ZAŠTITA OD SAJBER NAPADA I IZAZOVA / PROTECTION FROM SYBER ATTACKS AND CHALLENGES

Robert Atanasov[1]
[1]MUP RSM
e-mail: r.atanasov@yahoo.com

Prelgedni članak
UDK / UDC 343.8:004

Sažetak

S*vakodnevno poslovanje preduzeća determinisano je upotrebom računarske tehnologije, informacionih sistema, interneta itd. Olakšava poslovanje, štedi vrijeme, energiju, resurse, olakšava i unapređuje radni proces. Ali, kao iu svakoj drugoj sferi, i u ovoj se javljaju devijantne pojave. Kriminalci nastoje da zloupotrebe nauku u kriminalne svrhe. Cilj je brzo steći protivpravnu imovinsku korist na inteligentan način. Štaviše, poznato je da u svijetu ne postoji potpuno pouzdan kompjuter koji je imun na sajber napade. Kompanije svakodnevno prijavljuju štetu, bilježe se ogromni gubici od sajber napada. To ih prisiljava da ulože mnogo novca u zaštitu svojih kompjuterskih sistema. Postoji raznolika fenomenologija ovog zločina. U radu je dat pregled osnovnih mjera zaštite od sajber napada..*

***Ključne riječi**: kompjuter, sajber napadi, promocija.*
JEL klasifikacija: O33

Abstract

The daily work of companies is determined by the use of computer technology, information systems, the Internet, etc. It facilitates business operations, saves time, energy, resources, facilitates and improves the work process. However, as in any other sphere, deviant phenomena occur in this one too. Criminals seek to abuse science for criminal purposes. The goal is to quickly acquire illegal property benefits in an intelligent way. Moreover, it is known that there is no completely secure computer that is immune from cyber attacks in the world. Companies report damage every day, huge losses from cyber attacks are registered. This forces them to invest a lot of money to protect their computer systems. There is a diverse phenomenology of this crime. The paper provides an overview of the basic protective measures against cyber attacks.

***Keywords**: computer, cyber attacks, promoting.*
JEL classification: O33

UVOD

Čini se da je funkcionisanje današnjeg društva, uključujući sve njegove posebnosti u životu građana, poslovanje preduzeća, funkcionisanje institucija u društvu ili državi, život građana u domaćim uslovima, uključujući sve kategorije uopšte, postalo ovisni o kompjuterskoj tehnologiji i upotrebi kompjuterskih sistema, kao nikada do sada. "Potreba za novim tehnologijama zahtijeva pojačanu eksploataciju prirodnih bogatsva uz istovremeno osvajanje automatizacije inteligencije u smislu efikasnijeg poslovanja u budućnosti."[240]

Čini se da je i upotreba kompjuterske tehnologije postala takva neophodna nužnost u funkcioniranju građana i država, bez koje se uopće ne može zamisliti funkcioniranje svijeta. u svakodnevnom radu. Sa razvojem tehnologije dolazi i potreba za sajber sigurnosti kako bi se zaštitili podaci i infrastruktura organizacija od različitih syber prijetnji."[241]

Pritom se podrazumijeva da ta neophodna ovisnost i nužnost, bez kojih se ne može zamisliti funkcioniranje svijeta, nije nastala kao namet, kao teret ili kao uvjet, već naprotiv, nastala je kao rezultat čovjekovog truda i njegovog cilja da život učini što lakšim, što ugodnijim, što će omogućiti veće zadovoljstvo, ispunjenost i ličnu sreću. Ili kao što je veliki Hegel rekao: "Ljudsku istoriju pokreće sopstveni interes pojedinca."

To je zato što upotreba računarske tehnologije i informacionih sistema olakšava svakodnevni rad, štedi vreme, energiju, resurse, olakšava i unapređuje proces rada. Rad i korištenje informacionih sistema je potpuno jednostavan, praktičan, efiktivan i efikasan način rada. Ali, kao i u svakoj drugoj stvari, podrazumijeva se da u ovoj stvari nije sve savršeno. Naravno, ne može sve biti savršeno sa svih strana, što znači da i koriscenje kompjuterske tehnologije i sistema sa sobom nosi određene rizike, opasnosti i negativnosti. Takve opasnosti će biti minimizirane ili ih uopšte neće biti ako nisu izložene otvorenosti, odnosno ako se ne radi o otvorenom sistemu koji omogućava slobodan protok informacija, podataka, animacija.

