Originalni naučni rad
UDK 336.7:005.915]004
DOI 10.7251/BLCZR0723109B

KIBERNETIČKA SIGURNOST U BANKARSTVU: ANALIZA IZAZOVA I STRATEGIJA ZA ZAŠTITU FINANCIJSKIH INSTITUCIJA

Marija Boban[1]
Vedran Uroš[2]
Tomislav Jurić Ćivro[3]

SAŽETAK

Ovaj rad govori o značaju kibernetičke sigurnosti u bankarskom sektoru. Kao rezultat osjetljivih podataka kojima banke rukuju i prirode njihovog poslovanja, bankarska industrija vrlo je ranjiva na kibernetičke napade. U radu su opisane različite vrste kibernetičkih prijetnji na koje su banke osjetljive te se pojašnjava potencijalni utjecaj takvih prijetnji na bankovni sustav. Naglašava se potreba za uvođenjem i primjenom snažnih mjera kibernetičke sigurnosti u cilju sprječavanja neovlaštenog pristupa, povrede podataka i financijskih gubitaka. Dodatno, ističe se važnost obuke i svijesti zaposlenika u smanjenju rizika od kibernetičkih napada. U radu se prolazi i kroz razloge zašto bi kibernetička sigurnost trebala biti jedan od glavnih prioriteta u bankarskom sektoru, kako bi se održao kredibilitet banaka i očuvalo povjerenje njihovih klijenata. Cilj ovog rada je prikazati pregled onoga što podrazumijevamo pod pojmom kibernetike te njezin utjecaj na bankarski sektor, isto tako pojasniti temeljne principe kibernetike i identificirati izazove s kojima se banke susreću pri implementaciji ovog oblika sigurnosti. Osim toga, u ovom radu se raspravlja o strategijama koje banke koriste kako bi osigurale uspješnu implementaciju kibernetike i zaštitile vlastite operacije te osjetljive podatke svojih klijenata.

KLJUČNE RIJEČI: *bankarski sektor, kibernetika, kibernetički kriminal, kibernetički napad, kibernetička sigurnost*

1 Prof. dr. sc. Marija Boban, redovita profesorica - Sveučilište u Splitu - Pravni fakultet – Split, Hrvatska – mboban@pravst.hr

2 Vedran Uroš - univ.mag.ing.comp v.pred. – Veleučilište „Marko Marulić“ u Kninu – Knin, Hrvatska – vuros@veleknin.hr

3 Tomislav Jurić Ćivro – diplomant - Veleučilište „Marko Marulić“ u Kninu – Knin, Hrvatska tomislavkomi@gmail.com. Ovaj rad je pisan temeljem istraživanja i prema obranjenom završnom radu: Kibernetička sigurnost u bankarstvu: analiza izazova i strategija za zaštitu financijskih institucija, 6.2024.

CYBER SECURITY IN BANKING: ANALYSIS OF CHALLENGES AND STRATEGIES FOR THE PROTECTION OF FINANCIAL INSTITUTIONS

SUMMARY

This paper discusses the importance of cyber security in the banking sector. As a result of the sensitive data that banks handle and the nature of their business, the banking industry is highly vulnerable to cyber attacks. The paper describes the different types of cyber threats to which banks are sensitive and explains the potential impact of such threats on the banking system. The need to introduce and apply strong cyber security measures in order to prevent unauthorized access, data breach and financial losses is emphasized. Additionally, the importance of employee training and awareness in reducing the risk of cyberattacks is emphasized. The paper goes through the reasons why cyber security should be one of the main priorities in the banking sector, in order to maintain the credibility of banks and preserve the trust of their clients. The aim of this paper is to present an overview of what we mean by the term cybernetics and its impact on the banking sector, as well as clarify the fundamental principles of cybernetics and identify the challenges that banks face when implementing this form of security. In addition, this paper discusses the strategies that banks use to ensure the successful implementation of cyber and protect their own operations and the sensitive data of their customers.

