ZAŠTITA I SIGURNOST PODATAKA U INFORMACIJSKOM SUSTAVU

Hajman, Dražena

VISOKA POSLOVNA ŠKOLA ZAGREB
s pravom javnosti

Dražena Hajman

ZAŠTITA I SIGURNOST PODATAKA U INFORMACIJSKOM SUSTAVU

(završni rad)

Zagreb, rujan 2017.

VISOKA POSLOVNA ŠKOLA ZAGREB
s pravom javnosti

Preddiplomski stručni studij
Smjer manager komunikacija

ZAŠTITA I SIGURNOST PODATAKA U INFORMACIJSKOM SUSTAVU

(završni rad)

MENTOR:
Dr. sc. Oliver Hip

STUDENT:
Dražena Hajman
MBS: 4/14 MI

Zagreb, rujan 2017.

I Z J A V A S T U D E N T A

Izjavljujem da sam završni rad naslova **„ZAŠTITA I SIGURNOST PODATAKA U INFORMACIJSKOM SUSTAVU“** izradila samostalno, pod nadzorom i uz stručnu pomoć mentora dr.sc. Olivera Hipa.

Izjavljujem da je završni rad u potpunosti napisan i uređen prema Pravilniku o završnom radu na stručnim preddiplomskim i specijalističkim diplomskim stručnim studijima VPŠZ-a te sukladno uputama u priručniku „Metodologija pisanja seminara i završnog rada.“

Izjavljujem da je završni rad lektoriran na jeziku na kojemu je napisan: Dinka Lovreškov.

Izjavljujem i da sam suglasan da se trajno pohrani i objavi moj završni rad

ZAŠTITA I SIGURNOST PODATAKA U INFORMACIJSKOM SUSTAVU

u javno dostupnom institucijskom repozitoriju *Visoke poslovne škole Zagreb* i javno dostupnom repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o znanstvenoj djelatnosti i visokom obrazovanju, NN br. 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14 i 60/15).

Ime i prezime
studenta
Dražena
Hajman
OIB:
86148451267

_____

(potpis)

Sažetak

Tema završnog rada je „Zaštita i sigurnost podataka u informacijskom sustavu“. U radu se opisuju načini zaštite informacijskih podataka, te opasnosti koje mogu kompromitirati i uništiti podatke. u 21. stoljeću ekonomski prosperitet nacija i njihova sposobnost da uspješno sudjeluju u regionalnim i svjetskim integracijama prije svega ovisi od njihove sposobnosti zaštite vitalnih privatnih, poslovnih i državnih podataka a da pri tome ne ugroze privatnost građana, produktivnost ekonomije i efikasnost rada državnih organa. Zaštitu podataka možemo definirati kao skup metoda, tehnika i pravnih normi kojima se ograničava pristup podacima od strane programa i ljudi, te štiti fizički integritet cjelokupnog računalnog sustava. Veliki broj dokumenata predstavlja neku vrstu intelektualnog vlasništva i poslovnu tajnu te zahtijeva najveću moguću razinu nadzora i zaštite pristupu dokumentu, kao i raspolaganja njegovim sadržajem. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite. Osnovni oblik obrane od virusa i ostalih štetnih prijetnji u informacijskom sustavu je zaštita računala. Riječ je o dosta složenom postupku koji osim primjene odgovarajućih programa od korisnika zahtijeva i oprezno ponašanje.

Ključne riječi: *računalni podaci, zaštita podataka, antivirusni programi, kriptografija*

Summary

The topic of the final theses is "Security and Data Security in the Information System". This paper describes the ways of information protection, and the dangers that can threaten and destroy data. In the 21st century, the economic prosperity of the nations and their ability to successfully participate in regional and global integration depends primarily on their ability to protect vital private, business and state data without jeopardizing the privacy of citizens, productivity of the economy and the work efficiency of state organs. Data protection can be defined as a set of methods, techniques and legal norms that restrict access to data by programs and people, and protect the physical integrity of the entire computer system. A large number of documents represent some kind of intellectual property and business secret and require the highest possible level of supervision and protection of access to the document as well as disposal of its content. Many security mechanisms such as antivirus programs, computer security protocols (for example IPSec), access control, encryption, watermarks can be used to protect documents. However, effective protection does not only apply one solution, but a combination of these protection methods. The basic form of defense against viruses and other harmful threats in the information system is computer protection. It is a rather complex procedure that, apart from applying the appropriate programs, requires cautious behavior of the user.

Key words: *computer data, data protection, antivirus programs, cryptography*

SADRŽAJ

1. UVOD

Informacijske i komunikacijske tehnologije (ICT) u današnje vrijeme globalnog poretka predstavljaju osnovu za privredni razvoj i efikasno upravljanje ograničenim resursima u privredi i državnoj upravi.

Prodiranjem u sve pore društva, informacijske i komunikacijske tehnologije su postale osnova za poslovne i upravljačke sustave, koji postaju sve složeniji. Ovakav razvoj je doveo do izuzetno otežane kontrole i zaštite vitalnih podataka, što je dovelo i do povećanja troškova upravljanja. Očigledno je da u 21. stoljeću ekonomski prosperitet nacija i njihova sposobnost da uspješno učestuju u regionalnim i svjetskim integracijama prije svega ovisi od njihove sposobnosti zaštite vitalnih privatnih, poslovnih i državnih podataka a da pri tome ne ugroze privatnost građana, produktivnost ekonomije i efikasnost rada državnih organa.

Završni rad podijeljen je u tri cjeline. U prvom dijelu rada pisala sam o važnosti podataka, te potrebi da se isti zaštite od zloupotrebe. Drugi dio rada govori o načinima zaštite podataka, kako fizičkim tako i softverskim. Zadnji dio rada prikazuje viruse i ostale štetne prijetnje koje u informacijskim sustavima mogu uzrokovati kompromitiranje i gubitak podataka.

2. ZAŠTO ZAŠTITITI PODATKE?

Dokumenti su temeljni poslovni resurs svake organizacije jer sadrže ključne informacije o poslovanju, kao što su planovi, izvještaji, poslovni rezultati, projekti, nacrti, izračuni, sheme i slično. Veliki broj dokumenata predstavlja neku vrstu intelektualnog vlasništva i poslovnu tajnu te zahtijeva najveću moguću razinu nadzora i zaštite pristupu dokumentu, kao i raspolaganja njegovim sadržajem. Zaštita dokumenata postaje teško ostvariv zadatak uz trend zamjene papirnatih dokumenata elektroničkim oblikom. Digitalne dokumente važno je zaštititi od neovlaštenog kopiranja i upotrebe, kao i od curenja podataka osjetljivih dokumenata te prijetnji povjerljivosti i integritetu podataka u dokumentu. Gubitak dokumenata zbog slučajnog brisanja, prepisivanja, kvarenja čvrstog diska može stajati tvrtku mnogo novaca i uzrokovati gubitak produktivnosti. U današnjem poslovnom okruženju očekuje se da je moguće zaštititi dokumente od neovlaštenog pristupa, iskorištavanja ranjivosti alata za čitanje dokumenata te od neprimjerene upotrebe .

Organizacije koje posjeduju dokumente s važnim i povjerljivim informacijama, posebnu pažnju poklanjaju sljedećim aspektima sigurnosti:

- tajnost– podaci u dokumentu smiju biti dostupni samo ovlaštenim korisnicima,
- autentičnost – jednoznačno prepoznavanje ovlaštenih korisnika,
- odgovornost - praćenje pristupa i izmjena,
- integritet - upozorenje je li dokument bio mijenjan,
- izvornost - provjera izvora dokumenta.

