CYBER KRIMINAL I POSLOVANJE

CYBER CRIME AND BUSINESS

Džemal Kulašin*

SAŽETAK

Svjedočimo sve učestalijim i raznovrsnijim manifestacijama cyber kriminala koji svojim razmjerama ugrožava ne samo velike kompanije već i mala i srednja preduzeća uzrokujući ozbiljne zastoje u kontinuitetu poslovanja. Npr. prošle godine je čak 80% evropskih kompanija bilo izloženo barem jednom cyber udaru, gdje su apsolutno dominirali sofisticirani ransomware napadi kojih se na dnevnom nivou bilježilo čak i do 4000.

Cyber kriminal se, stoga, danas svrstava u vodeće korporacijske rizike, jer producira respektabilne finansijske troškove koji se na svjetskom nivou izražavaju u cca 500 milijardi dolara godišnje, prijeteći eksponencijalnim troškovnim rastom. No, znakovito je da se i pored svih objektivnih pokazatelja u velikom broju poslovnih sistema ne poklanja dovoljno pažnje zaštiti informacionih sistema, te se mjere često svode na interventno djelovanje u cilju uspostavljanja kontinuiteta poslovanja.

Posebnu ranjivost sistema, čak i brendiranim svjetskim kompanijama pokazali su upravo ransomware napadi, koji su jasno detektirali najslabiju kariku u zaštiti. Stoga je fokus ovog rada potenciranje te najslabije karike uz naglašavanje nekoliko mjera kako bi se prevenirali cyber napadi kojih će biti sve i više, samo u različitim manifestnim oblicima.

Ključne riječi: Cyber kriminal, poslovanje, ransomware, phishing, ISO 27001

SUMMARY

We are witnesses of increasingly frequent and varied manifestations of cyber crime which in its scale threatens not only large enterprises, but also small and medium enterprises causing serious deadlocks in business continuity. For example, in the last year about 80% of European enterprises were exposed to at least one cyber stroke, where sophisticated ransomware attacks were absolutely dominant, counting up to 4000 daily strikes.

Cyber crime is, therefore, nowadays classified into leading corporate risks, since it produces respectable financial expenses, which amount to, world-wide, cca 500 billion dollars annually, and are threatening with exponential growth in cost. However, it is significant that, regardless of all objective indicators in large number of business systems, there is not enough attention given to the protection of information systems, and those measures often bring down to intervention actions with the purpose of establishing continuity of business.

Particular system vulnerability, even in branded world enterprises, was demonstrated precisely through ransomware attacks, which clearly detected the weakest link in the protection. Therefore the focus of this paper is exponentiation of this weakest link along with pointing out several measures in order to prevent cyber attacks which will continue to grow in number, only changing their manifest form.

