Nebojša Jeremić[1], Nemanja Jakovljević[2], Miloš Jeremić[3]

STRUČNI RAD
UDK 343.9:004.738.5
DOI: 10.56362/Rev22100057J

ULOGA INTERNE REVIZIJE U SMANJENJU RIZIKA OD RANSOMVERA

UVOD

Iako je lista rizika u oblasti sajber bezbednosti dugačka i često se dopunjuje i menja, ransomver se i dalje nalazi u samom vrhu te liste, kao pretnja visokog rizika po bezbednost organizacije. Uopšteno posmatrano, pored toga što može da dovede do potpunog zaustavljanja poslovnih operacija, može i da izazove probleme poput curenja podataka i narušavanja poslovnog ugleda i reputacije. Imajući u vidu pomenutu ozbiljnost rizika od ransomvera, interni revizori bi trebalo da imaju za cilj da pomognu svojim organizacijama da smanje ove pretnje, zajedno sa ukupnim rizicima za sajber bezbednost. Kako su pretnje ransomverom poprimile ozbiljne razmere, interni revizori mogu da igraju vitalnu ulogu u pregledu aktivnosti i pružanju suda zasnovanog na relevantnim dokazima, upućenog menadžmentu i revizorskom odboru sa ciljem da razumeju rizike informacione i sajber bezbednosti organizacije, njegovu sposobnost da odgovori na njih i raspoložive mogućnosti za potencijalni oporavak (5, 2). Postoji više načina za ulazak ransomvera u informacioni sistem, a najčešći su napadi koji uključuju pokretanje iz neotkrivenih softverskih ranjivosti, ili kada zaposleni otvori e-poruku i klikne na vezu koja oslobađa zlonamerni virus. Virus, ubačen na jedan od pomenuta dva načina, može da prodre u centar poslovnih operacija i natera organizacije da razmotre plaćanje višemilionske otkupnine. Kako se napadi na informacione sisteme organizacija ubrzavaju i prilagođavaju izmenjenom okruženju u postkovid uslovima, ključna uloga interne revizije je evoluirala. Interna revizija danas mora da razmišlja kako da pomogne organizaciji da predvidi, da se pripremi i da odgovori na eventualne napade ransomverom. Ukupna otpornost na sajber bezbednost je kritičan faktor u odbrani od napada ransomvera. To zahteva od organizacija da osnaže kapacitete

REZIME

Iako je lista rizika u oblasti sajber bezbednosti dugačka, ransomver (ransomware) se i dalje nalazi u samom vrhu, kao pretnja visokog rizika po bezbednost organizacije. Ransomvare može da dovede do potpunog zaustavljanja poslovnih operacija i narušavanja poslovnog ugleda i reputacije. Cilj ovog radaje da ispita ulogu interne revizije u smanjenju rizika od ransomvera. Glavni zaključak je da efikasno otkrivanje ransomvera uključuje kombinaciju tehnologije i znanja, u čemu su najbolji način za odbranu preventivne aktivnosti, a funkcija interne revizije može značajno da pomogne u tome.

Ključne reči: ransomver (ransomware); sajber rizici; sajber pretnje, sajber bezbednost; sajber osiguranje, model tri linije.

[1] Doktor nauka i viši interni revizor za finansije i računovodstvo, Telekom Srbija a.d., e-mail: nebojsaje@telekom.rs
[2] Student doktorskih studija Ekonomskog fakulteta u Beogradu, e-mail: jakovljevic.i.nemanja@gmail.com
[3] Diplomirani ekonomista i master pravnik, e-mail: milos.jeremic@rocketmail.com

i otpornost na sajber napade koji se ne mogu predvideti ili predupredi. Stoga je neophodna bliska saradnja sa dobavljačima usluga i softverskih rešenja, industrijskim grupama, odnosno članovima komora, kupcima, agencijama i međunarodnim udruženjima, bezbednosnim analitičarima i drugim učesnicima u lancima snabdevanja.

Da bi formirale koordinisanu odbranu, organizacije moraju da obezbede da njihove sistemske i aplikativne kontrole ostanu ažurirane i efikasne u postupcima upravljanja bezbednosnim incidentima u informacionom sistemu organizacije. Interna revizija može da ima neprocenjivu ulogu u proceni poslovnog okruženja i rizika po poslovanje, obavljanju tehničkih revizija rukovođenih promenljivim rizicima, pregledu i oceni implementirane sajber bezbednosti, saopštavanju rezultata i obezbeđivanju izveštavanja odbora za reviziju i menadžment (4, 3). Veoma efikasan način za procenu internih kontrola je korišćenje okvira zasnovanog na riziku. Interna revizija može da iskoristi sveobuhvatne standarde kao što su standardi u seriji NIST 800. Publikacije SP 800 su razvijene da bi podržale potrebe bezbednosti i privatnosti informacija i informacionih sistema Savezne vlade SAD i da pruže praktične smernice o tome kako se baviti opipljivim rizicima i tehničkim kontrolama (41, 1). Kada je interna revizija u toku sa trendovima u sajber bezbednosti i vodećim pozitivnim praksama, ona je u dobroj poziciji da nezavisno prati otpornost organizacije na bezbednosne napade i incidente. Interni revizori nesumnjivo aktivno propagiraju potrebu da organizacije moraju da krenu u ofanzivu agresivnim testiranjem svojih odbrambenih mera. Međutim, iako je tim za odgovor na incidente taj koji će igrati glavnu ulogu tokom neposrednog odgovora na napad ransomvera, najvažnija uloga interne revizije se ogleda u prevenciji napada i kasnije, ukoliko se napad dogodi, u sagledavanju neadekvatnih kontrola i oporavku celokupnog poslovnog sistema. Sposobnost revizije da obezbedi nezavisnu analizu, profesionalno uveravanje, da primeni usvojena znanja i da sprovede reviziju informacione bezbednosti će svakako značajno koristiti organizaciji kod predupređivanja nastanka budućih pretnji i smanjivanja uticaja budućih sajber napada (26, 4).

Interna revizija sagledava mogućnosti za prevenciju napada ransomvara i adekvatnost kontrola i mogućnosti za oporavak poslovnog sistema, ukoliko se napad dogodi.

Ransomver je vrsta zlonamernog softvera, odnosno virus koji preti da objavi ili blokira pristup podacima ili računarskom sistemu i to pretežno na način da ih šifruje, sve dok targetirana žrtva ne plati otkupninu (11, 3). U mnogim slučajevima, zahtev za otkupninu je praćen rokovima i instrukcijama za uplatu, a sve je češća pojava da se uplata otkupnine zahteva u kriptovalutama (24, 1). Ako targetirana

žrtva ne plati otkupninu na vreme, podaci zauvek nestaju ili se iznos otkupnine povećava, sa novim rokovima za plaćanje. Kada virus uđe u računar, tajno ga inficira, napada datoteke i menja kredencijale za logovanje (10, 2). Kao rezultat toga, kompjuterska infrastruktura je talac osobe koja kontroliše virus (34, 1). Vlasnik računara ne može da pristupi zaraženim datotekama, osim ako ne plati otkupninu napadaču. Napadač je jedini koji može da pristupi datotekama, jer su skrivene iza lozinke za šifrovanje. Ponekad će napadač zaključati ceo računar, a zatim zatražiti otkup pre nego što objavi novu lozinku (40, 1).

