Примљено: 08. септембар 2023.
Прихваћено: 06. октобар 2023.

351.817:578.834
COBISS.SR-ID 132361993
DOI: 10.5937/ssb2302153I

САЈБЕР БЕЗБЕДНОСТ ТОКОМ ПАНДЕМИЈЕ КОВИД-19

Маја ИЛИЋ, дипломирани менаџер безбедности*

* majai2307@gmail.com

САЈБЕР БЕЗБЕДНОСТ ТОКОМ ПАНДЕМИЈЕ КОВИД-19

Сажетак: *У раду је обрађена тема кризе ковида-19, која је захватила читав свет и из корена променила перцепцију целог света. Рад започиње основним терминима који се користе у сајбер безбедности, затим се даље обрађују врсте сајбер напада уопште, а касније ће бити речи о специфичностима напада који су вршени у току пандемије ковида-19. Описани су начини како су ти напади вршени, ко их је вршио и које организације су биле погођене. Представљена је табела са подацима о сајбер нападима у првих неколико месеци пандемије. Детаљније су обрађени напади на здравствене организације, нарочито оне укључене у борбу против ковида-19. Такође су обрађене одбрамбене и контрамере, као и начини како спречити такве нападе. Биће речи и о резилијентности, које су то кључне способности за отпорност организација за време криза. На крају ће бити речи о томе како се организација Светске банке понашала у новим условима пословања које је са собом донела пандемија и да ли је успела да се понаша резилијентно.*
Кључне речи: *пандемија, ковид-19, сајбер безбедност, сајбер напади, здравствене организације*

Увод

Пандемија ковид-19, која је захватила читав свет, била је јединствена и непредвидива. Пандемија је променила животе милијарди људи широм света, што је довело до „нове нормалности" која се односи на социјалне норме и начин живота током пандемије. Осим снажног утицаја на друштво и економију у целини, пандемија је створила и низ околности које се тичу сајбер криминала, које су такође утицале на друштво и економију. Повећано неповерење и анксиозност изазвано пандемијом повећала је вероватноћу да ће сајбер напади успети, што одговара повећању броја и опсега сајбер напада. У једном тренутку велики број људи био је „затворен" у својим домовима, многе фирме су привремено престале са радом или су прешле на режим рада

од куће, а самим тим људи су користили интернет више него икада. Јавља се и проблем досаде који доводи до преузимања разних садржаја са интернета који могу инфицирати уређаје корисника. За време пандемије људи су се осећали небезбедно, нису веровали својим владама из разлога што је постојало много различитих информација, па чак и много дезинформација, чија сврха и јесте општа паника и страх и усмеравање у погрешном правцу. Мере без преседана које су преузеле владе широм света имају поприличан утицај на друштво у целини. Организације широм света биле су приморане да веома брзо усвоје нове начине пословања, да се прилагоде новим условима – све је морало да се усагласи са мерама против пандемије. Само избијање пандемије учинило је организације веома подложним сајбер криминалу. Томе је највише допринела промена посла на даљину, односно преко интернета. Са друге стране, изненадан и убрзан одговор на пандемију створио је одређене безбедносне пропусте организација (Škiljić, 2020). Организације су приморане да дозволе својим запосленима да пређу на режим рада од куће, без нужног разматрања импликација сајбер безбедности. Обрадиће се основни појмови који се тичу сајбер безбедности, врсте сајбер напада уопште, а затим и врсте напада током пандемије ковида-19, као и напади на здравствене организације. Затим ће бити речи о одбрамбеној стратегији, као и контрамерама које се могу предузети ради заштите од сајбер напада. Такође ће бити представљена резилијентност сајбер безбедности током пандемије.