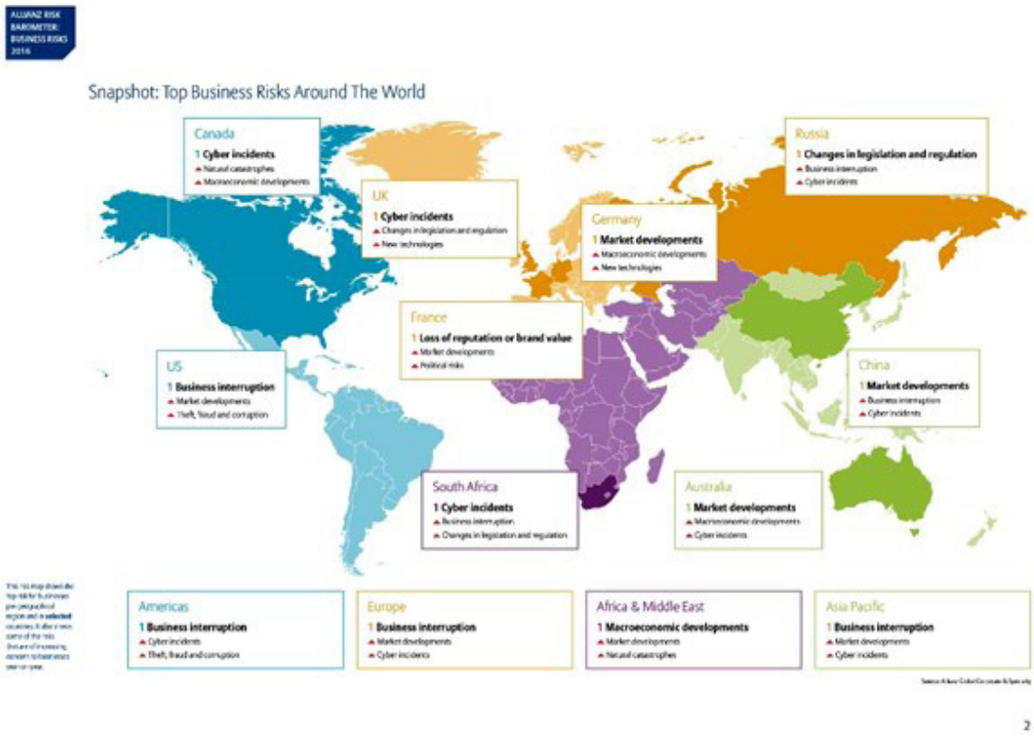
Keywords: Cyber crime, business, ransomware, phishing, ISO 27001

* - *Univerzitet u Travniku, Fakultet za menadžment i poslovnu ekonomiju, Kiseljak*

UVOD

Općenito, uslijed sve bržeg integriranja informatičke i telekomunikacijske tehnologije, pojam računarski kriminalitet postaje preuzak te se u stručnoj literaturi i svakodnevnoj praksi računarski kriminalitet zamjenjuje širim pojmom cyber kriminal (eng. cyber crime). Pojam cyber kriminal obuhvata sva krivična djela počinjena unutar cyber prostora uz pomoć ili na samoj informacionoj i telekomunikacijskoj tehnologiji, koja čini njegovu infrastrukturu. Jednostavnije, cyber kriminal[1] obuhvata skup krivičnih djela koja podrazumijevaju upotrebu Interneta, računara ili drugih elektronskih uređaja [1]. Dakle, slično računarskom kriminalu, i cyber kriminal predstavlja oblik kriminalnog ponašanja kod kojeg se korištenje računarske tehnologije i informacionih sistema ispoljava kao način izvršenja krivičnog djela, i gdje se računar ili računarska mreža upotrebljavaju kao sredstvo ili cilj izvršenja.

Kako je savremeno poslovanje obilježeno intenzivnim integriranjem informatičke i telekomunikacijske tehnologije, potpuno je jasno da su upravo kompanije postale poželjnom metom cyber kriminalaca. Tako se i potencijalni rizici sa kojima se suočavaju kompanije značajno mijenjaju i kompanije su sve manje zabrinute zbog učinka tzv. tradicionalnih rizika (prirodne katastrofe, konkurencija itd.) ali raste njihova zabrinutost u pogledu učinka tzv. netradicionalnih problematičnih događaja, posebno cyber incidenata [2,3]. Štaviše, u posljednje vrijeme čak se determinira i novi model cyber kriminala pod imenom CaaS (eng. Cybercrime-as-a-Service, odnosno Cyber-kriminal-kao-usluga), po uzoru na modele Cloud tehnologije, kao što su Saas (eng. Software-as-a-Service, Softver kao usluga) i Paas (eng. Platform as-a-Service, Platforma kao usluga), čime se ova vrsta kriminala komercijalizira te cyber kriminalci mogu ovakve vrste "usluga" naprosto i kupovati [4].