Oduvijek je postojala potreba zaštite osjetljivih podataka, a time i dokumenata koji sadrže takve podatke. Tokom povijesti razvijeno je mnogo metoda kojima su ljudi pokušavali i uspijevali očuvati tajnost važnih podataka. Mnoge metode su bile jednostavne i nisu pružale dovoljnu zaštitu. U takvim slučajevima tajnost je često bila narušena. Razvojem kriptografije i tehnologije otkriveni su vrlo dobri načini kriptiranja i zaštite dokumenata. Kriptiranje je dobar način sprječavanja neovlaštene osobe od pregledavanja sadržaja osjetljivog dokumenta. Ali kada se dokument dekriptira tajnim ključem, ovlaštena osoba loših namjera može spremiti, kopirati, ispisati ili proslijediti dokument. Ograničavanje pristupa dokumentu nekolicini pojedinaca jedan je od pristupa zaštite dokumenta, no uvijek postoji mogućnost da jedna od osoba kojoj je

povjeren pristup oda podatke. U tom slučaju treba se pronaći osobu koja je odala informacije, što nije uvijek jednostavan zadatak. Rješenje koje osigurava zaštitu osjetljivih informacija ne može ovisiti o samo jednoj tehnologiji. Mnogi sigurnosni mehanizmi, kao što su antivirusni programi, sigurnosni protokoli mreža računala (npr. IPSec), kontrola pristupa, kriptiranje, vodeni žigovi, mogu se upotrijebiti za zaštitu dokumenata. No efikasna zaštita ne primjenjuje samo jedno rješenje, već kombinaciju spomenutih metoda zaštite.

2. ZAŠTITA I SIGURNOSTI U INFORMACIJSKOM SUSTAVU

Sigurnost računala (en. computer security) je područje računarstva koje se bavi nadzorom, praćenjem i sprečavanjem raznih opasnosti koje mogu prouzročiti nestabilnost, prestanak rada ili bilo kakvu vrstu štete na softveru, pa i hardveru računala[1]. Pod pretpostavkom da je računalo sigurno od svih opasnosti (virusi, crvi i razne vrste infekcija), korisnik bi trebao biti u mogućnosti napraviti baš ono što hoće na računalu, što nije slučaj ako je računalo napadnuto od strane nekog štetnog programa koji je napisan sa namjerom da naškodi radu računala.

U načine i alate za stvaranje sigurnih sustava ubrajamo Backup, Anti-virusni softver, Firewall, Anti- spyware, sigurnosne zakrpe, sigurne šifre, preventive, dobra sigurnosna praksa i ostale vrste zaštite kao što su kontrola pristupa, enkripcija i uočavanje upada[2].

Kada govorimo o zaštiti računalnih sustava i podataka, stiče se dojam, pogotovo kod korisnika osobnih (kućnih) računala kako je ovaj aspekt zaštite gurnut u stranu i više se vodi računa o drugim područjima zaštite. Velike i ozbiljne kompanije ipak nisu zapostavile ni ovaj dio zaštite, koji neki nazivaju i tehnička zaštita, te se ovaj vid informatičke sigurnosti razvijao paralelno sa razvojem informatike i računarstva.

Kroz razvoj informacijskih sustava vidi se da je značajno povećanje rizika sigurnosti računalnih sustava prouzrokovala pojava umreženih računalnih sustava odnosno pojava Interneta.

Sve dok su računalni sustavi bili „izolirani“ od drugih računala osnovna mjera zaštite bila je autentifikacija tj. osiguravanje da računalu a time i podacima imaju pristup samo određene osobe. Što je više osoba koristilo računalni sustav to je i njegova zaštita postala kompleksnija, a sigurnost je opadala. Autentifikacija se uglavnom ostvarivala lozinkama i drugim sigurosnim informacijama. Suvremeni sustavi pored toga sve češće koriste i biometrijske informacije za autentifikaciju, kao što je otisak prsta, skeniranje irisa oka, prepoznavanje glasa i druge inovativne metode.

Pristup umreženim sustavima ima mnoge prednosti ali pored toga omogućava i drugim osobama da imaju pristup našem računalu. Na taj način potencijalne opasnosti postaju sve brojnije. Pojava Interneta 1983. omogućila je razvoj raznih vrsta zloćudnog softvera (malware) kao što su virusi, crvi, trojanski konji, rootkit, spyware i adware i

[1] https://bs.wikipedia.org/wiki/Sigurnost_racunara - pristup ostvaren 24.08.2017.
[2] Baþa, M. Uvod u računalnu sigurnost. Zagreb : Narodne novine d.d., 2004

drugi. Da bi se računalni sustav mogao zaštititi moraju se prvo shvatiti osnovni principi rada ovih zloćudnih aplikacija.

Sa aspekta sigurnosti, u današnjem svijetu postoje tri glavne kategorije u koje možemo razvrstati poslovne informacijske sustave čije su računalne konfiguracije vrlo različite, te se u jednom poslovnom sustavu mogu koristiti:

1. Velika računala za centralnu obradu podataka
2. Manja računala za decentralizirano prikupljanje i obradu podataka
3. Osobna računala za automatizaciju uredskog poslovanja

Što se tiče samog aspekta sigurnosti, važno je identificirati rizike koji mogu predstavljati sigurnosni problem za jedan računalni sustav, a među najčešće rizike spadaju[3]:

1. Računalni kriminal
2. Sabotaža
3. Špijunaža
4. Nedovoljna čistoća u prostorijama u kojima su smještena računala
5. Slučajno ili namjerno kvarenje računalnih sustava
6. Razne vremenske nepogode
7. Neovlašteno korištenje, modificiranje i brisanje informacija

U svakoj kompaniji, prije dizajniranja samog sustava, odnosno, u sklopu projektiranja informacijskog sustava, potrebno je obraditi i aspekt zaštite i sigurnog korištenja informacijskog sustava. U velikim kompanijama, državnim institucijama i agencijama u proces zaštite i sigurnosti informacijskih sustava, podataka, te rada sa istim ulaže se mnogo napora i novca. Prije samog definiranja aspekta fizičke zaštite, potrebno je obraditi pojam računalnog kriminala. U svijetu postoje razna mišljenja što u stvari predstavlja računalni kriminal, te se donose zakonske odredbe koji će isti tretirati i primjereno sankcionirati. Gledajući područje Republike Hrvatske, oblici kompjuterskog kriminala između ostalog su[4]:

[3] http://www.budimo-sigurni.hr – pristup ostvaren 29.08.2017.
[4] Dokumenti sa Microsoftove konferencije o sigurnosti informacijskih sustava – „Microsoft Security Days -2008“

1. Krađa računarske opreme
2. Krađa računalnog vremena
3. Krađa softvera radi neovlaštenog korištenja i prodaje
4. Upadanja u računalnu i komunikacijsku mrežu radi kopiranja i mijenjanja podataka
5. Kopiranje podataka iz računalnih centara bežičnim putem
6. Pronevjere zaposlenog osoblja u poduzeću
7. Neovlašten pristup računalima, te mjestima za pohranu i obradu podataka
8. Uništavanje i oštećenje računalne i mrežne opreme

Ovo je samo dio oblika računalnog kriminala koji se može pojaviti. Cilj zaštite računalnih sustava i podataka je očuvanje njihove povjerljivosti, integriteta i dostupnosti. Povjerljivost znači da su informacije dostupne samo onim osobama kojima i trebaju biti dostupne. Integritet osigurava promjenu informacija samo od strane ovlaštenih osoba i to samo na ovlašten način. Dostupnost osigurava da informacije uvijek budu dostupne ovlaštenim subjektima. Uobičajeno se sigurnost informacijskih sustava realizira kroz tri procesa i to dokazivanje identiteta, ovlasti i evidentiranje. Da bi pristupili informacijama osobe dokazuju svoj identitet na osnovu kojeg dobivaju odgovarajuće ovlasti, prava pristupa, pri čemu se sve akcije subjekata evidentiraju. Da bi se zaštitili od računalnog kriminala, imamo mjere zaštite koje se dijele na:

1. Organizacijske
2. Tehničke
3. Komunikacijske

3.1. Tehnička i fizička zaštita

Gledajući tehničke mjere, u koje spada i fizička zaštita, one obuhvaćaju zaštitu hardvera, softvera, prijenosa i obrade podataka. Kod poslova fizičke zaštite općenito, potrebno je razlikovati fizički sigurnosni događaj što predstavlja sigurnosni događaj ili pojava koja utječe na sigurnost ljudi ili imovinu organizacije. Primjeri fizičkih sigurnosnih događaja su[5]:

[5] Dokumenti sa Microsoftove konferencije o sigurnosti informacijskih sustava – „Microsoft Security Days -2008“

- požar,
- prirodne nesreće (potresi, uragani i sl.),
- nedostupnost objekta odnosno neprikladnost za uporabu,
- poremećaj u radu kritične infrastrukture (električna energija i sl.),
- neposredno fizičko ugrožavanje ljudi itd.
- Incident kao pojedinačni, neočekivani i nepoželjan događaj (ili više takvih povezanih događaja), prilikom kojeg postoji velika mogućnost za prekid ili ugrožavanje rada informacijskog sustava.

