Sigurnosni aspekt poslovnih informacijskih sustava i primjena istih na primjeru poduzeća XY

Benić, Tomislav

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studij

Informacijske tehnologije

TOMISLAV BENIĆ

SIGURNOSNI ASPEKT POSLOVNIH INFORMACIJSKIH SUSTAVA I PRIMJENA ISTIH NA PRIMJERU PODUZEĆA XY

STRUČNI ZAVRŠNI RAD

Zaprešić, 2021. godine

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studij

Informacijske tehnologije

STRUČNI ZAVRŠNI RAD

SIGURNOSNI ASPEKT POSLOVNIH INFORMACIJSKIH SUSTAVA I PRIMJENA ISTIH NA PRIMJERU PODUZEĆA XY

Mentor:
Lacković, fali titula

Student:
Tomislav Benić

Naziv kolegija:
e-KANALI U POSLOVANJU

JMBAG studenta:
0224055120

Sadržaj

SAŽETAK

Cilj ovog rada je upoznati čitatelja/e kako sigurnost informacijskih sustava nije statičan, već dinamičan objekt koji prati tehnički razvoj. U vremenima kada je bilo manje velikih računala kojima su upravljali isključivo stručnjaci, IT sigurnost nije igrala nikakvu ulogu i bila je usmjerena na fizičku zaštitu pristupa sustavu. Sa sve većim stupnjem elektroničkog predstavljanja, umrežavanja i kontrole stvarnih procesa u informacijskim sustavima, širi se opseg pojma “IT sigurnost” i tako utječe na vrstu potrebnih i dostupnih sigurnosnih mehanizama.. IT sigurnost ima različite aspekte, ali konkretno, važno je sustavno razjasniti što se od čega treba zaštititi, koje prijetnje postoje te kojih mjera se treba pridržavati.

Ključne riječi: informacijski sustavi, mjere zaštite, sigurnost

ABSTRACT

The aim of this paper is to acquaint the reader(s) that the security of information systems is not a static, but a dynamic object that monitors technical development. In times when there were fewer large computers operated exclusively by experts, IT security played no role and was focused on physically protecting access to the system. With the increasing degree of electronic representation, networking and control of real processes in information systems, the scope of the term "IT security" is expanding and thus affects the type of necessary and available security mechanisms. IT security has different aspects, but specifically, it is important to specify what to protect against, what threats exist and what measures to follow.

Key words: Information systems, caution measures, security

1. UVOD

Informacije koje se tiču pojedinaca imaju vrijednost. Tvrtke se sve više oslanjaju na računalne sustave i mreže kako bi olakšale svoje kritično poslovanje. Danas organizacije djeluju u globalnom multi-poduzetnom okruženju uz korištenje suradnje putem telekomunikacijskih mreža, posebice interneta. S povećanjem korištenja informacijskog sustava, velika se pozornost sada usmjerava na sigurnost.

Uz povećanu digitalizaciju većine organizacijskih procesa, raste potreba za zaštitom informacija i sprječavanjem neovlaštenog pristupa osjetljivim informacijama. Mnoge tvrtke postale su plijen hakera i drugih ljudi koji imaju zlonamjerne namjere. Stoga postoji snažna potreba za zaštitom osjetljivih informacija od neovlaštenog pristupa i što je još važnije, postoji snažna potreba za sprječavanjem neovlaštenog fizičkog pristupa sigurnim područjima.

U svjetlu gore navedenih zapažanja, ovaj rad nastoji identificirati i analizirati sve potencijalne ranjivosti sustava informacijske sigurnosti te primjenu istih na poduzeću XY te mjere zaštite koje preporučuju institucije koje djeluju na području informacijske sigurnosti.

2. POJAM INFORMACIJSKOG SUSTAVA

Kako bismo definirali informacijski sustav, moramo biti upoznati sa pojmovima podatak, informacija i sustav.

Jednostavno rečeno, podatak je skup simbola kojima zapisujemo činjenice, ne razmatrajući kontekst iste (Varga, 2014.)

Informacija nastaje onda kada te podatke stavimo u neki kontekst i postaje činjenica s određenim značenjem koja donosi novost, otklanja neizvjesnost te služi kao podloga za odlučivanje (Varga, 2014.).

Prema hrvatskoj enciklopediji sustav je „skup elemenata povezanih u funkcionalnu cjelinu“. U našem slučaju skup elemenata predstavlja informacije koje povezujemo u cjelinu zvanu informacijski sustav.

Informacijski sustav je „sustav koji prikuplja, pohranjuje, čuva, obrađuje i isporučuje informacije važne za organizaciju i društvo, tako da budu dostupne i upotrebljive za svakog tko ih želi koristiti, uključujući poslovodstvo, klijente, osoblje i ostale“. (Varga, 2014.)

Prema Vargi, informacijski sustav za cilj ima opskrbiti poslovni sustav svim informacijama koje su mu potrebne za:

- Izvođenje poslovnog procesa
- Upravljanje poslovnim sustavom
- Suradnju i komunikaciju unutar poslovnog sustava i prema okolini

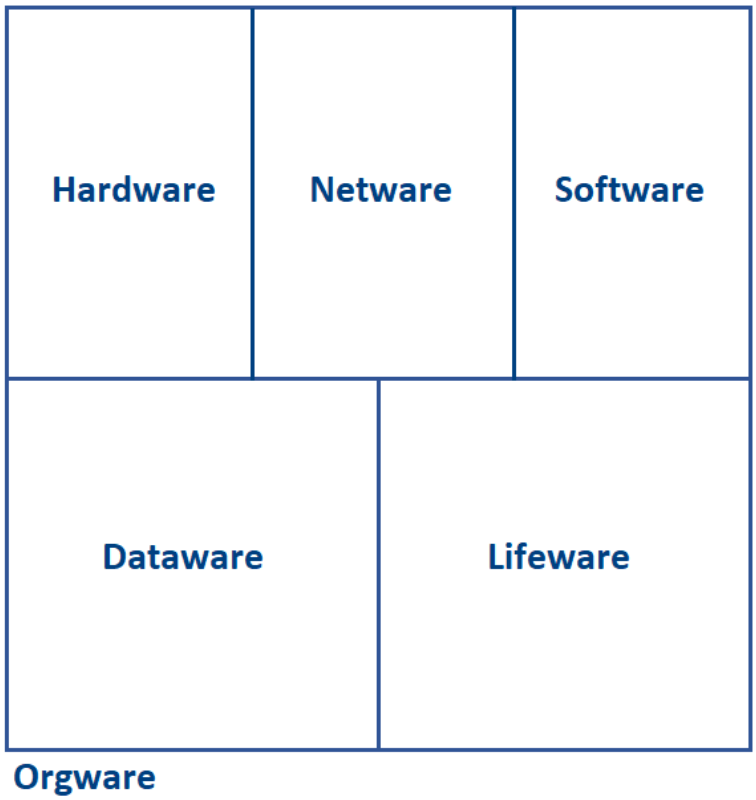
Dakle, poslovni sustav mora imati vlastiti informacijski sustav da bi opstao. Informacijski sustav može biti ručni ili automatiziran uz pomoć suvremene informacijske tehnologije. Poslovni sustav prikuplja podatke iz raznih internih i vanjskih izvora koje informacijski sustav zatim pretvara u nove i vrijedne podatke. Konačna svrha informacijskog sustava je pružiti vrijedne informacije poslovnom sustavu kako bi mogao poslovati i donositi poslovne odluke, odnosno odlučivati.