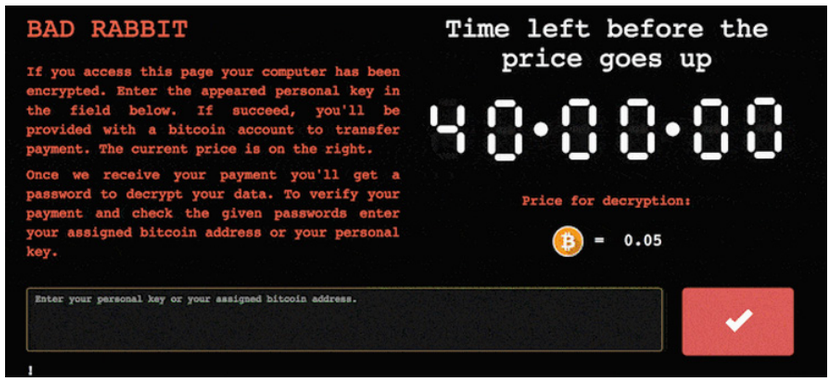
Slika 1: Rangiranje rizika za poslovanje u svijetu [2]

1 Nekad se označava i kao visokotehnološki kriminal ili e-kriminal

Bez dileme, otvoren je široki front: kompanije - cyber kriminal(ci) gdje kompanije bilježe veoma značajne finansijske gubitke, kako direktno zbog zastoja u poslovanju i troškova povratka podataka, tako i indirektno zbog negativnog utjecaja na imidž. Stoga, nije iznenađenje da su, prema istraživanjima[2], kompanije sve zabrinutije zbog rastuće sofisticiranosti cyber napada, njihove učestalosti i težine, ali je doista iznenađujuće kako se ova cyber "zabrinutost" kompanija ne implementira u praksi! Naime, gotovo polovina svih anketiranih kompanija (44%) nema nikakvu konkretnu strategiju u borbi protiv cyber kriminala, dok 48% kompanija uopće ne educira zaposlenike temama vezanim za cyber sigurnost. Još je drastičniji podatak da čak više od polovine kompanija (54%) nema nikakav sigurnosni protokol koji treba slijediti u slučaju da dođe do cyber napada [3]. Nasuprot toga, cyber napadi su iz godine u godinu sve učestaliji, te je, npr. prošle godine čak 80% evropskih kompanija bilo izloženo barem jednom cyber udaru, gdje su apsolutno dominirali ransomware napadi kojih se na dnevnom nivou bilježilo čak i do 4000 ("WannaCry", "Bad Rabbit" i sl.); pogotovo je ransomware, kao danas najprominentniji oblik cyber kriminala (iznova) pokazao da je ljudski faktor općenito najslabija karika u korporativnoj informacijskoj zaštiti.

2. RANSOMWARE NAPADI

Šta je, u stvari, ransomware? Ransomware je vrsta zlonamjernog softvera (eng. malware) koji u većoj ili manjoj mjeri ograničava pristup zaraženom računaru (tzv. locker ransomware), ili kriptira osjetljive podatke zaraženog računara (tzv. crypto ransomware), pri čemu je zajedničko da zahtjevaju plaćanje otkupnine[3], obično u bitcoinima, kako bi se ograničenje "uklonilo". Iako još uvijek široj javnosti ransomware zvuči kao novina na polju cyber kriminala, to ipak nije tačno, jer se prvi slučaj ransomware-a bilježi još 1989. godine. Bio je to "AIDS trojan" koji je na zaraženim računarima ispisivao do tada netipičnu poruku da žrtva u tačno određenom vremenskom roku treba platiti 189 dolara otkupnine na poštanski pretinac korporacije PC Cyborg u Panami, kako bi se trojanca riješili. Doduše, prve verzije ransomware-a nisu bile posebno uspješne jer se algoritam za dešifriranje, zbog tadašnjih slabih ključeva, vrlo brzo uspijevao razviti [5]. No, za razliku od početaka, današnji tipični ransomware programi su izuzetno opasni, jer jakim ključevima šifriraju osjetljive podatke, kao što su poslovni dokumenti, video snimci, fotografije i sl. Pritom, nastoje i da blokiraju procese antivirusnih i antispyware programa, uz istovremeno sakrivanje vlastitih procesa na napadnutom računaru bez aktivne opcije za deinstalaciju [6].