Fizička zaštita treba osigurati zaštitu od sljedećih neželjenih događaja i incidenata[6]:

1. Neispravnih instalacija
2. Neovlaštenog pristupa računalima i podacima
3. Fizičkog uništavanja računala i računalne opreme
4. Požara
5. Poplava
6. Zagađene okoline
7. Štetnih zračenja
8. Neurednog napajanja električnom energijom
9. Nepovoljnih klimatskih i temperaturnih uvjeta
10. Elementarnih nepogoda

Ove mjere zaštite se mogu realizirati na više načina, ovisno o visini raspoloživog proračuna za sigurnost, shvaćanja pojma sigurnosti i važnosti podataka koje treba zaštititi.

2.1.1. Video nadzor

Nešto što je do nedavno bilo rezervirano samo za bogate kompanije, danas je rašireno čak i po domaćinstvima. Video nadzor kao element fizičke zaštite je vrlo bitna i neizostavna karika jer pojavom video nadzora imamo mogućnost prikaza „live“ slike sa više sigurnosno zanimljivih lokacija, u bilo koje vrijeme i sa bilo kojeg mjesta gdje je

[6] Dokumenti sa Microsoftove konferencije o sigurnosti informacijskih sustava – „Microsoft Security Days -2008“

instalirana oprema za nadzor. Obično se pri planiranju postavlja jedan takozvani sigurnosni centar gdje su smješteni monitori (u zadnje vrijeme samo jedan) na kojima se prikazuje slika koju snima kamera u sustavu video nadzora. Prednosti ovog sustava su cijena, koja svakim danom sve više pada, fleksibilnost, jednostavno proširenje sustava kao i to što tehnologija video nadzora predstavlja tehnologiju budućnosti. Kraće vrijeme instalacije i mogućnost instalacije kamera za nadzor na praktično svako mjesto doprinjelo popularizaciju ovog sustava zaštite.

Slika 1. *Video nadzor*

Izvor: https://marinelama6.files.wordpress.com/2013/02/video_nadzor.jpg - pristup ostvaren 15.09.2017.

Sa razvojem tehnologija, dolazi do opadanja cijene ovih uređaja a isto tako dolazi do lakšeg i fleksibilnijeg održavanja. Što se tiče primjena ovog sustava fizičke zaštite, moguće je isti koristiti i za sam nadzor radnika, odnosno radnog procesa unutar poduzeća čemu se u zadnje vrijeme masovno pribjegava. Pogodnost ovog sustava je u tome što se podaci dobiveni sa kamera digitalno zapisuju i pohranjuju pa ih je moguće i naknadno pregledati Video nadzorom, kad su u pitanju informacijski sustavi, obično se pokrivaju prostorije u kojima se nalaze serveri, prostorije kojima se prilazi do serverskih

prostorija, kao i ulazi i izlazi u objekt gdje se vrši obrada podataka, te samo mjesto obrade podataka.[7]

3.1.2. Fizička zaštita

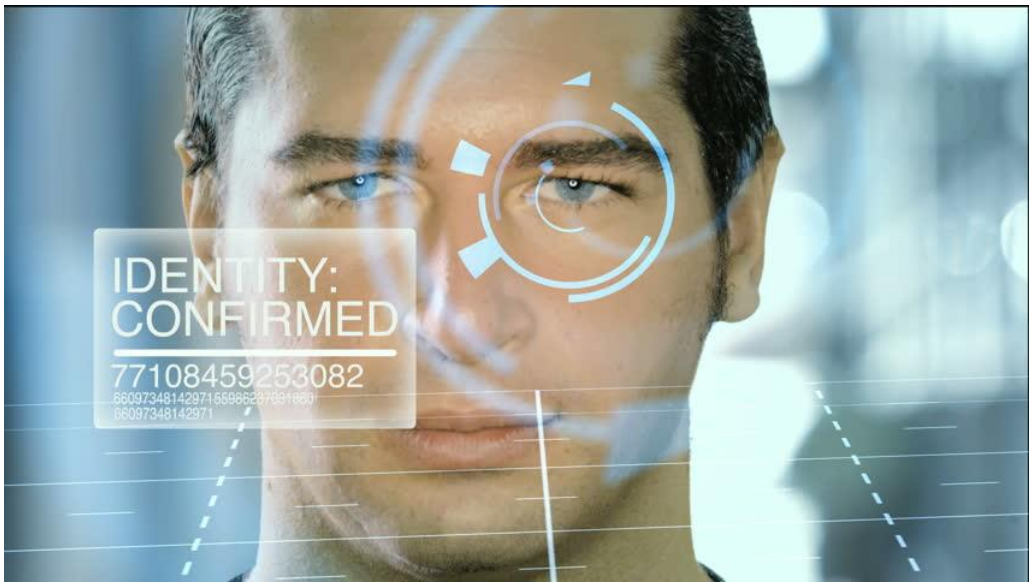
Pod poslovima tjelesne zaštite podrazumijevamo onemogućavanje neovlaštenih pristupa prostorijama za obradu računalnih podataka, mjestima gdje se čuvaju podaci, sprečavanje uništenja, oštećenja i krađe računalne i mrežne opreme. Ovo se obično regulira preko posebne zaštitarske tvrtke.

3.1.3. Ograničavanje pristupa

Jedna od bitnih karika u lancu sustava sigurnosti računalnog sustava predstavlja ograničavanje pristupa računalima i podacima. Pod pojmom fizičkog ograničavanja pristupa podrazumijeva se svako sprečavanje neovlaštenog pristupa računalima, mrežnoj opremi i podacima. Kontrola i ograničavanje pristupa mogu se izvesti na mnogo načina, a kombinacije u današnjem svijetu su bezbrojne. Jedan od najprimitivnijih i najrasprostrajnijih oblika ograničavanja pristupa je članstvo, odnosno pripadnost određenoj organizaciji, poduzeću, udruženju i drugo. Sve osobe koje su članovi, odnosno koji su registrirani, imaju pristup određenim podacima i informacijskim sustavima ovisno kako je to regulirano unutarnjom organizacijom same poslovne jedinice, tvrtke, organizacije. Često se stavljaju različiti oblici pripadnosti, pa tako na primjer, u jednoj obavještajnoj agenciji, nivo 1 znači pristup svim informacijama, dok u drugoj nivo 1 znači pristup samo osnovnim informacijama. Znači, mogućnosti organizacije u ograničavanju pristupa su bezbrojne. U današnje vrijeme, vrlo popularni sustavi za ograničavanje pristupa su preko elektronskih kartica ili skenera lica, prsta, mrežnice oka i drugog[8].

[7] Tisab Inženjerig - projektiranje sustava protuprovalne zaštite kuća, stanova, banaka i poslovnih objekata str. 8

[8] Narcis Behlilović , Pamela Begović, Saša Mrdović - Različiti aspekti zaštite pristupa digitalizovanoj kulturnoj baštini, Elektrotehnički fakultet u Sarajevu



Slika 2. *Identifikacija putem mrežnice oka*

Izvor: http://ak8.picdn.net/shutterstock/videos/12637988/thumb/1.jpg - pristup ostvaren 15.09.2017.

