Utjecaj zaposlenika na sigurnost informacijskih sustava organizacije

Selthofer, Klaudia

Sveučilište Sjever

Završni rad br. 389/2024

Utjecaj zaposlenika na sigurnost informacijskih sustava organizacije

Klaudia Selthofer, 0336053785

Koprivnica, lipanj 2024.

Sveučilište Sjever

Odjel za poslovanje i menadžment

Završni rad br. 389/2024

Utjecaj zaposlenika na sigurnost informacijskih sustava organizacije

Studentica:

Klaudia Selthofer

Mentor:

Matija Varga, doc. dr. sc.

Koprivnica, lipanj 2024. godine

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL: Odjel za ekonomiju

STUDIJ: preddiplomski stručni studij Poslovanje i menadžment

PRISTUPNIK: Klaudia Selthofer | MATIČNI BROJ: 0336053785

DATUM: 03.07.2024 | KOLEGIJ: Informatika

NASLOV RADA: Utjecaj zaposlenika na sigurnost informacijskih sustava organizacije

NASLOV RADA NA ENGL. JEZIKU: The impact of employees on the security of the organization's information systems

MENTOR: doc. dr. sc. Matija Varga | ZVANJE: docent

ČLANOVI POVJERENSTVA:

1. doc. dr. sc. Mirko Smoljic, predsjednik povjerenstva
2. doc. dr. sc. Joško Lozic, član
3. doc. dr. sc. Matija Varga, član, mentor
4. doc. dr. sc. Katerina Fotova Čiković, zamj. član
5.

Zadatak završnog rada

BROJ: 389/PIM/2024

OPIS:

Informacijski sustavi smatraju se jezgrom mnogih poslovnih operacija. Omogućuju brzu obradu podataka i učinkovitu komunikaciju, a istovremeno nude mnoge strateške prednosti. Ali s većom ovisnošću o informacijskim sustavima raste prijetnja od kibernetičkih opasnosti. Studije su pokazale da se često ljudski element pokaže najranjivijim dijelom u sigurnosti informacijskog sustava. Zaposlenici bi mogli namjerno ili slučajno postati rizik za sigurnost što bi moglo dovesti do ozbiljnih utjecaja na tvrtku. Ovaj rad će iznijeti više o tome što su točno informacijski sustavi i razne kategorije u koje spadaju, dajući kratak pregled toga kako su ti sustavi rasli tijekom vremena. Srž rada će se koncentrirati na različite metode kojima zaposlenici mogu utjecati na sigurnost informacijskog sustava. Analizirat će se različiti napadi na koje bi zaposlenici mogli biti ranjivi ili bi ih mogli započeti greškom, poput krađe identiteta, zlonamjernog softvera, doxinga i ubacivanja SQL-a. Također će biti uključene studije slučaja o tim incidentima. Ove studije nude stvarne primjere duboko pogođenih organizacija. Provedeno je istraživanje kako bi se dobio bolji uvid u to što zaposlenici misle i koliko znaju o sigurnosnim prijetnjama kao dio studija slučaja koji pokazuju primjere gdje je utjecaj zaposlenika evidentan. Anketa istražuje teme kao što su koliko radnici znaju o sigurnosti, razumiju li pravila za održavanje sigurnosti na poslu, kako rade svoj posao, te zašto je važno kada kolege rade zajedno. Zaključak ovog rada konstan je rad analize stanja informacijskih sustava organizacija kao i prijedloga za poboljšanja.

ZADATAK URUČEN: 5.7.2024 | POTPIS MENTORA:

SVEUČILIŠTE SJEVER

UNIVERSITY NORTH

Sažetak

U današnje vrijeme u digitalnom svijetu informacijski sustavi ključni su za rad organizacija, pomažu ubrzati rukovanje podacima i čine međusobni razgovor učinkovitijim. Iako su ovi sustavi vrlo važni, mogu biti napadnuti od strane cyber kriminala i opasnosti koje bi mogle stvarno naškoditi s očuvanjem sigurnosti podataka i održavanjem stvari stabilnim u poslovanju. Zaposlenici su ovdje često vrlo važni zbog toga kako se ponašaju i koliko znaju o sigurnosti na internetu, to bi moglo promijeniti koliko su sigurni u sebe i informacijski sustavi. Kada radnici pogriješe ili ne znaju što se događa, dopuštaju različite vrste loših stvari kao što je krađa nečijeg online identiteta, širenje loših računalnih programa ili čak slučajno otkrivanje slabih točaka u sigurnosti. Vrlo je važno uspostaviti ovu vezu tako da kada neko mjesto sastavi dobar plan za očuvanje sigurnosti, to uključuje i pametna tehnološka rješenja i osiguravanje da svi koji tamo rade znaju što se događa. Stroga pravila o tome kako se brinuti o informacijama tvrtke govore nam da su cyber opasnosti veliki problem i da svi ljudi koji rade za tvrtku trebaju znati kako zaštititi podatke. Bitno je naučiti dobre načine zaštite od tih rizika.

Ključne riječi: informacijski sustavi, rukovanje podacima, zaposlenici, cyber opasnosti

Summary

In today's digital world, information systems are crucial for the operation of organizations, they help speed up data handling and make mutual conversations more efficient. Even though these systems are very important, they can be vulnerable to cybercrime and threats that could really harm the security of data and keeping things stable in business. Employees here are often very important because of how they behave and how much they know about internet security, this could change how confident they are in themselves and their information systems. When workers make mistakes or don't know what's going on, they allow all kinds of bad things to happen, such as stealing someone's online identity, spreading bad software, or even accidentally discovering security vulnerabilities. It's very important to make this connection so that when a place puts together a good security plan, it includes smart technology solutions and making sure everyone who works there knows what's going on. Strict rules on how to take care of company information tell us that cyber dangers are a big problem and that all people who work for the company need to know how to protect data. It is important to learn good ways to protect yourself from these risks.

Keywords: information systems, data handling, employees, cyber threats

Popis korištenih kratica

IBM - International Business Machines, tvrtka za razvoj računarstva i informacijskih tehnologija

ENIAC - Electronic Numerical Integrator And Computer, ime prvog elektroničkog računala

INFOSEC – Information Security, informacijska sigurnost

CIA TRIAD - Confidentiality, Integrity, Availability - povjerljivost, integritet i dostupnost

ETL - Extract, transform, load - izdvajanje, transformiranje, učitavanje

DDoS – Denial of service attack, napadi uskraćivanjem resursa

.EXE – Executable, izvršna datoteka

.COM – Commercial, vršna internetska domena

SQL - Structured Query Language, strukturni upitni jezik, programski jezik visoke razine

IT - Information technology, informacijska tehnologija

MOL - Mađarska multinacionalna naftna i plinska kompanija

CERT - Computer Emergency Response Team, nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava

MUP – Ministarstvo unutarnjih poslova

Sadržaj

1. Uvod

U našem današnjem digitalnom svijetu, informacijski sustavi se smatraju jezgrom mnogih poslovnih operacija. Omogućuju brzu obradu podataka i učinkovitu komunikaciju, a istovremeno nude mnoge strateške prednosti. Ali s većom ovisnošću o informacijskim sustavima raste prijetnja od kibernetičkih opasnosti. Studije su pokazale da se često ljudski element pokaže najranjivijim dijelom u sigurnosti informacijskog sustava. Zaposlenici bi mogli namjerno ili slučajno postati rizik za sigurnost što bi moglo dovesti do ozbiljnih utjecaja na tvrtku. Sigurnost informacijskih sustava nije samo tehnički problem, već se bavi i načinom na koji se oblikuje kultura tvrtke i svijest zaposlenika. Najnovije sigurnosne postavke mogu zakazati ako se ljudi koji rade ne pridržavaju sigurnosnih protokola ili nisu dovoljno obučeni za uočavanje opasnosti. Bitno je da saznamo koliki su učinak ti radnici imali na očuvanje sigurnosti informacijskih sustava tako da se mogu napraviti snažni planovi zaštite. Ovaj rad će iznijeti više o tome što su točno informacijski sustavi i razne kategorije u koje spadaju, dajući kratak pregled toga kako su ti sustavi rasli tijekom vremena. Srž rada će se koncentrirati na različite metode kojima zaposlenici mogu utjecati na sigurnost informacijskog sustava. Analizirat će se različiti napadi na koje bi zaposlenici mogli biti ranjivi ili bi ih mogli započeti greškom, poput krađe identiteta, zlonamjernog softvera, doxinga i ubacivanja SQL-a. Također će biti uključene studije slučaja o tim incidentima. Ove studije nude stvarne primjere duboko pogođenih organizacija. Provedeno je istraživanje kako bi se dobio bolji uvid u to što zaposlenici misle i koliko znaju o sigurnosnim prijetnjama kao dio studija slučaja koji pokazuju primjere gdje je utjecaj zaposlenika evidentan. Anketa istražuje teme kao što su koliko radnici znaju o sigurnosti, razumiju li pravila za održavanje sigurnosti na poslu, kako rade svoj posao, te zašto je važno kada kolege rade zajedno.

2. Informacijski sustav

Informacijski sustav - predstavlja dio u svakom poslovnom sustavu kojemu je uloga svakoj razini upravljanja, odlučivanja i općenitom poslovanju opskrbiti potrebne informacije. S obzirom da je informacijski sustav uglavnom namijenjen za realni poslovni sustav, ono što čini svrhu kreiranja strukture samog informacijskog sustava zapravo su poslovni procesi. (Klasić, Klarin, 2009:13)

Kao **osnovni cilj informacijskih sustava** možemo izdvojiti prikupljanje, pohranjivanje, obrađivanje, analiziranje i distribuiranje neopipljivih resursa poslovanja iz čega možemo izdvojiti podatke, informacije i znanje kako bi sami poslovni procesi mogli izvršiti svoju provedbu i poslovne transakcije svoju obradu. Prava informacija na pravom mjestu, u pravo vrijeme i uz minimalne zahtijevane troškove zapravo je osnovni cilj informacijskog sustava.

Odrediti što je to prava informacija jedan je od najvećih problema čak i za najiskusnije menadžere. Ni jedan menadžer ne može uvijek znati koje su informacije i podaci potrebni za rješavanje nekog problema poduzeća. Prvi korak je definirati problem kako bi mogli odrediti što nam je zapravo od informacija potrebno u informacijskom sustavu. (Bošillj Vukšić, Ćurko, 2020:174)

Sam pojam poslovnog sustava u pravilu je složeni sustav. Kada se susrećemo sa jednostavnim poslovnim sustavima zapravo se susrećemo sa poslovnim sustavom kojemu je u razmatranju samo dio funkcija ili ima manji obujam posla kojeg obavlja (što ne mora uvijek biti).