KEY WORDS: *banking sector, cybernetics, cybercrime, cyberattack, cyber security*

UVOD

Porast korištenja interneta, digitalnih usluga, te sam razvitak tehnologije rezultirao je optimalnom prilikom za razvojem i pokušajima kibernetičkih napada. Kada je riječ o kibernetičkim napadima ključnu ulogu imaju računala, te su samim tim računala meta kibernetičkih napada, a isto tako se koriste kao glavni alat u samom napadu. Odnosno, svako računalo ili neki drugi uređaj spojen na internet, predstavlja potencijalnu metu kibernetičkog napada. Sama definicija kibernetičkih napada podrazumijeva svaki postupak neke osobe ili organizacije koji u cilju ima napad na informacijske sustave, od pojedinačnih osobnih uređaja do velikih infrastruktura, poput cijele države, pri kojemu se krši jedno od načela na kojima se temelji informacijska sigurnost (Al-Zaidy, 2014).

Rast i razvoj država temelji se na ekonomiji i gospodarstvu, u čemu bankarstvo zauzima važnu ulogu. Korisnici diljem svijeta svakodnevno se služe bankarskim proizvodima i uslugama, osobito digitalnim uslugama koje banke pružaju u današnje vrijeme. Upravo zato, bankarska informacijska tehnologija (engl. *Information Technology*, u daljnjem tekstu: IT) mora se razvijati sukladno potrebama na tržištu. Kibernetički napadi u bankarskom sektoru mogu uzrokovati goleme štete pojedinačnih klijenata kao i velike monetarne gubitke koji mogu imati utjecaja na državnu ekonomiju.

BANKARSKI SEKTOR KAO META KIBERNETIČKIH NAPADA

Bankarski, sektor zauzima važno mjesto u suvremenom gospodarstvu zahvaljujući svojoj ulozi financijskog posredovanja, odnosno kanaliziranja sredstava od štediša prema ulagateljima. Zdrav i učinkovit bankarski sektor potiče akumuliranje štednje i omogućuje da se ona dodijeli najproduktivnijim ulaganjima, čime se potiču inovacije i gospodarski rast.

Banke su glavni financijski posrednici u svim europskim državama (European Commission, 2021).

Iza svih vrsta kriminalnih aktivnosti obično se kriju razni motivi. U slučaju bankarskog sektora takvih je motiva mnogo, obzirom da se radi o sektoru punom osjetljivih informacija i velikih količina novca. Stoga nije začuđujuće da je upravo bankarski sektor česta meta raznih pojedinaca i kriminalnih organizacija.

KIBERNETIČKA SIGURNOST

Obradović (2018) definira kibernetiku kao interdisciplinarnu znanost koja se bavi prijenosom informacija te upravljanjem živim organizmima i procesima s definiranim ciljem. Središnji državni ured za razvoj digitalnog društva (n.d.) definira kibernetičku sigurnost kao skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi. Kako navodi Prskalo (2022), u današnje vrijeme društvene i poslovne interakcije sve se češće odvijaju u kibernetičkom prostoru. Upravo zato, kibernetička sigurnost postaje sve važnija tema, ali i izazov suvremenog doba.

Zakoni o kibernetičkoj sigurnosti u Republici Hrvatskoj imaju za cilj osigurati zaštitu informacijskih sustava te podataka prijetnji i napada. Glavni zakon koji regulira područje kibernetičke sigurnosti u Hrvatskoj je Zakon o kibernetičkoj sigurnosti, koji je usklađen s europskim direktivama i standardima.

Kako se u članku 1. Zakona o kibernetičkoj sigurnosti (NN 14/2024) navodi „*Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti, kriteriji za kategorizaciju ključnih i važnih subjekata, zahtjevi kibernetičke sigurnosti za ključne i važne subjekte, posebni zahtjevi za upravljanje podacima o registraciji naziva domena i kontrola njihove provedbe, dobrovoljni mehanizmi kibernetičke zaštite, nadležna tijela u području kibernetičke sigurnosti i njihove zadaće i ovlasti, stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti, prekršajne odredbe, praćenje provedbe ovoga Zakona i druga pitanja od značaja za područje kibernetičke sigurnosti*."

Ovaj zakon propisuje obveze organizacija i pružatelja usluga informacijskih tehnologija u vezi sa zaštitom informacijskih sustava, obvezu prijavljivanja sigurnosnih incidenata, kao i postupke zaštite osjetljivih podataka. Također, spomenuti zakon predviđa sankcije za nepoštivanje propisanih mjera kibernetičke sigurnosti.

