CYBER SIGURNOST KAO POSLOVNI ZAHTJEV (PROCES)/CYBER SECURITY AS A BUSINESS REQUIREMENT (PROCESS)

Edin Alić[1], Muhamed Ćosić[2]
[1]Internacionalni Univerzitet Travnik u Travniku, Aleja Konzula - Meljanac bb, Travnik, BiH,
[2]Internacionalni Univerzitet Travnik u Travniku, Aleja Konzula - Meljanac bb, Travnik, BiH,
email: alicedin@hotmail.com ,drmuhamedcosic@gmail.com

UDK / UDC 004.056.5:005.8
Pregledni članak

Sažetak

Današnje moderno poslovanje odlikuje se stalnim razvojem tehnologije koju organizacije koriste u svakodnevnom radu. Sa razvojem tehnologije dolazi i potreba za cyber sigurnosti kako bi se zaštitili podaci i infrastruktura organizacija od različitih cyber prijetnji. Cyber sigurnost postaje ključni segment strategije poslovanja svake organizacije, jer se suočava sa sve većim brojem napada koji mogu ozbiljno ugroziti reputaciju, finansijsku stabilnost i operativnu sposobnost. Cyber sigurnost nije samo tehničko pitanje, već strateški zahtjev koji zahtijeva uključivanje svih sektora i višeg rukovodstva u planiranje, implementaciju, kontrolu i unapređenje sigurnosnih politika i procedura. Kroz usvajanje i primjenu odgovarajućih mjera cyber sigurnosti, organizacije mogu zaštititi svoje podatke, povjerenje kupaca, reputaciju i finansijska sredstva, te osigurati kontinuitet poslovanja i usklađenost sa zakonskim propisima.

Ključne riječi: Cyber sigurnost korporativna sigurnost, poslovni zahtjevi.

Abstract

Today's modern business is characterized by the constant development of technology that organizations use in their daily work. With the development of technology it comes the need for cyber security to protect the data and infrastructure of organizations from various cyber threats. Cyber security is becoming a key segment of every organization's business strategy, as it faces an increasing number of attacks that can seriously threaten reputation, finansial stability and operational capability. Cyber security is not only a technical issue, but a strategic requirement that requires the involvement of all sectors and senior management in the planning, implementation, control and improvement of security policies and procedures. Through the adoption and application of appropriate cyber security measures, organizations can protect their data, customer trust, reputation and finansial resources, and ensure business continuity and compliance with legal regulations.

Keywords: Cyber security, corporate security, business requirements.

UVOD

Tehnološki razvoj i sve šira primjena tehnologije donosi brojne prednosti poput ubrzanja poslovnih procesa, automatizacije poslovanja, olakšanog pristupa i razmjene informacija, mogućnosti rada na daljinu, lakšeg pristupa tržištima te smanjenja troškova. Različite aktivnosti poput online kupovine, internet bankarstva i drugih poslovnih usluga izlažu organizacije različitim vrstama cyber prijetnji. To znači da su organizacije i pojedinci podložni krađi identiteta, pokušajima iznude ili gubitku važnih podataka i informacija. Sigurnost informacija više nije samo tehničko pitanje, već strateški dio strategije poslovanja svake organizacija bilo da je mala, srednja ili velika. Svaka organizacija, bez obzira na veličinu ili djelatnost, izložena je cyber prijetnjama koje mogu ozbiljno ugroziti njezinu reputaciju, finansijsku stabilnost i operativnu sposobnost. Cyber sigurnost predstavlja ključni segment informacione sigurnosti, fokusiran na zaštitu digitalnih podataka i infrastrukture. Cyber sigurnost obuhvata zaštitu tehničkih komponenti kao što su: radne jednice (PC), serveri, mobilni uređaji, kompjuterske mreže, te podaci od zlonamjernih napada[75]. Sve veća važnost kibernetičke sigurnosti u digitalnom dobu višestruko je pitanje koje obuhvaća tehnološke, organizacijske i dimenzije nacionalne sigurnosti, a sve veće oslanjanje na I[76]T i evoluirajuća priroda kibernetičkih prijetnji zahtijevaju proaktivan i prilagodljiv pristup kibernetičkoj sigurnosti.

