Sigurnost informacijskih sustava

Zubović, Ana

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

ANA ZUBOVIĆ

SIGURNOST INFORMACIJSKIH SUSTAVA

DIPLOMSKI RAD

Rijeka, 2022.

SVEUČILIŠTE U RIJECI
POMORSKI FAKULTET

SIGURNOST INFORMACIJSKIH SUSTAVA
INFORMATION SYSTEMS SECURITY

DIPLOMSKI RAD

Kolegij: Poslovni informacijski sustavi
Mentor: izv. prof. dr. sc. Edvard Tijan
Komentor: izv. prof. dr. sc. Saša Aksentijević
Studentica: Ana Zubović
Studijski smjer: Logistika i menadžment u pomorstvu i prometu
JMBAG: 0112066562

Rijeka, rujan 2022.

Studentica: Ana Zubović

Studijski program: Logistika i menadžment u pomorstvu i prometu

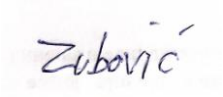
JMBAG:0112066562

IZJAVA O SAMOSTALNOJ IZRADI DIPLOMSKOG RADA

kojom izjavljujem da sam diplomski rad naslova Sigurnost informacijskih sustava izradila samostalno pod mentorstvom izv. prof. dr. sc. Edvard Tijan te komentorstvom izv. prof. dr. sc. Saša Aksentijević.

U radu sam primijenila metodologiju izrade stručnog/znanstvenog rada i koristila se literaturom koja je navedena na kraju diplomskog rada. Tuđe spoznaje, stavove, zaključke, teorije i zakonitosti koje sam izravno ili parafrazirajući navela u diplomskom radu na uobičajen, standardan način citirala sam i povezala s fusnotama i korištenim bibliografskim jedinicama, te nijedan dio rada ne krši bilo čija autorska prava. Rad je pisan u duhu hrvatskoga jezika.

Studentica



Ime i prezime studentice

Ana Zubović

Studentica: Ana Zubović

Studijski program: Logistika i menadžment u pomorstvu i prometu

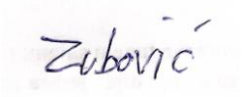
JMBAG: 0112066562

IZJAVA STUDENTA – AUTORA
O JAVNOJ OBJAVI OBRANJENOG DIPLOMSKOG RADA

Izjavljujem da kao studentica – autorica diplomskoga rada dopuštam Pomorskom fakultetu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Pomorskoga fakulteta.

U svrhu podržavanja otvorenog pristupa diplomskim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Pomorskoga fakulteta, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog ograničenja moga diplomskog rada kao autorskoga djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/licenses/.

Studentica – autorica



SAŽETAK

U ovom diplomskom radu obrađena je tema sigurnosti informacijskih sustava. U sklopu rada prikazane su informacije o informacijskim sustavima, sigurnost informacijskih sustava i metode zaštite informacijskih sigurnosti. Informacijska sigurnost skup je mjera i tehnika koje se koriste za kontrolu i zaštitu svih podataka kojima se rukuje. Kod informacijske sigurnosti riječ ranjivost odnosi se na slabost u sustavu, koja dopušta napadaču narušavanje povjerljivosti, integriteta, dostupnosti, kontrole pristupa i dosljednosti sustava ili njegovih podataka i aplikacija. Ranjivost je rezultat grešaka ili nedostataka u dizajnu sustava. U širem smislu može biti i rezultat tehnoloških ograničenja. Kada se velike količine podataka ili informacija elektronički pohranjuju, ranjive su na mnoge vrste prijetnji. Nedostatak sigurnosti pristupa ili također nedostatak sigurnosti u načinu komuniciranja i prijenosa informacija na internetu može biti opasan do te mjere da hakeri mogu uzeti te informacije.

Ključne riječi: informacijski sustavi, napadi, sigurnost, upravljanje sigurnošću, zaštitne mjere

SUMMARY

This thesis deals with the topic of security of information systems. As part of the work, information on information systems, security of information systems and methods of protection of information security are presented. Information security is a set of measures and techniques used to control and protect all data handled. In information security, the word vulnerability refers to a weakness in a system that allows an attacker to compromise the confidentiality, integrity, availability, access control, and consistency of the system or its data and applications. Vulnerabilities are the result of errors or flaws in system design. In a broader sense, they can also be the result of technological limitations. When large amounts of data or information are stored electronically, they are vulnerable to many types of threats. The lack of security of access or also the lack of security in the way of communicating and transferring information on the Internet can be dangerous to the extent that hackers can take this information.

Keywords: information systems, attacks, security, security management, protective measures

SADRŽAJ

1. UVOD

Sustavi koji upravljaju informacijama moraju jamčiti njihovu cjelovitost, odnosno da se informacija prikazuje onako kako je zamišljena, bez izmjena ili manipulacija koje nisu izričito odobrene. Glavni je cilj jamčiti prijenos podataka u sigurnom okruženju koristeći sigurne protokole i tehnike za izbjegavanje rizika. Povjerljivost jamči da će samo ovlaštene osobe ili subjekti imati pristup prikupljenim informacijama i podatcima te da oni neće biti otkriveni bez odgovarajućega dopuštenja. Sustavi informacijske sigurnosti moraju jamčiti da njihova povjerljivost ni u jednom trenutku nije ugrožena.

Sigurnost informacijskoga sustava odnosi se na proces pružanja zaštite računala, mreža i povezanih podataka. S pojavom tehnologije sve se više informacija pohranjuje na mreži te postaje bitno zaštititi ih od neovlaštenih korisnika koji bi ih mogli zloupotrijebiti.

U ovom diplomskom radu opisana je sigurnost informacijskih sustava s naglaskom na ranjivost informacijskoga sustava i moguće napade na informacijski sustav. Prikazani su alati za informacijsku sigurnost i programske metode zaštite koje se danas rabe kako bi korisnici zaštitili svoje podatke.

1.1. PROBLEM, PREDMET I OBJEKTI ISTRAŽIVANJA

Sve do pojave i širenja uporabe računalnih sustava sve informacije od interesa za neku organizaciju držale su se na papiru i pohranjivale u velikom broju ormara. Računalni sustavi omogućuju digitalizaciju sve te količine informacija smanjujući prostor koji zauzimaju, ali prije svega olakšavaju njihovu analizu i obradu. Od pojave velikih izoliranih sustava do danas, u kojima je umrežavanje norma, problemi koji proizlaze iz informacijske sigurnosti također su se mijenjali i razvijali, ali su tu i rješenja koja su se trebala prilagoditi novim tehničkim zahtjevima. Povećava se sofisticiranost napada i time se povećava kompleksnost rješenja, ali bit je ista.

Relevantne spoznaje o problematici i problemu istraživanja znanstvena su podloga za definiranje predmeta istraživanja, a to je istražiti aktualne probleme sigurnosti informacijskih sustava.

Problem i predmet istraživanja odnose se na objekt istraživanja, a to je informacijska sigurnost.

1.2. RADNA HIPOTEZA

Sukladno bitnim odrednicama problema, predmeta i objekta istraživanja, postavljena je radna hipoteza. Hipoteza od koje se polazi jest da se pojavom sofisticiranijih napada stvara velika potreba za sigurnošću podataka te se teži većoj razini zaštite informacijskih sustava.

1.3. SVRHA I CILJEVI ISTRAŽIVANJA

Svrha je istraživanja diplomskog rada *Sigurnost informacijskih sustava* utvrditi kojim se mjerama i metodama postiže informacijska sigurnost nekoga sustava.

Cilj je diplomskoga rada *Sigurnost informacijskih sustava* istražiti i ustanoviti načine na koje se provodi zaštita informacijskih sustava i održava njihova sigurnost.

1.4. ZNANSTVENE METODE

Metode istraživanja koje su uključene u izradu diplomskoga rada temelje se na neizravnom ispitivanju, odnosno takvom pri kojem je istraživačka osnova akademska i publicistička građa, a koja se sama temelji na izravnim ispitivanjima teorijske građe. U tom teorijskom kontekstu metode istraživanja uključuju:

• metodu komparacije

• metodu valorizacije i selekcije referentne bibliografske građe

• metodu deskripcije

• metodu kritičkoga iščitavanja sadržaja koja je korištena u kontekstu stvaranja konceptualnog konteksta

• metodu sintetizacije

• metodu dedukcije koja je korištena u izradi zaključka.

1.5. STRUKTURA RADA

Rad je strukturno podijeljen na šest međusobno povezanih poglavlja i započinje uvodom. U uvodu su definirani problem, predmet i objekti istraživanja, radna hipoteza, svrha i ciljevi istraživanja, znanstvene metode i struktura rada. U drugom poglavlju rada opisani su informacijski sustavi, klasifikacija informacijskih sustava te vrste informacijskih sustava. U trećem poglavlju rada prikazana je informacijska sigurnost gdje su prikazana temeljna načela informacijske sigurnosti, ranjivost informacijskoga sustava, napadi na informacijski sustav, alati za informacijsku sigurnost i kontrola sigurnosti informacijskih sustava. U četvrtom poglavlju rada prikazane su programske metode zaštite informacijskih sigurnosti uključujući vatrozid, virtualnu privatnu mrežu, sustave za otkrivanje napada, sustave za zaštitu od provale i infrastrukturu javnoga ključa. U petom poglavlju rada opisan je sustav upravljanja i revizije informacijskih sustava. Diplomski rad završava zaključkom.

2. OPĆENITO O INFORMACIJSKIM SUSTAVIMA

Zadatak je informacijskoga sustava prikupljanje, pohrana, čuvanje, obrada i isporuka informacija, koje su važne za organizaciju i društvo, tako da budu dostupne i upotrebljive za svakoga tko se želi njima koristiti, uključujući poslovodstvo, klijente, osoblje i ostale. Informacijski sustav omogućuje prikupljanje, razmjenu, organiziranje, analizu, prezentiranje i dostavu pravodobnih, relevantnih, potpunih i točnih informacija tako da budu dostupne i upotrebljive korisnicima.[1]

Sastavni je dio informacijskoga sustava i osoblje obrazovano za rad u sustavu te odgovarajuća oprema. Današnji se informacijski sustavi pretežito ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije. Posebno je značajna uporaba informacijskih sustava unutar poslovnih sustava, gdje služe za njihovo upravljanje i kao potpora izvođenju poslovnih procesa. Osnovne su komponente takva informacijskoga sustava: sustav za obradbu transakcija, upravljački izvještajni sustav ili upravljački informacijski sustav, sustav za potporu odlučivanju i sustav uredskoga poslovanja. Podatci i informacije unutar informacijskoga sustava danas se najčešće pohranjuju i čuvaju u bazama podataka.[2]

Informacijski sustav nekoga tehnološkog ili organizacijskog sustava ono je što ga neprestano opskrbljuje važnim informacijama ili podatcima. Informacija je obrađeni podatak koji za korisnika ima značajnu vrijednost ili neku smisao, dok je podatak samo prikaz činjenica, pojmova, brojeva, imena ili slično.[3]

Hardver se sastoji od ulaznoga/izlaznoga uređaja, procesora, operativnoga sustava i medijskih uređaja. Softver se sastoji od različitih programa i postupaka, tj. procedura. Baza podataka sastoji se od organiziranoga skupa podataka.[4]

---

[1] Tijan, E., UVOD U PIS, 10. 3. 2021., Rijeka, PFRI, br. slajda 6 i 8 (31. 8. 2022.)

[2] informacijski sustav. *Hrvatska enciklopedija*, mrežno izdanje. Leksikografski zavod *Miroslav Krleža*, 2021., pristupljeno 3. 9. 2022. <http://www.enciklopedija.hr/Natuknica.aspx?ID=27410>.

[3] https://www.fpz.unizg.hr/ztos/iszp/a2.pdf (pristupljeno 3. 9. 2022.)

[4] Prachi Juneja, https://www.managementstudyguide.com/types-of-information-systems.htm (pristupljeno 3. 9. 2022.)

Mreža se sastoji od središta koje šalje podatke svakom povezanom uređaju, komunikacijskih medija i mrežnih uređaja. Ljudi se sastoje od operatera uređaja, mrežnih administratora i stručnjaka za sustave.[5]

2.1. KLASIFIKACIJA INFORMACIJSKIH SUSTAVA

Informacijski sustav može se klasificirati na temelju upotrebe informacija u bilo kojoj organizaciji. Stoga se informacijski sustav može podijeliti na sustav operativne podrške i sustav podrške upravljanju.[6]

1. SUSTAV OPERATIVNE PODRŠKE

U sustavu operativne podrške podatke unosi krajnji korisnik koji obrađuje informacijske proizvode, tj. izvješća koja koriste unutarnji i/ili vanjski korisnici. Svrha je sustava operativne podrške olakšati poslovanje, kontrolirati proizvodnju, podržati unutarnju i vanjsku komunikaciju te ažurirati središnju bazu podataka. Sustav operativne podrške dalje je podijeljen na sustav za obradu transakcija, sustav kontrole procesa i sustav poslovne suradnje.[7]

→U organizaciji proizvodnje postoji nekoliko vrsta transakcija u odjelima. Tipični su organizacijski odjeli prodaja, računi, financije, pogon, inženjering, ljudski resursi i marketing.[8]

U tim transakcijama mogu se pojaviti prodajni nalog, povrat, gotovinski primitci, kreditne potvrde, materijalno knjigovodstvo, upravljanje zalihama, računovodstvo amortizacije itd. Te se transakcije mogu kategorizirati u skupnu obradu transakcija, obradu pojedinačne transakcije i obradu transakcija u stvarnom vremenu.[9]

[5] Ibidem.

[6] Ibidem.

[7] Ibidem.

[8] Ibidem.

[9] Ibidem.

→U proizvodnoj organizaciji određene odluke donosi računalni sustav bez ikakve ručne intervencije. U toj vrsti sustava važne se informacije šalju u sustav u stvarnom vremenu čime se omogućuje kontrola procesa.[10]

→U novije vrijeme sve je veći naglasak na timskom radu ili suradnji između različitih funkcionalnih timova. Sustav koji omogućuje zajednički rad poboljšanjem komunikacije i dijeljenja podataka naziva se sustavom poslovne suradnje.

2. SUSTAV PODRŠKE UPRAVLJANJU

Menadžeri zahtijevaju precizne informacije u specifičnom formatu kako bi donijeli organizacijsku odluku. Sustav koji menadžerima omogućava učinkovit proces donošenja odluka naziva se sustav podrške upravljanju. Sustavi za podršku upravljanju kategorizirani su kao informacijski sustavi za upravljanje, sustavi za podršku odlučivanju, stručni sustavi i računovodstveni informacijski sustavi. Upravljački informacijski sustav pruža informacije menadžeru, olakšavajući rutinski proces donošenja odluka i rješavanje specifičnih problema.[11]

2.2. VRSTE INFORMACIJSKIH SUSTAVA

Iako mnogi informacijski sustavi nude razne prednosti i mogućnosti, poduzeća obično rabe ovih devet informacijskih sustava u svojim tvrtkama. Koji se god informacijski sustav primjenjuje u poslovanju, prednosti koje će sustav ponuditi jesu:

- svojim istraživanjem i razvojem potaknut će inovacije u poslovnim aktivnostima
- omogućit će automatizaciju, smanjujući korake koji se poduzimaju za dovršetak zadatka
- pomaže da hardver, softver, pohrana podataka i mrežni sustav budu sigurni i ažurirani.[12]

[10] Ibidem.

[11] Ibidem.

[12] Ibidem.

Vrste informacijskih sustava

a) *Knowledge Management Systems* (sustavi potpore znanju)

Postoje različiti sustavi upravljanja znanjem koje organizacija primjenjuje kako bi osigurala neprestani protok novoga i ažuriranoga znanja u poduzeće i njegove procese.