3.1.4. Protupožarna zaštita

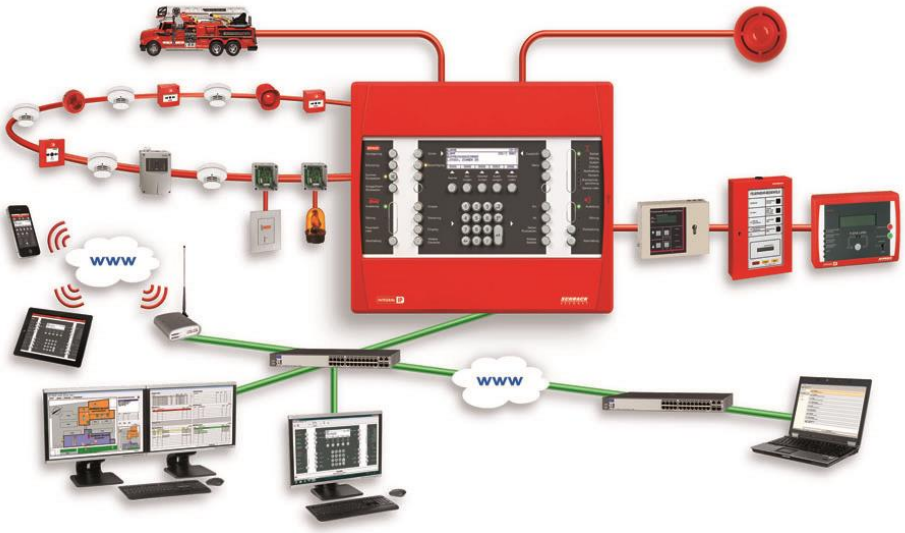
Jedna od ključnih elementarnih nepogoda koje pogađaju informacijske sustave je vatra, odnosno požar. Pošto je za rad informacijskih sustava potrebna električna energija, opasnost od pojave požara samim tim se povećava. Kao i kod sustava za ograničavanje pristupa tako i kod sustava protupožarne zaštite postoje mnogobrojne varijante. Neke od osnovnih komponenti svakog protupožarnog sustava su :

- senzori za detekciju požara,
- instalacije za gašenje požara,
- uređaji za dojavu požara
- centralni procesor za obradu signala koji dolaze sa senzora.

Svi protupožarni sustavi u svrhu što veće efikasnosti trebaju ispunjavati sljedeće kriterije[9]:

- Pouzdanost u radu, te pouzdanost i preciznost detekcije ;
- Imunost na lažne alarme;
- Otpornost na surova okruženja i vanjske utjecaje;
- Mogućnost brzog proširenja sustava

[9] http://www.zastita.hr – pristup ostvaren 02.09.2017.



Slika 3. *Protupožarni sustav*

Izvor: https://www.schrack-seconet.com/export/sites/seconet/_data/product/productArticlesImages/BX-Grafik_DE_weiss.jpg - pristup ostvaren 15.09.2017.

U današnje vrijeme, većina protupožarnih sustava ima gore nabrojane karakteristike. Praksa je pokazala da se požar na instalacijama i računalima najbrže gasi prahom, te prekidom dovoda kisika u prostoriju sa računalima. Ovo zadnje se provodi posebno u prostorijama gdje se nalaze serveri, koji su u prostorijama sa posebnom ventilacijom. Zbog zagrijavanja komponenti računalnih sustava prilikom rada, prostorije u kojima se nalaze velika računala (serveri) se klimatiziraju. Uz ovu klimatizaciju uvodi se i kontrola dovoda kisika u prostoriju, da bi se u slučaju požara dopremanje istog u prostoriju moglo zaustaviti. Isto tako, za zaštitu ljudi i opreme, u prostoriji gdje se nalazi centralni kompjuter za obradu potrebno je postaviti antistatičnu podnu oblogu, koja je sačinjena od antistatičnih materijala koji upijaju elektricitet.

Slika 4. *Klimatizirana prostorija sa serverima*

Izvor: http://www.hanstockaircon.co.uk/wp-content/uploads/2017/01/server-cooling.jpg pristup ostvaren 15.09.2017.

3.1.5. Osiguranje napajanja električnom energijom

Jedan od problema koji se javljaju prilikom korištenja računala i računalne opreme je osiguranje konstantnog i adekvatnog napajanja električnom energijom. Poznato je da računala troše velike količine električne energije pa je neophodno osigurati dovoljne količine iste za njihov neometan i neprekidan rad. U samoj električnoj mreži dolazi do mnogobrojnih variranja napona, što predstavlja opasnost za rad računala. Jedna od mjera zaštite koja je danas najzastupljenija je UPS.

Slika 5.*UPS*

Izvor: http://www.storagereview.com/images/StorageReview-Eaton-9PX-UPS.jpg - pristup ostvaren 15.09.2017.

UPS je skraćenica od Uninterrubtible Power Supply što znači nesmetano napajanje električnom energijom[10]. Izvodi se na principu akumulatora, u kojem se akumulira električna energija, a prilikom normalnog napajanja UPS radi kao regulator napona. U slučaju prekida u napajanju električnom energijom, baterije iz UPS-a napajaju računalnu opremu određeno vrijeme koje je potrebno da se pokrenu alternativni izvori energije, čije je zadatak da napajaju sustav električnom energijom u kritičnom periodu.

2.2. Antivirusni programi

Osnovni oblik obrane od virusa je zaštita računala. Riječ je o dosta složenom postupku koji osim primjene odgovarajućih programa od korisnika zahtijeva i oprezno ponašanje. Osnovna zaštita od virusa na samom računalu provodi se upotrebom programa za borbu protiv virusa[11]. Zajedničkim imenom ovakvi programi se nazivaju antivirusni programi. Zamisao je da se na računalo postavi računalni program koji će stalno provjeravati sve zapise koji dospijevaju na računalo. Program u sebi ima podatke koji mu omogućavaju prepoznavanje različitih virusa. Zbog toga će u trenutku kad naiđe na zapis zaražen virusom spriječiti aktiviranje tog zapisa i podići uzbunu. Jednostavno rečeno, na ekranu će se pojaviti prozor s upozorenjem da je određeni zapis zaražen virusom ili nekom drugom vrstom zloćudnog softvera. Pri instalaciji program

[10] Petrić, D. Internet uzduž i poprijeko. Zagreb: BUG & SysPrint, Kompletan vodić, 2002
[11] http://www.virusi.net/ieNews/clanak.asp?ID=17 – pristup ostvaren 02.09.2017.

od korisnika zahtjeva da odredi stupanj zaštite. Najniži stupanj zaštite ne sadrži nikakvu automatiku već korisnik može samostalno pokrenuti provjeru u slučaju kad na računalo uonosi neke podatke. Ovakav način rada je izuzetno nesiguran jer korisnik može jednostavno zaboraviti provjeru. Najviši stupanj zaštite zapravo uključuje stalnu provjeru podataka koji se koriste, nadzor nad svim pristiglim elektroničkim porukama i periodičnu provjeru svih podataka na računalu. Ovakav oblik zaštite bez sumnje troši nešto više računalnih resursa. Zbog toga neki autori odbacuju ovakvo rješenje unatoč njegovim očiglednim prednostima. Vrlo je važno naglasiti da je bilo koji program za zaštitu od virusa u stanju prepoznati samo viruse koji su postojali u trenutku njegovog pisanja. Pojavi li se novi virus samo dan nakon što je program izašao, taj je virus programu nepoznat, pa prema tome ne može prepoznati virus, odnosno ne može spriječiti njegovo širenje, ali može upozoriti na moguću opasnost.

Pod antivirusnim programima podrazumijevamo softverske pakete sposobne da detektiraju, izdvoje i (ili) eliminiraju viruse[12]. Svi antivirusni programi sastoje se iz više cjelina. Jedan njegov dio "Monitor" je rezidentan u memoriji i osigurava neprestalnu zaštitu od virusa, dok drugi dio "Scan" omogućava skeniranje cijelog sustava. Anti-virusi su danas neophodan dio softvera koji svatko treba imati instaliran na svom računalu. Ovi programi uključuju različite načine nadgledanja i zaštite računala od malicioznog koda.

Najčešće se radi o zaštiti u realnom vremenu i skeniranju na zahtjev korisnika, dok moderne verzije ovih programa nude razne druge oblike zaštite od virusa koji se šire putem Interneta. Postoji dosta kompanija koje razvijaju i nude ove programe. One nude dopunu antivirusnih definicija svakodnevno. Dosadašnja praksa bazirala se na svakodnevnom osvježavanju baze. Broj danas poznatih virusa je nekoliko desetaka tisuća, s time da se opasnim smatra nekoliko stotina. Kvalitetna zaštita svodi se na opreznost, upotrebu dobrih antivirusnih programa, te redovno osvježavanje virusnih definicija.

[12] https://hr.wikipedia.org/wiki/Antivirusni_program - pristup ostvaren 02.09.2017.

