**SVEUČILIŠTE U ZAGREBU**

**FAKULTET ORGANIZACIJE I INFORMATIKE**

**Jurica Mlakar**

**KNJIGA IZ KOLEGIJA SIGURNOST INFORMACIJSKIH SUSTAVA**

**INFORMACIJSKA SIGURNOST I RAČUNALNI KRIMINAL**

**Mentor:**

**Prof. dr.sc. Željko Hutinski**

**mag. Inf. Tonimir Kišasondi**

**Varaždin, 2013.**

**Sadržaj**

[1. Informacijska sigurnost 1](#_Toc377064800)

[1.1. CIA teorem 1](#_Toc377064801)

[1.2. Informacijska sigurnost 2](#_Toc377064802)

[1.3. Zaštita 3](#_Toc377064803)

[1.4. Ranjivost 3](#_Toc377064804)

[1.5. Rizik 4](#_Toc377064805)

[1.6. Ostali pojmovi 5](#_Toc377064806)

[2. Računalni kriminal i zlouporaba računala 7](#_Toc377064807)

[2.1. Primjer nositelja prijetnji u sustavima 7](#_Toc377064808)

[2.1.1. Ljudi namjerno 8](#_Toc377064809)

[2.1.2. Ljudi nenamjerno 9](#_Toc377064810)

[2.1.3. Tehnička greška 10](#_Toc377064811)

[2.1.4. Prirodne sile 11](#_Toc377064812)

[2.2. Slučajevi računalnog kriminala 12](#_Toc377064813)

[2.3. Cyber ratovanje 14](#_Toc377064814)

[3. Postupanje pojedinih država prema računalnom kriminalu 17](#_Toc377064815)

[3.1. Konvencija o računalnom kriminalu 17](#_Toc377064816)

[4. Literatura 19](#_Toc377064817)

# 

# Informacijska sigurnost

## CIA teorem

Kako bi se informacijski sustav mogao zaštiti potrebno je znati što je bitno zaštititi. Uz funkcije informacijskog sustava potrebno je osigurati samu informaciju i to njene tri značajke:

* Tajnost (engl. **C**onfidentiality)
* Cjelovitost (engl. **I**ntegrity)
* Dostupnost (engl. **A**vailability)

Informacijski sustav pomoću svoje imovine mora osigurati sve ili barem neke radne funkcije, ali obavezno konzistentnost sve tri značajke svih informacija u njemu. U nastavku će biti prikaz informacijskog sustava i njegovih elemenata u odnosu na značajke informacija.

Imovina

Osnovne funkcije IS-a

Informacijski sustav

**FIZIČKA IMOVINA I HARDVER**

**SOFTVER**

**SERVISI**

**Dostupnost**

**Tajnost**

**LJUDI**

**INFORMACIJSKA IMOVINA**

**NEOPIPLJIVA IMOVINA**

**PRIJENOS INFOMACIJA**

**GENERIRANJE INFORMACIJA**

**KORIŠTENJE INFORMACIJA**

**ČUVANJE INFORMACIJA**

**OBRADA INFORMACIJA**

**Cjelovitost**

Slika 1. Odnos informacijskog sustava i značajki informacija

Iz navedenog proizlazi da se informacijski sustav može prikazati kao skup:

IS={CIA, Imovina, Funkcije}

## Informacijska sigurnost

Sigurnost informacijskih sustava bitna je tema kojoj organizacije diljem svijeta pridaju mnogo pažnje i to s dobrim razlogom. Sigurnosne prijetnje dolaze iz više izvora od računalnog kriminala do špijunaže, sabotaža, prirodnih nepogoda. Kako je šteta nanesena od strane računalnog kriminala sve veća što pokazuju financijski pokazatelji bitno je definirati, planirati, projektirati, implementirati, održavati i kontinuirano poboljšavati informacijsku sigurnost.

Informacijska sigurnost definirana je kroz razne odredbe i standarde te će biti navedene definicije iz izvora koji su relevantni za ovo područje.

Prema **Zakonu o informacijskoj sigurnosti**, I. Osnovne odredbe, Članak 2. navodi:

„**Informacijska sigurnost** je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“

Osim zakona informacijska sigurnost definirana je i **ISO 27001** standardom:

**Informacijska sigurnost** podrazumijeva očuvanje povjerljivosti, integriteta i dostupnosti informacije; uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost.

Uz ovaj pojam ISO 27001 definira još neke bitne pojmove vezane uz ovo područje:

**Sigurnosni događaj** je prepoznatljiv slučaj stanja sustava, usluge ili mreže koji upućuje na moguću povredu politike informacijske sigurnosti ili neuspjeh zaštite ili do tada nepoznate okolnosti koje mogu biti važne za sigurnost.

**Sigurnosni incident** naznačen je jednim ili nizom neželjenih ili neočekivanih sigurnosnih događaja koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti i informacijske sigurnosti.

## Zaštita

Nakon definicije same informacijske sigurnosti dolazi se do pojma zaštite informacijskog sustava, kao nositelja svih informacija potrebnih za nesmetan rad poslovnog sustava.

