SAJBER (CYBER) BEZBJEDNOST - PRIJETNJE I ZAŠTITA SAJBER (CYBER) BEZBJEDNOST – ZAŠTITA / CYBER SECURITY CYBER SECURITY - THREATS AND PROTECTION CYBER SECURITY - PROTECTION

Dr Vlado Jovanić[1], Glavni inspektor, Zamjenik načelnika, Ma Boris Tušinski[2],
[1]Uprava za policijsku podršku, MUP RS, Jug Bogdana 108, 78 000 Banja Luka, Republika Srpska,
[2]OSA/OBA Bosna i Hercegovina
e-mail: vlado.jovanic@hotmail.com, vlado.jovanic@gmail.com
boris.tusinski@gmail.com

Pregledni članak
https://www.doi.org/10.58952/zr20251403380
UDK / UDC 004:343.4:004.056.5

Sažetak

Sajber (cyber) bezbjednost u trenutnim globalnim odnosima razmjene podataka i informacija putem IKT (informaciono komunikacione tehnologije) predstavlja određeno stanje koje treba da garantuje svaki dvostrani oblik zaštite od sajber napada u razmjeni podataka na bazi komunikacijskh platformami koje se koriste u razmjeni. Ova vrsta bezbjednosti podrazumijeva određenu praksu i potrebu poslovnog subjekta kojom se štite informacije (digitalne informacije) u smislu ljudskih (lični podaci i kredencijali), infrastrukturnih (objekti i poslovno okruženje), procesnih (odvijanje proizvodnih procesa i procedura) i tehničko-tehnoloških (uređaji i oprema za skladištenje, razmjenu i zaštitu informacija) resursa. Svaki propust, namjerni ili slučajni (softverski, hardverski ili ljudski) može dovesti do bezbjednosnog upada-proboja i kontaminiranja sistema sa nesagledivim posljedicama i štetom. Za efikasnu prevenciju i suprotstavljanje sajber napadima i VTK neophodno je da svi korisnici IKT ulože maksimalan napor i sredstva u bezbjednosnu zaštitu sistema i okruženja u kojem posluju implementirajući najbolji i najefikasniji sistem zaštite koji se trenutno nudi na tržištu. U radu ćemo analizirati neke najčešće sajber prijetnje-napade na tredicionalne sisteme- platforme bezbjednosne zaštite (članak: Sajber bezbjednost-prijetnje) ljudskih, materijalno tehničkih, infrastrukturnih i finansijskih resursa i predložiti poboljšanje, odnosno najbolji sistem zaštite kako bi se izbjegli potencijalni napadi i eventualne intervencije (članak: Sajber bezbjednost- zaštita).

Ključne riječi: *sajber (cyber) bezbjednost, sajber prijetnje-napadi, analiza tradicionalnih sistema-platformi zaštite, prijedlog za poboljšanje, najbolji sistem zaštite.*
JEL Klasifikacija: K14, K24, K40, K42

Abstract

Cyber security in the current global relations of data and information exchange through ICT (information communication technology) represents a certain condition that should guarantee any two-sided form of protection against Cyber Attacks in the exchange of data based on the communication platforms used in the exchange. This type of security implies a certain practice and the need of a business entity to protect information (digital information) in terms of human (personal data and credentials), infrastructural (facilities and business environment), procedural (manufacturing processes and procedures) and technical-technological (devices and equipment for storing, exchanging and protecting information) resources. Any omission, intentional or accidental (software, hardware or human) can lead to a security intrusion-breakthrough and contamination of the system with incalculable consequences and damage. For effective prevention and countering of Cyber Attacks and VTK, it is necessary that all ICT users invest maximum effort and resources in the security protection of the system and environment in which they operate by implementing the best and most effective protection system currently offered on the market. In the paper, we will analyze some of the most common cyber threats-attacks on traditional systems-platforms of security protection (article: Cyber security-threats) of human, material, technical, infrastructural and financial resources and propose an improvement, that is, the best protection system in order to avoid potential attacks and eventual interventions (article: Cyber security-protection).

Keywords*: cyber (cyber) security, cyber threats-attacks, analysis of traditional protection systems-platforms, proposal for improvement, best protection system.*