Uz Zakon o kibernetičkoj sigurnosti, u Republici Hrvatskoj postoje i drugi relevantni zakoni koji se bave povezanim područjima, poput Zakona o zaštiti osobnih podataka (NN 106/2012) i Zakona o elektroničkim komunikacijama (NN 73/2008), koji doprinose cjelovitom pravnom okviru za kibernetičku sigurnost.

Kroz ove zakone i institucionalne mehanizme, Republika Hrvatska nastoji osigurati adekvatnu razinu kibernetičke sigurnosti kako bi zaštitila svoje informacijske sustave i podatke od sve složenijih kibernetičkih prijetnji.

IZAZOVI KIBERNETIČKE SIGURNOSTI U BANKARSTVU

Suvremeni razvoj tehnologije odražava se na različite društvene i ekonomske aspekte (Njavro, 1989). Mikšić (1988) navodi kako se nove tehnologije trebaju promatrati iz per-

spektive organizacijskih metoda koje je potrebno dobro organizirati. Utjecaj digitalizacije, odnosno napredak tehnologije utjecao je na način života općenito. Isti je slučaj i kada je riječ o poslovanju. Razvoj novih usluga i proizvoda ne bi bio moguć bez primjene novih tehnologija. Ulaganje u nove tehnologije u poslovanju otvara mogućnosti pronalaska novih poslovnih i kadrovskih rješenja.

Zahvaljujući novim tehnologijama, danas možemo izvršavati različite bankovne transakcije bez fizičkog odlaska u poslovnice banke. Primjerice, u svakom trenutku možemo provjeriti stanje vlastitog računa, slati ili primati transakcije. Međutim, jedan od ključnih izazova koji se postavljaju pred banke postaje sigurnost i zaštita podataka. Internet kao javni medij nema formalne mehanizme kontrole. Odnosno, postoje rizici pokušaja prevare ili krađe podataka i sredstava. Banke se iz tog razloga koriste različitim algoritmima sa što sigurniji protok podataka

Kada je riječ o nezakonitim društvenim djelovanjima, kibernetički kriminal predstavlja jedan od najučestalijih djelovanja s kojim ne izostaju negativne posljedice koje nosi sa sobom (Hamidović i sur., 2016). Sve veći broj podataka, poput informacija o imovinskom, radnom ili zdravstvenom stanju stanovništva, pohranjuje se u informacijskim sustavima. Ti su podaci dostupni institucijama nadležnima za njihovu pohranu i obradu. Kada tim podacima pristupaju oni koji ih koriste neovlašteno u nezakonite svrhe, tada postaju ugrožene ne samo fizičke osobe, nego i vojni, vladini, financijski, privredni i drugi informacijski sustavi. Unatoč golemim naporima sigurnosnih agencija, ponekad se ni informacijski sustavi s najvišom razinom sigurnosti ne mogu oduprijeti kibernetičkim napadima (Hamidović i sur., 2016).

Ukoliko se radi o napadu na određeni ekonomski subjekt, takav napad može dovesti tvrtku u stečaj. Neka djela se izvode slučajno, neka se koriste u socijalne ili političke svrhe, dok su neki predmet studioznog proučavanja, planiranja i djelovanja profesionalnih kriminalaca. Definirati ovaj oblik kriminala je vrlo teško jer se radi o novom obliku kriminalnog ponašanja koji nije u potpunosti određen spram drugih oblika (Bača, 2004).

Bača, (2004) kibernetički kriminal dijeli u sljedeće kategorije:

- djela u kojima je kriminal bio povezan sa samim računalom (krađa računala, komponenti ili uništenje)
- računalo je okolina u kojoj je kriminal počinjen (krađa podataka, provale u računalo)
- računalo je alat ili instrument za izvođenje ili planiranje kriminala
- računalo se slučajno pojavljuje u drugim kriminalnim djelima ili se koristi kao simbol za zastrašivanje ili prijevaru“

Zlouporaba računala u kriminalne svrhe, kao što su komunikacija i pohrana podataka, predstavlja značajan izazov u društvenoj sferi, posebno u pogledu pronalaženja podataka i kriminalističkih istraga. Očekuje se da će prevalencija takvog kibernetičkog kriminala s vremenom nastaviti rasti.