CYBER SIGURNOST JE PROCES, A NE PROIZVOD!

Najveći izazov u cyber sigurnosti dolazi iz kontinuiranog razvoja tehnologije, što omogućava raznim kriminalcima rastuću paletu mogućnosti za zloupotrebu opreme i aplikacija. Osim toga, razne skupine kriminalaca neprestano razvijaju nove metode za izvođenje napada, što dodatno komplicira situaciju. Cyber sigurnost postaje najvažniji poslovni zahtjev za organizacije koje svoje poslovne procese prebacuju na online platforme, dok ljudi postaju ovisni o tehnologijama poput mobilnih uređaja, računara, tableta i interneta. Značaj cyber sigurnosti leži u potrebi za očuvanjem privatnosti i sigurnosti informacija, podataka i uređaja. U današnjem digitalnom dobu, cyber prijetnje postaju sve učestalije, stoga se posvećuje posebna pažnja u planiranju cyber sigurnosti. Cyber sigurnost često se smatrala isključivo tehnološkim problemom za koju je bio zadužen informatički (IT) odjel sa svim tehnološkim rješenjima koje je posjedovao u tom trenutku, a bio je odvojen od osnovnog poslovanja organizacije. Danas je cyber sigurnost mnogo više od IT problema. Sigurnost je odgovornost korporativnog upravljanja i top menadžmenta organizacije,"**ona je poslovni zahtjev, a ne tehničko pitanje"**. Sama cyber sigurnost treba biti

[75] Termin „cyber" (sajber; kibernetski / kibernetički prostor; eng. Cyber (space)) se koristi u ovom dokumentu i označava prostor koji je široko rasprostranjen i međupovezan digitalnim tehnologijama, uspostavljen uz pomoć i posredovanje kompjutersko-digitalne tehnologije. Pojam cyber prostor se danas koristi za sve što je na Internetu.

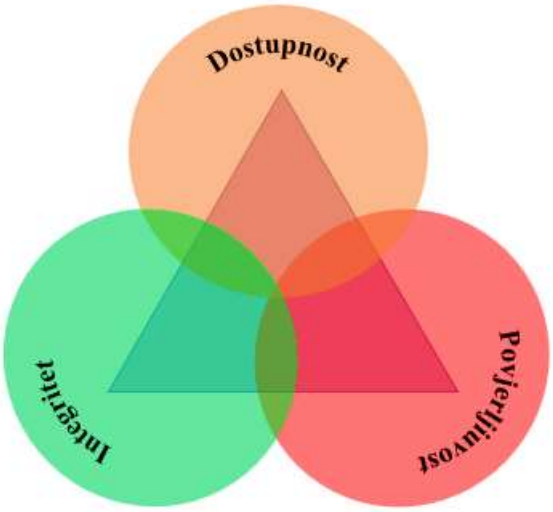
[76] Abrahams, T.O., et.all.: a review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection, Computer Science & IT Research Journal 5(1), 2024., p.3

integrisana u strateško planiranje i upravljanje organizacije kako bi se potaknula odgovornost svih zaposlenih u implementaciji sigurnosnih pravila i propisa koji sprečavaju sve vrste cyber napada. Ona zahtjeva uključivanje svih sektora i višeg rukovodstva u planiranje, implementaciju, kontrolu i unapređenje, te uspostavu politika, procedura za osiguranje cyber sigurnosti. Kada cyber sigurnost postane integrisani dio poslovne strategije i upravljanja organizacijom, svaki zaposlenik preuzima odgovornost za zaštitu podataka i informacija, što doprinosi ukupnoj sigurnosti organizacije u digitalnom okruženju.