Slika 1: Poruka na računaru nakon infekcije ransomoware-om Bad Rabbit [7]

2 Kao ilustracija, u radu se navode rezultati istraživanja provedenom 2016. godine u 122 zemlje, na uzorku od 9500 ispitanika visoko pozicioniranim u tehnološkom sektoru različitih kompanija

3 U korijenu riječi ransomware je otkupnina; eng. ransom - otkupnina, wares - roba

Zanimljivo je da su poslovni sistemi, odnosno kompanije različitog obima, među prvim i glavnim ciljevima napadača ransomware-om. Razlog je što su njihovim sistemima baze podataka i servisi koji sadrže vrijedne informacije važne za poslovanje, a ujedno su takvi sistemi često slabo zaštićeni!? Kako je nemogućnost pružanja usluga za mnoge kompanije direktan gubitak prihoda i ugleda, u slučaju uspješnog napada često se odlučuju na plaćanje otkupnine kako bi što prije uspostavile kontinuitet poslovanja [5]. Tako je početkom ove godine ransomware "WannaCry" uzdrmao cijeli svijet (napad zabilježen u čak 150 zemalja!), kada je jakim zaključavanjem računarskih sistema napravio ozbiljne zastoje i u svjetski poznatim kompanijama poput: Renault-a, najvećeg francuskog proizvađača automobila, Telefonica-a, najveće španske telekomunikacijske kompanije, Deutsche Bahn-a, čuvene njemačke željezničke kompanije, američkog Fedex-a, itd.; "WannaCry" je čak zaključao i 70.000 računara u britanskim bolnicama, zbog čega je Britanski nacionalni zdravstveni sistem bio prisiljen da privremeno zatvori vrata brojnih odjela i hitne pomoći [8]. Ipak, iako se može činiti da su cyber kriminalu najviše na udaru velike kompanije, indikativno je da su glavna meta cyber napadačima ipak mala i srednja preduzeća sa 30-50 zaposlenih koja napadačima, uz male rizike donose visoke zarade, jer je nivo cyber zaštite u takvim poslovnim sistemima uglavnom na prilično niskom stepenu [9].

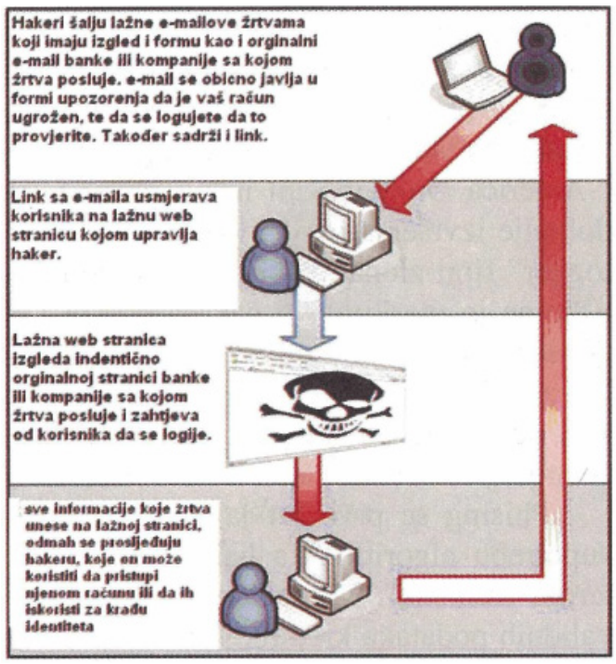
Jedno od važnijih pitanja je - kako se širi ransomware, i kako se računar njime zarazi? Ransomware se veoma često širi kao tzv. trojan, odnosno kao vrsta prikrivenog malware-a, gdje im dodatni impuls daju i sigurnosni propusti koji su relativno česti u pojedinim programskim paketima instaliranih na većini računara (Internet Explorer, Firefox, Adobe Acrobat Reader, Flash itd.); famozni "Wannacry" napadao je (neažurirane) računare na kojima nije bilo sigurnosne zakrpe MS17-010, namijenjene za operativne sisteme Windows XP(?!). Svi ovi sigurnosni propusti aktivno se iskorištavaju od strane tvoraca zlonamjernih kodova kako bi automatski zarazili računar žrtve. Takvi napadi poznati su i kao drive by download, jer korisnik nije svjestan da uz sadržaj koji preuzima sa Interneta na svoj računar preuzima i zlonamjerni sadržaj; to je upravo slučaj sa kriptovirusom "Bad Rabbit", koji je išao kao "regularna" instalacija Adobe Flash-a [6]. Uz to, treba naglasiti da pojedine vrste ransomware-a imaju i osobine crva (eng. worms), te se šire kompromitiranom mrežom zbog čega je dovoljno da samo jedan računar bude inficiran, i da cijela mreža bude dovedena u opasnost. Ipak, gotovo 90% inicijalizacije napada ransomware-om dolazi putem e-mail poruka, jer djelatnici neadekvatno reaguju na tzv. phishing [10].