Slika 6. *ESET NOD32 Antivirusni paket*

Izvor: https://images-na.ssl-images-amazon.com/images/I/61cOuBYzgQL._SX425_.jpg pristup ostvaren 16.09.2017

U ovom pristupu, antivirus program provjera datoteku uspoređujući je sa rječnikom poznatih virusa koje su tvorci antivirusnih programa identificirali. Ako dio koda datoteke odgovara virusnoj identifikaciji u riječi takav antivirusni program može poduzeti jednu od sljedećih akcija:

1. pokušati popraviti datoteku uklanjajući virus unutar datoteke
2. staviti datoteku u karantenu (tako da je datoteka nedostupna drugim programima i virus se ne može dalje širiti)
3. obrisati inficiranu datoteku

Najpopularniji i najpoznatiji antivirusni programi su:

- ESET NOD32
- Symantec
- Norton
- Sophos
- Kaspersky
- AVG
- Avira
- Panda
- McAfee
-

2.3. Vatrozid

Vatrozid ili Firewall je sigurnosni element smješten između neke lokalne mreže i javne mreže (Interneta), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautoriziranih korisnika (blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika)[13]. Nije nužno da svi korisnici u LAN-u (Local Area Network) imaju jednaka prava pristupa Internet mreži. Postavljanjem Firewall uređaja između dva ili više mrežnih segmenata može se kontrolirati i prava pristupa pojedinih korisnika pojedinim dijelovima mreže. U takvom slučaju Firewall je dizajniran da dopušta pristup valjanim zahtjevima, a blokira sve ostale.

Firewall ujedno predstavlja idealno rješenje za kreiranje Virtualne Privatne mreže (VPN) jer stvarajući virtualni tunel kroz koji putuju kriptirani podaci (omogućuje sigurnu razmjenu osjetljivih podataka među dislociranim korisnici). Firewall je servis koji se tipično sastoji od firewall uređaja i Policy-a (pravilnika o zaštiti), koji omogućuje korisniku filtriranje određenih tipova mrežnog prometa sa ciljem povećanja sigurnosti i pruža određeni nivo zaštite od provale.

Slika 7.*Hardverski vatrozid*

Izvor: https://getvoip.com/uploads/hardware-firewall-700x304.jpg - pristup ostvaren 16.09.2017.

Osnovna namjena Firewall-a je da spriječi neautorizirani pristup sa jedne mreže na drugu. U suštini, ovo znači zaštitu lokalne mreže od Internet-a. Ako vaš sustav raspolaže Firewall-om, to znači da je odluka o tome šta je dozvoljeno, a šta nije već

[13] Petrić, D. Internet uzduž i poprijeko. Zagreb: BUG & SysPrint, Kompletan vodić, 2002.

donijeta. Ove odluke su u direktnoj vezi sa politikom sigurnosti vašeg informacijskog sustava. Pri planiranju ponude informacijskih servisa, politika sigurnosti određuje opcije konfiguracije servisa.

Osnova rada Firewall-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smijera. Za Firewall je tipičan i kompromis između sigurnosti i lake upotrebe. Stav da "sve što nije dozvoljeno je zabranjeno" zahtijeva da se svaki novi servis individualno omogućava.

Firewall je odgovoran za više važnih stvari unutar informacijskog sustava:

1. Mora implementirati politiku sigurnosti. Ako određeno svojstvo nije dozvoljeno, Firewall mora onemogućiti rad u tom smislu.
2. Firewall treba bilježiti sumnjive događaje.
3. Firewall treba upozoriti administratora na pokušaje proboja i kompromitiranja politike sigurnosti.
4. U nekim slučajevima Firewall može da osigurati statistiku korištenja.

Firewall može biti softverski ili hardverski :

- Softverski firewall omogućava zaštitu jednog računala osim u slučaju kada je isto računalo predodređeno za zaštitu čitave mreže.
- Hardverski firewall omogućuje zaštitu čitave mreže ili određenog broja računala. Za ispravan rad firewall-a, potrebno je precizno odrediti niz pravila koja kakav mrežni promet je dopušten.

2.4. Zaštita podataka šifriranjem

Sigurnost računalnih sustava postaje sve važnija jer sve više korisnika na sve više načina koristi sve više informacija u računalnom svijetu. U takvom sustavu postoji i sve veća opasnost od neovlaštene upotrebe informacija, podmetanja krivih informacija ili uništavanja informacija. U računalnim sustavima informacije se prenose raznovrsnim otvorenim i nesigurnim komunikacijskim putevima. Pristup do tih puteva ne može se fizički zaštititi pa napadač može narušiti sigurnost sustava. Zbog toga zaštitni komunikacijski mehanizmi nad nesigurnim komunikacijskim kanalom postaju najvažniji oblik ostvarenja sigurnosti. Pokazuje se da je najdjelotvornija zaštita poruka njihovo kriptiranje.

Kriptografija je znanost koja se bavi transformacijom informacija u formu koja će biti čitljiva samo onima kojima je informacija namijenjena, dok će za ostale biti neupotrebljiva. Usporedno sa razvojem kriptografije razvila se i znanost pod nazivom kriptoanaliza , kojoj je cilj da analizom kriptirane poruke odgonetne njen sadržaj. Kriptoanaliza se bavi razbijanjem šifri, odnosno otkrivanjem sadržaja otvorenog teksta na osnovu šifri a bez poznavanja ključa. U širem smislu, kriptoanaliza obuhvaća i proučavanje slabosti kriptografskih elemenata.

Osnovni zadatak kriptografije je omogućiti dvjema osobama (pošiljatelju i primatelju - u kriptografskoj literaturi su za njih rezervirana imena Alice i Bob) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža, ...) na način da treća osoba (njihov protivnik - u literaturi se najčešće zove Eva ili Oskar), koja može nadzirati komunikacijski kanal, ne može razumjeti njihove poruke. Poruku koju pošiljatelj želi poslati primatelju zvat ćemo otvoreni tekst (engl. plaintext). Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak se naziva šifriranje, a dobiveni rezultat šifrirani tekst (engl. ciphertext) ili kriptogram. Nakon toga pošiljatelj pošalje šifrirani tekst preko nekog komunikacijskog kanala. Protivnik prisluškujući može doznati sadržaj šifri ali ne može odrediti otvoreni tekst. Za razliku od njega, primatelj koji zna ključ kojim je šifrirana poruka može dešifrirati šifrirani tekst i odrediti otvoreni tekst.

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 šifri i obratno. Funkcije se biraju iz određene obitelji funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo prostor ključeva . Kriptosustav se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifri ključeva.

3.4.1. Metode šifriranja

Povijesno najduže korištena metoda šifriranja je metoda olovke i papira. Primjer ove metode je supstitucija. Također su uz ovu metodu vezane kodne knjige koje su služile za standardno šifriranje jer su u njima bile fraze i riječi i tako se olakšalo šifriranje[14].

[14] Douglas R. Stinson, "Cryptography: Theory and practice", CRC Press, 1995

Primjer kodne knjige je nomenclator. Još jedna davno korištena metoda je metoda transpozicije. Ideja te metode je u pomicanju slova naprijed ili nazad za određen broj mjesta. Primjeri su caesar šifra i rot13. Općenito danas postoje dvije vrste metoda šifriranja. To su metoda simetričnog šifriranja i metoda asimetričnog šifriranja. Metoda simetričnog šifriranja je donedavno bila jedina poznata metoda. Metoda koristi jedinstveni ključ. Prednost je svakako njena jednostavnost i brzina, a od mana treba spomenuti problem sigurnosti, pogotovo u slučaju krađe ključa. Od 1976. i pojave javnog ključa možemo govoriti i o metodi asimetričnog šifriranja. Razlika je u tome što ova metoda koristi dva odvojena ključa – javni i tajni. Javni se koristi za šifriranje, a tajni za dešifriranje. Iz imena javni ključ jasno je da isti ne mora biti tajan. Prednost ove metode je svakako veća kvaliteta šifriranja koja omogućuje veću sigurnost i, što je često iznimno važno, tajnost. Mana je definitivno količina vremena koja je potrebna za svaki postupak dešifriranja.

Još jedna važna metoda šifriranja je jednosmjerno šifriranje. Njegova glavna osobina je ireverzibilnost tj. ne može se dobiti originalni sadržaj. Danas se koristi za potvrde, (digitalne) potpise, softver, ... Za još sofisticiranije metode šifriranja koristi se tzv. jako šifriranje. Ta kompleksnija metoda je u nekim državama zabranjena[15].