KIBERNETIČKI NAPADI

Prijetnje kibernetičkoj sigurnosti postaju sve sofisticiranije, a kao što je već spomenuto, posljedice uspješnih napada mogu biti teške. Mogu uključivati financijske gubitke,

štetu ugledu te pravne i regulatorne posljedice. Sprječavanje i ublažavanje kibernetičkih napada zahtijeva proaktivne mjere kao što su mjere mrežne sigurnosti, obuka zaposlenika i podizanje svijesti, enkripcija podataka i sigurnosno kopiranje te planiranje odgovora na incidente.

Najčešći kibernetički napadi na bankarski sektor mogu se svrstati u:

Phishing - Phishing je vrsta kibernetičkog kriminala gdje napadači pokušavaju prevariti pojedince da dijele osjetljive podatke kao što su korisnička imena, lozinke i podaci o kreditnoj kartici predstavljajući se kao pouzdani entitet. Na primjer, u bankarskom sektoru, phishing e-pošta može izgledati kao da je od legitimne banke, tražeći od primatelja da klikne na poveznicu kako bi potvrdio podatke o svom računu. Međutim, poveznica vodi do lažne web stranice dizajnirane za krađu vjerodajnica za prijavu žrtve (Dhamija i sur., 2006)

DDoS napad (eng. *Disturbed denial of service*/Distribuirano uskraćivanje usluge) odnosi se na namjeran i zlonamjeran pokušaj da se poremeti redoviti tok prometa prema određenom poslužitelju, usluzi ili mreži preplavljujući ih ogromnom količinom internetskog/mrežnog prometa. Na primjer, unutar bankarske industrije, DDoS napad mogao bi se izvršiti na web stranicu banke, čineći je nedostupnom korisnicima i potencijalno rezultirajući financijskim gubicima i štetom za ugled banke (Kolias i sur., 2017).

Malware (Malicius softweare) and Ransomware - Malware (Zlonamjerni softver) je klasa softvera posebno dizajnirana za ometanje, oštećenje ili dobivanje neovlaštenog pristupa računalnim sustavima. Obuhvaća niz zlonamjernih programa uključujući viruse, crve, trojance i špijunski softver. Ransomware je, s druge strane, vrsta zlonamjernog softvera koji kriptira žrtvine datoteke i zahtijeva plaćanje, često u kriptovaluti, u zamjenu za vraćanje pristupa podacima (Ye i sur.,2017).

Social Engineering, odnosno društveni inženjering unutar bankarskog sektora obuhvaća stratešku manipulaciju pojedinaca unutar organizacije putem psiholoških taktika kako bi se nezakonito dobio neovlašteni pristup osjetljivim informacijama ili izvršile prijevarne aktivnosti. Ovo iskorištavanje ljudskog ponašanja uključuje različite tehnike kao što su izgovori, mamljenje, phishing i tailgating, gdje akteri prijetnji iskorištavaju društvene interakcije kako bi prevarili zaposlenike da otkriju povjerljive informacije ili daju pristup ograničenim područjima (Krombholz i sur., 2015). Primjer društvenog inženjeringa u bankarstvu uključivao bi počinitelja koji preuzima masku bankovnog zaposlenika tijekom telefonske interakcije i nagovara predstavnika korisničke službe da otkrije vjerodajnice za prijavu pod lažnom izlikom da provodi rutinsku sigurnosnu provjeru. Nadalje, drugi primjer bi mogao uključivati napadača koji iskorištava fizički pristup prostorijama banke maskirajući se u izvođača radova, naknadno instalirajući zlonamjerni hardver ili ulazeći u osjetljiva područja na prijevarne načine. Ove metode socijalnog inženjeringa iskorištavaju ljudsko povjerenje i mogu predstavljati značajne sigurnosne rizike za bankarske institucije, naglašavajući imperativnu potrebu za sveobuhvatnom obukom za podizanje svijesti i strogim protokolima provjere za učinkovito ublažavanje takvih prijetnji (Kalajžić, 2019).