Šest komponenti čini svaki informacijski sustav (Spremić i Srića, 2000.):

1. **Hardware** – Fizička oprema koja se koristi za ulaz, izlaz i obradu. Struktura hardvera ovisi o vrsti i veličini organizacije. Sastoji se od ulaznog i izlaznog uređaja, operativnog sustava, procesora i medijskih uređaja. To također uključuje računalne periferne uređaje.
2. **Software** – Programi/aplikacijski program koji se koristi za kontrolu i koordinaciju hardverskih komponenti. Koristi se za analizu i obradu podataka. Ovi programi uključuju skup uputa koje se koriste za obradu informacija.
3. **Netware** – Mrežni resursi odnose se na telekomunikacijske mreže kao što su intranet, ekstranet i internet. Ovi resursi olakšavaju protok informacija u organizaciji. Mreže se

sastoje od fizičkih uređaja kao što su mrežne kartice, usmjerivači, čvorišta i kabeli te softvera kao što su operativni sustavi, web poslužitelji, poslužitelji podataka i aplikacijski poslužitelji. Telekomunikacijske mreže sastoje se od računala, komunikacijskih procesora i drugih uređaja međusobno povezanih komunikacijskim medijima i kontroliranih softverom. Mreže uključuju komunikacijske medije i mrežnu podršku.

4. **Lifeware** – Povezan je s radnom snagom potrebnom za pokretanje i upravljanje sustavom. Ljudi su krajnji korisnik informacijskog sustava, krajnji korisnik koristi informacije proizvedene za vlastitu svrhu, glavna svrha informacijskog sustava je dobrobit krajnjeg korisnika. Krajnji korisnik mogu biti računovođe, inženjeri, prodavači, kupci, službenici ili menadžeri itd. Ljudi su također odgovorni za razvoj i upravljanje informacijskim sustavima. Uključuju analitičare sustava, računalne operatere, programere i drugo službeno osoblje IS-a te upravljačke tehnike.,
5. **Orgware** – organizacijski postupci kojima se raznim postupcima sve komponente usklađuju u jednu cjelinu
6. **Dataware** – Podacima se upravlja pomoću suustava upravljanja bazama podataka. Softver baze podataka koristi se za učinkovit pristup potrebnim podacima i za upravljanje bazama znanja.



Slika 1 - Komponente IS-a

Izvor: izrada autora

3. MJERE ZAŠTITE INFORMACIJSKIH SUSTAVA

Kako su računala i drugi digitalni uređaji postali sve važniji u poslovanju i trgovini, također su postali ranjiviji na cyber-napade[1]. Kako bi s povjerenjem koristili računalni uređaj, tvrtka ili pojedinac prvo mora biti siguran da oprema nije ni na koji način ugrožena i da su sve veze sigurne. U ovom ćemo poglavlju proći kroz osnove sigurnosti informacijskog sustava, kao i neke od postupaka koji se mogu poduzeti za ublažavanje sigurnosnih zabrinutosti. Započet ćemo s pregledom na visokoj razini o tome kako tvrtke mogu ostati sigurne. Razmotrit će se nekoliko različitih sigurnosnih mjera koje tvrtka može koristiti. Nakon toga, proći ćemo kroz nekoliko sigurnosnih mjera koje pojedinci mogu poduzeti kako bi zaštitili svoje osobno računalo.

3.1. Trijada informacijske sigurnosti – CIA

Trijada informacijske sigurnosti, poznata kao CIA (hrv. PID), model je osmišljen da vodi politike za informacijsku sigurnost unutar organizacije. Skraćenica je za tri koraka koje tvrtka mora poduzeti kako bi zaštitila svoj informacijski sustav: Confidentiality (povjerljivost), Integrity (integritet) i Availability (dostupnost).

3.1.1. Confidentiality (povjerljivost)

Prema Stapletonu, kada je riječ o zaštiti podataka, želimo biti u mogućnosti ograničiti pristup onima kojima je dopušteno da ih vide; svima ostalima treba zabraniti da saznaju bilo što o njegovom sadržaju. Time je definirana povjerljivost. Uzmimo za primjer Veleučilište koje je prema zakonu dužno ograničiti pristup povjerljivim informacijama o studentima. Samo pojedinci kojima je dopušten pristup bi trebali imati pristup evidenciji ocjena.

3.1.2. Integrity (integritet)

Integritet je jamstvo da informacija kojoj se pristupa nije promijenjena i da uistinu predstavlja ono što je namijenjeno. Integritet informacija pokazuje da informacija ispravno prenosi svoje namjeravano značenje, baš kao što osoba s integritetom znači ono što govori i može joj se vjerovati da će dosljedno predstavljati istinu. Zla namjera može uzrokovati gubitak integriteta informacija, na primjer kada netko kome nije dopušteno izvrši promjenu kako bi namjerno nešto pogrešno predstavio (Stapleton, 2014.). Na primjeru Veleučilišta to možemo prikazati na način da student, u ovom slučaju ćemo ga nazvati hakerom[2], uđe u veleučilišni sustav i izmijeni ocjenu. Integritet se također može nenamjerno izgubiti, primjerice kada napon računala ošteti

[1] Cyber - pridjev koji se odnosi na ili je karakterističan za kulturu računala, elektroničke komunikacijske mreže, informacijske tehnologije i virtualnu stvarnost (Oxford dictionary)

[2] Haker je računalni stručnjak koji koristi svoje tehničko znanje kako bi prevladao problem; u popularnoj kulturi koristi se za nekoga tko sa svojim tehničkim znanjem koristi svoje sposobnosti kako bi provalio u računalne sustave (https://en.wikipedia.org/wiki/Hacker)

datoteku ili kada netko s ovlasti za unošenje promjena izbriše datoteku ili unese pogrešne podatke.

3.1.3. Availability (dostupnost)

Treća komponenta CIA trijade prema Stapletonu je dostupnost informacija. Informacijama može pristupiti i uređivati ih bilo tko kome je to dopušteno u razumnom vremenskom okviru ako su dostupne. Odgovarajuće vrijeme može ukazivati na mnoge stvari ovisno o vrsti informacija. Trgovac dionicama, na primjer, treba brz pristup informacijama, dok prodavač može biti zadovoljan time da sljedećeg jutra dobije podatke o prodaji za dan u izvješću.

Slika 2 - CIA trijada

Izvor: https://www.researchgate.net/figure/The-Confidentiality-Integrity-Availability-CIA-triad

3.2. Alati informacijske sigurnosti

Kako bi se osigurala CIA trijada, organizacije mogu birati između raznih alata. Svaki od ovih alata može se koristiti kao dio opće politike sigurnosti informacija.