Zapravo, otvorenost kompjuterskog sistema prema van i slobodan pristup bilo kom drugom računarskom sistemu koji se nalazi bilo gde u svetu čini ga lakom metom za napade, pretnje, opasnosti itd.

U njegovom funkcionisanju, od proizvodnje prvog računara do danas, u njegovom svakodnevnom unapređenju, čovek je istovremeno radio na njegovom unapređenju u smislu njegove sve veće delotvornosti, efikasnosti, primenljivosti i, istovremeno, njegove zaštite i bezbednosti.

Ali ono što čini čovječanstvo onim što je danas zapravo je njegova raznolikost. Dakle, danas ne možete pronaći dva identična živa bića koja će biti apsolutno identična po svojoj strukturi, sadržaju, DNK ili molekularnosti. To se prije svega odnosi na čovjeka i živa bića kojima je on svakodnevno okružen u svom okruženju, odnosno čovjek je živo biće, stvorenje prirode kao i sve ostalo. Otuda je sasvim logično misliti da se ne može očekivati od svake osobe na planeti da misli

[240] Huseinagić E., Modern Technologies To Improvement Business and Living Environment, Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024, Travnik, str. 188.

[241] Alić E, Ćosić M., Syber Security as a Business a Requirement (Process), Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024, Travnik, str. 177.

isto, da se ponaša isto, da teži istom cilju ili čak skoro isto kao i druga osoba u svom okruženju ili porodici, što znači da ne postoje dva identična čoveka na zemlji.

Dakle, određena kategorija ljudi će težiti pozitivnim ljudskim karakteristikama, odnosno težiti da budu pošteni, savjesni, moralni, istiniti, pošteni itd. Ali s druge strane, postoji još jedna kategorija ljudi koji zadiru i vrijeđaju slobodu, dostojanstvo i dušu druge osobe, vođeni mračnom stranom njihove ličnosti – žudnjom za moći, pohlepom, proždrljivošću itd. A takvo devijantno ponašanje ili zločin među pojedincima u svojim različitim oblicima prisutan je od samog stvaranja čovjeka, odnosno od kada je stvoreno njegovo izvorno lično vlasništvo, što znači da različitost karaktera ili zločina kod čovjeka nije nastala u posljednjih 20 godina, 30 ili 100 godina, naprotiv, različitost ljudskog karaktera ispoljava čovjeka od samog postojanja ljudskog bića.

Dakle, dok jedna kategorija ljudi nastoji da svoj život učini lakšim, jednostavnijim, praktičnijim kroz svakodnevno unapređenje svog rada kroz kompjutersku tehnologiju i sisteme, svojih ličnih koristi, profite i beneficije pa i na štetu druge savjesne i moralne grupe ljudi.

Tako su rad i dosadašnja iskustva ljudi u svijetu pokazali i dokazali da ni nikada a ni danas ne postoji 100% pouzdan i siguran računar od eksterne izloženosti rizicima, sajber napadima i prijetnjama. Činjenice koje idu u prilog ovoj tvrdnji je sama računarska tehnologija, odnosno paralelno sa razvojem i unapređenjem računarskih tehnologija razvijaju se i programi koji se odnose na zaštitu računarske tehnologije. Ali uprkos tome, smatra se da do danas nije ni izmišljen nit izgrađen 100% efikasan sistem mera odbrane i bezbednosti od sajber napada sajber kriminalaca kompanija, kao i ogromni gubici koje cyber kriminal stvara sada i uvijek, kako za kompanije tako i za pojedince koji troše milione dolara na sigurnost svojih sistema oštećene kompanije i osobe čiji su sistemi predmet napada uspješnih cyber kriminalaca, ali i o dojavama vlada moćnih i razvijenih zemalja, vojnih institucija u razvijenim zemljama institucije koje su i same organizovane za borbu protiv ove vrste sajber kriminala, moćne bankarske korporacije itd. koji svakodnevno pokazuju da su jednako ranjivi i nimalo pošteđeni za razliku od bilo kojeg drugog pravnog, fizičkog ili običnog korisnika običnog pametnog elektronskog uređaja.