Sustav znanja jedan je od sustava za upravljanje znanjem koji olakšava integraciju novih informacija ili znanja u poslovni proces te nudi podršku i resurse različitim tehnikama stvaranja znanja, aplikacijama umjetne inteligencije i sustavima grupne suradnje za razmjenu znanja. Također koristi se grafikama, slikama itd. za širenje novih informacija.[13]

Primjeri:

- dizajneri se često koriste računalno potpomognutim sustavima projektiranja (CAD) za automatizaciju procesa projektiranja

- financijske radne stanice koriste se za analizu ogromnih količina financijskih podataka uz pomoć novih tehnologija

- sustavi virtualne stvarnosti nalaze se u znanstvenom, obrazovnom i poslovnom području za korištenje grafike i različitih sustava za prezentiranje podataka.[14]

b) *Management Information System* – upravljanje temeljem dokazanih matematičkih/statističkih metoda

Informacijski su sustavi upravljanja proučavanje ljudi, tehnologije, organizacije i odnosa među njima. MIS stručnjaci pomažu tvrtkama da ostvare najveću korist od ulaganja u osoblje, opremu i poslovne procese.[15]

Upravljački informacijski sustav pomaže menadžerima automatiziranjem različitih procesa koji su se u početku obavljali ručno. Poslovne su aktivnosti praćenje i analiza poslovnih rezultata, donošenje poslovnih odluka, izrada poslovnoga plana i definiranje tijeka rada.

Informacijski sustav upravljanja smatra se značajnim sustavom koji neizmjerno pomaže menadžerima.

---

[13] „The 6 Types Of Information Systems And Their Applications", 14. 7. 2022., https://emeritus.org/in/learn/the-6-types-of-information-systems-and-their-applications/ (pristupljeno 31. 8. 2022.)

[14] Ibidem.

[15] "WHAT IS MIS?", https://mays.tamu.edu/department-of-information-and-operations-management/management-information-systems/ (pristupljeno 31. 8. 2022.)

Neke prednosti upravljačkoga informacijskog sustava mogu biti ove: povećava učinkovitost i produktivnost tvrtke, pruža jasnu sliku uspješnosti organizacije, dodaje vrijednost postojećim proizvodima, uvodi inovacije i poboljšava razvoj proizvoda, pomaže u komunikaciji i planiranju poslovnih procesa te pomaže organizaciji osigurati konkurentsku prednost.[16]

c) *Decision Support System* – sustav za podršku odlučivanju

Sustav za podršku odlučivanju informacijski je sustav koji analizira poslovne podatke i druge informacije povezane s poduzećem kako bi ponudio automatizaciju donošenja odluka ili rješavanja problema. Menadžer se njime koristi u vremenima poteškoća koja se javljaju tijekom poslovanja.[17]

Općenito, sustav za podršku odlučivanju koristi se za prikupljanje informacija o prihodima, prodajnim brojkama ili zalihama. Koristi se u različitim industrijama, a sustav za podršku odlučivanju popularan je informacijski sustav.[18]

d) *Office Automation System* – automatizacija ureda

Sustav za automatizaciju ureda informacijski je sustav koji automatizira različite administrativne procese poput dokumentiranja, snimanja podataka i uredskih transakcija. Sustav uredske automatizacije podijeljen je na menadžerske i uredske djelatnosti. Ovo su neke od poslovnih aktivnosti koje se obavljaju u okviru te vrste informacijskoga sustava:

- e-mail
- govorna pošta
- obrada riječi.[19]

e) *Transaction Processing System/Data Processing System* – evidencija i obrada podataka o poslovnim transakcijama

Sustav za obradu transakcija automatizira proces prikupljanja, izmjene i dohvaćanja transakcija. Posebnost je te vrste informacijskoga sustava da povećava performanse, pouzdanost i dosljednost poslovnih transakcija. Pomaže tvrtkama u glatkom obavljanju svakodnevnih operacija bez ikakvih problema.[20]

f) *Executive Information System* – podvarijanta za izvršne rukovoditelje

[16] Ibidem.

[17] Ibidem.

[18] Ibidem.

[19] Ibidem.

[20] Ibidem.

Izvršni informacijski sustav (EIS) sustav je za podršku odlučivanju (DSS) koji se koristi za pomoć višim rukovoditeljima u procesu donošenja odluka.

To čini pružanjem jednostavnoga pristupa važnim podatcima potrebnim za postizanje strateških ciljeva u organizaciji. EIS obično ima grafičke prikaze na sučelju jednostavnom za korištenje. Izvršni informacijski sustavi mogu se koristiti u mnogim različitim vrstama organizacija za praćenje učinka poduzeća kao i za prepoznavanje prilika i problema.[21]

g) *Expert System* – sustav s ugrađenim znanjem i simulacijom zaključivanja

Ekspertni sustav računalni je program koji se koristi metodama umjetne inteligencije za rješavanje problema unutar specijalizirane domene koja obično zahtijeva ljudsku stručnost.[22]

h) *Group Support System/Groupware* – sustav za podršku skupnom radu

Grupni je program klasa računalnih programa koji pojedincima omogućuju suradnju na projektima sa zajedničkim ciljem s geografski raspršenih lokacija zajedničkim internetskim sučeljima kao sredstvom za komunikaciju unutar grupe. Grupni softver također može uključivati sustave za pohranu s daljinskim pristupom za arhiviranje često korištenih podatkovnih datoteka. Članovi radne grupe mogu ih mijenjati, pristupati im i dohvaćati ih. Grupni softver poznat je i kao softver za suradnju.[23]

i) *Geographic Information System* – geografski informacijski sustav

Geografski informacijski sustav (GIS) računalni je sustav za hvatanje, pohranjivanje, provjeru i prikaz podataka koji se odnose na položaje na Zemljinoj površini.

GIS može prikazati mnogo različitih vrsta podataka na jednoj karti kao što su ulice, zgrade i vegetacija. To omogućuje ljudima da lakše vide, analiziraju i razumiju uzorke i povezanost.[24]

---

[21] „Executive Information System (EIS)", https://www.techopedia.com/definition/1016/executive-information-system-eis (pristupljeno 31. 8. 2022.)

[22] Zwass, V.. "expert system." Encyclopedia Britannica, February 10, 2016. https://www.britannica.com/technology/expert-system. (pristupljeno 31. 8. 2022.)

[23] „Groupware", 29.10.2012., https://www.techopedia.com/definition/7481/groupware (pristupljeno 31. 8. 2022.)

[24] „GIS (Geographic Information System)", https://education.nationalgeographic.org/resource/geographic-information-system-gis (pristupljeno 31. 8. 2022.)

3. INFORMACIJSKA SIGURNOST

Informacijska sigurnost stanje je povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom potporom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.[25]

Informacijska sigurnost (ponekad se naziva *InfoSec*) pokriva alate i procese kojima se organizacije koriste za zaštitu informacija. To uključuje postavke koje sprječavaju neovlaštene osobe da pristupe poslovnim ili osobnim podatcima. Informacijska sigurnost područje je koje raste i razvija se i pokriva širok raspon područja, od sigurnosti mreže i infrastrukture do testiranja i revizije.[26]

Informacijska sigurnost štiti osjetljive podatke od neovlaštenih aktivnosti, uključujući inspekciju, modificiranje, snimanje i bilo kakvo ometanje ili uništenje. Cilj je osigurati sigurnost i privatnost kritičnih podataka kao što su podatci o korisničkom računu, financijski podatci ili intelektualno vlasništvo.[27]

Posljedice sigurnosnih incidenata uključuju krađu osobnih podataka, neovlašteno mijenjanje podataka i brisanje podataka. Napadi mogu poremetiti radne procese i naštetiti ugledu tvrtke, a imaju i dojmljivu cijenu.[28]

Organizacije moraju izdvojiti sredstva za sigurnost i osigurati da su spremne otkriti, odgovoriti na napade i proaktivno spriječiti napade kao što su krađa identiteta, zlonamjerni programi, virusi, zlonamjerni insajderi i ucjenjivački softveri.[29]

[25] "Što je to informacijska sigurnost", https://www.uvns.hr/hr/sto-je-to-informacijska-sigurnost (pristupljeno 4. 9. 2022.)

[26] "Information Security: The Ultimate Guide", https://www.imperva.com/learn/data-security/information-security-infosec/ (pristupljeno 4. 9. 2022.)

[27] Ibidem.

[28] Ibidem.

[29] Ibidem.

3.1. TEMELJNA NAČELA INFORMACIJSKE SIGURNOSTI

Osnovna su načela informacijske sigurnosti povjerljivost, integritet i raspoloživost. Svaki element programa informacijske sigurnosti mora biti dizajniran za implementaciju jednoga ili više tih načela. Zajedno se nazivaju *CIA Triad*.[30]

CIA Triad prikazan je na slici 1.

Slika 1. *CIA Triad*

Izvor: https://www.f5.com/labs/articles/education/what-is-the-cia-triad (pristupljeno 5. 9. 2022.)

Povjerljivost: mjere povjerljivosti osmišljene su kako bi se spriječilo neovlašteno otkrivanje informacija.

[30] Ibidem.

Svrha je načela povjerljivosti zadržati privatnost osobnih podataka i osigurati da budu vidljivi i dostupni samo onim pojedincima koji ih posjeduju ili im trebaju za obavljanje njihovih organizacijskih funkcija.[31]

Integritet: integritet uključuje zaštitu od neovlaštenih promjena (dodavanja, brisanja, izmjena itd.) podataka. Načelo cjelovitosti osigurava da su podatci točni i pouzdani te da se ne mijenjaju netočno, bilo slučajno ili zlonamjerno.[32]

Raspoloživost: raspoloživost je zaštita sposobnosti sustava da softverske sustave i podatke učini potpuno dostupnima onda kada su ovlaštenom korisniku potrebni. Svrha je raspoloživosti učiniti tehnološku infrastrukturu, aplikacije i podatke dostupnima kada su potrebni za organizacijski proces ili za klijente organizacije.[33]

Kombinacijom prvih triju osnovnih načela tvore se dodatna načela kojima se upotpunjuje i dodatno opisuje svrha informacijskoga sustava:

- neporecivost – svojstvo koje osigurava nemogućnost poricanja izvršene aktivnosti ili primitka informacije (podatka)
- dokazivost – svojstvo koje osigurava bilježenje i praćenje određenih aktivnosti
- autentičnost – svojstvo koje osigurava da je identitet korisnika zaista onaj za koji se tvrdi da jest
- pouzdanost – svojstvo očekivanoga ponašanja i rezultata.[34]

3.2. RANJIVOST INFORMACIJSKOGA SUSTAVA

Ranjivost je slabost koju je moguće slučajno aktivirati ili namjerno iskoristiti, a posljedica toga može biti nanošenje štete informacijskom sustavu i poslovnim ciljevima.[35]

[31] Ibidem.

[32] Ibidem.

[33] Ibidem.

[34] Ibidem.

[35] Tijan, E., SIGURNOST INFORMACIJSKIH SUSTAVA, 19. 6. 2021., Rijeka, PFRI, br. slajda 28 (5. 9. 2022.)

Ranjivosti koje se povezuju s resursima uključuju, između ostaloga, slabosti fizičke sigurnosti, organizacije, internih akata, zaposlenika, upravljačke strukture, hardvera, softvera i informacija.[36]

Ranjivost je stanje ili skup stanja koji može omogućiti nekoj prijetnji da utječe na resurse, primjerice nedostatak mehanizma kontrole pristupa jest ranjivost koja bi mogla omogućiti ostvarenje prijetnje neovlaštenoga pristupa što može dovesti do gubitka ili oštećenja resursa.[37]

Najjednostavnije rečeno, ranjivost računalnoga sustava greška je ili slabost u sustavu ili mreži koja se može iskoristiti za nanošenje štete ili omogućiti napadaču da na neki način manipulira sustavom.

Životni ciklus upravljanja ranjivostima ima cilj omogućiti organizacijama da identificiraju slabosti informacijskoga sustava, da određuju prioritet imovine, da procjenjuju, prijavljuju i otklanjaju slabosti i da potvrde da su eliminirani.[38]

U informacijskoj sigurnosti ranjivost je sigurnosni nedostatak ili slabost koja dopušta uljezu da smanji sigurnost informacijskoga sustava. Ranjivost zahtijeva tri elementa: slabost sustava, pristup uljeza slabosti i sposobnost uljeza da iskoristi slabost pomoću alata ili tehnike.[39]

Koraci su u životnom ciklusu upravljanja ranjivostima:

1. otkrivanje: popis svog sadržaja na internetu i identificiranje pojedinosti, uključujući operativni sustav i otvorene usluge za prepoznavanje ranjivosti; identificiranje sigurnosnih propusta prema redovnom automatiziranom rasporedu

2. određivanje prioriteta imovine: kategorizacija imovine u grupe ili poslovne jedinice i dodjeljivanje poslovne vrijednosti grupama imovine na temelju njihove kritičnosti za poslovanje

[36] Ibidem.

[37] Tijan, E., SIGURNOST INFORMACIJSKIH SUSTAVA, 19. 6. 2021., Rijeka, PFRI, br. slajda 29 (5. 9. 2022.)

[38] "Vulnerability Management Life Cycle", https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm (pristupljeno 5. 9. 2022.)

[39] Ibidem.

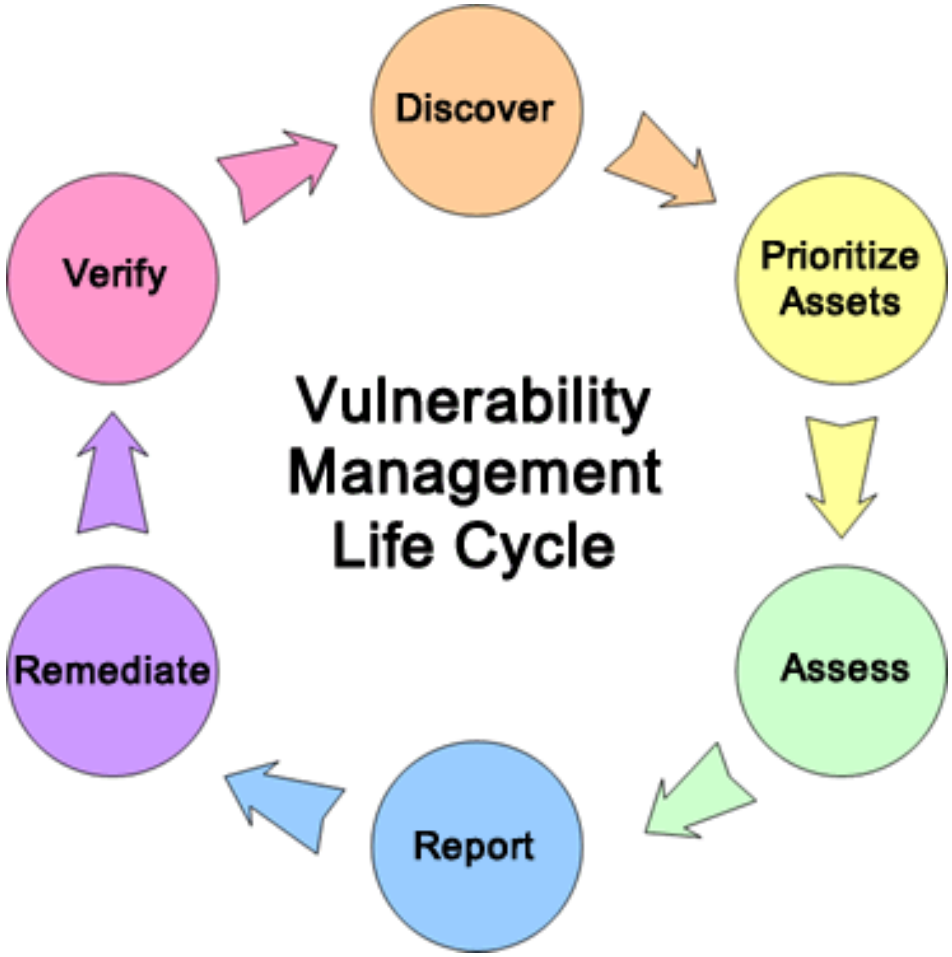
3. procjena: određivanje osnovnoga profila rizika kako bi se moglo eliminirati rizike na temelju kritičnosti imovine, prijetnje ranjivosti i klasifikacije imovine

4. izvješće: određivanje razine poslovnoga rizika povezanoga s imovinom u skladu sa sigurnosnim politikama; dokumentiranje sigurnosnoga plana, praćenje sumnjivih aktivnosti i opisivanje poznate ranjivosti

5. popravak/saniranje: određivanje prioriteta i popravak ranjivosti u skladu s poslovnim rizikom; uspostava kontrole i pokazivanje napretka

6. provjera: provjera jesu li prijetnje uklonjene.