UVOD

Vrijeme u kojem živimo pretpostavlja veoma brzo prilagođavanje bezbjednosnim trendovima prijetnji sajber (cyber) napadima na dnevnom nivou. Svaki novi dan predstavlja u bezbjednosnom smislu novi izazov za bezbjednost poslovne infrastrukture i njen menadžment. Sa druge strane, bezbjednosne strukture društva koje štite društvo od svih oblika ugrožavanja i zakonodavac kao autoritet koji kroz kreiranje pravnih okvira u materijalnom (inkriminacija određenih ponašanja u vidu krivičnih djela iz oblasti visokotehnološkog kriminaliteta) i procesnom smislu (procedure za sprječavanje, dokumentovanje i dokazivanje krivičnih djela) to omogućava, imaju takođe obavezu da u pogledu sajber bezbjednosti i zaštite iz svog domena rada prate bezbjednosne trendove i djeluju proaktivno, preventivno i u krajnjem slučaju represivno. Od vizije, fleksibilnosti i spremnosti upravljačke strukture za bezbjednosne promjene u poslovnom subjektu, bezbjednosnom razmišljanju, aktivnostima i prihvatanju novih trendova, posebno u tehnološkom pogledu omogućit će i bezbjedan rad i održiv opstanak djelatnosti u poslovnom subjektu a takođe i olakšati rad bezbjednosnim strukturama na identifikaciji i otkrivanju bezbjednosnih prijetnji i izvršilaca. Upravljanje i vođenje segmenta sajber (cyber) bezbjednosti u poslovnom subjektu zahtijeva prilagodljivost, izgradnju povjerenja i visok stepen razvijene bezbjednosne samosvijesti svih zaposlenih. Za uspostavu visokog nivoa karakteristika kvaliteta u pogledu sajber (cyber) bezbjednosti, rukovodioci i menadžeri moraju upravljati okruženjima visokog stresa i inspirisati timove koje vode u poslovnom subjektu na podizanju bezbjednosne kulture. Pored navedenog za viši nivo bezbjednosti neophodna je i uvezanost poslovnih subjekata sa bezbjednosnim stukturama u pogledu saradnje i razvijanja mehanizama zaštite i brzog reagovanja u kriznim situacijama. Ovo je svakako imperativ a dobre prakse u javno-privatnom partnerstvu to i dokazuju. Bezbjednost nije povlastica i nema alternativu, a ukoliko izostane u bilo kojem segmentu sistema ugrozit će sve aktere sistema.

Visokotehnološki-sajber (Cyber) kriminalitet kao tekovina globalnog tehnološkog razvoja postaje sve izraženiji. U principu žrtva može biti bilo ko, pojedinac kao korisnik interneta ili drugih digitalnih usluga (elektronsko-digitalno plaćanje usluga) ili neka organizaciona strukturakompanija koja koristi internet za obavljanje poslova iz svoje nadležnosti kroz povezivanje sa drugim strukturama ili pojedincima za pružanje usluga ili razmjenu informacija. Institucije sa visokim stepenom rizika za napad su bezbjednosne institucije (vojska ili policija), namjenska industrija, strukture koje se bave određenim poslovima od opšteg-javnog interesa (obrazovne institucije, finasnsijske institucije, energetske kompanije, telekomunikacioni sistemi, sistemi za snabdjevanje vodom, fabrike za različite segmente proizvodnje....). Za sve navedene učesnike u digitalnom saobraćaju (fizička ili pravna lica) zajednička preporuka je da se svi moraju pridržavati određenih bezbjednosnih protokola u komunikaciji kako bi se zaštitili od napada i eventualne štete. Praktično to znači da na internet ne treba upisivati lične podatke, postavljati lične i porodične fotografije, ne treba pristupati neprovjerenim sajtovima (nepoznate i neprovjerene IP adrese), izbjegavati online kupovinu (koristiti samo provjerene i preporučene dobavljače). Predmet napada VTK su svi aspekti digitalnih aktivnosti u sajber (Cyber) prostoru: krađa identiteta putem interneta, krađa podataka-kredencijala o transakcionim računima sa bankovnih i kreditnih kartica, zloupotreba i krađa korisničkih naloga, neovlašteni pristup nezaštićenom računaru. Svaka žrtva, u principu, kao i kod svih drugih djela, je djelimično doprinijela izvršenju krivičnog djela kojim je oštećena svojom nepažnjom u korištenju IKT.

Da ne bi dolazilo do krivičnih djela neophodno je da se svaki korisnik (fizičko ili pravno lice) upozna sa određenim mjerama i protokolima zaštite i da pronađe i implementira one bezbjednosne mehanizme i sistem koji su za njega s obzirom na poslove i okruženje u kojem te poslove obavlja najoptimalniji.[263]

1. SAJBER (CYBER) BEZBJEDNOST – ZAŠTITA

1.1.ANALIZA BEZBJEDNOSNIH PLATFORMI ZA RAZMJENU PODATAKA

Kvalitetan i funkcionalan sistem bezbjednosti se ne zasniva na složenim bezbjednosnim rješenjima i postavkama već na poštovanju i pravilnoj primjeni uspostavljenih bezbjednosnih mjera i mehanizama u kontinuitetu. U današnjem brzo promenljivom bezbjednosnom okruženju, zaštita ljudi, imovine i infrastrukture zahtjeva slojevit pristup. Ekspanzija rada na daljinu i korištenje interneta ili drugih mreža i sistema (internih ili eksternih mreža) u standardnom obavljanju poslova postavio je korisnike (fizičke i pravne subjekte) u položaj ranjivosti i od veoma malih bezbjednosnih propusta zaposlenih koji mogu dovesti do velikih finansijakih šteta ali i šteta po ugled organizacije u poslovnom svijetu. Ovo postavlja temelje bezbjednosne zaštite od ljudskih grešaka u interakciji razmjene informacija kako unutar same strukture i zaposlenih tako i od vanjskih napada. Digitalno doba u kojem živimo i radimo podrazumijeva da su informacije ekvivalent oređene materijalne vrijednosti i stoga je u razmjeni tih informacija potrebno koristiti bezbjedne platforme i aplikacije za dijeljenje i razmjenu. Naravno, zaštita ne treba da ograniči ili uspori saradnju i razmjenu informacija, već da ih maksimalno zaštiti, omogućavajući pristup datotekama i podacima i korisnicima na udaljenim lokacijama putem određenih konekcija koje su potpuno bezbjedne i zaštićene. Međutim, porast razmjene informacija putem IKT i sistema kao standardni način komunikacije i saradnje na daljinu doveo je i do razvoja sajber prijetnji i krivičnih djela koji egzistiraju na ranjivostima upravo platformi za razmjenu i dijeljenje datoteka, bez obzira koje mehanizme ili alate koriste ugroženi entiteti (alati i mehanizmi bazirani na oblaku ili hostovani alati) napadači i dalje pokušavaju penetrirati u platforme i aplikacije za razmjenu podataka ili u same baze podataka. Kako bi se postavio adekvatan sistem zaštite od sajber napada neophodno je izvršiti analizu, odnosno sagledati i ukratko se osvrnuti na bezbjednosnu ranjivost i rizike za efikasnu zaštitu podataka trenutno popularnih aplikacija i platformi za razmjenu podataka (interno ili eksterno dijeljenje) koje su bazirane na oblaku ili hostovani (Dropbox, OneDrive, WeTransfer, SherePoint, MOVEit). Suština bezbjednosti navedenih platformi je u sistemu i lokaciji enkripcije i dekripcije podataka.