STRATEGIJE ZAŠTITE FINANCIJSKIH INSTITUCIJA

Autori Coumo i Lawsky (2014) proveli su istraživanje u svrhu ispitivanja angažmana financijskih institucija u sprječavanju i upravljanju rizicima kibernetičke sigurnosti. Kako navode u rezultatima, sve financijske institucije su naglasile su važnost ulaganja u softvere

i programe za informacijsku sigurnost. Osim toga, institucije naglašavaju kako u posljednje vrijeme intenzivno rade na zapošljavanju komunikacijskih službenika čiji je glavni cilj odgovaranje na upite za vrijeme kibernetičkog napada. Ulaganja u programe, softvere te zapošljavanje komunikacijskih službenika je važno za prepoznavanje i upravljanje bilo kakvog oblika kibernetičkog rizika

Jedan od uzroka povećanja prijetnji kršenja elektroničkih informacija je generalni tehnološki napredak, što otežava očuvanje sigurnih podataka, ali i uspješno prepoznavanje i upravljanje rizicima (Al- Bassam i Al- Alawi, 2019). Navedeni izazovi su uzrokovali veću stopu kibernetičkog kriminala stoga je ulaganje u kibernetičku sigurnost ključno za očuvanje sigurnih podataka (Spalević, 2014). Rješavanje ovog pitanja nije zadatak isključivo tima zaduženog za rizike, nego njime trebaju biti upoznati svi zaposlenici tvrtke (Al- Bassam i Al- Alawi, 2019).

Autori Cebula i Young (2010) kibernetičke rizike definiraju kroz utjecaj na dostupnost, povjerljivost i cjelovitost informacija i informacijskih sustava, te navode kako je kibernetička sigurnost utemeljena na istim načelima. Dostupnost podrazumijeva činjenicu da pristup i upravljanje ovlaštenim informacijama ima isključivo ovlašteni korisnik u skladu sa zadanim uvjetima. Povjerljivost je definirana kao ograničenje pristupa informacijama tj. zabranu pristupa informacijama osobama koje za to nisu ovlaštene, a sve to u svrhu zaštite privatnosti informacija. Na posljetku, načelo cjelovitosti se zalaže za zabranu bilo kakve modifikacije povjerljivih informacija. Ćurak (2019) navodi kako se kibernetički rizici značajno povećavaju upotrebom informacijske tehnologije, a samim tim postaju jedni od najznačajnijih operativnih rizika poslovnih organizacija

Primjena različitih metoda fizičke kontrole koja podrazumijeva smanjivanje rizika kroz poduzimanje mjera kibernetičke sigurnosti u slučaju izloženosti prema kibernetičkim napadima definira se kao upravljanje kibernetičkim rizicima. Cjelokupan proces upravljanja rizicima obuhvaća aktivnosti identifikacije, kvantifikacije, integracije, prioritizacije izbora i primjene metode upravljanja te naravno nadzor (Harrington i Niehaus, 2004).

Refsdal i sur. (2015) navode kako se upravljanje kibernetičkim rizicima bavi isključivo rizicima koji su nastali kao posljedica kibernetičkih prijetnji. Kibernetički rizici podrazumijevaju povrede povjerljivosti podataka ili potpuni gubitak dostupnosti podataka radi napada u kibernetičkom prostoru.

Marotta i sur. (2017) navode kako je nemoguće izbjeći kibernetičke rizike budući bi njihovo izbjegavanje značilo provoditi poslovne aktivnosti bez primjene tehnoloških rješenja, odnosno tehnološke podrške. Ukoliko bi se odlučili za opciju upravljanja kibernetičkim rizicima potpunim izbjegavanjem negativnih implikacija kibernetičkih rizika, to bi značilo izostanak tehničke podrške što bi dovelo do operacija niže kvalitete i efikasnosti te bi ugrozilo osnovne ciljeve poslovanja.

Upravljanje rizikom je postao ključni zadatak čija učinkovitost djeluje na smanjenje negativnih utjecaja rizika koji se javljaju u poslovanju. Potreba upravljanja rizikom usmjerila je istraživače na razvijanje strategija razumijevanja rizika, metoda upravljanja istima te optimiziranja uporabe resursa u svrhu postizanja visoke razine kibernetičke sigurnosti. Iz svega navedenog se može vidjeti koliko se stavlja naglasak na važnost ulaganja u strategije upravljanja rizicima u poslovnim organizacijama (Kovač, 2021).

Obuka o svijesti o sigurnosti je vrsta prevencije koju IT i sigurnosni stručnjaci koriste kako bi educirali zaposlenike cijele organizacije o važnosti privatnosti podataka i cjeloku-

pne kibernetičke sigurnosti. Uloga obuke je povećati svijest zaposlenika o važnosti kibernetičke sigurnosti kako bi uspješno smanjili rizike povezane s kibernetičkim prijetnjama. Ista autorica navodi kako bi glavno načelo kojim bi se tvrtka trebala voditi prilikom izrade dobrog programa obuke o svijesti o sigurnosti, je kritičnost zaštite organizacije te pružanje pregleda odgovarajućih korporativnih postupaka i politika koji jasno definiraju kako sigurno raditi i kome se obratiti ukoliko zaposlenici identificiraju potencijalnu prijetnju. Obuka bi morala biti organizirana tako da uključi zaposlenike na svim razinama u organizaciji.

