Примљено: 31. октобар 2024.
Прихваћено: 30. новембар 2024.

УДК 343.9:004.738.5]:[351.824.11:336
COBISS.SR-ID 161904137
DOI: 10.5937/ssb2402045B

САЈБЕР НАПАДИ НА ФИНАНСИЈСКИ СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Јована БРАЈОВИЋ*
Дејана ЈОВАНОВИЋ ПОПОВИЋ**, редовни професор

* Generali Osiguranje Srbija, jovanabrajovic296@gmail.com
** Факултет безбедности, Универзитет у Београду, dejana@fb.bg.ac.rs

САЈБЕР НАПАДИ НА ФИНАНСИЈСКИ СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Сажетак: *Финансијски сектор критичне инфраструктуре представља један од најугроженијих сектора када је реч о сајбер нападима, с обзиром на његову критичну улогу у глобалној економији и природу пословања у данашњици. Дигитализација финансија отвара врата сајбер нападима кроз широку и распрострањену доступност финансијских услуга на модерним технологијама и мрежама. Овај рад бави се истраживањем мера заштите од сајбер напада у финансијском сектору кроз анализу три значајна инцидента: напада на Централну банку Бангладеша, компромитацију података компаније 'Capital One' и напад рамосвером на 'Travelex' компанију за трансфер новца. Примарни циљ истраживања је анализа утицаја сајбер напада на финансијски сектор критичне инфраструктуре и идентификација ефикасних мера заштите које могу смањити ризик од сличних напада у будућности. Користећи преглед међународне литературе и студију случаја, рад наглашава важност интеграције технолошких и организационих мера, као и значај изградње сајбер отпорности кроз континуирано унапређење безбедносних протокола и културе свести о сајбер безбедности. Резултати истраживања показују да, иако сајбер напади носе значајан ризик, они такође могу подстаћи финансијске институције на иновације и унапређење мера заштите.*

Кључне речи: сајбер напад, критична инфраструктура, финансијски сектор критичне инфраструктуре, мере заштите од сајбер напада, сајбер криминал

Увод

Критична инфраструктура представља круцијални сегмент функционисања државе и друштва и као таква ставља се на врх листе приоритета када се говори о заштити. Критична инфраструктура се састоји од више различитих сектора, у зависности од државе до државе, али већина држава би међу секторима критичне инфраструктуре навела и сектор финансија. Сектор финансија обухвата низ финансијских институција попут банака и осигуравајућих кућа, а међу-

зависност сектора финансија са другим секторима наглашава неопходност неометаног функционисања овог сектора. Сајбер напади постали су свакодневница у данашњем свету где су готово сви процеси рада и функционисања дигитализовани. Напредак технологије омогућио је управљање новчаним токовима и подацима на само неколико кликова, а управо ту се отвара простор за сајбер нападе који погађају и финансијске институције. Предмет овог рада представљају сајбер напади на финансијске институције и анализа њиховог утицаја на финансијски сектор критичне инфраструктуре. Финансијски сектор критичне инфраструктуре представља један од најрањивијих сектора када су у питању сајбер напади сходно природи пословања, али и чињеници да је највећи број сајбер напада мотивисан финансијском добити. Рањивост овог сектора критичне инфраструктуре поспешена је све већом дигитализацијом финансија и готово потпуном зависношћу сектора од телекомуникационих и информационих технологија и инфраструктуре. Студија случаја рада заснива се на анализи примера сајбер напада на Централну банку Бангладеша, "Capital one" и „Travelex" финансијске институције. Кроз студију случаја ова три сајбер напада рад даје анализу утицаја сајбер напада на финансијски сектор критичне инфраструктуре проучавајући добре, али и лоше праксе примењене у овим случајевима. Кроз студију наведена три случаја рад тежи приказивању последица које су сајбер напади произвели на финансијски сектор, како на појединачне институције тако и на финансијски систем уопште. Такође, рад кроз студију случаја анализира узроке настанка сајбер напада извлачећи потенцијална решења за заштиту финансијског сектора. Упоређујући појединачне случајеве из студије рад тежи проналажењу најоптималнијих начина унапређења мера заштите од сајбер напада, као и предвиђању могућих праваца у развоју сајбер напада.