3.2.1. Autentifikacija

Prema Bourgeoisu, provjera autentičnosti može se provesti korištenjem jednog ili više od tri čimbenika za identifikaciju nekoga: nešto što zna, nešto što ima ili nešto što jest. Danas je najrašireniji oblik provjere korištenje korisničkog ID-a i lozinke. U ovoj situaciji, korisnik se autentificira potvrđivanjem onoga što već zna (ID i lozinka). Međutim, ovu vrstu provjere autentičnosti lako je kompromitirati, te su povremeno potrebne jače metode provjere autentičnosti. Zato je drugi faktor neki token, koji ćese koristiti zajedno s ID-jem i lozinkom. No teško je identificirati nekoga samo na temelju onoga što posjeduje, npr. kluča ili pristupne kartice jer se identifikacijski token može izgubiti ili ukrasti, a s njime i identitet. To nas dovodi

do korištenja trećeg faktora – biometrije, a to identifikacija na temelju fizičkih karakteristika, kao što su skeniranje oka ili otiska prsta.

3.2.2. Kontrola pristupa

Nakon što je korisnik autentificiran, sljedeći korak je osigurati da može pristupiti samo odgovarajućim informacijskim resursima. To se postiže korištenjem kontrole pristupa. U nastavku ćemo spomenuti dvije vrste koje opisuje Bourgeois: ACL (Action Control List) i RBAC (Role-Based Action Control).

ACL, odnosno popis kontrole pristupa, za svaki informacijski resurs kojim organizacija želi upravljati izrađuje popis korisnika koji imaju mogućnost poduzimanja određenih radnji kojima se dodjeljuju specifične mogućnosti s kojima će obavljati svoje funkcije. Ako korisnik nije naveden na nekom od popisa, ne može ni znati da informacija postoji. Iako su ti popisi jednostavni za razumijevanje i održavanje, primarni im je nedostatak zasebno upravljanje resursima, a kako se broj korisnika i resursa s vremenom povećava, to je teže ACL održavati. Taj nedostatak je doveo do poboljšanja kontrole pristupa temeljen na ulogama ili skraćeno RBAC.

Tablica 1 - Primjer ACL-a

Izvor: izrada autora

Korisnik	FUNKCIJA 1	FUNKCIJA 2	FUNKCIJA 3	...	FUNKCIJA N
KORISNIK 1	X		X		
KORISNIK 2	X	X			
KORISNIK3	X	X			X
...					
KORISNIK N	X	X			X

Uz RBAC, umjesto da se određenim korisnicima daju prava pristupa informacijskom resursu, korisnicima se dodjeljuju uloge, a zatim se tim ulogama dodjeljuje pristup što omogućuje odvojeno upravljanje korisnicima i ulogama čime se pojednostavljuje upravljanje, ali i povećava sama sigurnost.

Tablica 2 - Primjer RBAC-a

Izvor: izrada autora

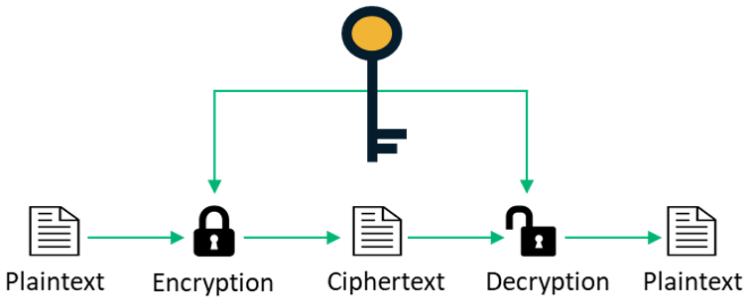
Uloga	FUNKCIJA 1	FUNKCIJA 2	FUNKCIJA 3	⋮	FUNKCIJA N
ADMINISTRATOR	X	X	X		X
KORISNIK	X	X			
ODRŽAVANJE	X	X			X
...					
FINANCIJE	X		X		X

Korisnik	Uloga
tbenic	ADMINISTRATOR
iivic	KORISNIK
pperic	KORISNIK
...	...
mmaric	FINANCIJE

3.2.3. Enkripcija

Enkripcija je tehnika šifriranja podataka tako da ih mogu dešifrirati samo ovlaštene strane. To je proces transformacije čovjeku čitljivog otvorenog teksta u nerazumljiv tekst, također poznat kao šifrirani tekst, u tehničkom smislu. Drugim riječima, šifriranje uzima čitljive podatke i čini ih nasumičnima te zahtijeva korištenje kriptografskog ključa, koji je skup matematičkih vrijednosti o kojima su se dogovorili i pošiljatelj i primatelj šifrirane poruke.[3]

Dvije glavne vrste šifriranja podataka su asimetrična enkripcija i simetrična enkripcija.[4] Simetričnu enkripciju postiže računalni program, koji kodira običan tekst koji treba prenijeti. Tada primatelj prima šifrirani tekst i dekodira ga . Kako bi to funkcioniralo, pošiljatelj i primatelj moraju se dogovoriti o metodi kodiranja kako bi obje strane mogle pravilno komunicirati. Obje strane dijele ključ za šifriranje, što im omogućuje da međusobno kodiraju i dekodiraju poruke. No ova vrsta enkripcije je problematična jer je ključ dostupan na dva različita mjesta.

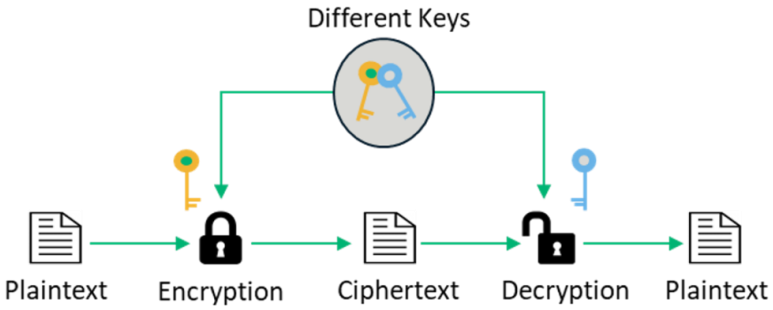


Slika 3 - Simetrična enkripcija

Izvor: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

[3] https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/, pristupljeno 26.10.2021.
[4] https://www.ibm.com/topics/encryption, pristupljeno 26.10.2021.

Kao alternativu za šifriranje simetričnog ključa koristi se asimetrično šifriranje s javnim ključem, u kojem se koriste dva ključa: javni ključ i privatni ključ. Da biste poslali šifriranu poruku, morate dobiti javni ključ, kodirati poruku i poslati je. Primatelj tada koristi privatni ključ za dekodiranje. Javni ključ može dobiti svatko tko želi primatelju poslati poruku. Svaki korisnik jednostavno treba jedan privatni ključ i jedan javni ključ kako bi osigurao poruke. Privatni ključ je neophodan za dešifriranje nečega poslanog s javnim ključem.



