisanih pravila suzbijamo zlouporabu sustava od strane zaposlenika. Na napada izvana sustav se od takvih napada brani kontrolom prometa s Interneta prema sustavu i obrnuto, sprječavanjem instaliranja programa u operacijski sustav ili kriptiranjem podataka.

6.3. Analiza rizika

Analiza rizika je postupak kojem je cilj ustanoviti ranjivosti sustava, uočiti potencijalne prijetnje (rizike) te na odgovarajući način kvantificirati moguće posljedice kako bi se mogao odabrati najučinkovitiji način zaštite, odnosno procijeniti opravdanost uvođenja dodatnih protumjera.

- Postoje dva osnovna pristupa analizi rizika:
    1. Kvantitativna analiza,
    2. Kvalitativna analiza.

Kvantitativna analiza podrazumijeva iskazivanje procijenjenih rizika na godišnjoj razini. Pritom valja imati na umu da je ta procjena subjektivne naravi te je stoga podložna pogreškama

Kvalitativne analize iskazuje rezultat samo relativan odnos vrijednosti šteta nastalih djelovanjem neke prijetnje i uvođenja protumjera.

U načelu kombinacija kvantitativne i kvalitativne analize predstavlja pristup prikladan za većinu institucija.

6.4. Povjerljivost

Povjerljivost podataka može biti narušena na nekoliko načina. Navedene su najčešće prijetnje povjerljivosti:

- *Hackeri(crackeri),*
- lažno predstavljanje,
- neovlaštena aktivnost,
- nezaštićeno preuzimanje podataka,
- trojanski konji i drugi oblici malicioznog koda.

Hackeri (crackeri).

Zlonamjerni *hackeri (crackeri)* su osobe koje koriste sigurnosne slabosti sustava tako da neovlašteno koriste sustav ili ga onesposobe. Mnogi *hackeri (crackeri),* osim sigurnosnih slabosti sustava, koriste i metode otkrivanja lozinki ovlaštenih korisnika. Naime, lozinke koje su riječi koje se nalaze u rječniku ili često korištene lozinke, iskusnijim *hackerima (crackerima)* pomoću programske podrške vrlo lako je otkriti. Iz tih razloga aktivnost *hackera (crackera)* predstavlja veliku opasnost povjerljivosti informacija.

Lažno predstavljanje.

Lažno predstavljanje je prijetnja u kojoj korisnik preko lozinke drugog korisnika dobiva mogućnost pristupa sustavu pod drugim imenom, te mu se tako „otvaraju vrata“ za obavljanje zlonamjernih radnji. Lažno predstavljanje je čest slučaj koje dozvoljavaju korisnicima da razmjenjuju lozinke.

Neovlaštena aktivnost.

Ovaj tip aktivnosti događa se kad ovlašteni korisnik sustava koristi podatke za koje nema ovlasti. Nedovoljna kontrola pristupa i zaštita podataka omogućuju neovlašten pristup, što može ugroziti njihovu povjerljivost.

Kopiranje podataka na nezaštićene lokacije.

Kopiranje podataka može ugroziti njihovu povjerljivost ako se podaci kopiraju na sustav s nedovoljnom sigurnosnom zaštitom. Primjer ove vrste prijetnje je kopiranje podataka sustava na lokacije sustava koje nemaju adekvatnu razinu zaštite.

Lokalna mreža.

Lokalna mreža predstavlja prijetnju jer podaci koji putuju mrežom mogu biti dohvaćeni u svakom čvoru mreže. Kako bi se izbjegla ova vrsta prijetnje svi tajni podaci koji bi smjeli biti dostupni samo u određenim čvorovima moraju biti kriptirani kako bi njihova povjerljivost ostala neupitna.

Trojanski konj.

Trojanski konj je vrsta aplikacije koja može izazvati vrlo velike štete sustavima. Primjer trojanskog konja je aplikacija instalirana na računalo sustava nakon što ga nesvjesno pokrene ovlašteni korisnik, te je tako programirana da kopira podatke na nezaštićene dijelove sustava.

6.5. Integritet

Integritet (eng. *Integrity)* predstavlja zaštitu podataka od namjernog ili slučajnog neovlaštenog mijenjanja. Dodatni element integriteta jesu zaštita procesa ili programa kako bi se onemogućilo neovlašteno mijenjanje podataka. Glavni zahtjev komercijalnih i državnih institucija jest osigurati integritet podataka kako bi se izbjegle zlouporabe i greške. To je imperativ kako korisnici ne bi mogli mijenjati podatke tako da ih izbrišu, promjene ili učine ključne podatke nesigurnima. Ključni elementi za postizanje integriteta podataka su identifikacija i provjera autentičnosti korisnika.

6.5.1. Zaštita integriteta

Kao i povjerljivost, integritet može biti ugrožen od *hackera* (*crackeri)*, lažnog predstavljanja, neovlaštenih aktivnosti i nedozvoljenih programa (virusi, trojanski konji) jer sve navedene aktivnosti mogu dovesti do neovlaštenog mijenjanja podataka.

Osnovni principi za kontrolu integriteta:

- dodjeljivanje pristupa na temelju potreba,
- razdvajanje obaveza,
- rotiranje obaveza.

6.6. Dostupnost

Dostupnost (eng. *availability*) je garancija ovlaštenim korisnicima sustava da će im sustav biti raspoloživ u svakom trenutku kad za njim imaju potrebu.

Dva su najčešća uzroka neraspoloživosti sustava:

- odbijanje usluge (eng. *Denial Of Service*) i
- gubitak mogućnosti obrade podataka.

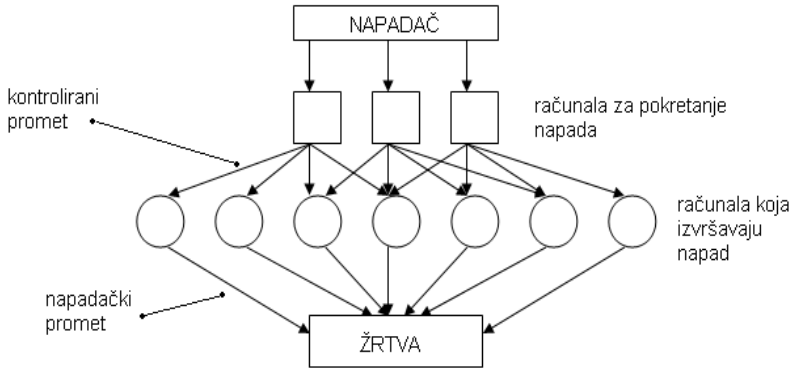
Odbijanje usluge je svaki zlonamjeran napad kojem je cilj uskraćivanje legitimnim korisnicima mogućnost pristupa (Internet) uslugama (npr. web poslužitelj). Napad odbijanja usluge možemo podijeliti u dvije kategorije:

1. Ranjivost poslužitelja na napade odbijanja usluge:

Napadi koji iskorištavaju poznate greške (propuste) u operacijskim sustavima i poslužiteljima. Ovi napadi koriste se za „rušenje“ programa. Tako uskraćuju se usluge (servisi) koji ti programi pružaju. Primjeri ranjivih operacijskih sustava uključuju sve sustave, kao što su na primjer Windows NT ili Linux i različite poslužitelje kao što su DNS ili Microsoft`s IIS Server. Svi ovi programi, koji imaju važnu i korisnu funkciju, posjeduju programske propuste (eng. *bug*) koje hakeri koriste kako bi ih „srušili“ ili hakirali. Ovakvi tipovi napada odbijanja usluge obično dolaze s jednog računala koji traže propuste u programima kako bi obavili napad. Ako je propust uočen, počinje napad odbijanja usluge s ciljem uskraćivanja usluge ovlaštenim korisnicima. Za ovakav tip napada nije potreban širokopojasni (brzi) pristup Internetu.