**Informacija** je imovina koja je bitna za poslovanje i zato zahtjeva i odgovarajuću zaštitu, budući da je izložena velikom broju različitih prijetnji i ranjivosti. (Prof. dr.sc. Željko Hutinski)

**Zaštita informacijskog sustava** dopunjuje sigurnost kao niz mjera i postupaka kojima se smanjuje razlika rizika od dodatnih uočenih ili pretpostavljenih izvora i oblika prijetnje. Ona zavisi od procjene značaja podatkovnog sadržaja, koja je podložna promjenama u zavisnosti od stava okruženja (zakonski i podzakonski akti), odnosno vlastite procjene u odnosu na promjenu značaja pojedinog sadržaja. (Prof. dr.sc. Željko Hutinski)

Zaštita informacijskog sustava zajednička je odgovornost svih zaposlenika poduzeća, tako da samo zdravi, zadovoljni i adekvatno educirani radnici, koji rade u primjerenim uvjetima rada, mogu pridonijeti unapređenju sigurnosti opreme i podataka u poslovnom sustavu. (Klasić, 2007.)

## Ranjivost

Ranije je navedeno kako je informaciju potrebno zaštititi budući da je sustav ranjiv, pa tako postoji rizik da informacija bude izložena neovlaštenom pristupu. **ISO 27002** ranjivost definira kao:

„Ranjivost je **slabost imovine** ili grupe imovina koju jedna ili više prijetnji mogu iskoristiti.“

**Nacionalni CERT** pak ranjivost opisuje kao **slabost** **računalnog sustava** koju je moguće slučajno aktivirati ili namjerno iskoristiti, te tako nanijeti štetu tom sustavu.

Ranjivost također možemo opisati i kao **stanje ili skup stanja** koja mogu omogućiti nekoj prijetnji da utječe na resurse ustanove. One se mogu pojaviti u bilo kojem dijelu računalnog sustava, a najčešće ih nalazimo u korisničkim programima i operativnom sustavu zbog grešaka u programskom kodu. Osim toga, ranjivosti se mogu pojaviti i zbog neprikladnog korištenja računalnih programa ili pogrešno podešene konfiguracije uređaja.

Bez obzira na uzrok, mjesto nastanka ili utjecaj na računalni sustav, iskorištavanjem određenih ranjivosti **napadač** može dobiti potpunu kontrolu nad sustavom, te **ukrasti, izmijeniti ili obrisati podatke** odnosno učiniti sustav djelomično ili potpuno nedostupnim.

Na ranjiva računala napadači, između ostaloga, postavljaju zlonamjerne programe koji im omogućavaju **daljnje napade na druge sustave**. Zbog toga je važno voditi računa o redovitom ažuriranju operativnog sustava računala i pripadajućih programa, te koristiti programe i uređaje prema sigurnosnim smjernicama za njihovu uporabu. (Nacionalni CERT)

Općenito možemo ranjivosti podijeliti na **ranjivosti aplikacije** i **ranjivosti operacijskog sustava**.

## Rizik

**ISO 27001** pri opisu upravljanja informacijskom sigurnošću ISMS navodi kako je dio cjelokupnog sustava upravljanjem, **temeljen na pristupu sa strane poslovnih rizika**, kako bi uspostavio, implementirao, nadzirao, provjeravao, održavao i unapređivao informacijsku sigurnost. (*NAPOMENA: Sustav upravljanja uključuje organizacijsku strukturu, politike, planiranje aktivnosti, odgovornosti, vježbe, procedure, procese i resurse*.)

**Rizik** je u literaturi definiran kao funkcija razine prijetnje, ranjivosti i vrijednosti informacijske imovine. (Jones, Ashenden, 2005, str 186)

Da bi se dakle nešto moglo smatrati rizikom moraju biti prisutne sve tri komponente:

* Prijetnja
* Ranjivost
* Vrijednost imovine

Rizik se jasnije može opisati kao vjerojatnost prijetnje da iskoristi neku ranjivost imovine te time ugrozi imovinu. S obzirom na navedene definicije rizik je moguće prikazati matematičkom formulom:

RIZIK = PRIJETNJA \* RANJIVOST \* VRIJEDNOST IMOVINE

Prikazanom formulom ne izračunava se rizik već formula služi za shvaćanje međuovisnosti prijetnje, ranjivosti i vrijednosti imovine na razinu rizika.

Postoji li visoka razina prijetnje i visoka razina ranjivosti, razina rizika je visoka. Kada je razina prijetnji visoka, ali poduzeće nije toliko ranjivo jer ima implementiranu prikladnu zaštitu tada će razina rizika biti srednja. Poduzeće također može posjedovati imovinu male vrijednosti. Ako u tom slučaju dođe do sigurnosnog incidenta poduzeće neće pretrpjeti velike gubitke, pa rizik nije visok. (Prof. dr.sc. Željko Hutinski)

U normi ISO 27001 su definirani još neki bitni pojmovi vezani uz ovo područje:

**Integritet -** Osobina očuvanja autentičnosti i cjelovitosti imovine

**Rezidualni rizik -** Preostali rizik nakon obrade rizika

**Prihvaćanje rizika -** Odluka da se rizik prihvati

**Analiza rizika - S**ustavna uporaba informacija za određivanje izvora i procjenu rizika

**Procjena rizika -** cjelokupan proces analize rizika i njegovog vrednovanja

**Vrednovanje rizika -** Proces usporedbe procijenjenog rizika s danim kriterijima, kako bi se ustanovio značaj rizika.

**Upravljanje rizikom -** Usklađene aktivnosti za usmjeravanje i kontrolu organizacije u smislu rizika. (*NAPOMENA: Izraz “kontrola" korišten je kao sinonim za mjera.)*