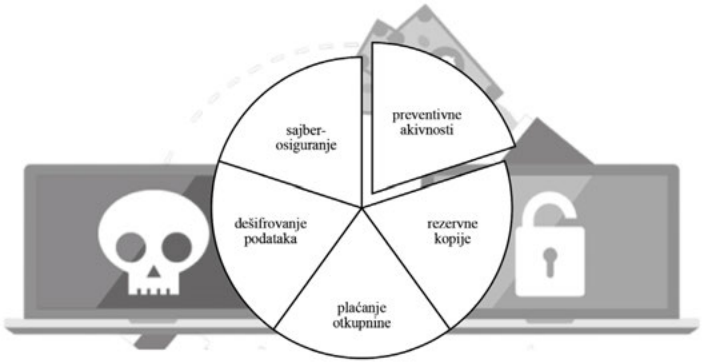
Organizacije sa privatnim vlasničkim informacijama, kao što su patenti, katastri, sudski spisi, podaci socijalne zaštite ili zdravstveni kartoni, mogu se naći kao poželjna meta. Napadi ransomverom usmereni su na organizacije koje imaju hitnu potrebu da pristupe svojim datotekama, kao što su organizacije koje zavise od baza podataka ili aplikacija za vođenje evidencije o poslovanju. Menadžeri takvih organizacija mogu biti skloni zaključivanju da će, iako napadač traži određenu sumu, izgubiti mnogo više ukoliko se prekid poslovanja nastavi, nego ako plate traženi iznos otkupnine. Svako ko ima informacije o korisnicima čiju privatnost zaista želi da zadrži, može se naći na meti. Napadač može imati saznanja koliko su podaci o privatnosti važni za targetiranu žrtvu i naplatiće joj veliku naknadu u zamenu za neobjavljivanje njenih podataka. U stvari, ransomver čak i ne mora da se šalje od napadača direktno na računar žrtve. Može se širiti samostalno. Virus može da bude ugrađen u internet oglas koji izgleda uobičajeno. Svako može kliknuti na njega i na kraju postati žrtva (30, 1). Iako su napadi najčešći na desktop i laptop računarima, svaki uređaj sa operativnim sistemom može postati žrtva. Ovo uključuje mobilne telefone, tablete i druge mobilne uređaje koji su jeftini i pristupačni (23, 1). S druge strane, softverska rešenja pomoću kojih se napada jeftina su i lako dostupna na mračnom vebu (*dark web*), a neki od novijih napada ransomvera izvedeni su pomoću virusa koji je jeftin i lako ga je pronaći. Cilj rada je da ispita ulogu interne revizije u smanjenju rizika od ransomvera analizom odgovora na ransomver, mera zaštite i *Modela tri linije*.

Ransomver ne mora da šalje napadača direktno na računar žrtve, jer se može širiti samostalno.

ODGOVOR NA RANSOMVER I MERE ZAŠTITE

Ransomver se distribuira različitim metodama, uključujući zaražene veb-lokacije, onlajn reklame i univerzalne serijske magistrale (USB), direktnim napadima, poput fišinga

(*phishing*), e-pošte ili URL adresa (31, 1). Generalno posmatrano, postoji više načina za odgovor na napad ransomverom sa različitim stepenom efikasnosti u različitim situacijama, a neki od njih mogu da uključuju preventivne aktivnosti, izradu rezervnih kopija podataka, dešifrovanje podataka, sajber osiguranje i plaćanje otkupnine (kao krajnja mera), o kojima će biti više reči u nastavku.



Izvor: Autori

Grafikon 1: Načini odgovora na ransomver

Rezervna kopija se odnosi na kopiranje fizičkih ili virtuelnih datoteka ili baza podataka na sekundarnu lokaciju radi očuvanja u slučaju kvara opreme ili katastrofe. Proces pravljenja rezervnih kopija podataka je ključan za uspešan plan oporavka od štete. Organizacije kreiraju rezervne kopije podataka za koje smatraju da su ranjivi u slučaju grešaka u softveru, oštećenja podataka, kvara hardvera, zlonamernog hakovanja, grešaka korisnika ili drugih nepredviđenih događaja (33, 2). Rezervne kopije snimaju i sinhronizuju snimak u trenutku koji se zatim koristi za vraćanje podataka u prethodno stanje. Kada se napad ransomvera identifikuje i zaustavi, tipičan odgovor je vraćanje pogođenih datoteka preko rezervnih kopija. Problem sa ovom opcijom je u tome što je ransomver možda zarazio mrežu pre aktivacije, a za to vreme su rezervne kopije ili arhivske datoteke takođe mogle biti šifrovane. Zato nije dovoljno samo kreirati rezervne kopije, nego je potrebno i zaštiti ih od napada, a to je moguće tako što će virusi biti zaustavljeni pre nego što stignu do rezervne kopije, jer zaražena rezervna kopija je beskorisna. Čak i ako se ransomver ne aktivira na drajvu rezervne kopije, može preko nje da inficira zaštićeni uređaj. Fokusiranje na uklanjanje ransomvera sa rezervnog servera je pogrešan pristup. Jedini način da se na adekvatan način zaštite rezervne kopije od ransomvera je da se virus spreči da dođe

do njih. Tradicionalno pravilo za pravljenje rezervnih kopija naziva se *3-2-1 sistem*. Ovaj sistem zahteva tri kopije svih datoteka na sistemu, i to: originalni fajl, kopiju u sistemu na drugom mediju i kopiju van sistema. Mnogi sistemski administratori preporučuju da se prva rezervna kopija koja se čuva na licu mesta sačuva na prenosivom mediju za skladištenje podataka, kao što je DAT traka. Druga kopija se čuva na licu mesta, dok se treća kopija čuva van lokacije.

Postoje tri vrste rezervnih kopija, i to:
1) potpuna rezervna kopija (u kojoj se kopira sve);
2) diferencijalna rezervna kopija (u kojoj se kopira sve što se promenilo od poslednje potpune rezervne kopije) ;
3) inkrementalna rezervna kopija (u kojoj se kopira sve što se promenilo od poslednje rezervne kopije bilo koje vrste).

Diferencijalno i inkrementalno pravljenje rezervnih kopija brže je od potpunih rezervnih kopija. Međutim, to je izazovno za izvođenje na DAT traci (32, 4). Traka je bolja za pune rezervne kopije. Izbor adekvatne rezervne kopije u velikoj meri zavisi od veličine organizacije, izloženosti riziku od ransomvera i složenosti poslovnih aktivnosti. Iskustveno, menadžerima se savetuje da implementiraju pravljenje potpune rezervne kopije jednom nedeljno i inkrementalne ili diferencijalne rezervne kopije jednom dnevno. Umesto da organizacija pravi inkrementalnu rezervnu kopiju koja briše ranije rezervne kopije određenih datoteka, sistem može da čuva originalno stanje dok posebno čuva novu verziju. Međutim, s obzirom na to da se te verzije obično drže na istom disku, infekcija ransomverom u najažurnijoj verziji će inficirati sve verzije. Napadi ransomverom će se najverovatnije desiti tokom radnog vremena jer ih aktivnosti korisnika obično pokreću. U ovim slučajevima moguće je isključiti sistem i zatim ga vratiti iz rezervne kopije. Ovo će privremeno izbrisati sve transakcije tog dana. Međutim, ovo će obezbediti da se virus izbriše. Kada se sistem vrati i korisnici dobiju većinu svojih podataka, IT stručnjaci će imati vremena da pregledaju inkrementalnu rezervnu kopiju van lokacije, uporede verzije datoteka i razmotre gde mogu da obezbede ažurniju verziju određenih datoteka.

Napadi ransomverom dešavaju se tokom radnog vremena jer ih obično pokreću aktivnosti korisnika.