2. Napad odbijanja usluge poplavom paketa:

Napadi koji iskorištavaju slabosti infrastrukture Interneta i njegovih protokola. Poplavom naizgled normalnih paketa iskorištavaju se resursi programa (poslužitelja). Na taj način uskraćuju se usluge legitimnim korisnicima. s računala posrednika (zombi računala) koje napadač već kontrolira (na zombi računala obavi se napad prije DoS napada). Napadač kontrolira zombi računala i u određenom trenutku s njih pokreće napad. Bolje od korištenja vlastite infrastrukture za počinjene napada (napad s vlastitog računala, ovakav napad je lakše detektirati), napadači preferiraju izvršavanje napada. Primjer napada odbijanja usluge poplavom paketa (Slika 9).



Slika 9.– Grafički prikaz primjera napada odbijanja usluge.

Jedini mogući način zaštite je educiranje korisnika uz implementiranje sigurnosnih kontrola pristupa i fizičke sigurnosti. Sve druge tehnike automatske detekcije, bilježenja i suprotstavljanja u ovoj vrsti napada nisu djelotvorne. Educiranjem korisnika sprječavaju se oni napadi kod kojih žrtve zbog neznanja pružaju napadaču željene informacije. Educiranje korisnika treba sadržavati upute kako prepoznati navedeni napad te na koji način pravilno reagirati.
Sigurnosne mjere kojima osiguravamo dostupnost dijelimo na:

- fizičke,
- tehničke,
- administrativne.

Fizičke mjere uključuju kontrolu pristupa koja sprječava neovlaštenim osobama pristup sklopovima u informacijskom sustavu, protupožarnim sustavima, sustavima za kontrolu temperature prostorija itd.

Tehničke mjere sprečavaju nefunkcioniranje sustava koje uzrokuje kvar opreme raznim mjerama poput zrcaljenja diskova, tj. više diskova sadrži iste informacije – ako se jedan pokvari, njegovu funkciju preuzima drugi. Jedna od mjera je konstantna provjera rada aplikacija – ako aplikacija ne izvršava zadatke ona se automatski ponovno pokreće.

Administrativne mjere uključuju kontrolu pristupa, kontrolu izvršavanja procedura i educiranje korisnika. Odgovarajuća osposobljenost programera i sigurnosnih stručnjaka također je bitan faktor dostupnosti sustava. Na primjer, ostane li prilikom kontrole sustava baza podataka zaključana, korisnici se ne mogu koristiti podacima koje ona sadrži, tj. sustav postaje nedostupan.
Provjera sigurnosne politike obavljati će se periodično svakih godinu dana, a po potrebi je nužno provjeru provesti i ranije.
Prijevremenu provjeru sigurnosne politike potrebno je napraviti:

- ako se dogode sigurnosni incidenti,
- ako se otkriju potencijalne ranjivosti sustava,
- ako se implementiraju novi servisi, sklopovska podrška (*eng. hardware*) i programska potpora (*eng, software*,
- ako se dogode promjene u strukturi zaposlenika itd.

7. Klasifikacija resursa

Da bi se korisnici uputili na koji način rukovati pojedinim resursom potrebno je u svakoj instituciji izraditi Pravilnik o klasifikaciji informacijskih resursa. Obzirom na to da nije moguće za svaki resurs definirati na koji način se prema njemu odnositi u smislu zaštite, nastao je pojam klasifikacije. Cilj klasifikacije je svrstati svaki resurs u pojedinu klasu ovisno o kriterijima klasifikacije. Klasa resursa jednoznačno određuje na koji način je korisnik dužan koristiti resurs, s kolikom pažnjom i odgovornošću.

7.1. Klasifikacija informacije

Državne institucije dužne su prije puštanja u uporabu klasificirati informaciju. Klasifikacija je postupak procjene informacije prema:

- Vrijednosti,
- Osjetljivosti,
- Dostupnosti,
- Tajnosti,
- Važnosti za instituciju,
- Zakonodavnim zahtjevima.

Ovisno o izvršenoj procjeni svakoj informaciji dodjeljuje se klasa. Državne institucije klasificiraju informaciju prema 3 postojeće klase:

- Javno dostupno,
- Interna uporaba,
- Povjerljivo.

7.1.1. Javno dostupno

Klasa javno dostupno predstavlja podatke:

- Uporaba otvorena za sve korisnike, koji nisu tajna,
- Dijeljenje i objavljivanje ovih podataka ni na koji način ne štete državnim institucijama,
- Ne postoje zakonodavni zahtjevi za "skrivanjem" podataka.

7.1.2. Interna uporaba

Interna uporaba označava one podatke prema kojima se zbog zakonodavnih zahtjeva, moralnih obveza, prava privatnosti i sl. mora pažljivo i odgovorno odnositi s ciljem zaštite podataka od neovlaštenog pristupa, modificiranja, kopiranja, prijenosa i ostalih načina zlouporabe.

Podaci klasificirani kao interna uporaba namijenjeni su isključivo zaposlenicima državnih institucija koji imaju legitimno pravo pristupa ovakvim podacima.

Primjeri podataka klase interna uporaba:

- Podaci o zaposlenicima,
- Podaci ugovora s trećom stranom,
- Interni telefonski imenik,
- Podaci o količinama materijala, elemenata i vrstama roba,
- Podaci o lokacijama skladištenja materijala, elementima i vrstama roba.

Podaci klase interna uporaba:

- Moraju biti zaštićeni od neovlaštenog pristupa,
- Podaci moraju biti pohranjeni na sigurnim mjestima u smislu fizičke zaštite,
- Ukoliko podaci više nisu potrebni, moraju biti uništeni prema pravilima politike o uklanjanju medija i brisanja informacija.

7.1.3. Povjerljivo

Klasa povjerljivo označava podatke zbog zakonodavnih zahtjeva, podatke o projektima, elaboratima tehničkih mjera osiguranja i zaštite otvorenih i zatvorenih prostora objekata, kao i podaci o nazivima projekata, propisa institucija ili zbog ugovornih obveza podaci moraju biti strogo zaštićeni. Pristup povjerljivim podacima imaju samo pojedinci koji ih zbog prirode posla moraju koristiti.

Povjerljivi podaci:

- Pohranjeni su u elektroničkom formatu, moraju biti zaštićeni jakom lozinkom, pohranjeni na poslužiteljima s jakim sigurnosnim mjerama u svrhu zaštite od gubitka, krađe, neovlaštenog pristupa i razotkrivanja,
- Potrebno je redovito raditi sigurnosne kopije podataka,
- Sigurnosne kopije povjerljivih podataka potrebno je čuvati na mjestima sa strogim sigurnosnim kontrolama,
- Ne smiju biti proslijeđene bez eksplicitnog odobrenja odgovornih osoba,
- Prava pristupa povjerljivim podacima dodjeljuje se isključivo uz odobrenje odgovorne osobe,
- Mediji na kojima su povjerljivi podaci pohranjeni moraju se nalaziti u prostorijama do kojih je pristup omogućen samo ovlaštenim osobama,

- Ako se podaci šalju putem faksa ili elektroničke pošte mora se koristiti protokol i mehanizmi koji podatke štiti od neovlaštenog pregledavanja ili mijenjanja,
- Ukoliko podaci više nisu potrebni, moraju biti uništeni prema pravilima politike o uklanjanju medija i brisanja informacija.

Primjeri povjerljivih resursa:

- Podaci o zaposlenicima (radna mjesta i sl.),
- Podaci o visini plaća,
- Podaci o ugovorima s komitentima,
- Podaci o načinu postupanja,
- Podaci o vrstama roba i materijala koji se koristi u proizvodnji,
- Podaci o količinama roba,
- Podaci o skladištenju i lokaciji materijala i roba.

