BEZBJEDNOSNO UPRAVLJANJE / SECURITY MANAGEMENT

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

Stručni članak
https://www.doi.org/10.58952/zr20261501779
UDK / UDC 005.8:355.48

Sažetak
Upravljanje bezbjednošću u poslovnom subjektu predstavlja zahtjevan izazov obzirom na trenutne globalne prijetnje. Od lidera (nadležno lice za bezbjednost poslovnog subjekta) se zahtijeva upravljanje sistemom ravnoteže empatije, snage, vizije i prilagodljivosti, dok istovremeno ispunjava često suprotstavljene zahtjeve zaposlenih, zajednice i nadređenih. Dakle, liderstvo u oblasti bezbjednosti, posebno u sajber bezbjednosti zahtijeva od rukovodioca prilagodljivost, izgradnju povjerenja, samosvijest, bez obzira da li vodi tim kroz situacije visokog pritiska (krizne situacije) u radu ili podstiče određene aktivnosti tima na postizanju višeg nivoa efikasnosti. Efektivno i efikasno upravljanje bezbjednosnim sektorom je garancija za operativni uspjeh i jedinstvo, kako bezbjednosnog tima tako i čitavog poslovnog subjekta. Sajber kriminal u bezbjednosnom smislu dovodi do teških finansijskih, poslovnih i pravnih posljedica u poslovnom subjektu. Ako se zanemari uloga i značaj sajber bezbjednosti u poslovanju, mogu nastati značajni i nenadoknadivi gubici za poslovni subjekt, zaposlene, kao i narušavanje poslovne reputacije. Upravljanje bezbjednosnim rizicima u sajber napadima je ključna aktivnost, odnosno sveobuhvatan proces kojim se vrši identifikacija, procjena i ublažavanje rizika povezanih sa potencijalnim sajber napadima. Da bi se proces nesmetano odvijao podrazumijeva se implementacija strategija-praksi koje pomažu poslovnim strukturama da zaštite svoje zaposlene, sisteme, podatke, infrastrukturu i druge resurse od svih potencijalnih vrsta bezbjednosnih ugrožavanja i napada.
Ključne riječi: *upravljanje, sajber bezbjednost, sajber kriminal, rizik, sajber napad, procjena, zaštita*
JEL Klasifikacija: K14, K24, K40, K42

Abstract
Security management in a business entity is a demanding challenge given the current global threats. A leader (a responsible person for the security of a business entity) is required to manage a system of balance of empathy, strength, vision and adaptability, while at the same time meeting the often conflicting demands of employees, the community and superiors. Therefore, leadership in the field of security, especially in cyber security, requires adaptability, trust building, self-awareness from the manager, regardless of whether he leads the team through high-pressure situations (crisis situations) at work or encourages certain team activities to achieve a higher level of efficiency. Effective and efficient management of the security sector is a guarantee for operational success and unity, both of the security team and of the entire business entity. Cybercrime in the security sense leads to serious financial, business and legal consequences for the business entity. If the role and importance of cyber security in business is ignored, significant and irreparable losses may occur for the business entity, employees, as well as damage to the business reputation. Security risk management in Cyber Attacks is a key activity, that is, a comprehensive process that identifies, assesses and mitigates risks associated with potential CyberAttacks. In order for the process to proceed smoothly, it is understood the implementation of strategies-practices that help business structures to protect their employees, systems, data, infrastructure and other resources from all potential types of security threats and attacks.
Keywords: *management, Cyber Security, Cyber Crime, risk, Cyber Attack, assessment, protection*
JEL Classification: K14, K24, K40, K42