Финансије као део критичне инфраструктуре и дигитализација финансија

Као један од осам сектора критичне инфраструктуре у Републици Србији, сектор финансија је такође ближе одређен Уредбом за одређивање критеријума критичне инфраструктуре и начину извештавања о критичној инфраструктури у Републици Србији. На основу ове уредбе, под финансијским сектором критичне инфраструктуре

у Републици Србији сматрају се системи, мреже, објекти или њихови делови, а чије уништење или оштећење може изазвати озбиљније последице у виду угрожавања или отежања економске стабилности државе. Овде се убрајају привредна друштва попут банака или осигуравајућих кућа, али и свих оних привредних друштава који у делатности финансија заузимају значајан удео у свом делокругу пословања. Такође, не треба изоставити ни органе државне управе под којима се подразумевају Пореска управа, Управа за трезор, Управа царине, Управа за јавни дуг, Агенција за осигурање депозита и др. (Службени гласник Републике Србије, 69/2022).

Финансијски сектор такође нуди широк спектар услуга и производа како појединцима тако и корпорацијама. Сваки значајан поремећај у испоруци услуга носи са собом значајне економске, социјалне и потенцијално политичке ефекте на стабилност заједнице. Важно је напоменути да је економска стабилност основ за политичку и војну безбедност (Dumitru & Ferarau, 2018). Узимајући у обзир увезаност великих приватних и државних предузећа на регионалном и међународном нивоу, укључујући велике светске банке, последице које оштећење или уништење финансијског сектора критичне инфраструктуре лако прелази границе и утиче на друге земље. Финансијске услуге играју суштинску улогу у расту привреде и економије, те су од виталног значаја за опстанак државе. На основу овога следи да су услуге банкарске индустрије и финансијског сектора уопште од велике важности за сваку државу (Somogyi, Nagy, 2021).

Увођењем нових финансијских технологија, старомодни начин пословања финансијских институција замењен је употребом нових технолошких решења. Ово се односи на дигиталне технологије које имају потенцијал, односно могућност да трансформишу пружање финансијских услуга, подстицање развоја нових, или модификовања већ постојећих пословних модела, апликација, процеса и производа (Pazarbasioglu et al., 2020). Овим решењима постиже се лака доступност клијентима, али и постизање економије обима, све то праћено ниским трошковима и великом ефикасношћу.

Дигитализација финансија настала је природно као продукт модерног друштва праћеног дигитализацијом и свих осталих процеса свакодневног функционисања. Дигитални финансијски сервиси су финансијски сервиси који се ослањају на дигиталне технологије за испоруку и употребу од стране потрошача. Дигитални финансијски сервиси доживели су своју експанзију услед иновација у технологији и

пословним моделима. Дигитализација финансијских сервиса значајно умањује потешкоће у сваком кораку током финансијског циклуса, од отварања рачуна до потврђивања трансакција, али и аутоматизације других специфичних процеса, попут, на пример, процена кредитне способности (Pazarbasioglu et al., 2020).

Како је дошло до уске повезаности између модерних технологија и финансијских институција и услуга тако се и формирао Финтек (енгл. Fintech). Финтек представља израз који обједињује финансије (енгл. Finance) и технологију (енгл. Technology) и користи се за технолошка решења која су у служби финансија. Финтек обухвата све активности од мобилног плаћања, трансфера, кредитних одобрења путем мобилних апликација, па све до крипто-валута и инвестиција у роботе. Развојем финтека су се у почетку бавили искључиво екстерни сарадници финансијских институција, да би се касније исти определили за интерни развој у циљу смањења трошкова и повећања иновативности (Goldstein, Jiang & Karolyi, 2019).

Банке, али и друге финансијске институције почеле су да своје услуге нуде путем мобилних апликација, као и веб-сајтова. Значај заштите финансијског сектора повећава се заједно са опсегом и модернизацијом његових модела рада с обзиром на све већу потхрањеност овог система корисничким подацима. Како би се испратио брз напредак недолазећих претњи потребно је држати корак са развојем технологија и бити спреман на благовремену реакцију. Заштита финансијских институција од сајбер напада се постиже само континуираним праћењем и вишеструким мерама заштите финансијских система.

Сајбер напади и мере заштите од сајбер напада

Сајбер напади представљају врсту напада који за циљ имају злонамерно ометање или саботирање рада рачунара или рачунарских мрежа, крађу или уништавање података или се напад на рачунар користи у сврхе неког другог вида напада. Постоји мноштво врста сајбер напада, а њихов број се константно увећава, међутим, постоји неколико основних типова међу којима су најчешћи фишинг, рансомвер, дистрибуирано ускраћивање услуга (DDOS) и друге врсте малвера, односно злонамерних софтвера. Сајбер напади се такође у великој мери разликују по својој софистицираности, при чему сајбер криминалци

покрећу како насумичне тако и циљане нападе на предузећа, односно компаније.