Definicija cyber sigurnosti, kako je navedena u britanskoj strategiji „UK National Cyber Security Strategy 2016 – 2021" glasi: cyber sigurnost referira na zaštitu informacionih sistema (hardware, software i ostalih povezanih struktura), podataka na njima i usluga koje oni pružaju kako bi se mogli spriječiti neautorizovani upadi, pravljenje štete i pogrešna praksa[77]. Cyber sigurnost ne bi mogla egzistirati bez informacione sigurnosti, koja je zapravo proizašla kao specifična grana informacione sigurnosti, a danas je ključni elemenat u svakoj strategiji poslovne i nacionalne sigurnosti. Da bi se shvatila cyber sigurnost u potpunosti, bitno je prvo razumjeti pojam informacione sigurnosti. Informaciona sigurnost obuhvata skup mjera, politika, procedura i tehnologija koje se koriste za zaštitu povjerljivosti, integriteta i dostupnosti informacija (CIA trokut). CIA trokut je koncept u informacionoj sigurnosti koji predstavlja tri ključne komponente sigurnosti informacija:

- Povjerljivost (eng. **C**onfidentiality): Zaštitu informacija od neovlaštenog pristupa ili otkrivanja. Cilj je osigurati da samo ovlaštene osobe imaju pristup osjetljivim informacijama.
- Integritet (eng. **I**ntegrity): Odnosi se na zaštitu integriteta informacija, što znači osiguravanje da informacije ostanu netaknute, neizmijenjene i vjerodostojne tokom prijenosa ili pohrane.
- Dostupnost (eng. **A**vailability): Osiguranje da su informacije dostupne onima kojima su potrebne. To uključuje sprečavanje bilo kakvih prekida u pružanju usluga ili blokiranje pristupa informacijama u realnom vremenu.

[77]https://assets.publishing.service.gov.uk/media/5a81914de5274a2e8ab54ae9/national_cyber_security_strategy_2016.pdf



Shema 1: CIA trokut
Izvor:Autori rada

Informaciona sigurnost i osiguranje informacija postaju sve važniji u eri u kojoj mnoge organizacije informacije prepoznaju kao ključnu imovinu.[78] Sa razvojem digitalne tehnologije, nastaju različite vrste sigurnosti koje su prilagođene specifičnim izazovima i potrebama poslovnog okruženja. Osim klasičnih aspekata informacione sigurnosti, kao što su zaštita podataka i prevencija neovlaštenog pristupa, pojavljuju se i nove vrste sigurnosti kao što su računarska sigurnost, mrežna sigurnost, sigurnost protoka informacija i sigurnost informacionih sistema. Današnji poslovni sektor sve više ovisi o korporativnoj sigurnosti, koja se sve više usmjerena na zaštitu od cyber prijetnji, te se stvaraju posebni odjeli korporativne sigurnosti sa naglaskom na cyber zaštitu. Korporativna sigurnost je ključna poslovna funkcija koja se bavi zaštitom zaposlenih, imovine i poslovnih aktivnosti unutar velikih poslovnih sistema. Obzirom na brze promjene u savremenom poslovnom i tehničkom okruženju uzrokovane različitim faktorima, rizici i prijetnje postaju sve veći i nepredvidljivi.

Zbog toga korporativna sigurnost obuhvata širok spektar zaštitnih aktivnosti, uključujući otkrivanje i sprečavanje korporativnog kriminala, upravljanje rizicima te zaštitu imovine, zaposlenih, poslovne tajne i intelektualnog vlasništva. Cilj joj je osigurati vitalne vrijednosti organizacije u skladu sa važećim zakonima, što je ključno za njezinu ulogu u sigurnosti poslovanja. Tokom proteklih dvadeset godina, cyber prostor postao je ključno okruženje za poslovanje. Internet je postao dio svakodnevnog života za mnoge ljude, kako privatno tako i poslovno. U