Životni ciklus upravljanja ranjivostima prikazan je na slici 2.



Slika 2. Životni ciklus upravljanja ranjivostima

Izvor: https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm (pristupljeno 6. 9. 2022.)

3.3. NAPADI NA INFORMACIJSKI SUSTAV

Prijetnje informacijskoj sigurnosti mogu biti brojne poput softverskih napada, krađe intelektualnoga vlasništva, krađe identiteta, krađe opreme ili informacija, sabotaže i iznude informacija.[40]

Vrste prijetnji sigurnosti informacijskoga sustava jesu sljedeće:

- neovlašteni pristup
- računalni virusi
- krađa
- sabotaža.[41]

Jedan je od najčešćih sigurnosnih rizika u vezi s računalnim informacijskim sustavima opasnost od neovlaštenoga pristupa povjerljivim podatcima.[42]

Računalni je virus vrsta softvera koji je namjerno napravljen da uđe u računalo bez dopuštenja ili znanja korisnika, sa sposobnošću da se umnoži i tako nastavi širiti. Osnovna je funkcija računalnih virusa proizvoditi neželjene učinke na računalu.

Virus je program koji može inficirati druge programe modificirajući ih tako da uključe kopiju njega samoga, koja također može biti modificirana. Pod infekcijom se smatra mogućnost virusa da ubaci svoje naredbe u postupak izvršenja programa, odnosno pokušaj izvođenja legitimnoga programa uzrokovat će i izvođenje virusa.[43]

Virusni program i dalje može uzrokovati padove i gubitak podataka. U mnogim slučajevima štete uzrokovane računalnim virusom mogu biti slučajne, nastati samo kao rezultat lošega programiranja.[44]

---

[40] Ekclhart, A., Fenz, S., Goluch, G., Weippl, E. Ontological mapping of common criteria's security assurance requirements IFIP International Information Security Conference, Springer, 2007., str 85.

[41] Ibidem.

[42] Politika sustava informacijske sigurnosti, dostupno na: https://podaci.dzs.hr/hr/pages/dzs/politika-sustava-informacijske-sigurnosti/ (pristupljeno 20. 8. 2022.)

[43] Ibidem.

[44] Kim, H., K., Kim, T., H., Kim J., Reliability assurance in development process for TOE on the common criteria International Conference on Software Engineering Research and Applications, Springer, 2003. (20. 8. 2022.)

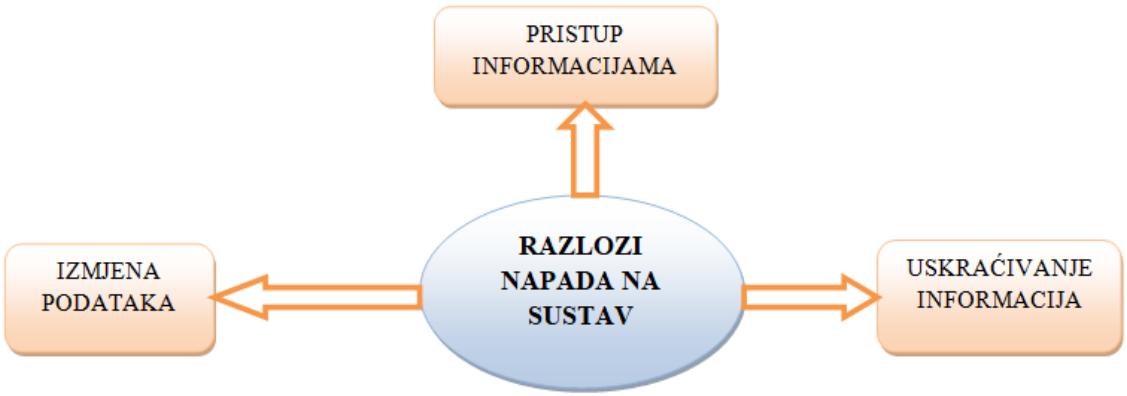
Informacijski sustavi često su izloženi različitim vrstama prijetnji koje mogu uzrokovati različite vrste šteta, koje mogu dovesti do značajnih financijskih gubitaka. Štete informacijske sigurnosti mogu varirati od malih gubitaka do potpunoga uništenja informacijskoga sustava.[45]

Implementirane prijetnje informacijskoj sigurnosti mogu zaustaviti aktivnosti i uzrokovati značajnu štetu. Nenamjerne prijetnje informacijskoj sigurnosti, koje su nastale u nedostatku izražene volje za nanošenjem štete, ponekad su najopasnije.[46]

Pod prijetnjom informacijskoj sigurnosti podrazumijeva se namjerna ili nenamjerna radnja koja negativno utječe na informacijski sustav ili podatke pohranjene u njemu i od koje je potrebna stručno organizirana zaštita.[47]

Glavni kriterij koji omogućuje klasificiranje prijetnje kao slučajne, a ne temeljene na sebičnim ciljevima, slučajnost je njezina pojavljivanja. Iza takva postupanja ne stoji nikakva namjera da se nanese šteta zaštićenim informacijama ili da se organizira njihovo curenje ili uništavanje.

Razlozi napada na sustav informacija su prikazani na slici 3.



Slika 3. Razlozi napada na sustav informacija

Izvor: Izrada autorice prema Revizijska izvješća, 2021.

[45] Ibidem.

[46] Geric, S., Hutinski, Z., Information system security threats classifications. Journal of Information and Organizational Sciences, 2007., str. 32. (25. 8. 2022.)

[47] Ibidem.

Napadači mogu napadati sustave sigurnosti informacija kako bi došli do informacija do kojih normalnim, zakonitim putem ne mogu doći te kako bi saznali neke povjerljive ili tajne podatke koji ih zanimaju a da bilo što ne rade s njima, već da ih saznaju.[48]

Među glavnim uzrocima koji mogu proizvesti napade na informacijske sustave jesu:

- ranjivost računalnih sustava, odnosno kvarovi ili nedostatci koji dovode sredstva u opasnost jer nisu učinkovito zaštićena
- slučajno otkrivanje povjerljivih informacija od strane zaposlenika
- gubitak i krađa elektroničkih uređaja koji pohranjuju važne podatke
- društveni inženjering koji se općenito sastoji od manipulacije određenim ljudima kako bi se dobili povjerljivi podatci kao što su lozinke ili drugi podatci od velike vrijednosti i važnosti.[49]

Vrste napada na računalnu sigurnost uključuju:

- zlonamjerni softver
- ubacivanje SQL koda
- krađa identiteta
- *Doxing*
- napad uskraćivanjem usluge – *DdoS* (engl. *Distributed denial-of-service*, distribuirano uskraćivanje usluge).
- *Phishing*
- socijalni inženjering.

U nastavku je pojašnjen svaki od navedenih napada.

[48] Maidl, M., Von, Oheimb, D., Hartmann, P., Robinson, R., Formal security analysis of electronic software distribution systems International Conference on Computer Safety, Reliability, and Security, Springer, 2008., str. 415.

[49] Loch, K., Carr, H., Warkentin, M., Threats to Information Systems, Today's Reality, Yesterday's Understanding, Management Information Systems Quarterly 16.2, 1992.

3.3.1. Zlonamjerni softver

Zlonamjerni softver (engl. *Malware*) može doći u različitim oblicima, što je prikazano u tablici 1.

Tablica 1. Karakteristike zlonamjernog softvera

VIRUS	KARAKTERISTIKE
Virus	Program sposoban za reprodukciju u cijelom sustavu. Nakon što ga se aktivira, širi se cijelim sustavom i svim uređajima spojenim na njegovu mrežu.
Crvi	Vrlo ih je teško otkriti i njihova je radnja da zaraze računalo i naprave svoje kopije kako bi ih proširili mrežom, bez intervencije.
Trojanci	Prerušeni su u legitimni softver za nanošenje štete ili prikupljanje podataka.
Špijunski softver	Tajno bilježi što korisnik radi.
Ransomware	Otima i zaključava datoteke i podatke, šifrira ih, prijeti da će ih izbrisati osim ako se ne plati otkupnina (često se traži u kriptovalutama). To je sofisticirani *malware* s puno aktivnosti u današnje vrijeme.
Adware	Oglašavanje koje se može koristiti za širenje zlonamjernoga softvera. Ne mora nužno oštetiti opremu i može djelovati kao špijun koji prikuplja i prenosi podatke kako bi proučio ponašanje korisnika i bolje ciljao vrstu oglašavanja koje korisnik prima.
Bot mreže	Računalne mreže zaražene crvima ili trojancima koji se koriste za izvršavanje *online* zadataka bez dopuštenja korisnika.

Izvor: izrada autorice rada prema https://ashwiniscl.wordpress.com/information-system-attacks/ (pristupljeno 25. 8. 2022.)

Neprijateljski, nametljiv i namjerno neugodan, zlonamjerni softver nastoji upasti, oštetiti ili onemogućiti računala, računalne sustave, mreže, tablete i mobilne uređaje, često preuzimanjem djelomične kontrole nad operacijama uređaja. Ometa normalno funkcioniranje. Motivi zlonamjernoga softvera različiti su. Zlonamjerni softver može biti usmjeren na zarađivanje novca, sabotiranje sposobnosti za obavljanje posla, davanje političkih izjava i slično.

Iako zlonamjerni softver ne može oštetiti fizički hardver sustava ili mrežnu opremu, može ukrasti, šifrirati ili izbrisati podatke, promijeniti ili oteti osnovne funkcije računala i špijunirati aktivnosti računala bez znanja ili dopuštenja korisnika.[50]

Zlonamjerni softver može se otkriti s mnogo različitih nenormalnih ponašanja, što uključuje:

- usporavanje računala – jedna je od nuspojava zlonamjernoga softvera smanjenje brzine operativnoga sustava (OS – engl. *Operating system*, operativni sustav), bilo da se korisnik kreće internetom ili se samo koristi svojim lokalnim aplikacijama. To se obično događa kada je računalo spojeno na botnet, tj. mreža porobljenih računala koja se koriste za izvođenje DDoS napada, slanje neželjene pošte ili rudarenje kriptovalute.
- zaslon je preplavljen oglasima – neočekivani skočni oglasi tipičan su znak zaraze zlonamjernim softverom. Posebno su povezani s oblikom zlonamjernoga softvera poznatoga kao *adware*. Štoviše, skočni prozori obično dolaze u paketu s drugim skrivenim prijetnjama zlonamjernog softvera.
- rušenje sustava – to može doći kao zamrzavanje ili BSoD (engl. *Blue screen of death*, plavi ekran smrti), najčešće se pojavljuje na Windowsovim sustavima nakon što naiđe na pogrešku.
- gubitak prostora na disku – to može biti zbog zlonamjernoga softvera koji se skriva u tvrdom disku, odnosno *bundlewareu*.[51]

[50] Ibidem.

[51] Ibidem.

3.3.2. Ubacivanje SQL koda

Ubacivanje SQL koda tehnika je ubacivanja koda koja može uništiti bazu podataka. To je jedna od najčešćih tehnika mrežnoga hakiranja.[52]

Ubacivanje SQL koda napadaču omogućuje miješanje u upite koje aplikacija postavlja svojoj bazi podataka.[53]

Može se zaključiti da omogućuje napadaču pregled podataka koje inače ne može dohvatiti. To može uključivati podatke koji pripadaju drugim korisnicima ili bilo koje druge podatke kojima sama aplikacija može pristupiti.

U mnogim slučajevima, napadač može modificirati ili izbrisati te podatke, uzrokujući stalne promjene sadržaja ili ponašanja aplikacije.[54]

3.3.3. Krađa identiteta

Do krađe identiteta dolazi kada se netko koristi osobnim podatcima korisnika, kao što su ime, broj osiguranja ili broj kreditne kartice, bez dopuštenja korisnika, za počinjenje prijevare ili drugih zločina.[55]

Učestalost krađe identiteta dramatično je porasla. Hakeri mogu koristiti mnoštvo metoda za dobivanje osobnih podataka, koji se mogu iskoristiti za izvođenje zlonamjernih radnji.[56]

Osobni podatci mogu se pronaći na internetu, pojedinci aktivno objavljuju podatke o sebi kako bi uključili informacije iz blokova potpisa, stranica društvenih mreža, organizacijskih stranica, životopisa, biografija ili intervjua.[57]

---

[52] https://www.w3schools.com/sql/sql_injection.asp (pristupljeno 26. 8. 2022.)

[53] Ibidem.

[54] Ibidem.

[55] https://www.sandiego.edu/its/security-and-privacy/identity-theft.php (pristupljeno 26. 8. 2022.)

[56] Ibidem.

[57] Ibidem.

Krađa identiteta ponajprije se koristi za obavljanje financijskih transakcija korištenjem računa na ime korisnika. To može biti kupnja brojem kreditne kartice ili uzimanje kredita za automobil. Podatci o osobnom identitetu mogu se ukrasti prekopavanjem po smeću u potrazi za osjetljivim dokumentima, infiltriranjem u organizacije koje upravljaju velikim količinama osobnih podataka i hakiranjem računalnih sustava.[58]

3.3.4. Doxing

Izraz *Doxing* kratica je za *ispuštanje doxa*, a *dox* je u slengu naziv za dokumente. *Doxing* je obično zlonamjeran čin koji se koristi protiv ljudi s kojima se haker ne slaže ili ne voli.[59]

Doxing je čin otkrivanja identifikacijskih informacija o nekome na mreži, kao što su njegovo pravo ime, kućna adresa, radno mjesto, telefonski broj, financijski i drugi osobni podatci. Ta se informacija zatim plasira u javnost bez dopuštenja osobe čije se informacije iznose. *Doxing* napadi mogu varirati od relativno trivijalnih, poput lažnih prijava e-poštom ili dostave *pizze* do daleko opasnijih, poput uznemiravanja nečije obitelji ili poslodavca, krađe identiteta, prijetnji ili drugih oblika internetskoga zlostavljanja ili čak uznemiravanje osobe.

3.3.5. Ddos napadi

Distribuirani napad uskraćivanja usluge (DDoS) zlonamjeran je pokušaj da se internetska usluga učini nedostupnom korisnicima, obično privremenim prekidom ili obustavom usluga njezina hosting poslužitelja.[60]

[58] Ibidem.

[59] https://www.kaspersky.com/resource-center/definitions/what-is-doxing (pristupljeno 26. 8. 2022.)

[60] https://www.imperva.com/learn/ddos/ddos-attacks/ (pristupljeno 26. 8. 2022.)

DDoS napadi postižu učinkovitost korištenjem više kompromitiranih računalnih sustava kao izvora prometa napada. Iskorištavani strojevi mogu uključivati računala i druge umrežene resurse kao što su IoT (engl. *Internet of things*, internetske stvari) uređaji.[61]

Te se mreže sastoje od računala i drugih uređaja (kao što su IoT uređaji) koji su zaraženi zlonamjernim softverom, što omogućuje da ih napadač daljinski kontrolira. Ti pojedinačni uređaji nazivaju se botovi, a skupina botova naziva se botnet.

Nakon što je botnet uspostavljen, napadač može usmjeriti napad slanjem daljinskih uputa svakom botu. Kada je žrtvin poslužitelj ili mreža na meti botneta, svaki bot šalje zahtjeve na ciljnu IP adresu, potencijalno uzrokujući preopterećenje poslužitelja ili mreže, što dovodi do uskraćivanja usluge normalnom prometu.[62]

Najočitiji je simptom DDoS napada iznenadna sporost ili nedostupnost stranice ili usluge.[63]

3.3.6. Phishing

Phishing napadi podrazumijevaju aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih internetskih stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka.