Slika 4 - Asimetrična enkripcija

Izvor: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

3.2.4. Lozinka

Kompromitirane lozinke uzrokovale su 80 posto svih povreda podataka u 2019., što je rezultiralo financijskim gubicima i za tvrtke i za potrošače.[5] Zbog toga se moraju uspostaviti dobra pravila o zaporkama kako bi se osiguralo da lozinke ne mogu biti ugrožene. U nastavku su neke od uobičajenih politika koje bi organizacije trebale postaviti:

- Lozinka treba imati 8 znakova ili više,
- Lozinka treba sadržavati kombinaciju slova, brojeva i znakova,
- Lozinka se ne smije dijeliti ni s jednim drugim računom,
- Lozinka ne bi trebala sadržavati osobne podatke korisnika poput adrese ili telefonskog broja, imena djece ili kućnih,
- Lozinka se mora mijenjati svakih 60 do 90 dana osiguravajući da se lozinke koje su možda ukradene ili nagađane neće moći koristiti protiv tvrtke,
- Lozinka se ne smije dijeliti ni sa kime.

3.2.5. Sigurnosna kopija

Sigurnosna kopija ili „backup“ je kopija podataka koja se izrađuje u svrhu osiguranja u slučaju oštećenja ili gubljenja izvornih podataka.[6] Još jedan bitan alat za informacijsku sigurnost je sveobuhvatan plan sigurnosne kopije za cijelu organizaciju. Ne samo da bi podaci na korporativnim poslužiteljima trebali biti sigurnosno kopirani, već bi također trebalo napraviti sigurnosnu kopiju pojedinačnih računala koja se koriste u cijeloj organizaciji. Dobar rezervni plan trebao bi se sastojati od nekoliko komponenti:

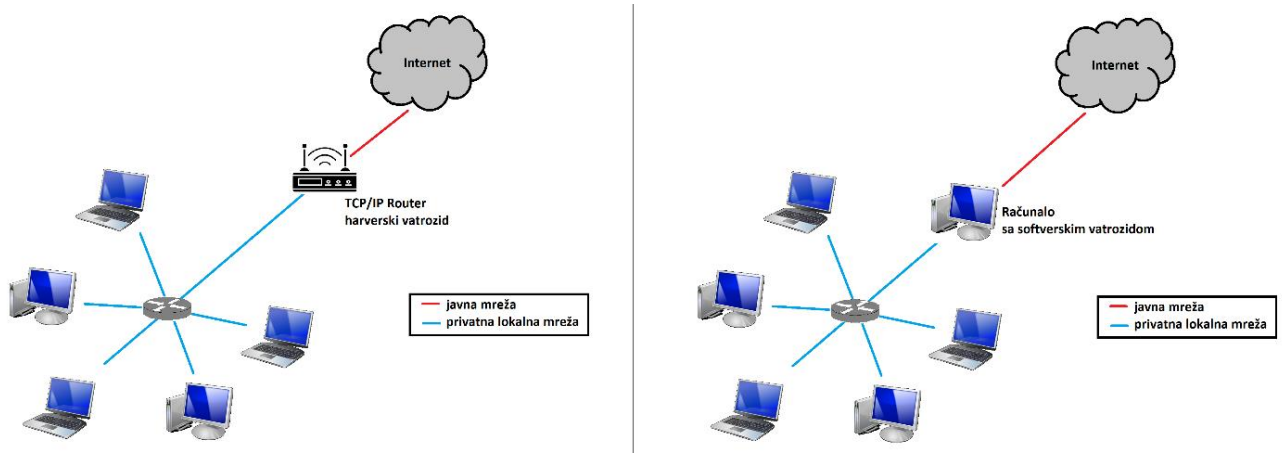
[5] idagent.com/blog/10-password-security-statistics-that-you-need-to-see-now/ , pristupljeno 02.11.2021.
[6] https://mooc.carnet.hr/mod/book/view.php?id=26069 , pristupljeno 02.11.2021.

- Organizacija bi trebala napraviti potpunu inventuru svih informacija koje treba sigurnosno kopirati i odrediti najbolji način za njihovu sigurnosnu kopiju.
- Kritične podatke treba sigurnosno kopirati svakodnevno, dok se za manje kritične podatke preporučuje sigurnosno kopirati tjedno.
- Neophodno je da dio plana sigurnosnog kopiranja bude pohranjivanje podataka na „offsite“mjesto...

Kako su informacije postale strateško bogatstvo, cijela industrija je nastala oko tehnologija potrebnih za provedbu pravilne strategije sigurnosnog kopiranja. Tvrtka može sklopiti ugovor s davateljem usluga za izradu sigurnosnih kopija svih svojih podataka ili mogu kupiti velike količine online prostora za pohranu i to učiniti sami. Tehnologije kao što su mreže prostora za pohranu i arhivski sustavi sada se koriste u većini velikih poduzeća.

3.2.6. Vatrozid

„Vatrozid je mrežni sigurnosni sustav koji nadzire i kontrolira dolazni i odlazni mrežni promet na temelju unaprijed određenih sigurnosnih pravila.“[7] Vatrozid može postojati kao hardver ili softver (ili oboje). Hardverski vatrozid je uređaj koji je spojen na mrežu i filtrira pakete na temelju skupa pravila. Softverski vatrozid radi na operativnom sustavu i presreće pakete kako stignu na računalo. Vatrozid štiti sve poslužitelje i računala tvrtke zaustavljajući pakete izvan mreže organizacije koji ne zadovoljavaju strogi skup kriterija.[8] Vatrozid se također može konfigurirati da ograniči protok paketa koji napuštaju organizaciju. To se može učiniti kako bi se eliminirala mogućnost da zaposlenici gledaju YouTube videozapise ili koriste Facebook s računala tvrtke.



Slika 5 - Hardverski i softverski vatrozid

Izvor: izrada autora prema https://cyber-sourceselect.blogspot.com

Neke organizacije mogu odlučiti implementirati više vatrozida kao dio svoje mrežne sigurnosne konfiguracije, stvarajući jedan ili više dijelova svoje mreže koji su djelomično zaštićeni. Ovaj segment mreže naziva se DMZ, posuđujući izraz demilitarizirana zona od

[7] https://en.wikipedia.org/wiki/Firewall_(computing), pristupljeno 03.11.2021.
[8] http://www.it4nextgen.com/types-of-firewall, pristupljeno 03.11.2021.

vojske, i to je mjesto gdje organizacija može smjestiti resurse kojima je potreban širi pristup, ali još uvijek moraju biti osigurani. Uobičajeni DMZ je podmreža koja se nalazi između javnog interneta i privatnih mreža.[9]

3.2.7. VPN

VPN je vrlo uobičajen i koristan način održavanja visoke razine komunikacijske kohezije unutar tvrtke, čak i u slučaju udaljene lokacije. Omogućuje svakom korisniku pristup intranetu tvrtke ili bilo kojoj stranici spojenoj na VPN, uz veliku učinkovitost i sigurnost. VPN se može definirati kao privatna mreža koja koristi javnu mrežu za međusobno povezivanje udaljenih korisnika ili web-mjesta. Veze koje povezuju 2 točke ove mreže usmjeravaju se putem interneta. Te su veze često šifrirane različitim metodama, osiguravajući siguran most između različitih korisnika.[10]

U vrijeme pandemije, poslovanje se moralo prebaciti na „home office“ odnosno proširiti na različite lokacije koje često mogu biti vrlo udaljene jedna od druge. Potreba za komunikacijom između ljudi koji rade na ovim različitim mjestima još je veća, a kako bi se poslovi održavali, zaposlenicima je potrebno rješenje poput VPN-a. Zapravo, VPN omogućuje zaposlenicima da održe istu razinu komunikacije i informacija u pogledu računalnih usluga. Stoga će svatko iz bilo koje podružnice moći pristupiti istim podacima na istom intranetu kao da je fizički u glavnom uredu. Izgradnjom VPN-a, tvrtka može proširiti sve svoje intranetne resurse na zaposlenike koji rade iz udaljenih ureda ili svojih domova.

