Uloge i odgovornosti Voditelja informacijske sigurnosti

Korinčić, Dominik

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:355310

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Dominik Korinčić

ULOGE I ODGOVORNOSTI VODITELJA INFORMACIJSKE SIGURNOSTI

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Dominik Korinčić

ROLES AND RESPONSIBILITIES OF THE CHIEF INFORMATION SECURITY OFFICER

ULOGE I ODGOVORNOSTI VODITELJA INFORMACIJSKE SIGURNOSTI

SPECIALIST THESIS

SPECIJALISTIČKI RAD

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija Informacijska sigurnost.

Mentor: prof. dr. sc. Boris Vrdoljak

Specijalistički rad ima: 122 stranica. Specijalistički rad br.:_____.

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Stjepan Groš – predsjednik
2. prof. dr. sc. Boris Vrdoljak – mentor
3. prof. dr. sc. Ivan Magdalenić, Sveučilište u Zagrebu Fakultet organizacije i informatike - član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Stjepan Groš – predsjednik
2. prof. dr. sc. Boris Vrdoljak – mentor
3. prof. dr. sc. Ivan Magdalenić, Sveučilište u Zagrebu Fakultet organizacije i informatike - član

Datum obrane: 2. veljače 2024.

Sažetak

U današnje vrijeme poslovanje treba razumjeti informacijsku sigurnost ne samo na razini svijesnosti nego i na razini planiranja, budžetiranja i implementiranja. Integriranje informacijske sigurnosti u poslovne procese postaje preduvijet održivog poslovanja. Opasnosti i računalni napadi koji su usmjereni kako na organizacije u korporativnom sivijetu tako i na one iz javnog sektora iziskuju stručnjake koji će se usredotočeno baviti i nositi odgovonrnost za informacijsku sigurnost. Širina i složenost ovog područja iziskuje stručnost i iskustvo te konstantnu volju za stjecanjem novih znanja. Političke odluke te posljedična legislativa idu u prilogu formalnih zahtjeva za provođenjem određenih aktivnosti po pitanju informacijske sigurnosti. To samo po sebi daje dodatni značaj i obvezu. Sistematizacija pozicije voditelja informacijske sigurnosti predstavlja odgovor na navedene zahtjeve, a stručnost i složenost aktivnosti kojima se navedeni stručnjak treba baviti predstavljaju izazove koji iziskuje konstantno i cijeloživotno učenje.

Ključne riječi:

Voditelj informacijske sigurnosti, klasificirani podaci, informacijska sigurnost, upravljanje rizikom, ISO/IEC 27001, kontrole, sigurnosni incident, kriptografija, zakon, ranjivost, upravljanje ranjivostima, politika informacijske sigurnosti, pravilnik, procedure

Summary

Nowadays, business needs to understand information security not only at the level of awareness but also at the level of planning, budgeting and implementation. Integrating information security into business processes becomes a prerequisite for sustainable business. Dangers and computer attacks that are aimed both at organizations in the corporate world and at those from the public sector require specialists who will focus on and bear responsibility for information security. The breadth and complexity of this field requires expertise and experience and a constant will to acquire new knowledge. Political decisions and the resulting legislation are in support of formal requirements for the implementation of certain activities in the field of information security. This in itself gives additional significance and obligation. The systematization of the position of information security manager is a response to the aforementioned requirements, and the expertise and complexity of the activities that the aforementioned expert should deal with represent challenges that require constant and lifelong learning.

Keywords:

Information security manager, classified data, information security, risk management, ISO/IEC 27001, controls, security incident, cryptography, law, vulnerability, vulnerability management, information security policy, rulebook, procedures

Sadržaj

1. Uvod

Područje ovog rada obuhvaća opis aktivnosti i odgovornosti koje Voditelj informacijske sigurnosti treba zadovoljiti. Trendovi u tehnologiji preslikavaju se na trendove u informacijskoj tehnologiji i predstavljaju smjer u kojem se kreću izazovi za informacijsku sigurnost. Računarstvo u oblaku (engl. *cloud computing*) i posljedična rješenja u kojima dobar dio poslovnih subjekata svoju informatičku infrastrukturu migrira, rezultiraju time da se danas susrećemo s informatičkim infrastrukturama koje su – ili potpuno u oblaku ili su svojevrsno hibridno rješenje, ono u kojem poduzeća određeni dio infrastrukture imaju lokalno, a drugi dio imaju u oblaku. Globalizacija i svojevrsna konvergencija tzv. zapadnog svijeta ishodile su i određene regulacije. Tim se regulacijama nastoje zaštiti ekonomski sustavi i društvo, kao i privatnost građana (GDPR, PCI DSS, PSD i dr.). To je rezultiralo određenim direktivama, koje su u konačnici završile u zakonima zemalja članica EU-a. Samim time, navedeno je postala obveza prema kojoj tehnologija mora biti usklađena.