Pritom se prije svega misli na podatke kao što brojevi kreditnih kartica, korisnička imena i zaporke, PIN kodovi i slično iako postoje i druge mogućnosti.[64]

Phishing je brzo rastuća prijetnja u *cyber* svijetu i uzrokuje milijarde dolara štete svake godine internetskim korisnicima.

---

[61] Ibidem.

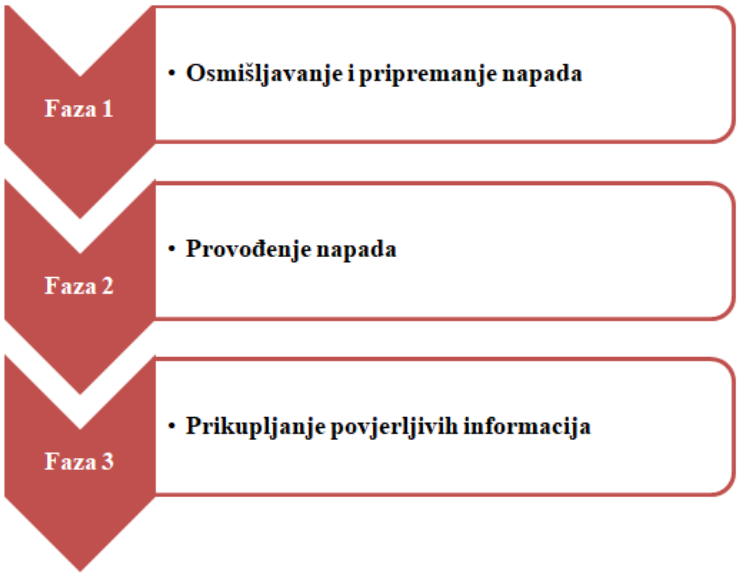
[62] Ibidem.

[63] Ibidem.

[64] "Phishing napadi", CARNET CERT, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-01-106.pdf?fbclid=IwAR1OGJqEs8cqzHaNudGRwQm5J3gfVoaL-HcGe1pXVlK_MjVg7IhIxV3WI1s (pristupljeno 27. 9. 2022.)

To je nezakonita aktivnost koja se koristi skupinom društvenoga inženjeringa i tehnologijom za prikupljanje osjetljivih informacija internetskih korisnika.

Životni ciklus *phishinga* prikazan je na slici 4.



Slika 4. Životni ciklus *phishinga*

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-01-106.pdf (pristupljeno 20. 9. 2022.)

Osmišljavanje i pripremanje napada prva je faza životnoga ciklusa *phishinga*.

U fazi pripreme napada napadač prikuplja informacije o organizaciji koja se želi kompromitirati te o korisnicima koji su potencijalne mete napada. Budući da učinkovitost napada u velikoj mjeri ovisi o tome koliko je napad pažljivo i detaljno planiran, iskusniji neovlašteni korisnici toj fazi posvećuju dosta vremena i resursa.[65]

Prvi korak osmišljavanja, odnosno pripreme napada podrazumijeva identifikaciju ciljne organizacije, detaljnu analizu sadržaja i uočavanje sigurnosnih propusta unutar internetskih stranica, identifikaciju ranjivosti na strani klijenta te druge slične postupke. Na temelju prikupljenih informacija napadač kreira lažiranu kopiju internetskih stranica ciljne organizacije te osmišljava sadržaj *phishing* poruka koje će prosljeđivati potencijalnim metama napada.

[65] Ibidem.

Načini kreiranja lažiranih internetskih stranica ovise u prvom redu o iskustvu i vještini neovlaštenih korisnika, a slično vrijedi i za lažiranje poruka elektroničke pošte. Dosadašnja iskustva pokazuju da se *phishing* napadi mogu prilično razlikovati u složenosti i sofisticiranosti, što kasnije utječe i na njihovu učinkovitost. Poruke elektroničke pošte nastoje se oblikovati tako da djeluju službeno, pri čemu se sadržajem poruke kod korisnika pokušavaju izazvati osjećaji koji će smanjiti mogućnost realne procjene situacije (strah, nesigurnost i sl.). Fazi osmišljavanja i pripreme također pripada i postupak identifikacije ranjivih e-poruka poslužitelja koji će se iskoristiti za prosljeđivanje poruka elektroničke pošte. U tu svrhu najčešće se koriste nezaštićena e-pošta ili *proxy* poslužitelji (eng. *open relay*), a sve češće se koriste i kompromitirana osobna računala na kojima su instalirani specijalni programi koji omogućuju slanje e-poruka. Nakon što su pripremljeni svi upravo opisani elementi, napadač može nastaviti sa sljedećim fazama provođenja napada.[66]

Provođenje napada druga je faza životnoga ciklusa *phishinga*.

U fazi provođenja napada napadač šalje pripremljene poruke elektroničke pošte na adrese korisnika koji su odabrani kao potencijalne mete napada. Osim sustava elektroničke pošte poruke je moguće distribuirati i putem *newsgrupa* i drugih sličnih *instant messaging* servisa, oglašavanjem *bannerima* na internetskim stranicama i sl.[67]

Osim korisnika koji su ciljane mete napada napadači se vrlo često koriste i dodatnim kanalima kojima bi mogli privući veći broj korisnika. Tako, na primjer, napadači lažirane internetske stranice vrlo često prijavljuju na internetske tražilice kako bi se na taj način privukli oni korisnici koji se za dolazak do adresa internetskih stranica koriste alatima kao što je npr. pretraživač *Google*. Nakon što su poruke poslane na pripremljene adrese napadač se prikriva i očekuje prve žrtve napada.[68]

Prikupljanje povjerljivih informacija i njihovo iskorištavanje treća je i završna faza životnoga ciklusa *phishinga*.

U finalnoj fazi napada napadač lažiranim internetskim stranicama prikuplja povjerljive informacije od krajnjih korisnika i pohranjuje ih za kasnije korištenje.

[66] Ibidem.

[67] Ibidem.

[68] Ibidem.

Prikupljeni podatci mogu se iskoristiti za izravno ostvarivanje financijske koristi ili ih je moguće dalje prodavati zainteresiranim osobama. Krajnji je cilj te faze svakako financijska korist.[69]

3.3.7. Socijalni inženjering

Socijalni inženjering tehnika je manipulacije koja iskorištava ljudsku pogrešku za dobivanje privatnih informacija, pristupa ili dragocjenosti. U kibernetičkom kriminalu te prijevare imaju tendenciju namamiti korisnike koji ništa ne sumnjaju u izlaganje podataka, širenje zlonamjernim softverom ili davanje pristupa ograničenim sustavima. Napadi se mogu dogoditi *online*, osobno i drugim interakcijama.[70]

Socijalni inženjering jedan je od rijetkih tipova napada koji se općenito mogu klasificirati kao netehnički napadi, ali se u isto vrijeme može učinkovitije kombinirati s tehničkim tipom napada poput špijunskoga softvera i trojanaca.[71]

Kategorije socijalnoga inženjeringa uključuju:

1. prijevaru temeljenu na računalu ili tehnologiji (pristup temeljen na tehnologiji jest prevariti korisnika da povjeruje da je u interakciji sa stvarnim računalnim sustavom i natjerati ga da pruži povjerljive informacije)
2. ljudsku obmanu (postiže se prijevarom, iskorištavanjem žrtvinoga neznanja i prirodne ljudske sklonosti da bude od pomoći).[72]

Socijalni inženjer ne mora imati nikakvo tehničko znanje o hakiranju ili korištenju bilo kakvih sofisticiranih alata za izvođenje napada. Ljudska manipulacija obavlja se osobno ili medijima poput telefona, e-pošte ili VOIP-a (engl. *Voice over Internet Protocol,*

[69] Ibidem.

[70] Puneeth, M., Farha, J.S., Yamini, M. and Sandhya, N. (2015) Social Engineering on Social Networking Sites. International Journal of Advanced Engineering Research and Science, 2, 57–60.

[71] Costantino, G., La Marra, A., Martinelli, F., Matteucci, I.: Candy: A Social Engineering Attack to Leak Information From Infotainment System, pp. 1–5. IEEE (2018)

[72] Gong, N.Z., Liu, B.: Attribute inference attacks in online social networks. ACM Trans. Privacy Secur. (TOPS) 21(1), 1–30 (2018)

komunikacijska tehnologija koja omogućava telefonske razgovore koristeći prijenos zvučne komunikacije internetom).[73]

Napadi socijalnoga inženjeringa ovise o ljudskim pogreškama pa je sprječavanje sigurnosnih proboja takvim napadima teško.[74]

ETA (engl. *Education, training and awareness raising*, obrazovanje, obuka i podizanje svijesti) primarna je mjera za sprječavanje napada društvenoga inženjeringa koja pomaže poboljšati:

- sigurno rukovanje informacijama
- identificiranje potencijalne napade
- razvitak samopouzdanja za rukovanje tijekom napada.[75]

Takve informacije mogu se dostaviti internetskom stranicom, televizijom, radijem, novinama, društvenim medijima ili SMS-om.

Zajedno s ETA programom pojedinac bi trebao implementirati različite sigurnosne tehnologije koje mogu spriječiti i otkriti potencijalne napade društvenoga inženjeringa tako da se mogu ispravno nositi s njima nakon što se otkriju.[76]

3.4. ALATI ZA INFORMACIJSKU SIGURNOST

Različiti aspekti kibernetičke sigurnosti, uključujući sigurnost aplikacija, informacijsku sigurnost, mrežnu sigurnost, oporavak od katastrofe, operativnu sigurnost i još mnogo toga, neophodni su za pružanje sigurnosti od višestrukih kibernetičkih prijetnji koje su u obliku *Ransomwarea, Malwarea, Phishinga* itd. Stoga alati za informacijsku sigurnost igraju važnu ulogu kada je u pitanju zaštita osjetljivih i privatnih podataka poduzeća, ali i pojedinaca.

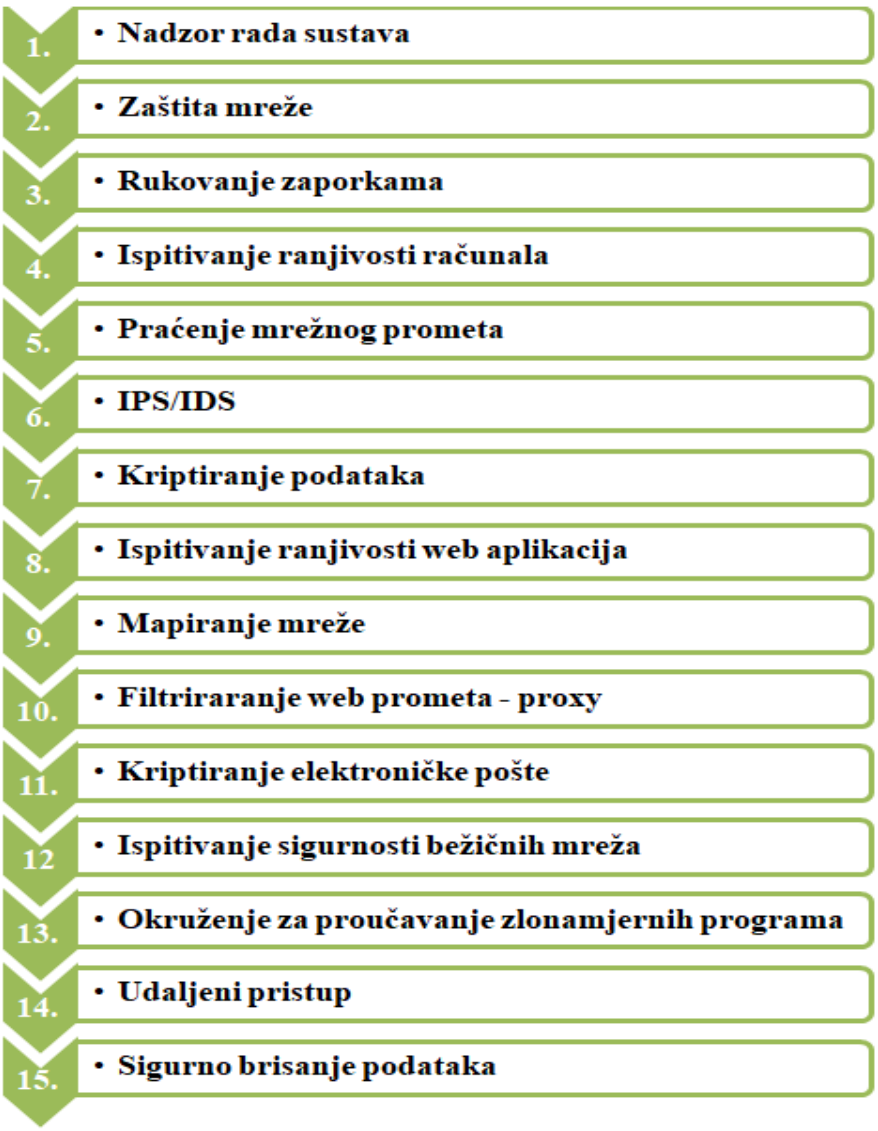
[73] Ibidem.

[74] Joshi, C., Aliaga, J.R., Insua, D.R.: Insider threat modeling: an adversarial risk analysis approach. IEEE Trans. Inf. For. Secur. 16, 1131–1142. (2021).

[75] Ibidem.

[76] Ibidem.

Sigurnosni alati za informacijsku sigurnost su prikazani na slici 5.



Slika 5. Sigurnosni alati za informacijsku sigurnost

Izvor: izrada autorice rada prema https://www.cis.hr/sigurnosni-alati.html (pristupljeno 27. 8. 2022.)

Pod nadzorom rada sustava misli se na automatizirano periodičko provjeravanje i prijavljivanje stanja IT sustava (poslužitelja, mrežne opreme, pisača, VoIP sustava i sl.). Takav nadzor omogućuje pravovremeno otkrivanje anomalija u radu sustava. Nadziranje se može odnositi na bilo koji aspekt rada sustava.[77]

[77] Ibidem.

Bilo da se radi o osnovnim uslugama kao što je plaćanje na daljinu ili upravljanje ugovorom o električnoj energiji, ili o dobrim stvarima kao što su društvene mreže, ili platforme za *online* igranje, korisnici zahtijevaju strogu zaštitu svoje privatnosti, ali i visoku dostupnost informacijskoga sustava i snažnu zaštitu od zlonamjernih napada.[78]

Nadzor mrežne sigurnosti automatizirani je proces koji prati mrežne uređaje i promet radi sigurnosnih ranjivosti, prijetnji i sumnjivih aktivnosti. Organizacije ga mogu rabiti za brzo otkrivanje i reagiranje na povrede informacijske sigurnosti. Softver za nadzor mrežne sigurnosti otkriva i analizira ranjivosti, upozoravajući na moguće sigurnosne probleme. Upozorenja o informacijskoj sigurnosti omogućuju brzu zaštitu organizacije od upada u mrežu i naknadnih problema. Softver za nadzor mrežne sigurnosti prikuplja metriku oko komunikacija klijent – poslužitelj, mrežnoga opterećenja, šifriranih prometnih sesija i drugih mrežnih operacija kako bi otkrio kibersigurnosne prijetnje. Također, moguće je koristiti se softverom za nadzor mrežne sigurnosti za otkrivanje uzoraka u tokovima mrežnoga prometa.[79]

3.5. KONTROLA SIGURNOSTI INFORMACIJSKIH SUSTAVA

Kontrole informacijske sigurnosti mjere su koje se poduzimaju kako bi se smanjili rizici informacijske sigurnosti kao što su povrede informacijskih sustava, krađa podataka i neovlaštene promjene digitalnih informacija ili sustava.