Kvalitetu VPN-a uglavnom određuju tri glavna čimbenika:

1. Sigurnost: sustav mora moći zaštititi podatke koji se razmjenjuju, jer putuju kroz javnu mrežu, npr. ranije spomenutom enkripcijom,
2. Pouzdanost: prijenos informacija trebao bi biti pouzdan u bilo koje vrijeme i pod bilo kojim uvjetima, čak i u slučaju rukovanja maksimalnim brojem istodobnih veza te
3. Skalabilnost: VPN bi trebao moći podnijeti rast bez većih izmjena u strukturi.

Razmotrimo dvije vrste VPN-a: *Remote-access VPN* i *Site-to-site VPN*[11]*:*

3.2.7.1.Remote-access VPN

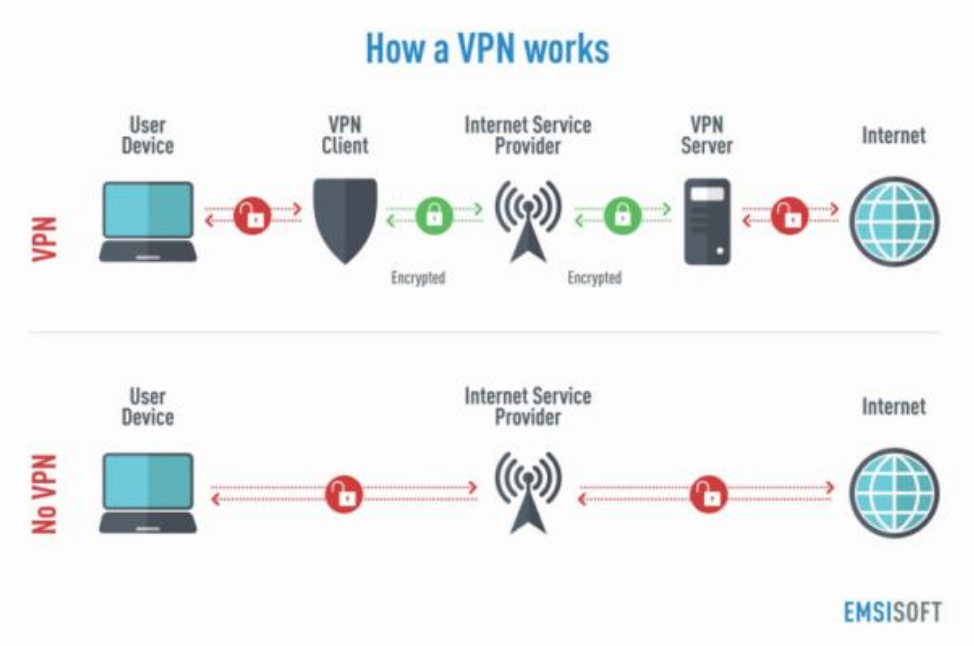
VPN s daljinskim pristupom omogućuje pojedinačnim korisnicima da uspostave sigurne veze s udaljenom računalnom mrežom. Ti korisnici mogu pristupiti sigurnim resursima na toj mreži kao da su izravno priključeni na mrežne poslužitelje. Za postavljanje VPN-a s daljinskim pristupom potrebne su dvije glavne komponente:

1. Poslužitelj mrežnog pristupa (NAS – Network Access Server) – također se naziva medijski pristupnik ili poslužitelj udaljenog pristupa (RAS – Remote Access Server). NAS može biti namjenski poslužitelj ili može biti jedna od više softverskih aplikacija

[9] https://www.fortinet.com/resources/cyberglossary/what-is-dmz, pristupljeno 03.11.2021.
[10] https://www.lifewire.com/what-is-a-vpn-5189778, pristupljeno 06.11.2021.
[11] Posavec, S.: Razvitak i tehnološke značajke virtualnih privatnih mreža, preuzeto s https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1605/datastream/PDF/view / pristupljeno 11.11.2021..

koje se pokreću na zajedničkom poslužitelju. To je NAS na koji se korisnik povezuje s interneta kako bi koristio VPN. NAS zahtijeva da korisnik unese valjane vjerodajnice za prijavu na VPN. Za provjeru autentičnosti korisničkih vjerodajnica, NAS koristi ili vlastiti proces provjere autentičnosti ili zasebni poslužitelj za provjeru autentičnosti koji radi na mreži.

2. Klijentski softver: zaposlenici koji žele koristiti VPN sa svojih računala zahtijevaju softver na tim računalima koji mogu uspostaviti i održavati vezu s VPN-om. Većina današnjih operativnih sustava ima ugrađeni softver koji se može povezati s VPN-ovima s udaljenim pristupom, iako bi neki VPN-ovi mogli zahtijevati od korisnika da umjesto toga instaliraju određenu aplikaciju. Klijentski softver postavlja tunelsku vezu s NAS-om, što korisnik označava svojom internet adresom. Softver također upravlja šifriranjem potrebnom za sigurnost veze.



Slika 6 - Usporedba korištenja Interneta sa i bez VPN-a

Izvor: *https://securityboulevard.com/2020/03/vpn-a-key-to-securing-an-online-work-environment/*

3. PRIMJENA SIGURNOSNIH MJERA NA PRIMJERU PODUZEĆA XY

Kako bi se osigurala odgovarajuća razina povjerljivosti, cjelovitosti i dostupnosti poslovnim informacijama koje nastaju u poslovnim odnosima s klijentima, uvodi se sustav upravljanja informacijskom sigurnošću u skladu sa zahtjevima međunarodne norme ISO 27001:2013. Ti ciljevi se ostvaruju pomoću:

- Uspostave procesa procjene rizika informacijske sigurnosti,
- Uvođenja kontrola radi obrade rizika informacijske sigurnosti,
- Postavljanje ciljeva informacijske sigurnosti,
- Osiguravanje neophodnih resursa potrebnih za realizaciju ciljeva informacijske sigurnosti i održavanje željene razine rizika te posljedično ispunjavanje zahtjeva svih zainteresiranih strana,
- Osiguravanja trajnog unaprijeđena sustava upravljanja informacijskom sigurnošću putem internih audita, upravljanja nesukladnostima, korektivnih radnji i ocjene uprave,
- Komuniciranjem i osiguranjem dostupnosti ove politike zainteresiranim stranama te
- Redovitim revizijama ove politike.