3.4.2. Moderna kriptografija

U modernoj kriptografiji još se uvijek koristi šifriranje simetričnim ključem. Primjer za to je IBM-ova DES šifra koju i danas koristi Unix, kao i njen prethodnik šifra Lucifer. Najčešći problem ove metode je i danas način prijenosa ključa. Postoje i varijante metode kod kojih su ključevi različiti ali se mogu jednostavno jedan iz drugoga izračunati. Dolazimo do paradoksa da bi najsigurnije bilo poslati ključ šifrirano i počinje vrtnja u krug. DES je javno dostupna i korištena metoda šifriranja od 1976. godine, iako se danas smatra nesigurnom, često je možemo naći u upotrebi (ATM, šifriranje e-mailova, kod pristupanja sustava s udaljenosti itd.) Oba spadaju u "blok" metode i jedan od razloga popularnosti je činjenica da su oba proglašena službenim metodama šifriranja od strane vlade S.A.D. Postoje brojne varijacije tih metoda pa tako i trostruki DES koji je bitno sigurniji.

[15] Douglas R. Stinson, “Cryptography: Theory and practice”, CRC Press, 1995

Također postoje metode šifiriranja koja su prilagođene šifriranju protoka podataka, kao npr. RC4. Kako nizovi podataka prolaze kroz program, mijenja se dio koji šifrira podatke, a način promjene se kontrolira ključem, a ponekad i samim podacima koji se šifriraju[16].

Jedna od čestih upotreba šifriranja u današnje doba je i kontrola pristupa (ustanovama, računalima, podatcima,...) ali i preračunavanja čitavih sadržaja u jedinstven broj izuzetno malom vjerojatnosti dvostrukih rješenja za različite sadržaje. Sličan način ali s drugom namjenom je MAC, odnosno šifriranje pristupne poruke, kada tajna, ključna lozinka daje šifrirani tekst koji se uspoređuje s spremljenim za kontrolu pristupa, odnosno vjerodostojnosti.

3.4.3. Javni ključevi

Glavi problem u simetričnom šifriranju je rukovođenje tajnim šiframa, ključevima koji su korišteni za šifriranje i dešifriranje poruke. Zbog toga se nakon objavljivanja rada koji su napisali Whitfield Diffie i Martin Hellman 1976. godine pojavilo šifriranje s javnim ključevima. Metoda je toliko promijenila rad s ključevima da ju David Kahn opisuje kao "najveći, revolucionarni napredak u kriptografiji od renesanse"[17].

Stvaranje javnog i privatnog ključa je povezano matematičkim postupkom, nakon čega se dobiveni tekst javnog ključa može slobodno podjeliti, ali se njime skriven tekst može otključati samo privatnim ključem. Godine 1978. Ronald Rivest, Adi Shamir i Len Adleman objavili su RSA algoritam. Napokon je 1997. godine obznanjeno kako je zapravo James H. Ellis u GCHQ, britanskoj obavještajnoj službi zapravo ranih 1970-ih izmislio asimetrično šifriranje javnim ključem te da su i Diffie-Hellman i RSA algoritam zapravo već izmislili Malcolm J. Williamson, odnosno Clifford Cocks.

Često korišteni primjeri su RSA algoritam, digitalni potpisi, VPN, SSL/TLS i program PGP, koji se također temelje na ovakvim metodama. Današnje metode bazirana su na problemima gdje se brzo i jednostavno pomoću računala tekst šifrira ali je rješenje "teško", u metematičom smislu. Dok se RSA na problemu faktorizacije prirodnih brojeva, DSA i Diffie-Hellman metode se oslanjanju na problem diskretnih logaritama.

[16] Douglas R. Stinson, “Cryptography: Theory and practice”, CRC Press, 1995
[17] Douglas R. Stinson, “Cryptography: Theory and practice”, CRC Press, 1995

Problemi moderne kriptografije su svakako sigurnost, ali i zakonska ograničenja u mnogim zemljama. Pitanje sigurnosti je goruće pitanje zbog sve veće pojave programa za razbijanje lozinki kao što su: Crack i John the Ripper. Drugi veliki problem su zakonska ograničenja. U SAD-u se recimo kriptografija smatra oružjem. Do 1999. u Francuskoj je bila znatno ograničena upotreba kriptografije. Od ostalih država sa strogim zakonskim ograničenjima upotrebe kriptografije prednjači Kina ispred Bjelorusije, Mongolije, Rusije, Pakistana, Tunisa i drugih.

3. VIRUSI I OSTALE ŠTETNE PRIJETNJE U INFORMACIJSKOM SUSTAVU

Zlonamjerni softver, zloćudni softver, štetni softver ili na engleskom malware je pojam koji označava softver koji radi štetu korisniku (pojam je nastao od riječi malicious i software što u doslovnom prijevodu znači "zloćudni" ili "zlonamjerni" softver)[18].

Radi se o računalnim programima koji se pokreću na računalnom sustavu bez stvarnog korisnikovog pristanka i imaju neku vrstu nepoželjnog učinka, kao što je oštećenje programa i podataka koji se nalaze na sustavu, širenje na druga računala, krađa podataka (osobito povjerljivih podataka kao što su lozinke i brojevi kreditnih kartica), omogućavanje neovlaštenog udaljenog pristupa na računalo, prikazivanje reklamnih poruka, masovno slanje neželjene elektroničke pošte (spama), sudjelovanje u napadima na druga računala putem mreže, i drugo.

Prema načinu širenja zloćudni programi mogu se podijeliti u više skupina: računalni virusi, crvi, trojanski konji. Prema načinu djelovanja i cilju zloćudne programe dijelimo na špijunske programe, oglašivačke programe, ucjenjivački softver (softver koji traži otkupninu) itd. Fizička šteta nastala djelovanjem štetnih programa nije česta, no, nažalost, ipak se može dogoditi.

3.1. Računalni virusi

Računalni virus je program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt. Kod je napisan s jasnom namjerom vlastitog razmnožavanja. Virus se pokušava proširiti na računala privijanjem na host program. Može oštetiti hardver, softver i podatke. Može se nalaziti i zaraziti bilo koji program, sektor za podizanje operativnog sustava, dokument koji podržava makronaredbe i to tako da promijeni sadržaj te datoteke te u nju kopira svoj kod. Računarski virus se obično sastoji od dva dijela:

- Prvi dio je samokopirajući kod koji omogućava razmnožavanje virusa
- Drugi dio je korisna informacija koja može biti bezopasna ili opasna .

[18] https://hr.wikipedia.org/wiki/Zloćudni_softver - pristup ostvaren 04.09.2017.

Vrste računalnih virusa:

- boot sektor virusi – napadaju Master boot sektor
- parazitski – zaraze izvršne datoteke dodavanjem svog sadržaja u strukturu programa
- svestrani virusi – napadaju boot sektore i izvršne programe
- virusi pratioci – stvaraju .com datoteku koristeći ime već postojećeg .exe programa i ugrađuju svoj kod u nju
- link virusi – u trenu inficiraju napadnuti računalni sustav, a mogu izazvati pravi kaos na disku
- makro virusi – imaju mogućnost da sami sebe kopiraju, brišu i mijenjaju dokumente[19]

3.2. Računalni crvi

Računalni crvi su računalni programi koji umnožavaju sami sebe. Pri tome koriste računalne mreže putem kojih se kopiraju na druga računala, a pretežno bez sudjelovanja čovjeka[20]. Za razliku od virusa, svojim djelovanjem ne moraju inficirati druge programe. Mogu stići i kao privitak u elektroničkoj pošti te im pristup računalu omogućavaju propusti u operativnim sustavima i aplikacijama. Crvi otežavaju rad mreže, a mogu oštetiti podatke i kompromitirati sigurnost računala. Vrste računalnih crva:

- Crv – može oštetiti podatke i kompromitirati sigurnost računala.
- Mailer i mass-mailer – sami se šalju elektroničkom poštom.
- Miješane prijetnje – kombiniraju karakteristike virusa, crva i trojanskih konja s propustima u softveru za svoje pokretanje, prijenos i širenje napada.

Crvi "šetaju" putem diskova ili mrežom, ali najviše e -mailom i putem chata. Na samo jednom računalu, opasnost od crva je u tome da se može umnožiti toliko puta da potpuno napuni disk i "uguši" sustav[21].

[19] Baþa, M. Uvod u računalnu sigurnost. Zagreb : Narodne novine d.d., 2004.

[20] https://hr.wikipedia.org/wiki/Zloćudni_softver - pristup ostvaren 07.09.2017.