7.2. Pravila klasifikacije

Svi resursi moraju zadovoljavati sljedeće kriterije:

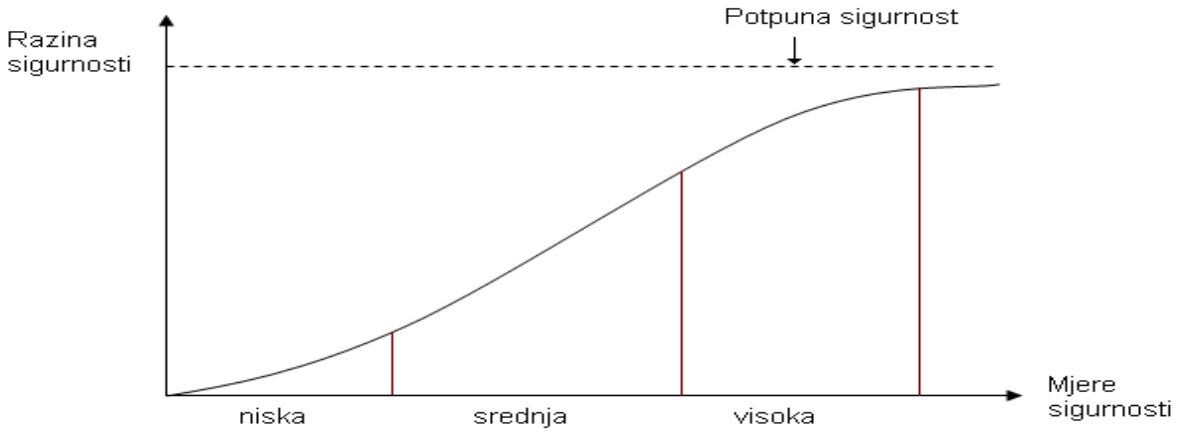
- Ministarstva i državne institucije dužne su provesti klasifikaciju resursa prije njegova puštanja u uporabu,
- Svaki resurs (CD, DVD, papirnati dokumenti, web stranice i sl.) mora imati jasno istaknutu oznaku stupnja klasifikacije, osim ako je riječ o javno dostupnim podacima,
- Prije usmenog priopćavanja klasificiranih podataka drugim osobama (koje imaju pravo pristupa tim podacima) obavezno se daje prethodno upozorenje o stupnju njihove klasifikacije,
- Povjerljivi podaci ne smiju se dijeliti ni na koji način (usmeno, pismeno, elektroničkim putem itd.) osobama koje nemaju pravo pristupa tim podacima,
- Svaku uočenu nepravilnost (neovlašteni pristup, mijenjanje, brisanje, dijeljenje informacija i sl.) korisnik je dužan prijaviti odgovornoj osobi,
- Klasificirane podatke dobivene od treće strane potrebno je klasificirati prema pravilima klasifikacije tvrtke; ukoliko ne postoji mogućnost klasifikacije prema internim pravilima, potrebno je proširiti postojeća pravila u skladu s ukazanim potrebama,
- Odgovorna osoba dužna je uspostaviti metode vođenja evidencije o pristupu povjerljivim podacima.

7.3. Klasifikacijske oznake

Klasifikacijska oznaka pojedinog informacijskog sustava trebala bi biti jedinstvena zbog toga što u suprotnome može doći do miješanja nejednakih klasifikacijskih oznaka više informacijskih sustava. Klasifikacijske oznake važno je što bolje označiti (npr. različitim bojama, oblicima) i istaknuti ih na uočljivim mjestima kako bi bili sigurni da su ih korisnici uočili (posebno ako je riječ o povjerljivim resursima).

8. Sigurnost informacijskog sustava

Sigurnost informacija je termin kojim opisujemo s kolikom vjerojatnošću se možemo pouzdati da će informacija biti dostupna, ispravna i tajna (ukoliko informaciju definiramo kao tajnu) [17]. Budući da su informacije dio informacijskog sustava, sigurnost informacijskog sustava možemo povezati sa sigurnošću informacija.



Slika 10 – Grafički prikaz odnosa razine i mjera sigurnosti.

Odnos razine sigurnosti i mjera sigurnosti (razina sigurnosti proporcionalna je s mjerama sigurnosti) je grafički prikazan (Slika 10). Ukoliko su mjere sigurnosti male, razina sigurnosti je također mala i samim time je ranjivost velika. Povećanjem mjera sigurnosti raste i razina sigurnosti, a važno je primijetiti da koliko god ulagali sredstava i pažnje u mjere sigurnosti sustav nikada ne može biti potpuno siguran.

8.1. Operacijska sigurnost

Operacijska sigurnost uključuje dva gledišta sigurnosti informacijskih sustava:

1.) Povećanje svijesti među potencijalnim žrtvama;

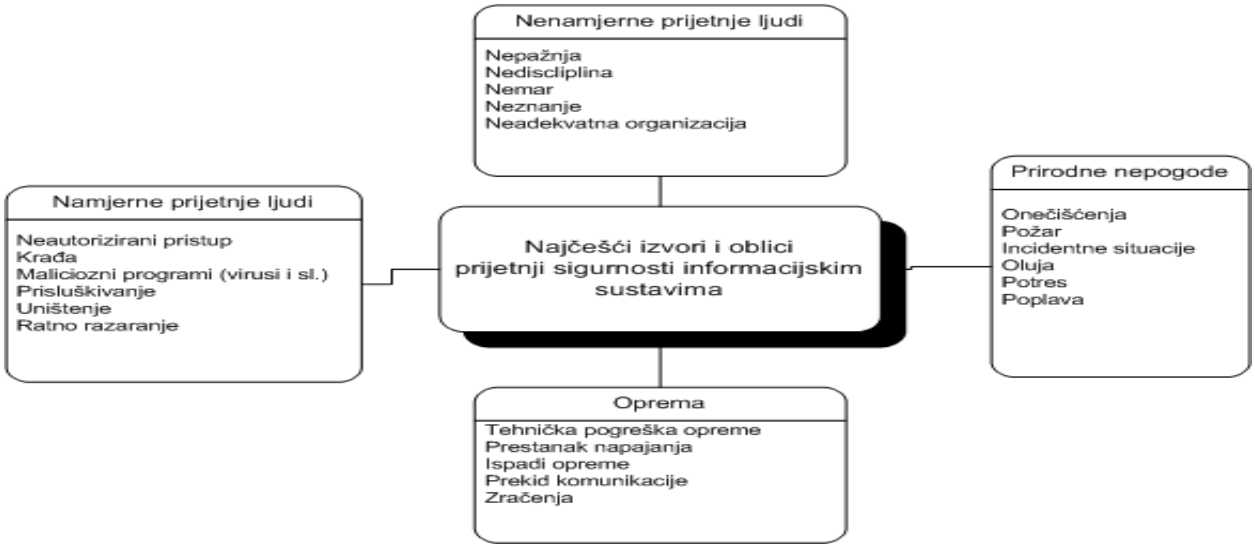
2.) Način na koji se računalni kriminalci mogu spriječiti u počinjenju djela.

1.) Povećanje svijesti postiže se tako da kad god je to moguće zaposlenici budu uključeni u sigurnosni program te ih po potrebi educirati na koji način je sigurnost ugrožena i kako svi dijele rizik i odgovornost. Jednom kada se analiziraju rizici sustava, potrebno je odrediti količinu informacija koja će se podijeliti sa zaposlenicima. Jasno je da povjerljive informacije neće biti dostupne svima, već samo malom broju osoba kojima su one nužne za obavljanje poslova. Općenito gledajući, operacijska sigurnost ne može postojati i biti dostatna sama sebi. Jedini način na koji ona može postojati jest uključivanje operacijske sigurnosti u programe ostalih načina zaštite sustava institucija.

Postoje brojni čimbenici koji mogu ugroziti sigurnost informacija.

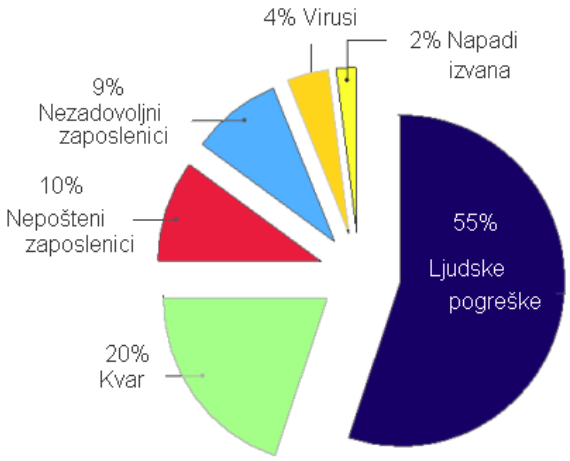
Četiri (4) glavne prijetnje (Slika 11):

- ljudi – namjerne prijetnje,
- ljudi – nenamjerne prijetnje,
- oprema,
- prirodne nepogode.



Slika 11 - Shematski prikaz kategorije izvora i oblika prijetnji nesigurnosti.