**Obrada rizika** - Proces odabira i primjene mjera za promjenu rizika

## Ostali pojmovi

Uz sve navedene pojmove bitno je spomenuti i ostale pojmove koji se svakodnevno koriste u kontekstu informacijske sigurnosti, a do sada nisu jasno definirani. Njih je William Stallings u svojoj knjizi definirao na sljedeći način:

**Prijetnja** (*engl. Threat*)je potencijal za povredu sigurnosti, koji postoji ako postoje okolnosti, mogućnost, akcija ili događaj koji može ugroziti sigurnost i prouzrokovati štetu.

**Napad** (*engl. Attack*) je definiran kao napad na sigurnost sustava koji proizlazi iz inteligentne prijetnje; to jest inteligentni čin koji predstavlja namjerni pokušaj (pogotovo u smislu metode ili tehnike) da se izbjegne sigurnosne servise i prekrši sigurnosna politika sustava.

**Sigurnosni napad** je akcija koja kompromitira sigurnost informacija posjedovanih od strane organizacije.

**Sigurnosni mehanizam** je mehanizam dizajniran za otkrivanje, sprečavanje i oporavak od sigurnosnih napada.

**Sigurnosni servis** povećava sigurnost sustava za obradu podataka i prijenos informacija u organizaciji. Namjena servisa je suprotstavljanje sigurnosnim napadima. Servis koristi jedan ili više sigurnosnih mehanizama kako bi osigurao pružanje usluge.

**Vektor napada** je put ili sredstvo kojim napad može biti ili je napravljen na kritičnom djelu infrastrukture. Drugim riječima vektori napada omogućuju hakerima da iskoriste ranjivosti sustava, uključujući i ljudske pogreške. (MIT, 2011.)

Ranjivost može biti specifični problem u kodu koji ima utjecaj na sigurnost, dok je vektor napada način pokretanja napada, odnosno dohvaćanja ranjivosti. Jednostavnije bi se moglo zaključiti da vektor napada predstavlja metodu ili tip napada. Na primjer, operativni sustav ili web preglednik mogu imati propust koji je iskorišten od strane web stranice.

Osim vektora napada za koje je potrebno napredno tehničko znanje, pri konstruiranju napada koriste se i ljudski nedostaci. Na primjer, korisnik početnik može otvoriti privitak e-mail pošte koja sadrži virus, a većinu korisnika se može uvjeriti da barem jednom u životu otkriju pristupne podatke iz na oko nerelevantnih razloga.

# Računalni kriminal i zlouporaba računala

## Primjer nositelja prijetnji u sustavima

Kako bi se kompletni informacijski sustav uspješno štitio od prijetnji iz okoline i internih izvora prijetnji bitno je biti upoznat s informacijama koje treba zaštititi, sustavima za pohranu, prijenos i obradu informacija u sustavu, te prijetnjama kojima je sustav izložen.

Izvor prijetnji mogu biti:

1. Ljudi namjerno
   1. Kompromitacija intelektualnog vlasništva
   2. Namjerno djelo kršenja granica
   3. Namjerno djelo iznude informacija
   4. Namjerno djelo krađe
   5. Namjerno djelo sabotaže ili vandalizma
   6. Namjerni softverski napadi
2. Ljudi nenamjerno
   1. Djelo ljudske pogreške ili propusta
3. Tehnička greška
   1. Odstupanja u kvaliteti usluge dobavljača
   2. Tehnički zastoj hardvera ili greške
   3. Tehnički softverski propust ili greške
   4. Tehnološka zastarjelost
4. Prirodne sile

**Computer Crime and Security Survey, (CSI/FBI)** jasno prikazuje stanje u svijetu.

Otkriveno je da su „najskuplji“ sigurnosni incidenti bili povezani uz financijsku računalnu prijevaru s prosječno prijavljenim gubitkom od 500.000,00$. Drugi u prosjeku „najskuplji“ incidenti bili su povezani s „bot“ računalima u organizacijskoj mreži s prijavljenom štetom od 350.000,00$ po ispitaniku.

Sigurnosni incidenti povezani s malicioznim kodom bili su najčešći i incident je zabilježilo 49% od svih ispitanih organizacija. Drugi najčešći incidenti povezani su sa zloupotrebom mreža unutar organizacija, te se incident pojavio kod 44% ispitanika. Dok je treći najčešći incident bio povezan s krađom laptopa i ostalih mobilnih uređaja u iznosu od 42%.

### Ljudi namjerno

Najčešći nositelj prijetnji, koji dominira u svijetu dolazi od strane pojedinaca koji svojim djelovanjem najčešće neautorizirano koriste, uništavaju ili neregistrirano vrše promijene nad sadržajem. Oni na razne načine ugrožavaju informacijski sustav ili nanose direktnu štetu poslovnom sustavu kroz kompromitaciju softverskog proizvoda poduzeća i sl. U nastavku će biti opisani načini na koje ljudi kao nositelji prijetnji mogu ugroziti sustav.