Dešifrovanje datoteka može da bude još jedan dobar način da se odgovori na ransomver. Jedna opcija je korišćenje besplatnih alata, a druga opcija je traženje pomoći od organizacija koje se bave sajber bezbednošću. Treća opcija je da se pribavi pomoć od državnih organa, kao što su Ministarstvo unutrašnjih poslova (na primer Odeljenje za suzbijanje

visokotehnoloskog kriminala), nacionalni CERT ili bezbednosno-informativna agencija. Plaćanje otkupnine dovodi organizaciju u opasnost da ne povrati podatke i da ugrozi koncept kontinuiteta poslovanja. Kada se izabere ova opcija, oporavak je težak i može potrajati dugo. Korišćenje sajber osiguranja može biti deo ove opcije. Plaćanje otkupnine sa sobom povlači rizik da organizacija ponovo bude targetirana, da joj se uskrati ključ za dešifrovanje uprkos plaćanju otkupnine, da bude primorana da plati više za obećani ključ i da na taj način pruži podršku sumnjivim i prevarenim aktivnostima. Tako dolazimo do preventivnih aktivnosti koje su najbolji način za odgovor na ransomver jer obezbeđuju formiranje zaštitnog zida za odbranu od njega, a one između ostalog mogu da uključe i angažovanje odeljenja za internu reviziju. Prevencija uključuje primenu zaštitnih mera koje se smatraju najboljom sajber praksom u oblasti mrežnih procesa, konfiguracije i arhitekture. Bezbednost informacija može da se poboljša primenom softvera za praćenje ponašanja i novih tehnologija i korišćenjem bezbednog filtriranja bezbednosnog protokola za prenos hiperteksta (HTTPS) za sav veb-saobraćaj. Host Intrusion Prevention Service (HIPS) i druge tehnologije bez potpisa su neophodne za snažnu sajber odbranu, zajedno sa pregledom i primenom plana odgovora na incidente. Korisnički interfejs nikada ne treba zanemariti, jer korisnici mogu biti najslabija karika kada je u pitanju bezbednosti. Važna je obuka za zaposlene o bezbednosti, u kombinaciji sa simuliranim fišing napadima na redovnoj osnovi i obučavanje korisnika da se povezuju samo na sajtove koji koriste kriptografiju (HTTPS) i da koriste vezu virtuelne privatne mreže (VPN) za daljinski pristup. Ispitivači penetracije mogu utvrditi da li će napadači moći da pronađu rezervne kopije. Datoteke rezervnih kopija podataka su mete napada ransomvera, ali ako se ne mogu pronaći, organizacija će moći da se oporavi od napada. Mere zaštite konfiguracije uključuju mapiranje disk jedinica i skrivanje mrežnih deljenja tako da počinioci ne mogu da pronađu ključna sredstva. Najbolji način je konfigurisanje kontrole pristupa i naloga da funkcionišu na principu najmanje privilegija. Primena politike ograničenja softvera i politike pristupa bez poverenja se može smatrati korisnom. Ako potencijalni napadači ne mogu da uđu, možda neće moći da šifruju datoteke sa podacima ili aplikativni softver. Blokiranje reklama, zlonamernih linkova i onemogućavanje makroskripti unapređuje mogućnost korišćenja pomoćnih programa ili rutina u memoriji. Poboljšanja u arhitekturi mreže uključuju kategorizaciju podataka na osnovu vrednosti razdvajanje mreža i

Korisnici mogu biti najslabija karika kada je u pitanju zaštita od ransomvera.

podataka po fizičkoj i logičkoj osnovi. Smanjenje površine napada putem segmentacije mreže dovodi do bolje zaštite imovine visoke vrednosti. Podaci se mogu zaštititi ili tako što se osetljivi podaci ne povezuju na internet, ili kreiranjem skrivenog prostora za skladištenje. Instaliranje i održavanje zaštite i detekcije zasnovane na softveru, kao što su antivirusni, antispam i antiphishing softveri, mogu da budu važna preventivna aktivnost.

Specijalni alati za procenu i odgovor na sajber rizike mogu da budu od velike koristi. Oni su uglavnom dizajnirani da mere zrelost, otpornost i snagu napora organizacije u oblasti sajber bezbednosti. Organizacije koje ih koriste mogu svoje podatke o rizicima da objedine na jednom mestu i da proaktivno identifikuju, procene i ublaže rizik koji ugrožava njihovu informacionu imovinu, IT i bezbednost informacija pomoću jednog integrisanog alata. Oni su uglavnom izgrađeni na korporativnoj platformi za upravljanje poslovanjem, a mogu se dalje proširiti na druge oblasti upravljanja poslovanjem, kao što su upravljanje usklađenošću. Pomoću njih organizacije mogu da identifikuju, evidentiraju, odrede prioritete, procene i adresiraju IT i sajber rizike na integrisan način, koristeći standardne okvire kao što su ISO 27001 i NIST. Oni mogu da naprave i održavaju centralizovani registar rizika da bi imali potpun i aktuelni pregled svih rizika i da otkriju ranjivosti u procesima, tehnologiji i kanalima dobavljača.

Sajber osiguranje je u osnovi ugovor između osiguravajuće kuće i kompanije.

Sajber osiguranje kao vid odgovora na ransomver je u osnovi ugovor između osiguravajuće kuće i kompanije, koji se sklapa sa ciljem da se kompanija što bolje zaštiti od potencijalnih gubitaka koji mogu da nastanu usled eventualnih računarskih ili mrežnih incidenta. Ovakva vrsta osiguranja pruža određeni nivo sigurnosti tako što daje organizaciji mogućnost da se oporavi od sajber napada ili da odgovori na njega. Osiguranje može da pokrije tužbe, troškove, iznude, različite vrste sudskih troškova i pravne takse, obaveštenje korisnika o kršenju privatnosti podataka, vraćanje ličnih identiteta pogođenih klijenata, oporavak ugroženih podataka, popravku oštećenih računarskih sistema i drugo, u zavisnosti od veličine i obuhvata ugovornog paketa (37, 2). Osim svoje specifične svrhe u sprečavanju napada ransomvera, sajber osiguranje je dragoceno i iz drugih razloga. Pre nego što dođe do napada, proces osiguranja podiže svest o sajber pretnjama, identifikuje kako organizacije treba da reaguju i edukuje osiguranike. Osiguravajuća društva sada zahtevaju mnogo više informacija o tome kako se organizacije koje se osiguravaju bore protiv phishing napada, koji čine veliku većinu sajber incidenata. Nakon napada, sajber osiguranje takođe može

poslužiti kao mehanizam za sazivanje obučenog tima stručnjaka, uključujući forenzičke analitičare i pravne savetnike, da proceni incident i da preporuči adekvatan odgovor. Međutim, sajber osiguranje obično ne pokriva sve. Nepokriveni gubici i događaji pretežno mogu da uključuju incidente izazvane nemarom, gubitak poslovnog ugleda, gubitak poslovnih tajni, i drugo. Sajber osiguranje svakako u pomenutom kontekstu nije apsolutno i konačno rešenje, ali ono može da bude važna komponenta u široj strategiji upravljanja rizikom (29, 1). Da bi se borili protiv ransomvera, IT odeljenja u organizacijama i dalje moraju da nauče zaposlene kako da prepoznaju pretnje, da ograniče privilegije korisnika i uspostave dovoljnu sajber higijenu kako bi izbegli da budu laka meta. Kolektivna odgovornost bez individualne nije adekvatna za osiguravanje zaštite. Pored toga, postoji rizik da, ako se osiguranje koristi za plaćanje počiniocima, nema garancije da će se obezbediti ključ potreban za dešifrovanje zahvaćenih podataka ili datoteka, te stoga organizacije mora da primeni i druge tehnike odgovora na ransomver.

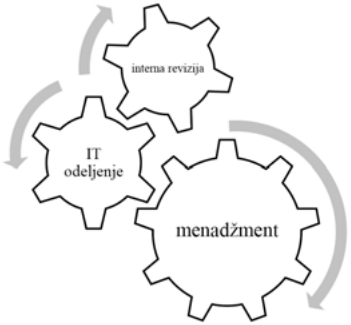
NADLEŽNOSTI ZA REŠAVANJE SAJBER INCIDENATA

Pristup poboljšanju efektivnosti i efikasnosti rizika i kontrolnih funkcija unutar organizacije je dat u IIA-ovom modelu tri linije, koje su pravilno odvojene i njihovo efikasno funkcionisanje je suštinski korak u proceni uloge aktivnosti interne revizije u sajber bezbednosti, uključujući i ransomver.