2.1. Ransomware širenje putem phishing-a

Šta je, u stvari, phishing? U najkraćem, phishing predstavlja oblik savremenog cyber varanja, odnosno predstavlja kriminalnu radnju gdje cyber prevarant (eng. cybercrook) šalje e-mail s ciljem da prevarom dođe, npr. u posjed osjetljivih podataka korisnika kao što su brojevi kreditnih kartica, PIN-ovi, pristupni podaci bankama, matični brojevi i sl. Svi ovi podaci korisnika predstavljaju njegov digitalni identitet i ako napadač uspije u namjeri da ih preuzme, može ih zloupotrijebiti na različite načine i time steći značajnu finansijsku dobit, što najčešće i jeste krajnji cilj. Prvi konkretan napad ovom tehnikom zabilježen je u SAD-u 2001. godine, da bi već od 2004. godine phishing postao prepoznatljiv kao dio privrednog kriminala. Posljedice ovih napada u toj prelomnoj godini bile su dramatične, jer je preko 1,2 miliona korisnika u Americi bilo izvjesnim oblikom žrtve, uz evidentirane štete od 929 miliona dolara [11].

Iz konteksta ove kriminalne radnje očito je da se odnosi na "pecanje" on-line korisnika elektronskim mamcem, te je stoga i nastala karakteristična terminološka odrednica phishing kao sinonim riječi fishing (eng. pecanje). Iz terminološke odrednice pecanje

otkriva se i ciljanje hakera na nedostatke svijesti ali i spoznaje korisnika o načinima i tehnikama očuvanja informacijske sigurnosti. Zbog toga se ova vrsta cyber kriminala svrstava u tzv. socijalni inženjering, jer se koristi metodama zasnovanim na afektivnim segmentima pojedinca gdje se korist napadaču producira na "slabostima" žrtve u smislu lakovjernosti, ishitrenosti ali i neznanja. Sam način "preuzimanja" povjerljivih podataka dirigiran je tipom e-mail poruke koja se generira, gdje razlikujemo dva tipična slučaja, a) lažna e-mail poruka i b) klonirani e-mail.



Slika 3.1: Tok phishing napada [12]

Lažni e-mail nosi provokativni sadržaj za primatelja (npr. bankarski nalog je pred blokiranjem, i sl.), kako bi se korisnik naveo na ishitrenu reakciju, gdje se često kao prilog (eng. attachment) nalazi key-logger kao spyware za praćenje rada tipkovnice žrtve, a sve češće i neki od kriptovirusa iz skupine ransomware-a. Za razliku od ove vrste phishing napada, klonirani e-mail zloupotrebljava brend kompanije (poput eBay, Amazon, PayPal, VISA, America online i sl.) kako bi se korisnik naveo da utipka (i time "pokloni") svoje podatke na sajtu kojeg uobičajeno koristi za novčane transakcije. Ovaj tip Internet prevare predstavlja napredniji vid phishing-a označen kao pharming, što se u ovom kontekstu prevodi kao "uzgajanje žrtve" i "presretanje". Pharming napad je sofisticiraniji, i zahtijeva znatno viši nivo znanja napadača i računarske opreme. Koristi se koncept prevare gdje korisnika "na putu" do web sajta čiji URL utipkava čeka kompromitirani, klonirani web sajt na kojeg korisnik, sa punim povjerenjem, unosi svoje osjetljive podatke [12].