Kada se informacijski sustav sastoji od niza informacijskih podsustava tada govorimo u sustavu koji podržava složeni poslovni sustav. Svaki od tih podsustava može se smatrati osnovnim informacijskim sustavom. (Klasić, Klarin, 2009:16)

Dakle, prema Klasić i Klarin, (2009:17), zadatke informacijskog sustava možemo podijeliti na:

- prikupljanje
- kategoriziranje
- obradu podataka
- pohranu
- strukturiranje

- distribuciju podataka svim radnim razinama poslovnog sustava

Kako bi postavljene zadaće informacijskog sustava uspostavljene određenom namjerom bile obavljene, potrebno je ispuniti dvije osnovne funkcije poduzeća: izvještavati informacije potrebne za proizvodnju ili pružanje usluga, poslovanja i upravljanja, te vođenje evidencije dokumentacije. Ako je informacijski sustav uspostavljen isključivo zbog jedne poslovne zadaće sa jednostavnom obradom podataka tada se radi o jednostavnom informacijskom sustavu. Kod većeg broja korisničkih skupina, različitih polja primjene, većih datoteka, složenosti i međuovisnosti od obrade do obrade, zajedničkih kodiranja, te složenih dokumentacija radi se o složenom ili integralnom informacijskom sustavu. Također postoji i inteligentni informacijski sustav koji se razlikuje samo po tome što se sastoji od većeg broja inteligentnih metoda i procesa koje izvodi automatizmom i uglavnom samostalno. (Šimović, 2010:17)

2.1. Povijest informacijskih sustava

U povijesti razvoja informatike otkrivamo što je bilo dostupno od tehničkih sredstava kako bi potrebni podaci bili obrađeni i primjenjivi u svakodnevnom načinu života i rada. Izdvojive su četiri osnovne faze koje prikazuju razvoj obrade podataka koje su unatoč suvremenosti i dan danas u primjeni.

1. **Faza ručne obrada podataka** poznata je po tome što su se podaci obrađivali sporo uz uporabu ručnog rada, stvari za samu pohranu podataka i alata koji su bili dostupni kako bi pisanje određenog medija bilo moguće. Ovim načinom dobiva se prilično malo podataka što se tiče količine, a također se ne može ni računati na obradu kada govorimo o pouzdanosti i točnosti.

2. **Faza mehaničke obrade podataka** nastala je uslijed napretka znanosti i same tehnike. Kreće sredinom 17.stoljeća dok su izumljeni prvi uređaji koji su služili kao pomoć pri obradi podataka. Njihovi konstruktori bili su najpoznatiji matematičari i fizičari tog doba (na primjer, Blaise Pascal konstruktor je uređaja za kojeg se govori da je nositelj suvremenih računala). Henry Mill sa svojim mehaničkim pisaćim strojem, jedan je od značajnih utjecaja informacijskih znanosti, te društvenih odnosa u potpunosti. Produktivnost, točnost i količina obrađenih podataka odlika su ove faze.

3. **Faza elektromehaničke obrade podataka** svoj početak upisuje tijekom druge polovice 19.stoljeća, prilikom pokreta javnog natječaja vlade SAD-a za konstruiranje uređaja koji olakšava i ubrzava obradu popisa stanovništva. Hermann Hollerith odnio je pobjedu svojim prijedlogom bušene kartice koja se koristi kao nositelj podataka (izumljenu od strane Jacquarda i primijenjenu za vođenje tkalačkim stanom prilikom čega kreće i automatizacija proizvodnog procesa), a za obradu podataka želio je upotrebu posebnog elektromehaničkog uređaja. Time kreće i masovna obrada iznimno velikog broja količine podataka, a Hollerith nakon obogaćenja osniva tvrtku iz koje se 1924. godine razvio IBM (International Business Machines). Ova faza poznata je i pod nazivima: kartička obrada podataka, mehanografska obrada podataka i birotehnička obrada podataka.

4. **Faza elektroničke obrade podataka** događa se 1944. godine s početkom ENIAC-a iza kojeg stoji i naziv prvog pravog elektroničkog računala. U ovoj fazi odlika su velika brzina obrade iznimno velikih količina podataka i zanemarivih grešaka. Obrada i prijenos podataka, integracija medija te privremena i trajna pohrana podataka omogućene su upravo u ovoj fazi. Internet kao najpoznatiji, tada i najnoviji način obrade podataka, također se upisao u ovu fazu. (Klasić, Klarin, 2009:20:21)

2.2. Elementi informacijskih sustava

Pod informacijski sustav ubrajamo sljedeće elemente:

Hardver – svi materijalni i vidljivi dijelovi koji čine sastav računala.

Softver – programi i rješenja koja čine temelj rada hardvera.

Korisnici (engl. Lifeware) – Korisnici informacijskog sustava

Organizacija (engl. Orgware) – funkcije organizacije i njezini načini sklapanja hardvera i softvera u cjelinu.

Mreža (engl. Netware) – poveznica komunikacijskog dijela i njihova realizacija i koncepcija.

Podaci (engl. Dataware) – informacijski resursi i baze podataka kao koncepirana i organizirana cjelina. (Bošillj Vukšić, Ćurko, 2020:175)

2.3. Vrste informacijskih sustava

Postoje različiti kriteriji kada je u pitanju podjela informacijskih sustava. Podijeliti ih možemo na konceptualno ustrojstvo u poslovodstvu, prema svrsi ili prema vrsti funkcije u poslovnom sustavu. Ne postoje stroge granice u jednom poduzeću između dva podsustava kada je u pitanja praksa, ali su ti podsustavi u drugom poduzeću strogo odvojeni. (Klasić, Klarin, 2009:22)

Tablica 1. „Vrste informacijskih sustava prema konceptualnom ustroju poslovodstva."

Ustroj poslovodstva		**Vrste IS-a**	
Poslovodstvo	Strateški nivo	Odlučivanje	**Sustav potpore odlučivanju**
Izvršno vodstvo	Taktički nivo	Upravljanje	**Izvršni informacijski sustavi**
Operativno vodstvo	Operativni nivo	Izvođenje	**Transakcijski sustavi**

Izvor: Klasić, K; Klarin, K. (2009:23) Informacijski sustavi: načela i praksa.

Strateškoj razini namijenjeni su sustavi potpore odlučivanju, dok su taktičkoj namijenjeni izvršni informacijski sustavi čija su izvješća ključ za upravljanje. U operativnoj razini nalaze se sustavi za transakcije čija je namjena izvođenje procesa osnovne djelatnosti. Primjer toga su sustavi u kojima knjižimo bankarske transakcije ili evidencija pojedinih koraka u proizvodnji. (Klasić, Klarin, 2009:23)

2.4. Informacijski sustavi prema namjeni

Podjela informacijskih sustava prema namjeni uključuje sustav obrade podataka, sustav podrške uredskom radu, sustav podrške u odlučivanju i ekspertne sustave.

Sustavi obrade podataka sastoje se od unosa, obrade i pohrane podataka koji prikazuju stanje i poslovne događaje sustava. Baze podataka služe za pohranu podataka, te im se pristupa pomoću posebnih programa čija je funkcija poput tražilice za baze podataka.

Sustavi podrške uredskom radu odnose se na podršku kod obavljanja svih poslova administracije i podršku komunikacije. Pomoćni sustavi kod obrade dokumenata su prezentacije, potpora rada u skupini i slično, a za komunikaciju podršku uglavnom čine elektronička pošta i videokonferencije.

Sustavi podrške u odlučivanju sastavljeni su od niza modela pomoću kojih se stvaraju potrebne informacije za odlučivanje, te podrške grupi ili pojedincu.

Ekspertni sustavi su kao što i samo ime kaže, podrška ekspertima i stručnjacima. Glavna im je funkcija riješiti probleme konfiguracije i dijagnosticiranja. Kategoriziraju se na podršku pri učenju, stručnom ili znanstvenom radu i projektu. (Klasić, Klarin, 2009:23)

3. Informacijska sigurnost

Informacijska sigurnost sastoji se od propisanih mjera i određenih standarda za sigurnost, te poslova koje primjenjuje svaka organizacija. Njima se postiže stanje povjerljivosti, raspoloživosti i cjelovitosti podataka. Informacijsku sigurnost ponekad nazivaju i InfoSec jer organizacija štiti svoje informacije pomoću alata i procesa koje pokriva InfoSec. Tu spada zaštita od neovlaštenih pristupa podatcima bili oni poslovni ili osobni. Koliko god napredna bila, informacijska sigurnost je područje koje se još uvijek razvija i raste pa pokriva i širok raspon područja. Neka od područja su razna testiranja, infrastrukture, revizije i sigurnosti mreže. Osjetljivi podaci zaštićeni su na način postojanja inspekcije, raznih vrsta nadzora i modificiranja kako bi se spriječilo uništenje ili samo ometanje. Najbitniji su financijski podaci, korisnički računi i intelektualno vlasništvo pa je u velikom cilju osigurati njihovu sigurnost i privatnost. Incidenti koji se mogu dogoditi uključuju brisanje ili promjenu podataka i krađu osobnih podataka. Napadi mogu biti brojni, a također mogu i uvelike naštetiti ugledu organizacije i poremetiti rad što najčešće završava velikom cijenom. Svaka organizacija mora biti spremna na rizike izdvajanjem sredstava za sigurnost organizacije, te naučiti adekvatno

odgovoriti na potencijalne napade i spriječiti krađe identiteta uz popratne razne načine ucjenjivanja. (Zubović, 2022)

3.1. Temeljna načela informacijske sigurnosti

Integritet, raspoloživost i povjerljivost čine osnovna načela informacijske sigurnosti. Svaki od elemenata je dizajniran tako da je u stanju implementirati jedno ili više načela. Njihov skup čini naziv CIA Triad.

Slika 1: Cia Triad

Izvor: ("What Is the CIA Triad?", 2019)

U ovom slučaju, američka obavještajna agencija nema nikakve veze s nazivom „CIA". Iza svakog slova kriju se engleski nazivi: confidentiality – povjerljivost, integrity – integritet i availability – dostupnost. Zajedno čine temelj sigurnosti svake organizacije. CIA je toliko važna za sigurnost organizacije da prilikom svakog napada, krađe identiteta, pada web stranice ili drugo, možemo sa sigurnošću potvrditi da je prekršeno jedno ili više ova tri načela koja čine CIA sustav. Stručnjaci vrše procjene na temelju utjecaja prijetnji i ranjivosti na ova 3 načela. Nakon rezultata procjene, implementira se skup sigurnosnih kontrola kako bi organizacija smanjila rizik.

1. Povjerljivost – odnosi se na snagu i trud organizacije da očuva privatnost i tajnost podataka. U praksi se govori o kontroliranju pristupa važnim podacima kako bi se spriječila potencijalna i neovlaštena otkrivanja. Samo ovlašteni zaposlenici trebaju imati

pristup imovini, te se nastoji osigurati isključivo njihov pristup dok se za neovlaštene aktivno onemogućava svaki pristup imovini i podacima.