[78] Cherdantseva Y., Hilton, J: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals, In book: Almeida, F. and Portela, I.(eds.), Organizational, Legal, and Technological Dimensions of IS Administrator, IGI Global Publishing, 2013, p.2

poslovnom svijetu, cyber prostor predstavlja široko prihvaćeno područje za bržu i naprednu komunikaciju. Istraživanja Microsofta i nezavisnih istraživačkih organizacija već dugi niz godina upozoravaju na povećanu ranjivost organizacija i privatnih korisnika na internetu. Nažalost, cyber napadi su postali svakodnevni dio života za svakog korisnika, utičući na milijarde ljudi širom svijeta.

RAZVOJ CYBER PRIJETNJI

Razvoj cyber prijetnji je nepredvidljiv proces koji se kontinuirano mijenja kako tehnologija napreduje. Obzirom na to odakle dolaze, cyber prijetnje možemo svrstati u tri grupe:

- U prvoj grupi se nalazimo mi kao pojedinci i često smo sami sebi najveća prijetnja. „Loše" lozinke, „namjerni ili nenamjerni" klik, neadekvatno upravljanje korisničkim računima, nedostatak ulaganja u sigurnosne tehnologije i aplikacije.
- Druga skupina su napadači izvana koji nisu zaposleni ili povezani sa organizacijom. Oni mogu biti pojedinci, kriminalne skupine, hakerski kolektivi (skupine). Motivi napada na organizaciju mogu biti različiti od finansijskih do političkih.
- Ciljani napadi su treća kategorija cyber prijetnji a odnose se na cyber napade u svrhu špijunaže, sabotaže, destabilizacije ili čak kao sredstvo cyber ratovanja. Takvi napadi često imaju visoku razinu tehničke sofisticiranosti i mogu biti usmjereni na kritičnu tehnološku infrastrukturu.

Organizacije trebaju identificirati potencijalne prijetnje koje dolaze iz svake od ovih skupina i preduzeti odgovarajuće mjere kako bi se zaštitile od njih. Ovo uključuje obrazovanje zaposlenih o cyber sigurnosti, uspostavu politika i procedura zaštite od prijetnji, kao redovno praćenje i nadogradnju sigurnosnih mjera.

CYBER SIGURNOST – KLJUČNI POSLOVNI RIZIK

Bitno je prepoznati, analizirati, te pripremiti prevenciju za moguće prijetnje i ranjivosti koje bi mogle ugroziti imovinu organizacije. Procjena i upravljanje rizicima omogućuju određivanje prioriteta u sigurnosnim naporima i raspodjeli resursa temeljem vjerojatnosti i uticaja rizika. Cyber sigurnost predstavlja ključni poslovni rizik u današnjem digitalnom dobu zbog:

- Finansijskih gubitaka
- Gubitak povjerenja kupaca
- Pravni i regulatorni problemi
- Gubitak intelektualnog vlasništva
- Prekid poslovanja

Važno je da organizacije prepoznaju cyber sigurnost kao ključni poslovni rizik i preduzmu sve potrebne mjere kako bi se zaštitile. Pojavljivanjem novih uređaja na mreži, te njihovim povezivanjem sa drugim uređajima pospješuje se područje napada u djelokrugu cyber sigurnosti. Sve veća zastupljenost „internet stvari", računara u oblaku, sistema velikih podataka te

digitalizacije poslovanja, eksponiraju se slabe točke sistema, čime se u opasnost dovodi veći broj žrtava. Sve je teže biti ukorak sa napadima obzirom na njihovu sve veću sofisticiranost.[79]
Primarni cilj hakera varira ovisno o motivaciji i vrsti napada. Umjesto toga, pokušavaju doći do osjetljivih informacija potrošača koje organizacija posjeduje, poput IBAN-a, JMB-a, brojeva kreditnih kartica i drugih osjetljivih podataka. Mnoge organizacije pružaju usluge putem interneta, te čuvanje ovakvih podataka postaje obaveza. Ova vrsta informacija postala je vrlo tražena roba na crnom tržištu, gdje hakeri mogu prodati te podatke organizacijama ili pojedincima koji su spremni platiti više.