**Kompromitacija intelektualnog vlasništva**

Primjer podrazumijeva **piratstvo i povredu autorskog prava**. Zakon o autorskom pravu i drugim srodnim pravima na primjer u Poglavlju 8., sadrži „Posebne odredbe za računalne programe“ gdje se računalni program u Članku 107. opisuje:

„Računalni program je zaštićen kao jezično djelo po ovom Zakonu ako je izvoran u smislu da predstavlja vlastitu intelektualnu tvorevinu svog autora. Pojam računalni program obuhvaća izražaj računalnog programa u bilo kojem obliku uključujući i pripremni dizajnerski materijal. Ideje i načela na kojima se zasniva bilo koji element računalnog programa, uključujući i ona na kojima se zasnivaju njegova sučelja, nisu zaštićena autorskim pravom.“

**Zaštita** od ovog oblika prijetnje postoji u obliku tehničkih mehanizama poput ugrađenih kodova za pravo kopiranja, namjernih smještanja loših sektora na medij i sl.; zaštita u obliku licenci; online registracije i aktivacije softverskog proizvoda i suradnja s organizacijama koje se bave sa zaštitom od softverskog piratstva i zaštitom od povrede autorskih prava.

**Namjerno djelo kršenja granica**

Granice sustava predstavljaju dijelovi informacijskog sustava kojima se može pristupiti samo od strane ovlaštenih osoba. Primjer nositelja prijetnje predstavlja bilo koji pojedinac koji neovlašteno pristupi i/ili prikuplja podatke. Ovisno o razini znanja i ekspertize nazivaju se hakeri, script kiddies, pocket monkey, crackeri itd.

U konkretnim situacijama konkurentsko istraživanje preko interneta može postati ilegalna radnja ako se pređu granice zakona i etičnosti. Tada se legalna radnja pretvara u ilegalnu te se naziva **industrijska špijunaža**.

Osim industrijske špijunaže zabilježeni su slučajevi špijunaže vlada država što predstavlja direktnu prijetnju nacionalnoj sigurnosti.

Sustav je moguće zaštititi označavanjem virtualnih granica sustava kroz upozorenja i naprednim sustavima autentifikacije i autorizacije korisnika.

**Namjerno djelo iznude informacija**

Javlja se ako pojedinac dođe do podataka koji imaju iznimnu vrijednost za sustav, te za njihovo neobjavljivanje traži kompenzaciju. Ovakvi slučajevi mogu itekako naštetiti poslovanju poduzeća kojem su otuđeni. Najčešće se radi o slučajevima krađe korisničkih računa, brojeva kreditnih kartica ili drugih podataka pogodnih za ucjenu vlasnika.

**Namjerno djelo krađe**

Radnja ovog tipa podrazumijeva ilegalno preuzimanje tuđeg vlasništva, koje se zatim koristi i/ili zloupotrebljava bez znanja vlasnika. Za razliku od iznude ovdje se ukradeni podaci koriste za direktno pribavljanje koristi za počinitelja.

**Namjerno djelo sabotaže ili vandalizma**

Ovakve radnje osim što čine direktnu štetu reputaciji poduzeća, mogu imati i mnogo snažnije posljedice ako se napad izvodi s ciljem uništavanja imovine žrtava. Konkretan primjer su aktivnosti cyber-aktivista tj. haktivista koje mogu graničiti s **kibernetičkim terorizmom** ako se sabotira rad informacijskih sustava koji se brinu za stabilan rad postrojenja koja bi u suprotnom mogla ugroziti sigurnost ljudi. Tu primjer mogu biti nuklearna postrojenja, opskrba električnom energijom bolnica ili sustavi istraživačkih centara.

**Namjerni softverski napadi**

Korištenjem malwera, odnosno zloćudnog koda ili softvera najčešći je oblik koje čovjek kao nositelj prijetnji koristi kako bi izvršio napad na informacijski sustav. Ova vrsta prijetnji i najznačajniji incidenti malicioznog koda u povijesti biti će opisani u ostalim poglavljima ove knjige.

### Ljudi nenamjerno

Mnoge prijetnje dolaze od strane osoba koje imaju ovlašten pristup informacijskom sustavu. Zbog manjka edukacije mnogi ovlašteni korisnici mogu prouzrokovati značajnu štetu, što možemo definirati kao djelo ljudske pogreške ili propusta.

Konkretan primjer je odavanje pristupnih podataka, greške u radu s osjetljivim sustavom, nesreće uzrokovane nepažnjom i sl. Kako bi se rizik od ovakvih prijetnji sveo na minimum potrebno je podizati svijest o informacijskoj sigurnosti među djelatnicima poduzeća, provoditi edukacije za zaposlene te uvesti procedure kojima bi se provodile sigurnosne mjere.

### Tehnička greška

Nositelji prijetnji je svakako i kompletna infrastruktura, oprema i energenti, odnosno dobavljači o kojima ovisi funkcioniranje informacijskog sustava. Ovakve prijetnje se kao i sve ostale mogu predvidjeti i na njih se može u određenoj mjeri utjecati uvođenjem redundantnog sustava.

**Odstupanje u kvaliteti usluge**

Ovdje se isključivo govori o vanjskim dobavljačima čije su usluge neophodne za nesmetan rad informacijskog sustava. Konkretan primjer je nepravilan dovod električne energije koji može oštetiti hardverski dio sustava. Ukoliko dođe do prekida dovoda električne energije sustav bez odgovarajućih mjera zaštite ne može egzistirati.