2. Integritet – osiguranje podataka od neovlaštenih izmjena i uvjerenje da su vjerodostojni, ispravni i autentični.

3. Dostupnost – brine o tome da su sve mreže, aplikacije i sustavi dostupni i pokrenuti u pravo vrijeme kada su i potrebni ovlaštenim korisnicima ("What Is the CIA Triad?", 2019)

3.2. Ranjivost informacijskog sustava

Kada govorimo o ranjivosti ona se može podijeliti na slučajno aktiviranu ranjivost i namjerno iskorištenu, posljedice su velike štete u informacijskim sustavima. Ranjivosti povezane s resursima isključivo se odnose na slabosti. Te slabosti uključuju slabosti informacija, zaposlenika, organizacije, fizičke sigurnosti, internih akata, hardvera, softvera i upravljačke strukture. Ranjivost je stanje dopuštenja određenoj prijetnji da može utjecati na resurse. To je greška koja za posljedicu omogućava napadaču pristup i manipulaciju sustavom. Identifikacija slabosti informacijskog sustava cilj je životnog ciklusa upravljanja ranjivostima kao što je i određivanje, procjena, prijava i uklanjanje slabosti i potvrđivanje da je isto eliminirano. Dakle, najveći nedostatak informacijske sigurnosti je ranjivost koja dopušta napadaču ili uljezu da svede sigurnost informacijskog sustava na minimum. Da bi ranjivost bila iskoristiva, elementi koje mora sadržavati su: slab sustav, pristup napadaču ili uljezu, znanje i sposobnost napadača da iskoristi tu slabost sebi učinkovitim alatima i tehnikama. (Zubović, 2022)

4. 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.″

„Vrste prijetnji sigurnosti informacijskoga sustava jesu sljedeće ″:

- neovlašteni pristup
- računalni virusi
- krađa
- sabotaža. (Zubović, 2022)

4.1. Motivacija za napad na informacijski sustav

Važno je razumjeti što je zapravo motivacija neprijatelja koja stoji iza napada na informacijski sustav kako bi shvatili što neprijatelj želi postići. Samim prepoznavanjem motiva za napad od uvelike je pomoći pri odabiru načina zaštite koju će organizacija primijeniti. Isto tako, time je unaprijed omogućen i uvid u potencijalni scenarij napada pa entiteti lakše i brže usmjeruju svoje napore i znanje u obrani od napada na određeni resurs. Svi navedeni razlozi, koji su primijećeni prilikom izvještajnog razdoblja, uključeni su za procjenu motivacije drugu godinu za redom od strane ETL 2023. Upravo zbog toga, odabrano je čak pet vrsta motivacije prijetnji:

1. **Financijska dobit:** bilo koja izvedena financijski povezana akcija od strane cybercrima.

2. **Špijunaža:** saznanje informacija o privatnim, osjetljivim ili klasificiranim podacima, te intelektualnom vlasništvu pretežno od državnih grupa.

3. **Ometanje:** bilo kakvo ometanje učinjeno u ime geopolitike.

4. **Uništenje**: bilo koja sabotaža koji nosi nepovratne posljedice.

5. **Ideološka:** akcija koja je povezana ideologijom aktivizma poput npr. hakiranja.

Većina prijetnji može biti definirana od strane jedne ili više motivacija, tada su neke motivacije dominantnije. Primarna motivacija kod ransomware napada je financijska dobit no i ovdje ipak postoji motivacija za ometanje u malom postotku. Motivacija za većinu događaja na kraju ostaje nejasna. Toj nejasnoći glavnu ulogu igra neznanje motiva ili informacije koje su ograničene i nisu objavljene. Tako na drugom mjestu, odmah iza financijske dobiti kao primarne motivacije, nalazi se ometanje. Kako je manipulacija osjetljivim informacijama važan dio, ipak se najviše napada može pripisati DDoS (Distributed Denial of Service) napadima. Distributed Denial of Service ima za cilj onemogućiti uslugu i rad korisnicima na način da preopteretі poslužitelj ili mrežu sa velikim postotkom prometa. Dakle, glavni cilj napadača je doći do informacija o tajnim i povjerljivim podacima koje zakonskim putem nikada ne bi saznali, isključivo zbog saznanja ("ENISA THREAT LANDSCAPE", 2023).

Opasnost od neovlaštenog pristupanja povjerljivim podacima jedan je od najčešće vladajućih sigurnosnih rizika kada je u pitanju informacijski sustav. Virus u računalu čini vrstu namjerno stvorenog softvera s ciljem nedopuštenog ulaska u računalo kako bi se umnožio i nastavio svoje širenje. Jedini cilj računalnog virusa je napraviti neželjene učinke na poslovnim ili osobnim računalima.

Virus može zaraziti ostale programe na način da zarazom uključe njegovu kopiju koja također može biti zarazna. Pod zarazom se definira sposobnost virusa da svojim naredbama u programu pokuša proizvesti legitiman program koji će također imati funkciju proizvodnje virusa. Program zaražen virusom i dalje ima mogućnosti uzrokovati rušenje i gubitke podataka. S druge, pozitivnije strane, postoji većina situacija kada su štete koje je počinio virus zapravo bile slučajne posljedice lošeg programiranja.

Financijski gubici rezultat su mnogobrojnih vrsta prijetnji na informacijske sustave, posljedice su ogromne. Također, štete možemo podijeliti od malih do onih koje značajno unište informacijski sustav. Ako prijetnje dođu do realizacije, aktivnosti mogu biti trajno zaustavljene što nosi brojne gubitke organizacije. Ponekad su prijetnje koje nisu imale ikakvu namjeru, već su rezultat nedostatka volje za provedbu štete, upravo one najopasnije.

Dakle, možemo zaključiti da prijetnje na informacijski sustav mogu biti nenamjerne ili namjerne, te je posljedica bilo kojih gubitak pohranjenih podataka u informacijskom sustavu. Za takve bi prijetnje bilo poželjno imati dobro organiziranu zaštitu. Najlakši način prepoznavanja da je prijetnja slučajna je zapravo njezina neočekivana i slučajna pojava. Iza takve prijetnje ne postoji želja za nanošenjem štete kao ni curenje ili uništavanje zaštićenih informacija u informacijskim sustavima.

Ne mora nužno svaki napad na sustav sigurnosti imati za cilj novčanu ucjenu, neki napadači samo žele isključivo iz znatiželje saznati neke povjerljive ili tajne podatke do kojih zakonitim ili normalnim putem nisu u mogućnosti doći. (Zubović, 2022)

4.2. Glavni uzroci proizvedenih napada na informacijske sustave:

- nedostaci računalnih sustava zbog kojih dolazi do opasnosti za informacije uslijed neučinkovite zaštite
- zaposlenici odgovorni za slučajno otkrivanje povjerljivih informacija
- nestanak i krađa uređaja koji sadrže povjerljive informacije
- društveni inženjering poznat po manipulaciji ljudima za bitne i povjerljive podatke zauzvrat. (Loch, Carr, Warkentin, 1992).

4.3. „Vrste napada na računalnu sigurnost″:

• zlonamjerni softver

• ubacivanje SQL koda

• krađa identiteta

• doxing

• napad uskraćivanjem usluge – DdoS (engl. Distributed denial-of-service, distribuirano uskraćivanje usluge).

• phishing (Zubović, 2022)

4.3.1. Zlonamjerni softver

Zlonamjerni softver (maliciozni softver) čini sve programe čijeg dolaska na naše računalo nismo svjesni, a cilj im je prouzročiti štetu.

„Vrste zlonamjernih programa″:

Tablica 2: Vrste zlonamjernih programa

Osnovna podjela	**Ostale vrste**
virusi	ransomware
crvi	spyware
trojanski konji	adware
	spam

Izvor: ("Zlonamjerni programi, razlike i način djelovanja", 2021).

Virusi: virusi svoje umnožavanje postižu prilikom pokretanja programske datoteke (nastavak je .exe) koja sadrži zaraženi kod. Virusni kod će se izvršiti istovremeno prilikom slučajnog pokretanja zaraženog programa.

Osnovne vrste virusa:

Boot sektor virusi – koriste svoj zlonamjerni kod kako bi ga kopirali u mali program neophodan za pokretanje operativnog sustava, te time osiguravaju da se zlonamjerni kod aktivira prilikom svakog starta sustava.

Programski virusi – aktiviraju se kada se pokrene zaražena izvršna datoteka, najčešći nastavci su .com ili .exe

Makrovirusi - virusi napisani u višem makroprogramskom jeziku mogu se kopirati, brisati i mijenjati dokumente

Crvi – širi se samostalno na način da koristi mrežu da bi se proširio na druga računala. Iako ne nanosi direktnu štetu, toliko se umnožava da preoptereti računalne resurse, čineći ga neupotrebljivim. Njegova pojava najčešća je u obliku privitka elektroničke pošte.

Trojanski konji - Posebnost trojanskog konja je u tome što se predstavlja kao koristan program. Korisnik vjeruje da je program neopasan i dozvoljava mu instalaciju na računalo. Nakon instalacije, trojanac omogućava autoru zlonamjernog softvera pristup računalu putem tzv. stražnjih vrata (eng. backdoor), što omogućava krađu osobnih podataka, lozinki i slično. Za razliku od crva, trojanac se ne može samostalno umnožavati. *Naziv dolazi iz grčke mitologije. Trojanci su prihvatili velikog konja kao poklon od Grka, vjerujući da je to znak mira, ali nisu znali da su u njemu bili skriveni grčki vojnici koji su noću izašli, otvorili vrata grada i omogućili napadačkoj vojsci da uđe.

Ransomware (kriptovirus) - Ransomware, poznat i kao kriptovirus, je zlonamjerni softver koji enkriptira korisnikove podatke. Autori ransomwarea zahtijevaju otkupninu kako bi korisnici dobili ključ za dešifriranje podataka. Plaćanje otkupnine nije preporučljivo jer to financira kriminalne organizacije, a nema garancije da će podaci biti vraćeni. Redovito stvaranje sigurnosnih kopija podataka (backup) jedini je pouzdan način zaštite. Glavni način zaraze obično je otvaranje privitaka u e-pošti.

Spyware - vrsta špijunskog softvera koji prati i bilježi aktivnosti korisnika, kao što su posjećene web stranice, korišteni programi, pa čak i financijski podaci. Te informacije šalje naručitelju, obično marketinškoj agenciji. Zaraza spywareom često se događa kada korisnik posjećuje sumnjive ili neprikladne web stranice.

Adware - iako nije zlonamjerni softver, ometa rad korisnika stalnim prikazivanjem reklama koje iskaču bez kontrole. Često se reklame šalju velikom broju korisnika putem neželjene pošte poznate kao spam. Naziv "spam" potječe iz serije Monty Python koja je reklamirala mesnu konzervu pod nazivom Spam. ("Zlonamjerni programi, razlike i način djelovanja", 2021).

4.3.2. Ubacivanje SQL koda

SQL kod je tehnika napada koja iskorištava sigurnosne propuste u web aplikacijama koje pristupaju bazama podataka. Na ovaj način napadač može ugroziti sigurnost web aplikacije koja koristi korisnički unesene podatke za kreiranje SQL upita. SQL (Structured Query Language) je specijalizirani jezik za upravljanje bazama podataka i najčešće se koristi u današnjim web aplikacijama. Web aplikacije često koriste podatke koje unesu korisnici za stvaranje dinamičkih SQL upita. Ranjivost se pojavljuje kada podaci uneseni od strane korisnika nisu pravilno filtrirani ili kada nema odgovarajućih ograničenja na ulazne podatke. Napadač može iskoristiti ovaj propust za izmjenu SQL upita koji se izvršava. Ako uspije, upit će se izvršiti s dozvolama izvorne SQL naredbe, što može dovesti do preuzimanja kontrole svih podataka u bazi. (CARNet CERT, LS&S, 2008)

4.3.3. Krađa identiteta

Krađa identiteta nastaje prilikom prisvajanja nečijeg identiteta. To mogu biti osobni podaci, podaci o bankovnom računu ili broj kartice. Cilj napadača je prijevara ili neka druga vrsta kaznenih djela. Krađa identiteta spada u najbrže rastuću aktivnost vezanu za kriminal na svjetskoj razini bez prepoznavanja lokacije. Žrtve krađe identiteta kao i napadači mogu biti locirani na potpuno krivim stranama svijeta. Upravo iz tog razloga policija teško istražuje ovu vrstu kaznenog djela, te ne može uvijek pomoći žrtvi u potpunosti. Računalo i ostali pametni uređaji glavna su pomoć napadačima kada su u pitanju krađe identiteta ("Krađa identiteta – što je i kako se zaštititi?", 2015).