Основни појмови

Пре него што дубље уђемо у ову тему потребно је да дефинишемо неке основне појмове као што су сајбер безбедност и сајбер простор. Наравно, постоји много дефиниција ових појмова, али једна од обухватнијих гласи овако: „Сајбер безбедност, односно безбедност сајбер простора представља очување поверљивости, интегритета и доступности информација у сајбер простору" (The International Organization for Standardization, 2012). Поред тога, може се односити и на друге наративе попут аутентичности, одговорности, непорицања и поузданости. Иако општа, ова дефиниција је довољно прецизна јер означава које атрибуте је неопходно обезбедити. Појам сајбер безбедност има две целине:

1) Сајбер (енгл. *cyber*) – за коју можемо да кажемо да се односи на коришћење информационе технологије и рачунара. Састоји се од хардвера и софтвера;
2) Безбедност – која представља стање заштићености субјеката од разних облика угрожавања.

Сајбер простор „је измишљени простор у коме се одвија комуникација путем компјутера", али и других уређаја, „нарочито преко интернета" (Клајн и Шипка, 2012). Нешто комплекснија дефиниција, према „ISO/IEC 27032" стандарду, посматра сајбер простор као сложено окружење које је производ интеракције људи, софтвера и услуга на Интернету, које настаје помоћу технолошких уређаја и мрежа повезаних на њега, а које не постоји у физичком облику. Једноставно речено, сајбер простор је виртуелни, интернет простор.

Сајбер напад је „сваки офанзивни маневар који циља рачунарске информационе системе, рачунарске мреже, инфраструктуру, па чак и уређаје намењене личној употреби" (Computer Security Resource Center, 2023). Нападач може бити било која особа која има приступ интернету, односно сајбер простору. Оно што је кључно јесте да нападач покушава да приступи подацима, датотекама и другим поверљивим информацијама без овлашћења и са потенцијално злонамерном намером.

Сајбер напад могу извршити државе, појединци, групе, организације, али и анониман извор. Обично се служе сајбер оружјем ради остварења свог циља. А сајбер оружјем се обично сматра злонамеран софтвер који се користи за војне, паравојне и обавештајне циљеве. То могу бити рачунарски вируси, тројанци, "spyware" и црв који могу да унесу код у одређени уређај и на тај начин дођу до свог циља.

Врсте сајбер напада

Сајбер напад може бити активан или пасиван. Активан напад покушава да промени системске ресурсе или да утиче на њихов рад. Пасивни напад покушава да искористи или научи информације из одређеног система, али не утиче на системске ресурсе. Такво је на пример прислушкивање. Активан напад доводи у питање интегритет и доступност, док пасивни напад угрожава поверљивост. То су уједно три основна стуба сајбер безбедности „ЦИА" троугла.

Напад се може извршити унутар организације (интерно) или ван ње (екстерно). Унутрашњи, односно интерни напад покреће особа унутар организације – „инсајдер", то јест особа која је овлашћена да приступи системским ресурсима, али их користи на начин који није одобрен од стране надлежног лица. Спољни, односно екстерни напад долази из окружења, изван организације – „аутсајдер" који нема овлашћење приступа и који је нелегитиман (Shirey, 2000). Сајбер напади имају две категорије: синтетички и семантички напади.

Синтетички напади су једноставни, заправо то су злонамерни софтвери који укључују вирусе, црве и тројанце. Наведени злонамерни програми обично врше напад преко мејла, веб броусера, ажурирања и слично.

- Вируси су програми који се накаче на други програм или фајл како би се самореплицирали. Обично се крију на необичним локацијама у меморији уређаја и бирају најпогоднији фајл како би се реплицирали. Неки вируси мењају свој дигитални код приликом реплицирања, како не би био откривен.
- За разлику од вируса, црвима нису потребни други програми за реплицирање, потпуно су самостални. Они се реплицирају преко интернета, користећи протоколе. Новији црви користе већ познате рањивости уређаја, како за продирање тако и за реплицирање – познат је случај када је црв "Code Red II" заразио више од 259.000 система за мање од 14 сати (Janczewski and Colaric, 2007). Црви такође могу бити дизајнирани за индустријску шпијунажу.
- Тројански коњ је дизајниран тако да извршава легитимне задатке, међутим, он ради много више од тога – без знања корисника извршава и нежељене задатке. Тројанци могу бити уграђени у пробне верзије програма и тако могу прикупити податке о мети, а да особа ни не зна да се то дешава.