Prvu liniju predstavlja menadžment, koji poseduje i upravlja podacima, procesima, rizicima i kontrolama (39, 2). Za sajber bezbednost, ova funkcija često pripada administratorima sistema i drugima koji su zaduženi za upravljanje imovinom organizacije.

Druga linija obuhvata funkcije rizika, kontrole i nadzora usklađenosti koje su odgovorne za obezbeđivanje da procesi i kontrole prve linije postoje i da efikasno funkcionišu. Ove funkcije mogu uključivati grupe odgovorne za obezbeđivanje efikasnog upravljanja rizikom i za praćenje rizika i pretnji u prostoru sajber bezbednosti.

Kao treća linija pojavljuje se aktivnost interne revizije, koja obezbeđuje višem menadžmentu i odboru nezavisno i objektivno uveravanje o upravljanju, upravljanju rizikom i kontrolama (9, 2). Ovo obuhvata procenu ukupne efikasnosti aktivnosti koje obavljaju prva i druga linije u upravljanju i ublažavanju rizika i pretnji sajber bezbednosti.



Izvor: Autori, na osnovu (43,7)

Grafikon 2: IIA model tri linije

Sajber pretnje dizajnirane su da sruše sisteme ili zaključaju podatke, tako da su česte i nastaju svuda gde se čuvaju osetljivi podaci, a kad god se napad dogodi, krajnji rezultat može uključivati kršenje zakona i propisa, novčane kazne, oštećenje ugleda i gubitak prihoda. Osetljivi ili poverljivi podaci mogu se klasifikovati i čuvati interno ili eksterno. Interno, većina organizacija se oslanja na tehnologiju, kao što su bezbedne konfiguracije, zaštitni zidovi i kontrole pristupa, što čini njihovu početnu odbranu. Međutim, u namenskom napadu, kada je zaštitni zid preopterećen, napadači mogu dobiti pristup. Da bi se smanjio rizik da takvi napadi dođu do zaštitnog zida, preduzimaju se preventivne mere. To je izazovan proces koji uključuje ograničavanje pristupa i blokiranje neovlašćenog saobraćaja (25, 2). Detektivne kontrole, kao što je praćenje, takođe treba da budu implementirane da prate poznate ranjivosti na osnovu obaveštajnih podataka o softverima i zlonamernim veb lokacijama. Mnoge organizacije uspostavljaju listu prihvatljivog i listu neprihvatljivog saobraćaja. Međutim, sprovođenje aktivnog praćenja i čestog ažuriranja je problematično zbog dinamičke prirode mrežnog saobraćaja. Ako napadač uspe da pristupi sistemu, sledeća linija napada verovatno podrazumeva dobijanje administrativne privilegije i prikrivanje svojih tragova. Menadžment takođe mora biti oprezan prema šemama napada koje obuhvataju društveni inženjering, uključujući phishing e-poruke i sumnjive linkove. Čovek je najslabija karika u IT bezbednosti. Napadači ubeđuju ovlašćene pojedince da podele osetljive podatke, daju im svoje sistemske akreditive, navodeći ih da kliknu na veze koje vode do lažnih veb-lokacija ili obavljaju radnje koje instaliraju zlonamerni softver na računar žrtve (3, 2). Većina bezbednosnih incidenata jesu posledica propusta u primeni nekih osnovnih mera zaštite i nesmotrenosti u radu. Virusa je sve više, sofisticirani su i sve više ciljaju na određe-

nu svrhu ili mrežu. Jednom kada je virus instaliran, može se replicirati širom mreže, poremetiti performanse sistema i dostupnost i izvršiti krađu podataka (35, 2). Zato zdrav razum i svest o rizicima mogu biti najbolji saveznici u odbrani od pretnji iz digitalnog sveta, a saveti IT odeljenja se ne mogu razlikovati mnogo od preporuka koje interni revizori mogu uputiti za zaštitu, poput sledećih:

- Čuvati svoju lozinku, PIN, i druga sredstva koja se koriste za autentifikaciju.
- Koristiti različite lozinke za svoje naloge i postarati se da one budu što duže.
- Redovno ažurirati uređaje i aplikacije.
- Čuvati se od prevara na internetu (ne nasedati na atraktivne ponude, ignorisati sumnjive mejlove i linkove).

Navedeno deluje jednostavno zaposlenima koji su „samo" korisnici informacionih tehnologija, ali to nije toliko kompleksno ni u slučaju administratora ili drugog odgovornog za neki sistem/servis/aplikaciju. Bezbednosni zahtevi su samo nadogradnja funkcionalnih zahteva i za nekoga ko uspešno održava sistem primena mera zaštite ne bi trebalo da predstavljaju preveliki izazov.

Uloge druge linije, koje se često sastoje od IT rizika funkcije upravljanja i usklađenosti sa IT, ključ su za bezbednosni stav organizacije i definiciju programa. Rizici sajber bezbednosti su znatno dinamičniji nego većina tradicionalnih rizika i zahtevaju pravovremeni odgovor. Kršenje bezbednosti može dovesti do promena u sklonosti, a obezbeđivanje nadzora i kreiranje politika, standarda i ograničenja su ključni principi druge linije. Pojedinci u ulogama druge linije treba blisko da sarađuju sa ulogama prve i treće linije da bi kreirali efektivnu svest među rukovodiocima da obezbede da izveštavanje o rizicima i kontrolama sajber bezbednosti bude adekvatno i ažurno. Kako druga linija kreira i izveštaje o svojim procenama rizika, trebalo bi da nastavi da akcentuje sajber bezbednost kao prioritet. Dok je upravljanje prvenstveno odgovornost odbora i višeg menadžmenta, procena upravljanja je jedna od primarnih uloga aktivnosti interne revizije. IIA standard 2110.A2 zahteva da aktivnost interne revizije proceni da li organizacija upravljanjem informacionim tehnologijama podržava strategije i ciljeve (7, 3). Odeljenje interne revizije može da bude konsultovano u vezi sa osiguranjem u aktivnostima sanacije, određivanja prioriteta odgovora i kontrolnih aktivnosti (2, 5). U okviru procene efikasnosti procesa upravljanja rizikom, zahteva u IIA standardu 2120 – Rizik, uloga internog revizora je da nezavisno proceni

rizike i kontrole sajber bezbednosti, da obezbedi usklađenost sa interno važećim aktima, standardima i proceni rizik. Pored toga, aktivnost interne revizije procenjuje efikasnost organizacionih kontrola (38, 1). Važno je napomenuti da IT opšte kontrole predstavlja osnovu, ali ne nudi kompletno rešenje za ublažavanje rizika od sajber bezbednosti. Složenost sajber bezbednosti zahteva dodatne slojeve kontrole, kao što je praćenje rizika, otkrivanje i podsticanje korektivnih akcija (27, 3). Pošto sigurnost zasnovana na tradicionalnim, odvojenim evaluacijama nije dovoljna da se prati tempo rizika sajber bezbednosti, potrebna je inovativna strategija osiguranja, a neophodne su i kontinuirane tehnike revizije da bi se procenili: promene u bezbednosti konfiguracije, pojavljivanja nestandardnih rizika i trendova, vremena odgovora i aktivnosti sanacije. Kada je moguće, interni revizor treba da posmatra i intervjuiše tehničko osoblje koje je obavljalo posao, koristeći rezultate i naučene lekcije koje treba uključiti u buduće procedure interne revizije sajber bezbednosti.