„Krađa identiteta može obuhvaćati krađu˝:

brojeva platnih i kreditnih kartica,

putovnice,

imena,

adrese,

podataka iz vozačke dozvole,

podataka za prijavljivanje za ostale usluge ("Krađa identiteta – što je i kako se zaštititi?", 2015).

4.3.4. Doxing

Doxing (ili Doxxing) podrazumijeva objavljivanje osobnih informacija o nekome na internetu, kao što su pravo ime, kućna adresa, radno mjesto, broj telefona, financijski podatci i druge privatne informacije. Ove informacije se javno dijele bez pristanka te osobe. Bez obzira na razloge iza ovog čina, glavna namjera doxinga je narušavanje nečije privatnosti, što može dovesti do neugodne situacije i ponekad imati ozbiljne posljedice ("What is Doxing – Definition and Explanation", 2023).

4.3.5. Napad uskraćivanjem usluge – DDoS

DDoS napad napada web stranice i poslužitelje ometanjem mrežnih usluga kako bi se preuzeli softverski resursi. Napadači koji stoje iza ovih napada isporučuju ogromne količine prometa na web mjesto, uzrokujući njegovo neispravno funkcioniranje ili čak potpuno gašenje. Takvi napadi su sve češći. DDoS napadi imaju širok doseg i ciljaju različite industrije i tvrtke diljem svijeta. Neke su industrije, poput igara, e-trgovine i telekomunikacija, pogođene više od drugih. DDoS napadi jedna su od najčešćih računalnih prijetnji i mogu ugroziti vaše poslovanje, internetsku sigurnost, prodaju i ugled. Tijekom DDoS napada, niz botova ili mrežnih bombaša preplavi web stranicu ili uslugu HTTP zahtjevima. To u biti znači da više računala napada isto računalo, otuđujući stvarne korisnike. Kao rezultat toga, pružanje usluga može povremeno biti odgođeno ili na drugi način prekinuto ("Što je DDoS napad?", 2021).

4.3.6. Phishing

Phishing je oblik napada u kojem napadač kontaktira potencijalnu žrtvu. Napast će nekoga kome vjeruje ili koga poznaje i od žrtve će tražiti da poduzme određene korake kako bi postigao svoj cilj. Općenito se preporuča brzo djelovati i prijevaru izvesti što je brže moguće, kako žrtva ne bi imala dovoljno vremena vidjeti što se događa. Ljudi koji upadnu u zamku odaju svoje podatke, što bi ih u konačnici moglo stajati novca. Poruka obično sadrži poveznicu i žrtva se želi prevariti na način da slijedi tu poveznicu. Poveznica može ponuditi preuzimanje određenih dokumenata ili preusmjeriti potencijalne žrtve na web stranice koje nastavljaju oponašati određene usluge kojima vjerujemo. Ako žrtva otvori poruku i slijedi poveznicu, od nje će se u

sljedećem koraku tražiti osobni podaci. Poruka ima za cilj uvjeriti žrtvu da su njihovi podaci već ugroženi i da ih treba ponovno unijeti kako bi potvrdili svoj račun i identitet. Nakon što se podaci unesu u označena polja i žrtva potvrdi da je informacija unesena, ona se šalje napadaču ("Što je phishing (krađa identiteta) – 4 ključna pitanja", 2022).

5. Organizacija informacijske sigurnosti

Pri organizaciji informacijske sigurnosti ključno je jasno definirati sve odgovornosti u skladu sa sigurnosnom politikom. Vodstvo organizacije mora aktivno podržavati provedbu sigurnosne politike i primjereno sankcionirati kršenje pravila. Također je bitno učinkovito koordinirati zaposlenike kako bi implementacija sigurnosne politike bila uspješna.

Koraci koji se poduzimaju kod organizacija informacijske sigurnosti:

Autorizacija - Procjena sigurnosne razine određenih dijelova opreme, primjerice prijenosnih računala.

Ugovor o povjerljivosti - Dokumentiranje vrijednosti koje organizacija posjeduje s ciljem zaštite od kopiranja, uništavanja ili zamjene od strane zaposlenika, partnera ili trećih strana.

Konzultacije sa stručnjacima za informacijsku sigurnost - Savjetovanje sa stručnim organizacijama za računalnu sigurnost radi dobivanja relevantnih savjeta i smjernica u slučaju sigurnosnih incidenata.

Suradnja s drugim organizacijama - Održavanje kontakta s drugim organizacijama radi razmjene znanja o sigurnosti informacijskih sustava i brzog informiranja u slučaju sigurnosnog incidenta.

Redovite sigurnosne provjere sustava - Periodična provjera sigurnosti informacijskog sustava kako bi se osiguralo njegovo ispravno funkcioniranje.

Sigurnost pristupa za treće strane - Osiguravanje da informacije kojima treća strana ima pristup budu zaštićene na jednako visok način.

Identifikacija rizika kod pristupa treće strane - Procjena mogućih rizika prije dodjele pristupnih prava trećoj strani kako bi se informacijski sustav mogao adekvatno zaštititi.

Sigurnosni zahtjevi u ugovorima s trećim stranama - Formalno definiranje pravila zaštite u ugovorima s trećim stranama koje imaju pristup informacijskom sustavu, u skladu sa sigurnosnom politikom organizacije. (CARNet CERT, LS&S, 2009)

5.1. Zaštita od zaposlenika

Zaposlenici često čine nenamjerne pogreške, ali mogu također počiniti i zlonamjerne radnje. Kako bi se osigurala zaštita informacija i imovine organizacije, potrebno je imati na umu i proučiti sljedeće:

Definiranje uloga i odgovornosti - Jasno definiranje uloga i odgovornosti za zaposlenike, ugovorne radnike i treće strane.

Provjera - Provođenje provjera potencijalnih zaposlenika, ulagača ili poslovnih partnera radi povećanja sigurnosti informacijskog sustava.

Uvjeti zaposlenja - Uključivanje klauzule u ugovor koja obvezuje sve strane na poštivanje sigurnosne politike organizacije prije zapošljavanja ili sklapanja ugovora s ulagačima ili trećim stranama.

Odgovornosti rukovoditelja - Informiranje zaposlenika o njihovim ulogama i odgovornostima u provedbi sigurnosnih mjera.

Edukacija o informacijskoj sigurnosti - Osposobljavanje zaposlenika i trećih strana kako bi bili svjesni važnosti zaštite informacijskog sustava i postigli zadovoljavajuće rezultate.

Postupak raskida ugovora - Jasno definiranje procedura koje se provode prilikom raskida radnog odnosa ili ugovora, uključujući vraćanje imovine organizacije koja je dana na korištenje i ukidanje prava pristupa informacijskom sustavu. (CARNet CERT, LS&S, 2009)

5.2. Provjera pristupa

Važno je jasno definirati koji će korisnici imati pristup određenim informacijama. Upravo zbog toga, potrebno je poduzeti sljedeće korake:

Provjera pristupa u skladu s poslovnim zahtjevima - Pristup informacijama treba biti usklađen s poslovnim potrebama kako bi se spriječio neovlašteni pristup podacima.

Politika provjere pristupa - Uspostavljanje skupa pravila za određivanje razina pristupa za zaposlenike.

Upravljanje pristupom korisnika - Kontrola pristupa kako bi se onemogućio neovlašteni pristup informacijama.

Registracija korisnika - Uspostavljanje formalnog postupka registracije za dobivanje pristupa višenamjenskim informacijskim sustavima.

Upravljanje privilegijama - Definiranje razine privilegija u informacijskom sustavu za svakog zaposlenika.

Upravljanje korisničkim lozinkama - Izrada formalne izjave kojom se korisnici obvezuju čuvati lozinke tajnima i zabranjuje njihovo odavanje tijekom bilo koje vrste komunikacije (e-mailom, telefonom, pismeno).

Odgovornost korisnika - Povećanje svijesti korisnika o njihovoj odgovornosti vezanoj uz lozinke i opremu koja im je dana na korištenje kako bi se smanjila mogućnost neovlaštenog pristupa.

Provjera pristupa mreži - Uspostavljanje provjere mrežnih servisa i usluga radi zaštite mrežnog sustava od neovlaštenih aktivnosti.

Provjera pristupa operacijskom sustavu - Uvođenje sigurnosnih mehanizama unutar operativnog sustava kako bi se spriječio neovlašteni pristup računalnim resursima.

Praćenje pristupa i korištenja sustava - Dokumentiranje i provjeravanje pristupa te korištenja sustava kako bi se pravovremeno uočili pokušaji neovlaštenih aktivnosti.

Bilježenje događaja - Bilježenje svih aktivnosti u sustavu u slučaju sigurnosnog incidenta kako bi se moglo rekonstruirati što se dogodilo.

Praćenje uporabe sustava - Praćenje aktivnosti korisnika kako bi se osiguralo da izvode samo one aktivnosti za koje su ovlašteni. (CARNet CERT, LS&S, 2009)

5.3. Važnost sigurnosne politike

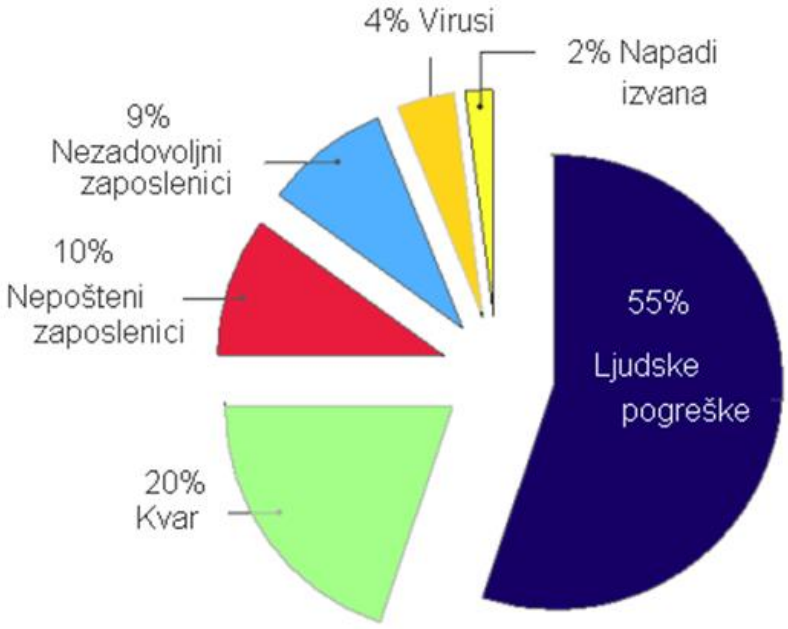
Studije pokazuju da je uspostava sigurnosne politike postala preporučljiva za svaku organizaciju. Ipak, čak i uz pravilno provođenje tih politika, sigurnosni incidenti se i dalje događaju. Šteta koja nastane zbog takvih incidenata može biti velika i ozbiljno ugroziti stabilnost poslovanja organizacije. Velike tvrtke često su suočene sa sigurnosnim incidentima bilo zbog materijalne koristi ili krađe povjerljivih podataka što može ozbiljno narušiti njihovo poslovanje. Tvrtke koje ne zaštite svoje informacijske sustave u skladu s postojećim rizicima često su meta napada ili zlonamjernih djelovanja zaposlenika. U današnje vrijeme, kada se tvrtke bore za tržišne pozicije, gubitak podataka, poput informacija o novom proizvodu, može imati ozbiljne posljedice. Uvođenjem i provođenjem sigurnosne politike, tvrtke osiguravaju adekvatnu zaštitu podataka, a u slučaju incidenta mogu pravno goniti počinitelje, ukoliko je to predviđeno sigurnosnom politikom. Institucije koje posjeduju velike baze povjerljivih podataka moraju te podatke zaštititi kako bi spriječile financijsku štetu, krađu identiteta i druge neugodnosti za osobe čiji se podaci nalaze u bazi, ukoliko te informacije dospiju u pogrešne ruke. Uspostavljanje sigurnosne politike smanjuje mogućnost otkrivanja povjerljivih podataka i uspostavlja strogi nadzor nad svim područjima djelatnosti organizacije. (CARNet CERT; LS&S, 2009)

6. Utjecaj zaposlenika

Kao što je opisano u prethodnim poglavljima, sigurnost informacijskih sustava može biti ugrožena na različite načine. Prijetnje možemo kategorizirati prema izvoru:

1. namjerne prijetnje od strane ljudi,
2. nenamjerne prijetnje od strane ljudi,
3. kvarovi opreme,
4. prirodne nepogode.