Ova obuka predstavlja temelj za minimiziranje prijetnji kibernetičkoj sigurnosti koje mogu uzrokovati velike probleme za organizaciju. Ključne teme svake obuke su važnost postavljanja lozinke i upravljanje istom, sigurnost e-pošte, web/internetska sigurnost, ali i fizička odnosno uredska sigurnost.

Organizacija koja provodi obuku o svijesti o sigurnosti sa svojim djelatnicima osigurava razvijanje svijesti i znanja o djelovanju i prepoznavanju napada na kibernetičku sigurnost, kod svakog zaposlenika a samim tim smanjuje vjerojatnost javljanja greške koja može uzrokovati štetu. Upravo ova činjenica i je ključna uloga obuke. Prolaskom kroz obuku ljudska ranjivost se pretvara u čvrste stupove obrane kibernetičke sigurnosti.

UPOZNATOST ZAPOSLENIKA BANAKA S POJMOVIMA KIBERNETIČKE SIGURNOSTI

U sklopu ovoga rada provedeno je istraživanje čiji cilj je bio ispitati upoznatost zaposlenika banaka s pojmovima kibernetičke sigurnosti i kibernetičkih napada te prikupiti podatke o obuci o kibernetičkoj sigurnosti koju prolaze na svom radnom mjestu.

U skladu s općim ciljem istraživanja, postavljeni su specifični ciljevi:

- Ispitati u kojoj mjeri su zaposlenici banaka upoznati s vrstama kibernetičkih napada.
- Ispitati prolaze li zaposlenici banaka obuku o kibernetičkoj sigurnosti.
- Ispitati koliko se zaposlenici banaka smatraju kompetentnima nakon takvih obuka.
- Ispitati imaju li zaposlenici banaka dosadašnjih iskustava sa slučajem kibernetičkog napada u banci u kojoj su zaposleni ili su bili zaposleni.

U istraživanju je sudjelovao 21 sudionik, od kojih 19 sudionika (90,5 %) ženskog spola, te 2 sudionika (9,5 %) muškog spola.

Za potrebe istraživanja izrađen je anketni upitnik, u čijem su ispunjavanju sudjelovali zaposlenici banaka, koji su se dobrovoljno i anonimno uključili u istraživanje. Sudionici su popunjavali online anketni upitnik koji se sastojao od tri dijela. Prvi dio upitnika činila su pitanja vezana uz njihove socio-demografske podatke, drugi dio upitnika činila su pitanja vezana uz to koliko su upoznati s pojmom kibernetičke sigurnosti, kibernetičkog napada i vrstama kibernetičkih napada, a trećim dijelom obuhvaćena su pitanja vezana uz obuku o kibernetičkoj sigurnosti koju prolaze u sklopu svog radnog mjesta, procjeni kompetencija za pravilno postupanje u slučaju takvih napada, eventualnom prethodnom iskustvu te sposobnosti praćenja kontinuiranih promjena u ažuriranjima. Upitnik se sastojao od ukupno 17 pitanja, zatvorenog tipa u kojima su sudionici mogli odabrati jedan ili više ponuđenih odgovora, ovisno o pitanju. Podaci prikupljeni u istraživanju obrađeni su tehnikama deskriptivne statističke analize.

Prema dobivenim rezultatima banka u kojoj su zaposleni većini sudionika osigurava obuku o kibernetičkoj sigurnosti (95,2%), a samo jednom sudioniku (4,8%) poslodavac ne osigurava obuku o kibernetičkoj sigurnosti. Nadalje, učestalost takve vrste obuke razlikuje se od poslodavca do poslodavca. Pa tako niti jedan sudionik ne prolazi takvu obuku svaki mjesec, odnosno jednom mjesečno. 5 sudionika (25%) prolazi obuku svaka 3 mjeseca, 6 sudionika (30%) prolazi ju svakih 6 mjeseci, 7 sudionika (35%) prolazi ju jednom godišnje, 1 sudionik (5%) svakih nekoliko godina te 1 sudionik (5%) navodi kako nije definirano, odnosno ponekad ju prolazi i više puta mjesečno.