KAKO INTERNA REVIZIJA POMAŽE ORGANIZACIJI U ODGOVORU NA RANSOMVER

Interna revizija ima ključnu ulogu u pomaganju organizacijama u stalnoj borbi protiv sajber pretnji, obezbeđujući nezavisnu procenu postojećih i potrebnih kontrola i pomažući odboru za reviziju i menadžmentu da razumeju i reše različite rizike u digitalnom svetu (6, 1). Pretnje od sajber napada su značajne i stalno se razvijaju, pa su narasla i očekivanja od zainteresovanih strana da interna revizija razume i proceni sposobnosti organizacije u upravljanju IT i ICT rizicima. Iskustvena praksa pokazuje da je prvi efikasan korak za internu reviziju sprovođenje procene sajber rizika i sastavljanje nalaza u sažeti rezime. Nakon njega treba da bude definisan i usvojen plan interne revizije za sajber bezbednost zasnovan na riziku. Interna revizija treba da igra integralnu ulogu u proceni i identifikovanju mogućnosti za jačanje bezbednosti organizacije. Istovremeno, interna revizija ima dužnost da informiše komitet za reviziju i odgovarajuće odbore i komisije izvršnog i nadzornog odbora, koji se bave korporativnom ili IT bezbednošću, o tome da li kontrole koje je rukovodstvo uspostavilo pravilno funkcionišu. Tu postoji sve veća zabrinutost u svim korporativnim organima jer se direktori i same organizacije suočavaju sa regulatornim rizicima i posledično potencijalnim finansijskim obavezama. Pre sprovođenja procene sajber bezbednosti interni revizori treba da imaju u vidu nekoliko faktora. Pre svega, treba da konsultuju i uključe IT

profesionalce sa potrebnim iskustvom i veštinama (13, 4). Interni revizori moraju posedovati dovoljno znanja o ključnim informaciono-tehnološkim rizicima i raspoloživim revizorskim tehnikama zasnovanim na tehnologiji, kako bi izvršili poslove koji su im dodeljeni. Ipak, ne očekuje se od svih internih revizora da imaju isti nivo stručnosti kao interni revizor čija je primarna dužnost revizija informacione tehnologije. Ključno je uključiti revizorske profesionalce sa odgovarajućom dubinom tehničkih veština i znanjem o IT okruženju i povezanim rizicima (18, 4). Interni revizor koji poznaje informacione sisteme može biti nezamenljiv resurs (20, 1), koji procenom celokupnog okvira sajber bezbednosti, a ne samo stavki koje su izabrane, može da pruži značajan doprinos bezbednosti organizacije (19, 2). Ova evaluacija uključuje razumevanje trenutnog stanja u odnosu na karakteristike okvira, u kom pravcu se organizacija kreće i minimalne očekivane prakse sajber bezbednosti u delatnosti ili poslovnom sektoru. Inicijalna procena bi trebalo da pruži informacije o daljim, detaljnijim pregledima (22, 5). U tom smislu, interni revizori mogu da izvrše testiranje da li su uspostavljene kontrole od upada na mrežnom nivou. Takve kontrole uključuju:

1. Sisteme za prevenciju upada, koji se pretežno primenjuju (NetworkIntrusionPrevention) prema javnim IT servisima i drugim povezanim informacionim sistemima.
2. Komponente sistema za prevenciju upada, kojima se upravlja preko centralizovanog upravljačkog sistema.
3. Zaštitu od upada na mrežnom nivou, koja omogućava detektovanje i blokiranje napada kroz propuštanje uobičajenog mrežnog saobraćaja i slanje upozorenja.
4. Zaštitu od upada na mrežnom nivou, koja se sprovodi povezivanjem mrežnih uređaja za prevenciju upada (in-line) u cilju otkrivanja napada.

Početna procena bi trebalo da podstakne interne revizore da izvrše dodatne detaljne preglede sajber bezbednosti zasnovane na riziku (28, 4), uključujući i ocenu adekvatnosti kontrola u sistemima za zaštitu od malicioznog koda, i to na sledeći način:

1. Sistemi za zaštitu od malicioznog koda se podešavaju tako da neprekidno obavljaju zaštitu od malicioznog koda, smeštaju u karantin fajlove za koje se sumnja da sadrže maliciozni kod, uklanjaju maliciozni kod i sve povezane fajlove, onemogućuju isključivanje važnih podešavanja i funkcionalnosti od strane korisnika.
2. Ažuriranje baza definicija malicioznog koda i mehanizama pretraživanja obavlja se periodično.

3. Koriste se dva ili više softverska proizvoda za zaštitu od malicioznog koda različitih proizvođača u pojedinim delovima informacionog sistema.
4. U slučaju pojave malicioznog koda, na informatičkoj opremi organizacije preduzimaju se mere za izolaciju i uklanjanje malicioznog koda i uklanjanje posledica dejstava istog.
5. Redovno se prate informacije o pojavi novih malicioznih kodova iz relevantnih izvora.

Efikasno upravljanje rizikom je proizvod višestrukih slojeva odbrane od rizika (17, 2). Interni revizori i zaposleni koji su bili angažovani na rešavanju incidenata mogu da analiziraju uzrok incidenta, tako što će detaljno da istraže zašto i kako se incident desio, kako bi se sprečilo njegovo ponovno pojavljivanje. Oni mogu da analiziraju obim ugroženosti IT bezbednosti i da provere da li su dokazi o incidentu prikupljeni i sačuvani, kao i da li su postojeće mere adekvatne. Interni revizori predlažu, ako je potrebno, ažuriranje internih akata iz domena IT bezbednosti i zaštite, a ukoliko je moguće predlažu i korektivne mere da bi se sprečilo ponovno pojavljivanje incidenata. Napred nabrojani primeri odbrane za rizike sajber bezbednosti mogu se koristiti kao primarno sredstvo za demonstriranje i strukturiranje uloga, odgovornosti za donošenje odluka, rizika i kontrola, kako bi se postigli efektivno upravljanje rizikom i veća sigurnost. Poslovne operacije u IT odeljenjima podrazumevaju obavljanje svakodnevnih aktivnosti upravljanja rizicima, kao što su identifikacija rizika i procena rizika. Oni pružaju odgovore na rizik definisanjem i implementacijom kontrola za ublažavanje ključnih IT rizika i izveštavanjem o napretku. Uspostavljeno okruženje rizika i kontrole pomaže da se to postigne. Upravljanje rizikom je proces izrade i implementacije politika i procedura, koji pritom osigurava da se postojeće procedure ažuriraju, da se reaguje na nove strateške prioritete i rizike, da se obezbedi praćenje kako bi se dostigla usklađenost sa ažuriranim politikama i da se obezbedi nadzor nad efektivnošću kontrola usklađenosti. Interna revizija treba da sarađuje sa menadžmentom i korporativnim organima u razvoju strategije i politike sajber bezbednosti. Interna revizija treba da identifikuje i reaguje na mogućnosti u cilju poboljšanja sposobnosti organizacije da identifikuje, proceni i snizi rizik sajber bezbednosti na prihvatljiv nivo, i treba da razume da rizik od sajber bezbednosti nije samo spoljašnji, nego da je fokus potrebno staviti i na procenu i ublažavanje potencijalnih pretnji koje bi mogle da proisteknu iz aktivnosti zaposlenog ili poslovnog partnera.

