DOI 10.7251/ZRSNG2525047M

Cybersecurity u kontekstu održivog poslovanja i zaštite podataka
Cybersecurity in the Context of Sustainable Business Operations and Data Protection.

Srđan Mičić, Federalna uprava policije Sarajevo/Directorate of Fedral Police Sarajevo

Sažetak **– Kako se digitalna tehnologija ubrzano razvija, tako rastu rizici i prijetnje od njene zloupotrebe. Obzirom da poslovni modeli u današnje vrijeme sve više zavise od digitalizacije i tehnoloških napredaka to ih izlaže povećanim rizicima u oblasti cyber bezbjednosti, kao i u očuvanju privatnosti njhovih podataka. Veliki dio kompanija su prepoznale ozbiljnost prijetnji cyber kriminala, te su dale značaj cyber bezbjednosti u svom poslovanju, što je dovelo do smanjenja rizika od cyber napada u velikoj mjeri i kopmpromitacije njihovih podataka, ali uprkos tome neke od njih nisu uspjele da se u potpunosti zaštite. Ovaj rad pored strategije i organizacionih mjera bezbjednosti koje kompanije mogu implementirati kako bi smanjile rizike i osigurale bezbjednost u svom radu, kako informacionog sistema tako i podatka, istražit će vrste i načine izvšenja cyber napada na kompanije. Istraživanje pokazuje da je jedan bitan segment bezbjednosti u kontekstu održivog poslovanja i zaštite podataka, kreiranje i implementacija bezbjednosnih politika koje se odnose na postupanje po procedurama od strane uposlenika koji u svom radu imaju pristup poslovnim podacima, kao i onih koji su zaduženi za informacionu bezbjednost kompanije.**

Ključne riječi **- Cyber bezbjednost, zaštita podataka, bezbjednosne politike, održivost poslovanja**

Abstract **– As digital technology rapidly evolves, the risks and threats of its misuse also increase. Since modern business models increasingly rely on digitalization and technological advancements, they are exposed to heightened risks in the field of cybersecurity, as well as in the protection of their data privacy. A significant number of companies have recognized the seriousness of cybercrime threats and have prioritized cybersecurity in their operations. This has significantly reduced the risks of cyberattacks and data compromise. However, despite these efforts, some companies have not been able to fully protect themselves. This paper, in addition to examining strategies and organizational security measures that companies can implement to minimize risks and ensure the security of both their information systems and data, will also explore the types and methods of cyberattacks targeting companies. The research demonstrate that a crucial aspect of security in the context of sustainable business operations and data protection is the creation and implementation of security policies. These policies pertain to compliance with procedures by employees who have access to business data in their daily work, as well as those responsible for the company's information security.**

Keywords **- Cybersecurity, data protection, security policies, business sustainability**

I. UVOD

U savremenoj digitalizaciji, poslovni modeli se velikom brzinom transformišu u skladu napretkom digitalizacije ka održivim praksama koje podrazumevaju korišćenje tehnologije za pobollšanje resursa i efikasnosti.

Nakon procesa digitalizacije zamjena postojećih analognih poslovnih rješenja digitalnima, u svrhu uvođenja digitalnog načina poslovanja kao jedne od aktivnosti digitalne transformacije. U posljednje vrijeme se sve češće spominje digitalna transformacija koja utiče na sve sektore privrede i mijenja način poslovanja i komunikacije. Digitalna transformacija se odnosi na proces koji započinje od trenutka kada kompanija počne razmišljati o uvođenju digitalnih tehnologija u svim područjima poslovanja i traje do trenutka njihove potpune integracije. Navedeni proces često ne prati adekvatna edukovanost u pogledu informatičkog znanja uposlenika kompanija što dovodi do određenih bezbjednosnih propusta. Takođe, nepostojanje adekvatnih internih procedura kod kompanija, kao i na nacionalnom nivou može dovesti do raznih bezbjedonosnih propusta, što bi značilo da digitalna transformacija uključuje i pojedince, nije dovoljno samo uvesti digitalnu tehnologiju u poslovanje, važno je i educirati uposlenike kompanije.