1.SAJBER NAPADA I SAJBER KRIMINALCI - IZAZOVI

Danas, fakt je da se ne može izgraditi 100% efikasan sistem odbrambenih i sigurnosnih mjera od sajber napada sajber kriminalaca. Sama činjenica da imamo uređaj, odnosno računar koji je povezan na internet, znači da je naš računar "živ", što znači da je aktivan, što znači da je izložen spoljnim uticajima, što znači da je aktivna u svakom trenutku i opasnost od potencijalnih hakerskih napada, akcija, procesa bez obzira da li se na računaru nalaze interesantne informacije ili ne, da li je naša kompanija globalno uspješna ili ne, da li je lokalna kompanija, poznato ime, da li je poznata ličnost ili običan građanin, penzioner itd

Mora se znati da kako sto se sami kompjuterski sistemi usavrašavaju, tako i sajber virusa, koji su sve više ambizcioznije i sofisticiranije. U takvim uslovima javjla se kao nužna potreba da svaka kompanija i svaki građanin redovno vrši analizu rizika i reviziju bezbjednosti sitem preko poboljšavanje i to u odnosu:

- Povjerljivost informacija. Da bude dostupan samo onima koji imaju ovlašteni pristup traženim

podataka. Štiti tačnost i potpunost informacija i proces obrade informacija,

Samo ovlašteni korisnici imaju pristup podacima i drugim sistemskim uslugama potrebnim za

Pored razvoja čovječanstva, društva, država pa samim tim i same kompanije potvrđuju da nikada u istoriji čovječanstva, društvo ili kompanija nije imala toliki obim podataka kao danas. "Najnoviji trendovi u digitalizaciji i digitalnim vještinama, kružnoj ekonomiji, su aktuelne ekonomske teme u Jugoistočnoj Evropi. Savremeni poslovni svet je fokusiran ka promovisanju održljivog ekonomskog rasta koji će poboljšati mogućnosti za gradjane, firme i inostrane investitore."[242] Zapravo, danas informacija znači bogatstvo, znači moć. Ne govorimo o gigabajtima ili eksabajtima, govorimo o ogromnoj količini, odnosno bazi podataka razbacanoj po sistemima kompanije preko njenih data centara, podijeljenoj između fajlova, baza podataka, prostora za pohranu itd. Paradoks je veći jer veliki broj kompanija nije ni svestan osetljivosti podataka kojima raspolaže, a što je od neprocenjive vrednosti za samu kompaniju. Otuda proizilazi neophodna potreba koja se nameće za njihovu zaštitu i sigurnost. Opasnost koja se tiče podataka kojima raspolažu kompanije ili građani razvijenog društva odnosi se prije svega na osjetljivost samih podataka, odnosno na šta se odnose, kako se raspolažu, kako se dijele, ko im može pristupiti i koliki je rizik ili opasnost od njihovog izlaganja spolja.

U složenim kompanijama koje imaju ogromnu bazu podataka, nedostatak jasnog pregleda osjetljivih podataka dostupnih samoj kompaniji može zakomplikovati sistem mjera i primjenu efikasnih politika i kontrola za zaštitu ovih baza podataka. Imamo novi ekonomski model koji nema nikakvih marginalnih troškova koji će vrlo brzo postati pokretač snažnog ekonomskog rasta i otvaranja radnih mjesta.[243] Rizik eksterne izloženosti dostupnosti sopstvenih podataka kompanije je takođe tema koja bi trebalo da bude od posebnog značaja. Poslovni partneri, klijenti, pružaoci usluga i drugi saradnici s kojima se dijele podaci i informacije povećavaju rizik kompanije ne samo za povjerljivost podataka, kontrolu i neuspjele revizije cjelokupnog procesa, već i za kolateralnu štetu koja može nastati zbog kompanija uzrokovana povjerenjem zaposlenih u kompaniju, povjerenjem kupaca, vrijednošću brenda, štetom koja bi preduzeću nastala zbog oštećenja brenda kompanije itd. Opasnost koja vreba kompaniju zbog dostupnosti ogromne baze podataka proizlazi iz činjenice da je danas gotovo sva poslovna komunikacija gotovo elektronička. I nažalost, bas preku takvu izmazenu e-mail podataka i komunikacije, najlakši način je da IT sistem kompanije postane predmet SAJBER napada sa neprocenlivi finansijskim stetima i prodorom u elektronsku infrastrukturu kompanije.