Te sigurnosne kontrole namijenjene su zaštiti dostupnosti, povjerljivosti i integriteta podataka i mreža, a obično se provode nakon procjene rizika informacijske sigurnosti.[80]

Temeljne kontrole informacijske sigurnosti uključuju:

- obavljanje dubinske analize s trećim stranama i poslovnim partnerima koji rukuju osjetljivim podatcima
- praćenje kritičnih sustava u kojima se nalaze osjetljive informacije

[78] https://www.cis.hr/sigurnosni-alati/nadzor-rada-sustava.html (pristupljeno 27. 8. 2022.)

[79] https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html (pristupljeno 27. 8. 2022.)

[80] Ibidem.

- implementiranje enkripcije za kritične poslovne podatke
- opsežan program upravljanja ranjivostima i dobro osmišljen plan odgovora na incidente za brzo prepoznavanje i otklanjanje ranjivosti
- testiranje programa svake godine
- obuku i edukaciju, posebno za one koji su u interakciji s visokorizičnim podatcima, kako bi razumjeli povezane rizike i odgovornosti kao i najbolje prakse za njihovu zaštitu.[81]

Vrste kontrola informacijske sigurnosti uključuju sigurnosne politike, postupke, planove, uređaje i softver namijenjen jačanju informacijske sigurnosti.[82]

[81] https://www.mossadams.com/articles/2021/08/cost-effective-information-security-program#information-security-program (pristupljeno 27. 8. 2022.)

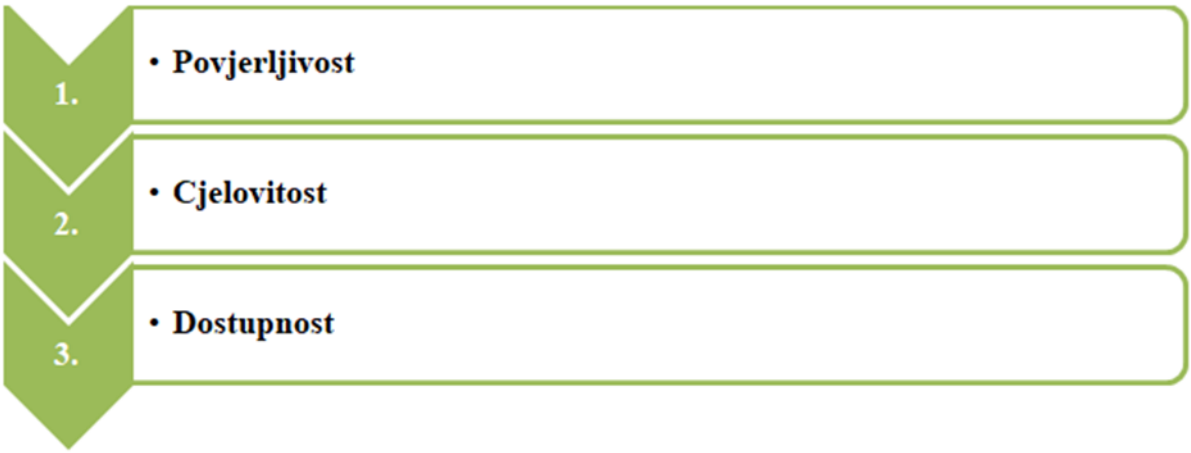
[82] Ibidem.

4. PROGRAMSKE METODE ZAŠTITE INFORMACIJSKIH SIGURNOSTI

Informacijska sigurnost pokriva alate i procese koji se koriste za zaštitu informacija. To uključuje postavke pravila koja sprječavaju neovlaštene osobe da pristupe poslovnim ili osobnim podatcima. Informacijska je sigurnost područje koje raste i razvija se i pokriva širok raspon područja (od sigurnosti mreže i infrastrukture do testiranja i revizije).[83]

Informacijska sigurnost opsežan je i svestran pojam zbog čega je potrebno odrediti aspekte koji karakteriziraju informacijsku sigurnost.[84]

Osnovna načela informacijske sigurnosti prikazana su na slici 6.



Slika 6. Osnovna načela informacijske sigurnosti

Izvor: izrada autorice prema https://www.imperva.com/learn/data-security/information-security-infosec/ (pristupljeno 27. 8. 2022.)

Mjere povjerljivosti osmišljene su kako bi se spriječilo neovlašteno otkrivanje informacija.

[83] Ben, Arfa, Rabai, L., Jouini, M., Ben, Aissa, A., Mili, A., An economic model of security threats for cloud computing systems. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012., str. 102.

[84] Ibidem.

Svrha je načela povjerljivosti zadržati privatnost osobnih podataka i osigurati da budu vidljivi i dostupni samo onim pojedincima koji ih posjeduju ili im trebaju za obavljanje njihovih organizacijskih funkcija.[85]

Glavni aspekti informacijske sigurnosti prikazani su u tablici 2.

Tablica 2. Glavni aspekti informacijske sigurnosti

Povjerljivost	Cjelovitost	Dostupnost
• relevantnost i dosljednost informacija • zaštita od neovlaštenoga mijenjanja i brisanja	• zaštita od neovlaštenoga čitanja podataka	• dostupnost podataka • dostupnost usluga

Izvor: izrada autorice prema https://www.imperva.com/learn/data-security/information-security-infosec/ (pristupljeno 27. 8. 2022.)

Cjelovitost uključuje zaštitu od neovlaštenih promjena (dodavanja, brisanja, izmjena itd.) podataka. Načelo cjelovitosti osigurava da su podatci točni i pouzdani te da se ne mijenjaju.[86]

Dostupnost je zaštita sposobnosti sustava da softverske sustave i podatke učini potpuno dostupnima kada su korisniku potrebni (ili u određeno vrijeme).[87]

Informacijska sigurnost razlikuje se od kibernetičke sigurnosti po opsegu i svrsi. Ta se dva pojma često koriste kao sinonimi, ali, točnije, kibernetička sigurnost potkategorija je informacijske sigurnosti. Informacijska sigurnost široko je područje koje pokriva mnoga područja kao što su fizička sigurnost, sigurnost krajnjih točaka, enkripcija podataka i mrežna sigurnost.

[85] https://www.imperva.com/learn/data-security/information-security-infosec/ (pristupljeno 27. 8. 2022.)

[86] Ibidem.

[87] Ibidem.

Također je usko povezana s informacijskim osiguranjem, koje štiti informacije od prijetnji kao što su prirodne katastrofe i kvarovi poslužitelja.[88]

Informacijska sigurnost ponajprije se bavi prijetnjama povezanima s tehnologijom, s praksama i alatima koji ih mogu spriječiti ili ublažiti. Druga povezana kategorija sigurnost je podataka, koja se usredotočuje na zaštitu podataka organizacije od slučajnoga ili zlonamjernoga izlaganja neovlaštenim stranama.

Program informacijske sigurnosti sastoji se od procesa i mehanizama, uključujući tehničke, administrativne i fizičke zaštitne mjere, osmišljene za zaštitu sigurnosti i funkcionalnosti od bilo kakvih potencijalnih opasnosti i neovlaštenoga pristupa podatcima.

Dobar program informacijske sigurnosti sastoji se od sveobuhvatnoga skupa politika i procedura informacijske sigurnosti.[89]

Sveobuhvatni je cilj informacijske sigurnosti razviti, implementirati i upravljati sigurnosnim programom koji postiže šest osnovnih ishoda učinkovitoga upravljanja sigurnošću:

1. strateško usklađivanje s poslovnom strategijom za podršku organizacijskim ciljevima
2. provođenje odgovarajuće mjere upravljanja rizikom kako bi se zaštitila povjerljivost, integritet i dostupnost kritičnih informacija i sustava
3. optimiziranje i ulaganje u sigurnost za isporuku vrijednosti
4. razvijanje sigurnosne arhitekture za djelotvorno i učinkovito upravljanje resursima infrastrukture
5. praćenje i izvještavanje o procesima informacijske sigurnosti kako bi se osiguralo postizanje ciljeva
6. integriranje relevantnih čimbenika osiguranja kako bi se osiguralo da procesi funkcioniraju kako je predviđeno.[90]

[88] Ibidem.

[89] Ibidem.

[90] https://is.bryant.edu/information-security/information-security-program (pristupljeno 28. 8. 2022.)

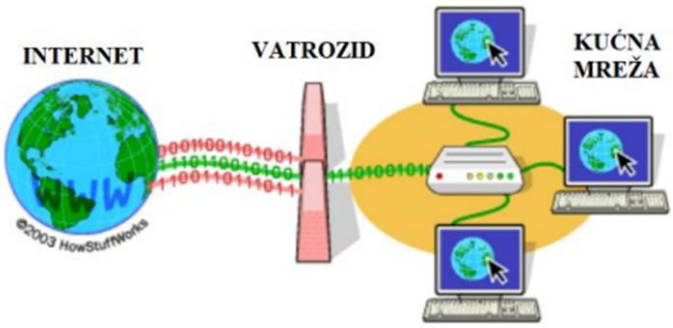
4.1. VATROZID

Vatrozid se definira kao alat za informacijsku sigurnost koji nadzire dolazni i odlazni mrežni promet i dopušta ili blokira pakete podataka na temelju skupa pravila informacijske sigurnosti.[91]

Vatrozid je sigurnosni sustav za blokiranje neovlaštenoga pristupa računalu pri čemu omogućuje komunikaciju s drugim ovlaštenim servisima. Vatrozidi se općenito postavljaju kako bi izolirali mrežne čvorove od izlaznoga i ulaznoga podatkovnog prometa ili čak određenih aplikacija.[92]

Vatrozidi rade koristeći softver, hardver ili metode temeljene na oblaku za zaštitu mreže od bilo kakvoga vanjskog napada. Primarni je cilj vatrozida blokiranje zlonamjernoga prometa i podatkovnih paketa dok dopušta prolazak legitimnoga prometa. Vatrozidi pomno ispituju ulazni promet na temelju unaprijed definiranih sigurnosnih pravila i filtriraju promet koji dolazi iz nezaštićenih ili sumnjivih izvora kako bi spriječili napade. Promet se čuva na ulaznoj točki računala, koja se zove priključci, gdje se informacije zapravo razmjenjuju s vanjskim uređajima.[93]

Funkcije vatrozida na mreži prikazane su na slici 7.



Slika 7. Funkcije vatrozida na mreži

Izvor: obrada autorice prema https://www.comodo.com/resources/home/how-firewalls-work.php (pristupljeno 28. 8. 2022.)

[91] https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/ (14.9.2022.)

[92] https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html (27.9.2022.)

[93] Ibidem.

Za svaki mrežni paket koji napušta ili ulazi u računalnu mrežu vatrozid treba odlučiti hoće li taj paket prihvatiti, odbaciti ili poduzeti neku drugu akciju.

Pravila su definirana tako da bilo koji zaposlenik iz odjela ljudskih resursa ne može pristupiti podatcima s poslužitelja koda, a istovremeno je definirano drugo pravilo kao da administrator sustava može pristupiti podatcima i iz odjela ljudskih resursa i tehničkoga odjela. Pravila se mogu definirati na vatrozidu na temelju potreba i sigurnosnih politika organizacije.[94]

Iz perspektive poslužitelja mrežni promet može biti odlazni ili dolazni. Vatrozid održava poseban skup pravila za oba slučaja.

Uglavnom je dopušten prolaz odlaznoga prometa, koji je potekao sa samoga poslužitelja. Ipak, postavljanje pravila o odlaznom prometu uvijek je bolje kako bi se postigla veća sigurnost i spriječila neželjena komunikacija.

Vatrozidi su mrežne sigurnosne komponente koje upravljaju dolaznim i odlaznim mrežnim prometom na temelju skupa pravila. Proces ispravne konfiguracije vatrozida kompliciran je i sklon pogreškama, a pogoršava se kako mreža raste. Loše konfiguriran vatrozid može dovesti do velikih sigurnosnih prijetnji; u slučaju mrežnoga vatrozida mogla bi biti ugrožena sigurnost organizacije, a u slučaju osobnoga vatrozida ugrožava se sigurnost pojedinoga računala.[95]

4.1.1. Packet filtering

Packet filtering najosnovniji je tip vatrozida koji kontrolira protok podataka prema mreži i iz mreže. To je rješenje za mrežnu sigurnost koje mrežnim paketima omogućuje kretanje između mreža i kontrolira njihov protok pomoću skupa korisnički definiranih pravila, IP adresa, portova i protokola. Paketi se usmjeravaju *Packet filtering* paketom samo ako odgovaraju unaprijed definiranim pravilima filtriranja; inače se odbijaju.[96]

[94] Ibidem.

[95] Ibidem.

[96] https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-packet-filtering-firewall (pristupljeno 10. 9. 2022.)

Glavne su prednosti *Packet filtering* paketa to što su brzi, jeftini i učinkoviti.

Statički filtar paketa nema zamjetan utjecaj na brzinu, a njegovi niski zahtjevi za obradu učinili su ga privlačnom alternativom od samoga početka u usporedbi s drugim vatrozidima koji su usporavali odziv.[97]

Vatrozidi više razine, s druge strane, pružaju izvanredne performanse. Međutim, ne mogu se zaštititi od zlonamjernih paketa podataka koji stižu s pouzdanih izvornih IP-ova jer nemaju potrebnu sposobnost pregleda paketa. Također, budući da nemaju državu, ranjivi su na izvorno usmjeravanje i sitne napade.[98]

Budući da te mreže rastavljaju komunikaciju na male bitove ili pakete i neovisno ih prenose mrežom, mogu biti tolerantne na pogreške. Paketi se mijenjaju kada prođu vatrozidom i stignu na svoje odredište kako bi se njihovi podatci prikazali točnima.[99]

Prebacivanje paketa, kada se provodi učinkovito, povećava kapacitet mrežnoga kanala, smanjuje kašnjenje prijenosa i poboljšava učinkovitost komunikacije. U paketima se mogu naći dvije značajne komponente:

- zaglavlja (zaglavlja paketa koriste se za slanje podataka na ispravno odredište) Sadrže elemente internetskoga protokola, adrese i sve druge informacije potrebne za isporuku paketa na odredište.
- korisni teret (unutar paketa, korisni teret korisnički su podatci)
  To su podatci koji pokušavaju doći do svoga odredišta.

Packet filtering dopušta ili odbija mrežne pakete na temelju sljedećih specifikacija:

- izvorna IP adresa – adresa s koje se paket šalje
- odredišna IP adresa – odredišna adresa paketa
- protokol – protokoli sesije i aplikacije koji se koriste za prijenos podataka
- priključci: izvorni i odredišni priključci i kodovi
- oznake: oznake u TCP (engl. *Transmission control protocol*, protokol kontrole prijenosa) zaglavlju, kao što je je li paket zahtjev za povezivanje
- smjer: dolazni ili odlazni.[100]

[97] Ibidem.

[98] https://www.uio.no/studier/emner/matnat/ifi/IN3210/h19/slides/08-firewalls.pdf (pristupljeno 10. 9. 2022.)

[99] Ibidem.

Kontrola i nadzor mrežnih podataka, kako bi se osigurala njihova valjanost i sukladnost, ključna je uloga *Packet filteringa*. U većini je slučajeva *Packet filtering* učinkovit u obrani od napada s računala izvan interne mreže.[101]

Packet filtering smatra se konvencionalnom i isplativom metodom sigurnosti jer većina uređaja za usmjeravanje ima ugrađene mogućnosti filtriranja.[102]

4.1.2. Application-level gateway

Application-level gateway može obavljati različite funkcije na aplikacijskom sloju infrastrukture. Višestruki pristupnici aplikacija mogu raditi na istom glavnom računalu, ali svaki pristupnik zaseban je poslužitelj sa svojim procesima.[103]

Djeluje na sljedeći način:

- korak 1: korisnik kontaktira s aplikacijskim pristupnikom pomoću TCP/IP aplikacije kao što je HTTP (engl. *Hypertext Transfer Protocol*, protokol prijenosa hiperteksta)
- korak 2: aplikacijski pristupnik pita o udaljenom hostu s kojim korisnik želi uspostaviti vezu; također traži korisnički ID i lozinku koji su potrebni za pristup uslugama pristupnika aplikacije
- korak 3: nakon provjere autentičnosti korisnika pristupnik aplikacije pristupa udaljenom hostu u ime korisnika kako bi isporučio pakete.[104]

Razlike između *Packet filteringa* i *Application-level gatewaya* prikazane su u tablici 3.