Kako je sama digitalna transformacija proces uvođenja digitalnih tehnologija u sve segmente poslovanja,

mijenjajući iz korijena poslovne procese i navike, može se sa sigurnošću reći da se radi i o određenoj kulturnoj promjeni u kojoj se neprestano mijenjamo, prilagođavamo promjenama i razvijamo.[1]

Sa porastom digitalizacije raste i rizik od cyber napada koji mogu da naruše bezbjednost podataka kompanije, ometanje u radu kompanije i ponekad i prekid rada kompanije. Ovi napadi su sve više sofisticiraniji a na njihovoj meti su kompanije širom svijeta te usljed napada često pretrpe velike finansijske gubitke, postanu nepouzdane klijentima a neke i trajno obustave svoj rad. Cilj ovog rada je da istraži cyber bezbjednost i privatnost podataka doprinose održivosti poslovnih modela i koje strategije kompanije mogu koristiti za umanjenje rizika od navedenih aktivnosti.[2]

II. CYBER BEZBJEDNOST KAO KLJUČNI FAKTOR ODRŽIVOSTI

U pogledu definisanja značenja termina "Cyber bezbjednosti", pored već poznatih definicija, najjednostavnije objašnjenje je da je cilj bezbjednosti da spriječi ono sto nije dozvoljeno. Ova jednostavna definicija krije u sebi pitanje: A šta to nije dozvoljeno? To zavisi od kompjuterskog sistema koji se štiti i treba biti definisano individualno za svaki takav sistem zavisnosti od potreba kompanije[3].

Cyber bezbjedonst se odnosi na praksu zaštite kompjuterskih mreža, sistema i podataka od digitalnih napada. Ove pretnje mogu dovesti do finansijskih gubitaka, gubitka poverenja korisnika i pravnih posledica.

Kompanija koja je vlasnik podataka, odnosno odgovorna lica koja donose odluke u organizaciji, određuju kome i šta je dozvoljeno raditi sa tim podacima. Dokument kojim se ovo iskazuje i koji je polazište za sve što se tiče bezbjednosti je bezbjedonosna politika.

Bezbjedonosna politika opisuje željeno stanje kompjuterskog sistema sa aspekta bezbjednosti. Bezbjednosna politika u principu navodi šta je dozvoljeno, a šta nije. U nekoj kompaniji ova politika može navesti da samo generalni i finansijski direktor imaju pristup informacijama o trenutnom stanju računa. Bezbjedonosna politika se ne bavi načinima na koje se postiže da se u navedenom sistemu dešavaju samo dozvoljene stvari.

III. RIZICI I PRETNJE

Kompamije širom svijeta su izložene stalnim rizicima i prijetnjama od cyber napada. Postoji veliki broj vrsta cyber napada nastavku će biti prikazani najćešći napadi:

Ransomware napadi

Ransomware je vrsta zlonamjernog softver-programakoji se može na više načina instalirati u kompjuterski sistem jedne kompanije, a ima zadatak da kriptuje "zaključa" podatke podatke kompanije. Nakon čega napadač traži novac od kompanije u zamjenu za enkripcijski ključ. Neki od načina instaliranja navedenog programa:

- Slanjem programa u skrivenoj datoteci putem e-maila (najčešči). Kada korisnik otvori e-mail poruku u pozadini koju on ne primjeti se instalira navedeni program i počinje da kriptuje(zaključava podatke), te ostvaruje komunikaciju sa napadačem preko "remote control"-daljinskog pristupa.
- Instaliranjem programa kroz bezbjedonosni propust u sistemu. Kada u sistemu postoji bezbjedonosni propust (propust u operativnom sistemu) koji napadač iskoristi i neovlašteno se uključi u sistem i pokrene instalaciju.
- Instaliranje putem USB Memorijskog uređaja ili drugih vrsta pokretne memorije od strane uposlenika kompanije.