3. SISTEMSKI PRISTUP PROBLEMU CYBER KRIMINALA

Samo iz ove kratke analize ransomware napada može se uočiti koliko je potrebna stalna edukacija u vezi problematike cyber kriminala kako bi se razvijala (i mijenjala) svijest djelatnika o opasnostima iz cyber prostora. Jer, za uspješno provođenje korporativne informacijske sigurnosti potrebno je osigurati ljudski potencijal sa potrebnom razinom znanja i kompetencijama kako bi se učinkovito vladalo tehnikama i odgovorilo na sve brojnije i opasnije izvore

ugrožavanja [13]. U prilog ovome je i često zanemarena činjenica da informacijska sigurnost ne počiva na tehnologiji i programima već prvenstveno na ljudima, njihovom znanju i kompetencijama, te su glavni ključ (i) korporativne informacijske sigurnosti ipak - ljudi [9]. No, edukacija koja vodi znanju i kompetencijama ljudskih potencijala treba biti podrazumijevani segment savremenog sistemskog pristupa očuvanja informacijske sigurnosti.

3.1. (Pod)sistem informacijske sigurnosti

Sistemski pristup informacijskoj sigurnosti danas postaje nužan jer su potencijalne i stvarne prijetnje informacijama kao najvrijednijoj imovini poslovnih sistema, u uvjetima globaliziranog i komunikacijski potpuno povezanog poslovanja, postale tako velike da predstavljaju prioritetni poslovni rizik. U ovom kontekstu, može se govoriti i o fazama vezanim za pojam sigurnost, gdje je došlo do prerastanja tzv. IT sigurnosti u Informacijsku sigurnost i njenog daljnjeg razvoja kroz primjene standarda u ovom području. Tako je nastao i termin informacijska imovina i disciplina upravljanje informacijskom sigurnošću, za čiju odgovornost je postala nadležna uprava poslovnog sistema, a čiji reprezentant su ISO/IEC 2700x standardi. Neka obilježja ove faze su: politike informacijske sigurnosti, sigurnosne procedure, organizacija za sigurnost, CISO[4], auditi sigurnosti, certifikacija sustava sigurnosti, i sl. Konačno, dolazi se i do aktuelne faze odnosa prema informacijskoj sigurnosti, odnosno pojava i primjena koncepta korporativne informacijske sigurnosti (eng. Information Security Governance) [14]. Dakle, novi, (pro) aktivni pristup u kompanijama prema cyber kriminalu podrazumijeva uspostavljanje sigurnosne strategije uz definiranje jasne i provodljive sigurnosne politike, podržane od strane najvišeg menadžmenta, te njeno operacionaliziranje kroz (pod) sistem informacijske sigurnosti tzv. ISMS (Information Security Management System).

3.1.1. Standard ISO 27001

Podloga za uspostavljanje sistema informacijske sigurnosti danas je mahom standard objavljen od strane Međunarodne Organizacije za Standardizaciju (ISO) - ISO 27001, koji može biti implementiran u bilo kojem tipu organizacije, profitnoj ili neprofitnoj, privatnoj ili državnoj, maloj ili velikoj. Napisan od strane istaknutih svjetskih stručnjaka na polju informacijske sigurnosti, standard striktno propisuje metodologiju za primjenu sistema upravljanja informacijskom sigurnošću u organizaciji. Pomaže i omogućava da se uspostavi dosljednost zaštite u čitavom preduzeću, sadržavajući potrebne sigurnosne provjere[5] koje se odnose na implementaciju određene tehnologije, hardvera ili softvera; npr. standard za lozinku može da postavi pravila o njenoj kompleksnosti, redovitost u provođenju sigurnosnih kopija (eng. backup), kao spasonosnog rješenja u slučaju uspješnog cyber incidenta, itd. [15].