---

[100] https://madmuc.usask.ca/Pubs/shw320.pdf (pristupljeno 10. 9. 2022.)

[101] Ibidem.

[102] Ibidem.

[103] https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ag1467936.html (pristupljeno 12. 9. 2022.)

[104] https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/ (pristupljeno 12. 9. 2022.)

Tablica 3. Razlike između *Packet filteringa* i *Application-level gatewaya*

Packet filtering	*Application-level gateway*
najjednostavnije	još složenije
zasloni temeljeni na pravilima povezivanja	zasloni na temelju ponašanja
revizija je teška	aktivnost može revidirati
mali utjecaj na performanse mreže	veliki utjecaj na performanse mreže
mrežna topologija ne može se sakriti	topologija mreže može se sakriti od napadača
transparentno za korisnika	nije transparentno za korisnika
korisnik vidi samo adrese i vrstu servisnoga protokola	korisnik vidi puni podatkovni dio paketa

Izvor: izrada autorice rada prema https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/ (pristupljeno 12. 9. 2022.)

Application-level gateway jedan je od vatrozidnih sustava. Uslugu pružaju različiti procesi koji održavaju potpuno stanje i redoslijed TCP veze.

Prednosti su *Application-level gatewaya*:

- izravne veze između unutarnjih i vanjskih računala nisu dopuštene
- podržana je provjera autentičnosti na razini korisnika
- naredbe aplikacije analiziraju se unutar dijela paketa podataka koji se odnosi na sadržaj.[105]

Nedostatci su *Application-level gatewaya*:

- sporije od filtara paketa
- potrebno je da interni klijent zna za njih
- ne može se podržati svaka moguća vrsta veze.[106]

[105] https://www.careerride.com/nw-application-gateway.aspx (pristupljeno 12. 9. 2022.)

4.1.3. Circuit level gateway

Circuit level gateway vatrozid je koji pruža sigurnost povezivanja protokola korisničkog datagrama i TCP-a te radi između transportnih i aplikacijskih slojeva OSI (engl. *Open Systems Interconnection*, međusobno povezivanje otvorenih sustava) kao što je sloj sesije. Za razliku od *Application-level gatewaya*, *Circuit level gateway* nadzire rukovanje TCP paketa podataka i ispunjavanje sesije pravila i politika vatrozida.[107]

Karakteristike različitih vrsta vatrozida prikazane su u tablici 4.

Tablica 4. Karakteristike različitih vrsta vatrozida

Značajka	*Packet filtering*	*Circuit level gateway*	*Firewall for condition inspection*	*Application-level gatewaya*
provjera odredišta / IP adrese	DA	NE	DA	DA
provjera TCP rukovanja	NE	DA	DA	DA
inspekcija dubokoga sloja	NE	NE	NE	DA
virtualizirana veza	NE	NE	NE	DA
utjecaj resursa	minimalno	minimalno	mali	umjereno

Izvor: izrada autorice rada prema https://www.compuquip.com/blog/characteristics-of-a-circuit-level-gateway (pristupljeno 14. 9. 2022.)

Circuit level gateway provjerava TCP rukovanje kako bi provjerio dolazni promet bez trošenja puno vremena i resursa.

[106] Ibidem.

[107] https://www.techopedia.com/definition/24780/circuit-level-gateway (pristupljeno 12. 9. 2022.)

Međutim, budući da ti vatrozidi ne provjeravaju informacijski paket ili njegov sadržaj, paket koji ima ispravno TCP rukovanje, ali također sadrži zlonamjerni softver, mogao bi proći kroz *Circuit level gateway*.

Važno je napomenuti da se te karakteristike temelje na širokim generalizacijama svakoga rješenja vatrozida.

Razlike između *Packet filteringa, Application-level gatewaya* i *Circuit level gatewaya* prikazane su u tablici 5.

Tablica 5. Razlike između *Packet filteringa, Application-level gatewaya* i *Circuit level gatewaya*

Packet filtering	***Application-level gateway***	***Circuit level gateway***
jednostavan i najmanje siguran	najsigurniji pristup	sigurniji od filtera paketa, ali ne tako siguran kao aplikacijski pristupnik
mnogi usmjerivači pružaju tu funkciju	jedinstveni program za svaku aplikaciju	TCP veze
propušta ili odbija pakete na temelju pravila	dobar za autentifikaciju i zapisivanje	dopuštenje dano adresom priključka
teško upravljati	nije uvijek transparentno za korisnike	nema provjere razine aplikacije
lako je pogriješiti	koristi se za e-poštu	može razumjeti što nosi u paketu

Izvor: izrada autorice rada prema https://www.rfwireless-world.com/Terminology/Application-Gateway-Vs-Circuit-Level-Gateway.html (pristupljeno 14. 9. 2022.)

Glavni je nedostatak vatrozida taj što ne može zaštititi mrežu od napada iznutra.

Circuit level gateway raspoređeni su na sloju sesije OSI modela i nadziru sesije poput TCP trosmjernoga rukovanja kako bi vidjeli je li tražena veza legitimna ili nije. Glavni pregled događa se prije uspostavljanja veze.[108]

Circuit level gateway relativno su jeftini i pružaju anonimnost privatnoj mreži.

Circuit level gateway ne filtriraju pojedinačne pakete. Nakon uspostavljanja veze napadač to može iskoristiti.[109]

4.1.4. Firewall for condition inspection

Firewall for condition inspection prati stanje aktivnih mrežnih veza dok analizira dolazni promet i traži potencijalne prometne i podatkovne rizike.[110]

Firewall for condition inspection prati status veze. Portovi se mogu dinamički otvarati i zatvarati ako je potrebno za dovršetak transakcije. Primjerice, kada se uspostavi veza s poslužiteljem koristeći HTTP, poslužitelj će pokrenuti novu vezu natrag na sustav korisnika na nasumičnom priključku. *Firewall for condition inspection* automatski će otvoriti priključak za tu povratnu vezu.[111]

Firewall for condition inspection smatra se sigurnijima od *Packet filteringa*. *Firewall for condition inspection* obrađuju podatke sloja aplikacije, stoga su u mogućnosti dublje proučiti transakciju kako bi razumjeli što se događa.[112]

Firewall for condition inspection registrira podatke o vezi i strukturira te informacije u tablicu stanja temeljenu na kernelu (računalni program u jezgri operacijskoga sustava računala).

---

[108] Ibidem.

[109] Ibidem.

[110] https://www.fortinet.com/resources/cyberglossary/stateful-firewall (pristupljeno 14. 9. 2022.)

[111] https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/ (pristupljeno 14. 9. 2022.)

[112] Ibidem.

Firewall for condition inspection ispituje zaglavlja paketa i pamti informacije o njima (općenito izvornu/odredišnu IP adresu/portove). Vatrozid zatim koristi te informacije pri obradi paketa.[113]

Firewall for condition inspection najbolja su ravnoteža između performansi filtera paketa i sigurnosti *Application-level gatewaya*.

Ravnoteža između performansi i zaštite između *Packet filteringa* i *Application-level gatewaya* izvrsna je.

Budući da je funkcionalnost pregleda stanja trenutačni standard, većina dobavljača podržava tu vrstu vatrozida i nudi ga u svojoj ponudi.

4.1.5. *The next generation fire*wall

The next generation firewall unutar treće je generacije tehnologije vatrozida, dizajniran za rješavanje naprednih sigurnosnih prijetnji *Application-level gatewaya* putem inteligentnih sigurnosnih značajki svjesnih konteksta. NGFW (engl. *Next-Generation Firewall*, vatrozid sljedeće generacije) kombinira tradicionalne mogućnosti vatrozida kao što su filtriranje paketa i pregled stanja s drugima kako bi se donijele bolje odluke o tome koji promet dopustiti.[114]

The next generation firewall ima mogućnost filtriranja paketa na temelju aplikacija i provjere podataka sadržanih u paketima (umjesto samo njihovih IP zaglavlja).[115]

Specifikacije *The next generation firewall*a razlikuju se ovisno o dobavljaču, ali općenito uključuju neku kombinaciju sljedećih značajki:

- svijest o aplikaciji ili sposobnost filtriranja prometa i primjene složenih pravila na temelju aplikacije (a ne samo na temelju priključka) – je ključna značajka *The next generation firewalla*, oni mogu blokirati promet iz određenih aplikacija, kao i održavati veću kontrolu nad pojedinačnim aplikacijama

[113] Ibidem.

[114] https://www.vmware.com/topics/glossary/content/next-generation-firewall.html (pristupljeno 14. 9. 2022.)

[115] Ibidem.

- dubinska inspekcija paketa, koja provjerava podatke sadržane u paketima – poboljšanje u odnosu na tradicionalnu tehnologiju vatrozida, koja je pregledavala samo IP zaglavlje paketa kako bi odredila njegov izvor i odredište
- IPS (engl. *Intrusion Prevention System,* sustav za sprječavanje upada) koji nadzire mrežu zbog zlonamjernih aktivnosti i blokira ih tamo gdje se pojave. To praćenje može se temeljiti na potpisima (usklađivanje aktivnosti s potpisima dobro poznatih prijetnji), na temelju pravila (aktivnost blokiranja koja krši sigurnosna pravila) ili na temelju anomalija (nadziranje abnormalnog ponašanja).
- visoke performanse, koje vatrozidu omogućuju praćenje velikih količina mrežnoga prometa bez usporavanja – uključuju niz sigurnosnih značajki koje zahtijevaju vrijeme obrade, stoga su visoke performanse važne kako bi se izbjeglo ometanje poslovnih operacija
- vanjsko obavještavanje o prijetnjama ili komunikacija s mrežom za obavještavanje o prijetnjama kako bi se osiguralo da su informacije o prijetnjama ažurne i pomoglo u identificiranju loših aktera.[116]

Uz navedene temeljne značajke *The next generation firewall* mogu sadržavati dodatne značajke kao što su zaštita od virusa i zlonamjernoga softvera.[117]

The next generation firewall pružaju mnogo bolju i snažniju sigurnost od tradicionalnoga vatrozida.

Tradicionalni vatrozidi ograničeni su u svojim mogućnostima: oni mogu blokirati promet određenim priključkom, ali ne mogu primijeniti pravila specifična za aplikaciju, zaštititi od zlonamjernoga softvera ili otkriti i blokirati nenormalno ponašanje. Kao rezultat toga napadači mogu izbjeći otkrivanje ulaskom kroz nestandardni port, nešto što bi *The next generation firewall* spriječio.[118]

[116] Ibidem.

[117] https://www.fortinet.com/products/next-generation-firewall (27.9.2022.)

[118] Ibidem.

Zahvaljujući svojoj prirodi koja je svjesna konteksta i sposobnosti primanja ažuriranja od vanjskih mreža za obavještavanje o prijetnjama, *The next generation firewall* mogu zaštititi od širokoga niza naprednih prijetnji koje se neprestano mijenjaju, a mogu čak koristiti i inteligentnu automatizaciju za održavanje sigurnosnih politika do danas bez potrebe za intervencijom zaposlenog IT osoblja.[119]

The next generation firewall nude poboljšanu sigurnosnu infrastrukturu koju je lakše i jeftinije održavati, ažurirati i kontrolirati. Oni kombiniraju nekoliko sigurnosnih značajki u jedno rješenje i prijavljuju incidente jednim sustavom izvješćivanja.

Alternativa održavanja mnogo različitih sigurnosnih proizvoda dodatno opterećuje IT osoblje i povećava mogućnost za proboje sigurnosti.[120]

Tradicionalni vatrozidi oslanjaju se na inspekciju porta/protokola i blokiranje kako bi zaštitili poslovne mreže na podatkovnoj vezi i transportnim slojevima.

Taj statični pristup bio je učinkovit u prošlosti, kada je IT okruženje bilo manje dinamično nego što je sada, a aplikacije su se mogle identificirati prema priključku. Ali s rastućom složenošću virtualiziranih mreža i naprednijim sigurnosnim prijetnjama, to više nije dovoljno. *The next generation firewall* pametniji je, može filtrirati pakete na temelju aplikacije, pa čak i na temelju ponašanja, čineći precizne razlike koje su daleko učinkovitije od generičkih metoda koje koriste tradicionalni vatrozidi. Također se poziva na vanjske podatke kako bi identificirao prijetnje. Taj dinamičan, fleksibilan pristup omogućuje mu prepoznavanje i obranu od napadača koji su mnogo sofisticiraniji nego u prošlosti.[121]

Ciljane i sofisticirane sigurnosne prijetnje uzrokuju više štete internim mrežama nego ikad prije. Tradicionalne tehnologije vatrozida uvelike se oslanjaju na inspekciju porta/protokola, što je neučinkovito u virtualiziranom okruženju gdje se adrese i portovi dodjeljuju dinamički.

---

[119] https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/ (pristupljeno 14. 9. 2022.)

[120] Ibidem.

[121] Ibidem.

4.2. VIRTUALNA PRIVATNA MREŽA (VPN)

VPN (engl. *Virtual private network,* virtualna privatna mreža) pruža *online* privatnost i anonimnost stvaranjem privatne mreže iz javne internetske veze. VPN-ovi maskiraju adresu IP-a (engl. *Internet protocol,* internetski protokol) tako da se *online* radnjama gotovo ne može ući u trag.[122]

VPN usluge uspostavljaju sigurne i šifrirane veze kako bi pružile veću privatnost čak i od zaštićene Wi-Fi pristupne točke.

VPN je računalna mreža u kojoj se veze između njezinih čvorova koriste javnim mrežama (internet/WAN) jer u određenim slučajevima ili uvjetima ne dopuštaju izgradnju vlastite infrastrukture. Kada se VPN poveže, međupovezanost između čvora kao što je neovisna mreža koja je zapravo stvorila posebnu liniju prolazi kroz vezu ili javnu mrežu.

Na svakom mjestu tvrtke, radnim stanicama, poslužiteljima i bazama podataka povezanih jednom ili više lokalnih mreža (LAN – engl. *Local area network,* lokalna mreža), LAN je pod kontrolom mrežnoga upravitelja i može se konfigurirati i podesiti za isplativost.[123]

Internet ili druge javne mreže mogu se koristiti za povezivanje stranica, uštedu troškova u odnosu na korištenje privatnih mreža i smanjenje opterećenja širokopojasnoga mrežnog prometa pružateljima javnih mreža.[124]

Postoje dvije vrste VPN-a:

- VPN s udaljenim pristupom
- VPN od mjesta do mjesta.[125]

VPN s udaljenim pristupom naziva se i virtualna *dial-up* mreža (VPDN). VPDN je vrsta veze korisnik-na-LAN, veze koja povezuje mobilnoga korisnika s lokalnom mrežom (LAN). To znači da korisnik može pristupiti privatnoj mreži s bilo kojega mjesta.

[122] Ibidem.

[123] Ibidem.

[124] Riadi, I., Network Security Optimization using Microtic Based Application Filtering Introduction Theoretical Basis, JUSI, Universitas Ahmad Dahlan Yogyakarta, vol. 1, no. 1, pp. 71–80, 2011.

[125] Ibidem.

Taj VPDN obično rabe zaposlenici koji su izvan ureda i zahtijevaju vezu s mrežom ureda tvrtke.[126]

Site-to-site VPN je koji se koristi za povezivanje različitih područja koja su već popravljena, taj uređaj koji koristi namjenski VPN povezan je internetom. *Site-to-site* VPN podijeljen je na dva dijela:

- ekstranet
- intranet.[127]

Intranet je mjesto gdje se VPN koristi samo za povezivanje raznih lokacija koje su ipak jedna agencija ili jedna tvrtka, kao što je središnji ured povezan s ispostavom.