Семантички напад је ширење и модификација тачних и нетачних информација. Модификоване информације се могу урадити и без употребе рачунара, иако њихова употреба у ту сврху ствара нове могућности. Да би се неко усмерио ка погрешном правцу, или да нападач прикрије своје трагове, користи се ширење нетачних информација.

Питања сајбер безбедности током пандемије

Током пандемије ковид-19 сајбер криминалци и групе за напредну трајну претњу (енгл. *Advanced Persistent Threat*) искористили су предност новонастале ситуације за „гађање" рањивих система и људи. У наставку ће бити покушано установљавање корелације између пандемије и пораста сајбер напада у том периоду. Као што је већ речено, пораст анксиозности и страха због пандемије доводи до повећања стопе успешности сајбер напада. Наравно да су главне жртве ових напада здравствени системи различитих држава, јер је угрожена здравствена безбедност људи широм света. Пандемија је такође покренула питање сајбер безбедности у односу на нову нормалу – очекивање од запослених да раде од куће, што повећава могућности за фишинг (енгл. *phishing*) и рансомвер (енгл. *ransomware*).

Сајбер напади током пандемије

Категорије сајбер напада током пандемије:
1) Преваре и фишинг (енгл. *phishing*)
2) Малвер и дистрибуирано ускраћивање приступа систему (енгл. *DDoS*)

Сајбер криминалци и групе за напредну трајну претњу (Alshamrani, et al., 2019) (НТП) покрећу сајбер нападе на рањиве организације, као и људе путем превара и крађа идентитета повезаних са ковидом-19 (Xiao, et al., 2018). Они искоришћавају ситуацију произведену пандемијом ради остваривања одређене добити и прикупљања информација у вези са вакцинама против ковида-19 применом различитих техника као што су разни злонамерни софтвери. Примери ових напада током пандемију су "Hades" и "Patchwork/Dropping the Elephant".

Најчешћи, а уједно и најефикаснији напад током ове пандемије извршен је преко различитих врста превара и фишинга (NCSC, 2020a) (World Economic Forum, 2020). Заправо, фишинг напади имају стопу успешности од 30% и више. Веома је забрињавајућа чињеница што је нападачу потребно неколико кликова да оствари свој циљ, односно да би остварио финансијску добит или друге интересе. Они то раде тако што шаљу милионе мејлова жртвама, нудећи им помоћ у финансирању, која је током пандемије свима била преко потребна, коју обезбеђује влада, послодавци, банке и слично. И многи људи су се на то и

„упецали". Бројни фишинг напади садрже корона-вирус или ковид-19 као наслов не би ли „упецали" што више људи. У првом кварталу 2020. године дошло је до повећања од 600% фишинг напада е-поште повезаних са корона вирусом (Sjouwerman, 2020). Сајбер криминалци користе софистицираније технике како би намамили жртве, као што је коришћење „https" протокола за шифровање на својим веб локацијама. Заправо, око 75% фишинг сајтова је опремљено SSL-ом (енгл. *Security Sockets Layer*). Поред тога, корисници е-поште и "Software-as-a-Service (SaaS)" су највише циљани сектори за крађу идентитета.

Учестали напади током пандемије вршили су се и преко злонамерног софтвера (енгл. *malware*). Овај софтвер укључује рачунарске вирусе, црве, тројанске коње, шпијунски софтвер (енгл. *spyware*) и рансомваре (енгл. *ransomware*) (Legal Guidance, Cyber/online crime, 2019). Сајбер криминалци и групе за НТП искористили су ситуацију проузроковану пандемијом да нападну рањиве системе и људе различитим врстама малвера преко е-поште и веб локација. Заправо, 94% рачунара заражено је преко е-поште. Специфични типови малвера, какав је рансомваре (Arabo and Pranggono, 2013), ефикаснији су за институције које су у великој мери укључене у борбу против ковида-19.