Stručnjaci iz oblasti računarske tehnologije i zaštite, ali ne samo stručnjaci, već i svi visoki poslovni ljudi na visokim pozicijama u kompaniji ili društvu, poput menadžera, rukovodilaca, državnih službenika, slažu se da je gubitak podataka jedan od najvecih i najosjetljivija šteta koja može nastati u jednoj kompaniji ili entitetu.

[242] Georgievski G., Digitalization A Path for Successful Development of the Macedonian Economy, Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024, Travnik, str. 216.

[243] Degryse C., Digitalizacija ekonomije i njezin utjecaj na tržišta rada, Radni dokument 2016.02, Brussels, 2016, p. 6.

Potrebno je da se uzme u obzir činjenica da je opasnost od curenja ili gubitka podataka neizbježna. Zato svaka kompanija ili subjekt mora nastojati da unaprijedi svoj sistem zaštite podataka, posebno opasnosti koje se odnose na slučajno brisanje, zlonamjerno brisanje , hardverski kvarovi, sajber napadi, korupcija softvera, praznine u politikama na održavanju i bezbednosti sistemu, itd.

Istovremeno, rizik od curenja ili gubitka podataka nije prisutan samo u preduzećima, privrednim subjektima ili određenim državnim organima, rizik od gubitka ili curenja podataka i informacija je takođe vrlo osjetljiv, opasan i značajan za svakog građanina, bez obzira na sfere u kojoj posluju, na kojoj je poziciji ili koju funkciju obavlja u društvu, bez obzira da li je zaposlen u privatnom sektoru, državnom sektoru ili penzioner. Vješti sajber kriminalci (hakeri) vrlo lako mogu probiti sigurnosni prsten elektronskog sistema koji koristi običan građanin, bez obzira da li se radi o zaštiti korisničke e-mail adrese, lozinke itd. U takvim uslovima, oni su u stanju da iscrpe kompletan sadržaj kompjuterskog sistema kojim lice raspolaže, bez obzira da li se radi o običnom građaninu ili poslovnom čoveku.

Ukoliko je probijen zaštitni zid njegovih elektronskih računa, to znaci da je sajber kriminalac uspio doći do podataka o svim finansijskim sredstvima sa bankovnih računa, ličnih podataka, razmjene lične komunikacije, službene razmjene podataka, informacija, prepiske, poruka ili kontakata jedne osobe. službena e-mail adresa preduzetnika i sl. Štaviše, ako govorimo o ozbiljnom preduzetniku ili biznismenu, može se pretpostaviti šta bi se desilo kada bi svi njegovi zvanični podaci postali dostupni i rasplozlivi ljudima koji uspeju da hakuju njegovu e-mail adresu. U e-mail adresi ozbiljnog biznismena sigurno bi bilo bezbroj podataka i sadržaja o poslovnim ugovorima, e-mail kontaktima drugih poslovnih partnera, ugovorima i drugim osjetljivim podacima. Na ovaj način, biznismen čiji je elektronski sistem provaljen vrlo lako postaje žrtva sajber kriminalaca koji dalje vrlo lako počinju da raspolažu žrtvom upuštajući se u još jednu nezakonitu radnju, odnosno ucenjujući vlasnika raznim ucenama bilo za svote novca ili na principu povjerljivosti ili konspirativnosti pr. "Ako želite da ne otkrivamo razgovore ili prepisku, morat ćete platiti iznos novca u ovom iznosu, itd."