Jedina zaštita u ovom slučaju je uvođenje UPS uređaja, odnosno uređaja koji mogu dovoljno dugo održavati dovod električne energije do sigurnog gašenja uređaja ili paljenja agregata. Kako bi se sustav zaštitio od nepravilnog dovoda električne energije koriste se potiskivači prednapona. (Prof. dr.sc. Željko Hutinski)

Većina informacijskih sustava podržava rad s korisnicima preko interneta i kompletno poslovanje ovisi o tome. Ukoliko dođe do kvara od strane pružatelja internetskih i komunikacijskih usluga, sustavi poput bankarskih mogu pretrpjeti velike gubitke. (Prof. dr.sc. Željko Hutinski)

**Tehnički zastoj hardvera ili greške**

Greške se očituju u obliku ispada čvrstih diskova, prestanka rada uređaja pri previsokim temperaturama ili preopterećenja. Zaštita od ovakvih izvora prijetnji moguća je uvođenjem redundantnih dijelova sustava, RAID tehnologije s „**hot swappable**“ diskovima koji se mogu zamijeniti bez gašenja sustava, senzora za praćenje atmosferskih uvjeta gdje se uređaji nalaze i ostalih zaštitnih mehanizama. (Tonimir Kišasondi, mag.inf, EUCIP)

**Tehnički softverski propust ili greške**

Softverski propusti nedopustivi su kod sustava gdje se obavljaju financijske transakcije ili na primjer razmjena povjerljivih podataka. Propusti se mogu npr. prikazati u obliku sigurnosnih propusta ili u obliku rušenja aplikacije.

Konkretan primjer bio bi softverski propust na uređajima za klađenje na utrke. Naime softver funkcionira tako da na uređaju ima pohranjenu bazu od nekoliko tisuća snimki utrka koje se nasumice prikazuju na ekranu nakon uplate. Ukoliko bi se uređaj ugasio usred prikaza utrke, ponovnim uključivanjem uređaja softver bi ponovio prethodnu utrku nakon nove uplate. Slučajnim „otkrićem“ propusta nanijeta je velika šteta poduzeću koje posjeduje mrežu takvih uređaja.

**Tehnološka zastarjelost**

Tehnološka zastarjelost može biti uzrok svih navedeni primjera prijetnji koje za posljedicu imaju štetu nad hardverom. Potrebno je analizirati i unaprijed planirati uvođenje nove tehnologije kako se zastarjela tehnologija ne bi negativno odrazila na rad informacijskog sustava i u konačnici na organizaciju.

### Prirodne sile

Prirodne sile sve su češći uzrok prijetnji informacijskim sustavima. S obzirom na tu činjenicu mnoge države propisuju točnu regulativu za svoje informacijske sustave kojima štite sustave od svih fizičkih prijetnji od kojih su najčešće prirodne sile.

Pod prirodne sile podrazumijevaju se: potresi, poplave, požari, uragani, tsunamiji, požari i kontaminacija prašinom.

Zaštita od prirodnih sila realizira se putem udaljenih redundantnih sustava u slučaju potresa. Po mogućnosti se takvi sustavi smještaju na drugo tektonsko područje. Također potrebno je voditi brigu o tome da se sustav ne smješta u blizini rijeka, velikih prometnica i ostalih mogućih izvora prijetnji.

Ako pak postoji opasnost od poplave ili požara unutar smještajnih kapaciteta opreme, bitno je zaštititi opremu podignutim podom, posebnom ventilacijom i protupožarnim serverskim ormarima.

Brzo obavještavanje nadležnih službi također može biti ključno u sprječavanju velike štete zbog čega se ugrađuju senzori, te se definiraju planovi i procedure za oporavak u slučaju katastrofe (DRP - Disaster Recovery Plan). Uz njih definiraju se i planovi za kontinuitet poslovanja (BCP - Bussines Continuity Plan) i planovi odgovora na incidente (IRP - Incident Response Plan). (Prof. dr.sc. Željko Hutinski)

## Slučajevi računalnog kriminala

Začetnici računalnog kriminala su špijuni koji su povjerljive podatke uspješno prikupljali i distribuirali obavještajnim agencijama s kojima su surađivali. Obavještajne agencije koristile su razne metode kako bi došle do povjerljivih podataka. Kako je rekao nepoznati KGB-ov operativac:

„It's easier to break fingers then to break codes.“

Špijuni su često godinama bili zaposleni u organizacijama od kojih su trebali prikupiti podatke. Obavještajne agencije regrutirali su ih pomoću tzv. MICE što predstavlja kraticu od novac, ideologija, prisila i ego. To su četiri strategije kojima se ovisno o osobi, odnosno njihovim slabostima pristupa potencijalnim agentima. Često je bilo lakše utjecati na ljude nego penetrirati u sustav što povijest i pokazuje.

**Klaus Fuchs** bio je njemački fizičar i špijun za područje atomske energije, koji je 1950. godine bio uvjeren da prikuplja podatke u Manhattan Project koji su vodili Amerika, Velika Britanija i Kanada. Manhattan Project bavio se istraživanjem atomske energije te je tijekom trajanja projekta proizvedena i prva atomska bomba za vrijeme drugog svjetskog rata.