Са неког ширег аспекта, сајбер нападе можемо, на основу мете, класификовати у нециљане и циљане. Нециљани напади функционишу по принципу обима, односно нападач циља што више уређаја. Неретко се ови напади изводе уз помоћ природе, односно отворености интернета. Као примери оваквих напада углавном се јављају фишинг, рамсовер и скенирање. Циљани напади јесу такви да нападач на уму има неку конкретну организацију или особу, или је плаћен за циљање исте. Овакви напади изискују време за припрему како би се пронашао најадекватнији начин за постизање успешног напада. Такође, они представљају и већу претњу с обзиром на ниво припреме. Најчешћи облици циљаних напада јесу фишинг, подметање ботнетова, али и подметање у ланцу снабдевања (Biju, Gopal & Prakash, 2019).

Многи аутори се слажу да се сајбер напади могу класификовати на следећи начин:

1. фишинг;
2. напад ускраћивањем услуга;
3. употреба ботова;
4. спам;
5. „човек у средини" метода;
6. спуфинг;
7. логичке бомбе;
8. малвери;
9. SQL injection;
10. напад на лозинку.

Мере заштите од сајбер напада могу се поделити у неколико врста, као и сами напади, међутим, важно је напоменути да када говоримо о финансијским институцијама и финансијском сектору уопште ове мере имају већу тежину и озбиљност тиме што су праћене многобројним стратегијама и плановима заштите којима се ове мере ефикасно координирају и планирају. Превасходно је неопходно објаснити основне видове заштите од сајбер напада.

Мере заштите могу се поделити на:

1. антивирусни програми;
2. заштитни зид;
3. аутентикација;
4. контрола приступа;

5. енкрипција података;
6. сегментација мреже;
7. редовно ажурирање софтвера.

Поред горенаведених мера које можемо сврстати у тактичке, односно практичне мере, важно је истаћи и значај стратегијских мера. Стратегијске мере се односе на (NIST, 2018):

1. развој и изградњу безбедносних политика;
2. развој и имплементацију безбедносних политика;
3. обучавање и едукацију запослених;
4. изградњу "Zero trust" културе;
5. усклађеност са међународним и државним регулативама и стандардима.

Сајбер напад на Централну банку Бангладеша

Сајбер напад на Централну банку Бангладеша 2016. године потресао је глобални финансијски систем до његових темеља. У фебруару 2016. године Централна банка Бангладеша доживела је сајбер напад, током којег су нападачи покушали да украду 951 милион долара са њеног рачуна резерви у Њујоршкој банци федералних резерви (ФЕД). Нападачи су успели да се неприметно увуку у мреже банке и дођу до система мреже за Светске међубанкарске финансијске телекомуникације (СВИФТ) (Bukth & Huda, 2017). Може се закључити да је већ прва линија одбране била лоше постављена, односно да заштитни није адекватно одиграо своју улогу и дошло је до неовлашћеног упада у систем. Касније је откривено да је "Dridex" малвер коришћен за напад. У основи, нападачи су били у могућности да се крећу бочно унутар мрежа банака и да, уз помоћ команди са својих командно-контролних сервера, компромитују администраторске креденцијале и искористе их за напад (Mapoka, Zuva & Zuva, 2019). 4. фебруара 2016. године нападачи су послали тридесет пет лажних захтева за исплату у укупном износу од 951 милион долара ФЕД-у (Bukth & Huda, 2017). ФЕД је био опремљен сигурносним протоколима када су у питању биле СВИФТ трансакције. Од укупног броја пристиглих захтева од стране нападача, тридесет је успешно заустављено, међутим, пет трансакција су успешно обрађене, што је резултирало пребацивањем

81 милиона од стране ФЕД-а на међународне рачуне. Поставља се питање колико је ефикасан био систем контроле захтева за исплату и пребацивање новца. Новац је у веома кратком року прошао токове такозваног прања новца, те је завршио на рачунима казина на Филипинима. Претпоставља се да је пренос новца на Филипине вероватно изабран због строгих закона о банкарској тајности и изузећа казина из закона против прања новца (Bull Jr & Fincannon, 2024). Наравно, последице овог сајбер напада би вероватно биле мање да је контрола трансакција ка Филипинима била строже уређена, нарочито када су усмерене ка казинима и сличним видовима пословања.