Dropbox

Dropbox platforma koristi enkripciju za podatke u transferu-tranzitu prilikom same razmjene i za podatke koji se ne razmjenjuju. To praktično znači da se Dropbox uslugom moraju dekriptovati traženi podaci za razmjenu na serverima kako bi se omogućio pristup korisniku, ali isto tako se omogućava i drugima koji imaju pristup Dropbox serverima da pristupe ili ostvare uvid u podatke koje traži udaljeni korisnik. Pored zaposlenih na Dropbox platformama pristup podacima u ovakvim situacijama mogu imati i potencijalni sajber napadači.

[263] Jovanić, V.: Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta, Doktorska disertacija, Travnik, 2024., strana 156.

OneDrive

Ova platforma za razmjenu podataka koristi isti sigurnosni pristup kao i Dropbox. Podaci korisnika se dekriptuju na serverima provajdera a nakon toga se razmjenjuju sa korisnikom. I kod ove platforme se potencijalno stvara ista vrsta ranjivosti kao i mogućnost za zlonamjerno presretanje kao i kod Dropbox platforme.

SharePoint

Kao još jedan Mikrosoftov (Microsoft) proizvod, i ova platforma je dizajnirana za korištenje u kompanijama koje se bave određenim poslovima. Međutim, sa bazbjednosnog aspekta i ona kao i predhodne dvije platforme koristi isti pristup u pogledu bezbjednosne ranjivosti kod razmjene podataka sa korisnikom, jer svako ko ima pristup SharePoint serverima ima pristup i podacima korisnika.

WeTransfer

Bezbjednosno korištenje ove platforme za razmjenu podataka je sličan kao i kod Dropbox-u i OneDrive platforme. U kontekstu stepena i mogućnosti bezbjednosne ranjivosti, WeTransfer platforma se smatra manje sigurnom od navedenih rješenja zbog nižeg nivo nadzora i nadogradnje u poslovnim strukturama koje koriste ovu vrstu zaštite.

MOVEit

Predstavlja softver koji se koristi za prenos i razmjenu datoteka i uglavnom ga koriste neke velike globalne kompanije. Kao jedinstveno, odnosno samostalno rješenje u konkretnoj kompaniji, predpostavlja obezbjeđenje kontinuiteta instaliranja i ažuriranja softvera.

Analizirajući navedene platforme kao uobičajene i standardne sistemske bezbjednosne mjere i mehanizme, njihov način rada i efikasnost, odnosno bezbjednosnu ranjivost, jasno je da ne postoji siguran i potpun način zaštite. Bezbjednost se mora sagledavati sa dva aspekta, sa unutrašnje (interne) bezbjednosti i zaštite unutar poslovne strukture i sa vanjskog (eksternog) uticaja na bezbjednost, odnosno svih vrsta ugrožavanja izvan poslovne strukture. Dakle, bezbjednost nije samo jedan zatvoreni perimetar, već sloj prstenova perimetara zaštite (fizička, infrastrukturna, sistemska, korisnička...) koje čine jedan zatvoreni krug kao kompaktnu strukturu koja je otporna na unutrašnje i vanjske bezbjednosne prijetnje i ranjivosti ali omogućava brzu i efikasnu razmjenu podataka i informacija.

1.2. MOGUĆA BEZBJEDNOSNA RJEŠENJA

Da bi smo neku tehnologiju prihvatili kao bezbjednu za korištenje po dizajnu, mjere zaštite podataka i bezbjednosni mehanizmi moraju biti integrisani u sistem od samog početka, dakle ne kao nekakav dodatak ili naknadno rješenje i razmišljanje već protkano u osnovi konstrukcije same platforme. Tehnologije koje ispunjavaju navedene bezbjednosne uslove daju prioritet vitalnim bezbjednosnim karakteristikama kao što su end-to-end (s kraja na kraj) enkripcija, kontrola pristupa (logovanje), mehanizmi provjere autentičnosti i kontinuirana bezbjednosna ažuriranja. Implementacijom ovog nivoa bezbjednosti u samu strukturu tehnoloških rješenja, poslovni subjekti (kompanije) mogu uspostaviti mnogo veću i snažniju osnovu za zaštitu svojih podataka unutar bezbjednosnog okvira usmjerenog na podatke i interno i eksterno. Iako se poslovni subjekti uglavnom fokusiraju na vanjske (eksterne) bezbjednosne prijetnje i ranjivosti, u realnim poslovnim okruženjima interne bezbjednosne prijetnje i ranjivosti predstavljaju najmanje isti rizik.