[21] Petrić, D. Internet uzduž i poprijeko. Zagreb: BUG & SysPrint, Kompletan vodić, 2002

4.3. Trojanski konj

Trojanski konj je štetni program koji se predstavlja kao neki posve drugi program koji radi nešto korisno ili zanimljivo (npr. računalna igra). Za razliku od virusa ne može se sam replicirati (osim ako ga korisnik ne prekopira npr. na drugo računalo)[22]. Može izvoditi razne aktivnosti poput krađe korisničkih lozinki, brojeva kreditne kartice i drugih osjetljivih informacija koje potom šalje nekoj drugoj osobi ili može nepotrebno zauzimati resurse računala usporavajući ga na taj način.

Vrlo često moderniji trojanski konji pristupaju različitim internetskim stranicama kako bi preuzeli neku, obično inficiranu, datoteku ili više njih. Nakon preuzimanja ih pokreću te tako instaliraju dodatan štetni softver na zaraženom računalu. Mogu se također spajati na određene IRC kanale kako bi primali naredbe od zlonamjernog korisnika.

U posebnu vrstu trojanskih konja spada i backdoor koji omogućuje neovlaštenoj osobi pristup zaraženom računalu, najčešće s administratorskim pravima. Neovlaštena osoba može tako pristupati datotekama, pa čak ih brisati ili dodavati.

4.4.Špijunski softver

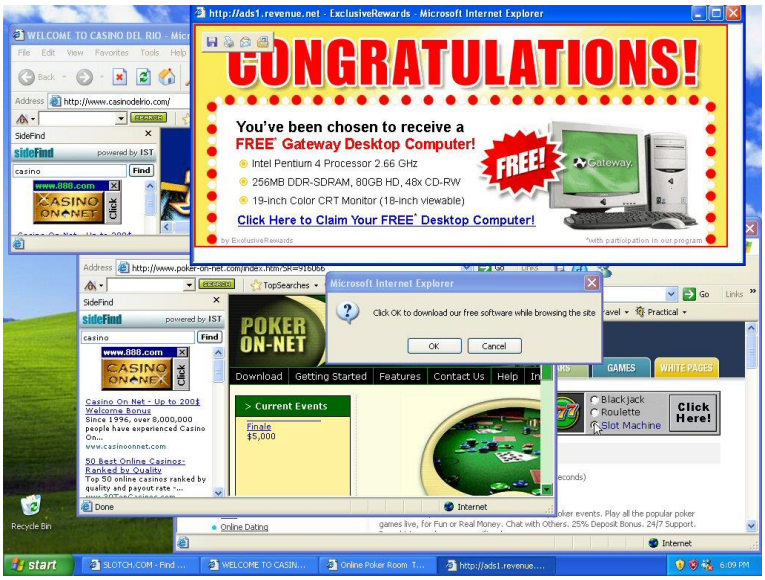
Špijunski softver (engleski naziv spyware) je štetni program koji sakuplja informacije o korisnikovom korištenju računala i preuzima kontrolu nad njegovim računalom. Korisnik često ne zna za njegovu prisutnost, a obično se ne replicira. Špijunski softver može, osim praćenja kako korisnik koristi svoje računalo, također i prikupljati osobne informacije te mijenjati postavke računala (često dodavanjem raznih ključeva u registarsku bazu - registry - Windowsa).

Simptomi koji mogu ukazivati na prisutnost špijunskog softvera su sporija internetska veza, promijenjena početna stranica internetskog preglednika i/ili gubitak funkcionalnosti nekih programa.

[22] https://hr.wikipedia.org/wiki/Zloćudni_softver - pristup ostvaren 07.09.2017.

4.5.Oglašivački softver

Oglašivački softver (engleski naziv adware - advertising-supported software) prikazuje korisniku oglase čak i kad trenutno nije spojen na Internet (drugim riječima, nije online), a može se instalirati zajedno s određenim aplikacijama[23] (npr. s Kaaza peer-2-peer programom). Narušava privatnost korisnika, poput špijunskog softvera. Neki od poznatijih primjera oglašivačkog softvera su Zwinky, ErrorSafe, Gator i BonziBUDDY.



Slika 8.*Oglašivački software*

Izvor: http://www.pcpitstop.com/images/spycheck/stormbig.jpg - pristup ostvaren 17.09.2017.

4.6.Keylogger

Keylogger (dolazi od engleskih riječi key i logger) je štetni program kojem je cilj praćenje korisnikovih unosa preko tipkovnice[24]. Pojedini bezopasni, legitimni programi koriste neke njegove funkcije za pozivanje specijalnih programskih funkcija (hotkeys). Povremeno keylogger namjerno instalira neka osoba na računalo ili više računala kako bi mogla tajno pratiti druge korisnike (npr. roditelji kako bi pratili kako djeca koriste

[23] https://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver - pristup ostvaren 07.09.2017.
[24] https://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver - pristup otvaren 07.09.2017.

računalo dok su roditelji, primjerice, na poslu). Osim te osnovne funkcije keylogger može s vremena na vrijeme (ili na svaki korisnikov klik miša) uzimati snimak ekrana tako da se na njemu može vidjeti, između ostaloga, s kojim programima korisnik trenutno radi ili gdje surfa na Internetu.
Ponekad je nevidljiv u Upravitelju zadataka (Task manager) koji prikazuje procese koji se trenutno izvode na računalu, kako bi spriječio ili otežao mogućnost otkrivanja od strane korisnika. Informacije koje keylogger prikupi u većini slučajeva šalju se zlonamjernoj osobi.

4.7.Ucjenjivački softver

Ucjenjivački softver ili rensomver (engl. ransomware) je vrsta štetnog softvera koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja[25]. Neki oblici ransomwarea kriptiraju datoteke, dok druge jednostavno zaključavaju sustav te prikazuju poruku koja korisnika nagovara na plaćanje otkupnine.

4.8. Hakerski upadi

Haker [izvorni prijevod s njemačkog jezika - netko tko radi namještaj sa sjekirom]. Termin „haker“ ima različito značenje među računalnim programerima[26]. Objektivno mišljenje u društvu jest da je haker negativna osoba. Mediji pokušavaju hakere opisati kao kriminalce ili bar kao osobe koje obožavaju nanijeti što više štete drugim osobama. Među programerima termin „haker“ se više upotrebljiva kao znak poštovanja prema drugom programeru, a ne kao uvreda.
Slavni programerski leksikon poznat kao „The Jargon File“ definira riječ „haker“ kao[27]:

[25] https://hr.wikipedia.org/wiki/Zloćudni_softver - pristup ostvaren 07.09.2017.
[26] Marin Perko - HAKERI, GOSPODARI INTERNETA - diplomski rad, Sveučilište u Zagrebu, 2008 god
[27] Marin Perko - HAKERI, GOSPODARI INTERNETA - diplomski rad, Sveučilište u Zagrebu, 2008 god

1. Osoba koja uživa istraživati detalje računalnih programa i traži način da poveća učinkovitost sustava, za razliku od ostalih korisnika koji uče i koriste samo osnove programa

2. Osoba koja programira s posebnim entuzijazmom ili osoba koja više uživa u programiranju nego o raspravljanu o istom

3. Osoba koja cijeni vrijednosti pravog „hacka“

4. Osoba koja brzo programira

5. Osoba koja je stručnjak za neki korisnički program ili provodi puno vremena koristeći ga (na primjer Unix hacker)

White hat hackers (bijeli šeširi)

Poznati su kao „dobri“ hakeri, uvijek koriste svoje znanje za dobrobit računalnog sustava. Iako „razbijaju“ računalne sustave to rade kako bi oni bili još više optimizirani i bolji. Surađuju sa proizvođačima programa te im ukazuju na nedostatke njihovih programa. Obično završe kao vrlo dobro plaćeni mrežni administratori, programeri i sigurnosni savjetnici.

Gray hat hackers (sivi šeširi)

Oni su svojevrsni hibrid white i black hat hakera. Ponekad, iz zabave, probiju i naprave pomutnju u računalnom sustavu nekom neutralnom korisniku. Iako oni misle da je ovakva vrsta aktivnosti bezazlena, posljedice toga što rade ih mogu odvest i i u zatvor.