Slika 2. Klaus Fuchs

**Aldrich Ames** je bivšikontraobavještajni časnik i analitičar Centralne obavještajne agencije (CIA) koji je 1994. godine uvjeren da prikuplja podatke za Rusiju. Smatra se da je drugi najuspješniji po broju kompromitirane imovine CIA-e. Tijekom devet godina rada u kontraobavještajnoj jedinici imao je godišnji prihod od 60 000$, ali je mjesečno preko kreditnih kartica trošio 30 000$. Njegov životni stil uključivao je i novi Jaguar, kao i kuću u vrijednosti preko pola milijuna dolara koju je platio gotovinom. Njegova slabost bila novac i zbog novca je i uhvaćen. (Robinson, Stephen, 1995.)

Slika 3. Aldrich Ames

**Robert Hanssen** bivši je američki agent Saveznog ureda za istrage (FBI), koji je 22 godine u razdoblju od 1979. do 2001. godine prikupljao podatke za Ruske obavještajne agencije. Optužen je za prodaju američkih tajni Sovjetskom savezu, kasnije Rusiji za 1.4 milijuna dolara u gotovini i dijamantima. Optužen je na doživotnu kaznu zatvora bez mogućnosti pomilovanja, a njegov pothvat je od strane komisije FBI sigurnosnog programa proglašen kao „vjerojatno jedan od najgorih obavještajnih katastrofa u američkoj povijesti“. (FBI, 2002. )

Slika 4. Robert Hanssen

**Anna Chapman** Ruskinja po nacionalnosti, glasi kao jedna od najpoznatijih i najzgodnijih žena u svijetu računalnog kriminala. 2010. godine uhićena je s još devet ljudi pod sumnjom da radi za Illegals Program, odnosno špijunsku mrežu pod vanjskom obavještajnom agencijom Ruske federacije. Priznala je krivnju za optužbe da djeluje kao agent strane vlade, bez obavještavanja Američkog državnog odvjetništva. Deportirana je u Rusiju 8. srpnja 2010. godine kao dio razmjene zatvorenika.

Sudjelovala je u mnogim operacijama gdje je kao KGB-ov „Honeypot“, zahvaljujući svom atraktivnom izgledu zavodila ugledne i visokopozicionirane službenike političkog i ekonomskog društva SAD-a, pridobila njihovu naklonost i izvlačila povjerljive informacije i dostavljala ih Ruskoj obavještajnoj agenciji SVR (Sluzhba Vneshney Razvedki).

Slika 5. Anna Chapman

## Cyber ratovanje

**Cyber ratovanje** definira se kao korištenje računalne tehnologije kako bi se poremetile aktivnosti neke države ili organizacije, namjernim napadanjem komunikacijskih sustava od strane druge države ili organizacije. Cyber rat je asimetričan što znači da se koristi puno manje vojne sile za razliku od klasičnog rata. (Oxford Dictionaries)

Ovakav način ratovanja za cilj uglavnom ima distribuciju propagande, prouzrokovati štetu tehnološke infrastrukture (elektrane, komunikacijske ili bilo koje strateški važne sustave), trajno prikupljanje informacija i sl.

Napadi se vrše pomoću nedopuštenog prisluškivanja (*engl. „Eavesdropping“*), eksploatacije pomoću Trojanaca, Crva, DDoS napada ili pomoću Rootkit alata i Keyloggera.

**Case study: Titan Rain**

Slučaj Titan Rain naziv je dobio od strane federalne vlade SAD-a za seriju koordiniranih napada na Američke informacijske sustave od 2003. godine u kojemu su Kineski hakeri, odnosno cyber-špijuni ilegalno pribavljali tajne podatke SAD-a. Otkrilo se da su napadi trajali barem tri godine.

Titan Rain hakeri pribavljali su podatke iz Sandia National Laboratories gdje je dizajniran veći dio američkog nuklearnog arsenala. Osim navedenog laboratorija na meti se našla i kompanija Lockheed Martin. To je Američka globalna kompanija koja se bavi zrakoplovstvom, obranom, sigurnošću i naprednim tehnologijama. Napadnut je i Redstone Arsenal (RSA) glavni komandni centar više Američkih vojnih organizacija, te NASA. Otkrio ih je Shawn Carpenter, veteran Američke ratne mornarice koji je bio odgovoran za sigurnost informacijskog sustava Sandia National Laboratories. (Time Magazine, 2005.)

**Case study: 2007 Estonia cyberware**

Cyber napadi na Estoniju započeli su 27.04.2007. godine kao serija napada koji su preplavili stranice estonskih organizacija, uključujući i stranice estonskog parlamenta, banaka, ministarstava, novina i ostalih medija. Napade je izvršila Rusija potaknuta micanjem kipa Bronze Soldier of Tallinn, odnosno Sovjetskog memorijalnog centra smještenog u gradu Tallinn u Estoniji, piše The Guardian.

Cilj napada bio je utjecaj na javnost. Ovo je prvi primjer kako **DDoS** napad može onesposobiti nacionalnu infrastrukturu. **Distributed Denial of Service** napad ostvaren je korištenjem metoda „ping floods“ od strane pojedinaca, do korištenja botnet-a za distribuciju spama. Spam je korišten za napade na veće informativne portale, uključujući i stranice političkih stranaka poput The Estonian Reform Party kojoj je na čelu tada aktualni premijer Estonije Andrus Ansip.