UVOD

Kao novo područje za razvoj bezbjednosnih politika, sajber bezbjednost se identifikuje kao veoma važan i nezaobilazan faktor u sektoru ukupne bezbjednosti svake države. Tehnološki trendovi sajber ugrožavanja su daleko ispred bezbjednosnih politika poslovnih subjekata. Ovakvo stanje zahtijeva brz i sveobuhvatan razvoj novih pravnih i političkih okvira.[272] Implementacija i razvoj bezbjednosnih sajber politika u svim segmentima društva, prije svega u strukturama koje se bave bezbjednošću društva (obavještajne službe, vojska, policija, sudovi i tužilaštva, IKT sektor) omogućit će bezbjedan saobraćaj u razmjeni podataka putem IK mreža (telekom operateri, internet provajderi, druga sredstva komunikacije) između fizičkih i pravnih lica što predstavlja važan podsticajan faktor u razvoju bezbjednog poslovnog okruženja države kao i modernizaciju upravljanja ukupnom bezbjednošću društva. Prema tome, bezbjedan sajber prostor omogućiće građanima da ostvaruju svoja prava u pogledu pristupa informacijama i rješavanju poslovnih i statusnih pitanja. Od suštinske je važnosti imati razvijenu svijest o mogućnostima, rizicima i prijetnjama koje nosi sajber prostor.[273] U kontekstu navedenog neophodno je da zakonodavac shvati svoju ulogu u pogledu razvijanja zakonodavnih i institucionalnih okvira vezanih za politike sajber bezbjednosti uz poseban naglasak na uspostavljanje principa visokih standarda i kontrole upravljanja u oblasti sajber bezbjednosti. Ovakav pristup omogućava sveobuhvatno angažovanje svih zainteresovanih subjekata države u izradi politika upravljanja sajber bezbjednošću. Sajber bezbjednost možemo predstaviti kao skup strategija, tehnologija, procesa i praksi osmišljenih i uspostavljenih za zaštitu kompjuterskih sistema, mreža, uređaja, programa i podataka od neovlaštenog pristupa, krađe, oštećenja ili ometanja. Dakle, osnovna svrha sajber bezbjednosti je da osigura povjerljivost, integritet i dostupnost informacija zainteresovanim subjektima u digitalnom okruženju. Korištenje novih i naprednih rješenja za sajber bezbjednost, omogućava poslovnim subjektima pored minimiziranja rizika od prijetnji i unaprijeđenje povjerenja prema poslovnim partnerima.[274]

1. UPRAVLJANJE RIZICIMA KOD SAJBER NAPADA

Sajber bezbjednost više nije opcioni aspekt poslovanja, već neophodni preduslov za očuvanje podataka, kontinuitet rada i pravnu sigurnost. Savremene kompanije, institucije i organizacije u velikoj mjeri zavise od digitalnih sistema, kako za skladištenje podataka, tako i za obavljanje svakodnevnih aktivnosti. Međutim, upravo ta digitalna zavisnost otvara vrata raznim oblicima zloupotreba i sajber napada.[275] Za uspješno vođenje segmenta bezbjednosti, posebno sajber bezbjednosti, u poslovnom subjektu kod kojeg poslovni-proizvodni proces zahtijeva bezbjednosnu kulturu na visokom nivou zbog vrijednosti podataka i informacija koje se koriste i koje nastaju u radu, neophodno je da se razvijaju strategije upravljanja koje su usklađene sa potencijalnim izazovima i koje podrazumijevaju visok stepen bezbjednosti i povjerenja između zaposlenih, rukovodioca i klijenata. Ovo prije svega podrazumijeva izgradnju timova visoke efikasnosti i uspostavljanje kvalitetnog sistema bezbjednosne otpornosti na prijetnje i ugrožavanja kako unutrašnje tako i vanjske. U praksi to predpostavlja procjenu sajber bezbjednosti i uspostavljanje bezbjednosne politike procedura, kontrole i permanentne implementacije novih bezbjednosnih sistema i rješenja u kontekstu novih bezbjednosnih trendova rizika i prijetnji.

[272] Uvod u upravljanje sajber bezbjednošću-Priručnik za narodne poslanike, DECAF Geneve Centre For Security Sector Governance, 2021., strana broj 4.
[273] Ibid.
[274] https://unija.com/bs/rjesenja-za-sajber-sigurnost/ 11.11.2025. 14.45
[275] https://zuniclaw.com/sajber-bezbednost/ 11.11.2025. 14.52

Neadekvatne i zastarjele bezbjednosne politike ugrožavaju poslovni subjekt, njegove poslovne procese, infrastrukturu i zaposlene (fizička i finansijska ranjivost i rizici).

1.1. PROCJENA SISTEMA SAJBER BEZBJEDNOSTI

Procjena sistema sajber bezbjednosti podrazumijeva profesionalnu, objektivnu i sveobuhvatnu analizu efikasnosti uspostavljenog sistema sajber bezbjednosti, uz preporuku smjernica za prevazilaženje i rješavanje problema u skladu sa utvrđenim prioritetima. Analiza podrazumijeva identifikaciju problema kroz provjeru i procjenu zaposlenih, procesa i informacionih sistema, a u skladu sa osnovnim elementima ključnih industrijskih standarda i dobre prakse od kojih su najznačajniji ISO 27001 standard i NIST okvir za sajber bezbjednost. Pored kreiranja sistema upitnika (efikasan način za sagledavanje postojećeg stanja bezbjednosti) za zaposlene, razgovora-intervjua sa zaposlenima, organizovanje bezbjednosnih radionica i detaljne analize visokorizičnih oblasti poslovanja, neophodno je ostvariti i saradnju sa donosiocima odluka nadležnim za tehničke, komercijalne i izvršne poslove u poslovnom subjektu. Kako bi se upotpunila vizija neophodih mjera sajber bezbjednosti IKT sistema u poslovnom subjektu potrebno je upoznati se sa tekućim i planiranim aktivnostima, tehnološkim i strateškim pravcima razvoja i trenutnim stavovima i odnosima prema postojećim i mogućim rizicima od sajber napada u poslovnom subjektu. Praktično to znači da je neophodno kroz analizu sagledati slabosti i probleme postojećih procedura i predložiti mjere i aktivnosti za sprovođenje potpune strategije sajber bezbjednosti. Upravljanje sajber bezbjednošću u poslovnom subjektu podrazumijeva uspostavljanje politika, procedura i praksi sa ciljem jačanja kapaciteta organizacije da spriječi, otkrije i umanji zlonamjerne aktivnosti, odnosno njihove počinioce u sajber prostoru, uz poštovanje važeće zakonske regulative, strateških okvira, obaveza i očekivanja.[276]