Централна банка Бангладеша је у то време поседовала штампач инсталиран и подешен тако да аутоматски штампа све СВИФТ трансакције. Међутим, када су надлежни 5. фебруара 2016. године радили рутинску проверу приметили су да штампач није одштампао ништа од претходног дана. Надлежни су у почетку мислили да је у питању мањи технички проблем, али, даљим сагледавањем ситуације и проблема, открили су поруке трансфера новца послате ФЕД-у (Bukth & Huda, 2017). Као додатна мера опреза и предострожности било би увођење барем још једног штампача за СВИФТ трансакције, те би њихова неусаглашеност слала сигнал да је у питању неправилност, што би предупредило развој сајбер напада на виши ниво. Уложени су напори за ступање у контакт са ФЕД-ом, како би се зауставило плаћање, али због времена напада било је прекасно и банка је изгубила 81 милион долара пре него што су успели да ступе у контакт са њима. Нападачи су искористили слабости у заштити система Централне банке Бангладеша, која је користила јефтине прекидаче од 10 долара за повезивање рачунара са СВИФТ мрежом, а као додатна слабост банка није имала адекватан заштитни зид (Bukth & Huda, 2017). Адекватна, квалитетна опрема која иде у корак са развојем технологије неопходна је како би се сајбер напади попут овог предупредили. Неадекватно конфигурисање заштитног зида само је отворило врата нападачима за улаз у системе банке, те је неопходно било адекватно ажурирати и пратити како физичке тако и сајбер мере заштите. Улагањем у средства и мере заштите финансијске институције се штите од већих трошкова него што би издаци за мере заштите били.

Пљачка Централне банке Бангладеша послужила је као оштар подсетник на важност сајбер безбедности у банкарству и финансијском сектору уопште. Овај догађај је подстакао финансијске институције широм света да преиспитају и побољшају своје мере заштите (Maroka,

Zuva & Zuva, 2019). Централна банка Бангладеша је предузела кораке да ојача своје мере сајбер безбедности и заштите и побољша интерну контролу како би спречила сличне инциденте у будућности (Maroka, Zuva & Zuva, 2019). Инцидент је такође резултирао и заоштравању дипломатских односа између Бангладеша и Филипина. Како је значајан део украдених средстава опран преко филипинских казина, то је довело до међусобних преговора о међународној сарадњи по питању истрага о сајбер злочинима (Karim & Hasan, 2021).

Сајбер напад на банку "Capital One"

Упркос значајним издацима у мере заштите, као и информациону инфраструктуру уопште, компанија "Capital One" је у јулу 2019. године открила да је дошло до сајбер напада, при чему су осетљиви подаци клијената били изложени неовлашћеном приступу. Компанија је у свом јавном саопштењу изјавила како је нападач успео да прибави личне податке клијената путем неовлашћеног приступа, а који су повезани са корисничким кредитним картицама (Novaes Neto et al., 2020). Случај овог сајбер напада показатељ је да је, и поред високих улагања у модерна решења, потпуна заштита од сајбер напада неизвесна. Компанија је навела да су компромитовани подаци исти подаци које банка уобичајено прикупља током процеса отварања рачуна или издавања кредитних картица, укључујући имена, адресе, поштанске бројеве, бројеве телефона, адресе е-поште, датуме рођења и пријављени приход, као и подаци о кредитима, лимитима и слично. Неовлашћени приступ личним подацима погодио је око 100 милиона појединаца у Сједињеним Државама и око 6 милиона у Канади, укључујући и информације малих предузећа. Компанија је открила напад захваљујући свом Програму одговорног откривања података 17. јула 2019. године. Међутим, компанији се замера што напад није био откривен кроз редовне операције у оквиру процедура сајбер безбедности, већ је за то била потребна интервенција спољног лица које је путем е-поште обавестило банку да су подаци клијената доступни на „GitHub" страници (Novaes Neto et al., 2020). Поставља се питање да ли се упад могао открити на други начин, као што су безбедносна скенирања, или преглед и праћење логовања и приступа у системе банке.

Банка је у саопштењу за јавност изјавила да су компромитовани подаци били шифровани, али је такође признала да је услед упада у систем постојала могућност да су подаци дешифровани. Банка није дала изјаву о томе како је до упада дошло. ФБИ је ухапсио Пејџ А. Томпсон, жену из Сијетла, због хаковања сервера које је "Capital One" изнајмио у облаку (Novaes Neto et al., 2020). Истражитељи су утврдили да је Томпсон раније радила у компанији за рачунарство у облаку чији су сервери провађени, а медији су брзо идентификовали компанију као "Amazon Web Services" (AWS), према њеном „LinkedIn" профилу (Sandler, 2019). Томпсон је користила софтверски алат за скенирање, који јој је омогућио да идентификује сервере са погрешно конфигурисаним заштитним зидовима, што јој је омогућило да изврши команде и приступи серверима (Khan et al., 2022). У случају овог сајбер напада, као и у случају напада на Централну банку Бангладеша, може се закључити важност добро конфигурисаног заштитног зида као прве линије одбране од напада.