Statistički podaci (Slika 12) pokazuju da najvećim postotkom probleme sigurnosti uzrokuju ljudske greške. One se najčešće dogode zbog nedovoljne pažnje i educiranosti zaposlenika. Drugi najveći uzrok grešaka u sustavima je kvar opreme, slijede zaposlenici koji svoj položaj u instituciji koriste za vlastitu korist i zaposlenici koji na ovakav način izražavaju svoje nezadovoljstvo prema poduzeću ili nadređenoj osobi.



Slika 12 - Grafički prikaz uzroka grešaka i problema sigurnosti.

Kako bi spriječili mogućnost obavljanja ovakvih neželjenih radnji potrebno je uvesti odgovarajuće mjere. Mjerama poput educiranja zaposlenika smanjuje se vjerojatnost njihove pogreške kojima bi mogli ugroziti integritet i sigurnost sustava. Uvođenjem kontrole pristupa podacima i definiranjem sankcija onima koji se ne pridržavaju propisanih pravila suzbijamo zlouporabu sustava od strane zaposlenika.

2.) Napadi koji najčešće uzrokuju najveće štete su napadi "izvana". Oni sudjeluju u vrlo malom postotku, a cilj im je pribavljanje informacija, njihovo mijenjanje ili uništavanje. Sustav se od takvih napada brani kontrolom prometa s Interneta prema sustavu i obrnuto, sprječavanjem instaliranja programa u operacijski sustav ili kriptiranjem podataka. Uvođenjem ovakvih mjera u informacijskim sustavima podižemo njegov stupanj sigurnosti, a mogućnost obavljanja neželjenih radnji svodimo na minimum.

Kako bi se postigla maksimalna sigurnost sustava potrebno je obratiti pažnju na [17]:

- Sigurnosnu provjeru,
- Fizičku sigurnost,
- Sigurnost podatka,
- Sigurnost informacijskog sustava,
- Sigurnost poslovne suradnje.

8.2. Zaštita od malicioznih programa

8.2.1.Antivirusna zaštita

Maliciozni programi (virusi, crvi, trojanski konji itd.) su svi oni programi kojima je svrha zlonamjeran učinak na računalo (računalni sustav) ili koji obavljaju akcije na računalu bez znanja (pristanka) korisnika. Da bi računalo bilo zaštićeno od malicioznih programa, korisnik je dužan pridržavati se nekoliko jednostavnih pravila:

- na svakom računalu mora biti instaliran antivirusni program;
- baza podataka s informacijama o novim virusima mora biti redovito ažurirana;
- korisnik mora provoditi provjere na prisutnost virusa kod svih datoteka na elektroničkim medijima nesigurnog ili neautoriziranog porijekla ili datoteka nabavljenih preko neprovjerenih mreže (uključujući Internet);
- činiti provjeru na prisutnost virusa kod svih privitaka elektroničke pošte i preuzetih datoteka;
- korisnik ne smije svojevoljno isključivati antivirusnu zaštitu;
- korisnik ne smije otvarati datoteke sumnjivog sadržaja;
- u programu za pregled pošte treba isključiti mogućnost automatskog otvaranja primljene pošte.

Ako sumnjate u zaraženost vašeg računala malicioznim programom (neobična tromost računala pri radu), svakako je potrebno učinite sljedeće:

- kontrolom tipki Ctrl+Alt-Del otvoriti Windows *Task Manager*;
- otvoriti karticu *Processes*;
- kartica Processes daje na uvid aktivne procese;
- ako primijetite sumnjivi proces kopirajte njegove ime (s ekstenzijom) u Internet tražilicu ili bilo koju drugu tražilicu te pokrenite pretragu;
- ukoliko je među rezultatima pretrage pronađena stranica s riječju virus, *malware*, trojan vjerojatno se radi o malicioznom programu.

8.2.2. Elektronička pošta

Elektronička pošta dio je svakodnevne poslovne i privatne komunikacije. Njeno korištenje može ozbiljno ugroziti sigurnost informacijskog sustava.

Potencijalne prijetnje i ranjivosti elektroničke pošte:

- Virusi

-Elektronička pošta može biti malicioznog karaktera - u privitku je datoteka koja sadrži virus,

- Nesigurnost protokola

-Poruke putuju kao običan tekst, te ih je lako pročitati ili izmijeniti sadržaj;
-Lako je krivotvoriti adresu pošiljatelja,

- Nezgode

-Pritiskom na krivu tipku ili odabirom krivog korisnika u adresaru poruka može doći neželjenom korisniku (ili više njih).

Phishing je vrsta napada u kojem napadač putem elektroničke pošte ili lažnih Internet stranica pokušava doći do povjerljivih informacija u cilju stjecanja financijske koristi ili terorizma. Najčešće je riječ o zaporkama, PIN brojevima, brojevima kreditnih kartica, raznim izvješćima te drugim sličnim povjerljivim informacijama. Ukoliko napadač uspješno obavi napad i prikupi željene informacije, pruža mu se mogućnost pristupa informacijskim sustavima financijskih ustanova ili nekim drugim sustavima preko kojih može steći određenu financijsku korist ili doći do informacija o količinama te lokacijama skladištenja materijala, elemenata ili roba.

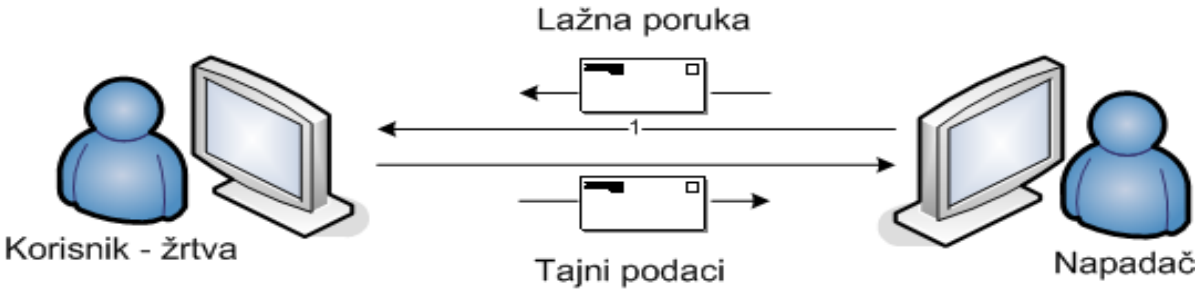
Tijek provođenja *phishing* napada moguće je podijeliti u tri faze:

1) Osmišljavanje i pripremanje napada,
2) Provođenje napada,
3) Prikupljanje povjerljivih informacija i njihovo iskorištavanje.

Prva faza (1) je osmišljavanje i pripremanje napada najvažniji je dio napada. U toj fazi napadač pokušava skupiti što više informacija o žrtvi, o detaljima žrtvinog operacijskog sustava i informacijskog sustava itd. Što više informacija posjeduje, napadač će s većom vjerojatnošću uspješno obaviti napad i ostati neotkriven.

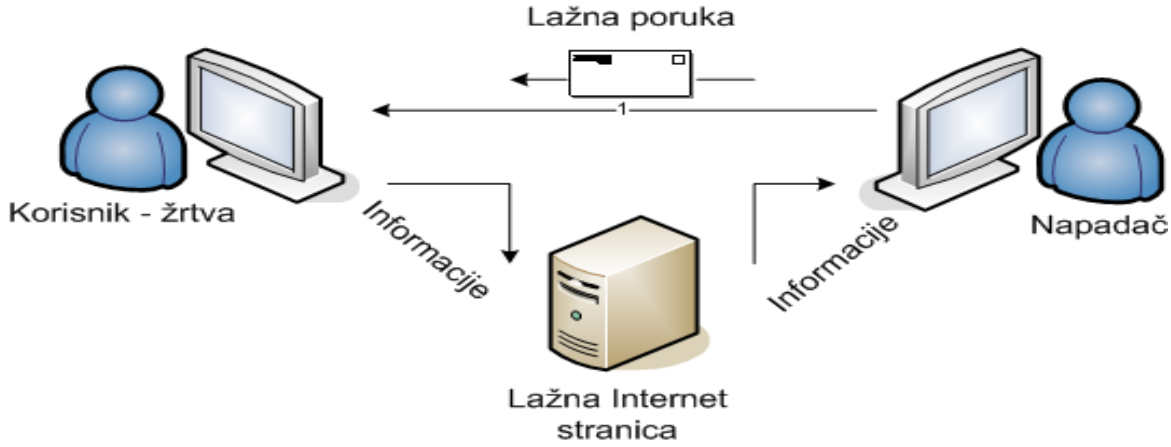
Druga faza (2) je provođenje napada. Postoji dvije metode provođenja napada. Metoda koja će se provoditi ovisiti će o prikupljenim podacima u prvoj fazi.