Aktivnosti i mjere efikasnog upravljanja sajber bezbjednošću u poslovnom subjektu obuhvata sljedeće aktivnosti:

- Bezbjednosni konsalting - pružanje profesionalnih savjeta u vezi sa konkretnim aktivnostima u pogledu uspostave i primjene politika sajber bezbjednosti u poslovnom subjektu. Proces upravljanja sajber bezbjednossću je permanentan i razvojno složen uz preklapanje nadležnosti, mogućnosti, obaveza i potreba u pogledu vizija za implementaciju i očekivanja na lokalnom, regionalnom i međunarodnom nivou. Analiza procedura i bezbjednosnih politika, uz preporuke prilagođene potrebama konkretnog poslovnog subjekta, omogućava sveobuhvatno planiranje i kreiranje jasnih bezbjednosnih ciljeva, odnosno usklađenost sa zakonskim okvirima i najboljom međunarodnom praksom (Evropa), uz prilagođavanje stepena usklađenosti sa lokalnim uslovima, odnosno postojećim nacionalnim zakonskim okvirima i kapacitetima.
- Izrada konkretnih strategija sajber bezbednosti - profesionalno usmjeravanje kao i kod savjetovanja u oblasti kreiranja i uspostave bezbjednosnih sajber politika, bezbjednosno upravljanje podrazumijeva kreiranje i izradu konkretne strategije za poslovni subjekt kroz definisanje jasne i bezbjednosno prihvatljive vizije i misije, kao i aktivnosti koje su potrebne za njihovo postizanje i implementaciju u određenim vremenskim okvirima (kratkoročni, srednjeročni i dugoročni koraci).
- Konkretizacija aktivnosti u poslovnom subjektu na podizanju svijesti zaposlenih u oblasti sajber bezbjednosti - jačanje bezbjednosnih kapaciteta svijesti sakog pojedinca u poslovnom subjektu predstavlja najbolju strategiju za postizanje najvišeg stepena

[276] https://www.pwc.rs/sr/usluge/revizija-informacionih-sistema/usluge-u-oblasti-sajber-bezbednosti.html 11.11.2025. 14.55.

otpornosti u konkretnom sajber prostoru (eng. cyber resilience), kroz organizovanje i izvođenje edukacija na podizanju svijesti o prevenciji, odnosno permanentnoj zaštiti od svih bezbjednosnih rizika. Edukacija treba da bude prilagođena konkretnom poslovnom subjektu i uslovima u kojima obavlja svoje poslove (javna uprava, javni ili privatni poslovni subjekt, bezbjednosna struktura, obrazovni javni ili privatni subjekt i dr.), kao i nivoima odlučivanja, odnosno prirodi posla.

Uspješno implementirana strategija upravljanja sajber bezbjednošću podrazumijeva prije svega sveobuhvatnu analizu IT infrastrukture i drugih resursa u poslovnom subjektu. Analiza omogućava identifikaciju sistemskih slabosti ugrožavanja i postavljanje parametara prema potrebama za prevazilaženje i onemogućavanje potencijalnih napada.

Analiza infrastrukture uključuje nekoliko ključnih koraka:[277]

- Procjena mrežnih kapaciteta (sistema): identifikacija mogućih slabosti u mrežnim protokolima, firewall-ovima i konfiguracijama rutera, kao potencijalnim lokacijama-tačkama potencijalne ulazne tačke za napade. Na primjer, loše podešen firewall može omogućiti napadačima da zaobiđu osnovne sigurnosne mehanizme.
- Sigurnosne provjere: pregled trenutne postavke svih sistema, uključujući cloud okruženja i servere. Bezbjednosni audit pomaže u otkrivanju ranjivosti u softverima koji nisu ažurirani ili u pristupima korisnika koji nisu adekvatno zaštićeni.
- Preporuke za poboljšanja: na osnovu analize, stručnjaci za sajber sigurnost kreiraju prilagođene strategije za unapređenje sigurnosti. Strategija uključuje tehnološka rješenja, politike bezbjednosti i obuku zaposlenih.