Na Likertovoj skali od 1 do 5, 19 sudionika (90,5%) smatra kontinuirano educiranje osoblja izuzetno važnim, 1 sudionik (4,8%) važnim te 1 sudionik (4,8%) djelomično važnim, a niti jedan od sudionika educiranje osoblja ne smatra uglavnom ili potpuno nevažnim.

Sudionici su također na Likertovoj skali od 1 do 5 procijenili reakcije banke u kojoj su zaposleni na kibernetički napad. Pritom je 8 sudionika (42,1%) reakciju banke procijenilo najboljom mogućom, 6 sudionika (31,6%) vrlo visokom, njih 4 (21,1%) srednjom, te 1 (5,3%) niskom, odnosno nedovoljnom.

Na pitanje bi li informacije o tome da se u njihovoj banci dogodio napad podijelili sa svojom okolinom, njih 6 (28,6%) navodi kako bi podijelilo tu informaciju. Nadalje, većina, odnosno njih 12 (57,1%) ne bi podijelilo tu informaciju.

13 sudionika (61,9%) ima dosadašnje iskustvo primitka e-pošte ili privitaka koji su im izgledali sumnjivo i koje nisu očekivali, a da su takvi sadržaji bili pokušaj Phishinga ili distribucije zlonamjernog softvera koje su prijavili. Njih 5 (23,8%) je primilo takve sadržaje, ali ih nisu otvorili ili kliknuli na njih. 2 sudionika (9,5%) ih nije nikada dosad primilo, a 1 sudionik (4,8%) nije siguran/sigurna.

ZAKLJUČAK

Jedan od primarnih razloga zašto je kibernetička sigurnost ključna u bankarskom sektoru je osjetljiva i povjerljiva priroda podataka i transakcija kojima upravljaju financijske institucije. Banke pohranjuju golemu količinu osobnih i financijskih podataka o svojim klijentima, uključujući osjetljive podatke kao što su detalji računa i povijest transakcija. Zaštita ovih informacija nije samo regulatorni zahtjev, već i temeljni element izgradnje povjerenja između banaka i njihovih klijenata. Narušavanja kibernetičke sigurnosti koja dovode do neovlaštenog pristupa ili krađe podataka mogu rezultirati ozbiljnom financijskom štetom i štetom po ugledu, narušavanjem povjerenja klijenata i povjerenja u bankovnu instituciju.

Štoviše, međusobno povezana i složena priroda bankovnih sustava pojačava potencijalni učinak kibernetičkih napada. Kako se financijske institucije sve više oslanjaju na međusobno povezane mreže i pružatelje usluga trećih strana kako bi olakšale transakcije i operacije, površina napada se širi, stvarajući brojne ranjivosti koje kibernetički kriminalci mogu iskoristiti. Ova međupovezanost također povećava uloge za kibernetičke napade, budući da proboj u jednom dijelu sustava može potencijalno ugroziti cijelu mrežu, što dovodi do kaskadnih učinaka na bankarske operacije i korisničke usluge.

Uz zaštitu osjetljivih podataka i ublažavanje rizika kibernetičkih napada, kibernetička sigurnost ključna je za osiguravanje regulatorne usklađenosti i održavanje stabilnosti i otpornosti financijskog sustava. Nadalje, u slučaju uspješnog kibernetičkog napada, stabilnost

financijskog sustava može biti ugrožena, što može dovesti do potencijalnog poremećaja osnovnih bankarskih usluga i sistemskog rizika.

Najveća važnost kibernetičke sigurnosti u bankarskom sektoru leži u zaštiti osjetljivih podataka, održavanju povjerenja klijenata, osiguravanju usklađenosti s propisima, očuvanju stabilnosti financijskog sustava i ublažavanju rizika od kibernetičkih napada. Kako tehnologija nastavlja oblikovati budućnost bankarstva, otpornost praksi kibernetičke sigurnosti unutar industrije bit će ključna u zaštiti financijskih institucija i njihovih dionika od upornih i evoluirajućih prijetnji.