Sigurne platforme zasnovana na oblaku (*Cloud*) posebno su dizajnirane da spriječe curenje podataka uzrokovano ljudskim greškama i propustima unutar poslovne strukture. Bazbjednosna zaštita bazirana na platformi oblaka (*Cloud)* sa sinhronizacijom opterećenja u eksploataciji nisu samo luksuzni parametri sistema, već osnovne bezbjednosne pretpostavke i potreba. U tom kontekstu bezbjednosni mehanizmi koji provjereno funkcionišu su:

- End-to-end (s kraja na kraj) enkripcija za sve podatke sa bezbjednosnom klasifikacijom: osjetljivi-važni podaci,
- Kontinuirana bezbjednosna edukacija (podizanje nivoa bezbjednosne svijesti) za sve zaposlene (bez izuzetka),
- Implementacija visoko automatizovanih alata za detekciju i eliminaciju bezbjednosnih prijetnji i ranjivosti,
- Kontinuirana kontrola, praćenje i nadogradnja implementirang sistema zaštite (uspješni bezbjednosni napadi koriste osnovne bezbjednosne propuste).

Shodno navedenom, zaštita podataka unutar poslovne strukture treba da podrazumijeva sljedeće principe:

Segmentna kontrola pristupa: isporučioci podataka u razmjeni mogu u svakom trenutku opozvati pristup datotekama ili ograničiti dozvole za isoruku i pristup podacima korisniku kako bi eliminisali ili smanjili utjecaj ljudske greške na bezbjednost razmjene i pristupa.

Zero-Trust (nulto povjerenje): pristup podacima, osjetljivim datotekama i njihova razmjena na platformi je omogućena samo ovlaštenim i autentificiranim korisnicima za koje je kod pristupa izvršena slojevita provjera.

Nulto povjerenje u bezbjednosnom kontekstu doslovno znači da se ne vjeruje nikome i da se svi korisnici i sve aktivnosti bezuslovno provjeravaju. Ovaj model definitivno treba da promjeni standardne načine razmišljanja u pogledu sajber i svake druge bezbjednosti u poslovanju. Ovakav pristup podrazumijeva da je potrebno zauzeti principijelan stav da se nikome unutar ili izvan mreža koje se koriste ne treba vjerovati po predhodnim provjerama i po automatizmu. Nakon svakog izlaska sa mreže i svaki novi pristup mreži i podacima nakon toga, bez obzira na predhodnu provjeru zahtijeva novu provjeru i bez obzira koliko to često bilo u toku radnog vremena. Ultimativno svaki korisnik mora biti potpuno (autentificiran) provjeren, a svaki zahtjev mora biti ovlašten. U kontekstu navedenog i svaka komunikacija mora biti enkriptovana. Potpuno i kontinuirano provjeravajnje korisnika, uređaja i sistema, osigurava da samo korisnici sa bezbjednosno validnom dozvolom mogu pristupiti mreži i osjetljivim podacima. Pristup „Nulto povjerenje“ (Zero Trust) je posebno interesantan i koristan za poslovne strukture sa velikim brojem procesa, informacija i podataka od velikog bezbjednosnog i materijalnog značaja. Provođenjem „pristupa s najmanjim privilegijama“, minimizira se rizik od bezbjednosnih proboja kroz kontinuirane provjere autentičnosti svih segmenata pristupa, što onemogućava i horizontalno kretanje napadača unutar kontaminirane mreže. Bez obzira što ovaj model zaštite zahtijeva značajna finansijska i druga ulaganja, od suštinskog značaja za zaštitu najosjetljivijih podataka je i to što obezbjeđuje jednostavnu i potpunu harmonizaciju (usklađenost) sa propisima za učešće u poslovanju sa drugim poslovnim subjektima.

Arhitektura-bezbjednost bez znanja (Zero Knowledge): podrazumijeva da neovlašteni i neautorizovani korisnici ne mogu pristupiti bazama podataka i datotekama, uključujući i isporučioca platforme za razmjenu.

Ovakav pristup kod razmjene podataka omogućava, pored veće bezbjednosti u radu, i podizanje nivoa eliminacije i otpornosti na greške u razmjeni. Međutim i pored mjera zaštite koje koriste pojedine platforme i aplikacije za razmjenu podataka, glavni problem i ograničenje predstavlja sistemska postavka u platformi prema kojoj se podaci moraju dekriptovati na serverima isporučioca podataka i u dekriptovanom modu dostaviti korisniku. Bezbjednosni princip „arhitektura-bezbjednost bez znanja“ osigurava da se podaci ne mogu dekriptovati na serverima isporučioca, a to predpostavlja princip prema kojem je isključivo vlasniku i kreatoru podataka omogućeno dekriptovanje. Bezbjednosni pristup na ovakvom principu garantuje najviši stepen bezbjednosti i zaštite podataka i daje dodatne mogućnosti u vidu potpune kontrole eksploatacije i vidljivosti krajnjeg korisnika, odnosno to podrazumijeva: - Garantovanje visokog stepena zaštite privatnosti - zaštita i sigurnost podataka egzistira i u situacijama kada su usluge provajdera ugrožene sajber napadom.