VAŽNOST CYBER SIGURNOSTI ZA POSLOVANJE

U digitalnom dobu, svi od pojedinaca do velikih organizacija mogu postati meta cyber napada.Napadi postaju sve raširenij i sofisticiraniji, dok kriminalci stalno traže nove načine za napad. Takvi napadi rezultiraju gubitkom povjerljivih podataka, gubitkom povjerenja korisnika, a u ekstremnim slučajevima mogu ugroziti i samu fizičku sigurnost pojedinca. Cyber sigurnost je ključna za poslovanje jer štiti podatke i povjerenje kupaca, čuva reputaciju i brend, osigurava usklađenost sa zakonskim propisima, štiti finansijska sredstva te osigurava kontinuitet poslovanja. Osiguranje cyber sigurnosti nije samo trošak novca; to je ključni korak prema održavanju stabilnosti, reputacije i dugoročnog uspjeha bilo koje organizacije. Mnoge organizacije podliježu strogim propisima o zaštiti podataka, poput Opšte uredbe o zaštiti podataka (GDPR) u Europskoj Uniji ili Zakona o zaštiti privatnosti potrošača (CCPA) u SAD-u. Osiguranje cyber sigurnosti pomaže organizacijama da zadovolje ove zahtjeve i izbjegnu kazne za nepoštivanje propisa.

STRATEŠKI CILJEVI CYBER SIGURNOSTI

Strateški cilj Bosne i Hercegovine je priključenje EU kroz pristupne pregovore do punopravnog članstva. Jedan od elemenata koji treba ispuniti tokom ovog procesa je adekvatan nivo cyber sigurnosti. Strateški ciljevi provode se kroz odgovarajuće legislativne, regulatorne i operativne mjere sa ciljem dostizanja i održavanja visokog nivoa sigurnosti informaciono-komunikacionih sistema. Strategije za cyber sigurnost koje bi se usvojile na svim nivoima vlasti, u skladu sa ustavnim i zakonski definisanim nadležnostima, treba minimalno da sadrže navedene strateške ciljeve[80]:

1. Osiguran sistematski pristup harmonizaciji i izradi zakonodavstva u oblasti cyber sigurnosti
2. Zaštićeni informaciono-komunikacioni sistemi za pružanje ključnih usluga
3. Podizanje nivoa svijesti i znanja o cyber sigurnosti

[79] European Union Agency for Network and Information Security ENISA (2019). Threat Landscape Report 2018 – 15 Top Cyberthreats and Trends. Preuzeto s https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[80] SMJERNICE ZA STRATEŠKI OKVIR CYBER SIGURNOSTI U BOSNI I HERCEGOVINI https://www.osce.org/files/f/documents/4/8/438386.pdf

4. Uspostavljena tijela zadužena za osiguranje, jačanje i poboljšanje cyber sigurnosti
5. Poboljšana sigurnost i otpornost informaciono-komunikacionih sistema
6. Ojačani kapaciteti za borbu protiv cyber kriminala
7. Uspostavljena efikasna saradnja u oblasti cyber sigurnosti u međunarodnim, regionalnim i domaćim okvirima
8. Izgrađeni kapaciteti za adekvatan odgovor na krizne situacije
9. Uspostavljeno javno-privatno partnerstvo.