Ako je riječ o preduzetniku iz određene djelatnosti, pr. turizam, metalurgija itd. iscrpljivanjem njegovih poslovnih kontakata, odnosno e-mail adresa, može se desiti da za određenu novčanu nadoknadu oni postanu dostupni i mogu se prodati drugoj osobi iz istog biznisa (konkurencije) koja ima interes za takve kontakte, podatke, itd. Takođe, izvlačenjem sadržaja sa e-mail adrese, veoma je lako za poslovne partnere tj klijenti vlasnika e-mail adrese, da dalje postanu predmet ucjene i prijetnji u cilju sticanja određene koristi u zamjenu za diskreciju, tajnost i slično. Da ne govorimo o tome ako se radi o poslovnom čovjeku, političaru ili javnoj ličnosti koji je putem svoje e-mail adrese razmjenjivao lične, političke, poslovne, povjerljive, intimne ili bilo kakve osjetljive informacije i podatke. Probijanje zaštićenog zida do njegovih elektronskih računa znači da je istog trenutka postao žrtva otkupnine, što znači da sve dok željeno dobro nije nadoknađeno, bez obzira da li se radi o novčanom iznosu za otkupninu ili nekoj drugoj povjerljivoj stvari , to će istovremeno značiti i kompromitiranje i uništavanje njegove karijere, uništavanje njegovog ličnog autoriteta, dostojanstva, integriteta, ugleda, pa čak i života.

Ukoliko dođe do krađe ličnih podataka, odnosno krađe ličnih računa sa ličnim podacima, to može dovesti i do krađe ličnog identiteta, pa sa ukradenim identitetom, sajber kriminalci dalje otvaraju elektronske račune u bankama, vrše kupovinu/prodaju imovine, itd., a u zemljama u kojima su servisi za građane potpuno automatizovani, kriminalci sa ukradenim ličnim podacima drugih mogu da pribave lična dokumenta sa ličnim podacima, pasoše, a sa tako stečenim lažnim ličnim identitetom mogu dalje podižu i koriste kredite od banaka, za kupovinu skupih automobila, stanova i sl. i na taj način nanose finansijsku štetu žrtvi, pa čak i stvaraju krivični dosije. Žrtva, u većini slučajeva, neće znati da se njen identitet „koristi" sve dok ne stignu „računi za naplatu".

2.KAKO DA SE ZAŠTITIMO!

Istraživanja pokazuju da više od 20% malih i srednjih preduzeća posluje bez pravljenja rezervne kopije svojih podataka, zato sto je i upravljanje sigurnosnom kopijom podataka veoma važna stvar, pa tako 50% kompanija je na mišljenja da njihov oporavak prikupljenih podataka ne uspijeva zbog lošeg upravljanja sigurnosnom kopijom. Dobar dio zaposlenih ljudi u kompaniji nije dovoljno obrazovan da zna da pravljenje rezervne kopije najvažnijih vitalnih podataka nije komplikovan proces, jer su dani ručnog pravljenja rezervnih kopija davno prošli. Danas se može birati između mnoštva komercijalno dostupnih rješenja za sigurnosnu kopiju sistema kako bi se zaštitio integritet i sigurnost povjerljivih podataka kompanije. Utvrđeno je nekoliko principa ili savjeta na najlakši način za zaštitu važnih podataka.

1. Primjena principa 3-2-1

Da biste definirali na šta treba napraviti sigurnosnu kopiju, poštujući pravilo 3-2-1, znaci zadržati najmanje 3 sigurnosne kopije na 2 različita medija, od kojih jedan ne bi trebao biti lociran lokalno.

2. Dislocirano cuvanje rezervnih kopija

U skladu sa pravilom 3-2-1, najmanje jedna rezervna kopija mora biti raspoređena t.j. dislocirana. Ako je vaša primarna sigurnosna kopija na licu mjesta ugrožena, možete se vratiti na održivu opciju vraćanja, i nije važno da li se koristi fizička ili pohrana u oblaku, najvažnije je da sigurnosne kopije budu netaknute.

3. Izvođenje dodatne sigurnosne kopije (backup)

Skladišni prostor obično čini veliki dio budžeta. Stoga, umjesto kopiranja cijelog skupa podataka u svakom ciklusu sigurnosne kopije, mogu se kopirati samo podaci koji su se promijenili od prethodne sigurnosne kopije. Ovo ne samo da štedi prostor za skladištenje, već i vrijeme.

4. Provjera t.j. potvrdu sigurnosnih kopija

Sigurnosna kopija podataka je dobra onoliko koliko su dobre mogućnosti vraćanja koje pruža, šta znači da nema apsolutno nikakve potrebe za čuvanjem beskorisnih sigurnosnih kopija. Stoga trebalo bi pronaći rješenje za zaštitu podataka koje podržava automatsku verifikaciju sigurnosne kopije.