Smatra se da je ovaj slučaj drugi po veličini međudržavnog cyber napada nakon slučaja Titan Rain. Slučaj je ozbiljno shvatio i NATO koji je u Estoniju poslao svoje najbolje ljude kako bi istražili cijeli slučaj i podigli razinu zaštite u Estoniji.

**Case study: GhostNet**

GhostNet je naziv dan od strane istraživača iz Information Warfare Monitor (IWM) za veliki slučaj cyber špijunaže koji je otkriven u ožujku 2009. godine. Napad je izvela Republika Kina koja se infiltrirala kod visoko rangiranih političara, ekonomista i medijskih kuća u čak 103 zemlje svijeta. Kompromitirani su informacijski sustavi ambasada, stranih ministarstava, uredi vlada i tibetanski centri Dalai Lame za prognanike u Indiji, Londonu i New Yorku. Sumnja se da je napad povezan s **Advanced persistent threat** (**APT**) napadima o kojima će više biti u nastavku.

IWM istraživači su također otkrili kako je Kineska vlada prikupljala podatke pomoću TOM-Skype, kinesku inačicu Skype-a, koji je pohranjivao sve podatke koje su korisnici razmjenjivali. Slučaj je izašao na vidjelo kada su jednoj tibetanskoj ženi, koju je ispitivala kineska obavještajna služba, predočeni transkripti njenih online razgovora. (BBC, 2009.)

**Case study: 2009+ Aurora**

Operacija Aurora provedena je napadom **Advanced persistent threat** (**APT**)  od strane aktera sa sjedištem u Shaoxing regiji u Kini i poveznicom s Narodnom oslobodilačkom vojskom. Prvu naznaku napada objavio je Google 12. siječnja 2010. godine u blogu, gdje navodi kako je napad počeo sredinom 2009. godine, te se nastavio do prosinca 2009.. Napad je bio usmjeren na desetke organizacija od kojih su Adobe Systems, Juniper Networks i Rackspace javno potvrdili da su bili mete.

Osim navedenih prema izvješćima medija mete su bile i poduzeća poput Yahoo-a, Symantec, poduzeća Northrop, Grumman, Morgan Stanley i Dow Chemical.

Kao posljedicu napada, Google je u svom blogu objavio da planira pokrenuti potpuno necenzuriranu verziju svoje tražilice u Kini. Iz Googlea su također poručili da će ako to nije moguće zatvoriti svoje kineske urede i napustiti Kinu.

Naziv napadu dao je Dimitri Alperovitz, potpredsjednik odjela za istraživanje napada iz poduzeća McAfee. Prema McAfee, primarni cilj napada bio je dobivanje pristupa kako bi se potencijalno promijenio izvorni kod repozitorija navedenih poduzeća.

**APT napad** najčešće se odnosi na određenu grupaciju, poput vlade neke države, koja ima mogućnost i namjeru trajnog i učinkovitog ciljanja određenog entiteta. Ovaj termin se obično odnosi na cyber napade, prije svega špijunažu preko interneta uporabom raznih obavještajnih podataka i tehnika za pristup osjetljivim informacijama. (Tonimir Kišasondi, mag.inf, EUCIP)

**Case study: 2006 + APT1**

Mandiant Intelligence Center je online centar koji služi za opremanje sigurnosnih timova u kontekstu obrane od najnaprednijih izvora prijetnji. U svom izvješću opisuju APT1 i izvode određene zaključke.

APT1 je izvor prijetnje najvjerojatnije sponzoriran od strane Kineske vlade i jedan je od najtrajnijih računalnih izvora prijetnji. Opseg i utjecaj APT1 operacija je potaknulo centar da napiše opširno izvješće na ovu temu. U pokušaju proširivanja obrane protiv APT1 operacija Mandiant je također objavio preko 3 000 indikatora koji pomažu u detekciji APT aktivnosti. Vjeruje se da je APT1 drugi Biro narodne oslobodilačke vojske, trećeg odjela Glavnog stožera (*engl. People's Liberation Army General Staff Department (GSD)*), koji je poznat po svojoj vojnoj jedinici Military Unit Cover Designator (MUCD) odnosno kao Unit 61398.

APT1 je odgovoran je za sustavnu krađu više stotina terabajta podataka od najmanje 141 organizacije. Fokusira se na ugrožavanje industrijski orijentiranih organizacija s engleskog govornog područja. APT1 održava veliku infrastrukturu računalnih sustava diljem svijeta. Analizom je otkriveno kako su se u više od 97% slučajeva koristili sustavi i IP adrese registrirani u Šangaju kako bi se mogao koristiti pojednostavljeni kineski jezik prilikom napada.

APT1 infrastruktura upućuje da se radi o organizaciji u kojoj radi najmanje na desetke, a vjerojatno i stotine ljudskih operativaca. Forenzički tragovi vode do zgrade od 12 katova smještene u području mješovite namjene Pudong u Šangaju.

# Postupanje pojedinih država prema računalnom kriminalu

## Konvencija o računalnom kriminalu

Konvencija o kibernetičkom kriminalu predložena je i usvojena na sjednici Vijeća Europe, a koju je Republika Hrvatska potpisala 23. studenog 2001. godine. Konvencija je stupila na snagu 2004. godine i dopunjena je dodatnim protokolom 2006. godine.