Tabela 1: Deloitte-ova šema sajber ranjivosti

Zaštita	Upravljanje rizikom sajber bezbednosti	Životni ciklus sigurnog razvoja	Program bezbednosti i upravljanje talentima
	• praćenje usklađenosti sa propisima • planiranje korektivnih akcija • ispitivanje regulatornog okruženja • procena rizika usklađenosti • kontrolni okvir	• sigurna izrada i testiranje • smernice za bezbedno kodiranje • pristup rolama u aplikaciji • bezbednosna arhitektura • zahtevi za bezbednošću	• bezbednosni pravac i strategija • bezbednosni budžet i upravljanje finansijama • upravljanje politikama i standardima • upravljanje izuzecima • upravljanje talentima
	Upravljanje trećim stranama	Upravljanje informacijama i imovinom	Upravljanje identitetom i pristupom
	• evaluacija i selekcija • tekući monitoring • prestanak usluge	• klasifikacija IT imovine • upravljanje evidencijom • kontrole fizičkog okruženja • fizičko rukovanje uređajima	• dodeljivanje korisničkih naloga • upravljanje privilegovanim korisnicima • sertifikacija pristupa • upravljanje pristupom
Budnost	Upravljanje pretnjama i ranjivostima	Upravljanje podacima i zaštita	Analitika rizika
	• reakcija na incidente i forenzika • testiranje bezbednosti aplikacije • modeliranje pretnji • praćenje i evidentiranje bezbednosnih događaja • testovi penetracije • upravljanje ranjivostima	• popis IT imovine • upravljanje obaveštenjima • sprečavanje gubitka podataka • strategija bezbednosti podataka • šifrovanje i skrivanje podataka • evidencija upravljanja pristupom na daljinu	• prikupljanje informacija • analiza incidenata, prevara i operativnih gubitaka
Otpornost	Upravljanje krizama i otpornošću	Bezbednosne operacije	Svest o bezbednosti i obuka
	• ažuriranje strategije, planova i procedura • testiranje i simuliranje napada • analiza uticaja na poslovanje • planiranje kontinuiteta poslovanja • planiranje oporavka od katastrofe	• upravljanje promenama • upravljanje konfiguracijom • mrežna odbrana • upravljanje bezbednosnim operacijama • sigurnosna arhitektura	• obuka o bezbednosti • podizanje nivoa svesti o bezbednosti • razmatranje odgovornosti trećih strana

Izvor: Autori, na osnovu (42, 4)

Kroz revizijski angažman revizori mogu da procene koliko je visok rizik po bezbednost informacija i da li su ispravke za tehničke ranjivosti dostupne, pa da pripreme izveštaj o ranjivostima sa preporukama za primenu ispravki radi otklanjanja ranjivosti. Ukoliko je procenjeni rizik po bezbednost informacija visok, a ispravke za tehničke ranjivosti nisu dostupne ili primena odobrenih ispravki ugrožava funkcionisanje sistema, neke od preporuka interne revizije mogu obuhvatiti privremene ili stalne korektivne mere za smanjivanje rizika za te ranjivosti, kao što su: deaktivacija sistemskih servisa koji su ranjivi ukoliko nisu neophodni

za funkcionisanje IT servisa, preispitivanje i kontrola prava pristupa ranjivoj opremi i servisima, pojačano nadgledanje ranjive opreme sa ciljem otkrivanja neregularnog funkcionisanja opreme, itd.

Interni revizori mogu da iskoriste odnose sa komitetom za reviziju kako bi: povećali svest i znanje o sajber pretnjama; osigurli da odbor ostane u velikoj meri zainteresovan za pitanja sajber bezbednosti i u toku sa promenama prirode rizika sajber bezbednosti; omogućili da rizik od sajber bezbednosti bude formalno integrisan u višegodišnje planove revizije. Uz sve to, interni revizori treba aktivno da prate kako nove tehnologije i trendovi utiču na organizaciju i njen profil rizika od sajber bezbednosti i da procene program sajber bezbednosti organizacija u odnosu na jedan od prihvatljivih okvira (12,1).

Interna revizija pruža holistički pristup identifikovanju ranjivih tački organizacije (16, 1). Bilo da je predmet angažovanja testiranje politika ili pregled da li su ugovori sa trećim stranama u skladu sa bezbednosnim protokolima, interna revizija nudi dragocen uvid u napore zaštite. Efikasno upravljanje IT-om je takođe ključno, a interna revizija može da pruži usluge uveravanja i za tu oblast. Dobra analitika podataka često pruža prvi nagoveštaj organizacijama da nešto nije u redu (21, 3). Interna revizija sve više u svoj rad uključuje analizu podataka i druge tehnologije (14, 1).

Pravilno planiranje je važno za prevazilaženje bilo kojeg broja scenarija rizika koji bi mogli uticati na tekuće procese organizacije, uključujući sajber napad, prirodnu katastrofu, ili sukcesiju. Interna revizija može pomoći u razvoju plana, obezbediti provere uveravanja o njegovoj efektivnosti i blagovremenosti i na kraju ponuditi analizu i kritike nakon što se planovi izvrše. U tom smislu, potreban je visok stepen saradnje sa zaposlenima odeljenja za IT bezbednost i zaštitu, koji pripremaju izveštaj sa ključnim indikatorima performansi procesa i, po potrebi, izveštaje o trendu ispravljanja ranjivosti po grupama za podršku, korišćenjem podataka iz specijalizovanih alata za otkrivanje ranjivosti, i sve to dostavljaju internim revizorima. Revizori i zaposleni u IT odeljenju organizacije mogu analizirati zajednički izveštaj sa ključnim indikatorima performansi procesa, pratiti trend ispravljanja ranjivosti i formulisati preporuke i u kom roku da se slabosti otklone. Interna revizija dakle može pružiti najveću vrednost doprinoseći uvidu stečenom iz njenog velikog obima posla (15, 3). Kroz preporuke interne revizije jača se Sajber spremnost, ali ako se iste ne uvaže, odnosno ako organizacija ne evoluira i ne poboljša svoje strategije i protokole, sve može biti uzaludno i organizacija ne može biti bolje pripremljena za sledeći napad.

ZAKLJUČAK

Organizacije, bez obzira na veličinu, omiljena su meta sajber napada ransomverom. Mnoge organizacije zavise od svojih računara, koje koriste za realizaciju poslovnih aktivnosti, za upravljanje ključnim datotekama, ili za komunikaciju. Svaki zastoj ima uticaj na krajnji rezultat poslovanja. Napadači manipulišu vlasnicima i zaposlenima s namerom da im ovi plate otkupninu kako bi povratili pristup svojim računarima. U mnogim slučajevima uspeli su ili da iznude velike sume novca ili da značajno poremete rad. Pretnje ransomverom se stalno razvijaju i postaju sve teže. Efikasno otkrivanje ransomvera uključuje kombinaciju tehnologije i znanja, a najbolji način za odbranu su preventivne aktivnosti, dok funkcija interne revizije može značajno da pomogne u tom segmentu. Menadžment treba da se uveri da su zaposleni edukovani o ransomveru, što može biti doprinos funkcije interne revizije kao odeljenja koje može da obezbedi nezavisno profesionalno uveravanje. Zaposleni bi trebalo da znaju kako da uoče znakove ransomvera, kao što su imejlovi, linkovi, reklame ili sumnjive datoteke. U organizaciji treba da bude uspostavljena mreža za nadzor i odbranu od sajber napada. Uz pomoć budnog nadzora moguće je evidentirati dolazni i odlazni saobraćaj, skenirati datoteke u potrazi za dokazima napada, kao što su neuspele modifikacije, uspostaviti osnovu za prihvatljivu aktivnost korisnika i istražiti sve aktivnosti koje se čini neuobičajenima. Antivirusni softveri se mogu koristiti za stavljanje na listu prihvatljivih lokacija i obaveštavanje o otkrivenim pretnjama, a konfigurisanje podešavanja e-sandučeta tako da automatski proverava postojanje zlonamernih poruka i blokiranje sadržaja sa ekstenzijama koje mogu predstavljati pretnju, može da bude veoma korisno. Uprkos svim zaštitnim merama i protivmerama, uvedenim da bi se sprečili napadi ransomvera, jedna od najvećih pretnji je društveni inženjering. Jedna slaba karika u sistemu može omogućiti napadaču da zaobiđe sajber zaštite. Od ključne je važnosti implementirati program za podizanje svesti o društvenom inženjeringu, koji pokriva načine za prepoznavanje sumnjivih linkova i priloga e-pošte, kao i često testiranje osoblja. Otvaranje veza i priloga u e-pošti i pristup zaraženim veb-lokacijama su dve uobičajene metode koje napadači koriste da bi dobili pristup digitalnoj infrastrukturi organizacije. Aktivnosti društvenog inženjeringa koje se mogu koristiti da motivišu pojedinca da nesvesno instalira zlonamerni softver uključuju obaveštenja e-poštom o isteku antivirusne zaštite, iskačuće prozore i e-poštu u vezi sa potrebom za instaliranjem ažuriranja,

kao i zahteve e-pošte za potvrdu isporuke paketa. Organizacije treba da implementiraju programe za filtriranje, koji mogu da minimiziraju ovaj vektor pretnje. Kada se incident dogodi, fokus treba da bude na zaustavljanju širenja i oporavku, uključujući rad sa specijalizovanim timom za forenziku na identifikaciji tačke preko koje je virus upao u sistem. Virus treba bezbedno ukloniti, sisteme treba ponovo zakrpiti i primeniti ažuriranja. Ovo može potrajati i iziskivati novac, ali je neophodno.