Prva metoda napada elektroničkom poštom (Slika 13) realizira se tako da napadač slanjem elektroničke pošte potakne korisnika na odavanje željenih informacija. Jedan od primjera ovog napada prikazan je slikom: napadač šalje korisniku žrtvi lažnu poruku tako da se predstavi kao financijska ustanova. U poruci traži da žrtva hitno pošalje tajne podatke zbog provjere ili gubitka dijela podataka. Ako korisnik ne primijeti prijevaru, šalje napadaču poruku u kojoj su sadržani tajni podaci. Napad je uspješno realiziran i napadač je došao do željenih podataka. Ovaj napad je najjednostavniji, a realizacija ovisi o needuciranosti korisnika žrtve.



Slika 13 - Shematski prikaz primjera(*eng. Phishing*)napada elektroničkom poštom.

Druga metoda napada elektroničkom poštom (Slika 13.1.) je pozivanje korisnika žrtve na lažne Internet stranice. Primjer tijeka napada: korisnik žrtva dobiva lažirani e-mail. U poruci se poziva da zbog određenog razloga posjeti Internet stranice neke ustanove. Iako žrtva ne sumnja u vjerodostojnost, Internet stranice navedene u poruci su lažirane. Naime, lažne stranice vrlo je teško uočiti. Na primjer, ukoliko je originalna adresa www.halo92.hr, lažna adresa može biti www.halo-92.hr. Cilj napadača je da se korisnik pokuša prijaviti na sustav na lažnoj Internet stranici. Ukoliko se korisnik pokuša prijaviti, vjerojatno će dobiti poruku o trenutnom nefunkcioniranju sustava.



Slika 13.1. - Shematski prikaz druge metode (*eng. Phishing)* napada elektroničkom poštom.

8.3. Vrste sigurnosnih kopija

Definirane su 3 vrste sigurnosnih kopija [18]:

- Tjedne:
  - izrada sigurnosnih kopija svih važnih podataka koje je nemoguće ili vrlo teško obnoviti (npr. vrsta materijala i elemenata i sl.),
  - podatke za koje je eksplicitno navedeno da je potrebno raditi tjedne kopije.

- Mjesečne:
    - sigurnosne kopije raznih izvješća koja obuhvaćaju vrstu, količinu, lokaciju i sl.,
    - podatke za koje je eksplicitno navedeno da je potrebno raditi mjesečne kopije.
- Godišnje:
    - izrada sigurnosnih kopija svih podataka (npr. podaci o količini, vrstama i lokacijama),
    - radi se jednom godišnje.

Periodički je potrebno kontrolirati ispravnost medija na kojima su pohranjene sigurnosne kopije. Ukoliko zbog istrošenosti medija, isteka roka valjanosti medija ili bilo kojeg drugog razloga postoji rizik za gubitkom podataka, odgovorna osoba dužna je kopirati sigurnosne kopije podataka na novi medij te obavljene akcije dokumentirati.

9. Mediji

9.1. Sigurnost medija

Mediji su resursi koji služe za pohranu podataka. Kao takvi igraju veliku ulogu u sigurnosti. Dolaskom do medija na kojem su pohranjeni povjerljivi podaci ili podaci za internu uporabu, napadaču mogu biti otvorena vrata za obavljanje zlonamjernih radnji.

Budući korisnici za razmjenu podataka koriste isključivo prijenosne medije (CD, DVD, USB memorije, pisana izvješća, itd.).

Pravilnik o sigurnosti medija definira sljedeće:

- Svi mediji moraju biti pohranjeni na sigurnom i zaštićenom mjestu;
- Svi mediji moraju biti čuvani prema specifikacijama proizvođača;
- Mediji s povjerljivim podacima ne smiju se davati na korištenje neovlaštenim korisnicima;
- Svako dijeljenje medija s povjerljivim podacima mora biti dokumentirano;
- Potrebno je tražiti ovlaštenje za uklanjanje medija od vlasnika medija sa podacima, te se mora voditi zapis o takvim aktivnostima;
- Ako više nisu potrebni, treba obrisati prijašnje sadržaje svakog ponovno iskoristivog medija koji će biti uklonjen iz institucije.

9.2. Uklanjanje medija

Svrha pravilnika o uklanjanju medija je smanjiti rizik od "curenja" osjetljivih informacija koje može nastati nepravilnim odbacivanjem medija ukoliko medij više nije potreban. Kako bi se rizik "curenja" sveo na minimum potrebno je uspostaviti formalne smjernice za sigurno uklanjanje medija. Osim definiranja smjernica, važno je naglasiti da je uklanjanje osjetljivih medija treba biti provjereno i dokumentirano.

Lista dokumenata koji mogu zahtijevati sigurno uklanjanje:

- Optički mediji (CD, DVD.),
- USB memorije,
- Papirnati dokumenti,
- Snimljeni glas,
- Sistemska dokumentacija itd.

Smjernice:

- Sve medije klasificirane kao osjetljive, koji više nisu za uporabu, potrebno je ukloniti na način da nitko ni na koji način nije u mogućnosti doći do podataka (ili dijela podataka) pohranjenih na mediju,
- Papirnate i optičke medije potrebno je ukloniti pomoću aparata za uklanjanje medija;
- USB i ostale memorije potrebno je ukloniti prema pravilima proizvođača ili fizičkim djelovanjem na medij,
- Ostale medije potrebno je ukloniti fizičkim djelovanjem, posebnim uređajima ili na treći način prema preporukama stručnjaka.

10. Ostali komunikacijski uređaji

10.1. Mobilni uređaji, PDA i pametni telefoni

Uređaji koji ujedinjuju funkcionalnosti mobitela i računala. Odnosno, pametni telefoni objedinjuju funkcije mobilnog telefona, pristupa internetu u realnom vremenu te omogućuju čitanje elektroničke pošte s poslužiteljima državnih institucija. Tako pojedinci jednostavnije organiziraju svoje radne obaveze, uspostavljaju kontakte, a imaju i mogućnost pregleda niza dokumenata (*Word, Excel, Adobe Reader, PDF,* itd.). Osim toga, ovakvi uređaji sadrže i niz dodataka kao što su *Wi-Fi* podrška, *Bluetooth*, MP3 *player*, kamera i dr.

Zabranjeno je povezivanje uređaja sa domenskim računalima osim uz pismeno odobrenje odgovorne osobe, te bilo kakvo spremanje službenih podataka na uređaj (podaci se kompromitiraju jer uređaji nemaju dovoljnu sigurnosnu zaštitu). Ukoliko korisnik ima dozvolu za povezivanje i spaja se bežičnom vezom mora se koristiti *WPA*2 sustav za zaštitu bežičnih lokalnih mreža (*WLAN* eng. Wireless *LAN*). Uključuje autentifikaciju korisnika i enkripciju podataka. Na uređaju mora biti aktiviran PIN kod za zaključavanje SIM kartice i PIN kod za zaključavanje telefona. Za ispravno korištenje službenog mobilnog uređaja isključivo je odgovorna osoba koja ga je zadužila. Mobilni uređaji koji imaju pristup organizaciji mreže i internetu koristiti će se u svrhu izvršenja poslovnih obveza državnih. Svi korisnici mobilnih uređaja imaju odgovornost za korištenje tih sredstava na profesionalno, zakonit i etički način.