Iako mnogi vjeruju da su vanjski napadi, poput onih od strane hakera, glavni izvor prijetnji za sigurnost sustava, istraživanja predstavljena u knjizi D. Seger, K., VonStroch, W. „Computer Crime: A Crimefighter's Handbook“, O'Reilly & Associates, ukazuju na suprotno. Statistički podaci prikazani na slici 2 pokazuju da najveći udio problema sigurnosti uzrokuju ljudske greške, koje se najčešće događaju zbog nedostatka pažnje i nedovoljne educiranosti zaposlenika. Drugi najčešći uzrok problema u sustavima su kvarovi opreme, a zatim slijede zaposlenici koji koriste svoj položaj za osobnu korist ili izražavaju svoje nezadovoljstvo prema poduzeću ili nadređenima na ovaj način. (Kovačević, 2008)



Slika 2: Problemi sigurnosti u velikim organizacijama

Izvor: Kovačević D. (2008). "Sigurnosna politika".

Kako bi se smanjila mogućnost neželjenih aktivnosti, potrebno je implementirati odgovarajuće mjere. Edukacijom zaposlenika smanjuje se šansa za pogreške koje bi mogle ugroziti integritet i sigurnost sustava. Pohranjivanje opreme koja sadrži podatke u posebne prostorije, uz propisivanje tko ima pristup i kontroliranje uvjeta poput temperature i vlage, produžuje vijek trajanja opreme i osigurava pouzdaniji rad sustava. Kontrola pristupa podacima i definiranje sankcija za nepoštivanje pravila pomažu u sprječavanju zlouporabe sustava od strane zaposlenika. Iako su napadi izvana rjeđi, oni često uzrokuju najveću štetu. Takvi napadi, koji

čine mali postotak svih prijetnji, obično imaju za cilj pribavljanje, mijenjanje ili uništavanje informacija. Sustavi se štite od ovih prijetnji kontrolom prometa između interneta i sustava, sprječavanjem instaliranja neovlaštenih programa i kriptiranjem podataka. Implementacijom ovih mjera povećava se sigurnost informacijskih sustava, minimizirajući mogućnost nepoželjnih radnji.

Za postizanje maksimalne sigurnosti sustava potrebno je obratiti pažnju na:

- fizičku sigurnost,
- sigurnosne mjere za osoblje,
- sigurnost komunikacija,
- operacijsku sigurnost.

Temelj fizičke sigurnosti je zaštita fizičke infrastrukture, uključujući zgrade, medije za pohranu podataka i komunikacijsku opremu. Ove mjere uključuju zaštitu računalne infrastrukture od prirodnih nepogoda, okolišnih problema, nezgoda i namjernih oštećenja.

Prirodne nepogode kao što su požari, poplave, gromovi i potresi mogu ozbiljno ugroziti sigurnost informacijskih sustava. Računalna oprema je osjetljiva na dim, prašinu, vibracije i vlagu, pa nedostatak adekvatne zaštite može rezultirati uništenjem sustava i podataka. Električna energija također predstavlja značajnu prijetnju. Kvaliteta električne energije je kritična, jer nekvalitetna energija može uzrokovati oštećenje sustava ili gubitak podataka. Kontrola temperature i vlage u prostorijama gdje se nalazi oprema je također ključna. Kako bi se postigla odgovarajuća fizička sigurnost, pristup računalima i opremi mora biti strogo kontroliran.

Pristup računalnim sustavima koji trebaju biti zaštićeni trebao bi se organizirati kroz više kontrolnih točaka. Na primjer, osoba koja želi ući u prostor s računalnom opremom mora prvo proći čuvara, zatim zaključane sobe s alarmnim sustavima ili drugim oblikom zaštite, čime se otežava pristup potencijalnim napadačima.

Ispitivanje fizičke sigurnosti informacijskih sustava ključno je za definiranje mjera sigurnosti. Najgori scenarij je onaj koji uključuje namjernu štetu pa je nakon definiranja mjera sigurnosti potrebno ispitati njihovu učinkovitost. Postoje tri osnovna tipa testova za ispitivanje fizičke sigurnosti: konstantna ispitivanja, nenajavljene provjere kako bi se osiguralo da zaposlenici ne zaobilaze mjere sigurnosti i simulacija napada na osjetljivim mjestima.

Najveća prijetnja informacijskim sustavima su ljudi koji s njima rade, bilo svakodnevno ili povremeno. Osobe koje nisu dovoljno kvalificirane mogu nenamjerno ugroziti sustav, dok namjerne radnje zaposlenika mogu biti motivirane osobnim zadovoljstvom, koristima ili drugim razlozima. Statistike pokazuju da većina prijetnji dolazi od osoba koje imaju pristup sustavu, bilo unutar ili izvan organizacije. Stoga je važno pažljivo birati zaposlenike i pravovremeno prepoznati potencijalne opasnosti kroz promatranje događanja unutar i izvan organizacije.

Umrežavanje računala povećava snagu i brzinu obrade podataka, ali također povećava ranjivost sustava. Sigurnost komunikacije može se poboljšati kontrolom pristupa, kriptiranjem podataka, zaštitom vatrozidima i drugim mjerama fizičke zaštite. Kontrola pristupa je ključna, a mnogi sustavi koriste zaporke za osiguranje pristupa. Bitno je da zaporke budu poznate samo ovlaštenim korisnicima i da se pridržavaju osnovnih pravila pri njihovom čuvanju poput nepohranjivanja zaporki u blizini računala, izbjegavanja jednostavnih zaporki i nečuvanja zaporki u datotekama na računalu. (Kovačević, 2008)

Osim tih pravila, mogu se definirati dodatna pravila kontrolirane od strane sustava:

Zaporke generirane od sustava: zahtijevaju korištenje slučajno generirane zaporke koju je teško pogoditi. Mana je što su takve zaporke teško pamtljive pa ih korisnici često moraju zapisivati.

Minimalna duljina zaporke: duže zaporke su bolje od kratkih jer ih je teže pogoditi i treba više vremena za njihovo probijanje. Mnogi sustavi nameću minimalnu duljinu zaporke.

Vijek trajanja zaporke: kako bi se otežalo pogađanje i probijanje lozinke, mnogi sustavi zahtijevaju periodičko mijenjanje zaporki. Ako korisnik ne promijeni zaporku na vrijeme, ona prestaje vrijediti.

Ograničen broj pokušaja: mnogi sustavi dopuštaju ograničen broj pokušaja pristupa sustavu. Ako korisnik više puta unese pogrešnu zaporku, sustav ga odbacuje.

Poruka o zadnjem pristupu: prikazivanje datuma ili vremena zadnjeg pristupa može biti korisno. Ako korisnik primijeti da je netko pokušao pristupiti sustavu, a on se nije dugo koristio sustavom to može potaknuti sumnju.

Šifrirani i skriveni zapisi o zaporci: mnogi sustavi koriste šifrirane zapise za čuvanje zaporki, koje se pohranjuju na dobro osiguranim mjestima.

Zaključavanje zaporki: administratori mogu zaključati zaporke korisnika kako bi ograničili pristup sustavu ako korisnik ne može koristiti sustav određeno vrijeme ili nakon radnog vremena.

Pametne kartice: neki sustavi zahtijevaju pristup putem pametnih kartica i upisa osobnog identifikacijskog broja prije provjere zaporke.

Dodatne zaporke: neki sustavi imaju mogućnost postavljanja dodatnih zaporki. Korisnik mora unijeti zaporku sustava pa svoju vlastitu zaporku.

Jednokratne zaporke: koriste se i vrijede samo jednom pa ih je teško ukrasti.

Vremenski ovisne zaporke: zaporke koje se mijenjaju svake minute. Pametna kartica sadrži trenutno vrijeme i tajni korisnički ključ.

Kriptografske metode: još jedan način ograničavanja pristupa podacima, osobito važan kod slanja povjerljivih podataka mrežom. (Kovačević, 2008)

Kriptografija osigurava:

Tajnost izvornog teksta: sprječava neovlašten uvid u sadržaj.

Autentičnost izvornog teksta: osigurava vjerodostojnost poruke.

Integritet izvornog teksta: sprječava neovlaštene promjene sadržaja i oštećenja.

Zaštita informacijskih sustava od neprijateljskih mreža ili pojedinaca važan je segment sigurnosti. Jedan od najboljih sustava za zaštitu mreža nazvan je sigurnosnom stijenom, koja kontrolira količinu i vrstu prometa između interneta i mreže.

Postoje dva načina konfiguriranja sigurnosnih stijena:

Određena dozvola: postavlja se skup uvjeta koji rezultira blokiranjem podataka dok se sav promet koji nije pokriven policom dopušta.

Određena zabrana: omogućuje samo unaprijed definiranoj vrsti prometa prolaz dok se svi ostali blokiraju.

Operativna sigurnost uključuje povećanje svijesti među potencijalnim žrtvama i sprječavanje računalnih kriminalaca u počinjenju djela. Povećanje svijesti postiže se uključivanjem zaposlenika u sigurnosne programe i edukacijom o sigurnosnim rizicima. Informacije se dijele samo s onima kojima su nužne za rad. Operativna sigurnost ne može sama po sebi biti dovoljna, već se mora integrirati s drugim sigurnosnim programima kako bi bila učinkovita. (Kovačević, 2008)

7. Studije slučaja

1. SolarWinds

Godina 2020. bila je nevjerojatno turbulentna, puna globalnih događaja koji su potresli svijet. No, kako je godina završavala, dogodio se još jedan veliki udarac: SolarWinds hakerski napad, jedan od najvećih kibernetičkih proboja u 21. stoljeću.

SolarWinds i njegov značaj

SolarWinds, velika softverska tvrtka sa sjedištem u Tulsi, Oklahoma, pruža alate za upravljanje mrežama i infrastrukturom tisućama organizacija diljem svijeta. Jedan od njihovih ključnih proizvoda je sustav za nadzor IT performansi pod nazivom Orion.