Наравно, битно је поменути и "DDoS" нападе, односно дистрибуирано ускраћивање приступа систему, јер се данас сматра најнеодбрањивијим сајбер нападом. Овај напад искоришћава бројне изворе напада, шири се коришћењем више хостова за покретање координисаног „DoS" напада на једну или више мета, што појачава моћ напада и компликује одбрану (Asri and Pranggono, 2015). Ови напади користе се за подривање здравствених организација широм света.

Табела 1. Примери сајбер напада на медицинске установе током пандемије ковида-19

Датум	Држава	Тип напада	Детаљи напада
Март 2020.	Чешка Република	"Ransomware"	Универзитетска болница у Брну, као једна од лабораторија за тестирање на ковид-19 у земљи, погођена је сајбер нападом и била је принуђена да угаси целу своју ИТ мрежу (Cimpanu, 2020).
Март 2020.	Велика Британија	"Ransomware"	Група рансомвера "The Maze" је објавила личне и медицинске детаље о хиљадама бивших пацијената једне лондонске медицинске истраживачке компаније која се бави тестирањем на ковид-19 (Goodwin, 2020).
Март 2020.	Француска	"DDoS"	Овај напад пореметио је приступ серверу и имејлу групе болница у Паризу које играју важну улогу у борби против ковида-19 (Hale, 2020).
Мај 2020.	Тајван	"Phishing"	Е-поруке су садржале алатку за хаковање са удаљеног приступа, који се представља као тајвански званичник за заразне болести, позивајући примаоце да се тестирају на ковид-19 (Lyngaas, 2020a).
Јун 2020.	Немачка	"Phishing"	Слати су фишинг мејлови вишим руководиоцима у компанији која испоручује личну заштитну опрему. Они су усмеравали руководиоце на лажне странице за пријаву на „Microsoft" како би украли њихове податке (Lyngaas, 2020b).
Јун 2020.	САД	"Ransomware"	Универзитет Калифорније у Сан Франциску који ради на вакцини против ковида-19 био је мета напада рансомвера и приморан је да плати 1,14 милиона долара сајбер криминалцима званим „Netwalker" (Tidy, 2020).

Јун 2020.	Канада	"Ransomware"	"CryCryptor ransomware" се маскира као апликација за праћење ковид-19 контаката на андроиду (Osborne, 2020).

Сајбер напади на здравствене организације

Здравствени сектор је једна од главних мета сајбер напада током ове пандемије. Разни покушаји хаковања здравствених организација широм света истакли су проблеме сајбер безбедности у овом сектору. То се односи на здравствена тела, фармацеутске компаније и истраживачке организације. Здравствене организације су рањиве на сајбер нападе, што се види из примера из 2017. године када је напад "WannaCry ransomware" онеспособио Националну здравствену службу у Великој Британији. Један од главних разлога зашто су баш ове организације погодне за сајбер нападе огледа се у ограниченом буџету које ове организације имају како би заштитиле своје ИТ системе. То је последица тога што их обично финансирају градови, или земље које су под строгим буџетским контролама. У неким мање развијеним државама многе здравствене организације још увек користе застарели софтвер због недостатка средстава. Данас је технологија толико напредовала да модерним болницама управљају рачунари. Они се користе за складиштење и праћење података о пацијентима, али и за контролу медицинских уређаја који се користе у интензивној нези.

Заједнички саветодавни извештај и смернице Националног центра за сајбер безбедност Уједињеног Краљевства и Агенције за сајбер безбедност и инфраструктурну безбедност Министарства за унутрашњу безбедност САД пружили су дискусију о питањима као што су крађа идентитета, малвер, коришћени програми за рад од куће, као што је "Zoom" и слично (NCSC, 2020a). Предвиђено је да ће групе за НТП наставити да „гађају" здравствену заштиту и основне услуге на глобалном нивоу (NCSC, 2020b).