Odeljenje interne revizija treba da pokaže zainteresovanost da sprovede reviziju informacione bezbednosti. Interni revizori bi trebalo da prave revizijski trag u realnom vremenu kada dođu do faze sprovođenja revizorskog angažmana i treba da steknu razumevanje da li je organizacija preduzela odgovarajuće i blagovremene napore da komunicira sa zaposlenima, dobavljačima i drugim zainteresovanim stranama. Revizori treba da izvrše reviziju odgovora organizacije, ali ne da se ograniče samo na ransomver, već da prošire revizijske angažmane i na druge oblasti. Tu pre svega mislimo na oporavak od katastrofe, planove za kontinuitet poslovanja i onoga što se dogodilo, identifikaciju koraka preduzetih odmah nakon inficiranja kako bi se sagledali nedostaci u kontroli i nedostaci u drugim segmentima. Interni revizori mogu da se uvere da organizacija primenjuje dobru sajber higijenu, da identifikuju učestalost i tip rezervnih kopija i postojanje višefaktorske autentifikacije. Rezervne kopije na starim ili alternativnim sistemima poput Linux-a mogu biti značajna zaštita, naročito u slučajevima kada su druge rezervne kopije zaražene. Interni revizori mogu da odgovore na pitanja koje su se mere zaštite podataka i sistema pokazale uspešnim, da li je organizacija osigurana po osnovu rizika od sajber napada, da li je osiguranje na nivou organizacije ili samo određenih delova ili profitnih centara, da li postoji adekvatna procena rizika na nivou organizacije, kakav je način razmišljanja o potrebi reagovanja na incidente, a i materijalnost obavezno treba da bude uzeta u obzir. Ovi primeri za reagovanje mogu internoj reviziji da ponude pomoćne alate za korektivno delovanje, a pre svega i preventivno, u cilju odgovora na rizike u organizaciji (1, 3). Prevencija je ključna, a interna revizija može u revizijskom univerzumu mapirati ključne IT rizike kao najveće pretnje. Ako menadžment očekuje da će ransomver biti velika pretnja, bilo zato što je visoka frekvenca u delatnosti ili zato što je organizacija već imala iskustvo sa njim, onda interni revizori mogu da usmere predmet svojih angažmana na te kritične oblasti. Dobra je ideja sprovesti ankete ili diskusije zasnovane na intervjuima, kako bi se identifikovale glavne pretnje,

mapirale kontrole svake pretnje i procenila adekvatnost postojećih kontrola. Iako interni revizori generalno nisu odgovorni za izbor softvera za sajber bezbednost i uspostavljanje obuka zaposlenih za prepoznavanje rizika od ransomvera, oni i dalje mogu da obezbede sigurnost u vezi sa IT praksama i kontrolama, tako što će sprovoditi revizije informacione bezbednosti.

Kada IT timovi sprovode phishing testove kako bi videli da li su zaposleni prevareni putem e-pošte koje mogu da izazovu probleme sa ransomverom, interni revizori su tada u mogućnosti da pregledaju te rezultate i osiguraju da organizacija ima zadovoljavajući nivo otpornosti na ransomver (8, 1). Ako rezultati pokažu nedostatke u reagovanju zaposlenih na ransomver, ili druge rizike sajber bezbednosti, onda bi interni revizori verovatno želeli to da saopšte drugim zainteresovanim stranama, kao što su odbor za reviziju i menadžment. Na primer, jedna od preporuka revizora može biti da se zaposlenima šalju mejlovi, ili da se na internim portalima organizacija prevode i distribuiraju bilteni „OUCH!" SANS instituta, ugledne američke organizacije koja se bavi edukacijom i istraživanjem u oblasti IT bezbednosti. Rukovodioci interne revizije bi mogli da pregledaju politike rada na daljinu kako bi osigurali da IT timovi na odgovarajući način upravljaju njima, imajući na umu rizik od ransomvera. Dok se interni revizori često oslanjaju na uputstva kolega iz IT odeljenja, oni i dalje mogu da revidiraju oblasti kao što su evidencije pristupa, kako bi se uverili da se samo odobreni uređaji, sa odgovarajućim tehnologijama za otkrivanje pretnji i zaštitu podataka, povezuju na njihove mreže. Neretko, revizori prikupljaju i informacije iz više odeljenja kako bi bili sigurni da su svi na istom zadatku, a to je odbrana od sajber napada (na primer, trebalo bi da provere sa finansijskim timovima kako oni obračunavaju potencijalne troškove napada ransomvera, a zatim da se uvere da drugi ključni akteri, poput odbora i višeg rukovodstva, to razumeju i slažu se sa ovim pristupom (36, 3)). U suprotnom, može se pojavit problem kao što je nedostatak budžeta za oporavak od napada ransomvera. Bez obzira na svoju veličinu ili prihod, organizacije bi trebalo da pretpostave da će biti meta ransomvera i treba da ispitaju svoje mere za prevenciju, reagovanje i oporavak. Funkcija interne revizije ima priliku da ostvari značajan uticaj kada je u pitanju upravljanje rizikom od ransomvera. Planiranje i fokusiranje na unutrašnje usklađivanje mogu dati značajan doprinos smanjenju napada ransomvera.

LITERATURA

1. Abdullatif, M., & Kawuq, S. (2015). The role of internal auditing in risk management: evidence from banks in Jordan. J. Econ. Admin. Sci. 31 (1), 30-50.
2. Alina, M., Cerasela, E., & Gabriela, G. (2017). Internal Audit Role in Cybersecurity. Ovidius University Annals, Series Economic Sciences, 17(2), 510513.
3. Anders, B. (2019). Cybersecurity Tools for CPAs. CPA Journal, 89(6), 72-73.
4. Calderon, G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. International Journal of Auditing, 25(1), 24-39. https://doi.org/10.1111/ijau.12209.
5. Carataș M., A., Spătariu E., C., & Gheorghiu G. (2017). Internal Audit Role in Cybersecurity. Ovidius University Annals: Economic Sciences Series, XVII (2), 510-513.
6. Chaudhary, R., & Hamilton, J. (2016). Internal Audit's Critical Role in Cybersecurity. New Perspectives on Healthcare Risk Management, Control & Governance, 35(2), 20-29.
7. Christ, H., Eulerich, M., Krane, R., & Wood, A. (2021). New Frontiers for Internal Audit Research. Accounting Perspectives, 20(4), 449-475. https://doi.org/10.1111/1911-3838.12272.
8. Dmitrović, V., Stojanović, D., & Jakovljević, N. (2022). Challenges for information and cyber security of banks in a pandemic environment and user attitudes. In book: Stability, institutional growth and perspectives of the development of the Croatian financial system in the conditions of the Covid-19 pandemic. Chapter: Sveučilište u Rijeci, Ekonomski fakultet.
9. Eaton, V., Grenier, H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. Current Issues in Auditing, 13(2), C1-C9. https://doi.org/10.2308/ciia-52419.
10. Garrie, D., & Halprin, P. A. (2021). Placing Ransomware in Context and Avoiding Liability for Paying Ransomware Claims. Journal of Internet Law, 24(5), 1-19.
11. Islam, S., Farah, N., & Stafford, F. (2018). Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal, 33(4), 377-409. https://doi.org/10.1108/MAJ-07-2017-1595.
12. Jakovljević, N, Jakovljević J. (2021). The impact of the Covid-19 global pandemic on the responsibility of auditors. 92-113. https://mfin.gov.rs/aktivnosti/asopis-finansije-broj-1-62021.
13. Jakovljević, N. (2021). Analysis of auditor's characteristics. Monografija konferencije SPIN21. 366-374. http://spin.fon.bg.ac.rs/wp-content/uploads/2021/11/Zbornik-SPIN2021-final.pdf.
14. Jakovljević, N. (2021). Analysis of the impact of the Covid-19 epidemic through the sojourn tax and the attitudes of the respondents. Trendovi u poslovanju. 2/2021(18) 20-29. http://www.trendovi.vspep.edu.rs/index.php/tp/article/view/246.
15. Jakovljević, N. (2021). Aplicaton of the digital games in the audit profession. Monografija konferencije SPIN21. 374-382. http://spin.fon.bg.ac.rs/wp-content/uploads/2021/11/Zbornik-SPIN2021-final.pdf.
16. Jakovljević, N. (2021). Application of artificial intelligence in audit. Monografija konferencije STES21. 277-290. http://stes.unibl.org/wp-content/uploads/2021/11/Dru%C5%A1tvene_zbornik_2021.pdf.
17. Jakovljević, N. (2021). Irregularities in conducting the list of assets and liabilities. Trendovi u poslovanju, 1/2021(17), 94-104. http://www.trendovi.vspep.edu.rs/index.php/tp/article/view/230.