Savjeti za unaprjeđenje infrastrukture:

1. Redovno ažuriranje mrežne opreme i softvera: zastarjeli sistemi često sadrže poznate ranjivosti koje napadači mogu lako iskoristiti.
2. Implementacija VPN rješenja: VPN (Virtual Private Network) obezbjeđuje šifrovanu komunikaciju između uređaja i mreže, štiteći podatke čak i kada se koriste nesigurne mreže, poput javnih Wi-Fi mreža.

1.2. POLITIKE (PRAVILA, PROCEDURE) I AŽURIRANJA

Uspostavljanjem bezbjednosnih politika (procedure, pravila) stvaraju se osnovne pretpostavke za upravljanje rizikom u bezbjednosnim izazovima ugrožavanja. Međutim, samo uspostavljanje bezbjednosnih politika i dimenzionisanje potrebnih bezbjednosnih parametara ne pretpostavlja automatsku i trajnu zaštitu od ugrožavanja i rizika ukoliko su vremenski i prostorno neadekvatne i ne prate nove trendove prijetnji u pogledu evoluiranja i nadogradnje sistema. Neadekvatne i neprilagođene politike-procedure ostavljaju bezbjednosne praznine koje stvaraju ranjivosti i izlažu poslovni subjekt fizičkim, infrastrukturnim, ljudskim i finansijskim rizicima. Zato je potrebno uspostaviti bezbjednosnu platformu koja podrazumijeva razvijanje specifičnih politika poslovnog subjekta u pogledu zakonodavnih i pravnih limita (nacionalni standardi i najbojle prakse) koji su propisani u teritorijalnom ustroju (država) u kojem egzistira i posluje i kontinuirano bezbjednosno ažuriranje (praćenje bezbjednosni trendova prijetnji). Za bezbjedno poslovno okruženje neophodno je uspostaviti sistem sveobuhvatne obuke i rješenja za usklađenost sa politikama koje su odraz dobrih praksi prakričara i stručnjaka iz konkretnog bezbjednosnog sektora (fizička, sajber, infrastrukturna, finansijska ili ljudska bezbjednost).

[277] https://unija.com/bs/rjesenja-za-sajber-sigurnost/, 11.11.2025. 14.45

Za uspješno postavljen i vođen sistem bezbjednosti u poslovnom subjektu neophodno je u kontekstu bezbjednosnih politika: kontinuirano ažuriranje; svakodnevna obuka; pravno i zakonski usklađivanje i provjera; pomoć u implementaciji i upravljanje dokumentima i procesima u jednom potpuno integrisanom sistemu zasnovanom na nekoj pouzdanoj softverskoj platformi. Dakle, bezbjednosne politike koje obuhvataju i pokrivaju sva operativna poslovna područja, provjerene i uspostavljene od strane eminentnih IT i stručnjaka za javnu bezbjednost i koje su usklađene sa važećim zakonodavnim propisima, mogu pružiti potrebnu i potpunu zaštitu proizvodnog procesa i drugih resursa nekog poslovnog subjekta.
Razvoj bezbjednosnih politika, softvera za upravljanje i obuka o usklađenosti na jednoj platformi treba da obuhvati:

- Odabir kompanije sa adekvatnom ponudom za razvoj i usklađivanje politika sa specifičnim osvrtom na profil i potrebe poslovnog subjekta.
- Dostupnost ažuriranja elektronskim putem koja prate izmjene zakonskih propisa, praksi i standarda.
- Kontinuirani pristup i obuka osoblja za primjenu bezbjednosnih politika.
- Uspostavljanje mobilne i mrežne platforma za bezbjedno pohranjivanje i pristup sadržajima obuka i politika-procedura.
- Uspostavljanje sinhronizacije upravljanja pohranjenih dokumenata za upravljanje procedurama i integracija sa višim nivoima bezbjednosnih poltika.
- Akreditacija politika uz pribavljanje potrebnih uslova za sticanje akreditacija i njihovo održavanje.
- Upravljanje i implementacija bezbjednosnih politika u cilju brzog usvajanja i preusmjeravanje fokusa zaposlenih na prioritetne poslove.