Заједнички саветодавни извештај Националног центра за сајбер безбедност Уједињеног Краљевства и Канадског комуникационог безбедносног института сугерише да руске обавештајне службе стоје иза сајбер напада "APT29" или „Удобан медвед" (NCSC, 2020c). Тај напад био је упућен различитим организацијама које се баве развојем вакцине против ковида-19. Како би остварили своје циљеве

коришћене су различите технике као што су: скенирање рањивости, јавна експлоатација и фишинг, а све у циљу добијања приступа циљаној мрежи и постављања малвера познатог као "WellMess" или "WellMail" ради проузроковања даље штете (NCSC, 2020c).

Одбрамбена стратегија и контрамере

У овом делу представиће се одбрана и контрамере сајбер нападима које се иначе препоручују компанијама, организацијама, као и корисницима интернета. Наравно, не постоје две исте организације, стога свака организација мора спроводити периодичну процену ризика за себе и на основу тога донети мере за заштиту својих података. Ако узмемо у обзир детаље ових напада, можемо их класификовати, према одбрамбеној стратегији, у оне засноване на мрежи ("network-based") и оне засноване на софтверу ("software-based").

Стратегије засноване на мрежи

Енкрипција података је један од основних начина заштите. Она омогућава корисницима да заштите поверљиве и личне податке. Циљ енкрипције је да спречи било кога ко жели да приступи подацима неког корисника, без дозволе, тако што учини те податке нечитљивим. Временом је развијен "IPsec – Internet Protocol Security", који омогућава шифровану, односно енкриптовану комуникацију између два компјутера преко "IP" адресе. "IPsec" омогућава поверљивост, интегритет и аутентичност порекла података. Он се користи већ неколико година за креирање приватне интернет адресе "VPN" између уређаја и мреже од поверења, која успоставља сигурне конекције на Интернет.

"SSL – Secure Socket Layer" је врста енкрипције која штити размену података између претраживача и сервера и онемогућава пресретање. Управо то спречава хакере да дођу до жељених информација. У суштини, "SSL" пружа сигурност како компанијама тако и муштеријама. Такође, вредно помена је и "Transport Layer Security" који се обично користи за мејлове, слање порука и гласовне команде, а обезбеђује сигурност комуницирања на интернету. И "SSL" и "TLS" се највише користе у осигуравању веб сајтова – "HTTPS".

Један од најбољих, по мом мишљењу, алата за заштиту може бити квантна криптографија. Представља перспективну надолазећу техно-

логију која истовремено производи два дела заједничког, тајног криптографског кључа користећи квантно стање светлости (Jang-Jaccard and Nepal, 2014). То је заправо систем који је у потпуности обезбеђен од компромитовања информација без знања лица које је поруку послало или примило. Практично није могуће копирати или чак прегледати податке у квантној криптографији а да власник не буде обавештен.

Стратегије засноване на софтверу

У зависности од процене ризика одређене организације, неки подаци могу бити заштићени само шифром. Уколико се тим информацијама приступа са неке друге локације користе се софистицираније методе попут биометријске аутентификације и „PIN" кода. Безбедност информација може се повећати тако што ће се правила приступа информацијама објединити у правилнику те организације, као и подизањем свести запослених.

Добар приступ заштите података јесте уклањање свих података који нису неопходни за свакодневну употребу. Архиве података треба да осигурају да се подаци чувају онолико дуго колико је то потребно, као и да буду изван пословне мреже јер то смањује ризик од неауторизованог приступа.

Криптографија је важна метода која осигурава размену података између корисника помоћу енкрипције података. То је најраспрострањенији механизам заштите података. "Advanced Hash Standard" је најскорија техника криптографије коју је развио амерички Национални институт стандарда и технологије. Користи се за апликације које укључују шифровање великом брзином као замену за „RSA" алгоритам 2048-битним кључем и за неизводљиво учешће органа за сертификацију (Karlsruhe Institute of Technology, 2019).

Сајбер напади и контрамере

Постоји неколико предложених техничких контрамера које се односе на сајбер нападе узроковане пандемијом ковида-19. Лични уређаји, попут мобилних телефона, компјутера и слично, представљају мету за хакере. Оно што свако може да предузме ради заштите јесте да се апликације и програми преузимају само из проверених извора, затим редовно скенирање уређаја ради откривања

могућих злонамерних програма. Такође једна од мера превенције јесте прављење резервне копије података.