SolarWinds napad

Ovaj hakerski napad poznat je po proboju lanca opskrbe koji je uključivao SolarWinds Orion sustav. Hakeri, za koje se vjeruje da su povezani s državnim akterima i koje je Microsoft nazvao Nobelium, stekli su pristup mrežama i podacima tisuća korisnika SolarWindsa. Razmjeri napada su ogromni, što ga čini jednim od najvećih ikada zabilježenih.

Kako je napad izveden

Hakeri su upotrijebili tehniku napada na lanac opskrbe kako bi ubacili zlonamjerni kod u Orion softver. Umjesto da izravno napadnu mreže, ciljali su treću stranu s pristupom sustavima organizacije. Ovaj pristup omogućio im je da postave stražnja vrata kroz koja su mogli pristupiti i manipulirati podacima bez detekcije.

Posljedice napada

Napad je ugrozio podatke i mreže tisuća organizacija, uključujući i mnoge vladine agencije poput Ministarstva domovinske sigurnosti i Ministarstva financija kao i velike privatne tvrtke poput FireEye, Microsofta i Cisca. Hakerski proboj otkrila je tvrtka FireEye, koja je također bila žrtva napada.

Trajanje i otkrivanje napada

Hakeri su prvi put pristupili sustavima SolarWindsa u rujnu 2019., a napad je otkriven tek u prosincu 2020., što znači da su napadači imali neometan pristup više od godinu dana. Ovo dugo razdoblje neotkrivenosti pripisuje se sofisticiranosti zlonamjernog koda Sunburst. ("SolarWinds hack explained: Everything you need to know", 2023)

Tko stoji iza napada

Istražitelji vjeruju da je napad djelo ruske obavještajne službe, iako ruska vlada odbacuje bilo kakvu umiješanost. Unatoč tim negiranjima, mnogi stručnjaci povezuju ovaj napad s ranijim cyber napadima za koje se sumnja da su djelo ruskih operativaca.

Ovaj napad je još jedan podsjetnik na važnost informacijske sigurnosti i potrebu za stalnim unapređenjem obrambenih mjera protiv sofisticiranih prijetnji ("SolarWinds hack explained: Everything you need to know", 2023).

2. Colonial Pipeline

Što se dogodilo u ransomware napadu na Colonial Pipeline

Još jedan veliki kibernetički napad poremetio je javne usluge, dospjevši u vijesti tijekom vikenda 8.-9. svibnja 2021. Ovaj put, meta je bio glavni američki naftovod. Colonial Pipeline, koji se proteže od Teksasa do New Yorka i osigurava 45% opskrbe gorivom na istočnoj obali, prekinuo je rad nakon napada hakerske skupine DarkSide. Hakeri su kasnije izjavili da im nije bila namjera "stvarati probleme društvu", već su samo htjeli zaraditi novac.

Razmjeri napada i reakcija

Bez obzira na njihove namjere, hakeri iz DarkSide-a uspjeli su obustaviti kritičnu infrastrukturu na nekoliko dana. Ovaj događaj predstavlja jedan od najvećih poremećaja u energetskoj infrastrukturi SAD-a. Postavlja se pitanje kako je jedan od ključnih američkih naftovoda mogao biti tako lako kompromitiran i prekinut.

Detalji napada na Colonial Pipeline

DarkSide hakeri preuzeli su odgovornost za ransomware napad koji je uzrokovao obustavu Colonial Pipeline-a. U svojoj izjavi na web stranici, hakeri su naveli da im je cilj bio "zaraditi novac, a ne stvarati probleme društvu", što sugerira da napad nije prošao prema njihovim planovima.

Nakon otkrića ransomwarea, Colonial Pipeline je odlučio prekinuti rad kako bi izbjegli teže posljedice. Na poslužitelju koji je koristila hakerska skupina pronađeni su važni podaci i druge datoteke Colonial Pipeline-a.

Financijski aspekti ransomware napada

Cilj ransomware napada je jednostavan: zaraditi novac. Prosječna otkupnina koju plaćaju žrtve ransomware napada u Europi, SAD-u i Kanadi skoro se utrostručila, s 115.123 dolara u 2019. na 312.493 dolara u 2020. godini. U slučaju Colonial Pipeline-a, kompanija je platila 4,4 milijuna dolara kako bi povratila dio svojih podataka.

Posljedice obustave Colonial Pipeline-a

Ovaj incident je razotkrio koliko je energetska infrastruktura osjetljiva na kibernetičke napade. Nakon nedavnog napada na postrojenje za pročišćavanje vode u Floridi, gdje su hakeri pokušali otrovati gradski vodovod, postalo je jasno koliko su energetski sektor i osjetljivi podaci vrijedni i ranjivi na hakerske napade.

Utjecaj na tržište i društvo

Obustava rada naftovoda poput Colonial Pipeline-a ima značajan utjecaj na tržište, uključujući porast cijena nafte, te utječe na poslovne sektore ovisne o gorivu, poput zračnog i cestovnog prijevoza. Zatvaranje ovog naftovoda poremetilo je distribuciju benzina, dizela i avionskog goriva na cijelom sjeveroistoku SAD-a, a potpuni povratak u funkciju očekivao se tek nakon nekoliko dana.

Kako je došlo do napada i može li se to spriječiti?

Skupina DarkSide izvela je napad pomoću ransomwarea. Ova vrsta zlonamjernog softvera infiltrira se u IT infrastrukturu cilja, pristupa najosjetljivijim podacima, te ih šifrira, blokirajući pristup vlasnicima dok se ne plati otkupnina.

Pretpostavlja se da DarkSide djeluje iz Rusije i koristili su daljinski pristup za ulazak u sustav Colonial Pipeline-a. Tijekom pandemije COVID-19, većina tvrtki je radila na daljinu, što povećava rizik zbog nesigurnih mreža i alata za daljinski pristup. Hakeri su vjerojatno iskoristili ranjivu točku za ulazak u sustav, a zatim su koristili privilegije kako bi se kretali unutar IT infrastrukture, kradući i šifrirajući najvrijednije podatke.

Preventivne mjere za zaštitu kritične infrastrukture

Organizacije, osobito one u energetskoj industriji, trebaju se usredotočiti na dvije ključne stvari:

Osigurati krajnje točke primjenom principa najmanjeg privilegija

Osigurati daljinski pristup kroz snažno upravljanje privilegiranim korisnicima i autentifikaciju identiteta

Da je Colonial Pipeline implementirao politiku temeljem principa najmanjeg privilegija, hakeri ne bi mogli iskoristiti ukradene vjerodajnice za pristup osjetljivim podacima i sustavima. Također, daljinski pristup trebao bi zahtijevati višefaktorsku autentifikaciju i validaciju putem sustava za upravljanje privilegiranim pristupom kako bi se osiguralo da samo ovlašteni korisnici mogu pristupiti sustavima.

Uvođenjem rješenja za upravljanje privilegijama na krajnjim točkama moglo bi se zaustaviti svaki pokušaj ransomware napada. Robusna rješenja za upravljanje privilegijama blokiraju svaki proces ili aplikaciju koja pokušava izvesti nedopuštene operacije, poput šifriranja, bez obzira na razinu privilegija korisnika ("What happened in the colonial pipeline ransomware attack", 2023).

3. Ina

Više od 30 dana trajao je hakerski napad na domaću naftnu kompaniju upravo u trenutku kada su podaci trebali biti dostupni stručnjacima iz konzultantske kuće Lazard, koja je za Vladu procjenjivala financijsko stanje u Ini i tražila najpovoljniji model otkupa MOL-ovih dionica. Postojala je velika vjerojatnost da je napad stigao iz Mađarske, da je pažljivo isplaniran i da je ciljan upravo na petak, 14. veljače, poslijepodne, kada je u kompaniji bio manji broj informatičara. Virus je imao dovoljno vremena da se proširi cijelim IT sustavom Ine, zaključavajući većinu poslovne dokumentacije i baza podataka. Prema izvorima bliskim vrhu Ine, napad je omogućio Mađarima da redizajniraju cijeli sustav bez odobrenja Vlade. IT stručnjaci potvrdili su ove navode, a Microsoftovi informatičari pomagali su u otključavanju napadnutih servera, no do zaključka Nacionalovog broja tek je dio baza podataka bio obnovljen.

Napad je zaključao poslovne podatke Ine baš u vrijeme kada su stručnjaci iz Lazarda provjeravali financijsko stanje kompanije za Vladu. Prema Nacionalovim izvorima, zlonamjerni virus (malware) zaključao je internu prepisku i sve poslovne baze podataka. Napadom je bilo zahvaćeno ukupno 180 servera Ine i njenih članica, ali sustav maloprodaje ostao je netaknut jer je bio na zasebnoj domeni. Izvor je potvrdio da je napad bio pažljivo isplaniran i da su napadači točno znali što rade. Ina je napadnuta ransomwareom, što je potvrdio i CERT, nacionalno tijelo za prevenciju računalnih ugroza. Prema neslužbenim informacijama, napadači su tražili otkupninu od 1500 bitcoina, odnosno oko 100 milijuna kuna.

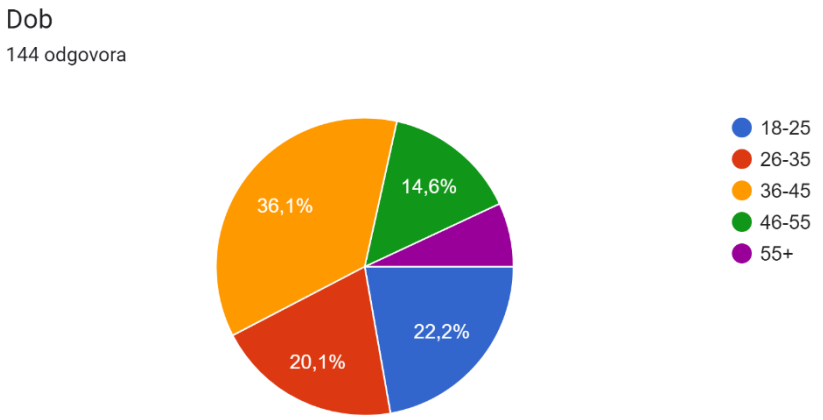
Najveći problem Ine bio je u nedostatku sustavnih sigurnosnih kopija (backup) baza podataka, što je otežalo oporavak sustava. Iako su iz Ine tvrdili da redovito rade backup, izvori su sumnjali u istinitost tih tvrdnji, jer bi oporavak u tom slučaju trajao samo nekoliko dana. U odgovoru Ine navodi se da je većina usluga oporavljena, no sustav još uvijek nije u potpunosti funkcionalan.

Tijekom napada, IT sektor Ine koristio je i usluge vanjskih suradnika. Na pitanje o kibernetičkom napadu, iz Ine su odgovorili da proces dubinskog snimanja kompanije nije bio ometan, ali izvori su tvrdili da konzultanti Lazarda nisu imali uvid u sve dokumente zbog kriptiranja. MUP je potvrdio da je kriminalističko istraživanje u tijeku, ali nisu mogli iznositi više detalja.