Ekstranet je mjesto gdje se VPN koristi za povezivanje tvrtke s drugim tvrtkama, poput partnera, dobavljača ili kupaca. Drugim riječima, administrativna je kontrola pod kontrolom neke od nadležnih agencija.[128]

Sigurnost računalnih mreža definirana je kao zaštita resursa od napora promjene i uništavanja uzrokovanih od strane nekoga tko nije dopušten, dvije su stvari koje su povezane sa sigurnošću i povjerljivošću podataka u računalnim mrežama, a to su reprezentacija podataka i kompresije podataka, što se kasnije povezivalo s problemom enkripcije.[129]

Sigurnost računalnih mreža zaštita je koja se pruža automatskom informacijskom sustavu radi postizanja cilja, odnosno održavanja dostupnosti, integriteta i povjerljivosti.[130]

[126] Ibidem.

[127] Ibidem.

[128] Kristanto, A., Computer Network, Graha Ilmu, Yogyakarta, 2003.

[129] Ibidem.

[130] Stallings, W., Cryptography and Network Security Principle and Practice, 5th Edition, Pearson Education, 2011.

4.3. SUSTAVI ZA OTKRIVANJE NAPADA (IDS)

IDS-ovi (engl. *Intrusion detection system*, sustav za detekciju upada) softver su koji nadziru računalne mreže radi otkrivanja zlonamjernih aktivnosti poput krađe informacija, cenzuriranja ili razbijanja mrežnih protokola.

IDS-ovi se široko koriste za otkrivanje i poznatih i nepoznatih napada na mreže od unutarnjih i vanjskih napadača. Većina tehnika koje se koriste u današnjem IDS-u ne može se nositi s dinamičnom i složenom prirodom kibernetičkih napada u računalnim mrežama.[131]

Detekcija upada operacija je praćenja događaja na mrežnom/računalnom sustavu i njihova analiza radi upozorenja o potencijalnim događajima kao što su prijetnje ili kršenja pravila korištenja ili standardne sigurnosne prakse.

IDS se uglavnom usredotočuje na otkrivanje potencijalnih događaja, bilježenje informacija o tim događajima i izvješćivanje o snimljenim informacijama sigurnosnim administratorima. Osim toga IDS-ovi se koriste za druge ciljeve kao što je otkrivanje problema u sigurnosnim politikama, prijavljivanje postojećih prijetnji i odvraćanje pojedinaca od sigurnosnih napada.[132]

Za učinkovit IDS-a komponente moraju biti pravilno osigurane. IDS se sastoji od različitih komponenti uključujući korisnike, senzore, poslužitelje baze podataka, poslužitelje za upravljanje i mreže. Osiguranje komponenti IDS-a ključno je jer su na meti napadača koji žele spriječiti IDS-ove u pristupu važnim informacijama, poznatim ranjivostima ili otkrivanju napada.[133]

Operativni sustavi i aplikacije svih komponenti moraju biti ažurni, a sve komponente IDS-a temeljene na softveru moraju biti zaštićene od prijetnji.

---

[131] Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., Survey of intrusion detection systems: Techniques datasets and challenges, Cybersecurity, vol. 2, no. 1, pp. 1–22.

[132] Ibidem.

[133] Biermann, E., Cloete, E. and Venter, L. M., A comparison of intrusion detection systems, Comput. Secur., vol. 20, no. 8, pp. 676–683

Također, može biti opcija korištenja više IDS tehnologija za sveobuhvatno i visokoprecizno otkrivanje napada. Postoje različite IDS tehnologije koje se koriste kao što su mrežne, bežične i *host-based*. Svaki od njih nudi fundamentalno različite mogućnosti prikupljanja informacija, snimanja, detekcije i prevencije. Nadalje, svaka tehnologija nudi prednosti kao što je učinkovitije otkrivanje određenih događaja ili otkrivanje s većom točnošću. Na primjer, IDS-ovi koji se temelje na hostu i koji se temelje na mreži mogu se integrirati kako bi pružili učinkovito rješenje. Pri odabiru IDS tehnologija treba uzeti u obzir različite karakteristike i prednosti svake tehnologije.[134]

Postoje neki važni čimbenici za učinkovito rješavanje napada pri primjeni IDS tehnologija:

- trajnost/pouzdanost sustava
- brzo otkrivanje
- minimalni broj lažno pozitivnih rezultata
- maksimalna stopa detekcije
- minimalna upotreba softvera/hardvera
- sposobnost točnog otkrivanja mjesta upada
- sposobnost rada s drugim tehnologijama.[135]

Detekcija upada proces je promatranja događaja koji se događaju u računalnom sustavu ili mreži i analiziranja tih događaja radi utvrđivanja upada. Postoje razne prijetnje uključujući zlonamjerni softver, DoS-DDoS napade, neovlašteni pristup, eskalaciju privilegija ili probni napad.

Iako su mnogi događaji koji se čine štetnim za sustav doista napadi, postoje neke iznimke; na primjer, korisnik može pogrešno upisati adresu računala ili se nesvjesno spojiti na krivi sustav. Sustav mora ispravno odvojiti upade od normalnoga mrežnog prometa.

Zaključno, IDS je softver koji pojednostavljuje i automatizira proces otkrivanja napada.

[134] Ibidem.

[135] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández and E. Vázquez, G., Anomaly-based network intrusion detection: Techniques systems and challenges, Comput. Secur., vol. 28, no. 1, pp. 18-28, Feb. 2009.

4.4. SUSTAVI ZA ZAŠTITU OD PROVALE (IPS)

Računalni sustavi suočavaju se s najvećom prijetnjom u obliku zlonamjernih podataka koji uzrokuju uskraćivanje usluge, krađu informacija, financijski gubitak i gubitak vjerodostojnosti itd. Nijedna obrambena tehnika nije se pokazala uspješnom u rješavanju ovih prijetnji. IDPS sustavi (engl. *Intrusion detection and prevention systems*, sustavi za otkrivanje i prevenciju upada) najbolje su od dostupnih rješenja.[136]

Te tehnike dobivaju sve više pozornosti. Iako IPS (engl. *Intrusion Prevention Systems*, sustavi za sprječavanje upada) pokazuju dobru razinu uspjeha u otkrivanju i sprječavanju pokušaja upada u mreže, pokazuju vidljiv nedostatak u svojim performansama kada se koriste na brzim mrežama.[137]

IPS je ponajprije obrambeni sustav temeljen na mreži s povećanjem globalne mrežne povezanosti i kombinira tehniku vatrozida s onom IDS-a ispravno s proaktivnom tehnikom. Taj je sustav proaktivna tehnika koja sprječava napade prije ulaska u mrežu ispitivanjem različitih zapisa podataka i detektira senzor za prepoznavanje uzorka ponašanja. Kada se identificira napad, sprječavanje upada blokira i bilježi uvredljive podatke.[138]

Trenutačno je postao neophodan zahtjev za sustavom koji osigurava rano otkrivanje/upozorenje od kršenja sigurnosti upada temeljenoga na znanju. Stoga sustav mora biti aktivan i pametan u klasificiranju i razlikovanju paketnih podataka, ako se otkriju neobični ili nestašni podatci, aktivira se upozorenje i izvršava se odgovor na događaj. Taj se mehanizam aktivira da prekine ili omogući obradu paketnih podataka povezanih s događajem. Sprječava napad prije ulaska u mrežu ispitivanjem različitih zapisa podataka i sprječava ponašanje prepoznavanja uzoraka.[139]

[136] https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips (20.8.2022.)

[137] Ibidem.

[138] https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/ (20.8.2022.)

[139] Ibidem.

4.5. INFRASTRUKTURA JAVNOGA KLJUČA (PKI)

PKI (engl. *Public key infrastructure*, infrastruktura javnih ključeva) upravlja izdavanjem digitalnih certifikata za zaštitu osjetljivih podataka, pružanje jedinstvenih digitalnih identiteta za korisnike, uređaje i aplikacije te sigurnu komunikaciju.[140]

Ovi PKI certifikati provjeravaju vlasnika privatnoga ključa i autentičnost toga odnosa u budućnosti kako bi pomogli u održavanju sigurnosti. Potvrde su slične vozačkoj dozvoli ili putovnici za digitalni svijet.

Najčešći oblik enkripcije koji se danas koristi uključuje javni ključ, koji svatko može rabiti za šifriranje poruke, i privatni ključ (također poznat kao tajni ključ), kojim bi se samo jedna osoba trebala moći koristiti za dešifriranje tih poruka. Te ključeve mogu koristiti ljudi, uređaji i aplikacije.[141]

Kriptografski algoritmi definirane su, vrlo složene matematičke formule koje se koriste za šifriranje i dešifriranje poruka. Oni su također sastavni dijelovi PKI autentifikacije. Ti algoritmi variraju ovisno o složenosti.[142]

Simetrična enkripcija jednostavan je kriptografski algoritam prema današnjim standardima, no nekada se smatrala vrhunskom tehnologijom. Njemačka vojska rabila ga je za slanje privatnih komunikacija tijekom Drugoga svjetskog rata.[143]

Uz simetričnu enkripciju poruka koja se upisuje kao običan tekst prolazi kroz matematičke permutacije da bi postala šifrirana. Šifriranu je poruku teško razbiti jer isto slovo običnoga teksta ne izlazi uvijek isto u šifriranoj poruci. Na primjer, poruka „HHH“ ne bi bila šifrirana s tri ista znaka.[144]

Za šifriranje i dešifriranje poruke potreban je isti ključ, otuda i naziv simetrična enkripcija.

---

[140] https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm (pristupljeno 28. 8. 2022.)

[141] https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki (pristupljeno 28. 8. 2022.)

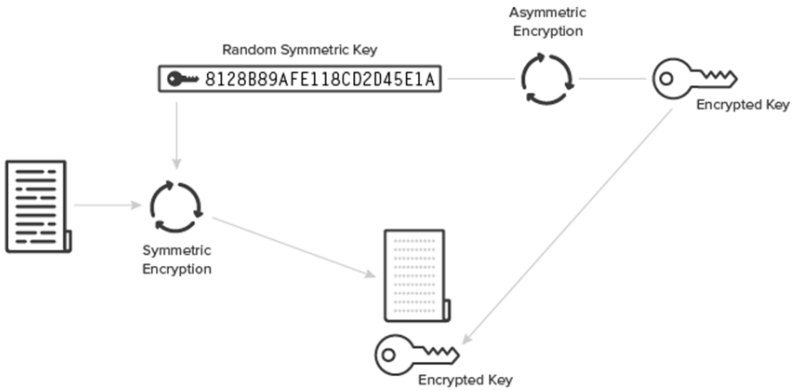
[142] Ibidem.

[143] Ibidem.

[144] Ibidem.

Iako je dešifriranje poruka iznimno teško bez ključa, činjenica da se isti ključ mora koristiti za šifriranje i dešifriranje poruke nosi značajan rizik. To je zato što ako distribucijski kanal koji se koristi za dijeljenje ključa bude ugrožen, cijeli je sustav za sigurne poruke pokvaren.[145]

Simetrična i asimetrična enkripcija prikazana je na slici 8.



Slika 8. Simetrična i asimetrična enkripcija

Izvor: https://www.keyfactor.com/resources/what-is-pki/ (pristupljeno 28. 8. 2022.)

Danas se često koriste i simetrična i asimetrična enkripcija. Asimetrična enkripcija puno je sporija od simetrične enkripcije, pa se njih dvije često koriste paralerno. Na primjer, netko može šifrirati poruku pomoću simetrične enkripcije i zatim poslati ključ za dešifriranje poruke pomoću asimetrične enkripcije (koja ubrzava proces dešifriranja jer je ključ puno manji od cijele poruke).[146]

[145] Ibidem.

[146] https://www.keyfactor.com/resources/what-is-pki/ (pristupljeno 28. 8. 2022.)

5. SUSTAV UPRAVLJANJA I REVIZIJE INFORMACIJSKIH SUSTAVA

Učinkovitost kontrole informacijskoga sustava ocjenjuje se revizijom informacijskoga sustava. Revizija ima cilj utvrditi štite li informacijski sustavi korporativnu imovinu, održavaju li integritet pohranjenih podataka, podupiru li učinkovito korporativne ciljeve i djeluju li učinkovito. To je dio financijske revizije koja provjerava računovodstvenu evidenciju i financijska izvješća organizacije. Informacijski sustavi dizajnirani su tako da se može pratiti svaka financijska transakcija.[147]

Treba postojati revizijski trag koji može utvrditi odakle je svaka transakcija nastala i kako je obrađena. Osim financijskih revizija operativnim se procjenjuje učinkovitost rada informacijskih sustava, a tehnološkim se revizijama provjerava jesu li informacijske tehnologije pravilno odabrane, konfigurirane i implementirane.[148]

Revizije se obično koriste kako bi se osiguralo da aktivnost zadovoljava skup definiranih kriterija. Za sve standarde ISO sustava upravljanja revizije se koriste kako bi se osiguralo da sustav upravljanja zadovoljava potrebne zahtjeve i relevantne norme, zahtjeve pojedinca i ciljeve organizacije te da ostaje učinkovit.[149]

Kako bi mjere informacijske sigurnosti bile eksplicitne, potrebne su pisane norme. Te su norme poznate kao standardi informacijske sigurnosti: generički skupovi propisa za idealno izvršenje određenih mjera. Standardi mogu uključivati metode, smjernice, referentne okvire itd.[150]

Osiguravaju učinkovitost sigurnosti, olakšavaju integraciju i interoperabilnost, omogućuju smislenu usporedbu mjera, smanjuju složenost i osiguravaju strukturu za novi razvoj.[151]

---

[147] https://www.britannica.com/topic/information-system/Information-systems-audit (pristupljeno 19. 9. 2022.)

[148] Ibidem.

[149] https://info-savvy.com/iso-27001-annex-a-12-7-information-systems-audit-considerations/ (pristupljeno 19. 9. 2022.)

[150] Ibidem.

[151] Ibidem.

Sigurnosni je standard „objavljena specifikacija koja uspostavlja zajednički jezik, sadrži tehničku specifikaciju ili druge precizne kriterije i dizajniran je da se koristi dosljedno, u pravilu, kao smjernica ili definicija."

Cilj je sigurnosnih standarda poboljšati sigurnost sustava informacijske tehnologije, mreža i infrastruktura. Dobro napisani standardi informacijske sigurnosti omogućuju dosljednost među razvojnim programerima i služe kao pouzdan standard za kupnju sigurnosnih proizvoda.

ISO je kratica za Međunarodnu organizaciju za standardizaciju. Međunarodni standardi omogućuju da stvari funkcioniraju. Ti standardi daju specifikaciju svjetske klase za proizvode, usluge i računala kako bi se osigurala kvaliteta, sigurnost i učinkovitost. Oni su ključni u olakšavanju međunarodne trgovine.[152]

ISO norma službeno je uspostavljena 23. veljače 1947. To je neovisna, nevladina međunarodna organizacija. Danas ima članstvo od 162 nacionalna tijela za normizaciju i 784 tehnička odbora i pododbora koji se brinu o razvoju normi. ISO je objavio više od 22 336 međunarodnih normi i srodnih dokumenata koji pokrivaju gotovo svaku industriju, od informacijske tehnologije, preko sigurnosti hrane, do poljoprivrede i zdravstvene zaštite.

ISO/IEC 27001 nadaleko je poznat jer pruža zahtjeve za ISMS (engl. *Information security management system*, sustav upravljanja sigurnošću informacija) iako postoji više od desetak standarda u području ISO/IEC 27000. Njihova uporaba omogućuje organizacijama bilo koje vrste da upravljaju sigurnošću imovine kao što su financijski podatci, intelektualno vlasništvo, podatci o zaposlenicima ili informacije koje su povjerile treće strane.[153]

Standard zahtijeva da organizacija planira i provodi raspored „internih revizija" kako bi bila u skladu sa standardom. Ako organizacija želi postići certifikaciju, zahtijevat će „vanjske revizije" koje provodi „certifikacijsko tijelo", organizacija s kompetentnim resursima za reviziju prema ISO 27001.[154]

[152] https://www.techtarget.com/searchdatacenter/definition/ISO (20.8.2022.)