Да би се спречили неауторизовани приступи подацима важно је периодично променити шифру приступа, као и избор адекватне и сложеније шифре. Уколико трећа страна више нема приступ одређеним подацима потребно ју је одмах уклонити и онемогућити даљи приступ.

Што се тиче фишинг напада, све поруке које садрже реч „Covid 19" и које садрже хиперлинкове који воде до потенцијално злонамерних сајтова потребно је пажљиво прочитати. Пре него што се порука отвори потребно је погледати ко је шаље, као и шта се тачно захтева. Требало би избећи одговарање на такве врсте порука и отварање линкова који се налазе у њима. Постоје системи за детекцију упада, као и за протекцију од истог који могу да буду вид заштите. Такође се препоручује употреба доброг антивирусног програма.

Резилијентност сајбер безбедности током ковида-19

Према Коту и Линкову (Kott and Linkov), кључни појам сајбер отпорности јесте прихватање подривања сајбер безбедности као могућности и да организација трпи због тога. Фокус јесте на способности организације да се опорави и адаптира, а не само да се одупре. Сајбер отпорност карактерише шта се десило током неког догађаја, а захтева припремљеност како за познате тако и за непознате претње (2019).

Холангел (Hollnagel) наводи четири способности/потенцијала отпорности – потенцијал за предвиђање, праћење, реаговање и учење. Способност предвиђања се односи на способност предвиђања догађаја у даљој будућности. Способност праћења односи се на то колико добро организација може да детектује промене услова рада. Организација мора бити свесна дешавања како у интерној тако и у екстерној средини. Способност реаговања подразумева знати шта треба учинити, као и способност правовременог и ефикасног одговора на дешавања. Способност учења представља свест о томе што се десило, као и способност да се учи из искуства. Даље, истиче да је учење правих лекција из правих искустава кључно (Hollnagel, 2017). Наравно, поседовање ових способности није гаранција отпорности током кризе. Организација која их поседује има веће шансе да се понаша резилијентно у односу на организацију која их нема.

Отпорност Светске банке

У наставку ће бити речи о томе како је пандемија ковида-19 утицала на способност Светске банке да остане сајбер резилијентна, односно да сачува своју способност да настави са радом и да се адаптира на нове услове пословања, како очекиваних тако и оних неочекиваних. Као и многе друге организације, тако је и Светска банка постала рањивија сајбер нападима у току пандемије. Прелазак на режим рада од куће је са собом донео нове и повећане ризике. Запослени су користили сопствену интернет мрежу док су радили од куће, што их излаже већем ризику од сајбер напада и пресретања информација од стране хакера. Поред тога, организације постају рањивије и изнутра јер се појављују запослени са малициозним намерама. Раније су се такви запослени брзо откривали, међутим, режим рада од куће то знатно отежава.

Иако се број фишинг напада повећао за време ковида, њихова успешност се мало повећала у односу на раније. Током пандемије Светска банка се суочила са нешто више сајбер напада него раније. Ти напади заправо нису створили велике проблеме за организацију јер су запослени радили од куће с времена на време и пре ковида. Међутим, када је утицај ових напада био већи одржани су састанци ради контроле кризе.

Горенаведене четири способности резилијентности биле су присутне, до одређеног нивоа, и пре пандемије. Ова организација има тим за сајбер претње која израђује квартални план претњи. Претње које је са собом донела пандемија нису биле предвиђене и стога се нису нашле у кварталном плану. Иако организација поседује одређене планове у случају избијања инфективне болести, они се односе на запослене те организације и предузимање потребних хигијенских мера. Међутим, ови планови нису могли да се примене на ситуацију током пандемије и донетих мрежа од стране влада.