5. Šifrirajte sigurnosne kopije

Šifrirajte sigurnosne kopije kako biste spriječili neovlašteni pristup najvažnijim vitalnim podacima. Budući da je svrha enkripcije podataka sigurnost podataka, provjerite da li se koristi AES 256 – standard šifriranja, univerzalno priznati standard za njegovu sigurnost. Šifriranjem sigurnosnih kopija u radu i mirovanju, to znači da im niko ne može pristupiti bez dozvole.

6. Automatizirajte rutine izrade sigurnosnih kopija

Redovno pravite rezervne kopije. Najbolje je ovu opciju automatizirati. Ovo će uštedjeti vrijeme i povećati učinkovitost sigurnosne kopije. To će također izbjeći rizik od pojave grešaka prilikom ručne zaštite podataka. Kod ove opcije potrebno je provjeriti da li su i kućni elektronski uređaji koje zaposleni donose u kancelariju također redovno rezervisani. Da bi se greške svele na najmanju moguću mjeru, sigurnosne kopije treba raditi bez uključivanja zaposlenih, uz minimalno opterećenje resursa njihovih uređaja.

7. Pristup sigurnosnoj kopiji treba kontrolisati

Neophodno je imati različite nivoe ograničenog pristupa rezervnim kopijama. Jer nisu svi u kompaniji odgovorni za aktivnosti vezane za zaštitu podataka. Najlakši način da se eliminiše neovlašćeni pristup je implementacija rezervnih kopija kontrole pristupa, čime će biti znatno olakšano praćenje kome i kada treba pristup resursima i aktivnosti zaštite podataka.

8. Saradnja sa kompetentnim partnerima

Saradnja sa kompetentnim partnerima koji imaju tim stručnjaka za IT bezbednost priznatih na domaćem i inostranom tržištu može značajno unaprediti sajber bezbednost. Ovi stručnjaci ili konsultanti pomažu organizacijama koje nemaju interne resurse za punu zaštitu.

Opste principi sajber bezbednosti

-Instalirajte dobru zaštitu na svim krajnjim tačkama u mreži (uključujući pametne telefone);
- Mreža treba da bude dobro opremljena sa konfigurisanim zaštitnim zidovima.
- Osim antivirusnih programa, potrebno je pronaći i primijeniti druge moćne alate za lov na prijetnje i napade na elektronske sisteme i mrežu.
- Instalirati SIEM sistema (Softver za upravljanje sigurnosnim informacijama i događajima) posebno za veće kompanije. SIEM sistem poboljšava otkrivanje prijetnji, usklađenost i upravljanje sigurnosnim rizicima i incidentima kontinuirana obuka zaposlenih o opasnostima od cyber napada i sigurnosti uz interaktivne sesije.

Pored program koji nude određeni nivo sigurnosti ili zaštite računarskih sistema u velikim kompanijama, uspostavljen je niz principa kojih se zaposleni i korisnici pametnih uređaja trebaju pridržavati kako ne bi postali žrtva sajber napada ili prevare kao što su kao phishing napad, društveni inženjering, ransomware, zlonamjerni softver, itd. Primjer uobičajenih znakova koji ukazuju da se radi o phishing napadu i na koje biste trebali obratiti posebnu pažnju je sljedeći:

-U međusobnoj elektronskoj komunikaciji koja se redovno odvija između nalogodavaca, iznenada se ukazuje "hitnost" za izvršenje određene uplate od strane nalogodavca (što se inače nikada ranije nije koristilo kao indikacija) uz izgovore da je to zbog obaveza plaćanja prema državnim institucijama, dobavljačima itd.

-Maskiranjem poruke kao da ju je poslao prethodno poznati kontakt, direktor, nadređeni itd. napadač zahtijeva hitno plaćanje priložene fakture, čime se krši standardni redosled uobičajenog svakodnevnog operacija. Dobro poznavanje internih procedura u tekućem izvršavanju radnih zadataka i aktivnosti u kompaniji, može umnogome pomoći da lakše prepoznate phishing napade i postupite u skladu s tim.