[153] Ibidem.

[154] Ibidem.

Kriteriji revizije i aktivnosti vezane uz provjeru operativnoga sustava trebaju biti pozorno pripremljeni kako bi se smanjili poremećaji poslovnih procesa. Potrebno je slijediti sljedeće smjernice:

- o revizijskim standardima za pristup sustavima i podatcima treba pregovarati s odgovarajućim menadžmentom
- opseg bi trebao biti dogovoren i kontroliran na testovima tehničke revizije
- obrada revizije trebala bi biti ograničena na pristup aplikacijama i podatcima samo za čitanje
- pristup, a ne samo za čitanje, trebao bi biti dopušten samo za izolirane kopije sistemskih datoteka, koje bi se trebale izbrisati kada je revizija dovršena, ili bi im trebalo osigurati odgovarajuću sigurnost ako je potrebno da se takve datoteke čuvaju u skladu sa zahtjevima za reviziju dokumentiranja
- potrebno je definirati i odlučiti o kriterijima za posebnu ili dodatnu obradu
- testovi revizije koji bi mogli utjecati na dostupnost sustava trebali bi se provoditi izvan radnog vremena
- kako bi se stvorio referentni trag, sav pristup treba biti kontroliran i zapisan.[155]

Organizacija određuje zainteresirane strane relevantne za ISMS i njihove zahtjeve relevantne za informacijsku sigurnost.

Opseg informacijske sigurnosti definira gdje je i za što točno ISMS primjenjiv te gdje i za što nije. Uspostava opsega stoga je ključna aktivnost koja određuje potrebne temelje za sve ostale aktivnosti u okviru implementacije ISMS-a.

Precizno poznavanje granica i primjenjivosti ISMS-a, a time i sučelja i ovisnosti između organizacije i drugih organizacija također je kritično. Sve kasnije izmjene opsega mogu rezultirati znatnim dodatnim naporima i troškovima.[156]

[155] https://info-savvy.com/iso-27001-annex-a-12-7-information-systems-audit-considerations/ (pristupljeno 19. 9. 2022.)

[156] https://info-savvy.com/iso-27001-implementation-guideline-clause-4-3-determining-the-scope-of-the-information-security-management-system/ (pristupljeno 19. 9. 2022).

6. ZAKLJUČAK

Sigurnost je informacijskih sustava zaštita računalnih sustava i mreža od otkrivanja informacija, krađe ili oštećenja njihova hardvera, softvera ili elektroničkih podataka kao i od prekida ili kvara usluga koje pružaju. Sigurnost znači imati sredstva za smanjenje ranjivosti informacija i resursa koliko god je to moguće. Iako se stopostotna sigurnost ne može postići, težnja bi trebala biti postizanje te vrijednosti.

Informacijska sigurnost ima cilj zaštititi podatke. Trebalo bi biti moguće osigurati da samo ovlašteni korisnici imaju pristup tim podatcima i da ne može doći do neovlaštenoga i nekontroliranoga pristupa. Kako bi se to moglo jamčiti, moraju se postići zaštitni ciljevi informacijske sigurnosti. Povjerljivost znači da podatke mogu pregledavati i upravljati samo ovlašteni i opunomoćeni korisnici. Povjerljivost je vjerojatno prvi element povezan sa sigurnošću informacija. Podatci se smatraju povjerljivim ako samo ovlaštene osobe imaju pristup podatcima. Integritet je namijenjen za sprječavanje neprimjetne promjene i manipulacije podatcima. Dostupnost je zaštita sposobnosti sustava da podatke, aplikacije i tehnološku infrastrukturu učini dostupnima kada su potrebni za klijente ili organizacijski proces.

Napadi su na informacijski sustav, nažalost, sve češći. Pod napadima na informacijski sustav podrazumijevaju se svi neovlašteni pristupi sustavu ili mreži. *Malware* je jedan od najčešćih napada na informacijske sustave, a odnosi se na zlonamjerne softverske viruse uključujući crve, *spyware*, *ransomware*, *adware* i trojance. Trojanski virus prerušava se u legitiman softver. *Ransomware* blokira pristup ključnim komponentama mreže, dok je *Spyware* softver koji krade sve povjerljive podatke bez znanja korisnika. *Adware* je softver koji prikazuje reklamni sadržaj kao što su natpisi na zaslonu korisnika. *Phishing* napadi jedan su od najistaknutijih raširenih tipova napada na informacijske sustave. To je vrsta napada društvenoga inženjeringa u kojem se napadač lažno predstavlja kao pouzdani kontakt i žrtvi šalje lažnu e-poštu. SQL napadi događaju se na internetskoj stranici koja se temelji na bazi podataka kada haker manipulira standardnim SQL upitom. Napad se događa ubacivanjem zlonamjernoga koda u okvir za pretraživanje internetske stranice čime poslužitelj otkriva ključne informacije.

Ispravno implementirane, učinkovite strategije sigurnosti podataka štite informacijsku imovinu od potencijalnoga napada, ali i štite od prijetnji iznutra i ljudske pogreške, koje su i danas među vodećim uzrocima povrede podataka.

Sigurnost podataka uključuje implementaciju alata i tehnologija. U idealnom slučaju ti bi alati trebali moći provoditi zaštitu poput enkripcije i maskiranja podataka.

Navedenim zaključcima i cjelokupnim radom dokazana je hipoteza postavljena na početku rada da se pojavom sofisticiranijih napada stvara velika potreba za sigurnošću podataka te se teži većoj razini zaštite informacijskih sustava. Najčešći oblik kojim se štite podatci su programske metode zaštite informacijskoga sustava, a one mogu biti na razini operacijskoga sustava ili na razini korisničkih programa.

LITERATURA

POPIS KNJIGA

1. Pavlić, M.: **Informacijski sustavi**, Školska knjiga, Zagreb, 2011.

POPIS ČLANAKA:

1. Ben, Arfa, Rabai, L., Jouini, M., Ben, Aissa, A., Mili, A., An economic model of security threats for cloud computing systems. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012. 100–105.
2. Biermann, E., Cloete, E. and Venter, L. M., A comparison of intrusion detection systems, Comput. Secur., vol. 20, no. 8, pp. 676–683
3. Costantino, G., La Marra, A., Martinelli, F., Matteucci, I.: Candy: A Social Engineering Attack to Leak Information From Infotainment System, pp. 1–5. IEEE (2018)
4. Ekclhart, A., Fenz, S., Goluch, G., Weippl, E. Ontological mapping of common criteria's security assurance requirements IFIP International Information Security Conference, Springer, 2007.
5. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández and E. Vázquez, G., Anomaly-based network intrusion detection: Techniques systems and challenges, Comput. Secur., vol. 28, no. 1, pp. 18-28, Feb. 2009.
6. Geric, S., Hutinski, Z., Information system security threats classifications. Journal of Information and Organizational Sciences, 2007.
7. Gong, N.Z., Liu, B.: Attribute inference attacks in online social networks. ACM Trans. Privacy Secur. (TOPS) 21(1), 1–30 (2018)
8. Joshi, C., Aliaga, J.R., Insua, D.R.: Insider threat modeling: an adversarial risk analysis approach. IEEE Trans. Inf. For. Secur. 16, 1131–1142 (2021).
9. Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J., Survey of intrusion detection systems: Techniques datasets and challenges, Cybersecurity, vol. 2, no. 1, pp. 1–22.

10. Kim, H., K., Kim, T., H., Kim J., Reliability assurance in development process for TOE on the common criteria International Conference on Software Engineering Research and Applications, Springer, 2003.
11. Kristanto, A.., Computer Network, Graha Ilmu, Yogyakarta, 2003.
12. Loch, K., Carr, H., Warkentin, M., Threats to Information Systems, Today's Reality, Yesterday's Understanding, Management Information Systems Quarterly 16.2, 1992.
13. Maidl, M., Von, Oheimb, D., Hartmann, P., Robinson, R., Formal security analysis of electronic software distribution systems International Conference on Computer Safety, Reliability, and Security, Springer, 2008.
14. Puneeth, M., Farha, J.S., Yamini, M. and Sandhya, N. (2015) Social Engineering on Social Networking Sites. International Journal of Advanced Engineering Research and Science, 2, 57–60.
15. Riadi, I., Network Security Optimization using Microtic Based Application Filtering Introduction Theoretical Basis, JUSI, Universitas Ahmad Dahlan Yogyakarta, vol. 1, no. 1, pp. 71–80, 2011.
16. Stallings, W., Cryptography and Network Security Principle and Practice, 5th Edition, Pearson Education, 2011.
17. Zwass, V.. "expert system." Encyclopedia Britannica, February 10, 2016. https://www.britannica.com/technology/expert-system.

MREŽNI IZVORI:

18. *Application-level gateway*, dostupno na: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ag1467936.html (12. 9. 2022.)
19. *Circuit level gateway*, dostupno na: https://www.techopedia.com/definition/24780/circuit-level-gateway (12. 9. 2022.)
20. *DdoS* napadi, dostupno na: https://www.imperva.com/learn/ddos/ddos-attacks/ (26. 8. 2022.)
21. Dodatak ISO 27001: A.12.7 Razmatranja revizije informacijskih sustava, dostupno na: https://info-savvy.com/iso-27001-annex-a-12-7-information-systems-audit-considerations/ (19. 9. 2022.)

22. Dodatak ISO 27001: A.12.7 Razmatranja revizije informacijskih sustava, dostupno na: https://info-savvy.com/iso-27001-annex-a-12-7-information-systems-audit-considerations/ (19. 9. 2022.)
23. *Doxing*, dostupno na: https://www.kaspersky.com/resource-center/definitions/what-is-doxing (20. 8. 2022.)
24. Filtriranje paketa vatrozidom, dostupno na: https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-packet-filtering-firewall (10. 9. 2022.)
25. Filtriranje paketa, dostupno na: https://madmuc.usask.ca/Pubs/shw320.pdf (10. 9. 2022.)
26. *Firewall for condition inspection*, dostupno na: https://www.fortinet.com/resources/cyberglossary/stateful-firewall (14. 9. 2022.)
27. *Firewall*, dostupno na: https://www.spiceworks.com/it-security/network-security/articles/what-is-firewall-definition-key-components-best-practices/ (14. 9. 2022.)
28. IPS, dostupno na: https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/ (20.8.2022.)
29. ISO standardi, dostupno na: https://www.techtarget.com/searchdatacenter/definition/ISO (20.8.2022.)
30. Karakteristike razčičitih vrsta vatrozida, dostupno na: https://www.compuquip.com/blog/characteristics-of-a-circuit-level-gateway (14. 9. 2022.)
31. Klauzula 4.3 Smjernice za implementaciju ISO 27001, dostupno na: https://info-savvy.com/iso-27001-implementation-guideline-clause-4-3-determining-the-scope-of-the-information-security-management-system/ (19. 9. 2022).
32. Koraci rada pristupnika na razini aplikacije, dostupno na: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/ (12. 9. 2022.)
33. Krađa identiteta, dostupno na: https://www.sandiego.edu/its/security-and-privacy/identity-theft.php (20. 8. 2022.)
34. Nadzor rada sustava, dostupno na: https://www.cis.hr/sigurnosni-alati/nadzor-rada-sustava.html (26. 8. 2022.)
35. Najčešći oblik enkripcije, dostupno na: https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki (26. 8. 2022.)

36. *Next generation firewall*, dostupno na: https://www.vmware.com/topics/glossary/content/next-generation-firewall.html (14. 9. 2022.)
37. Oblici *Malwarea*, dostupno na: https://ashwiniscl.wordpress.com/information-system-attacks/ (24. 8. 2022.)
38. *Phishing* napadi, *CARNET CERT*, *https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-01-106.pdf?fbclid=IwAR1OGJqEs8cqzHaNudGRwQm5J3gfVoaL-HcGe1pXVlK_MjVg7IhIxV3WI1s* (27. 9. 2022.)
39. *Phishing* napadi, dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-01-106.pdf (27. 9. 2022.)
40. PKI, dostupno na: https://www.tutorialspoint.com/cryptography/public_key_infrastructure.htm (28. 8. 2022.)
41. Politika sustava informacijske sigurnosti, dostupno na: https://podaci.dzs.hr/hr/pages/dzs/politika-sustava-informacijske-sigurnosti/ (20.8.2022.)
42. Politika sustava informacijske sigurnosti, dostupno na: https://podaci.dzs.hr/hr/pages/dzs/politika-sustava-informacijske-sigurnosti/ (20. 8. 2022.)
43. Prednosti i nedostaci *Application-level gateway-a*, dostupno na: https://www.careerride.com/nw-application-gateway.aspx (12. 9. 2022.)
44. Razlike između *Packet filtering-a*, *Application-level gateway-a* i *Circuit level gatewaya*, dostupno na: https://www.rfwireless-world.com/Terminology/Application-Gateway-Vs-Circuit-Level-Gateway.html (14. 9. 2022.)
45. Sigurnosni alati za informacijsku sigurnost, dostupno na: https://www.cis.hr/sigurnosni-alati.html (26. 8. 2022.)
46. Simetrična i asimetrična enkripcija, dostupno na: https://www.keyfactor.com/resources/what-is-pki/ (28. 8. 2022.)
47. SQL, dostupno na: https://www.w3schools.com/sql/sql_injection.asp (20. 8. 2022.)

48. Sveobuhvatni cilj informacijske sigurnosti, dostupno na: https://is.bryant.edu/information-security/information-security-program (28. 8. 2022.)
49. Što je sustav za sprječavanje upada, dostupno na: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips (20.8.2022.)
50. *The next generation firewall*, dostupno na: https://www.fortinet.com/products/next-generation-firewall (27.9.2022.)
51. Tradicionalni vatrozidi, dostupno na: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/ (14. 9. 2022.)
52. Ubacivanje SQL koda, dostupno na: https://www.mossadams.com/articles/2021/08/cost-effective-information-security-program#information-security-program (26. 8. 2022.)
53. Uvod u informacijske sustave, https://www.fpz.unizg.hr/ztos/iszp/a2.pdf (3. 9. 2022.)
54. Vatrozid, dostupno na: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html (27.9.2022.)
55. Vatrozidi – filtriranje paketa, dostupno na: https://www.uio.no/studier/emner/matnat/ifi/IN3210/h19/slides/08-firewalls.pdf (10. 9. 2022.)
56. Zaštita mreže, dostupno na: https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html (26. 8. 2022.)

KAZALO KRATICA

Kratica	Puni naziv na stranom jeziku	Tumačenje na hrvatskom jeziku
BSoD	engl. *Blue screen of death*	plavi ekran smrti
DdoS	engl. *distributed denial-of-service*	distribuirano uskraćivanje usluge
ETA	engl. *Education, training and awareness raising*	obrazovanje, obuka i podizanje svijesti
HTTP	engl. *Hypertext Transfer Protocol*	protokol prijenosa hiperteksta
IDPS	engl. *Intrusion detection and prevention systems*	sustavi za otkrivanje i prevenciju upada
IDS	engl. *Intrusion detection system*	sustav za detekciju upada
IoT	engl. *Internet of things*	internetske stvari
IP	engl. *Internet protocol*	internetski protokol
IPS	engl. *Intrusion Prevention System*	sustav za sprječavanje upada
IPS	engl. *Intrusion Prevention Systems*	sustavi za sprječavanje upada
ISMS	engl. *Information security management system*	sustav upravljanja sigurnošću informacija
LAN	engl. *Local area network*	lokalna mreža
NGFW	engl. *Next-Generation Firewall*	vatrozid sljedeće generacije
OS	engl. *Operating system*	operativni sustav

OSI	engl. *Open Systems Interconnection*	međusobno povezivanje otvorenih sustava
PKI	engl. *Public key infrastructure*	infrastruktura javnih ključeva
TCP	engl. *Transmission Control Protocol*	protokol kontrole prijenosa
VPN	engl. *Virtual private network*	virtualna privatna mreža

POPIS TABLICA

POPIS SLIKA