Способност праћења може да се види у томе што је организација инвестирала у интерне извештаје о сајбер претњама и инцидентима. Успостављени су кључни индикатори учинка који се користе на дневном, недељном или месечном нивоу, како би се обавестили доносиоци одлука на време. Такође постоји и извештај ИТ департмана о безбедносним ризицима.

Способност реаговања види се у томе што су развијене способности управљања инцидентима. За сајбер претње Светска банка има широку способност реаговања на сајбер инциденте која непре-

стано ради. Наравно, она има блиску сарадњу са Организацијом за управљање ИТ инцидентима. Светска банка је такође развила способност која осигурава да организација може да настави са пружањем услуга у случају измењених услова пословања.

Способност учења види се на томе да се сваки инцидент процењује током састанака тимова за сајбер инциденте. За веће инциденте постоји формални процес учења који укључује и актере компаније, као и анализу узрока и план акције за будуће догађаје.

Када је пандемија избила организација је била у могућности да се адаптира и прошири капацитет за рад на даљину. Оно што је такође помогло Светској банци да се понаша отпорно јесте што су од самог почетка пандемије пратили ситуацију и били у контакту са Кином, где је ковид и избио.

Закључак

Пандемија ковида-19 отпочела је 2019. године у Кини и врло брзо је постала глобална и захватила читав свет. Комплетна људска популација суочавала се са истим изазовима током пандемије, али су се разликовали ресурси који су им били на располагању. Сиромашне и мање развијене државе имале су више потешкоћа да заштите безбедност својих грађана јер нису имале довољно средстава и ресурса на располагању. Неке богатије и развијеније државе нису бринуле о средствима за борбу против пандемије, али су се суочававале са неким другим проблемима. Због велике анксиозности и страха које је проузроковала пандемија људи су били неповерљиви према својим владама, били су принуђени да раде од куће и самим тим користе интернет више него икада. Сајбер криминалци су увидели ту чињеницу и дошли су до закључка да ће сајбер напади бити успешнији него раније. Осим жеље за остваривањем личне користи, сајбер напади су се дешавали и ради подизања панике међу људима, тако што се илегално приступи информацијама о пацијентима здравствених установа и њиховим објављивањем. Често су се појављивале информације како грађани немају праву и тачну информацију о оболелим и преминулим особама од ковида-19, што само повећава неповерење и панику. Током ове пандемије сајбер криминалци и групе за НТП искористиле су ову ситуацију за циљање рањивих система и људи. Заправо, то је ситуација за коју је мало вероватно да ће се променити у блиској

будућности. Здравствене организације су главне мете сајбер напада током пандемије из разних разлога. Због тога је кључно да здравствене организације побољшају заштиту важних информација и података, као и имовине од сајбер напада, а за то је неопходна имплементација свеобухватног приступа сајбер безбедности. Тај свеобухватни приступ би могао поћи од изградње четири потенцијала резилијентности и њиховом константном развијању и доградњивању. Неопходно је да свака организација за себе уради процену ризика од сајбер напада, те да ради на адекватним мерама које могу да се примене како би се такви догађаји спречили. Наравно, и поред тога, веома важан корак јесте упознавање запослених са тим процедурама и мерама, подизање њихове свести о томе и примена донетих мера. Било би корисно и да организације широм света донесу правилнике у којима ће јасно бити дефинисане процедуре и поступци у случају избијања неке нове инфективне болести која ће организацију приморати на нове услове рада. Организација мора да ради на својој адаптибилности, јер што се брже адаптира на новонастале услове рада то мање штети њеном пословању. Зато најпре, свака организација мора да идентификује ризике по њено пословање и постојање.

ЛИТЕРАТУРА

Kott, A., and Linkov, I. (2019). *Cyber Resilience of Systems and Networks.* Springer International Publishing.

Alshamrani, A., Myneni, S., Chowdhary, A., and Huang, D. (2019). *A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges and Research Opportunities.* New York: IEE.

Arabo, A., and Pranggono, B. (2013). *Mobile Malware and Smart Device Security: Trends, Challenges and Solutions.* Sheffield: Sheffield Hallam University.