Phishing napadi

Phishing napad se vrši uz pomoć socijalnog inžinjeringa putem kojeg se imitira određeni korisnički račun te se korisniku imitacija izgleda korisničkog računa "nameće" kako bi isti upisao korisničko ime i lozinku. Neki od načina realizacije phishinga su:

Slanje linka putem e-maila, kada korisnik pokrene link na ekranu mu se pojavi izgled nekog od servisa na koji je potrebno upisati pristupne podatke u imitirani elektronski formular, te nakon upisa i pokušaja pristupanja navedeni podaci se dostavljaju napadaču. Navedeni elektronski formular u većini slučajeva bude identičan pravom elektronskom formularu.

Neovlaštenim pristupom u lokalnu LAN ili WiFi mrežu kroz koju se targetira računar u mrežnom sistemu te se usmjerava napad na njega, na način da mu blokira komunikaciju sa ostalim mrežnim uređajima dok ne unese pristupne podatke.

DDoS napadi

DDoS (Distributed Denial of Service) napadi su vrsta cyber napada u kojem napadači putem botnet (mreže zaraženih uređaja) salju veliki broj upita na server, mrežu ili uslugu, čime ometaju normalan rad i onemogućavaju pristup legitimnim korisnicima. Neki od načina realizacije DdoS napada su:

- Slanjem velikog broja zahtjeva prema cijelokupni mrežni sistemu u kompaniji, s ciljem ometanja ili onemogućavanja istog.

- Slanjem velikog broja zahtjeva prema određenom softveru-aplikaciji u mrežnom sistemuna kojoj je od strane napadača identifikovana ranjivost-propust.

BEC Prevare

BEC (Business Email Compromise) prevara kojoj napadač upotrebljava e-mail poštu da bi naveo nekoga da izvrši uplatu novca ili otkrije povjerljive podatke o kompaniji. Napadač se predstavlja kao osoba od povjerenja, a zatim traži da se plati lažna faktura ili da se predaju povjerljivi podaci koje može iskoristiti u drugoj prevari. Sve je više prijevara BEC jer sve više zaposlenika radi na daljinu. Tokom 2021 godine FBI primio gotovo 20 000 prijava o BEC-u [4]. Neki od načina izvršenja navedene prevare:

- Neovlaštenim pristupom poslovnom e-mail korisničkom računu s ciljem aktiviranja opcije "Forward" za preusmjere odlazno dolazne pošte na e-mail napadača.
- Neovlaštenim pristupom serveru gdje je smješten e-mail korisnički račun firme, s ciljem praćenja e-mail korespondencije kompanije sa klijentima.

IV. STRATEGIJE ZAŠTITE

Bezbjedonosne politke kompanija, odnosno postojanje jasnih pravila i procedura za korištenje informacionog sistema su ključni element zaštite. Navedenim politikama se definišu postupci prilkom uključivanja u sistem, vršenja obrade podataka kao i sve druge radnje koje su usmjerene na odnos uposlenika kompanije i podataka, odnosno informacionig sistema kompanije kojem uposlenik ima pristup. Višefaktorska autentifikacija (MFA) – Dodatni slojevi bezbjednosti pri pristupu sistemima, osigurava zaštitu od neovlaštenog pristupa zaštićenom sistemu[4]. Ograničavanje pristupa podacima ili dijelu mrežnog sistema kompanije odrerđenim korisnicima od strane administratora sistema je takođe bitan element zaštite što se takođe definiše bezbjednosnim politikama kroz nivoe pristupa u zavisnosti od potreba radnog mjesta uposlenika.

V. PRIVATNOST PODATAKA I REGULATIVA

Klijenti od kompanija očekuju visoke standarde zaštite njihovih podataka, što u velikoj mjeri utiče na poslovnu reputaciju kompanija i njihovu održivost u daljem radu.U pogledu regulacije zaštite privatnosti podataka na međunarodnom nivou postoje okviri koji regulišu zaštiru privatnosti podataka:

- GDPR (General Data Protection Regulation) – Evropskaregulativa koja zahteva transparentnost i odgovornost u obradi podataka[5].
- CCPA (California Consumer Privacy Act) – Američki zakon koji reguliše upotrebu i čuvanje podataka korisnika[6].
- ISO 27001 – Međunarodni standard za upravljanje informacionom sigurnosti[7].