Nadzorni odbor Ine nije imao puno informacija o prirodi napada i šteti. Predsjednik Nadzornog odbora Damir Vanđelić rekao je da će vjerojatno imati više informacija tijekom tjedna, ali nije čuo ništa što bi opravdavalo sumnje da je napad povezan s radom Lazardovih konzultanata. Nažalost, daljnje informacije nisu objavljene do dan danas ('HAKERSKI NAPAD NA INU pokrenut je iz Mađarske i zaključao je podatke o poslovanju potrebne Lazardu', 2020).

8. Anketno istraživanje

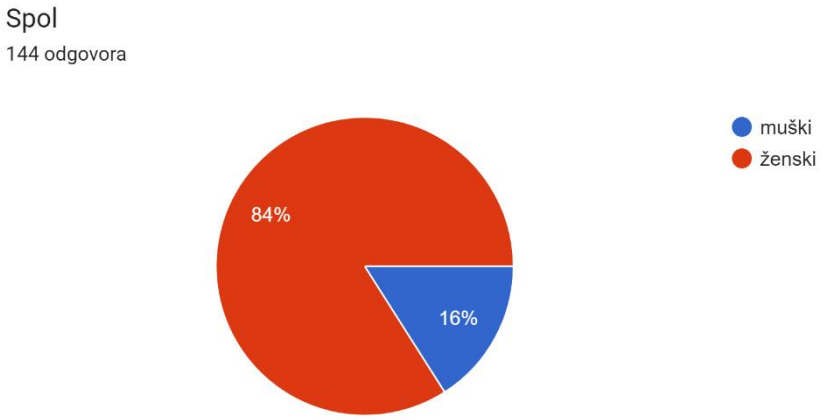
Grafikon 1: Dob ispitanika



Izvor: autorica

Najviše ispitanika je u dobi od 36 do 45 godina, njih čak 36,1%, slijedi ih dobna skupina od 18 do 25 sa svojih 22,2%, zatim skupina od 26 do 35 godina sa 20,1% i na kraju sa 7% imamo dobnu skupinu od 55+ godina.

Grafikon 2: Spol ispitanika



Izvor: autorica

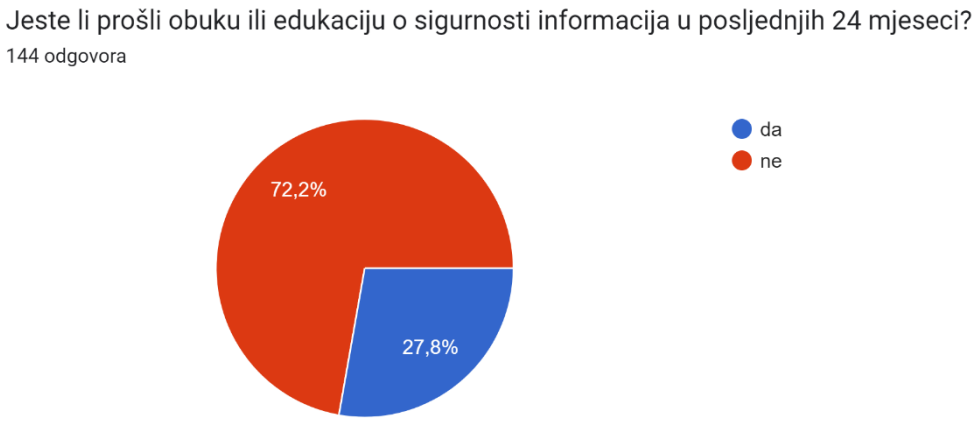
U ovom grafikonu vidimo da su najvećim brojem ispitanika upravo žene sa vodećih 84% dok je muškaraca 16%.

Grafikon 3: Važnost sigurnosti informacija u organizacijama

Izvor: autorica

Na pitanje o važnosti sigurnosti informacija u organizaciji 65,3% ispitanika smatra da su prilično svjesni koliko je sigurnost informacija važna. 27,8% ih smatra da su djelomično svjesni, dok njih 6,9% iskreno tvrdi da su vrlo malo svjesni.

Grafikon 4: Obuka ili edukacija o sigurnosti informacija u posljednjih 24 mjeseci

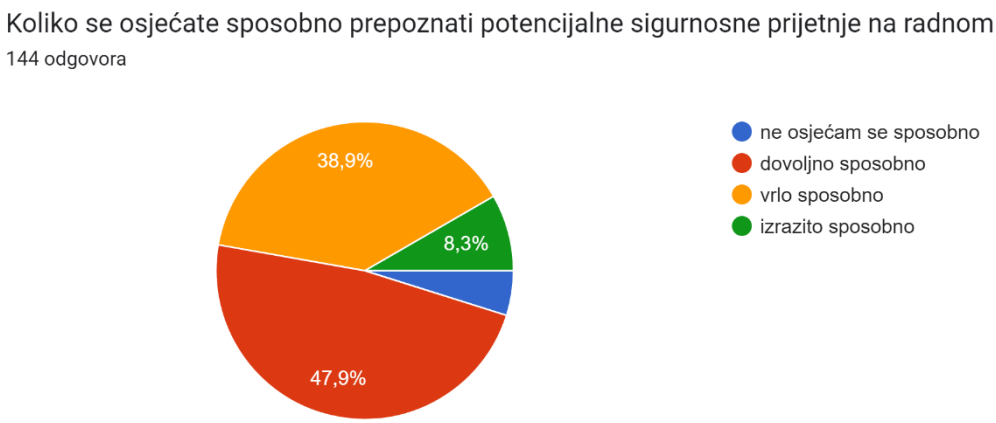


Izvor: autorica

Što se tiče obuke ili edukacije o sigurnosti informacija, tijekom posljednjih 24 mjeseci čak 72,2% zaposlenika nije prošlo ni jednu vrstu obuke ili edukacije. Ostalih 27,8% tvrdi da jesu.

Rezultatima ovog grafikona vidimo da nisu samo zaposlenici krivi za potencijalne propuste u sigurnosti informacija već i sami menadžeri koji zanemaruju obuke i edukacije za zaposlenike koje su ključne za informacijski sustav.

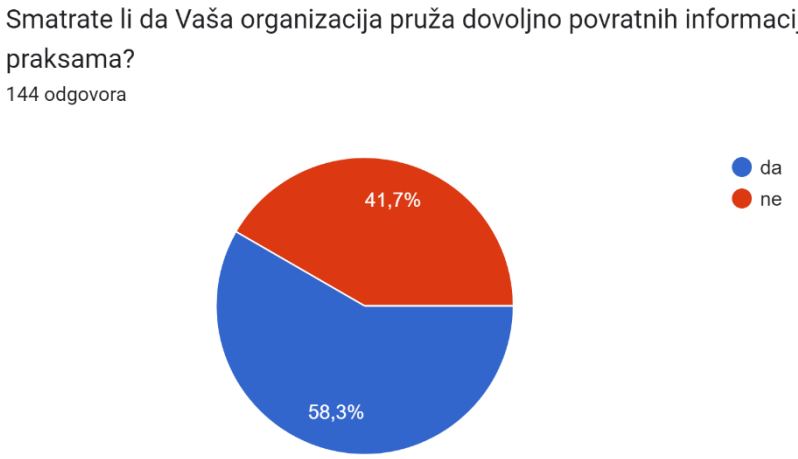
Grafikon 5: Osjećaj sposobnosti za prepoznavanje potencijalnih prijetnji na radnome mjestu



Izvor: autorica

47,9% ispitanika osjeća se dovoljno sposobno prepoznati potencijalne sigurnosne prijetnje na radnome mjestu, slijede ih oni koji se osjećaju vrlo sposobno, njih 38,9%. Izrazito sposobno osjeća se njih 8,3% i 4,9% se ne osjeća sposobno.

Grafikon 6: Pružanje dovoljno informacija i resursa o sigurnosnim praksama od strane organizacije



Izvor: autorica

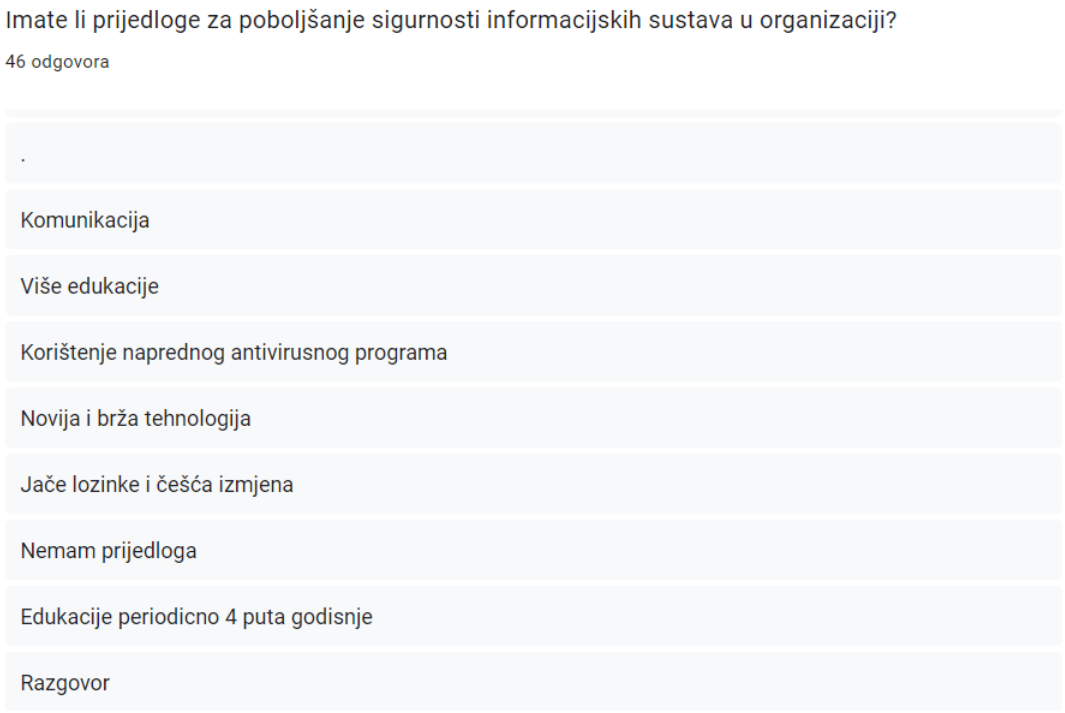
58,3% ispitanika smatra da njihova organizacija pruža dovoljno o sigurnosnim praksama, dok ostalih 41,7% ne smatra isto.

Grafikon 7: Važnost suradnja između zaposlenika za očuvanje sigurnosti informacijskih sustava

Izvor: autorica

U ovoj situaciji pola ispitanika smatra da je suradnja između zaposlenika vrlo važna, a druga polovica da je jako važna.