Digitalizacija poslovnih interakcija na globalnom nivou postavila je sajber bezbjednost kao ključni faktor u zaštiti sistema poslovnih transakcija razmjene podataka i informacija. Uporedo sa razvojem digitalizacije poslovanja razvijaju se i evoluiraju i sajber prijetnje koje ugrožavaju sve poslovne subjekte (bez obzira na veličinu) ali i pojedince koji koriste IKT u razmjeni podataka i informacija u svom radu. Zaštita od sajber prijetnji zahtijeva od poslovnih subjekata (i pojedinaca) određena ulaganja u napredna i efikasna sajber bezbjednosna rješenja i njihovu implementaciju kako bi minimizirali ili potpuno eliminisali rizik i obezbjedili nesmetan poslovni proces. Međutim, ulaganja i implementacija efikasnih mjera sajber bezbjednosti ništa neće promjeniti ukoliko se ne ulaže u njihov kontinuirani razvoj i nadogradnju, odnosno sajber bezbjednost zahtijeva određeno bezbjednosno upravljanje i angažovanje eksperata za sajber bezbjednost. Sajber bezbjednosno upravljanje je ključna komponenta sistema sajber bezbjednosti i bez njega je kompletan sistem potpuno bezvrijedan. Uspješno upravljanje sajber bezbjednošću podrazumijeva kombinaciju tehnoloških rješenja i ljudskih faktora u odnosu na različite aspekte zaštite u poslovnom subjektu, a prije svega upravljanje ključnim komponentama sistema:

- Mrežna bezbjednost (zaštita poslovne kompjuterske mreže od svih vrsta sajber prijetnji i napada i neovlašćenih pristupa).
- Bezbjednost poslovnih podataka (skladištenje i čuvanje podataka i informacija korištenjem enkripcije i kontrole pristupa-logovanje).
- Kontinuirana edukacija zaposlenih uz podizanje bezbjednosne kulture i svijesti u radu (prepoznavanje i izbjegavanje mogućih sajber prijetnji i rizika u poslovnoj interakciji).
- Kadrovska politika (bezbjednosna provjera svakog pojedinačnog kandidata koji se prijavi na konkurs za zapošljavanje bez obzira o kojem se radnom mjestu radilo sa posebnim

osvrtom na pozicije u kojima se koriste pristupi bezama podataka sa osjetljivim informacijama, uvođenje obaveznih ugovora o radu sa klauzulama o zaštiti i čuvanju podataka).
- Kontrola prava pristupa (korištenje principa „minimum privilegija“) - nulto povjerenje.
- Bezbjednost hardvera (zaštita kompjuterske i druge opreme koja se koristi u radu).
- Bezbjednost softvera (zaštita korisničkih programa od svih vrsta prijetnji i napada internih i eksternih).
- Reakcija na incidente (razvijanje politika protokola za detekciju, upravljanje i oporavak sistema i mreže od sajber napada).

2. NEOPHODNI KORACI U UPRAVLJANJU RIZICIMA U SAJBER NAPADU[278]

2.1. IDENTIFIKACIJA RIZIKA

Prvi korak kod upravljanja rizucima je prepoznavanje (predviđanje) potencijalnih sajber prijetnji i ranjivosti u sistemima. To podrazumijeva sprovođenje određenih politika i procedura:

- Skeneri ranjivosti - predstavljaju sistem procedura i postupaka koji analiziraju infrastrukturu i detektuju (otkrivaju) sistemske slabosti.
- Simulacije napada („red teaming“) - postupci koji omogućavaju da se izvrši realna procjena o mogućem pristupu sistemu od strane potencijalnih napadača.

2.2. PROCJENA RIZIKA

Nakon utvrđene identifikacije, neophodno je izvršiti procijenu mogućnosti, vjerovatnoću i razmjere rizika koji predstavlja identifikovana slabost. U praktičnom smislu to predstavlja izradu analize uticaja potencijalnog napada na poslovni proces, kao i realnu mogućnost da će napad biti uspješan. Faktori koji se procjenjuju u analizi:

- Finansijski gubici.
- Šteta ugledu kompanije i daljem poslovanju.
- Pravne posljedice po osnovu partnera i sklopljenih ugovora.
- Šteta u pogledu uništavanja, blokiranja ili gubitak poslovnih podataka.

2.3. MITIGACIJA RIZIKA

Mitigacija rizika predstavlja proces izbora i preduzimanja najboljih dugoročnih mjera za smanjenje, eliminaciju ili prevenciju potencijalnih rizika i njihovih negativnih posljedica. Mitigacija podrazumijeva identifikaciju, analizu i implementaciju najboljih opcija (strategija) za upravljanje rizikom. Ovo je definitivno najbitnija faza koja se sprovodi u skladu sa postojećim (predpostavljenim) ograničenjima i postavljenim ciljevima. Strategije su:[279]

- Kontrola rizika.
- Smanjenje rizika - predstavlja umanjenje posljedice incidenta ili mogućnosti da se incident desi.
- Zadržavanje rizika - predstavlja prihvatanje bilo kojeg ishoda incidenta i prihvatljiva je u situacijama malih-neznatnih rizika.
- Prebacivanje ili transfer rizika - kompanija dijeli posljedice incidenta sa drugom kompanijom kao i preduzimanje mjera za ublažavanje rizika.