Struktura standarda ISO/IEC 27001 je sveobuhvatna, tako da obuhvata ključne segmente informacijske sigurnosti: (1) administrativni aspekt, gdje se definiraju jasna uputstva, politike i procedure za generiranje informacija, njihovu distribuciju, čuvanje (skladištenje) i sl., (2) fizički aspekt, gdje se utvrđuje fizička kontrola pristupa, evidencija zaposlenih, video nadzor, zaštita radnih prostorija i sl. i (3) informatički aspekt, gdje se analiziraju se i definiraju performanse IT opreme, prava pristupa, kriptovanja, lozinke, protokoli, politike sa aspekta pojave rizika po sigurnost podataka i informacija.

Benetife standarda ISO/IEC 27001 možemo promatrati dvojako, iz pragmatičnog i marketinškog ugla. Gledano iz marketinškog ugla, kompanijama je omogućeno dobijanje certifikata, što znači da neovisno certifikacijsko tijelo daje potvrdu kompaniji da je implementirala informacijsku

4 CISO - akronim od: Chief Information Security Officer - Voditelj sigurnosti informacijskog sistema

5 Krucijalni dio dio standarda, tzv. Aneks A

sigurnost sukladno ISO 27001. No, puno je važniji pragmatični pogled, jer se broj cyber incidenata u certificiranim kompanijama drastično smanjuje te općenito raste povjerenje kako djelatnika tako i klijenata u pogledu cyber sigurnosti kao dijela opće korporativne informacijske sigurnosti [16].

ZAKLJUČAK

Cyber kriminal se svrstava u prve dugoročne rizike za poslovanje u sljedećih deset godina, jer uzrokuje direktne i indirektne štete koje se izražavaju u stotinama milijardi dolara. Njegov intenzitet i pojavni oblici dosegli su nivo da praktično i nema kompanije koja nije (bila) napadnuta, ili da određeni cyber napad traje, ali zbog (neočekivanog) izostanka odgovarajućih mehanizama monitoringa i zaštite, sigurnosni incident uopće se i ne registrira. Zbog toga je razumljivo što se o ovoj problematici intenzivno raspravlja na različitim nivoima, u cilju iznalaženja najboljih rješenja u cilju ublažavanja[6] ovog prijetećeg korporativnog rizika.

U ovom radu ciljano su analizirane manifestacije ransomware-a, kao najprominentnijeg i najštetnijeg oblika cyber kriminala[7], kako bi se "ukazalo" na slabu kariku korporativne informacijske sigurnosti. Pored ostalog, pokazano je da ransomware-i očito spadaju u kategoriju tzv. socijalnog inženjeringa, i u manjoj mjeri su tehnički sofisticirani te usmjereni na iskorištavanje ljudskih slabosti gdje kriminalci računaju na neracionalno razmišljanje žrtve zbog vremenskog ograničenja za plaćanje otkupnine.

Dakle, iz izloženih karakteristika ransomware napada može se zaključiti da je dominantni razlog "uspješnosti" cyber kriminala(ca) upravo - ljudski faktor. Sa jedne strane, radi o neprovođenju sigurnosnih mjera od strane djelatnika, pogotovo kada se radi o korištenju različitih servisa Interneta (npr. otvaranje sumnjivih e-mail poruka, preuzimanje priloga e-mail poruka od nepoznatih pošiljaoca, preuzimanje nekomercijalnog software-a sa nesigurnih web lokacija i sl.) dok je, sa druge strane, evidentno i izostajanje korporativne informacijske strategije uz različite negativne implikacije koje iz toga proizilaze (npr. neažuriranje aplikativnog i sistemskog software-a, nedosljednost u provođenju backup-a i sl.). Stoga, proizilazi i konačni zaključak rada formuliran kao nužnost kontinuiranog provođenja sigurnosne edukacije djelatnika u okviru sistemskog pristupa problematici cyber kriminala, odnosno očuvanju korporativne informacijske sigurnosti u općem smislu.