3.1. Upravljanje informacijskom sigurnošću

Poduzeće mora imenovati predstavnika uprave za informacijsku sigurnost s potrebnim ovlaštenjima i odgovornostima. U odnosu na informatički sustav, za organizaciju u našem slučaju definirati ćemo dvije uloge: administratora sustava i korisnike.

Administratora određuje direktor tvrtke. Zadaci administratora su:

− osigurati korisnicima informacijskog sustava prava pristupa sustavima u skladu s poslovnim potrebama,

− osigurati optimalno funkcioniranje informatičkog sustava, a u slučaju odstupanja, poduzeti potrebne mjere za sprječavanje ili smanjenje poslovne štete zbog kvara ili ograničenog rada sustava (otklanjanje neispravnosti, informiranje korisnika o odstupanjima, prijavljivanje grešaka za sustave koje održavaju vanjski partneri)

− pružiti informacije i edukacije korisnicima sustava u slučaju promjena na informatičkom sustavu,

− voditi kontinuirani nadzor rada informacijskog sustava te poduzimati korektivne i preventivne radnje u cilju sprečavanja neovlaštenog korištenja i potencijalne zloupotrebe sustava

Korisnici informatičke imovine dužni su istom postupati u skladu za zahtjevima sustava informacijske sigurnosti.. Politiku dodjele ovlaštenja na pojedinim dijelovima informacijskog sustava predlaže Administrator sustava, a odobrava Direktor tvrtke.

3.1.1. Informacijska imovina, klasifikacija informacija i upravljanje rizicima

3.1.1.1. Informacijska imovina

Sva informacijska imovina podijeljena je u sljedeće grupe:

- Osobna i prijenosna računala
- Poslužitelji (fizički i virtualni) i uređaji za pohranjivanje
- Programi
- Mrežna oprema i sigurnosni uređaji
- Pisači
- Mobilni telefoni
- Objekti

Važnost informacijske imovine određena je na način tako da joj se pridjeljuje vrijednost informacije koja se odnosi na nju a ima najveću važnost. Na primjer, ako se na računalu vrši obrada informacija važnosti 4 i 3, računalu se pridjeljuje važnost 4. Svoj imovini su dodijeljeni vlasnici, a organizacija ažurira popis informacijske imovine kod svake promjene.

3.1.1.2. Klasifikacija informacija

Klasifikacija informacija je postupak utvrđivanja zahtjeva informacije u odnosu na povjerljivost, cjelovitost i dostupnost, te u konačnici važnosti informacije za organizaciju.

a) Povjerljivost

S obzirom na svojstvo povjerljivosti, informacije se dijele u četiri razreda:

Vrlo povjerljivo – najosjetljivije informacije od strateške važnosti, čiji gubitak ili neovlašteno otkrivanje može dovesti do ozbiljnih financijskih gubitaka ili do zakonskih sankcija.

Povjerljivo – osjetljive informacije koje se odnose na poslovanje, čiji gubitak ili neovlašteno otkrivanje može uzrokovati probleme u odvijanju poslovnih procesa ili djelomični gubitak konkurentske prednosti.

Ograničeno – informacije koje su namijenjene isključivo djelatnicima za internu uporabu, ali čije otkrivanje trećim stranama ili gubitak ne bi uzrokovao probleme u poslovnim procesima.

Javno – sve ostale informacije koje su predviđene za javnu objavu.

b) Cjelovitost

S obzirom na svojstvo cjelovitosti, informacije se dijele u tri razreda:

Kritično – informacije čija je cjelovitost od strateške važnosti, a narušavanje cjelovitosti može dovesti do ozbiljnih financijskih gubitaka ili do zakonskih sankcija.

Važno – informacije čija je cjelovitost važna za poslovne od strateške važnosti, a narušavanje cjelovitosti može dovesti do problema u odvijanju poslovnih procesa.

Normalno – sve ostale informacije koje nemaju posebnih zahtjeva za cjelovitošću.

c) Dostupnost

S obzirom na svojstvo dostupnosti, informacije se dijele u tri razreda:

Kritično – (<=8 sata) informacije čija nedostupnost veća od 8 sati može uzrokovati značajne probleme u odvijanju poslovnih procesa

Važno – (<=24 sata)) informacije čija nedostupnost veća od 24 sata može uzrokovati značajne probleme u odvijanju poslovnih procesa.

Normalno – (<= tjedan dana) informacije čija dostupnost nema značajnijeg utjecaja na odvijanje poslovnih procesa, a koje bi trebalo obnoviti u roku od tjedan dana.

d) Kvantifikacija važnosti informacija

Kako bi se moglo kvantificirati važnost određene informacije, najprije se svakom svojstvo i svakom razredu treba pridijeliti brojčana vrijednost u skladu s tablicom:

Tablica 3 - Kvantifikacija važnosti informacija

Izvor: Izrada autora

	Povjerljivost (*C*)	**Cjelovitost (*I*)**	**Dostupnost (*A*)**	**Brojčana vrijednost**
Svojstvo	Vrlo povjerljivo	-	-	4
	Povjerljivo	Kritično	Kritično	3
	Ograničeno	Važno	Važno	2
	Javno	Normalno	Normalno	1

Nakon što se informacija ocijeni po sva tri svojstva, računa se umnožak vrijednosti svojstava:

C x I x A

dok se njena **važnost (V)** određuje prema tablici:

Tablica 4 - Važnost informacije

Izvor: Izrada autora

$<aX=C \times I \times A$	**Važnost (V)**
X < 3	1
3 ≤ X < 6	2
6 ≤ X < 12	3
12 ≤ X < 24	4
24 ≤ X	5

3.1.1.3. Upravljanje rizicima

Procjena rizika provedena je prilikom uvođenja sustava upravljanja informacijskom sigurnošću, a predviđeno je da se pregledava i po potrebi mijenja jednom godišnje. Na osnovi procjene rizika donosi se odluka o prihvatljivoj razini rizika informacijske sigurnosti te se određuje mjere za smanjenje rizika.

Organizacija određuje one rizike (koji su kombinacija prijetnji i ranjivosti, na osnovi norme ISO 27005:2018) u odnosu na informacijsku imovinu i njenu važnost čijom realizacijom može doći do uništenja ili oštećenjem informacija, te posljedično do štete za organizaciju.

Za svaki se rizik određuju se:

- vjerojatnost pojave i
- utjecaj rizika (šteta ukoliko se rizik dogodi).

Na osnovi kombinacije vjerojatnosti i utjecaja određuje se utjecaj rizika. Način izračuna razine rizika prikazan je u tablicama u nastavku.