Black hat hackers (crni šeširi)

Ovi hakeri su glavna prijetnja računalnim sustavima. Neki ih zovu i krekeri (crackers). Oni šalju i programiraju viruse, uništavaju podatke, napadaju Internet stranice i upadaju u tuđa računala. Pored toga black hats se bore protiv white hats-a, osnovni cilj im je biti najbolji među „najgorima“. Često su povezani s kriminalnim podzemljem, te često nelegalnim putem stiču novac.

Slika 9. H*aker*

Izvor: https://www.vecernji.hr/media/img/08/4f/11170d211ef23bf6d1a1.jpeg - pristup ostvaren 17.09.2017

Hakerski napadi i alati

Hakeri koriste trikove da pronađu prečac za nedopušteni ulaz u računalni sustav. Mogu koristiti ovaj ulaz za ilegalne ili destruktivne svrhe ili jednostavno mogu testirati vlastitu vještinu da vide jesu li sposobni za takav ulaz u sustav. Većini hakera je glavni motiv napada znatiželja i višak slobodnog vremena, pa je velika vjerojatnost da će haker u jednom trenutku, nakon bezbrojnih pokušaja, pronaći naprednu metodu napada i ući i u najbolje čuvani sustav. Ostali motivi su psihološka potreba, želja za učenjem, znatiželja, osveta, eksperimentiranje, nepovjerenje u druge osobe, samopriznanje, želja da nekoga pobjede ili zabava.

U osnovi, napadi su hakerske akcije koje su usmjerene na ugrožavanje sigurnosti informacija, računalnih sustava i mreža. Postoje različite vrste napada, ali se oni generalno mogu podijeliti u četiri osnovne kategorije:[28]

1) Presijecanje ili prekidanje (interruption) predstavlja napad na raspoloživost (availability). Presijecanjem se prekida tok informacija, tj. onemogućava se pružanje neke usluge ili funkcioniranje nekog sustava.

2) Presretanje (interception) predstavlja napad na povjerljivost (confidentiality). Presretanje može biti u praksi provedeno kao prisluškivanje prometa, nadziranje njegovog intenziteta, uvid u osjetljive informacije ili slično. Kao pasivni napad, teško se

[28] Marin Perko - HAKERI, GOSPODARI INTERNETA - diplomski rad, Sveučilište u Zagrebu, 2008 god

otkriva jer ne mijenja podatke, ne utječe na unutrašnje funkcioniranje sustava. Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.

3) Izmjena (modification) predstavlja napad na integritet (integrity). Po svojoj prirodi, to je aktivan napad. Ukoliko djeluje na prijenosnom putu, može se, na primjer, dogoditi napad „čovjek u sredini“ (man in the middle). Napad se može obaviti i unutar nekog računalnog sustava. U tom slučaju radi se o izmjeni podataka, pristupnih prava, načina funkcioniranja programa ili sustava i slično. Iako mijenja podatke i sustav, često ostaje neprimijećen izvjesno vrijeme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.

4) Proizvodnja (fabrication), predstavlja napad na autentičnost (authenticity). Napadač izvodi ovakav aktivni napad tako što generira lažne podatke, lažni promet ili izdaje neovlaštene naredbe. Vrlo često se koristi i lažno predstavljanje korisnika, usluge, poslužiteljskog računala, Web strane ili nekog drugog dijela sustava.

Hakerska skupina Anonymous

Anonymous - naziv je za internetski fenomen koji je nastao 2003. godine. Rabe ga različite skupine i pojedinci unutar cyber kulture s ciljem provođenja raznih akcija i publikacija pod tim nazivom - sa ili bez međusobnih konzultacija[29].

U početku se je pojavio kao zabavni pokret 4chana, a od 2008. Anonymousi se zalažu političkim prosvjedima za slobode govora, neovisnost Interneta i protiv različitih organizacija uključujući razne vladine ustanove, globalne korporacije i društva za zaštitu autorskih prava.

Sudionici su u početku djelovali samo na internetu, a u međuvremenu su pokrenuli svoje aktivnosti i izvan Interneta. Načini djelovanja Anonymousa obuhvaćaju prosvjede i hakerske napade. Premda ne postoji očita hijerarhija, općenito je teško potvrditi autentičnost poruka ili informacija dobivenih od Anonymousa.

[29] https://hr.wikipedia.org/wiki/Anonymous_(skupina) – pristup ostvaren 07.09.2017.

Slika 10. *Logo hakerske skupine Anonymous*

Izvor: http://cdn.pcwallart.com/images/anonymous-logo-transparent-wallpaper-2.jpg - pristup ostvaren 18.09.2017.

5. ZAKLJUČAK

Naš svijet je u prošlim desetljećima ušao u informacijsko doba i sve dublje kroči u sfere informatizacije svakodnevnih aktivnosti. Svjedoci smo da je današnji svijet nezamisliv bez informacijskih sustava, kako telefonskih mreža, mobitela tako i PC-a i Interneta. Na naš život već danas značajan utjecaj imaju informacije bilo da se radi o onima koje mi šaljemo u svijet ili one koje primamo od okoline. Kao što čuvamo našu kuću i stvari u njoj tako moramo čuvati i naše infrormacije i podatke.

Značaj informacijskih sustava uočljiv je u tome da je Američki Pentagon pored tradicionalnih terena ratovanja tj. kopno, voda, zrak i svemir uveo i novi peti teren Internet. Rat vođen putem interneta internacionalno je poznat pod nazivom Cyberwar. Prva pojava Cyberwar-a je bila za vrijeme rata u Kosovu kada su Kineski hackeri uspjeli srušiti stranicu Bijele kuće za 3 dana. Prvi ozbiljni virtualni napad desio se 2007. godine u Estoniji koja je 3 tjedna bila izložena napadima hackera širom svijeta. Napadači su uspjeli srušiti web stranice banki, policije, bolnica, državnih organa, medija, ministarstava pa čak i telefonskih linija policije. Napadi su bili toliko intenzivni da su građani Estonije mislili da je došlo da pada vlasti. Prvi veliki štetni softver koji je 2000. godine širom svijeta izazvao štete u milijardskim iznosima bio je crv „I LOVE YOU“ . Širio se e -mail porukama i aktivirao se otvaranjem poruke koja je sa subjektom „I love you“ bila jako privlačna za otvaranje. Kroz izloženo može se primjetit da se antivirusni softver i druge sigurnosne aplikacije u većini slučajeva reaktivno prilagođavaju novim štetnim pojavama. Naime, programeri ne mogu unaprijed znati na koji način će njihov softver biti napadnut pokušavaju u što većoj mjeri otežati rad virusima, crvima, hackerima i dr.

Programeri Anti-virusnih programa, Firewall-a i sl. aplikacija u toku eksploatacije istih „krpaju“ sigurnosne rupe uzrokovane novim virusima, crvima i itd. pa je prema tome izuzetno važno vršiti redovno aktualiziranje sigurnosnog softvera putem Interneta. Osnovne mjere za stvaranje sigurnih sustava jesu kriptografija, jaka autentifikacija provjereni softver i dr.

Kriptografija je tehnika koja može biti korištena za zaštitu podataka koji se prenose s jednog računara na drugi, smanjuje mogućnost da se presretnu ili preprave. Jaka autentifikacija koja osigurava da se točno zna tko se prijavio na neko računalo ili mrežu . Provjereni softver je u biti softver koji je prošao sva ispitivanja i provjere,

osiguravajući da u sebi ne posjeduje štetan kod, obično to prati neka licenca ili certifikat.

6. LITERATURA

Knjige

Baþa, M. Uvod u računalnu sigurnost. Zagreb : Narodne novine d.d., 2004.

Perko, M. HAKERI, GOSPODARI INTERNETA - diplomski rad, Sveučilište u Zagrebu, 2008.

Douglas R. Stinson, "Cryptography: Theory and practice", CRC Press, 1995.

Petrić, D. Internet uzduž i poprijeko. Zagreb: BUG & SysPrint, Kompletan vodić, 2002.

Dokumenti sa Microsoftove konferencije o sigurnosti informacijskih sustava – „Microsoft Security Days -2008.

Web sadržaj

http://www.budimo-sigurni.hr

http://www.zastita.hr

https://hr.wikipedia.org/

http://neptun.zvu.hr/katedre/310/Literatura/RT3_Nove%20tehnologije.../P21_sigurnost.pdf

https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka

Popis slika: