Utjecaj kibernetičkog kriminala na sigurnost poslovno-informacijskih sustava

Prevedan, Nika

Sveučilište Sjever

Završni rad br. 290/PIM/2021

Utjecaj kibernetičkog kriminala na sigurnost poslovno-informacijskog sustava

Koprivnica, rujan 2021.godine

Sveučilište Sjever

Odjel za Poslovanje i menadžment

Završni rad br. 290/PIM/2021

Utjecaj kibernetičkog krimanla na sigurnost poslovno-informacijskog sustava

Student

Nika Prevedan, 0336031118

Mentor

izv. prof. dr. sc. Ljerka Luić

Koprivnica, rujan 2021. godine

Zahvala

Zahvaljujem se na stručnom vođenju i usmjeravanju mentorici izv. prof. dr. sc. Ljerki Luić.

Sažetak

U završnom radu je razmotreno istraživačko pitanje utjecaja kibernetičkog kriminala na sigurnost informacijskog sustava. Istraživanje je provedeno putem intervju na Hrvatskom zavodu za mirovinsko osiguranje podružnice Bjelovar. Istraživanje je potkrijepljeno teorijama vezanim za kibernetički kriminal poslovno informacijskog sustava Republike Hrvatske, odnosno pojmovnim određenjem, vrstama, razvojem, utjecajem te mjerama sigurnosti koje se provode. Analizom dobivenih rezultata nakon provedenog istraživanja moguće je zaključiti kako zaposlenici nisu dovoljno educirani i informirani unutar samog poslovanja, te bez obzira na razvoj tehnologije sustav i samo radno mjesto nema dovoljnu zaštitu protiv ovog oblika kriminala. Usvojeni zakoni i norme se dovoljno ne provode. Kao daljnji nastavak istraživanja predlaže se detaljna provedba istraživanja na razini cijele Republike Hrvatske, provedba usvojenih zakona i normi, te programskih sigurnosti i edukacija zaposlenika unutar različitih organizacija. Nakon toga je potrebno ponovo provođenje istraživanja kako bi se utvrdilo postoji li napredak ili su potrebne dodatne aktivnosti za sprječavanje ovog oblika kriminala.

Ključne riječi: poslovno informacijski sustav, kibernetički kriminal, vrste, sigurnosne mjere i zaštite, kibernetički kriminal u Republici Hrvatskoj

Popis korištenih kratica

ISMS - Sustav upravljanja informacijskom sigurnošću

ISO - Međunarodna organizacija za normizaciju

IEC – Međunarodna elektronička komisija

CARNET - Hrvatska akademska i istraživačka mreža

CERT - odjel Hrvatske akademske i istraživačke mreže – CARNET

UVNS - Ured vijeća za nacionalnu sigurnost

ZSIS - Zavod za sigurnost informacijskih sustava

AZOP - Agencija za zaštitu osobnih podataka

HZMO - Hrvatski zavod za mirovinsko osiguranje

IMMS - Informacijski mirovinski sustav

LANA - Elektronička knjižica

ESUD - Elektronički sustav upravljanja dokumentima

OUTLOOK - Web aplikacija za upravljanje osobnim podacima

RAKE - Softver za upravljanje zadacima i alat za automatizaciju izgradnje

Sadržaj

1. Uvod

Danas sve organizacije koriste naprednu tehnologiju koja se sve više razvija i unaprijeđuje. Poslovno informacijski sustav je prilagođen organizacijama, te im olakšava razne procese u proizvodnji, administraciji, računovodstvu, logistici i ostalim područjima rada. Tu se javlja i kibernetički kriminal u poslovanju koji želi narušiti te procese i zlouporabiti osobne i važne podatke same organizacije. Svakim danom sve se više razvija kako se razvija i tehnologija. Uz ovaj oblik kriminala se razvijaju i sigurnosne mjere kojima se nastoji sprječiti.

1.1. PREDMET I CILJ RADA

Završni rad istražuje problematiku kibernetičkog kriminala u poslovanju. Cilj rada je istražiti njegov utjecaj na poslovanje, kako se odvija u Hrvatskoj, te istražiti kako utječe u jednoj od većih i važnih institucija u Hrvatskoj. Zatim na koje načine se može omogućiti zaštita poslovno informacijskih sustava i potreba da se unaprijed sprječi zloupotreba i ovaj oblik kriminala.

1.2. STRUKTURA RADA

Rad je podijeljen u tri dijela. Prvi dio je teorijski i sastoji se od dvije cjeline. Prva cjelina govori o poslovno informacijsko sustava, njegovim zadaćama i strukturi. U drugoj cjelini je objašnjen kibernetički kriminal. Kako je nastao i razvijao se, te kako utječe na poslovno informacijski sustav. Tu je i konvekcija o kibernetičkom kriminalu koja je iznimno važna za članice Europske unije i za Hrvatsku. Zatim su spomenute vrste, metode i tehnike kibernetičkog kriminala koje se najčešće javljaju u poslovanju, te njihov utjecaj.

Drugi dio se odnosi na sigurnost i zaštitu protiv kibernetičkog kriminala u poslovanju. Različite mjere su navedene, te kako okruženje može utjecati na sigurnost, sami zaposlenici i odgovorne osobe u poslovanju. Izrađeni su različiti sigurnosni programi koji donose sigurnost sustava i važni su u poslovanju. Javljaju se i mnoge institucije u Hrvatskoj koje se bave sprječavanjem ovog oblika kriminala, te je objašnjeno na koji način djeluju i provode zaštitu podataka, sustava, informacija i slično.

Treći dio se odnosi na sami utjecaj kibernetičkog kriminala u Hrvatskoj u poslovanju. Kako se odrazio na organizacije, koliko se pridodaje pažnja, te relevantne činjenice u 2017 i 2018. godini. Zatim slijedi straživački intervju koji se odnosi na važnu instituciju Hrvatski zavod za mirovinsko osiguranje podružnice Bjelovar. Kako na njih svakodnevno utječe kibernetički kriminal, kako ga sprječavaju i koliko su upućeni sami zaposlenici. Možemo iz toga uvidjeti razliku između glavnih tijela Hzmo-a i kadrovske službe, te kako se njihova mišljenja podudaraju ili razlikuju.

1.3. IZVORI PODATAKA

Za potrebe izrade završnog rada korištena je recentna literatura iz područja informatike odnosno informacijskih sustava i kibernetičkog kriminala. Korišteni su i razni mrežni i elektronički izvori, ali i mrežne stranice institucija koje provode zaštitu i sigurnost u Rrepublici Hrvatskoj.

1.4. ISTRAŽIVAČKO PITANJE

Rad se temelji na istraživačkom pitanju „Koliki je utjecaj kibernetičkog kriminala na sigurnost poslovno informacijskog sustava u Republici Hrvatskoj“, te na istraživačko pitanje „Koliko je to zastupljeno u HZMO-u podružnice Bjelovar“. Odabrana organizacija za provedbu intervjua je bio Hrvatski zavod za mirovinsko osiguranje podružnice Bjelovar koji se sastoji od četiri ispostave: Čazma, Daruvar, Grubišno Polje i Garešnica. Cilj je bio ispitati glavnu načelnicu i informatičara kako kibernetički kriminal utječe na HZMO i zaposlenike, te kako provode zaštitu i sigurnost protiv toga.

2. Poslovno informacijski sustav

Poslovni informacijski sustav sastoji se od mnogih automatiziranih funkcija. Neke su vrlo jednostavne (praćenje dijelova koji se montiraju u nekoj od proizvodnih industrija), a neke složene (obrada plaća u velikim korporacijama i ustanovama). Cjelokupni poslovno-informacijski sustav nekog poslovnog sustava moguće je promatrati kroz tri osnovna aspekta poslovanja: financijski, logistički i ljudski potencijali. (Luić, 2009:74)

Zadaća informacijskog sustava usmjerena je na povezivanje svih poslovnih funkcija. Pojedincima ili skupinama daje mogućnost da zadovolje svoje informacijske potrebe, omogućujući integraciju svih dijelova, poslova i funkcija u poslovnom sustavu. Poslovodstvo sudjeluje u svim procesima upravljanja informacijama i koristi se neizmjernom količinom kompjutorskih usluga. (Luić, 2009:72;83)

Tri temeljna obilježja modernog poslovanja: brzina, povezanost i dodana vrijednost, danas postaju ključni izvori uspjeha. Svaki aspekt poslovanja i organizacije, djeluje i mijenja se u realnom vremenu, te je naglašena brzina protoka informacija. Povezanost se očituje u elektroničkom povezivanju: proizvoda, ljudi, tvrtki, zemalja. Informacijske tehnologije postaju glavni uvjet poslovnog uspjeha. (Luić, 2009:84)

Učinkovitost djelovanja organizacije može se povećati unapređenjem i preustrojem poslovnih procesa. Poslovni proces je povezani skup aktivnosti i odluka, koji se izvodi na vanjski poticaj radi ostvarenja nekog mjerljivog cilja organizacije, traje određeno vrijeme i troši neke ulazne resurse pretvarajući ih u specifične proizvode ili usluge od značaja za kupca ili korisnika. Danas se poslovni procesi opisuju pomoću skupa grafičkih simbola s točno definiranim značenjem i čvrstim pravilima njihovog povezivanja. (Brumec, 2011:1;2;3)

Veći računalno informacijsko-komunikacijski sustav i društveno važniji raspolaže s više tajni i važnijih podataka. Time raste zanimanje pojedinca odnosno jako nadarenih računalnih stručnjaka (hakera) za prodor u njih. Radi se o povjerenju vlastitog znanja, sposobnosti, pokazivanju stručne nadmoći pojedinaca, ali pokušaja prodara iz neprijateljskih razloga i s lošim namjerama, te ubacivanjem "zlih" programa (crvi, virusi, trojanski konj, spam). (Javorović, Bilandžić, 2007:294)

3. Kibernetički kriminal poslovno informacijskog sustava

Računalni kriminal sve se više smatra kibernetičkim kriminalom. Kibernetički kriminal je pojam kojim se označavaju sva kriminalna djela u kojima je cilj ili sredstvo bilo uključeno računalo ili računalna mreža. Nastao je i razvijao se od sedamdesetih godina prošlog stoljeća kada je računalni kriminal bio prepoznat kao problem. Sam pojam se javlja početkom dvadesetih godina prošlog stoljeća. Ovaj pojam sa sobom je donio i pojam digitalnih dokaza koji se mogu koristiti u dokazivanju. (Bača, 2004:29)

Četiri su kategorizacije kibernetičkog kriminala:

1. Prva: djela u kojima je kriminal bio povezan sa samim računalom (krađa računala, komponenti ili uništenje)
2. Druga: računalo je okolina u kojoj je kriminal počinjen (krađa podataka, provale u računalo)
3. Treća: računalo je alat ili instrument za izvođenje ili planiranje kriminala
4. Četvrta: računalo se slučajno pojavljuje u drugim kriminalnim djelima ili se koristi kao simbol za zastrašivanje ili prijevaru (Bača, 2004:30)

Dragičević (2004.) navodi „računalni kriminal je ukupnost kaznenih djela, učinjenih na određenom području kroz određeno vrijeme, kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost, programske ili podatkovne osnovice računalnog sustava ili tajnosti podataka.“

Računalo se koristi za zločine u komunikacijama i pohrani podataka. Ova tehnologija pruža mnoge izazove u društvenim sferama koje su vezane uz pretraživanje podataka i kriminalistička istraživanja. Ovakav oblik kriminala će uvijek rasti s vremenom. (Težak, 2010:27)

Istraživanje računalnog kriminala se sastoji od fizičkih dokaza elektroničkog tip i što se radi s elektroničkom opremom. Potrebno je provjeriti zapise, ispitati informatore, svjedoke, te izvršiti nadzor računalnog sustava. Datoteke mogu sadržavati podatke o računalnom sustavu, zaporkama, razne druge informacije o organizaciji, zaposlenicima i klijentima. Ukoliko se u ovoj fazi identificira potencijalni počinitelj, može se naučiti o njemu, računalnoj opremi koju je koristio, stupanju njegova znanja i vještina. Ispitivanjem informatora, svjedoka i očevidaca

mogu dati informacije o tehnikama i metodama kojima se služi počinitelj. Fizičko i elektroničko nadziranje počinitelja može pomoći u procjeni informacija. (Bača, 2004:258)

Ukoliko se radi o napadu na određeni ekonomski subjekt, može dovesti tvrtku u stečaj. Neka djela se izvode slučajno, neka se korsite u socijalne ili političke svrhe, dok su neki predmet studioznog proučavanja, planiranja i bavljenja profesionalnih kriminalaca. Definirati ovaj oblik kriminala je vrlo teško jer se radi o novom obliku kriminalnog ponašanja koji nije u potpunosti određen spram drugih oblika. (Bača, 2004:22)

3. 1. Konvencija o kibernetičkom kriminalu

Konvencija o kibernetičkom kriminalu usvojena je na konferenciji Vijeća Europe u Budimpešti, a Republika Hrvatska potpisala ju je 23. studenog 2001. godine. Države članice Vijeća Europe i ostale potpisnice ove Konvekcije imaju cilj postići veće zajedništvo. Uvjerene su da je prvenstvena važnost potreba vođenja zajedničke kaznene politike usmjerena zaštiti društva od kibernetičkog kriminala i poticanjem međunarodne suradnje. Svjesne su promjena nastalih digitalizacijom, konvergencijom i globalizacijom računalnih mreža. Zabrinute su zbog mogućnosti da računalne mreže i elektroničke informacije budu iskorištene za počinjenje kaznenih djela, a dokazi budu pohranjeni i prenošeni. Prepoznaju potrebu za suradnjom između država i zaštitu legitminih interesa. Vjeruju da učinkovita borba protiv kibernetičkog kriminala zahtjeva povećanu, brzu i uhodnu međunarodnu suradnju u kaznenopravnim predmetima. Također su uvjerene da je ova Konvencija nužna radi odvraćanja od postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i podataka, te odvraćanja od njihove zloupotrebe. Na način opisan u Konvenciji, usvajaju se ovlaštenja dovoljna za učinkovitu borbu protiv takvih kaznenih djela, te olakšavajući otkrivanje, istraživanje i kazneni progon ovakvih djela na domaćoj i međunarodnoj razini. Namjera ove Konvencije je nadopuniti ostale konvencije kako bi se kriminalističke istrage i postupci povodom kaznenih djela povezanih s računalnim sustavima i podatcima učinili učinkovitijima, te se omogućilo prikupljanje dokaza u elektroničkom obliku. (Bača, 2004:315;316)

4. Vrste kibernetičkog kriminala

Nagli razvoj i širenje informatičkih, telekomunikacijskih tehnologija, te interneta doveo je do velikih promjena u životu i radu ljudi. Korištenje i pojava novih aplikacija, servisa i usluga u elektroničkom poslovanju omogućuju nove oblike poslovne komunikacije, suradnje i razmjene informacija uz unaprijeđenje postojećih poslovnih procesa. Povećava se broj ozbiljnih napada koji su štetniji, opasniji i složeniji. Razvoj sve većeg tehničkog znanja počinitelja i korištenje naprednije informatičke opreme omogućuju stvaranje naprednih softverskih alata namjenjenim lakšem i bržem izvođenju napada. Napadi se mogu podijeliti prema različitim kriterijima ovisno o stupnju opasnosti, namjeri počinitelja, učinku, mjestu dolaska napada, cilju, načinu i metodi koje se koriste. (Dragičević, 2004:38;46;47;49)

Tablica 1. Volja napadača, mjesto nastanka, učinak i informacijski resursi

Volja napadača	**Mjesto nastanka**
- **namjerno** - svjesno poduzimanje radnji koje dovode do štetnih posljedica - **slučajno** - osoba koja nije znala , niti je mogla znati, da će njezine radnje na bilo koji način dovesti do ugroza	- **unutarnji** - izvodi osoba ovlaštena za pristup informacijskom sustavu - **vanjski** - izvodi osoba neovlaštena za pristup informacijskom sustavu
Učinak	**Informacijski resursi**
- **aktivni** - promjena objekata koji se napada (npr. mijenjanje podataka) - **pasivni** - sam objekt ostaje nepromijenjen (npr. neovlašten pristup podatcima bez da ih se mijenja ili briše)	- **podatkovni resursi** - ugroženje povjerljivosti, cjelovitosti ili dostupnosti. Neovlašteni pristup i uvod, izmjena i brisanje podataka - **programska osnovica informacijskog sustava** - neovlašteni pristupi i izmjenu/brisanje sistematskog, aplikativnog ili komunikacijskog softvera - **infrastrukturu informacijskog sustava** - opasna vrsta zbog ometanja ili onemogućavanja daljnjeg rada (napadi na hardver ili sredstva komunikacije)

Izvor: Autor, prema Dragičeviću D.

4. 1. Cilj

Najčešći ciljevi napada su:

1. **Korisničke lozinke** - omogućavaju da se putem njih nesmetano pristupi računalnom sustavu. Ovdje pripada nepažnja ovlaštenih korisnika, te nelojalni službenici.
2. **Datoteke s brojevima kreditnih (bankovnih) kartica i kartica za identifikaciju radi pristupa sutavu** - počinitelji obavljaju razne nezakonite financijske transakcije na štetu vlasnika ili lažnom identifikacijom, osiguravaju fizički pristup računalnom sustavu kako bi se zaobišla provjera i izvršila neka druga zloupotreba.
3. **Računalni programi** - njihovo neovlašteno brisanje, mijenjanje, kopiranje programa radi osobnog korištenja ili daljnje distribucije. Opasan slučaj je krađa izvornog koda koji se iskorištava za pribavljanje imovinske koristi, otkrivanje sigurnosnih slabosti koje će se kasnije iskoristit za neku drugu zloupotrebu njegovim resursima.
4. **Web stranice i News grupe** - neovlaštena promjena sadržaja u cilju promoviranja vlastitih ciljeva, uvrijeda, izrugivanja. Predstavljaju veliku opasnost jer prikazuju da se uz sve mjere i sredstva zaštite može pristupiti i promjeniti sadržaj, te preuzeti kontrola nad radom sustava čak i u najzaštićenijim informacijskim sustavima.
5. **Onemogućavanje korištenja računalnog sustava** - ovlaštenom korisniku se nastoji onemogućiti korištenje računalnog sustava, bez da se ugrožava integritet podatkovne, programske ili tehničke osnovice. Primjerice, slanje velike količine istih poruka, tako da se sustav u velikoj mjeri iskoristi da se do trenutka uklanjanja ne može više koristiti.
6. **Materijalni (tehnički) resursi informacijskog sustava** - ostvarenje neposrednog fizičkog pristupa takvim resursima s namjerom da se otuđe, unište ili oštete kako bi se onemogućilo njihovo daljnje korištenje. Najčešći su slučajevi krađe, osobito s prenosivim računalom ili s manjim, skupim dijelovima poput mikroprocesora. (Dragičević, 2004:47;48;49)

4. 2. Metode

Kako bi počinitelji osigurali neovlašten i nezakonit pristup tuđem računalnom sustavu koriste se raznim metodama:

1. **Društveni inženjering** - obuhvaća raznovrsne načine pribavljanja lozinki i rezultat su nepažnje ili lakovjernosti žrtva. Najpoznatiji su: Shoulder surfing (otkrivanje lozinke fizičkim uvidom prilikom upisa lozinke) i Strviranje (traženje po tuđem smeću, bačenim papirima ili bilješkama kako bi se pronašla lozinka). Ovlašteni korisnik koji je napustio radno mjesto, a da se nije odjavio i nastavljanjem rada pod njegovim korisničkim računom.
2. **Maskiranje/varanje** - preuzimanje identiteta druge osobe ili uloge drugog računalnog sustava (lažno prestavljanje). Često se odvija putem komunikacije telefonom kako bi se iskoristila trenutačna nepažnja žrtve. Zlouporaba povjerenja je neovlašten pristup sustavu putem drugog računalnog sustava tako da se uspostavi veza povjerenja što omogućava korištenje resursa kojemu je pristupio, bez da se svaki put provjerava njihov identitet.
3. **Spoofing** - koristi se slabostima protokola interneta i nedovoljnom pažnjom korisnika. Login spoofing (predstavljanje putem sličnih maski za upis korisničkih lozinka), web-spoofing (nesvjesnim odabirom pogrešnog hiperlinka dolazi do neželjene web stranice gdje se prikupljaju osobni podatci), E-mail spoofing (neposredna promjena podataka zbog dobivanja odgovora primatelja), Dns-spoofing (traže se brojčane adrese računala, preusmjerava se komunikacija na napadačev server i prikupljaju se podatci) i IP-spoofing (pristup putem IP adrese).
4. **Programske manipulacije** - korištenje raznih programskih rješenja pomoću kojih se dolazi do korisničkih lozinka. Poznati su: Pocket ili Password Sniffer - program namjenjen kopiranju podataka iz paketa u kojima oni putuju mrežom.
5. **Ostale metode su**: ispitivanje (nasumično pogađanje lozinke pomoću pokušaja i promašaja), pretraživanje (pristup sustavu pomoću programa radi pribavljanja informacija), prisluškivanje (telefonskih linija ili ugrađivanje prislušnih uređaja), optičko špijuniranje (presretanje elektromagnetskog zračenja s monitora), druženje (neformalno druženje sa zaposlenicima nakon radnog vremena i prikupljanje podataka) i kopmromitiranje (ucjenjivanje, podmićivanje ili iskorištavanje drugih ljudskih slabosti ovlaštenih osoba). (Dragičević, 2004:52;53;54)

4. 3. Tehnike

Počinitelj ima određena prava koja pripadaju ovlaštenom korisniku čiji identitet je zloupotrijebio. Najčešće su to obični korisnici s malim pravima, te počinitelj koristiti slijedeće tehnike:

1. **Pregledavanje** - sadržaja dostupnih datoteka za što se računalo koristi, dostupnost drugih datoteka i promatranje memorije zbog programa koji se koriste. Korisnici često nisu svjesni da opretivni sustav ili drugi program bilježe njihovo kretanje na mreži. Isti je slučaj s izbrisanim datotekama, rezervnim kopijama i slično.
2. **Stražnja vrata/zamke** - cilj je omogućiti počinitelju neovlašteni pristup računalnom sustavu zaobilaženjem redovnog postupka identifikacije i autorizacije. Koriste ih programeri tijekom razvoja softvera. Kod Stražnjih vrata se radi o prečacima koje su ostavili neovlašteni korisnici, a kod zamki o prečacima koje su ostavili i zaboravili ovlašteni korisnici. Suvremeni uvjeti rada omogućuju da se osobno računalo povezuje s računalom tvrtke, te se može doći do podataka tvrtke.
3. **Programi za analizu i nadzor rada sustava** - programi kojima prvotna namjena nije bila da se omogući bilo kakva zlouporaba. Program SATAN je namjenjen analizi rada računalnih mreža s ciljem da se pronađu slabosti. Koristite ga napadači.
4. **Superzapping** - omogućava sistem-administratoru ili drugoj osobi s visokim ovlaštenjima da zaobiđu sigurnosni sustav da bi što prije izvršili popravke ili intervencije u programima, te u pogrešnim rukama se može zloupotrijebiti.
5. **Greške u programima** - nesvjesne greške tijekom razvoja ili provjere na programima koji su rezultat autorskog rada zaposlenih, kupljeni ili čak besplatni mogu ugroziti sigurnost.
6. **Manipulacija podatcima** - korištenje programa za rad s bazama podataka ili izmjenom postojećih programa tako da s većeg broja računa skidaju manje iznose novca i prebacuju na drugi račun (tehnika salame) ili prebacivanje iznosa nakon druge decimale pri financijskim transakcijama (Francusko zaokruživanje).
7. **Uskraćivanje usluga** – onemogućavanje ovlaštenom korisniku da se koristi računalnim ili mrežnim uslugama i servisima. Primjer je Spamming je slanje velikog broja istih ili različitih poruka putem elektroničke pošte s namjerom da se zaguši prostor i tako padne sustav (razne reklamne i marketinške aktivnosti). (Dragičević, 2004:55;56;58)

4. 4. Maliciozni programi

Računalni programi ili dijelovi programskog koda čije pokretanje dovodi do neželjenih posljedica na računalnom sustavu, podatcima, programima ili uskraćivanja mrežnih servisa i usluga. (Dragičević, 2004:58)

Virusi usporavaju rad računala, uzrokuju čudno ponašanje, te stvaraju ozbiljnu štetu računalu i podatcima. Dizajnirani su da zaraze što više računala i datoteka. Prenose se e-poštom ili MS Wordovim dokumentima, ovise o pošiljateljevu otvaranju i šire se kroz zajedničko dijeljenje zaraženih datoteka. Mogu modificirati ili uništiti datoteke sustava i mijenjati ili obrisati korisničke datoteteke-dokumente. (Težak, 2010:20)

Crvi su zlobni softverski programi dizajnirani da se šire putem računalnih umreženja. Instaliraju se otvaranjem e-poštanskog privitka ili poruke koji sadrže znakovite tekstove. Kada se ugnijezdi unutar softverskog umreženja, prodire u vatrozidove i druge mjere sigurnosti. Kopira sam sebe dok ne iscrpi sustavne zalihe. Morrisov crv je jedan od prvih računalnih crva distribuiran internetom. (Težak, 2010:20)

Malver je softver dizajniran za oštećivanje računalnog sustava bez znanja i privole korisnika. Mogu se priključiti na korisnikov sustav, ukrasti lozinku ili se masovno poslati na e-adrese korisnika u adresaru. (Težak, 2010:21)

Trojanski konj je mrežna softverska aplikacija dizajnirana da bi ostala prikrivena u instaliranom računalu. Može brisati, preoblikovati ili šifrirati datoteke, špijunira korisnikovo računalo, instalira viruse, usporava rada računala i slično. (Težak, 2010:21)

Spyware je špijunski softver koji predstavlja veliku prijetnju. Potajno je instaliran da bi preuzeo kontrolu nad postupcima računala bez korisnikova pristanka. (Težak, 2010:23)

Adware je softver za podržavanje reklamiranja. Paket koji nakon instaliranja uz neku korisnu funkciju, automatski skida i prikazuje neki reklamni materijal. (Težak, 2010:23)

Rootkit je program ili kombinacija nekoliko programa dizajniranih da preuzmu temeljnu kontrolu računalnog sustava bez znanja vlasnika ili administrator. Pruža slobodan pristup sustavima, skriva datoteke, mape, druge komponente i krije zlobne datoteke. (Težak, 2010:23)

5. Zaštita poslovno informacijskih sustava

Tablica 2. Mjere zaštite od kibernetičkog kriminala

Tehničko - tehnološke mjere	- izgradnju i primjenu tehničkih sustava (videonadzora, alarmnih sustava, sustav za ograničen pristup prostorijama, serverima, bazama) - uvođenje suvremenih tehničkih sustava zaštite
Kadrovske mjere	- sigurnosne procedure pri odabiru menadžerskih, stručnih kadrova - obaještavanje svih kadrova o njihovim dužnostima, pravima, odgovornostima - imenovanje informacijskog menadžmenta, voditelja virtualnih timova…
Obrazovne mjere	- obrazovanje svih zaposlenika kako bi preventivno djelovali, poštovali i provodili mjere zaštite - sigurnosna izobrazba , usavršavanje kadrova i stjecanje certifikata
Etičke mjere	- primjena propisanih ili dogovorenih normi ponašanja (pristojnost, poslovno, korektno…) u provedbi poslovnih kontakata u sustavu mreža - sprečavanje govora mržnje, diskriminacije, prijetnji i zlouporabe internet za ostvarivanje zlonamjernih ciljeva, interesa i namjera
Sankcije	- u skladu sa zakonskim propisima i pravnim aktima poslovne organizacije - saslušanja, opomene, smanjenje plaće, oduzimanje ovlasti, otkaz…
Fizičke mjere	- nadzor ulazno-izlaznih mjesta, identifikacija posjetitelja, sprečavanje neovlaštenog ulaska, kretanja po poslovnom prostoru, provala, krađa…
Protuobavještajne mjere	- sprječavanje ilegalnog, neovlaštenog prodora u baze tajnih podataka - poduzimaju na programskoj, hardverskoj, fizičkoj, tehničkoj, stručnoj, upravnoj, zaposleničkoj, korisničkoj i suradničkoj razini
Financijske mjere	- osiguranje potrebnih financijskih sredstava za izgradnju, održavanje i rad sustava
Organizacijske mjere	- organiziranje, izgradnju i dogradnju sustava - provedba određenih zaštitnih mjera (organizacija sigurnosnih zona, pristup podatcima, dokumentima…).

Izvor: Autor, prema Javorović B. i Bilandžić M.

5. 1. Radno mjesto i okruženje

Hrvatska ima Pravilnik o sigurnosti i zaštiti zdravlja pri radu s računalima koji je u skladu sa smjernicama EU-a. Poslodavac je obvezan izraditi procjenu opasnosti za sva radna mjesta s računalom i brigu o zdravlju radnika. Određena su i načela pri oblikovanju, izboru, naručivanju i mijenjanju programske opreme i radnih zadataka s računalom. Kod složenih radnih zadataka s računalom, radnici se moraju dodatno educirani za rad s programskom opremom i zadovoljavati stručne i psihofizičke preduvjete. Poželjno je educirati zaposlenike o organizaciji odmora i vježbi tijekom duljeg rada s računalom (danas se provodi puno vremena za računalom) i održvati preventivne zdravstvene preglede. Prilog pravilniku su zahtjevi koje mora ispunjavati radno mjesto, a poslodavcima je dan rok od četiri godine za zamjenu postojeće opreme i namještaja. Radno mjesto po mjeri zaposlenika povećava radne učinke jer zaposlenik može raditi brže, bolje, efikasnije i točnije). 2005. godine Vlada Republike Hrvatske donijela je Nacionalni program informacijske sigurnosti (definiraju se ciljevi informacijske sigurnosti na razini države, nadležnosti, poslovi pojedinih institucija i potrebnu međusobnu koordinaciju svih čimbenika informacijske sigurnosti). Strateška zadaća je postupno širenje procesa informacijske sigurnosti na državu u cjelini, uvođenjem odgovarajućih minimalnih sigurnosnih kriterija, te razvoj sigurnosne kulture. Nema niti sustavne organizacije tečajeva ili drugih oblika cjeloživotnog obrazovanja. U tvrtkama postoji potreba za dodatnom edukacijom zaposlenika, jer nema sustavne organizacije tečajeva ili dugih oblika cjeloživotnog obrazovanja. (K. Klasić, 2007.)

Kreiranje dobre lozinke koja neće upotrebljavati osobne podatke, smislene riječi, već treba kombinirati razne tipove znakova, fraze lozinka, često mijenjati ih i promjeniti e-adresu. (Težak, 2010:34)

5. 2. Programske mjere zaštite podataka

Kriptografija – znanstvena disciplina koja se bavi proučavanjem metoda slanja poruka u obliku da ih samo onaj kome su namijenjene može pročitati. (Bukovac T., 2016.) Današnji sustavi koriste se tzv. Asimetričnim ključevima (parom ključeva) – javni koji je u pravilu svima dostupan i koristi se za šifriranjem poruka, te tajnim koji posjeduje samo primatelj poruke i može ju jedini dešifrirati. Tako su podatci nečitljivi svakome osim primatelja, osobito kada se radi o brojevima kreditnih kartica i slično. (Težak, 2010:35)

Antispaywer - prati dolazni podatkovni promet (elektroničke pošte, web stranica, datoteke) i sprječava infekciju računala spyware programa (špijunski program). Često se ažuriraju od strane proizvođača kako bi bili u mogućnosti zaštititi sustav od najnovijih spyware programa. (Bukovac T., 2016.)

Antivirus - softverski alat za zaštitu računala i mreže od računalnih virusa. Pregledava dolazni podatkovni promet, skenira sadržaj, provjerava sve datoteke koje korisnik otvara, te word dokumente za mikro viruse. Uspoređuje kod sa potpisima virusa u bazi podataka i provjeravaju programe po ponašanju. Nakon otkrivanja virusa, zaražena datoteka se može izbrisati, prebaciti u karantenu ili ignorirati upozorenje. (Bukovac T., 2016.)

Zaštitni zid - mrežni sigurnosni sistem koji kontrolira dolazni i odlazni promet po određenim sigurnosnim pravilima. Zatim odlučuje da li će dopustiti podatkovni promet ili ga blokirati. Može biti softverskog ili hardverskog tipa. Sprječava neželjen pristup korisnikovom računalu na način da identificira i sprječava komunikaciju preko riskantnih portova (komunikacijski kanali po kojima računalo komunicira sa vanjskim mrežama). Može otkriti čudna ponašanja u dolaznom prometu. (Bukovac T., 2016.)

5. 3. Zakoni

Zakonima se žele postići uvjeti za siguran i nesmetan informacijski razvoj. Ovim se Zakonom utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti. Primjenjuje na državna tijela, tijela jedinica lokalne, područne (regionalne) samouprave, na pravne osobe s javnim ovlastima, fizičke i pravne osobe koje u svom djelokrugu koriste klasificirane i neklasificirane podatke. (Zakon RH o informacijskoj sigurnosti, NN 79/07)

Područje informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

1. sigurnosna provjera,
2. fizička sigurnost,
3. sigurnost podatka,
4. sigurnost informacijskog sustava,
5. sigurnost poslovne suradnje (Zakon RH o informacijskoj sigurnosti, NN 79/07)

Sigurnosnom provjerom se utvrđuju mjere i standardi koji se primjenjuju na osobe, tijela i pravne osobe koje imaju pristup klasificiranim podacima i certifikat o pristupu, broju i rokovima važenja. Fizička sigurnost se očituje u zaštiti objekta, prostora i uređaja tako da se oni kategoriziraju na sigurnosne zone, propisane mjere i standarde informacijske sigurnosti. Sigurnost podatka su opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka. Sigurnost informacijskog sustava su klasificirani i neklasificirani podatci koji se obrađuju, pohranjuju ili prenose u informacijskom sustavu te zaštita cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava. Sigurnost poslovne suradnje je provedba natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuje pravne i fizičke osobe. (prema Zakonu RH o informacijskoj sigurnosti, NN 79/07)

5. 4. Norme

Uvođenjem sustava upravljanja sigurnošću, organizacija se može suočiti s prijetnjama i na vrijeme reagirati kako bi postala prepoznat, pouzdan i moderan poslovni partner. U Velikoj Britaniji 1993. godine razvijena je norma BS 7799 standard koja osigurava fleksibilnost, definira upravljački okvir i primjenjiva je u organizacijama različitih tehničkih sustava. Iz tog standarda su proizašle dvije međunarodne norme informacijske sigurnosti usvojene od strane Hrvatskog zavoda za norme, a to su: HRN ISO/IEC 27001 i HRN ISO/IEC 17799. Razvojem informacijskih tehnologija, povećavao se broj normi i područje koje one pokrivaju. ISMS predstavlja sistemski pristup upravljanja sigurnošću informacija prisutnih u organizaciji, a uključuje procese, djelatnike, IT sustav i politiku. ISO i IEC zajedno čine sustav za međunarodnu standardizaciju. Njihova primjena osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, povećanje pouzdanosti sustava u slučaju katastrofe te pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja djelatnika vezanim uz informacijsku sigurnost. Implementacija norme ISO/IEC 27001 provodi se kroz 8 glavnih koraka:

1. Počinjanje projekta - usvajanje sigurnosne politike, potpora višeg menadžmeta, obuka tima
2. Definiranje ISMS-a - cilj, svrhu, opseg, granice, ograničenja, međusklopove, ovisnosti, izuzeća, opravdanja, strateški i organizacijski kontekst
3. Procjena rizika - vrijednost resursa, ranjivost, prijetnja, ostvarenje prijetnji i posljedice
4. Upravljanje rizikom - smanjenje, prihvaćanje, izbjegavanje i prijenos rizika; ciljevi, implementirati kontrole, izraditi plan (zadatke, odgovornosti, sudionike i dr.)
5. Obuka i osvješćivanje - vještina, obuka, kvalifikacija, iskusnost, ocjenjivanje
6. Priprema za reviziju - Izjava o primjenjivosti (ciljevi, odabrane kontrole,..)
7. Revizija - revizija dokumentacije i revizija implementacije
8. Osvješćivanje - redovna provjera i unaprjeđenje upravljačkog okvira (Bogati J., 2011.)

Implementacijom normi jasna je nadležnost, odgovornost i ovlast unutar informacijskog sustava. Nužne su za kvalitetnu, odgovornu i uspješnu provedbu sigurnosnih procedura i detaljno je određena zaštita i klasifikacija podataka, područje sustava, uporaba interneta i intraneta te suradnja s korisnicima izvan sustava. (Bogati J., 2011.)

5. 5. Institucije za informacijsku sigurnost u Republici Hrvatskoj

Različite institucije nastoje osigurati sigurnost poslovno informacijskog sutava i općenito informacija. U RH informacijski sutav je dobro reguliran i razrađen zakonima, normama i institucijama.

Djeluje pet najvažnijih institucija:

1. Nacionalni CERT
2. Ured vijeća za nacionalnu sigurnost (UVNS)
3. Zavod za sigurnost informacijskih sustava (ZSIS)
4. Agencija za zaštitu osobnih podataka (AZOP)
5. Hrvatska akademska i istraživačka mreža (CARNET)

Nacionalni CERT je odjel Hrvatske akademske i istraživačke mreže – CARNET. Osnovan je 30. listopada 2007. godine prema Zakonu o informacijskoj sigurnosti Republike Hrvatske. Nacionalno je tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti. Bavi se i incidentima sa znatnim učinkom prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga. Njegove usluge su dostupne široj javnosti i financiran je sredstvima koja osigurava Ministarstvo znanosti i obrazovanja, a drugi dio Europska unija kroz razne EU projekt. Provodi:

proaktivne mjere:

a) sigurnosne preporuke
b) praćenje računalno-sigurnosnih tehnologija
c) unapređenje svijesti o značaju računalne sigurnosti
d) edukacija i obuka o računalnoj sigurnosti i ostale

reaktivne mjere:

a) sigurnosna upozorenja
b) postupanje s računalno-sigurnosnim incidentima
c) koordinacija rješavanja značajnijih incidenata (prema Nacionalnom CERT-u)

Ured vijeća za nacionalnu sigurnost obavlja stručne i administrativne poslove obavještajnih agencija da one obavljaju svoje zakonom utvrđene obaveze iz područja nacionalne sigurnosti. Izrađuje objedinjena, periodična izvješća i strategijske procjene za potrebe Predsjednika Republike i Vlade. Također koordinira, usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, informacijskih sustava i poslovne suradnje. Izdaje certifikate za fizičke i pravne osobe za pristup nacionalnim, NATO i EU klasificiranim podacima. Nastojati dati svoj doprinos poslovima koji se ostvaruju na dobrobit slobode, prosperiteta i sigurnosti svih državljana. Odlukom Vlade u ime Republike Hrvatske zaključuje međunarodne sigurnosne ugovore za zaštitu klasificiranih podataka. (Ured vijeća za nacionalnu sigurnost)

Zavod za sigurnost informacijskih sustava središnje je državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava, upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka te koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. Djelokrug i zadaće utvrđeni su Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske, Zakonom o informacijskoj sigurnosti te Uredbom Vlade Republike Hrvatske o mjerama informacijske sigurnosti. Nadležan je i za poslove istraživanja, razvoja i ispitivanja tehnologija namijenjenih zaštiti klasificiranih podataka te izdavanja uvjerenja za njihovu uporabu. Njegovi standardi se rimjenjuju se na sva državna tijela, jedinice lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima koje u svom djelokrugu koriste klasificirane i neklasificirane podatke. Pokrenuo je suradnju s vodećim hrvatskim znanstvenim i istraživačkim ustanovama težeći poticanju novih oblika prijenosa znanja i daljnjem razvoju vlastitih sposobnosti korištenjem najboljih nacionalnih znanstvenih, inovacijskih i obrazovnih potencijala. (Zavod za sigurnost informacijskih sustava)

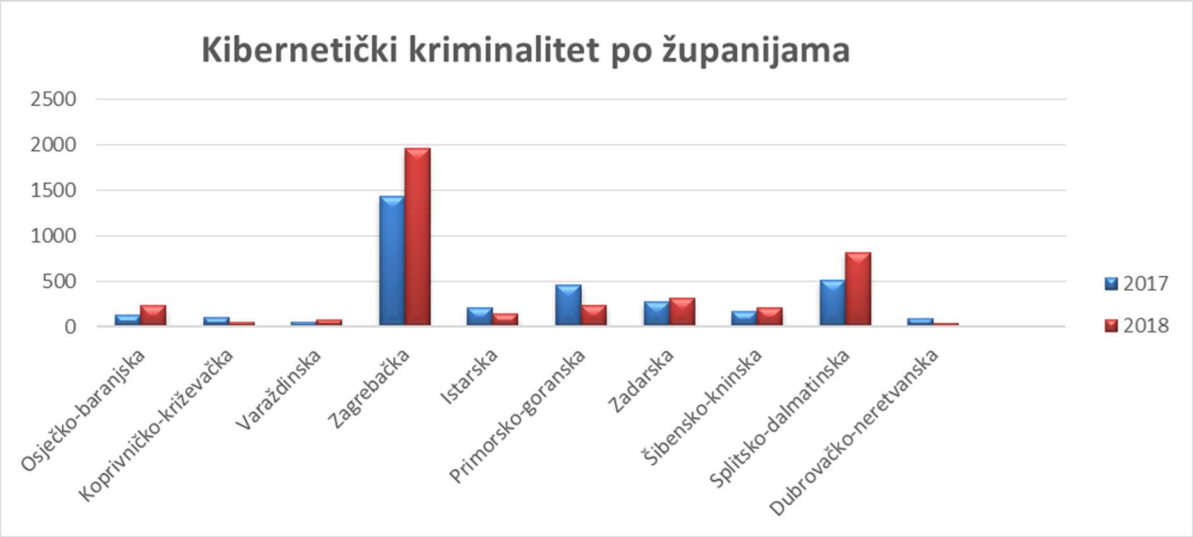
Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o provedbi Opće uredbe o zaštiti podataka kojim se osigurava provedba Uredbe Europskog parlamenta i Vijeća od 27. travnja. 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka. Propisuje

Konvenciju za zaštitu osoba automatizirane obrade osobnih podataka i Dodatni protokol u vezi nadzornih tijela i međunarodne razmjene podataka koji je zakonom potvrdio Hrvatski sabor. Njezini zadatci su podizanje razine svijesti dionika i svih ciljanih javnosti o važnosti zaštite osobnih podataka i njihovim pravima i obvezama, predlaganje mjera za stručno osposobljavanje i usavršavanje službenika za zaštitu osobnih podataka i ukupna provedba svih upravnih i stručnih poslova koji proizlaze iz Opće uredbe i Zakona o provedbi Opće uredbe o zaštiti podataka. Također ima određenu ndležnost, savjetodavne i istražne ovlasti u zaštiti osobnih podataka kojee su u skladu sa Zakonima Republike Hrvatske. (Agencija za zaštitu osobnih podataka)

Hrvatska akademska i istraživačka mreža je ustanova koja djeluje u sklopu Ministarstva znanosti i obrazovanja u području informacijsko-komunikacijske tehnologije i njezine primjene u obrazovanju. 1991. godine se javlja kao projekt tadašnjega Ministarstva znanosti i tehnologije te postaje prvi i jedini pružatelj internetskih usluga u Hrvatskoj. Osniva se ustanova CARNET radi inoviranja obrazovnoga sustava te poticanja napretka pojedinaca i društva u cjelina. Privatna je mreža akademske, znanstvene i istraživačke zajednice Republike Hrvatske i institucija u sklopu osnovnoga i srednjoškolskoga obrazovnog sustava. Preko CARNET mreže je povezano 2600 ustanova na 3800 lokacija širom Hrvatske. Najnovijim trendovima u području IKT-a, infrastrukture i obrazovanja osmišljavaju različite projekte i razvijaju nove usluge poput e-Maticu i Nacionalni informacijski sustav prijava i upisa u srednje škole, e-Građani mToken vjerodajnicu i e-Dnevnik S ciljem izgradnje digitalno zreloga društva razvili su program “e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće”. Surađuju s drugim europskim akademskim i istraživačkim mrežama, organizacijom GÉANT Association i organizacijama koje su zadužene za upravljanje internetskim resursima u svijetu. (Hrvatska akademska i istraživačka mreža).

6. Kibernetički kriminal u Hrvatskoj

Grafikon 1. Usporedba kibernetičkog kriminala po županijama u 2017. i 2018. godini



Izvor: Autor, prema MUP-u, 2019. godina

Prema tablici možemo zaključiti kako u nekim županijama u 2017 godini je dosta visok/niski broj prijava, razrješenja i naknadnog otkrivanja ovog oblika kriminaliteta. Za razliku od 2018. godine kada u tim istim županijama se uvelike smanjio/povećao broj. Primjerice u Zagrebačkoj županiji u 2017. godini je bilo 1424 prijave, razrješenja i naknadnog otkrivanja kibernetičkog kriminliteta, a u 2018. godini se udvostručio na broj 1960. Ukoliko uzmemo u oobzir Primorsko-goransku županiju, gdje je u 2017. godini više ovog oblika kriminaliteta nego u 2018. godini.

Problemu kibernetičkog kriminala u Hrvatskoj, njegovoj prevenciji, zaštiti informacijskog sustava i korisnika ne posvećuje se dovoljna pozornost. Uz objektivne okolnosti: Domovinski rat i gospodarsko zaostajanje, glavni razlozi su kašnjenje kaznenopravne regulative, nedovoljna informatička pismenost, nedostatnim ulaganjima u sigurnost i zaštitu informacijskih sustava, nižem stupnju korištenja i oslanjanja na informatičku tehnologiju u odnosu na gospodarski razvijene zemlje. Razlog je i ljudska slabost: neznanje, nemar, nepažnja i namjerne radnje. Ne poznaju se točne činjenice o rasprostranjenosti i broju takvih djela u Republici Hrvatskoj, jer su malobrojni otkriveni i prijavljeni slučajevi. (Dragičević, 2004:186)

6. 1. Prvi slučaj računalnog kriminala kod nas

Prvi slučaj računalnog kriminala se dogodio u bivšoj Socijalističkoj Frederativnoj Republici Jugoslaviji. 21.02.1983. godine uhičeni su dva službenika Istarske banke i jedan Filijale Zagrebačke banke u Puli. Prva dva službenika radeći kao operateri na sustavu, uz pomoć bivšeg rukovoditelja tog centra izveli su financijsku malverzaciju na računalu kojom su nmjeravali oštetiti banku za 10.113.353.50 dinara. Prijevara je otkrivena i prijavljena, te je vijeće okružnog suda osudilo prvu dvojicu na 3 godine i 8 mjeseci, te rukovoditenj na 4 godine i 10 mjeseci zatvora. (Babić, 2009:254:257)

Počinitelj je u Istarskoj banci otvorio 11 štednih knjižica sa saldom od 2,160 dinara, pripisane su kamate, te novi saldo iznosi 936,378 dinara za koje je banka oštećena. Djelo je izvedeno pomoću računala u banci. Prilikom kapitalizacije utvrđeno je da neke novootvorene štedne knjižice nemaju realnu upisanu kamatu (mali saldo i velika kamata), te da je programska greška. Te knjižice su glasile na "donosioca", te su njihovi brojevi uzeti s ugašenih - likvidiranih štednih knjižica. Nepoznati počinitelj je bez pisanih dokumenata - pristupnica odobrio matične podatke za 11 knjižica. Proknjižena su salda u odgovarajućim početnim iznosima. Operacija je izvedena tako da uplate - doznake za početni saldo nisu provedene u računalu kroz dnevni promet, niti prikazane u mjesečnom prometu za 11 mjeseci. Sve je izvedeno kako bi se prikrilo kazneno djelo. (Babić, 2009:255)

Ideja o milionima je pošla od bivšeg rukovoditelja računalnog centra Istarske banke. Dobro je poznavao proces, strukturu i funkcije programa, te je službenicima dao upute što i kako trebaju uraditi. U procesu obrade podataka događale su se greške, te su se aktivirali posebni programi kojima su se takve greške otklanjale. Namjerno je izazvana greška na računalu da bi se simulirala takva situacija, te omogućilo da se izvrši unos podataka direktno na računalo bez prateće dokumentacije. (Babić, 2009:256)

Ostalo im je još da naprave knjižice blankete, njih upišu stanje i kamate, jer bez njih se novac ne može podići. Do blanketa knjižica i pečata se moglo lako doći, jer za njih nitko nije zadužen. Dogovor je bio da se novac podigne nakon godine dana, jer za knjižice koje glase na "donosioca" ne zahtjeva identifikacija vlasnika. (Babić, 2009:257)

7. Intervju

Strukturirani intervju s načelnicom i informatičrom Hrvatskog zavoda za mirovinsko osiguranje: podružnice ureda Bjelovar. Utjecaj kibernetičkog kriminala na sigurnost poslovno informacijskog sustava na Zavodu za mirovinsko osiguranje u Bjelovaru.

Intervju s načelnicom odjela za mirovinsko osiguranje vođen je 16. rujna 2021., razgovorom u njezinom uredu u trajanju od 15 minuta. Odgovori na pitanja su detaljno bilježeni za kasniju interpretaciju.

1. Jeste li upoznati s kibernetičkim kriminalom u poslovanju?

Upoznata sam s kibernetičkim kriminalom u poslovanju. U našem poslovanju svakodnevno se obavještava o važnosti zaštite podataka, na pregledavanju sumnjivih mailova i slično. Često se događaju napadi kako bi došli do podataka naših klijenata.

2. Kakvom tehnologijom i programima raspolaže poduzeće?

Tehnologija i programi koji se koristi unutar HZMO-a je rad u bazi IMMS (informacijski mirovinski sustav). U bazi se nalaze podatci o aktivnim osiguranicima, korisnicima mirovine, individualnim poljoprivrednicima, doplatci za djecu, poslovi financija, interna poslovanja zavoda, zajednički kadrovski poslovi, poslovi uz II. stup mirovinskog osiguranja i poslovi uz donošenje rješenja. Sastoji se od programa LANA (elektronička knjižica) i ESUD-a (elektronički sustav upravljanja dokumentima).

3. Koje se sigurnosne mjere ili preventive koriste unutar HZMO-a podružnice Bjelovar?

Prilikom ulaska u bazu svaki zaposlenik ima svoju šifru jer sadrži zakonom zaštićene podatke, te se korisničko ime, vrijeme, mjesto i predmet rada bilježe. Također za različite programe, korisnici imaju različite lozinke. Svaki odjel i odsječak dobiva samo svoj mail koji sadrži radni zadatak, te su tako mailovi ograničeni. U vrijeme Covid-19 virusa, većinu upita obavljamo telefonskom komunikacijom koja je ograničena i kontrolirana. Također na ulasku u zgradu imamo zaštitare koji kontroliraju klijente.

4. Jeste li zadovoljni sa sigurnosnim mjerama i preventivom HZMO-a podružnice Bjelovar?

Sa sigurnosnim mjerama koje se provode nisam u potpunosti zadovoljna. Trebala bi se uvesti bolja zaštitita podataka, osobito osobni podatci koji su još uvijek u tiskanom obliku. Učestala

edukacija bi bila poželjna, jer dosta zaposlenika je starije starosne dobi dok tehnologija svakim danom sve više i više napreduje.

5. Događaju li se napadi, koji su to i koji je bio najizraženiji?

Napadi se često odvijaju putem mailova koje svakodnevno dobivamo. Čudne su naravi, uvijek nas informatičar obavještava koje mailove da ne otvaramo. Ti mailovi su pod imenom važnih institucija s kojima surađujemo poput porezne, FINE i ostalih, a adresa glasi na nepoznatog počinitelja. Imamo problema i s upadom u naše sustave, no oni su na vrijeme sprječeni. Ne sjećam se ni jednog izraženog napda.

6. Provode li se edukacije zaposlenika i koliko često o kibernetičkom kriminalu?

Edukacije o uvođenju novog programa u ustav se provode, ali o zaštiti ne. Svaki dan stižu obavijesti za neotvaranje sumnjivih mailova, te na početku ulaska u sustav stoji obavijest o zaštiti podataka klijenata i čega se trebamo pridržavati. Prije se sve dijelilo ručno pomoću spisa unutar organizacije, teško je bilo čuvati podatke korisnika, ali sada s napretkom tehnologija se to uvelike olakšalo.

7. Smatrate li da su zaposlenici dovoljno informirani i educirani?

Smatram da zaposlenici nisu dovoljno informirani i educirani.

8. Što biste promjenili ili uveli kao veću sigurnost unutar HZMO-a podružnice Bjelovar?

Kao veću sigurnost bi uvela česte edukacija zaposlenika o različitim načinima zaštite podataka, njihovoj sigurnosti putem računala i različitim opasnim načinima zlouporabe računala i informacija. Određena ograničenja na sustavu i samom radnom mjestu za pojedinca koji radi. Redovnu kontrolu podataka i mailova, te različite dodatne programske zaštite.

9. Smatrate li da bi poduzeća trebala više posvetiti pažnju kibernetičkom kriminalu u poslovanju, zašto?

Poduzeća bi trebala više posvetiti pažnju kibernetičkom kriminalu jer je to danas jako rašireno u organizacijama. Sve se više zlopupotrebljava računalo, odnosno sustavi kako bi se nanijela šteta velikim organizacijama.

Zatim je obavljen intervju u kadrovskoj službi s inforamtičarom cijele podružnice HZMO-a Bjelovar. Intervju je trajao 20 minuta i postavljena pitanja su ista.

1. Jeste li upoznati s kibernetičkim kriminalom u poslovanju?

Da upoznat sam s kibernetičkim kriminalom u poslovanju. Danas kako napreduju tehnologije, tako napreduje i ovaj oblik kriminala s kojim se vjerujem sve organizacije svakodnevno susreću.

2. Kakvom tehnologijom i programima raspolaže poduzeće?

Tehnologijom i programima s kojima raspolaže poduzeće su IMMS (informacijski mirovinski sustav). On se sastoji od programa LANA i ESUD-a. Osim njih još koristimo OUTLOOK (adrese, mailovi, kalendari) i RAKLE (prijave na mirovinsko osiguranje, isplata plaća radnicima različitih organizacija).

3. Koje se sigurnosne mjere ili preventive koriste unutar HZMO-a podružnice Bjelovar?

Sigurnosne mjere koje koristimo su Watrozidovi, ograničenja mailova po odjelima, svaki zaposlenik koristi svoju lozinku, kao i za različite aplikacije i imamo zaštitara na ulasku u zgradu HZMO-a kako bi provjeravao klijente.

4. Jeste li zadovoljni sa sigurnosnim mjerama i preventivom HZMO-a podružnice Bjelovar?

Zadovoljan sam sa sigurnosnim mjerama koje provodimo, ali s edukacijom zaposlenika nisam. Imamo seminare koji traju po tri dana, ali je problem što online se ne može mnogo zaposlenika prijaviti jer je ograničen broj sudionika. Radimo i na novom programu MALWARE SYTES NEALA AGENT koji skenira opasnosti, probleme ili zlouporabe. Vikendom se aktivira na svim računalima, a radnim danima svakih par sati kako bi se sačuvali podatci na dva ili tri mjesta i koji se šalju u Zagreb i Varaždin. Problem je kod novog programa što računala unutar poduzeća imaju 8GB ili 4GB. Računala od 4GB jako blokiraju, slabi su ili im nedostaje memorija.

5. Događaju li se napadi, koji su to i koji je bio najizraženiji?

Napadi se često događaju, osobito s mailovima s kojima najviše raspolažemo u radu. Najčešći napadi se događaju putem mailova. Najizraženiji se dogodio u Vukovaru gdje je jedna zaposlenica otvorila mail. Pisalo je da je od FINE, a zapravo je bio od hakera i svi sustavi na HZMO-u su pali u cijeloj Hrvatskoj. Nitko nije mogao raditi otprilike 5 do 6 sati dok, mi

informatičari iz različitih dijelova Hrvatske nismo uspjeli podići sustav i zaštititi ga. Od tada svi zaposlenici provjeravaju mailove i redovno ih obavještavamo.

6. Provode li se edukacije zaposlenika i koliko često o kibernetičkom kriminalu?

Edukacije ne, ali obavijesti upozorenja da. Novo smo uveli zoom i skyp edukacije o novim programima, sustavima i slično koji se pojavljuju u sustavu. Predstojnica podružnice Bjelovar koristi ADOBE OIDER privatni program za posebne važne podatke i poslovne partnere.

7. Smatrate li da su zaposlenici dovoljno informirani i educirani?

Zaposlenici nisu dovoljno educirani i informirani. To najviše vrijedi za stariju populaciju zaposlenika kojima se teško priviknuti na nove tehnologije, a najviše upoznavanje ovog oblika kriminala. Ne shvaćaju koliko je to opasno.

8. Što biste promjenili ili uveli kao veću sigurnost unutar HZMO-a podružnice Bjelovar?

Uveo bi veću educiranost kod zaposlenika, a redovno usavršavamo programe koji se nalaze u sustavu i zaštite kojima ih štitimo, pa sa sustavom ne bih ništa mijenjao.

9. Smatrate li da bi poduzeća trebala više posvetiti pažnju kibernetičkom kriminalu u poslovanju, zašto?

Smatram da bi poduzeća trebala posvetiti veću pažnju kibernetičkom kriminalu. Kada dođe do ovog oblika kriminala tada se gube neki podatci, zloupotrebaljavaju se, te stranke dosta znaju čekati kada padne sustav ili se ažurira kako bi bio siguran. Usporava se i rad u cijelom HZMO-u i tako neki radni zadatci ne mogu biti obavljeni na vrijeme ili je ponovo teško pronaći podatke koji su se pogubili.

8. Zaključak

Na temelju provedenog intervjua moguće je zaključiti kako glavna načelnica odjela za osiguranje HZMO-a podružnice Bjelovar smatra kako zaposlenici nisu dovoljno educirani, potrebno je uvođenje edukativnih programa, te nije dovoljna zaštita koja se provodi u sustavu i na radnom mjestu. Iz kadrovske službe, informatičar HZMO-a podružnice Bjelovar smatra da je najviše bitna edukacija zaposlenika koja nije dovoljna, dok je sustav dovoljno zaštićen i radi se svakodnevno na usavršavanju sigurnosti.

Na temelju izučavanja relevantnih literarnih izvora nameće se zaključak da je Kibernetički kriminal u poslovanju dosta raširen, ali se njemu ne pridaje dovoljna pažnja, te se ne prijavljuju i bilježe slučajevi. Potrebno je provesti opsežnije istraživanje u Republici Hrvatskoj putem anketnih upitnika, intervjua različitih organizacija, osobito velikih korporacija i slično kako bi se utvrdilo koliko je zastupljen, koje opasnosti danas donosi i na koji način se unaprijed može sprječiti. Također je važno da se norme i zakoni koji su doneseni o ovom obliku kriminala u stvarnosti provode.

9. Literatura

Tiskani izvori:

1. Brumec J. (2011.) Modeliranje poslovnih procesa, Prvi dio: Uvod u modeliranje, Koris, Varaždin/Zagreb

2. Babić V. (2009.), Kompjuterski kriminal: metodologije kriminalističkih istraživanja, razrješavanja i suzbijanja kompjuterskog kriminala, Rabic, Sarajevo

3. Bača M. (2004.) Uvod u računalnu sigurnost, Narodne novine d.d., Zagreb

4. Dragičević D. (2004), Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb

5. Javorović B., Bilandžić M. (2007.), Poslovne informacije i business intelligence, Golden marketing – Tehnička knjiga, Zagreb

6. Luić LJ. (2009.) Informacijski sustavi, Veleučilište u Karlovcu, Karlovac

Mrežni i elektronički izvori:

1. Agencija za zaštitu osobnih podataka, URL: https://azop.hr/djelatnost-agencije (pristupljeno 17. rujna 2021.)

2. Bukovac T. (2016.) Sigurnost informacijskih sustava, Diplomski rad, Sveučilište u Zagrebu, Zagreb, URL: http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf (pristupljeno 17. rujna 2021.)

3. Bogati J. (2011.) Norme informacijskog sustava ISO/IEC 27K. Praktični menadžment : stručni časopis za teoriju i praksu menadžmenta. Virovitica: Visoka škola za menadžment u turizmu i informatici u Virovitici, str. 112 – 117, URL: https://hrcak.srce.hr/76462 (pristupljeno 17. rujna 2021.)

4. Hrvatska akademska i istraživačka mreža, URL: https://www.carnet.hr/o-carnet-u/ (pristupljeno 17. rujna 2021.)

5. Klasić K. (2007.) Zaštita informacijskih sustava u poslovnoj praksi. Sigurnost: časopis za sigurnost u radnoj i životnoj okolini. Zagreb: Zavod za istraživanje i razvoj sigurnosti d.d., str. 37 - 47, URL: https://hrcak.srce.hr/11861 (pristupljeno 17. rujna 2021.)

6. Nacionalni CERT, URL: https://www.cert.hr/onama/ (pristupljeno 17. rujna 2021.)

7. Ured vijeća za nacionalnu sigurnost, URL: https://www.uvns.hr/hr/hr/o-nama/uvodna-rijec (pristupljeno 17. rujna 2021.)

8. Zakon Republike Hrvatske o informacijskoj sigurnosti, NN 79/07, URL: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti (pristupljeno 17. rujna 2021.)

9. Zavod za sigurnost informacijskih sustava, URL: https://www.zsis.hr/default.aspx?id=13 (pristupljeno 17. rujna 2021.)

Popis tablica

Popis grafikona

Prilog 1: Pitanja za intervju

Utjecaj kibernetičkog kriminala u HZMO-u podružnice Bjelovar

1. Jeste li upoznati s kibernetičkim kriminalom u poslovanju?

2. Kakvom tehnologijom i programima raspolaže poduzeće?

3. Koje se sigurnosne mjere ili preventive koriste unutar HZMO-a podružnice Bjelovar?

4. Jeste li zadovoljni sa sigurnosnim mjerama i preventivom HZMO-a podružnice Bjelovar?

5. Događaju li se napadi, koji su to i koji je bio najizraženiji?

6. Provode li se edukacije zaposlenika i koliko često o kibernetičkom kriminalu?

7. Smatrate li da su zaposlenici dovoljno informirani i educirani?

8. Što bi ste promjenili ili uveli kao veću sigurnost unutar HZMO-a podružnice Bjelovar?

9. Smatrate li da bi poduzeća trebala više posvetiti pažnju kibernetičkom kriminalu u poslovanju, zašto?