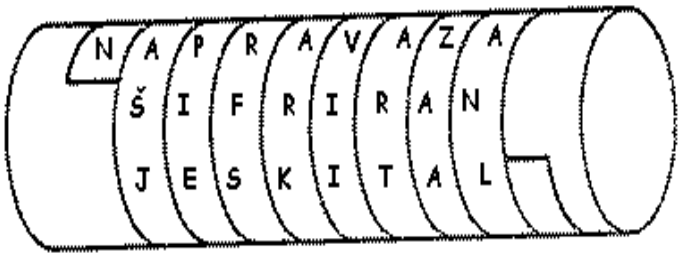
11. Sigurnost komunikacija

Komunikacija između računala doprinosi povećanju snage sustava, brzini obrade podataka, dostupnosti. Što više računala komunicira s drugim računalima to čini organizaciju koja je ranjiva. S vanjskim suradnicima, djelatnici navedenih državnih institucija (tema istraživanja ovog rada), računalima komunicira preko računalnih resursa i preko uslugama univerzalnih linija, nalik priključcima vode, struje, plina "*Utility computing*" i mrežnim strukturama nalik oblaku (*Cloud computing*) te komunicira mobilnim uređajima "*GSM*" mrežom [2]. Navedene komunikacije potrebno je zaštititi od napada i upada nepoželjnih osoba. Komunikacijska zaštita temeljna je metoda zaštite koja se koristi za zaštitu podataka koji se prenose komunikacijskom linijom, a u modernom društvu neprestano joj raste značaj. Komunikacije možemo učiniti sigurnijom kao i podatke koji se prenose mrežom primjenom jednih od metoda zaštite i sigurnosti a to je kriptiranje podataka.

11.1. Kriptologija

Kriptologija je grana znanosti koja obuhvaća kriptografiju i kriptoanalizu. Kriptografija je jedan dio komunikacijske zaštite i sigurnosti tj. to je postupak zaštite tajnosti podataka primjenom algoritama koji transformiraju razumljiv oblik teksta (čitljiv) u šifrirani tekst, nerazumljiv osobama koji ne poznaju algoritam transformacije. Tako bi definicija bila da je Kriptografija znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati [19]. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao tajnopis.

Neki elementi kriptografije bili su prisutni već kod starih Grka [20]. To je bio drveni štap pod nazivom *skital* (Slika 14) oko kojeg se namotavala vrpca od pergamenta, pa se na nju okomito pisala poruka. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.



Slika 14 - Naprava *Skital* koju su Spartanci u 5.stoljeću prije Krista upotrebljavali za šifriranje [21].

Primjenom kriptografije realiziraju se četiri osnovna sigurnosna zahtjeva (servisa):

- tajnost–osigurava da informacijski sadržaj poruke bude dostupan samo ovlaštenim korisnicima,
- integritet–osigurava otkrivanje neovlaštene izmjene informacijskog sadržaja poruke,
- autentičnost–omogućava provjeru identiteta sudionika komunikacije,
- neporecivost–sprječava mogućnost poricanja realizacije određenih aktivnosti sudionika u komunikaciji (kao što su slanje poruke, transakcija i dr.).

11.2. Kriptološke metode

Danas se primjenjuju tri vrste kriptiranja [2]:

- Simetrično kriptiranje-predstavlja oblik kriptiranja u kojem pošiljatelj poruke i primatelj moraju posjedovati identične ključeve kako bi mogli kriptirati, odnosno dekriptirati poruke. To znači da pošiljatelj mora prije komuniciranje nekim sigurnim kanalom primatelju uručiti ključ. Ovaj oblik kriptiranja predstavlja vrlo efikasan i brz postupak, ali postoji problem sigurne distribucije ključa. Siguran kanal nikako ne predstavljaju računalne mreže, već se ključ uručuje fizički uručivanjem.
- Asimetrično kriptiranje- predstavlja oblik koji koristi dva različita ključa. Jedan tajni, kojim se poruka kriptira i drugi javni kojim se poruka dekriptira. Asimetrično kriptiranje rješava problem distribucije ključa, što je osnovni razlog njihove sve veće primjene.
- Hibridno kriptiranje- predstavlja moderne oblike koji koriste paralelno oba oblika (simetrični i asimetrični) kako bi iskoristile prednosti svakoga.

Kriptografske metode potrebno je definirati kako bi se omogućila zaštita povjerljivosti, autentičnosti i/ili integriteta informacije. Ove metode potrebno je koristiti kod rizičnih, osjetljivih i povjerljivih podataka. Sigurnosnom politikom je potrebno odrediti koje tehnike kriptografije (koje kriptografske metode će se koristiti, način čuvanja i raspodijele ključeva, na koji način će se ostvariti digitalni potpis i sl.) će se upotrebljavati u skladu s važećim zakonodavnim restrikcijama i pravima uporabe.

Danas se uglavnom koriste četiri temeljne kriptološke metode [19]:

- transformacija- preuređenje poruke preraspodjelom znakova razumljive poruke,
- supstitucija-preuređenje poruke zamjenom znakova razumljivom teksta s bitovima znakovima izabranim iz neke druge abecede,
- aditivno kodiranje-preuređenje poruke kombiniranjem bitovima razumljivog teksta s bitovima šifriranog niza pomoću logičke operacije,
- multimedijsko kodiranje-preuređuje poruke kombiniranjem bitova razumljivog teksta s bitovima šifriranog niza pomoću logičke operacije ili ponovnom logičkom operacijom ili kombiniranjem djelomičnog rezultata s nizom bitova koji je proizveden prethodnim parcijalnim operacijama.

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Ovdje se radi o dvije funkcije jedna za šifriranje a druga za dešifriranje. Navedene funkcije preslikavaju osnovne elemente otvorenog teksta (slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata i obratno. U ovisnosti ključa biraju se određene funkcije. Pa tako nazivamo prostor ključeva da je skup svih mogućih vrijednosti ključeva.

11.3. Kriptosustav

Kriptosustav se sastoji od kriptoloških algoritama, te svih mogućih otvorenih tekstova, šifrata i ključeva. Definicija kriptosustava je da je to uređena petorka (P,C,K,E,D). Dakle P je konačan skup svih mogućih osnovnih elemenata otvorenog teksta. Konačan skup svih mogućih osnovnih elemenata šifrata je C, a K je konačan skup svih mogućih ključeva, dok je E skup svih funkcija šifriranja. Skup svih funkcija dešifriranja je D.

Kriptosustave klasificiramo prema sljedeća tri kriterija:

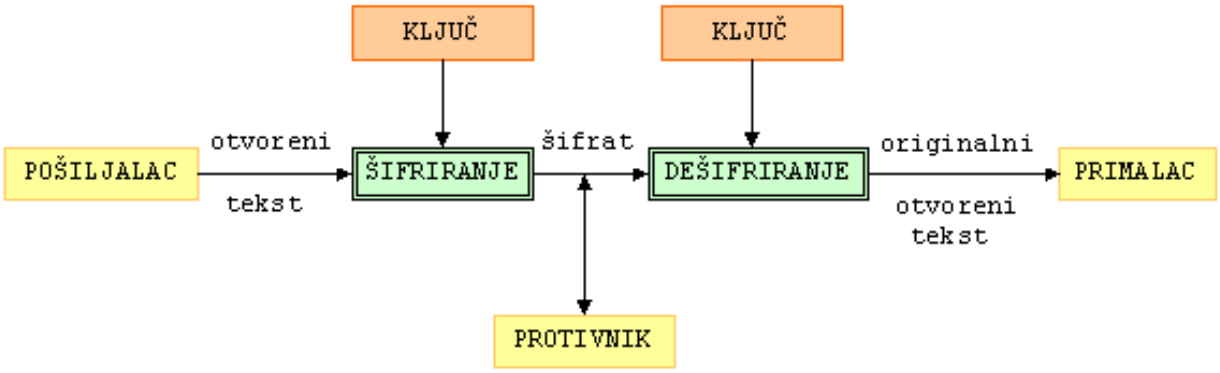
- Tip operacija koje se koriste pri šifriranju,

Imamo podjelu na supstitucijske šifre u kojima se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje s nekim drugim elementom, te transpozicijske šifre u kojima se elementi otvorenog teksta permutiraju (premještaju).

Npr. ako riječ TAJNA šifriramo u XIWOI, načinili smo supstituciju, a ako je šifriramo u JANAT, načinili smo transpoziciju. Postoje i kriptosustavi koji kombiniraju ove dvije metode.

- Način na koji se obrađuje otvoreni tekst,

Ovdje razlikujemo blokovne šifre, kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ K, te protočne šifre (*engl. streamcipher*) kod koji se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom niz ključeva (*engl. keystream*) koji se paralelno generira. Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno). Poruku koju pošiljalac hoće poslati primaocu (Slika 15) je otvoreni tekst (*engl. plaintext*) [20]. To može biti tekst na njihovom materinjem jeziku, numerički podaci ili bilo što drugo. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak se naziva šifriranje, a dobiveni rezultat je šifrat *(engl. ciphertext*) ili kriptogram. Nakon toga pošiljalac pošalje šifrat preko nekog komunikacijskog kanala. Protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac koji zna ključ kojim je šifrirana poruka može dešifrirati šifrat i odrediti otvoreni tekst.

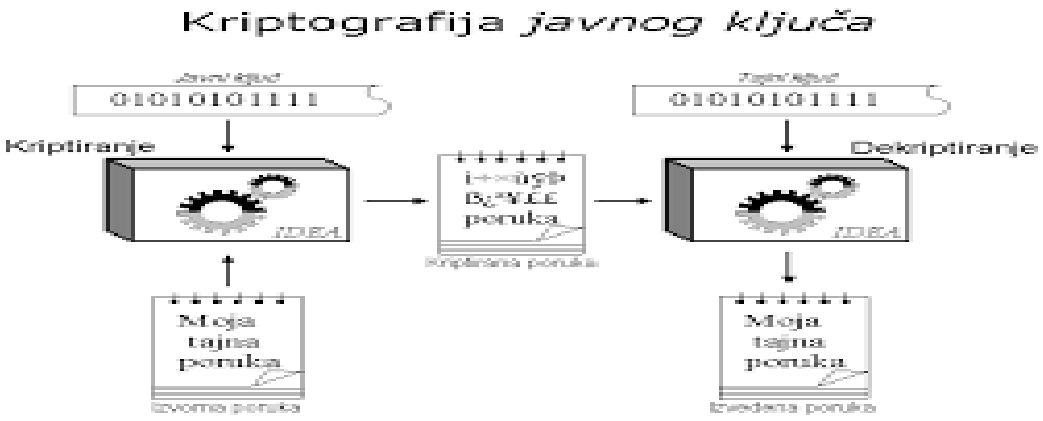


Slika 15 - Grafički prikaz poruke koju pošiljalac hoće poslati primaocu [21].

- Tajnost i javnost ključeva

Kod ovog kriterija je osnovna podjela na simetrične kriptosustave i kriptosustave s javnim ključem. Kod simetričnih ili konvencionalnih kriptosustava, ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno. Ustvari, najčešće su ovi ključevi identični. Sigurnost ovih kriptosustava leži u tajnosti ključa. Zato se oni zovu i kriptosustavi s tajnim ključem. Kod kriptosustava s javnim ključem ili asimetričnim kriptosustava ključ za dešifriranje se ne može izračunati iz ključa za šifriranje.

Ovdje je ključ za šifriranje javni ključ. Dešifrirati ovakvu poruku može samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ). Prijedlog navedenog problema razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala te ideju javnog ključa (Slika 16) prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine [20].



Slika 16 - Grafički prikaz Kriptografije javnog ključa.

Glavne prednosti kriptosustava s javnim ključem u odnosu na simetričkim su:

- nije potrebno za sigurnim komunikacijskim kanalom za razmjenu ključeva,
- za komunikacijske grupe N ljudi potrebno je 2N ključa za razliku od simetričkog,
- mogućnost potpisa poruke.

11.3.1. Digitalni potpis

Neki kriptosustavi omogućavaju korisnicima da digitalno potpišu svoju poruku. To je važno da osoba koja šalje poruku kasnije ne može zanijekati da je on poslao poruku. Digitalni potpis je kriptosustav sa s javnim ključem koji omogućava prenošenje korisnih svojstava "papirnatog potpisa" u digitalni svijet.

Digitalni potpis omogućava:

- autentifikaciju-primalac B može provjeriti dali je poruku stvarno napisao pošiljalac A,
- nepobitnost-pošiljalac A ne može poreći da nije poslao poruku.

Navedenim načinom digitalni potpis štiti obje strane u slučaju eventualnog spora.

Kriptosustav digitalnog potpisa uključuje tri algoritma:

- generiranje ključa (javnog i osobnog) za potpisivanje;
- potpisivanje poruke - generiranje poruke koju nazivamo potpis;
- provjeru potpisa.

Digitalni potpis se ostvaruje tako da pošiljalac A može poruku potpisati tako da uz poruku m priloži šifrat (šifriran njegovim tajnim ključem). Primalac B s obzirom na to da pozna javni ključ i uz dešifriranje šifrata može provjeriti je li pošiljalac A potpisao poruku.

11.4. Kriptoanaliza ili dekriptiranje

Kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.

11.4.1. Kriptoanalitički napadi

Osnovna nivoa kriptoanalitičkih napada su [18]:

- Napad kriptiranog teksta (šifeat) *(eng. ciphertexl.-only attack)*

Kriptoanalitičar posjeduje samo kriptirani tekst (šifrat) od nekoliko poruka šifriranih pomoću istog algoritma. Njegov je zadatak otkriti originalan tekst poruke.

- Napad poznatog osnovnog teksta *(eng. known plaintext attack)*

Kriptoanalitičar posjeduje originalan razumljivi tekst neke poruke, ali i njemu odgovarajući otvoreni (kriptirani) tekst. Njegov je zadatak otkriti ključ ili neki algoritam za dešifriranje poruka šifriranih tim ključem.

- Napad odabranog teksta *(eng.chosen plaintext attack)*

Kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Ovaj napad je jači od prethodnog, ali je manje realističan.

- Diferencijalna kriptoanaliza (*eng. differential cryptoanalysis)*

Kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može obraditi šifrat, te dobiti odgovarajući otvoreni tekst. Ovaj napad je tipičan kod kriptosustava s javnim ključem. Tu je zadatak kriptoanalitičara otkriti ključ za dešifriranje (tajni ključ).

- Potkupljivanje, ucjena, krađa i slično

Ovaj napad ne spada u kriptoanalizu, ali je vrlo efikasan i često primjenjivan u kombinaciji s "pravim" kriptoanalitičkim napadima [20].

12. Zaključak

U ovom radu cilj istraživanja je potvrda tvrdnje: "Važnost podataka i informacija u specifičnim i rizičnim ljudskim djelatnostima bitan je čimbenik života i zdravlja ljudi".

Tijekom istraživanja analizom su utvrđeni sljedeći sigurnosni rizici (R) te potencijalne prijetnje:

Prvi sigurnosni rizik (R1) je kako adekvatno zaštiti informacijske sustave od ljudi, bilo da se radi o ovlaštenim ili neovlaštenim korisnicima. U oba slučaja, najviše problema u zaštiti informacijskih sustava zadaju needucirani korisnici. Needucirani korisnici svojim postupcima kao što su slučajno brisanje ili mijenjanje podataka, nepažljivo rukovanje resursima itd., ugrožavaju sigurnost informacija u vrlo velikom postotku od ukupnog broja incidenata. Oni također često nesvjesno pomažu zlonamjernim korisnicima izvršavanje napada pružajući im potrebne podatke. Isto tako. needucirani korisnici ne shvaćaju kompleksnost računalne sigurnosti i to je danas jedan od glavnih problema računalne sigurnosti.

Drugi sigurnosni rizik (R2) je neorganizirano implementiranje sigurnosnih kontrola. Takvim načinom implementacije stvara se prividna sigurnost jer postoji velika vjerojatnost da je neka od kontrola izostavljena.

Daljnjom analizom istraživanja utvrđen je treći rizik (R3): kada bi navedene sigurnosno potencijalne prijetnje (R1 i R2) zlonamjerni korisnici usmjerili na rizične ljudske djelatnosti (područje interesa istraživanja), mogli bi iskoristiti za nanošenje materijalne štete i do ugrožavanja života i zdravlja ljudi.

Slijedom navedenih rizika kao i činjenice da je danas sigurnost informacijskih sustava nezaobilazna tema kojoj se posvećuje mnogo pažnje. Zaštita je postala moralna, poslovna i sigurnosna obaveza, te neophodan postupak pri osmišljavanju i izgradnji informacijskih sustava.

Trenutno stanje moglo bi se poboljšati sljedećim preporukama:

- Potrebno je kod uspostave sigurnosti informacijskih sustava posebnu pozornost usmjeriti na educiranje korisnika o računalnoj sigurnosti (kriminalu), te odgovornostima i dužnostima svakog pojedinca,
- Korisnici ne smiju zanemariti informacijski sustav, u smislu ne kontroliranja aktualnih problema sigurnosti, jer vrlo lako može postati žrtvom napada,
- Potrebno je periodično kontrolirati sigurnost sustava (testiranje sustava na napade). Informacijske sustave je potrebno redovito provjeravati kako bi se utvrdila usklađenost sa sigurnosnim implementacijskim standardima.

Svi korisnici računala također moraju biti svjesni sljedećih činjenica:

- sigurnost informacijskih sustava vrlo je široka tema koju je nemoguće jednoznačno definirati,
- računalna sigurnost je tema koju se ne smije ograničiti i koja zahtjeva neprekidnu pozornost,
- za uspostavu kvalitetne sigurnosti potrebno je široko znanje različitih područja računarstva, ali i drugih znanosti,
- računalo/informacijski sustav ne može biti u potpunosti siguran.

Vezano za oružane snage i uvažavajući veliki rizik od organiziranog kriminaliteta i terorizma, nameće se potreba djelotvornog i koordiniranog poduzimanja svih raspoloživih mjera i aktivnosti u cilju učinkovitijeg suzbijanja nezakonite proizvodnje, nabave, posjedovanja, trgovine i krijumčarenja malog i lakog oružja, te ujedno i svih drugih zlouporaba i negativnih pojava s tim u vezi. Riječ je o vrlo složenom procesu koji zahtijeva kontinuiranu suradnju svih ministarstava i drugih tijela državne uprave kako bi se postigao maksimalni učinak. U tom smislu potrebito će biti pojačana suradnja sa susjednim zemljama te zemljama šire regije. Nadalje, potrebno je osiguranje sigurnosnih mjera i vrhunske tehnologije neophodno razvijati i znanstvene resurse kojima bi se razvile metode i postupci za prevenciju i suzbijanje terorističkih djelovanja. Sigurnosna politika zaštite podataka i informacije bit će svakako od ključnog značaja u svim ovim oblicima komunikacija.

13. Literatura

[1] V. Anić, D.B. Rončević, I. Goldstein, S. Goldstein, LJ. Jojić, R. Matasović, I. Pranjković, Hrvatski enciklopedijski rječnik, EPH d.o.o. i Novi Liber, Zagreb, 2004.

[2] D. Kralj, kolegij Upravljanje ZNR i ZOP primjenom računala, predavanja, Veleučilište u Karlovcu, 2014/15, (20. travanj 2015.)

[3] Nuklearna podmornica Crnomorske flote, dostupno na: http://sh.wikipedia.org/wiki/Crnomorska_flota, (20. travanj 2015.)

[4] Vojna uporaba (Pu), dostupno na: http://radioaktivniotpad.org/vojna-uporaba-pu/, (22. travanj 2015.)

[5] Razno vojno naoružanje, dostupno na: http://www.hrvatski-vojnik.hr/hrvatski-vojnik/752001/pistolas.asp, (22. travanj 2015.)

[6] Inačice automatske pušake, dostupno na: http://www.hrvatski-vojnik.hr/hrvatski-vojnik/3682011/kalasnjikov.asp, (24. travanj 2015.)

[7] Razne strojnice, dostupno na: http://www.mup.hr/UserDocsImages/topvijesti/2013/travanj/izlozba/galerija_puske.jpg, (26. travanj 2015.)

[8] Vlada Republike Hrvatske, Nacionalna strategija i akcijski plan za kontrolu malog i lakog oružja, rujan 2009, dostupno na: http://www.propisi.hr/print.php?id=9632, (27. travanj 2015.)

[9] Institut „Ruđer Bošković“, dostupno na: http://portal.connect.znanost.org/2010/10/irb-kao-skladiste-radioaktivnog-otpada-poslovni-hr/, (28. travanj 2015)

[10] Prijevoz istrošenog goriva, dostupno na: http://www.hrvatski-vojnik.hr/hrvatski-vojnik/3672011/otpad.asp, (28. travanj 2015.)

[11] Strategiju zbrinjavanja radioaktivnog otpada, iskorištenih izvora i istrošenog nuklearnog goriva , dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2014_10_125_2382.html, (29. travanj 2015.)

[12] Sustav Bionadzora, dostupno na: http://portal.connect.znanost.org/2006/06/irb-i-morh-zajedno-protiv-nuklearno-biolosko-kemijskih-nesreca/, (29. travanj 2015.)

[13] Teroristički napadi na New York, dostupno na: http://hr.wikipedia. org/wiki/Napadi_11._rujna_2001. (30. travanj 2015.)

[14] Teroristički napad u Parizu, dostupno na: http://www.jutarnji.hr/video--teror-na-zapadu-europe-ovo-su-najkrvaviji-teroristicki-napadi-u-francuskoj-u-zadnjih-40-godina/1270008/, (30. travanj 2015.)

[15] S. Šegvić: Antiterorizam u kontekstu borbe protiv organiziranog kriminala, Zbornik radova Pravnog fakulteta u Splitu, god. 46, 4/2009., str. 667.-685, dostupno na: http://www.pravst.hr/zbornik.php?p=27&s=194 , (30. travanj 2015.)

[16] Žene teroristi, dostupno na: http://www.jutarnji.hr/sprijecen-teroristicki-napad-u-new-yorku-uhicene-dvije-fanaticne-sljedbenice-islamske-drzave/1324997/ , (30. travanj 2015.)

[17] Sigurnost informacijskog sustava, dostupno na: http://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, (1. svibanj 2015.)

[18] Vrste sigurnosnih kopija, dostupno na: http://narodne-novine.nn.hr/clanci/sluzbeni/2004_10_139_2433.html, (1. svibanj 2015.)

[19] V. Šimović, Informacijski sustavi, skripta ,Visoka škola za poslovanje i upravljanje Adam Krđelić, Zaprešić, 2005.

[20] A. Dujella, M. Maretić, dipl. inž., Kriptografija, Element, Zagreb 2007.

[21] Poruka otvorenog teksta: dostupno na: http://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html, (2. svibanj 2015.)

14. Popis kratica

SALW – *eng. Small Arms and Light Weapons (* malo i lako oružje)
IAEA - *eng. International Atomic Energy Agency* (Međunarodna agencija za atomsku energiju)
UN - Ujedinjeni narodi
UNDP – *eng. United Nations Development Programme* (Program Ujedinjenih naroda za razvoj)
EU - Europska unija
OESS – Organizacija za europsku sigurnost i suradnju
IRB - Institut "Ruđer Bošković
NE „Krško" – Nuklearna elektrana „Krško"
BTCW – *eng. The Biological and Toxical Weapons Convention* (Konvencija o biološkom i toksičnom oružju)
NATO – *eng. North Atlantic Treaty Organisation,* (Organizacija Sjevernoatlantskog saveza),
IS– Islamske države
OPWC – *eng.Organisation for the Prohibition of Chemical Weapons* (Organizacija za zabranu
kemijskog oružja)
DoS - eng. *Denial Of Service* (odbijanje usluge)
CD - engl. *Compact disk* (kompaktni disk)
DVD – *eng. Digital video disk (* optički disk*)*
USB – *eng. Universal Serial Bus* (univerzalna serijska sabirnica)
PDF – eng. *Portable Document Format* (hrv. format zapisa dokumenata)
WI-FI – *eng. Wireless-Fidelity* (bežična mreža*)*
WPA - *eng Wi-Fi Protected Access* (algoritam za sigurnu komunikaciju)
WLAN - *eng. Wireless Local Area Network* (označava lokalnu mrežu)
GSM - *eng. Global System for Mobile Communications* (Standard za mobilnu mrežu)

15. Popis slika