[278] https://unija.com/bs/rjesenja-za-sajber-sigurnost/ 11.11.2025. 14.45
[279] https://ie.mas.bg.ac.rs/data_store/upload/22_terotehnolosko3.pdf, 17.02.2026. 13.30

(Ugovor sa osiguravajućim kompanijama koje su predložile određene mjere za ublažavanje rizika od incidenata a u slučaju dešavanja pokrivaju određene troškove bez preuzimanja odgovornosti za incident.)

Implementacija navedenih strategija koje se fokusiraju na smanjenje identifikovanih rizika može se postići putem nekoliko metoda:

- Preventivno djelovanje **-** tehnička zaštita**:** podrazumijeva instalaciju antivirusnih programa, firewall-a, enkripciju podataka, sigurnosne kopije na izmješetenim serverima.
- Edukacija zaposlenih**:** kontinuirana obuka i edukacija zaposlenih o bezbjednosnim politikama i prepoznavanju mogućih prijetnji (podizanje bezbjednosne kulture).
- Dugoročne mjere - kontinuirano ažuriranje komponenti sistema i softvera: prepoznavanje sistemskih ranjivosti i njihova eliminacija kako bi se onemogućili i spriječili sajber napadi.

2.4. KONTROLA I PRAĆENJE

Podrazumijeva sistemsko praćenje i evaluaciju rezultata primjenjenih strategija i njihovo upoređivanje sa predpostavljenim kriterijumima. U kontekstu navedenog neophodno je uspostaviti sistem za kontinuirani nadzor kako bi se otkrili potencijalni sajber napadi u realnom vremenu što podrazumijeva:

- Permanentno praćenje cjelokupnog mrežnog saobraćaja**.**
- Otkrivanje i registrovanje anomalija u sistemu.
- Uspostava sistema za pravovremeno obavještavanje o incidentima.

2.5. PLAN ZA OPORAVAK OD NAPADA (DISASTER RECVERY PLAN)

Prevencija je najvažniji segment u sistemu zaštite i predpostavlja planiranje aktivnosti svih aktera u poslovnom subjektu za najgori scenario bezbjednosnog ugrožavanja. Ključni aspekt prevencije je Plan za oporavak od sajber napada koji treba da uključuje:

- Brzi odgovor na napad kako bi se minimizirao uticaj.
- Plan za vraćanje podataka i sistema u radno stanje.
- Analiza post-napada kako bi se identifikovali nedostaci u prethodnim strategijama.

Oporavak predstavlja ciljanu aktivnost povratka ugroženog perimetra u sistemu u stanje prije napada i ugrožavanja. Kao faza u odgovoru na bezbjednosni napad i ugrožavanje oporavak se razlikuje od faze odgovora na napad upravo po svom usmjerenju. Ova faza je fokusirana na donošenje adekvatnih odluka za konkretne aktivnosti koje se moraju donijeti i sprovesti nakon što su kroz analizu počinjene štete u napadu sagledane i prihvaćene kao neophodne i potrebne. Aktivnost i mjere za oporavak podrazumijevaju izgradnju i obnovu-restituciju uništene infrastrukture u napadu.

2.6. KONTINUIRANO POBOLJŠANJE

Spriječavanje rizika i upravljanje rizicima u sajber napadima predstavlja kontinuirani i dinamičan proces i aktivnost. Permanentno prilagođavanje i unapređivanje bezbjednosnih strategija u skladu sa trendovima prijetnji i novim tehnologijama je imperativ dugoročne i efikasne zaštite. Praktično, cilj spriječavanja i upravljanja rizicima u sajber prijetnjama i napadima predstavlja minimiziranje mogućnosti da će pokrenuti napad uspjeti, odnosno umanjenje posljedica uspješnog napada, i brz oporavak i vraćanje sistema u standardni mod rada