Након овог инцидента, "Capital One" предузима мере у циљу боље заштите и исправљања ранијих пропуста. Такође, они уводе и осигурање од крађе података за своје клијенте, чиме се даје на значају о свести озбиљности инцидента који се догодио. Систем заштите банке направио је неколико грешака које су омогућиле овај сајбер напад. Поред поменутог лоше конфигурисаног заштитног зида, од великог значаја је ограничити IAM улоге и дозволе које оне носе. Један од основних принципа сајбер безбедности, али и корпоративне безбедности нарушен је увођењем улоге која има изузетно велика права и приступе (Khan et al., 2022). Напомиње се да је од кључних постулата успешне сајбер заштите то да запослени имају приступ само оним подацима, у оном обиму, који су му неопходни за обављање радних задатака.

Сајбер напад на "Travelex"

"Travelex" је компанија специјализована за размену валута и финансијске трансакције основана у Лондону, у Великој Британији. У децембру, 31. децембра 2019. године, компанија доживљава сајбер напад рамсовером, што је довело до великих финансијских, али и губитака у поверењу клијената. Поједини аутори сматрају да је пропуст у одбрани од сајбер напада створен нередовним и неадекватним ажури-

рањем система, што је створило рањивости на систему и омогућило нападачима да изврше упад и крађу података (Lalisang, 2020). Нападачи су за Би-Би-Си тврдили да су преузели пет гигабајта поверљивих информација, укључујући датуме рођења клијената, податке о кредитним картицама и бројеве социјалног осигурања (Novak, 2020), а за откуп докумената су од компаније тражили да плати 6 милиона долара како би се системи омогућили за понован рад и спречило цурење украдених података на мрежу (Nish, Naumann, & Muir, 2022). Разлог успешности напада лежи у закрпи рањивости коју је компанија имплементирала на све сервере и тиме је отворила за упад споља (British Assessment Bureau, 2020).

Како би одбрана од сајбер напада била ефикасна неопходно је применити је свеобухватно на свим уређајима и комплетном мрежном систему. Непримењивањем закрпе за рањивост на свим серверима компанија је такорећи пожелела добродошлицу за све непожељне госте. Санирање рањивости закрпом обављено је неколико месеци пре самог напада, али је то урађено само на једном од сервера компаније. Рањивост на мрежи омогућила је нападачу приступ без налога и лозинке, као и могућност да се вишефакторска аутентификација искључи и дозволи неометана крађа и криптовање података (British Assessment Bureau, 2020). Компанија је услед прекида рада свих система трансакционе операције пребацила на рад оловком и папиром. Утицај напада проширио се на широк спектар банака које су се ослањале на компанијске девизне услуге (Nish, Naumann, & Muir, 2022). Напад је изазвао прекиде у раду у трајању од месец дана, а особље повремено није могло да користи компјутере да прати трговину валутама. Ремећење у раду банака носи ризик од утицаја на функционисање финансијског сектора као дела критичне инфраструктуре. Поставља се питање шта би се догодило да је сајбер напад на компанију имао утицаја на све банке у држави или на више већих глобално с обзиром на то каква је природа рада ове компаније била. Нападачи су користили изузетно ефикасну варијанту рамсовера под називом „REvil", оријентисаног ка финансијским институцијама. Извештаји процењују да је напад на крају коштао компанију скоро 30 милиона долара (Nish, Naumann, & Muir, 2022).