6 Eliminiranje ove vrste rizika je gotovo nemoguće, i realno je govoriti samo o njegovom ublažavanju do prihvatljivog nivoa

7 Samo u dvije posljednje godine, štete kompanijama od ransomware porasle su za čak 15 puta!

LITERATURA

[1] Begović, S., 2016, Kako se boriti protiv visokotehnolškog kriminala, Razvoj elektronskog poslovanja, Beograd, dostupno na: https://europa.rs/images/publikacije/Kako-se-boriti-protiv-visokotehnoloskog-kriminala.pdf

[2] ALLIANZ Zagreb d.d. za osiguranje, 2016, Allianzov barometar rizika za 2016, dostupno na https://www.allianz.hr/privatni-korisnici/press/objave-za-medije/allianzov-barometar-rizika-za-2016-godinu/

[3] Deželić, V., 2017, Velike tvrtke, organizacije iinstitucije neuspjevaju se pripremiti za cybernapade, dostupno na: http://www.ictbusiness.info/internet/velike-tvrtke-organizacije-i-institucije-ne-uspjevaju-se-pripremiti-za-cyber-napade

[4] Robinson, M., 2016, Cybercrime-as-a-Service poses a growing challenge, Security Intelligence, dostupno na: https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/ [pristup: 27.11.2017]

[5] CARNET, 2017, Ransomware - plati za svoje podatke, dostupno na: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2017-2-346_0.pdf

[6] Doevan, J., 2016, Šta je ransomware i kako ukloniti takav program, dostupno na: http://virusi.hr/ransomware-programi/
[7] Kessem L., 2017, Bad Rabbit ransomware attacks highlight risk of propagating malware outbreaks, Security Intelligence, dostupno na: https://securityintelligence.com/bad-rabbit-ransomware-attacks-highlight-risk-of-propagating-malware-outbreaks/
[8] Span, 2017, Prijeti li ransomware wannacry i vama, dostupno na: https://span.eu/2017/05/prijeti-li-ransomware-wannacry-i-vama/ [pristup: 03.11.2017]
[9] Đekić, M.,D., 2015, Kako sačuvati kontinuitet poslovanja uprskoj cyber incidentima, Tehnika - Menadžment, No. 65, Vol. 2, pp. 346-349.
[10] Economist Intelligence Unit, 2017, Combating fraud in the digital economy, dostupno na: http://rethinkpayments.economist.com/uk/combating-fraud-in-the-digital-economy
[11] Baća, M., Čosić, J., 2014, Prevencija računalnog kriminaliteta, Časopis "Policija i sigurnost" Zagreb, Broj 1, p. 146-158
[12] Hanić, H., Sućeska, M., 2008, Kompjuterski kriminal - pojavni oblici i preventiva, Fakultet kriminalističih nauka, Sarajevo
[13] Visoka škola za sigurnost & Centar za poslovnu sigurnost, 2016, Korporativna informacijska sigurnost, Savjetovanje, 04.10.2016 Zagreb, dostupno na: http://ustanova-ctz.hr/savjetovanje-korporativna-informacijska-sigurnost/
[14] Krakar, Z. i dr., 2014, Korporativna informacijska sigurnost, Fakultet organizacije i informatike Varaždin, Zagreb.
[15] Samardžić, J., 2015, Informaciona bezbednost - Pretnje za koje se moramo pripremiti, dostupno na: http://www.coming.co.rs/business_it/business_it_4
[16] Adelsberger, Z., 2015, Implementacija ISMS prema ISO /IEC 27001/2013, ICT Security Kladovo, 14.-16.maj 2015, dostupno na: http://www.slideshare.net/dejanjeremich/adelsberger-zdenko-implementacija-iso27001-2013