Vjerojatnost pojave rizičnog događaja kategorizirana je prema tablici:

Tablica 5 - Vjerojatnost pojave rizika

Izvor: Izrada autora

	Vjerojatnost pojave rizika (P)
5	Događaj će se vjerojatno dogoditi unutar 1 godine
4	Događaj će se vjerojatno dogoditi unutar 3 godine
3	Postoje izgledi da se događaj dogoditi unutar 5 godine
2	postoje izgledi da se događaj dogoditi unutar 7 godine
1	Mala je vjerojatno da se događaj dogoditi unutar 10 godina

Šteta na informacijskoj imovini (Š) slučaju ostvarenja rizičnog događaja prikazana je u nastavku:

Tablica 6 - Šteta na informacijskoj imovini

Izvor: Izrada autora

	Šteta na informacijskoj imovini (Š)
3	Izrazito velika šteta (havarija) – imovina je potpuno uništena
2	Značajnija šteta, ali je moguć oporavak informacijske imovine
1	Neznatna šteta

Utjecaj rizika (U) određuje se prema izrazu: **U=P×Š×V**

Nakon izračuna utjecaja rizika vrši se njegova kategorizacija na osnovi tablica u nastavku:

Tablica 7 - Kategorija rizika

Izvor: Izrada autora

Kategorija rizika	***U=P×Š×V***
5	od 60 do 75
4	od 26 do 45
3	od 15 do 25
2	od 6 do 12
1	od 1 do 5

Tablica 8 - Kategorizacija rizika

Izvor: Izrada autora

Kategorizacija rizika	
5	Katastrofalne posljedice – upitan je opstanak poduzeća
4	Velike posljedice – otežano je poslovanje na duži period
3	Srednje posljedice – teškoće u poslovanju u kraćem periodu
2	Neznatne posljedice – vro mali utjecaj na poslovanje
1	Bez posljedica – nema nikakvog utjecaja na poslovanje

Procjena rizika provodi se uz pretpostavku da se ne primjenjuju nikakve kontrolne mjere za smanjenje razine i prioriteta rizika. Za rizike kategorije od 4 i 5 na dalje biti će propisane mjere za ovladavanje rizika, dok se rizici kategorije 1, i 3 smatraju prihvatljivima, te nije potrebno provoditi mjere za njihovo ovladavanje. Procjena rizika ažurira najmanje jednom godišnje ili u slučaju promjene unutar tvrtke koja može imati utjecaj na sustav upravljanja informacijskom sigurnošću.

Na osnovi rezultata procjene rizika tvrtka određuje mjere za postupanje s rizicima. Svrha je postupanja s rizicima osiguravanje željenih rezultata sustava upravljanja informacijskom sigurnošću, sprječavanje ili smanjenje neželjenih učinaka, te osiguravanje trajnog unaprjeđenja.

3.2. Kontrola pristupa

U poduzeću je bitno odrediti uloge za pristup informacijama. Pristup poslovnim aplikacijama dodjeljuje se isključivo u skladu s poslovnim potrebama te operativnim procedurama. Zahtjev za pristup odobrava Administrator. Za upravljanje korisničkim pravima ovlašten je i odgovoran Administrator sustava. Svakom djelatniku se prilikom zaposlenja dodjeljuje jedinstveno korisničko ime. Na temelju korisničko imena se dodjeljuju prava pristupa određenim sustavima i resursima. Jedna od obaveznih mjera zaštite je postavljanje lozinke. Dužina lozinke mora biti najmanje 8 znakova, te sadržavati 3 od 4 uvjeta, velika slovo, mala slova, brojeve, specijalne znakove. Lozinka se mijenja minimalno svaka tri mjeseca i pamti 1 lozinku. Zabranjeno je odavanje lozinki drugim osobama i čuvanje na vidljivom mjestu. Izričito je zabranjeno korištenje lozinki drugih osoba.

3.3. Ostale mjere zaštite

Korisnici osobnih i prijenosnih računala odgovorni su za brigu o računala koja su zadužili, uz pridržavanje mjera za sigurnost podataka koje ćemo ukratko proći u nastavku.

3.3.1. Instalacija programa

Instalaciju odobrenih programa na radni stanicama i prijenosnim računalima mogu provoditi svi djelatnici sa dopuštenjem. Ažuriranja operativnih sustava vrši se automatski a nadzor ima administrator sustava. Zabranjena je instalacija neodobrenih programa bez odobrenja direktora ili administratora.

3.3.2. Antivirusna zaštita

Organizacija propisuje obavezno instaliranje i korištenje antivirusnih programa na svim računalima, koji se automatski osvježavaju novim definicijama, a licenca se redovito obnavlja. Antivirusni softver mora biti omogućen (aktivan) u vrijeme korištenja računala Postavke antivirusnog programa definira Administrator i ne smiju se mijenjati bez njegovog odobrenja.

3.3.3. Sigurnosne kopije

Tvrtka je uspostavila proces sigurnog kopiranja podataka te se sigurnosne kopije čuvaju 30 dana. Tvrtka testira sustav sigurnosnog kopiranja po potrebi a najmanje jedanput mjesečno.

3.3.4. Sigurnost komunikacije

Mrežna oprema nalazi se u prostoriji s nadzorom pristupa. Zaštita prema van osigurana je pomoću vatrozida. Mrežnu infrastrukturu održavaju zaposlenici tvrtke i ugovorena tvrtka za održavanje Servera i sistema.

Tvrtka koristi fiksnu i bežičnu mrežu. Fiksna mreža je segmentirana. Korisnicima je omogućen pristup samo onim segmentima za koje imaju ovlaštenja.

E-mail komunikacija realizirana je korištenjem usluga vanjskog dobavljača koji osigurava sigurnosnu pohranu i anti-spam zaštitu.

Potrebno je izbjegavati prijenos povjerljivih podataka preko javne mreže.

U sklopu unutrašnje procjene provjerava se i primjena kontrola sustava upravljanja informacijskom sigurnošću. Ukoliko to procjeni potrebnim, organizacija može organizirati i tehničku provjeru informacijskog sustava, kao što su penetracijsko testiranje ili provjera tehničkih ranjivosti.

4. ZAKLJUČAK

Informacijski sustavi danas su integrirani u sve komponente poslovanja, ali mogu li donijeti konkurentsku prednost? Tijekom godina bilo je mnogo odgovora na ovo pitanje. Rana istraživanja nisu mogla povući nikakve veze između IT-a i profitabilnosti, ali kasnija istraživanja su pokazala da učinak može biti pozitivan. IT nije lijek za sve; samo kupnja i ugradnja najnovije tehnologije neće, sama po sebi, učiniti tvrtku uspješnijom. Umjesto toga, kombinacija pravih tehnologija i dobrog upravljanja, dat će tvrtki najbolje šanse za pozitivan rezultat.

Većina poduzeća zabrinuta je za povjerljivost podataka, što zahtijeva sigurnost informacijskog sustava za osjetljive podatke. Zbog toga je važno da poduzeće razvije sveobuhvatan i sustavan pristup sigurnosti informacijskog sustava, kao što su sigurnosni plan i politika.