Kada je riječ o tehnološkom rješenju za zaštitu privatnosti podataka uglavnom se govori o enkripcija podataka koja sigurava da su podaci neupotrebljivi u slučaju neovlašćenog pristupa, te o određenim softverskim alatima koji bi prepoznali i alarmirali administratora u slučaju sumnjivih aktivnosti.

VI. ODRŽIVOST KROZ EDUKACIJU I UPRAVLJANJE RIZICIMA

Izrada tkz. "Backupa" rezervne kopije podataka kopanije, spriječilo bi gubitak istih u slučaju cyber napada ili eventualnog usled incidenta koji nemaju veze sa cyber napadom (kvar na serveru i sl.), a gubitak podataka bi kompanija pored narušenog povjerenja kod klijenatra mogao da ugrozi dalji rad u tehničkom smislu.

Kako je ljudski faktor je najčešći uzrok bezbjedonosnih incidenata, redovne obuke i simulacije incidenata mogu značajno smanjiti broj uspešnih cyber napada. Kontinuirana edukacija o cyber prijetnjama i podizanje svjesti uposlenika u kompaniji je od važnog značaja. Konstantno unaprijeđenjebezbjedonosnih politika, znatno bi smanjilo rizik od cyber napada. Rad na procijeni rizika s ciljem identifikacije bezbjedonisnih propusta i bi u znatnoj mjeri doprinjeo u prevenciji i sprječavanju napada.[8]

Takođe, izradom "Incident response plan" – Plan reagovanja na cyber napade, napravila bi se procedurakoja bi za cilj imala adekvatan odgovor na napad, kao i poduzamnje daljih mjera i radnji s ciljem se minimiziranja štete. [9] Angažmanom spoljih saradnika-kompanija koje se bave cyber bezbjednošću u pogledu identifikacije bezbjedonosnih propusta u sistemu, kao i eventualne sanacije načinjene štete nakon napada može pružiti veliku pomoć kompanijama.

VII. ZAKLJUČAK

Cyber bezbjednost i privatnost podataka su ključni elementi održivih poslovnih modela nakon transformacije iz analogne u digitalni način poslovanja. Implementacija regulativa, bezbjedonosnih politika, tehnoloških rješenja i edukacija zaposlenih doprinosi dugoročnoj stabilnosti kompanija, odnosno njihovoj cyber bezbjednosti. Važno je naglasiti značaj i ulogu administratora mrežnog sistema, kao i bezbjedonosnih politika kompanije u očuvanju bezbjedonosnog sistema na nivou kopanije. Kao što smo već pomenuli da je u većini slučajeva uzrok incidenta greška ljudskog faktora, nakon implementacije bezbjedonosnih politika u kompaniji neophodan je kontinuiran nadzor nad

sprovođenju i poštivanju istih od strane rukovodilaca i uposlenika. Takođe je potrebno redovno raditi na podizanju svjesti kod uposlenika s ciljem prevencije, te njihovog ozbiljnijeg pristupa samom problemu. Kako je cyber kriminal materija koja svakim danom evaluira i mjenja svoj oblik stoga je potrebno njegovo stalno prećenje, kao i upoznavanje uposlenika novim načinima izvršenja cyber napada.

REFERENCES

[1] https://www.nos.hr/digitalna-transformacija-poslovanja
[2] Smith, J., & Brown, L. (2022). "The Role of Cybersecurity in Sustainable Business Models". Journal of Cyber Security Studies
[3] Saša Mrdović, Sigurnost računarskih sistema (2014).
[4] https://www.ic3.gov/AnnualReport/Reports/2021_ic3rep ort.pdf
[5] European Union. (2016). General Data Protection Regulation (GDPR).
[6] California Legislative Information. (2018). California Consumer Privacy Act (CCPA).
[7] International Organization for Standardization. (2013). ISO/IEC 27001: Information Security Management Systems.
[8]https://cybersecurity.ba/jacanje-cyber-sigurnosti-kroz-viseslojnu-zastitu/
[9] https://www.dataguard.com/cyber-security/incident- response-plan/