Države članice Vijeća Europe i ostale države potpisnice ove Konvencije potpisale su konvenciju smatrajući da je cilj Vijeća Europe postići **vođenje zajedničke kaznene politike** usmjerene zaštiti društva od kibernetičkog kriminala od prvenstvene važnosti, i to među ostalim i putem usvajanja odgovarajućeg zakonodavstva i **poticanjem međunarodne suradnje**.

Zemlje potpisnice svjesne su dubokih promjena nastalih digitalizacijom, konvergencijom i neprekidnom globalizacijom računalnih mreža; zabrinute zbog mogućnosti da računalne mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela.

**Sažetak ugovora**

Konvencija je prvi međunarodni ugovor o zločinima počinjenim putem interneta i drugih računalnih mreža, koja se posebno bavi povredom autorskih prava, računalom povezanih prijevara, dječjom pornografijom i povredom sigurnosti mreža. Ona također sadrži niz ovlasti i postupaka kao što je pretraga računalnih mreža i njihovo presretanje.

Glavni cilj konvencije, kako stoji u uvodu, je nastaviti zajedničke kaznena politike usmjerene na zaštitu društva protiv kibernetičkog kriminala, posebice usvajanjem odgovarajućeg zakonodavstva i jačanjem međunarodne suradnje.

(Službene stranice Vijeća Europe)

Konvencija „pokriva“:

**Dio 1. – Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i**

**sustava.**

* Članak 2. – NEZAKONITI PRISTUP
* Članak 3. – NEZAKONITO PRESRETANJE
* Članak 4. – OMETANJE PODATAKA
* Članak 5. – OMETANJE SUSTAVA
* Članak 6. – ZLOPORABA NAPRAVA

**Dio 2. – Računalna kaznena djela**

* Članak 7. – RAČUNALNO KRIVOTVORENJE
* Članak 8. – RAČUNALNA PRIJEVARA
* Članak 9. – KAZNENA DJELA VEZANA UZ DJEČJU PORNOGRAFIJU
* Članak 10. – KAZNENA DJELA POVREDE AUTORSKIH I SRODNIH PRAVA

Konvencija sadrži još niz odredaba vezanih uz odgovornosti pravnih osoba, sankcije i mjere, međunarodnu suradnju i sl. Konvencija je dopunjena dodatnim protokolom pod nazivom: KRIMINALIZACIJA RASISTIČKOG I KSENOFOBNOG MATERIJALA TE PRIJENOS TIH PORUKA.

**Zašto je konvencija bitna?**

Računalni kriminal se može počiniti iz bilo koje zemlje prema sustavu koji se nalazi bilo gdje. Zbog toga je potrebno omogućiti međunarodnu suradnju, kako bi se počinitelje moglo privesti i sankcionirati. (Tonimir Kišasondi, mag.inf, EUCIP)

# Literatura

[1] William Stallings: Network Security Essentails, Applications and Standards, Third Edition, 2007.

[3] Zakon o autorskom pravu i srodnim pravima, <http://narodne-novine.nn.hr/clanci/sluzbeni/306987.html>

[4] Zakon o informacijskoj sigurnosti, Vlada Republike Hrvatske, Zagreb, 18. srpnja 2007.

[5] ISO/IEC 27000:2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[6] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[7] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management

[8] Robert Richardson, CSI Director: CSI Computer Crime & Security Survey, 2008.

[9] Robinson, Stephen. Books: The disreputable drunk who betrayed America, The Sunday Telegraph 2 July 1995

[10] "A Review of FBI Security Programs (Webster Report) (March 2002). Commission for Review of FBI Security Programs, United States Department of Justice.

[11] Ksenija Klasić, Hrčak - Portal znanstvenih časopisa Republike Hrvatske, 2007, Zaštita informacijskih sustava u poslovnoj praksi, <http://hrcak.srce.hr/index.php?id_clanak_jezik=18245&show=clanak> Dostupno 25.11.2013.

[12] Suspected Russian spies charged in US . BBC, 2010. <http://www.bbc.co.uk/news/10442223> Dostupno 25.11.2013.

[13] Anna Chapman – The World’s Most Sexiest Hacker, Atish Ranjan, 2013.

<http://www.techtricksworld.com/2013/07/anna-chapman-the-worlds-most-sexiest-hacker.html> Dostupno 25.11.2013.

[14] Cyberware <http://www.oxforddictionaries.com/definition/english/cyberwar> Dostupno 25.11.2013.

[15] Titan Rain [http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html#](http://content.time.com/time/magazine/article/0,9171,1098961-1,00.html) Dostupno 25.11.2013.

[16] Attack vector Massachusetts Inst. of Tech., The Future of the Electric Grid, Glossary, at 261 (2011) <http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf> Dostupno 25.11.2013.

[17] Major cyber spy network uncovered, BBC, 2009.

<http://news.bbc.co.uk/2/hi/americas/7970471.stm> Dostupno 25.11.2013.

[18] Konvencija o računalnom kriminalu <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG> Dostupno 25.11.2013.

[19] APT1 izvješće MANDIAN <http://intelreport.mandiant.com/> Dostupno 25.11.2013.