- Potpuna eliminacija ili minimiziranje unutrašnjih (insajderskih) prijetnji - pristup podacima je pod stalnom i potpunom kontrolom eksploatacije i vidljivosti.
- Mogućnost harmonizacije i usklađenosti - harmonizacija i usklađenost sa važećim propisima o zaštiti ličnih i tajnih podataka, krivičnim i krivičnoprocesnim zakonom kao i drugim propisima koji regulišu oblast razmjene informacija i postupanje pravnih subjekata koji učestvuju u pravnom saobraćaju putem IKT.

Model „bezbjednost bez znanja“ predstavlja nadogradnju, odnosno sljedeći nivo zaštite podataka u odnosu na predhodni sigurnosni model (Zero Trust). Generalno, enkripcija se koristi nad podacima koji se transportuju-prenose i onda kada se skladište-pohranjuju na serverima, ali se ne kriptuju i u toku eksploatacije kada serveri i aplikacije direktno pristupaju podacima. Ključni značaj ovog modela je upravo princip onemogućavanja pristupa i uvida neovlašćenim stranama u podatke u eksploataciji drugih korisnika u bilo kojem momentu. Mogućnost pristupa, uvida ili dekripcije podataka nemaju ni isporučioci-pružaoci usluga. Bezbjednosna poluga koja garantuje ovakav pristup je dislociranje kodova za enkripciju izvan ovog sistema što praktično onemogućava bilo kome unutar ili izvan sistema pristup podacima bez autorizacije. Ovo treba da predstavlja standard za koji nema pregovaranja.

2. ODRŽAVANJE BEZBJEDNOSNOG NIVOA

2.1. MJERE ZA ODRŽAVANJE NIVOA BEZBJEDNOSTI

Zaštita podataka na uređajima i sistemu ne predstavlja samo instaliranje antivirusnog softvera, već podrazumijeva izgradnju i razvoj slojevite strategije zaštite od svih oblika ugrožavanja. Sa globalnog aspekta, sajber bezbjednost nije samo informaciono-komunikaciono-tehnološki (IKT) problem i briga, već predpostavlja i individualnu odgovornost u poslovnoj i svakoj drugoj komunikaciji i interakciji korisnika globalnih mreža. Dakle, zaštita komunikacije, odnosno digitalnog otiska svakog korisnika u interakciji je imperativna (neophodna). Razvoj i evoluiranje sajber prijetnji je kontinuirana, tako da je i sa druge strane neophodno razvijanje alata i navika koje se moraju usvojiti i implementirati kako bi svaka interakcija korisnika, bez obzira da li je unutrašnja-interna ili vanjska-eksterna, ostala bezbjedna u odnosu na neautorizovane subjekte. Uspostavljeni bezbjednosni sistem je neophodno kontinuirano kontrolisati i terstirati kako bi se otklonile sve prijetnje i nedostaci u sistemu koji mogu dovesti do bezbjednosnog proboja ili ugrožavanja.

Neke od mjera su kontinuirani postupci bezbjednosne revizije fizičke-infrastrukturne (objekat, prostorije, prostor), digitalne (uređaji, tehnologija, procesi, pristupi-logovanje, sistem, mreže) i personalne (zaposleni i drugi korisnici) zaštite, odnosno testiranje odbrane od simuliranih napada na svaki od navedenih bezbjednosnih segmenata.

2.2. REVIZIJE BEZBJEDNOSTI

Moderna koncepcija bezbjednosti infrastrukture poslovnog subjekta ne podrazumijeva samo postavljanje fizičkih prepreka u vidu kapija, postavljanje naoružanih čuvara i uspostava bezbjednosnih perimetara. Bezbjednost predstavlja slojeviti sistem zaštite u kojem postoji visok stepen harmonizacije i sinhronizacije u radu tehnologije, ljudi i procesa (procedure) sa ciljem odvraćanja, otkrivanja, odlaganja ili efikasnog reagovanja na svaki oblik ugrožavanja.

Sajber bezbjednost podrazumijeva sveobuhvatan sistem alarma, detekrtora, kamera, obučene zaposlene sa visokim nivoom bezbjednosne svijesti i kulture, integrisane sisteme, hardver i softver i upravljanje rizicima na nivou poslovnog subjekta kako bi ostao izvan i ispred prijetnji koje se plasiraju ili razvijaju. Ako bezbjednost zamislimo kao lanac, onda je ona jaka onoliko koliko je jaka najslabija karika, odnosno svaka karika (otkrivanje, odvraćanje, brzina reagovanja, svijest zaposlenih, perimetri...) je bitna i ako su sinhronizovane za rezultat imamo bezbjednosnu otpornost poslovnog subjekta. Bezbjednosni sistem ne može biti samo uspostavljen kao vremensko prostorni perimetar koji je zaboravljen i zapušten. Revizije bezbjednosti upravo omogućavaju da mjere koje su uspostavljene i koje su u funkciji mogu blagovremeno da identifikuju ranjivost na uređaju ili sistemu prije nego što ih napadači uoče i iskoriste kao potencijalne izvore ugroženosti.