ZAKLJUČAK

Upravljanje bezbjednosnom zaštititom informacionog sistema koja nije adekvatna i prilagođena potrebama poslovnog subjekta, može dovesti do odgovornosti za ugrožavanje korisnika, poslovnih partnera, zaposlenih kao i organa koji imaju regulatornu funkciju u pogledu kontrole primjene zakona iz oblasti informacionih tehnologija, zaštite ličnih i tajnih podataka. Budući da je još uvijek najveći broj sajber napada koji je usmjeren na iskorištavanje slabosti ljudskog faktora, odnosno manipulaciju zaposlenih kroz socijalni inženjering, kako bi se kroz njihove nehotične propuste došlo do pristupa štićenim i poverljivim informacijama ili sistemu, i dalje najčešći metod napada, neophodno je sprovesti potrebne edukacije zaposlenih u poslovnom subjektu iz oblasti podizanja svijesti o bezbednosnoj kulturi. U kontekstu navedenog, analize savremenih trendova bezbjednosnih ugrožavanja ukazuju da su finansijski troškovi sajber incidenata visoki i da je neophodno uključiti organizacione, kadrovske i pravne mehanizme bezbjednosne zaštite pored implementiranih tehničkih rešenja. Zbog toga je neophodno da poslovni subjekti, prihvate i razumiju značaj preventivnog postupanja kroz uspostavu i implementaciju neophodnih bezbjednosnih mjera koje će im bezbjednost po svim aspektima ugrožavanja podići na najviši nivo zaštitite.

Da bi upravljanje i zaštita informacionih sistema bili blagovremeni i efikasni, neophodno je primijeniti kombinaciju različitih mjera zaštite, odnosno pored standarnih tehničkih mjera implementirati organizacione, kadrovske i pravne mjere. Dakle, nije u pitanju samo jedna opcija i rešenje, već sveobuhvatan bezbjednosni pristup i stav koji podrazumijeva pokrivanje svih segmenata poslovanja (infrastruktura, softverski programi i alati, interne procedure politika i pravila, zaposleni, ugovori, ispunjavanje domaćih propisanih regulatornih i osiguravajućih obaveza zaštite ličnih podataka i informacija). Primjena tehničkih, kadrovskih i organizacionih mjera upravljanja i zaštite u poslovnom subjektu moraju biti prilagođeni vrsti posla, podataka i informacija koji se obrađuju i koriste u poslu u kontekstu mogućih rizika kojima je izložen poslovni proces subjekta.

Pored domaćih regulatornih propisa iz oblasti bezbjednosti i zaštite informascionih sistema poslovni subjekti su dužni da sprovode i tehničke smjernice evropske agencije ENISA[280] koja preporučuje ključne mehanizme za bezbjednost, a prije svega praktičan pristup u kontroli sprovođenja prijema i edukacije zaposlenih i upravljanje bezbjednosnim rizicima i incidentima kako bi se obezbjedilo nesmetano odvijanje poslovnih procesa. Ove smjernice podrazumijevaju pripremu poslovnog subjekta za primjenu mjera NIS2[281] direktive kao praktičan osnov za upravljanje sajber incidentima u poslovnim strukturama koje se bave pružanjem usluga digitalnog poslovanja i aktivnostima koje imaju poseban značaj u razmjeni podataka i informacija putem IKT. Pored upravljanja tehničkim i organizacionim mehanizmima zaštite, neophodno je da se isto primjeni i u oblasti upravljanja mehanizmima pravne zaštite. To prije svega podrazumijeva kvalitetno odrađen i uspostavljen proceduralni pravni okvir u vidu poslovnih politika ugovora o povjerljivosti i čuvanju poslovnih tajni što može značajno uticati na brzo reagovanje u kriznim incidentima i ublažiti moguće posljedice.

[280] ENISA- European Union Agency For Sybersecurity, https://www.enisa.europa.eu/ 21.04.2026. 10.20

[281] https://bqc-isostandardi.ba/standardi/nis-2-regulativa-evropske-unije-za-jacanje-i-ujednacavanje-standarda-sajber-bezbjednosti/, 11.11.2025., 15.35

Preporuke za najvažnije tehničke, organizacione, kadrovske i pravne mjere zaštite:

Tehničke mjere:

- Enkripcija (šifrovanje). Svaki korisnik interneta, pojedinac ili organizacija, trebalo bi da zaštite bežičnu mrežu koju koriste od neovlaštenog pristupa kompjutri ili druom uređaju koji koristi internt.[282]
- Višefaktorska autentifikacija (MFA). Svaki korisnik računara u mreži treba da je vezan isključivo za jedan računar i da se na njega konektuje korištenjem lične lozinke (password) putem uređaja za pristup koji registruje svako logovanje.[283]
- Firewall i antivirusni softveri.
- EDR/XDR sistemi - napredni alati za detekciju i reagovanje na upade u realnom vremenu.
- VPN i zaštita domena - bezbjedan pristup mrežama i zaštita identiteta organizacije na internetu.
- Redovni backup podataka - ključ za brzi oporavak i kontinuitet poslovanja nakon incidenta.
- Pen testovi i skeniranje ranjivosti - proaktivne metode za otkrivanje slabosti u sistemima.