Последице сајбер напада

Сајбер напад на Централну банку Бангладеша уздрмао је свет финансија. Поред огромних финансијских губитака и шока за тржиште финансија, овај напад довео је и до ревизија безбедносних мера и протокола, јачања међународне сарадње и појачаног улагања у напредна технолошка решења за заштиту, како на нивоу институција тако и на пољу њихове међусобне сарадње с обзиром на то да заједно граде високоумрежен систем (Karim & Hasan, 2021). Када се говори о случају сајбер напада на "Capital One", може се рећи да је то прави пример нарушавања приватности података. Несумњиво да данашњи начин функционисања друштва захтева висок ниво поверљивости података, а да се појединци слажу да је заштита њихових података приоритет пословања свих институција, а нарочито финансијских. Нарушавање приватности података носи са собом многобројне последице по финансијске институције, сагледано из више углова (Siddique, 2019). Последице изазване сајбер нападима који су фокусирани на крађу података такве су да је ризик од прекида пословања или немогућности рада финансијских институција изузетно велики. Зависност других сектора критичне инфраструктуре од фунансијског сектора поставља финансијски сектор на такву позицију да је нарушавање рада, или прекид рада овог сектора озбиљнији него што се чини. Иако се не чини да напад на једну финансијску институцију може бити погубан по читав сектор, треба напоменути да су финансијске институције део глобалне мреже финансија и да се рањивости једног система лако могу рефлектовати и на остале институције, а самим тим и на читаву мрежу (George, Baskar & Srikaanth, 2024), што свакако да случај сајбер напада на "Travelex" потврђује. Било да се ради о издвајању средстава за изградњу нових здравствених капацитета, или улагању у заштиту животне средине, у данашњици је новац један од кључних покретача готово сваке активности. Немоћност рада финансијских токова, или компромитовање истих доводи до нарушавања рада осталих сектора, а тиме и угрожавања функционисања државе уопште. Сајбер напади на финансијске институције могу бити изузетно разорни, како за саме институције тако и за шири финансијски систем. Сагледавајући сваку од три студије случаја обрађене у раду, може се закључити да неретко веома ситне грешке и непажња у заштити од сајбер напада доводе до разорних последица. Сајбер напади често доводе до огромних финансијских губитака, нарушавања поверења клијената и зна-

чајних прекида у пословању. Напади попут оног на Централну банку Бангладеша или "Capital One", али и "Travelex" откривају слабости у безбедносним системима, што може покренути ланчану реакцију у финансијском сектору, јер један инцидент може угрозити и друге институције које су део истог међународног система. Ова врста међузависности значи да је једна рањивост у систему потенцијална претња за целу финансијску мрежу. Међутим, сајбер напади такође делују као снажан покретач за финансијске институције да унапреде своје безбедносне мере и јачају међусобну сарадњу. Сајбер напад на Централну банку Бангладеша поспешио је међународну сарадњу, али и свест о потреби за адекватном опремом заштите која прати трендове развоја напада. Такође, напади подстичу банке и друге финансијске институције да уложе више у развој напредних технологија за превенцију и откривање сајбер претњи, као и у обуку запослених у области сајбер безбедности. Случај са нападом на "Capital One", са друге стране, послужио је као оштар подсетник да, и поред модернизације мера заштите, људска улога игра кључан фактор кроз одређивање улога права и приступа у одговарајућој мери. Поред тога, постојање свести о заједничком ризику, попут случаја са "Travelex" компанијом, доводи до побољшане комуникације и координације између институција, што за циљ има развој заједничких стандарда и најбољих пракси у заштити финансијског сектора. Иако сајбер напади носе ризик од прекида пословања и могу озбиљно угрозити финансијске институције, они такође служе као катализатор за трансформацију безбедносних политика и пракси. Финансијске институције постају свесније потребе за заједничким деловањем и улагањем у сигурност система, чиме јачају своју отпорност на будуће претње и доприносе стабилности глобалног финансијског система.

Потенцијално решење за побољшање мера заштите од сајбер напада

Како би мере заштите од сајбер напада биле ефикасне и правовремене потребно је усагласити и развијати више сегмената мера заштите. Неопходно је пратити технолошки напредак и бити у корак са њим колико год је то могуће. Под овим се подразумева и употреба вештачке интелигенције и новоразвијених алата. Застареле технологије, или штедња на квалитету технологија, могу изазвати много више штете