Preporučeni koraci u reviziji bezbjednosti:

- Pregled i kontrola pristupa (ulazna vrata i perimetri, tovarne i druge kapije, propusnice, identifikacioni dokumenti, biometrija, kredencijali, logovi).
- Pregled perimetra (ograde, osvetljenje, detektori kretanja i pokrivenost nadzorom infrastrukture i prostora).
- Permanentno testiranje alarma i video nadzora (blagovremeno otklanjanje uočenih nepravilnosti u radu opreme u cilju efikasnog praćenja i uspostavljanje bezbjednosnih perimetara).
- Provjera standardnih i posebnih procedura (evidencije, logovanje i upravljanje kretanja posjetioca, isporuke i pristup tehničke podrške i izvođača radova izvan strukture).
- Procjena bezbjednosne svjesti i kulture osoblja (poznavanje i poštovanje procedura i protokola, analiza uticaja kontrola i vježbi na efikasnost).
- Dokumentovanje utvrđenih nepravilnosti (izvještaji) u toku kontrole i prijedlog mjera za poboljšanje i unapređenje bezbjednosnih perimetara, ispravljanje protokola, bezbjednosno pokrivanje neprokrivenih segmenata i ažuriranje politika.

Svaki plan aktivnosti pa tako i plan bezbjednosti funkcioniše samo ako je permanentno provjeravan i testiran na bezbjednosne prijetnje i adekvatno nakon analize testa nadograđen. Redovne revizije-kontrole obezbjeđuju održavanje sistema bezbjednosti efikasnim, usklađenim i otpornim na ugrožavanje.

Najbolje prakse:

1. Sprovođenje slojevitog bezbjednosnog pristupa.
2. Praćenje trendova najnovijih bezbjednosnih tehnologija.
3. Razvijanje bezbjednosne kulture i svijesti zaposlenih.
4. Kontinuirano praćenje i procjena uspostavljenih bezbjednosnih mjera i perimetara.

Svijest o bezbjednosnoj situaciji i posljedicama njenog izostanka je način razmišljanja a ne razvijena vještina. To znači u potpunosti spoznati poslovnu okolinu (užu i širu), prepoznati ispravno, uobičajeno (rutinsko) i normalno odvijanje procesa i brzo uočiti, izolovati i onesposobiti neobično ili potencijalno opasno odvijanje bezbjednosnih rutina. Dakle, samo budnost, posvećenost i pažnja mogu spriječiti bezbjednosne incidente i prije nego što se dogode ili razviju. U kontekstu navedenog neophodno je: kontinuirano skeniraje poslovnog okruženja (užeg i šireg); vršiti procjenu ponašanja zaposlenih i predviđanje mogućih prijetnji (praćenje bezbjednosnih izazova i trendova); svesti korištenje ličnih uređaja (mobilnih telefona, tableta, prenosnih računara ili drugih pamernih uređaja) na radnom mjestu na minimum, odnosno potpuno isključiti; prijava svih neuobičajenih i sumljivih aktivnosti. Bezbjednost treba da se bezuslovno i bez izuzetka podrazumijeva, da postane rutina i pozitivna navika koju ne preispitujete već je permanentno sprovodite i unapređujete. Bezbjednosnu kulturu u vidu podrazumijevanih sajber bezbjednosnih navika možemo definisati kroz primjenu 3 bezbjednosna principa:

1. Obezbjeđenje digitalnih pristupa (logovanje) snažnim pristupnim lozinkama i višefaktorskimautentifikacijama (MFA) tamo gdje je to moguće uz izbjegavanje korištenja jednostavnih lozinki tipa „0123“. Uspostaviti složene lozinke posebno kreirane za svaki nalog sa slojevitim stepenom bezbjednosti.
2. Redovna izrada rezervnih kopija korištenjem bezbjednih sistema mreža svih podataka. Idealno bi bilo van lokacije ili korištenjem aplikacije Oblaka uz redovnu bezbjednosnu kontrolu.
3. Uspostavljanje radne harmonije između zaposlenih koji su ključni faktor bezbjednosti i prva linija odbrane ili ranjivosti ako nisu bezbjednosno osvješćeni i obučeni. Sprovoditi jednostavne i redovne edukacije o bezbjednosnim prijetnjama i ranjivostima i kako da se prepoznaju, izoluju i eliminišu. Ovakvo znanje predstavlja najbolje oružje protiv socijalnog inžinjeringa i podizanja nivoa bezbjednosti.

2.3. ODGOVOR NA INCIDENTE I OPORAVAK[264]

Odgovor na incidente i oporavak su ključne komponente sajber bezbjednosti, koje omogućavaju efikasno otkrivanje, obuzdavanje, ublažavanje i oporavak od sajber incidenata. Odgovor na incidente fokusira se na trenutne radnje koje se preduzimaju za rješavanje proboja bezbjednosti, dok oporavak uključuje vraćanje sistema, podataka i operacija u normalno stanje.