Kako bi se postigla visoka razina sigurnosti informacijskog sustava, poslovanje bi također trebalo biti svjesno potrebe učinkovite obuke i pitanja vezanih uz ljude. Obuka o svijesti o sigurnosti pomaže korisnicima da se upoznaju sa sigurnosnim značajkama sustava, kao i njihovim dužnostima i sigurnosnim procesima za zaštitu osjetljivih podataka, a sigurnosne revizije trebale bi se provoditi redovito.

Zbog neograničene prirode mreže, informacijska sigurnost predstavlja poteškoću u današnjoj infrastrukturi. Organizacije bi trebale pomno slijediti politike informacijske sigurnosti kako bi se borile protiv izloženosti informacijama preko mreža. Područje upravljanja rizicima može pomoći u razvoju i implementaciji rješenja za povećanje integriteta, povjerljivosti i dostupnosti sustava, a radnje koje proizlaze iz usvojenih strategija moraju biti integrirane kao dio procesa minimiziranja rizika za organizaciju za postizanje poslovnog uspjeha uz uvođenje preventivnih i detektivskih kontrola.

Sigurnost informacijskog sustava podrazumijeva zaštitu vrijednih podataka potrošača i poduzeća od internih i vanjskih napada. Za to je potreban sigurnosni program za praćenje i zaštitu podataka tijekom pohrane, transporta i obrade. Budući da organizacije drže velike količine informacija, moraju štititi svoje klijente i održavati integritet povjerljivosti. Ključne borbe za informacijsku sigurnost uključuju zlonamjerni softver, ranjivosti, krađu identiteta, izvan mrežne sustave i zlouporabu podataka od strane zaposlenika ili drugih.

Politika informacijske sigurnosti i upravljanje sigurnošću važni su za organizacije kako bi osigurali usklađenost sa saveznim propisima kako bi zaštitili potrošače, spriječili bankrot u malim i srednjim organizacijama i zaštitili vrijedne interne informacije od nezadovoljnog zaposlenika ili vanjskog napadača. Kako su računalni i mrežni resursi sve više postali sastavni dio poslovanja, postali su i meta kriminalaca. Organizacije moraju biti u toku s načinom na koji štite svoje resurse. Isto vrijedi i za nas osobno: kako digitalni uređaji postaju sve više isprepleteni s našim životima, postaje nam ključno razumjeti kako se zaštititi.

5. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Tomislav Benić

Matični broj studenta: 6-120/17 ITI

Naslov rada: SIGURNOSNI ASPEKT POSLOVNIH INFORMACIJSKIH SUSTAVA I PRIMJENA ISTIH NA PRIMJERU PODUZEĆA XY

Svojim potpisom jamčim:

- Da sam jedini autor ovog rada.
- Da su svi korišteni izvori, kako objavljeni, tako i neobjavljeni, adekvatno citirani i parafrazirani te popisani u bibliografiji na kraju rada.
- Da ovaj rad ne sadrži dijelove radova predanih na Veleučilište Baltazar Zaprešić ili drugim obrazovnim ustanovama.
- Da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio nastavnik.

Datum | Potpis studenta

_____ _____

6. POPIS LITERATURE

Varga M.: Upravljanje podacima, 2014.

Varga M.: Informacijska tehnologija u poslovanju, 2004.

Bourgeois, D., Bourgeois, D.T.: Information systems for Business and Beyond

Stapleton, J.J.: Security without Obscurity, 2014.

Srića, V., Spremić, M.: Informacijskom tehnologijom do uspjeha, Sinergija, Zagreb, 2000.

Sustav, preuzeto s https://www.enciklopedija.hr/natuknica.aspx?ID=58904 / Pristupljeno 30.10.2021.

Enkripcija, preuzeto s https://www.ibm.com/topics/encryption / Pristupljeno 26.10.2021.

Enkripcija, preuzeto s https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/ Pristupljeno 26.10.2021.

Sigurnost lozinke, preuzeto s https://idagent.com/blog/10-password-security-statistics-that-you-need-to-see-now/ Pristupljeno 02.11.2021.

Backup, preuzeto s https://mooc.carnet.hr/mod/book/view.php?id=26069 / pristupljeno 02.11.2021.

Vrste vatrozida, preuzeto s http://www.it4nextgen.com/types-of-firewall / pristupljeno 03.11.2021.

DMZ, preuzeto s https://www.fortinet.com/resources/cyberglossary/what-is-dmz / pristupljeno 03.11.2021.

Vatrozid, preuzeto s https://en.wikipedia.org/wiki/Firewall_(computing) / pristupljeno 03.11.2021.

VPN, preuzeto s https://www.lifewire.com/what-is-a-vpn-5189778 / pristupljeno 06.11.2021.

Posavec, S.: Razvitak i tehnološke značajke virtualnih privatnih mreža, preuzeto s https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A1605/datastream/PDF/view / Pristupljeno 11.11.2021.

7. POPIS SLIKA, TABLICA I GRAFIKONA

Popis slika

Popis tablica

8. ŽIVOTOPIS

Datum rođenja: 29/10/1976 | **Spol:** Muško | **Državljanstvo:** hrvatsko

Mobile: (+385) 912376834

E-adresa: benic@a1net.hr

Home: Loborska ulica 10, Zagreb, 10000 Zagreb, Hrvatska

RADNO ISKUSTVO

Tehničar elektrotehnike

Aeroteh d.o.o.

01/10/2010 – Trenutačno

Zagreb, Hrvatska

Voditelj odjela servisa.

Koordinator sustav kvalitete.

Sistem administrator.

Interni auditor za ISO 27001.

Synco 700 ACS Engineering - Training course 2011.

HVAC in building systems Hydraulics - Training course 2011.

Domat SoftPLC Design and Engineering - Training course 2011.

Cerberus PRO IP5 - Training course 2014.

Tehničar elektrotehnike

Intel trade d.o.o.

01/12/2004 – 30/09/2010

Zagreb, Hrvatska

Servisni specijalista za HVAC i AHU.

SYM10T SymmetreE Technician Application Engineering - Training 2005.

HVAC/AHU Ciat

DDC Honeywell commissioning

Voditelj službe za održavanje objekta

Sljeme Medvednica d.o.o.

01/12/2003 – 30/11/2004

Zagreb, Hrvatska

Održavanje Hotela Tomislavov dom na Sljemenu.

Elektromonter

T.P.U. Hoffmann d.o.o.

01/09/1997 – 30/11/2003

Zagreb, Hrvatska

Izvođenje i vođenje elektroinstalaterskih radova.

OBRAZOVANJE I OSPOSOBLJAVANJE

Elektrostrojarska obrtnička škola

Elektromehaničar, Elektrotehnika

1994

Selsak cesta, Zagreb, Hrvatska

Elektrostrojarska obrtnička škola

Elektrotehničar, Elektrotehnika

1994

Selska cesta, Zagreb, Hrvatska

Ministarstvo unutarnjih poslova RH

Zaštitar tehničar

2014

Hrvatski olimpijski odbor

Trener hokeja na travi

2004

Fakultet strojarstva i brodogradnje

Rukovatelj rashladnim tvarima - UNIDO

2013