него што би коштала имплементација нових технологија, што можемо видети на примеру сајбер напада на бангладешку банку. Са друге стране, употреба нових технологија и решења мора бити испитана и проверена као сигурна. На примеру сајбер напада на "Capital One" можемо видети да, иако су применили релативно нову технологију складиштења у облаку, сигурност закупљене услуге није била на одговарајућем нивоу. Док је случај са сајбер нападом на "Travelex" показатељ да, без обзира на вид технологије који се користи, уколико се не примени свеобухватно и правовремено не ажурира сигурност од сајбер напада је упитна. Поред улагања у нове технологије и њихово испитивање, кључна је и едукација запослених о сајбер нападима и начинима заштите. Наравно, неизоставно је да су у питању континуиране и правовремене обуке узевши у обзир брз и стални напредак информационих технологија. Развијање свести код запослених и стварање такозване културе нултог поверења (енгл. Zero Trust) представљају основ за успешну заштиту од сајбер напада. На примеру случају сајбер напада на "Capital One" може се закључити да је неопходно размотрити и систематично дедељивати права приступа подацима на основу радне позиције, тако да запослени имају приступ само оним подацима којима је неопходно за обављање радних задатака. Такође, увођење двоструке аутентификације такође се може сматрати за обавезну ставку приликом приступа системима институције. Сарадња и размена информација и знања са институцијама из истог сектора је, као што је већ напоменуто, од изузетног значаја када је реч о сајбер нападима. На примерима бангладешке банке и "Capital One" банке може се видети како недостатак комуникације међу деловима једног система резултује великим последицама, те се стога јачање међусобне сарадње и комуникације истиче као препорука за унапређење мера заштите. "Travelex" случај одличан је пример за схватање увезаности међу финансијским институцијама и потребом да заједно раде на јачању заштите од сајбер напада.

Како би се оснажила отпорност на сајбер нападе и самим тим смањио и утицај истих на финансијски сектор критичне инфраструктуре, неопходно је систематично и темељно приступити сегментима сајбер безбедности. Ово захтева интеграцију, односно обједињавање стратешког управљања, технолошке модернизације и промене организационе културе. На управљачком нивоу, финансијске институције и надлежни унутар њих, као што су одбори и извршни тимови, играју кључну улогу у проглашавању сајбер безбедности за стратешки прио-

ритет, обезбеђујући при томе адекватне ресурсе како би се она постигла. Технолошка модернизација подразумева улагање у нове технологије, али и сегментацију мреже ради спречавања бочног кретања, као и вишефакторску аутентификацију за контролу приступа и енкрипцију података. Прелазак са застарелих система и адаптација на нове безбедносне алате у виду платформи поједностављује праћење и реаговање на претње. Оперативно је неопходно осигурати ванмрежне резервне копије и редундантност система како би се обезбедила непрекидност основних услуга у случају сајбер напада. Планирање заштите од сајбер напада подржано тренинзима путем симулација и вежби за реаговање на сајбер нападе омогућава особљу боље усвајање неопходних процедура и знања. Такође, увођење сајбер осигурања такође може помоћи у ублажавању финансијских последица сајбер напада (George, Baskar & Srikaanth, 2024).

Закључак

Експанзија сајбер напада је неизбежна садашњица и будућност, а примери из рада сведоче о њима у прошлости као примерима за развој мера заштите. Како технологија расте и развија се тако расте и развија се и претња од сајбер напада. Софистицираност сајбер напада и домишљатост нападача представљају само једну од препрека у борби са овим претњама. Тежња ка злоупотреби вештачке интелигенције и потенцијално коришћење квантних рачунара неизвесна су, али реална претња по заштиту података и финансија. Циљ истраживања јесте сагледавање утицаја сајбер напада на финансијски сектор критичне инфраструктуре и проналажење решења у виду мера за њихово ублажавање и заштиту од истих. Сајбер напади на финансијске институције, као што су инциденти са Централном банком Бангладеша, компанијом "Capital One" и компанијом за трансфер новца "Travelex", истичу важност развоја свеобухватних стратегија заштите које обухватају како технолошке тако и организационе мере. Иако су последице ових напада биле разорне, оне су такође послужиле као катализатори за унапређење сајбер безбедности у финансијском сектору. Кроз анализу ових случајева, овај рад показује да је смањење утицаја сајбер напада на финансијски сектор критичне инфраструктуре могућ само уз константно улагање у модернизацију технологије, унапређење организационих процедура и промовисање културе безбедности међу

запосленима. Ови напади такође наглашавају потребу за бољом сарадњом унутар сектора, али и спољним релевантним институцијама и разменом информација, као и државама међусобно, како би се финансијски сектор ефикасније одбранио од будућих претњи. Свакако да се као закључак може извући неопходност пажљиве, свеобухватне, детаљне и добро испланиране заштите од сајбер напада на свим нивоима функционисања финансијских институција уз непрекидни мониторинг и будно око над развојем и рапидним растом сајбер напада. Може се закључити да је систем заштите од сајбер напада комплексна слагалица делова од којих сваки мора одиграти своју улогу адекватно како би комплетна слика имала смисла. Сајбер напади циљају рањивости у овим системима, а рањивост само једног дела представља претњу и по све остале, те је добро комбиновање делова и постављање истих на одговарајуће место кључно како би заштита од сајбер напада била успешно примењена. Овај истраживачки рад пружа свој допринос кроз приказ утицаја сајбер напада на финансијски сектор критичне инфраструктуре у виду студије случаја на три финансијске институције сваки специфичан по узроку и последицама. Анализом ових случајева рад нуди решења и препоруке у циљу унапређења заштите финансијског сектора критичне инфраструктуре.