Grafikon 8: Prijedlozi za poboljšanje sigurnosti informacijskih sustava u organizaciji



Izvor: autorica

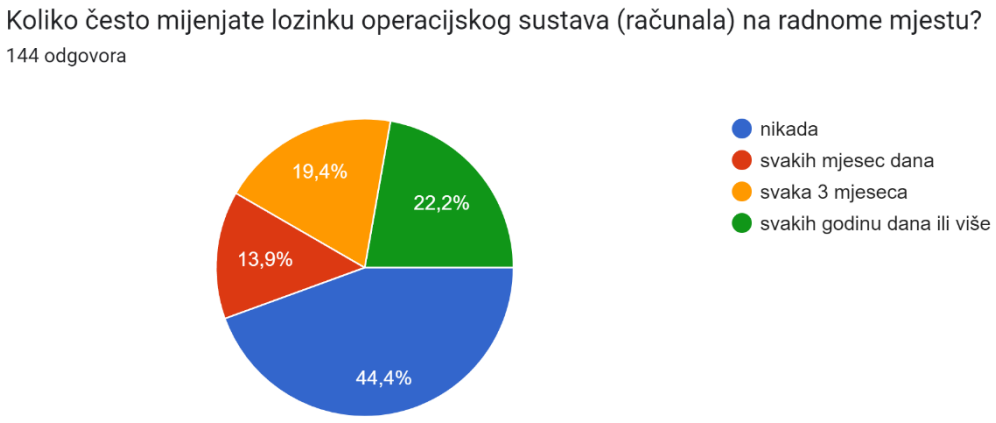
Na pitanje o prijedlozima za poboljšanje sigurnosti, od 144 ispitanika svoj odgovor je dalo njih 46. Iz tih 46 odgovora ovo su neki odgovori koji su se izdvojili od ostalih.

Grafikon 9: Korištenje lozinke prilikom pristupanja računalu

Izvor: autorica

88,9% ispitanika koristi lozinku prilikom pristupanja računalu, ostalih 11,1% ne koristi lozinku.

Grafikon 10: Mijenjanje lozinki na radnome mjestu



Izvor: autorica

Što se tiče mijenjanja lozinki operacijskog sustava na radnome mjestu, 44,4% ispitanika nikada ne mijenja svoju lozinku. 22,2% mijenja lozinku svakih godinu dana ili više. 19,4% mijenja lozinku svaka 3 mjeseca, a 13,9% što je i najmanje, svakih mjesec dana.

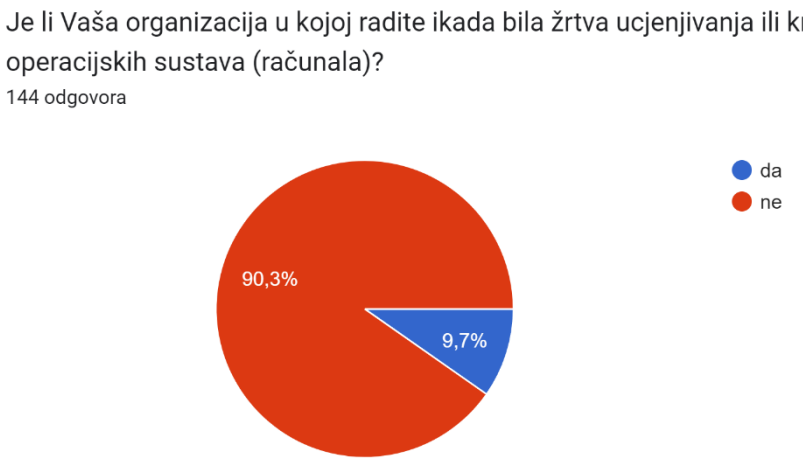
Ovim rezultatom vidimo koliko je svijest zaposlenika o sigurnosti informacija kriva jer upravo bi često mijenjanje lozinki operacijskog sustava kao i njihova jačina trebali biti prvi korak zaštite informacijskih sustava organizacije.

Grafikon 11: Držanje prijenosnog računala na stolu gdje je dostupno svima

Izvor: autorica

77,8% ispitanika smatra da nije ispravno držati prijenosno računalo na stolu gdje je dostupno svima dok ostalih 22,2% ne vidi problem u tome.

Grafikon 12: Žrtve ucjenjivanja ili krađe podataka informacijskih sustava



Izvor: autorica

90,3% ispitanika radi u organizacijama koje nikada nisu bile žrtve ucjenjivanja ili krađe podataka dok je 9,7% proživjelo ili krađu podataka ili ucjenjivanje.

Važno je uzeti u obzir rezultat ovog grafikona koji je očekivan upravo na ovaj način zbog mreže na kojoj se anketa i podijelila. Anketa je provedena uz pomoć Facebook poznanika i prijatelja, od kojih velika većina nije na radnoj poziciji povezanoj sa računalima. Stoga, većina ispitanika zbog zaštite ugleda organizacija ni nije informirana da je organizacija možda i bila žrtva ucjenjivanja ili krađe podataka. Predviđa se da bi rezultat bio obrnut ukoliko bi anketa bila podijeljena u grupi prisutnih menadžera, kontrolera, znanstvenika, informatičara i srodnih zanimanja.

Anketni upitnik: https://docs.google.com/forms/d/1nCsjvB7phfV-i-HAktNqIb8ssw-_s5B4vsD1Us56j_Y/edit#responses

9. Zaključak

Poznavanje načina na koji zaposlenici utječu na sigurnost informacijskog sustava ključno je za svaku tvrtku koja želi zaštititi svoje podatke i održavati točne informacije. Radnici su obično ključni, bilo kao temelj zaštite ili moguća slabost koja se uglavnom temelji na njihovoj svijesti, obrazovanju i djelima. Proučavanje rezultata ankete ukazuje na glavne čimbenike koji oblikuju utjecaj zaposlenika na mjere zaštite informacijskih sustava organizacije. Ovi rezultati ukazuju na važne dijelove bitne za razumijevanje i podizanje sigurnosnih radnji na radnom mjestu. Prepoznavanje važnosti sigurnosti podataka prilično je rašireno jer većina ispitanika to dobro razumije. Još uvijek velik dio zaposlenika ne razumije u potpunosti ili samo donekle razumije koliko su sigurnosni postupci ključni, što naglašava potrebu za stalnim podizanjem svijesti i podučavanjem. Nedostatak obuke i obrazovanja je stvarno veliki problem. Mnogi ljudi koji su odgovorili nisu prošli nikakvu obuku o čuvanju informacija u proteklih nekoliko godina, što pokazuje da menadžment ima veliku odgovornost. Kako bismo bili sigurni da su naši informacijski sustavi često sigurniji, vrlo je važna kvalitetna obuka. Rezultati pokazuju da već postoji pristojna polazna točka, ali također je jasno da moramo učiniti više kako bi svi radnici lakše uočili opasnosti. Dok većina ljudi misli da im njihove tvrtke daju dovoljno informacija i resursa za sigurnosne mjere, veliki broj radnika nije uvjeren u to. To pokazuje da tvrtke moraju postati bolje u komunikaciji o ovim stvarima i pružanju zaposlenicima pravih alata koji su im potrebni. Svi koji su odgovorili na anketna pitanja, slažu se da je suradnja važna ili jako važna za očuvanje sigurnosti informacijskih sustava. Moramo se zalagati za timsku atmosferu kako bi se zajedno mogli pozabaviti sigurnosnim problemima. Iako mnogi od njih koriste lozinke na svojim računalima, gotovo polovica se uopće ne trudi mijenjati te lozinke. Podaci pokazuju da postoji nesvijest o potrebi čestog mijenjanja lozinki, što je jednostavan, ali važan način da se stvari očuvaju sigurnima. Mnogi od onih koji su odgovorili iz mjesta su gdje nije bilo incidenata ucjena ili gubitka podataka, međutim ovi rezultati možda nisu potpuno točni na temelju načina na koji su postavljena pitanja. Oni možda ne pokazuju što se stvarno događa na radnim mjestima. Ishod iz ovog istraživanja naglašava da zaposlenici igraju veliku ulogu u održavanju sigurnosti informacijskog sustava. Postoje prijedlozi kao što je stalna edukacija, bolji razgovor unutar radne okoline i pružanje više pomoći, također navođenje ljudi na zajednički rad može ojačati sigurnost. Rukovodstvo ima dužnost pobrinuti se da zaposlenici dobiju odgovarajuće informacije i obuku. Ovo smanjuje rizik povezan s ljudskim utjecajima u održavanju sigurnosti informacijskih sustava.

Sveučilište Sjever

SVEUČILIŠTE SJEVER

IZJAVA O AUTORSTVU

Završni/diplomski/specijalistički rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, KLAUDIA SELTHOFER *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog/specijalističkog (*obrisati nepotrebno*) rada pod naslovom UTJECAJ ZAPOSLENIKA NA SIGURNOST INFORMACIJSKIH SUSTAVA ORGANIZACIJE *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)

Klaudia Selthofer
(vlastoručni potpis)

Sukladno članku 58., 59. i 61. Zakona o visokom obrazovanju i znanstvenoj djelatnosti završne/diplomske/specijalističke radove sveučilišta su dužna objaviti u roku od 30 dana od dana obrane na nacionalnom repozitoriju odnosno repozitoriju visokog učilišta.

Sukladno članku 111. Zakona o autorskom pravu i srodnim pravima student se ne može protiviti da se njegov završni rad stvoren na bilo kojem studiju na visokom učilištu učini dostupnim javnosti na odgovarajućoj javnoj mrežnoj bazi sveučilišne knjižnice, knjižnice sastavnice sveučilišta, knjižnice veleučilišta ili visoke škole i/ili na javnoj mrežnoj bazi završnih radova Nacionalne i sveučilišne knjižnice, sukladno zakonu kojim se uređuje umjetnička djelatnost i visoko obrazovanje.

10. Literatura

K. Klasić, K. Klarin: Informacijski sustavi, načela i praksa, Visoka škola za informacijske tehnologije, 2009.

V. Bosilj Vukšić, K. Ćurko, B. Jaković i dr.: Osnove poslovne informatike, Sveučilište u Zagrebu, Ekonomski fakultet, 2020.

V. Šimović: Uvod u informacijske sustave, Golden marketing – Tehnička knjiga, Učiteljski fakultet Sveučilišta u Zagrebu, 2010.

Kovačević, D: Sigurnosna politika, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, 20008.

Zubović, A: Sigurnost informacijskih sustava, Sveučilište u Rijeci, Pomorski fakultet, 2022.

Loch, K., Carr, H., Warkentin, M., Threats to Information Systems, Today's Reality, Yesterday's

Understanding, Management Information Systems Quarterly, 1992.

https://www.f5.com/labs/learning-center/what-is-the-cia-triad (29.05.2024.)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (29.05.2024.)

https://edutorij-admin-api.carnet.hr/storage/extracted/c4e1aebf-48e0-4d92-b6a9-0716a4e1c740/html/433_zlonamjerni_programi_-_razlike_nacin_djelovanja.html (03.06.2024.)

https://www.cert.hr/wp-content/uploads/2019/04/CCERT-PUBDOC-2008-01-215.pdf (06.06.2024.)

https://plaviured.hr/vodici/krada-identiteta-sto-je-i-kako-se-od-nje-zastititi/ (13.06.2024.)

https://www.kaspersky.com/resource-center/definitions/what-is-doxing (13.06.2024.)

https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-ddos-attack (13.06.2024.)

https://dir.hr/sto-je-phishing-krada-identiteta/ (13.06.2024.)

https://www.cert.hr/wp-content/uploads/2009/05/CCERT-PUBDOC-2009-05-265.pdf (14.06.2024.)

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (20.06.2024.)

https://www.wallix.com/what-happened-in-the-colonial-pipeline-ransomware-attack-2/ (20.06.2024.)

https://www.nacional.hr/hakerski-napad-na-inu-pokrenut-je-iz-madarske-i-zakljucao-je-podatke-o-poslovanju-potrebne-lazardu/ (21.06.2024.)

Anketa:https://docs.google.com/forms/d/1nCsjvB7phfV-i-HAktNqIb8ssw-_s5B4vsD1Us56j_Y/edit#responses