Evropske direktive (NIS 2)

U doba sve veće digitalizacije, osiguranje sigurnosti informacionih sistema postaje ključno za stabilnost i napredak društva. U skladu sa tim, Europska Unija je usvojila NIS 2 direktivu (Network and Information Security 2), proširenje prethodne NIS direktive iz 2016. godine[81].
Direktiva o sigurnosti mrežnih i informacionih sistema (NIS) uvedena je 2016. kao prva zakonodavna mjera na razini EU-a čija je svrha jačanje saradnje država članica u ključnom pitanju cyber sigurnosti. Utvrđene su sigurnosne obveze za operatere ključnih usluga (u najvažnijim sektorima poput energetike, prometa, zdravstva i finansija) te za pružaoce digitalnih usluga (internetska tržišta, tražilice i usluge u oblaku).

NIS 2 direktiva širi područje i unapređuje mjere zaštite kritičnih informacionih sistema i digitalnih usluga. Glavni cilj je osigurati visoku razinu sigurnosti i otpornosti informacionih sistema i infrastrukture kako bi se zaštitili građani, organizacije, kompanije i institucije od cyber prijetnji.[82]
NIS 2 direktiva, kao proširena od prethodne NIS direktive, donosi niz prednosti u jačanju cyber sigurnosti i zaštiti informacionih sistema u Evropskoj Uniji. Neke od glavnih prednosti uključuju:

- Prošireni opseg: Direktiva proširuje područje primjene i obuhvata veći raspon informacionih sistema i digitalnih usluga, uključujući i nove sektore poput dobavljača cloud usluga, online platformi i e-marketinga.
- Jačanje sigurnosnih mjera: Unapređenje mjera zaštite kritičnih informacionih sistema i digitalnih usluga, što pomaže u osiguravanju visoke razine sigurnosti i otpornosti na cyber prijetnje.
- Precizniji zahtjevi: NIS 2 direktiva detaljno opisuje procesne, tehničke i organizacijske zahtjeve sigurnosnih mjera, što olakšava njihovu implementaciju i osigurava ujednačeno usvajanje u državama članicama.
- Usklađenost sa standardima: Usklađenost sa standardima poput ISO 27001, što olakšava organizacijama da ispune sigurnosne zahtjeve i postignu visoku razinu cyber sigurnosti.

[81] NIS direktiva: (eng.) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (hr.) DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije
[82] https://eur-lex.europa.eu/eli/dir/2022/2555

- Jednoobrazna implementacija: NIS 2 direktiva osigurava ujednačenu implementaciju sigurnosnih mjera u svim državama članicama, što povećava učinkovitost i koherentnost zaštite informacionih sistema na razini EU.

Iako NIS 2 direktiva nudi niz prednosti, njena implementacija predstavlja izazov. Potrebno je osigurati dovoljno resursa i stručnjaka za provedbu propisanih sigurnosnih mjera. Također, važno je osigurati usklađenost državnih propisa sa evropskim standardima kako bi se izbjegli nesporazumi i nedoumice tokom primjene direktive.

Navedene mjere uključene su u NIS 2 direktivu:

a) Politike o analizi rizika i sigurnosti informacionih sistema,
b) Postupanje sa cyber incidentima,
c) Kontinuitet poslovanja, poput upravljanja sigurnosnim kopijama i obnovom sistema te upravljanje kriznim situacijama,
d) Sigurnost u opskrbnom lancu, uključujući aspekte sigurnosti vezane za odnose između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga,
e) Sigurnost u nabavi, razvoju i održavanju mrežnih i informacionih sistema, uključujući rukovanje ranjivostima i njihovo otkrivanje,
f) Politike i postupci za procjenu učinkovitosti mjera upravljanja rizikom cyber sigurnosti,
g) Osnovne prakse i obuka iz cyber sigurnosti,
h) Politike i postupci vezani uz korištenje kriptografije i, gdje je primjereno, šifriranje,
i) Sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom,
j) Korištenje autentifikacije as više faktora ili rješenja za kontinuiranu autentifikaciju, osigurane glasovne, video i tekstualne komunikacije te osigurani sistemi hitne komunikacije unutar subjekta, gdje je primjereno.