LITERATURA

1. Al- Bassam, S., Al- Alawi, A. (2019): The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University. VOLUME 14, ISSUE 7. ISSN No:1001-2400.
2. Al Zaidy, Ahmed. (2014). What are Cyber-Threats, Cyber-Attacks and how to defend our Systems. 10.13140/RG.2.2.30414.59208. Strayer University
3. Bača M. (2004.): Uvod u računalnu sigurnost, Narodne novine d.d., Zagreb
4. Cebula, J.J., Young, L.R. (2010): A Taxonomy of Operational Cyber Security Risks. Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
5. Cuomo, A. M., Lawsky, B. M. (2014): Report on Cyber Security in the Banking Sector. New York State Department of Financial Services.
6. Ćurak, M. (2019): Kibernetički rizici iz perspektive osiguranja. Financijska kretanja - najnoviji događaji i perspektive. Split: Ekonomski fakultet Sveučilišta u Splitu. str. 351-376.
7. Dhamija, R., Tygar, J.D., Hearst, M. (2006): Why phishing works Conference on Human Factors in Computing Systems - Proceedings, 1, pp. 581-590.
8. European Commission (2021): Tematski izvorni članak o Europskom semestru - Bankarski sektor i financijska sigurnost. Preuzeto s https://commission.europa.eu/system/files/2021-01/european-semester_thematic-factsheet_banking-sector-financial-stability_hr.pdf ,datum pristupa: 14.05.2024.
9. Hamidović, H., Hamidović, A., Zajmović, M. (2016): Okvir za rješavanje problema cyber kriminala. INFOTEH-JAHORINA, Vol. 15, 557-562
10. Harrington, S., Niehaus, G. (2004): Risk Management and Insurfance. McGraw Hill Irwin.
11. Kalajžić, I. (2019): Cybersecurity - the threat of social engineering. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
12. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. (2017) : DDoS in the IoT: Mirai and other botnets Computer, 50 (7), art. no. 7971869, pp. 80-84.
13. Kovač, D. (2021): Ulaganje u kibernetičku sigurnost. Zbornik radova Veleučilišta u Šibeniku. Vol. 15(1-2), pp. 61-73
14. Krombholz, K., Hobel, H., Huber, M., Weippl, E (2015): Advanced social engineering attacks
15. Journal of Information Security and Applications, 22, pp. 113-122.
16. Marotta, A. i sur. (2017): Cyber-insurance survey. Computer Science Review, Vol. 24. str. 35-61. ISSN 1574-0137.
17. Mikšić, D. (1988): Proizvodno i socijalno značenje novih tehnologija. Revija za sociologiju, 19 (3), 173-182
18. Njavro, Đ. (1989): Nove tehnologije — utjecaj na poduzeće. Ekonomski vjesnik, II (1), 117-128.
19. Obradović, D. (2018): Kibernetika – što je to?. Common Foundations 2018 - uniSTem: 6th Congress of Young Researchers in the Field of Civil Engineering and Related Sciences. Split: Sveučilište u Splitu, Fakultet građevinarstva, arhitekture i geodezije. 158-163

20. Prskalo, D. (2022): Kibernetička sigurnost kao ključna determinanta nacionalne sigurnosti Republike Hrvatske. Zbornik sveučilišta Libertas, 7 (8), 185-199
21. Refsdal, A. i sur. (2015): Cyber- Risk Management. SPRINGER BRIEFS IN COMPUTER SCIENCE.
22. Spalević, Ž.. (2014): Cyber Security as a Global Challenge of The Modern Era. Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide. doi:10.15308/sinteza-2014-687-692
23. Središnji državni ured za razvoj digitalnog društva (n.d.): Kibernetička sigurnost. Preuzeto s https://rdd.gov.hr/izdvojeno/kiberneticka-sigurnost/1436, datum pristupa: 21.svibnja.2024
24. Ye, Y., Li, T., Adjeroh, D., Iyengar, S.S. (2017) : A survey on malware detection using data mining techniques ACM Computing Surveys, 50 (3), art. no. 3073559,
25. Zakon o elektroničkim komunikacijama. Narodne novine, br. 73/2008. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2008_06_73_2420.html, datum pristupa: 14.05.2024.
26. Zakon o kibernetičkoj sigurnosti. Narodne novine, br. 14/2024. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html, datum pristupa:14.05.2024.
27. Zakon o zaštiti osobnih podataka. Narodne novine, br. 106/2012. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html, datum pristupa: 14.05.2024.