- Plan odgovora na incidente. Neophodno je razviti plan odgovora na incidente (IRP) u kojem su navedeni koraci koje treba slijediti u slučaju bezbjednosnog incidenta. Plan bi trebao definisati uloge i odgovornosti, uspostaviti komunikacijske protokole i obezbijediti jasan okvir za otkrivanje, obuzdavanje, iskorjenjivanje i oporavak od incidenata. IRP treba redovno revidirati, testirati i ažurirati kako bi se uskladio sa rastućim prijetnjama i organizacijskim promjenama.

- Otkrivanje i prijavljivanje incidenata. Rano otkrivanje sajber incidenata je ključno za minimiziranje potencijalne štete. Korisno je implementirati robusne sisteme za praćenje, sisteme za otkrivanje upada (IDS) i rješenja za upravljanje sigurnosnim informacijama i događajima (SIEM) kako bi se identifikovale anomalne aktivnosti i indikatori kompromisa. Neophodno je brzo prijavljivanje incidenata odgovarajućim internim timovima, osoblju za reagovanje na incidente i relevantnim vlastima.

[264] Tušinski B.: Savremene hibridne prijetnje - Sajber prijetnje, Završni Master rad, Banja Luka, 2023.

- Obuzdavanje i ublažavanje. Jednom kada se otkrije incident, moraju se poduzeti hitne mjere kako bi se isti obuzdao i spriječila daljnja šteta. Mjere trebaju uključivati izolaciju pogođenih sistema, onemogućavanje kompromitovanih naloga, zakrpe ranjivosti ili privremeno gašenje pogođenih usluga. Cilj je ograničiti obim incidenta i spriječiti njegovo širenje na druge sisteme ili mreže.

- Istraga i analiza. Nakon obuzdavanja, neophodno je sprovesti detaljnu istragu i analizu kako bi se razumjela priroda i obim incidenta. Ovo uključuje prikupljanje dokaza, analizu dnevnika, provođenje forenzičke analize i utvrđivanje osnovnog uzroka incidenta. Istraga pomaže u identifikaciji napadačeve ulazne tačke, kompromitovane imovine i potencijalnog uticaja na sisteme i podatke.

- Komunikacija i izvještavanje. Efikasna komunikacija je od vitalnog značaja tokom reagovanja na incident. Bitno je uspostaviti jasne linije komunikacije sa zainteresovanim stranama, uključujući interne timove, izvršni menadžment, pravne savjetnike, odnose s javnošću, klijente i regulatorna tijela. Pravovremeno i tačno izvještavanje pomaže u upravljanju uticajem incidenta, očuvanju povjerenja i usklađenosti sa zakonskim i regulatornim obavezama.

- Oporavak i restauracija. Jednom kada se incident obuzda i istraži, potrebno je fokusirati se na vraćanje pogođenih sistema, podataka i operacija u normalno stanje što uključuje obnavljanje iz rezervnih kopija, primjenu sigurnosnih zakrpa, ponovnu izgradnju kompromitovanih sistema ili ponovnu instalaciju softvera. Napori za oporavak daju prioritet kritičnim sistemima i podacima na osnovu njihovog poslovnog uticaja.

- Naučene lekcije i poboljšanja. Nakon incidenta sprovodi se detaljna post mortem analiza kako bi identifikovali naučene lekcije i oblasti za poboljšanje. Tu podrazumijevamo procjenu efikasnosti procesa reagovanja na incidente, utvrđivanje nedostataka u bezbjednosnim kontrolama i ažuriranje politika i procedura na osnovu nalaza incidenta. Kontinuirano poboljšanje osigurava bolje pripremljen odgovor na buduće incidente.

- Saradnja i eksterna podrška. Korisno je angažovati eksterno reagovanje na incidente i forenzičke eksperte, pravne savjetnike, agencije za sprovođenje zakona i organizacije specifične za industriju kako bi se pružila dodatna stručnost i podrška tokom reagovanja na incidente i napora za oporavak. Saradnja sa partnerima od povjerenja poboljšala bi sposobnost da se efikasno odgovori na buduće sajber incidente i ubrza oporavak od istih.

ZAKLJUČAK

Posjedovanje najnovije tehnologije i najnaprednijih alata u eri korporativne sajber bezbjednosti ne podrazumijeva automatski i garantovanu bezbjednost od ugrožavanja. Poslovni subjekti izdvajaju ogromna sredstva u zaštitne zidove (Firewall), detekciju, odvraćanje i sprječavanje napada stvarajući složenu i skupu digitalnu zaštitu. Međutim i pored toga sajber napadi i dalje pronalaze ranjivosti i uspjevaju napraviti štetu. Razlog za ovakvu situaciju je u stavu da tehnologija nije ciljani ishod bezbjednosti - već predstavlja samo skup alata-mehanizama kojima mora da upravlja ljudsko zanje i stručnost. Mnogi poslovni subkjekti su zbog ovoga u veoma nepovoljnoj bezbjednosnoj situaciji. Posjeduju tehnologiju ali nemaju potrebnu stručnost u internom okruženju za optimizaciju. Timovi zaduženi za bezbjednost su često nestručni, preopterećeni bez dovoljnog vremena za praćenje, identifikaciju i reakciju na bezbjednosnu prijetnju.