Kroz ove prednosti, NIS 2 direktiva doprinosi jačanju cyber sigurnosti u EU i osigurava bolju zaštitu informacionih sistema i digitalnih usluga od sve složenijih cyber prijetnji.

ZAKLJUČAK

Sa razvojem tehnologije dolazi i potreba za cyber sigurnosti. Ova sigurnost postaje ključni segment strategije poslovanja svake organizacije jer se suočava sa raznim cyber prijetnjama koje mogu ozbiljno ugroziti reputaciju, finansijsku stabilnost i operativnu sposobnost organizacije. Cyber sigurnost više nije samo tehničko pitanje, već je postala strateški dio poslovnih procesa svake organizacije. Cyber sigurnost se ne smatra samo tehničkim izazovom, već i poslovnim zahtjevom koji podrazumijeva uključivanje svih sektora i višeg rukovodstva u planiranje, implementaciju, kontrolu i unapređenje sigurnosnih politika i procedura. Ona zahtijeva integraciju u strateško planiranje i upravljanje organizacijom kako bi se potaknula odgovornost svih zaposlenih u implementaciji sigurnosnih pravila i propisa.

U digitalnom dobu, cyber sigurnost postaje ključni poslovni rizik zbog mogućih finansijskih gubitaka, gubitka povjerenja kupaca, pravnih problema, gubitka intelektualnog vlasništva i prekida poslovanja. Osiguranje cyber sigurnosti postaje vitalno za očuvanje stabilnosti, reputacije i

dugoročnog uspjeha organizacija. Kroz usvajanje i primjenu odgovarajućih mjera cyber sigurnosti, organizacije mogu zaštititi svoje podatke, povjerenje kupaca, reputaciju i finansijska sredstva, te osigurati kontinuitet poslovanja i usklađenost sa zakonskim propisima.

LITERATURA

1. Abrahams, T.O., et. all.: a review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection, Computer Science & IT Research Journal 5(1), 2024., p.1-25.
2. Cherdantseva Y., Hilton, J: Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals, In book: Almeida, F. and Portela, I.(eds.), Organizational, Legal, and Technological Dimensions of IS Administrator, IGI Global Publishing, 2013, https://www.researchgate.net/publication/283569185_Information_Security_and_Information_Assurance_The_Discussion_about_the_Meaning_Scope_and_Goals
3. Christensen, K. K., Liebetrau, T.: A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. Intelligence and National Security, *34*(3), 2019., 395-408.
4. CYBERSECURITY CAPACITY REVIEW, Bosnia and Herzegovina, Global Cyber Security Capacity Centre, mart 2019.
5. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022., https://eur-lex.europa.eu/eli/dir/2022/2555, pristupano 02.04.2024.
6. DIREKTIVA (EU) 2016/1148 EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS direktiva).
7. Dunn Cavelty, M., Wenger, A.: Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41*(1), 2020., p. 5-32.*
8. European Union Agency for Network and Information Security ENISA (2019). Threat Landscape Report 2018 – 15 Top Cyberthreats and Trends, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 , pristupano 31.03.2024.
9. Information security. Preuzeto sa https://en.wikipedia.org/wiki/Information_security
10. NCSS Good Practice Guide- Designing and Implementing National Cyber Security Strategies, 2016.
11. SMJERNICE ZA STRATEŠKI OKVIR CYBER SIGURNOSTI U BOSNI I HERCEGOVINI, https://www.osce.org/files/f/documents/4/8/438386.pdf , pristupano 01.04.2024.
12. Stubley, D. (2013, 2013-06-07). What is Cyber Security? https://www.7elements.co.uk/resources/blo g/what-is-cyber-security/ , pristupano 31.03.2024.

13. UK National Cyber Security Strategy 2016 – 2021. https://assets.publishing.service.gov.uk/media/5a81914de5274a2e8ab54ae9/national_cyber_security_strategy_2016.pdf , pristupano 28.03.2024.