Organizacione i kadrovske mjere:

- Politike i procedure bezbjednosti informacija.
- Razvoj i implementacija sveobuhvatne nacionalne strategije sajber sigurnosti. Ista mora uzeti u obzir evoluirajuće okruženje prijetnji, postaviti jasne ciljeve i ocrtati akcije za unapređenje sajber odbrane, zaštitu kritične infrastrukture, promociju međunarodne saradnje, te obezbjediti otpornost nacionalnog digitalnog ekosistema.[284]
- Jačanje javno-privatnih partnerstva u sajber sigurnosti.[285]
- Obuka i podizanje svijesti zaposlenih.
- Kadrovska politika - provjere kandidata prilikom zapošljavanja (npr. pozicija sa pristupom osetljivim sistemima), uvođenje klauzula o čuvanju podataka u ugovore o radu, kao i kontrola pristupa i prava po principu „najmanjih privilegija“.
- Plan upravljanja incidentima - jasno propisane procedure za prijavu, obradu i dokumentovanje bezbjednosnih incidenata, uz definisanje nadležnosti.
- Politika revizije i kontrole pristupa**.**

Pravni mehanizmi zaštite:

Ugovorne obaveze - zaštita kroz poslovne ugovorne odnose sa zaposlenima, eksternim saradnicima i IT dobavljačima.

Povjerljivost i poslovna tajna - kontrola pristupa kroz ugovorne obaveze prema različitim profilima i kategorijama fizičkih i pravnih i lica.

Sajber osiguranje - mehanizam za ublažavanje posljedica napada u finansijskom, reputacijskom i pravnom smislu.

Dakle, upravljanje sajber bezbjednošću nije stav po izboru, već neophodnost u vrijeme informacionih sistema koji su postali dio poslovnog okruženja u komuniciranju, uslugama i razmjeni informacija. Bezbjednosni sajber napadi su neizbježan faktor ugrožavanja i od sposobnosti poslovne strukture da se efikasno i adekvatno suprostavi napadu u mnogome zavisi i njen i poslovni opstanak svih fizičkih i pravnih lica koji su sa njom u poslovnim vezama.

[282] Jovanić, V.: *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta*, Doktorska disertacija, IUT PF Travnik, 2024., strana 162.
[283] Ibid, strana 163.
[284] Tušinski, B.: *Savremene hibridne prijetnje - Sajber prijetnje*, Završni Master rad, Banja Luka, 2023., strana 91.
[285] Ibid, strana 91.

Kombinacija upravljanja tehničkim, organizacionim, kadrovskim i pravnim mehanizmima i mjerama pored toga što štiti infrastrukturu, podatke i informacije poslovnog subjekta, pokazuje i poslovnu ozbiljnost, zrelost i odgovornost u poslovanju prema korisnicima, partnerima i zakonodavcu. Upravljanje bezbednošću podrazumijeva implementaciju tehnologije u cilju uvezivanja i uspostavljanja neophodnih mehanizama u vidu pravila, ugovora, obuka, planova i strategija suprostavljanja svim oblicima ugrožavanja i incidenta. Iz navedenih razloga je neophodno angažovanje i eksperata koji mogu da uvežu IKT, organizacioni, kadrovski i pravni okvir za adekvatno upravljanje bezbjednosnim odgovorima u sajber incidenatima.

LITERATURA

[1] Jovanić, V.: *Kriminalistički i krivičnopravni aspekti visokotehnološkog-Sajber (Cyber) kriminaliteta*, Doktorska disertacija, IUT PF, Travnik, 2024.
[2] Tušinski, B.: *Savremene hibridne prijetnje - Sajber prijetnje*, Završni Master rad, Banja Luka, 2023.
[3] Uvod u upravljanje sajber bezbjednošću - Priručnik za narodne poslanike, DECAF Geneve Centre For Security Sector Governance, 2021.

Internet izvori
[1] https://unija.com/bs/rjesenja-za-sajber-sigurnost/ 11.11.2025. 14.45
[2] https://zuniclaw.com/sajber-bezbednost/ 11.11.2025. 14.52
[3]https://www.pwc.rs/sr/usluge/revizija-informacionih-sistema/usluge-u-oblasti-sajber-bezbednosti.html 11.11.2025. 14.55
[4] https://ie.mas.bg.ac.rs/data_store/upload/22_terotehnolosko3.pdf, 17.02.2026. 13.30
[5] ENISA- European Union Agency For Sybersecurity, https://www.enisa.europa.eu/ 21.04.2026. 10.20
[6]https://bqc-isostandardi.ba/standardi/nis-2-regulativa-evropske-unije-za-jacanje-i-ujednacavanje-standarda-sajber-bezbjednosti/, 11.11.2025., 15.35