Posljedica ovakvog stanja neminiovno dovodi do parcijalnog i izolovanog pristupa u sprovođenju bezbjednosti (nema uvezanosti u dojavnom sistemu za sve učesnike u radu) što opterećuje odvijanje procesa ukupne bezbjednosti. Za postizanje svrsishodne i otporne sajber bezbjednosti neophodno je stvoriti simbiozu u poslovnom subjektu između ljudske stručnosti i dostupnih tehnoloških mogućnosti kako bi se dostigla otporna bezbjednosna granica. Uobičajeni-tradicionalni bezbjednosni modeli zaštite, uspostavljeni oko neke perimetarske platforme kao odbrane (Firewall, i VPN) nisu više dovoljni da zaštite poslovni subjekt od trendova novih sajber prijetnji. Bezbjednosni napadi i prodori su sve češći i sofisticiraniji što predpostavlja i novi pristup za izbor novih bezbjednosnih platformi, mehanizama, mjera i protokola za zaštitu osjetljivih podataka i sigurno djeljenje sa drugima.

Analizirajući bezbjednosne aplikacije, platforme i mehanizme za zaštititu podataka kako unutar poslovne strukture tako i u razmjeni prema vanjskim zahtjevima, korisnici i pružaoci usluga moraju biti svjesni važnosti i spremni da ulažu u IKT koje su sigurne po dizajnu sa fokusom na sigurnost podataka. Za odabir konkretne bezbjednosne zaštite u poslovnom subjeku, odnosno najbolje platforme za razmjenu informacija (datoteka) neophodno je voditi računa o specifičnostima poslovnih aktivnosti i potreba u odnosu na zaštitu od šteta i mogućih posljedica po konkretni poslovni subjekt. S obzirom na vrijednost i povjerljivost podataka u razmjeni, u kontekstu zaštite od narušavanja bezbjednosti i kompromitovanja podataka i sistema, trenutno su najbolje platforme „nulto povjerenje“ i „arhitektura bez znanja“. Najefikasnija strategija sajber bezbednosti predstavlja fuzija napredne tehnologije i visokokvalifikovanog ljudskog pristupa. Ove dvije platforme zajedno omogućavaju najviši stepen bezbjednosne zaštite. „Zero Trust“ („nulto povjerenje“) je platforma dizajnirana sa fokusom na bezbjednost u otpornosti pristupa samim podacima, ali se podaci i dalje mogu bezbjednosno ugroziti. „Zero Knowledge“ („arhitektura bez znanja“) je platforma dizajnirana da direktno štiti same podatke onemogućavajući neovlašteni pristup. Kombinacija ove dvije platforme sa dizajniranim bezbjednosnim protokolima čini ih neprobojnim i zato su pogodne kao ključna bezbjednosna zaštita u oblasti policijskih poslova sprovođenja i zaštite zakona, pravosuđu, finansijama, vojsci, velikim energetskim i drugim poslovnim subjektima koji raspolažu određenim podacima, informacijama i datotekama od velikog bezbjednosnog značaja.

U konstalaciji trenutnih globalnih odnosa u oblasti sajber bezbjednosti, neophodno je shvatiti i prihvatiti potrebu za potpuno novi filozofski pristup u razmišljanju o načinu na koji treba da se štitite podaci i informacije koje u svom radu proizvode i razmjenjuju poslovni subjekti.

Uz tradicionalnu sigurnost uspostavljenih perimetara, sigurnosni modeli usmjereni na podatke kao što su sigurnosne platforme „nultog znanja“ i „arhitekture bez znanja“ su od suštinskog značaja za istinsku zaštitu osjetljivih podataka koji se moraju čuvati i kojima se upravlja, odnosno koji se razmjenjuju u poslovnim transakcijama. Ovi modeli pružaju veću i jaču zaštitu za osjetljive podatke, u odnosu na druge platforme, smanjujući rizik od bezbjednosnih ugrožavanja i osiguravajući da informacije od značaja i visoke vrijednosti ostanu potpuno sigurne. Iako tranzicija može biti složena, potreba za čvrstim sigurnosnim okvirima je neophodna i bezuslovna. „Zero Trust“ i „Zero Knowledge“ platforme nisu samo trendovi, one su budućnost zaštite najkritičnijih informacijskih sistema i sredstava. Jedna od najpoznatijih kompanija koja nudi ovakve platforme sa mogućnošću prilagođavanja i potpune implementacije sa potrebnim specifičnim zahtjevima konkretnog poslovnog subjekta je „DekkoSecure“. Korištenjem ovakvih platformi koje su sigurne po dizajnu i fokusirane na sigurnost usmjerenu na same podatke, poslovni subjekt stiče značajnu prednost integracije bezbjednosnih mjera od samog početka a ne naknadno, omogućavajući da podaci ostaju potpuno bezbjedni u svakoj fazi svog životnog ciklusa. U trenutnoj komunikacijskoj globalizaciji imperativ za poslovne subjekte je da ulažu u tehnologije koje su sigurne po dizajnu ako žele u potpunosti eliminisati prijetnju konkurentskih strana i izbjeći štetne posljedice curenja ili bezbjednosnog proboja podataka.

LITERATURA

[1] Jovanić, V. (2024): *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta*, Doktorska disertacija, Travnik, 2024.

[2] Tušinski B.: *Savremene hibridne prijetnje - Sajber prijetnje*, Završni Master rad, Banja Luka, 2023.