- Obavijest klijenta o promjeni podataka kompanije, odnosno navodnoj promjeni u banci, transakcijskom računu za plaćanje i sl. Slanje određene poruke, (phishing) veze ili određenog priloga poruke putem e-pošte, pri čemu svako namjerno ili nenamjerno klikanje na link iz phishing poruke može sadržavati virus koji ima za cilj da zarazi računalo kako bi dalje bio podložan ucjena ili ponovno iscrpljivanje ličnih podataka kompanije ili korisnika itd. U takvim slučajevima, najvažnije je adekvatno reagovati, odnosno odmah prijaviti grešku kompaniji i nadređenom ili osobi koja održava IT sisteme kako bi se odmah reagovalo kako bi se izbjegla pojava dodatne štete.

3.PRINCIPI ZA SAJBER ZAŠTITA

Za veću zaštitu pri radu s elektronskom poštom, preporučuje se pridržavanje sljedećih principa:

- Ako je e-mail primljen sa nepoznate e-mail adrese. - adresa ili nepoznati pošiljalac, čak i ako ima odgovarajuću temu ili sadržaj, ne otvarajte priloge, ne klikajte na web linkove na koje vas usmjeravaju i ne postupajte po zahtjevima koji ih sadrže, u smislu navođenje podataka, prilaganje dokumenata itd.
- Nemojte otvarati priloge i web veze u porukama koje se automatski karakteriziraju kao neželjene ili bezvrijedne poruke.
- Ukoliko poruka sadrži web link (web link) na web stranicu, preporučljivo je kontaktirati pošiljatelja poruke kako biste potvrdili sigurnost navedene web stranice,
- Pažljivo provjerite sadržaj e-maila i primaoca e-pošte.
- Nemojte koristiti privatne elektronske adrese za razmjenu službenih dokumenata. Sajber kriminalci koriste nekoliko različitih načina ili oblika putem kojih pokušavaju da prodru u aktivni kompjuterski sistem kako bi dalje izvukli ono što im je potrebno.

Prilikom napada socijalnog inženjeringa, sajber kriminalci dolaze do raznih poruka s najrazličitijim sadržajem koje šalju ili putem društvenih mreža ili putem službenih e-mailova institucija krajnjim korisnicima kompjuterskih sistema kako bi ih namamili da otvore poslati link i na taj način ga zaraziti. Posebno je važno znati da je svaki računar samo mašina ili uređaj i da sigurnost i otpornost na eksterne sajber napade zavise prvenstveno od ličnih radnji korisnika u konkretnim situacijama i od znanja i edukacije u korišćenju računarskih sistema. Za postizanje određene pouzdanosti računarskih sistema i adekvatne efikasne zaštite potrebno je veliko znanje i iskustvo, nadogradnja i stalna edukacija.

– Uvijek instalirajte i koristite antivirusne programe.

Danas postoji mnogo proizvođača takvih programa ili softvera, a neki od njih čak nude i besplatnu verziju svog proizvoda kako bi pružili osnovnu zaštitu od kompjuterskih virusa. Antivirusni softver je veoma važan za sigurnost računara i preporučljivo je da ga nadogradite najnovijim definicijama čim postanu dostupne. Poželjno je skeniranje cijelog kompjutera barem jednom mjesečno ako češće nije moguće zbog preopterećenosti poslom, obaveza i sl.
– Periodično nadogradite softver, Različite aplikacije koje svakodnevno koristimo konstantno otkrivaju određene sigurnosne rupe koje su od velike važnosti za sigurnost računarskog sistema, te je stoga potrebno stalno nadograđivati softver koji koristimo najnovijim stabilnim verzijama kako bismo bili zaštićeni od najnovije pretnje.

– Budite oprezni kada instalirate ili preuzimate određene programe. Opšte je poznato da se putem interneta mogu pronaći i pristupiti svim vrstama programa, slika, filmova, muzike i još mnogo toga. Ali vrlo često preuzeta datoteka može biti obična zamka, odnosno nije ono što tražimo ili očekujemo, već virus ili program sa zlonamjernim kodom koji sadrži samo ime tražene datoteke.