Asri, S., and Pranggono, B. (2015). *Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure.* Sheffield: Shefield Hallam University.

Cimpanu, C. (2020, March 13). Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. *ZDnet*. Retrieved on https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

Computer Security Resource Center. (2023). *Cyber Attack.* National Institute of Standards and Technology (NIST). Retrieved on https://csrc.nist.gov/glossary/term/cyber_attack.

Goodwin, B. (2020, March 22). Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. *Computer Weekly*. Retrieved on https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus.

Hale, G. (2020). DDoS attacks on rise due to COVID-19. *Control Engineering*.

Hollnagel, E. (2017). The resilience potentials. In E. Hollnagel (Ed.), *Safety-II in Practice* (24–28). Routledge.

Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80,* 973–993.

Janczewski, L., and Colaric, A. (2007). *Cyber Warfare and Cyber Terrorism*. New York: Hershey.

Karlsruhe Institute of Technology. (2019). *Roadmap for cyber security research*. Karlsruhe, Germany.

Legal Guidance, Cyber/online crime. (2019, September 26). Cybercrime – prosecution guidance. *Crown Prosecution Service*. Retrieved on https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Lyngaas, S. (2020a, June 15). 'Vendetta' hackers are posing as Taiwan's CDC in data-theft campaign. *Cyber Scoop*. Retrieved on https://cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/.

Lyngaas, S. (2020b, June 8). Hackers target senior executives at German company procuring PPE. *Cyber Scoop*. Retrieved on https://cyberscoop.com/germany-ppe-coronavirus-hackers-ibm/.

NCSC. (2020a). *Advisory: COVID-19 exploited by malicious cyber actors.* London: National Cyber Security Centre. Retrieved on https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory.

NCSC. (2020b). *Advisory: APT groups target healthcare and essential services.* London: National Cyber Security Centre. Retrieved on https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory.

NCSC. (2020c). *Advisory: APT29 targets COVID-19 vaccine development.* London: National Cyber Security Centre. Retrieved on https://www.ncsc.gov.uk/news/apt-groups-target-healthcare-essential-services-advisory.

Osborne, C. (2020, June 24). New ransomware masquerades as COVID-19 contact-tracing app on your Android device. *ZDnet*. Retrieved on https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/.

Shirey, R. (2000). *Internet Security Glossary*. The Internet Society.

Sjouwerman, S. (2020, April 9). Q1 2020 Coronavirus-Related Phishing Email Attacks Are Up 600%. USA. *KnowBe4*. Retrieved on https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600.

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1,* 51–61.

The International Organization for Standardization. (2012, May 04). *ISO/IEC 27032 Standard.* Geneva: The International Organization for Standardization. Retrieved on https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

Tidy, J. (2020). How hackers extorted $1.14m from University of California, San Francisco. *BBC*.

World Economic Forum. (2020). *COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications.* Geneva: World Economic Forum. Retrieved on https://www.

weforum.org/publications/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications/.

Xiao, L., Xu, D., Mandayam, N., and Poor, V. (2018). *Attacker-Centric View of a Detection Game Against Advanced Persisten Threats.* New York: IEE.

Клајн, И. и Шипка, М. (2012). *Велики речник страних речи и израза.* Нови Сад: Прометеј.

CYBER SECURITY DURING COVID-19 PANDEMIC

Maja ILIĆ, Graduated Security Manager

Summary

The covid-19 pandemic has had a profound impact on the world, including exacerbating cybersecurity threats. This paper explores the various types of cyberattacks that emerged during the pandemic, the organizations that were targeted, and the methods employed by attackers. A particular focus is placed on attacks directed at healthcare organizations, which were particularly vulnerable due to the increased demand for their services. The paper also discusses defensive strategies and preventive measures that can be taken to mitigate cyberattacks, as well as the importance of organizational resilience in the face of crises. Finally, the paper examines the World Bank's response to the pandemic in terms of its ability to adapt to the new business environment and maintain resilience.

Keywords: *pandemic, covid-19, cyber, security, cyber attacks, health organizations.*