18. Jakovljević, N. (2021). Political neutrality in the audit profession: attitudes of respondents in the Republic of Serbia. BizInfo (Blace) Journal of Economics, Management and Informatics. 12(2), 23-38. https://doi.org/10.5937/bizinfo2102023J.
19. Jakovljević, N. (2021). Use of drones in the audit profession. Monografija konferencije SPIN21. 382-390. http://spin.fon.bg.ac.rs/wp-content/uploads/2021/11/Zbornik-SPIN2021-final.pdf.
20. Jakovljević, N., & Jakovljević, J. (2021). The impact of the Covid-19 global pandemic on the responsibility of auditors. Finansije. 92-113. https://mfin.gov.rs/aktivnosti/asopis-finansije-broj-1-62021.
21. Jeremić, N., Jakovljević, N., Jeremić, M. (2021) Agile internal audit. Revizor. 95-96, 57-76.
22. Jeremić, N., Jakovljević, N., Jeremić, M. (2022) The role of internal auditing in business continuity. Revizor. 97-98, 53-71.
23. Jethva, B., Traoré, I., Ghaleb, A., Ganame, K., & Ahmed, S. (2020). Multilayer ransomware detection using grouped registry key operations, file entropy and file signature monitoring. Journal of Computer Security, 28(3), 337-373. https://doi.org/10.3233/JCS-191346.
24. Kozlova, O., Kononovič, G., Kononovič, V., Romanюkov, G., & Timošenko, M. (2017). Dinamični Vlastivosti Procesiv Zabezpečennя Kiberbezpeki Na Prikladi Auditu Kiberbezpeki. Informatics & Mathematical Methods in Simulation, 7(3), 205-212.
25. Lankton, N., Price, J. B., & Karim, M. (2021). Cybersecurity Breaches and the Role of Information Technology Governance in Audit Committee Charters. Journal of Information Systems, 35(1), 101-119. https://doi.org/10.2308/isys-18-071
26. Lanz, J. (2014). Cybersecurity Governance: The Role of the Audit Committee and the CPA. CPA Journal, 84(11), 6-10.
27. Lanz, J. (2016). Communicating Cybersecurity Risks to the Audit Committee. CPA Journal, 86(5), 6-10.
28. Li, H., No, G., & Boritz, E. (2020). Are External Auditors Concerned about Cyber Incidents? Evidence from Audit Fees. Auditing: A Journal of Practice & Theory, 39(1), 151-171. https://doi.org/10.2308/ajpt-52593.
29. Madani, H., Ouerdi, N., Boumesaoud, A., & Azizi, A. (2022). Classification of ransomware using different types of neural networks. Scientific Reports, 12(1), 1-11. https://doi.org/10.1038/s41598-022-08504-6.
30. Marcus C. (2019). Avoid Getting Hit by Ransomware: Five Tips for Employees: When Lives Are on the Line, Your Employees Could Be Your Best Line of Defense. Journal of Health Care Compliance, 21(1), 43-46.
31. Mierzwa, S. J., Drylie, J. J., Cochi Ho, Bogdan, D., & Watson, K. (2022). Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal. Journal of Leadership, Accountability & Ethics, 19(2), 110-120. https://doi.org/10.33423/jlae.v19i2.5112.
32. Min, D., Ko, Y., Walker, R., Lee, J., & Kim, Y. (2022). A Content-Based Ransomware Detection and Backup Solid-State Drive for Ransomware Defense. IEEE Transactions on Computer-Aided Design of Integrated Circuits & Systems, 41(7), 2038-2051. https://doi.org/10.1109/TCAD.2021.3099084.
33. Oberly, J. (2019). Best Practices for Effectively Defending Against Ransomware Cyber Attacks. Intellectual Property & Technology Law Journal, 31(7), 17-20.
34. Sabillon, R, Cavaller, V., Serra-Ruiz, J. & Cano, J. (2017). "A comprehensive cybersecurity audit model to improve cybersecurity assurance", International Conference on Information Systems and Computer Science, pp. 253-259. https://doi.org/doi.org/10.1109/INCISCOS.2017.20.

35. Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits / Un modelo práctico para realizar auditorías exhaustivas de Ciberseguridad. Enfoque UTE, 9(1), 127-137. https://doi.org/10.29019/enfoqueute.v9n1.214.
36. Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Acc. Organ. Soc. 71, 15-29. https://doi.org/10.1016/j.aos.2018.04.005.
37. Sumner, P., & Keenan, R. (2022). Ransomware Attacks on Healthcare Providers -What You Need to Know. Journal of Health Care Compliance, 24(2), 11-69.
38. Tran N., & Andrea T. (2021). Cyber-Security Risks Assessment by External Auditors. Interdisciplinary Description of Complex Systems, 19(3), 375-390. https://doi.org/10.7906/indecs.19.3.3.
39. Turetken, O., Jethefer, S., & Ozkan, B. (2020). Internal audit effectiveness: operationalization and influencing factors. Managerial Audit. J. 35 (2), 238-271. https://doi.org/10.1108/MAJ-08-2018-1980.
40. Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. Business Horizons, 64(6), 787-797. https://doi.org/10.1016/j.bushor.2021.07.014.
41. Wertheim, S. (2019). Auditing for Cybersecurity Risk. CPA Journal, 89(6), 68-71.
42. Deloitte USA (2017) Cybersecurity and the role of internal audit: an urgent call to action.
43. The Institute of Internal Auditors (2020) GTAG, Assessing cybersecurity risk.

THE ROLE OF INTERNAL AUDIT IN REDUCING THE RISK OF RANSOMWARE

SUMMARY

Although the list of risks in the field of cyber security is long, ransomware is still at the very top, as a high-risk threat to the security of a business entity. Ransomware can also cause problems such as data leaks and damage to business reputation. The aim of the paper is to examine the role of internal audit in reducing the risk of ransomware. The main conclusion is that effective ransomware detection involves a combination of technology and knowledge, in which the best way to defend is preventative action, and an internal audit function can significantly assist in this.

Keywords: ransomware; cyber risks; cyber threats, cyber security, cyber insurance, Threa lines model.

Rad primljen: 5.8.2022 • Prihvaćen: 30.9.2022.