– obratiti pažnju i biti posebno oprezan kada čitate e-poštu i otvarate datoteke. E-pošta je, zbog svoje jednostavne primjene, jedan od najpopularnijih načina komunikacije među ljudima, te je upravo zbog toga u posljednje vrijeme sve više koriste sajber kriminalci za postizanje svojih ciljeva kroz razne lažne oblike.

– Koristite dobru, jaku lozinku. Kad god koristite bilo koju uslugu koja sadrži lozinku, potrebno je kreirati jaku lozinku koju bi mogao znati samo kreator. Obično napadači imaju različite vrste načina (obrasca) kako bi provalili lozinku. Posebno je važno koristiti sigurnu jaku lozinku koja će biti mješavina slova, brojeva i simbola, a još je važnije ne koristiti istu lozinku za više registracija. Pokušajte da koristite jednu lozinku za jednu registraciju i uvek, kada instalirate novi hardver ili softver koji zahteva lozinku za pristup, promenite podrazumevanu lozinku.

- Koristite zaštitni zid Firewall je računalni program koji djeluje kao čuvar računala, odnosno prati dvosmjerni mrežni promet i, ako je ispravno postavljen, detaljno ispituje promet i utvrđuje da li je legitiman ili ne, dozvoljavajući ili odbijajući pristup u sistem ili iz njega. Da bi sve ovo postigao, zaštitni zid nadgleda svaki paket koji se primi i pošalje sa vašeg računara. Postoje različite verzije zaštitnih zidova, neki su čak i ponuđeni i mogu se instalirati besplatno.

- Nikada ne odgovarajte na neželjene poruke.

- Ne otkrivajte tajne na internetu

Držite svoje lične podatke van interneta – posebno adresu, broj telefona i fotografije – što je više moguće. Budite sigurni da sve fotografije koje objavite imaju geografske oznake i da dokumenti ne sadrže privatne podatke.
-Provjerite postavke računa na društvenim mrežama.

Preporučujemo da odaberete stroga podešavanja privatnosti na društvenim mrežama i uslugama koje koristite, da profile ostavite otvorene samo za prijatelje i redovno pratite listu prijatelja,

- Igrajte pametno s računima trećih stran,

Ako je moguće, izbjegavajte prijavljivanje na web stranice koristeći društvenu mrežu ili druge račune koji sadrže vaše stvarne podatke. Povezivanje jednog naloga s drugim olakšava praćenje vaših aktivnosti na mreži, na primjer povezivanjem komentara sa svojim imenom. Da biste riješili problem, zadržite najmanje dva računa e-pošte, rezervirajte jedan za svoje račune sa pravim imenom, a drugi za web stranice na kojima želite da ostanete anonimni.

ZAKLJUČAK

Treba naglasiti da je sajber sigurnost, u suštini, ključna za očuvanje stabilnosti, integriteta i sigurnosti u digitalnom okruženju u kojoj funkcionišu sva društva. Ulaganje u sajber sigurnost nije poslovna ili društvena obaveza, već imperativ svakog pojedinca u očuvanju ličnog integriteta, autoriteta, privatnosti kao i u održavanju konkurentnosti, povjerenja i održivi razvoj kompanija u digitalnom dobu u kojem svijet danas funkcionise.

LITERATURA

1.Degryse C., Digitalizacija ekonomije i njezin utjecaj na tržišta rada, Radni dokument 2016.02, Brussels, 2016.
2.The Open Society, Technology and the future of work: the state of the debate, travanj 2015, p. 10.https://www.opensocietyfoundations.org/publications/technology-and-future-work-statedebate Pelle B. Entre contrôle et confiance: la géolocalisation, un risque pour
3. Национална канцеларија за бродбенд компетентност, Методологија за утврдување на индекс на дигитална економија и општество, Скопје, 2022 година
4.Spremić M., Digitalna transformacija poslovanja. Zagreb: Svečilišna tiskara d.o.o, 2017 godina

5. Huseinagić E., Modern Technologies To Improvement Business and Living Environment, Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024.

6.Alić E, Ćosić M., Syber Security as a Business a Requirement (Process), Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024.

7.Georgievski G., Digitalization A Path for Successful Development of the Macedonian Economy, Proceedings of International University Travnik in Travnik, XXVII International Conference: With Digitalization, Automation and Artificial Intelligence to more Efficient Work and Business in the Future, 17-18.05.2024.