Литература

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. International Research Journal of Engineering and Technology, 6(3), 4849–4852.

British Assessment Bureau. (2020). How the Travelex ransomware attack could have been avoided. Retrieved from https://www.british-assessment.co.uk/how-thetravelex-ransomware-attack-could-have-been-avoided/

Bukth, T., & Huda, S. S. (2017). The soft threat: The story of the Bangladesh bank reserve heist. SAGE Publications: SAGE Business Cases Originals.

Bull Jr, C. L., & Fincannon, C. (2024). Assignment 2.1: The 2016 Bangladesh Bank Heist.

Dumitru, D., Feraru, C. L. (2018). National Security Concept. Annals – Series on Military Sciences, 10(2), 90–101.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51–75.

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and beyond. The Review of Financial Studies, 32(5), 1647–1661.

Karim, Y., & Hasan, R. (2021). Taming the digital bandits: An analysis of digital bank heists and a system for detecting fake messages in electronic funds transfer. In National Cyber Summit (NCS) Research Track 2020 (pp. 193–210). Springer International Publishing.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. ACM Transactions on Privacy and Security, 26(1), 1–29.

Lalisang, B. (2020). Cyber-risk and Director's liability: Exploring the Dutch legal framework.

Mapoka, T. T., Zuva, K., & Zuva, T. (2019). Hack the Bank and Best Practices for Secure Bank. International Journal of Computer Science, Communication & Information Technology (CSCIT), 7, 17–21.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. Retrieved from https://www.nist.gov/cyberframework

Nish, A., Naumann, S., & Muir, J. (2022). Enduring cyber threats and emerging challenges to the financial sector. Carnegie Endowment for International Peace.

Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).

Novak, M. (2020, January 7). Travelex shutdown caused by Sodinokibi ransomware attack, reports say. CyberScoop. Retrieved from https://cyberscoop.com/travelex-sodinokibi-ransomware/

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. World Bank, 54, 1–54.

Sandler, R. (2019, July 29). Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested. Retrieved from Forbes: https://www.forbes.com/sites/rachelsandler/2019/07/29/capital-onesayshacker-breached-accounts-of-100-million-people-ex-amazonemployeearrested/

Siddique, N. A. (2019). Framework for the mobilization of cyber security and risk mitigation of financial organizations in bangladesh: a case study.

Somogyi, T., & Nagy, R. (2022). Cyber Threats and Security Challenges in the Hungarian Financial Sector. Contemporary Military Challenges/Sodobni Vojaški Izzivi, 24(3)

Уредба за одређивање критеријума критичне инфраструктуре и начину извештавања о критичној инфраструктури у Републици Србији (Службени гласник РС, бр. 69/2022).

CYBERATTACKS ON THE FINANCIAL SECTOR OF CRITICAL INFRASTRUCTURE

Jovana BRAJOVIĆ
Dejana JOVANOVIĆ POPOVIĆ, Full Professor

Summary

The financial sector of critical infrastructure represents one of the most vulnerable sectors when it comes to cyber attacks, due to its crucial role in the global economy and the nature of business today. The digitalization of finance opens the door to cyber attacks through the wide and pervasive availability of financial services on modern technologies and networks. This paper explores protective measures against cyber attacks in the financial sector by analyzing three significant incidents: the attack on the Central Bank of Bangladesh, the data breach at Capital One, and the ransomware attack on Travelex, a money transfer company. The primary aim of the research is to analyze the impact of cyber attacks on the financial sector of critical infrastructure and to identify effective protective measures that can reduce the risk of similar attacks in the future. By utilizing a review of international literature and case studies, the paper emphasizes the importance of integrating technological and organizational measures, as well as the significance of building cyber resilience through continuous improvement of security protocols and a culture of cyber awareness. The research findings indicate that while cyber attacks pose significant risks, they can also drive financial institutions toward innovation and enhancement of protective measures.

Keywords: *cyberattack, critical infrastructure, financial sector of critical infrastructure, protective measures against cyber attacks, cyber crime.*