Sve navedeno definira trendove kojih bi svaki Voditelj informacijske sigurnosti trebao biti svjestan, te bi trebao posjedovati znanje, stručnost i motivaciju za sustavno usvajanje novog relevantnog znanja. Spoj stručne literature i opisanih trendova iz poslovne prakse prikazuju zanimljivost i važnost uloga i odgovornosti Voditelja informacijske sigurnosti. Funkcija Voditelja informacijske sigurnosti u određenim sektorima postaje nužnost, a u velikom dijelu ostalih primjećuje se potreba za njome. Sigurnosni incidenti su troškovni i reputacijski čimbenici koje poslovni subjekti žele izbjeći, a njihove posljedice umanjiti. Navedeno otvara pitanje kakve, za koliku cijenu i koje kompetencije bi Voditelj informacijske sigurnosti trebao imati. U ovom radu opisat ćemo sve izazove i odgovornosti koje današnjica postavlja pred Voditelje informacijske sigurnosti.

Cilj je ovog rada opisati značaj uloge Voditelja informacijske sigurnosti unutar organizacija koje posluju u sektorima veće ili manje regulacije na području Republike Hrvatske. Sektori koji su regulirani podrazumijevaju privredne sektore koji imaju određenog regulatora, a sektori manje regulacije podrazumijevaju sektore koji nemaju zakonski određenog regulatora. Primjer regulatora za bankarski sektor je HNB, za osiguravajuća društva to je HANFA, za telekomunikacijski sektor to je HAKOM, dok je za energetiku mjerodavna HERA. Putem opisa

svakodnevnih aktivnosti koje su u korelaciji s trendovima prijetnji u informacijskoj sigurnosti, cilj ovog rada je prikazati potrebu za radnom pozicijom Voditelja informacijske sigurnosti i opisati vještine, znanje i iskustvo koje bi trebao imati adekvatan kadar. Uz navedeno, cilj je također opisati rješenje u obliku eksternalizacije funkcije Voditelja informacijske sigurnosti. To u većem dijelu rješava probleme kao što su: nerazumijevanje, nedostatak svjesnosti, nedostatak kadrova i isključiv troškovni pogled na informacijsku sigurnost.

Rad je podijeljen u sedam poglavlja. U uvodnom dijelu prikazan je teorijski koncept uloge Voditelja informacijske sigurnosti (engl. *chief information security officer*). Nakon teorijskog dijela, opisane su najčešće aktivnosti i odgovornosti Voditelja informacijske sigurnosti, poput podrške pri certifikaciji te upravljanja rizicima informacijskog sustava. U ovom su dijelu rada opisane svakodnevne aktivnosti, odgovornosti i zaduženja te su navedene očekivane i nužne kompetencije koje bi navedeni stručnjak trebao posjedovati. Nakon toga, dan je pregled relevantne legislative za informacijsku sigurnost u Republici Hrvatskoj. U petom su poglavlju prikazane aktivnosti i odgovornosti na primjerima položaja Voditelja informacijske sigurnosti unutar organizacija te je dan prikaz opisa eksternalizacije funkcije i njezine ponude po SaaS (engl. *Software as a Service*) ili FaaS (engl. *Function as a Service*) principu, a uz to, prikazani su neki od tehničkih alata kojima se koristi voditelj informacijske sigurnosti. U šestom su poglavlju opisani trendovi u industriji informacijske sigurnosti iz perspektive Voditelja informacijske sigurnosti. U sedmom poglavlju iznesen je zaključak ovog rada.

2. Vrijednost informacija i funkcije voditelja informacijske sigurnosti

U kontekstu organizacije, informacija je ono što omogućuje posao. Poslovni proces stvara i obrađuje podatak koji se pretvara u informaciju i znanje, a koji se upotrebljavaju za stvaranje vrijednosti i potiču organizaciju i njezine procese [1].

Upravljanje informacijama (eng. *information management*) organizacijama je promijenilo način upravljanja svojim poslovanjem, način natjecanja, te ima ključnu funkciju u ostvarivanju strateške i komparativne prednosti. Organizacije donose eksplicitne i implicitne odluke o potrebi za informacijama i njihovoj uporabi. Odluke se temelje na procjeni troškova i uporabi informacija za poslovnu strukturu i strategiju.

Organizacije su korisnici informacija, menadžeri i stvaratelji, a njihov ugled uvelike ovisi o organizacijskoj inteligenciji. Ona se očituje u sposobnosti osiguranja, analize i pravovremenog oporavka informacija.

ISO 27000 standard definira informacijsku sigurnost kao proces koji mora sačuvati povjerljivost, integritet i dostupnost (tzv. CIA), dok je glavna misija osigurati neprekidnost poslovanja i smanjiti štetu ograničavanjem negativnih učinaka sigurnosnih incidenata. [2]. Upravljanje sigurnošću informacija ograničeno samo na tehnologije i procese informacijske tehnologije nije samo po sebi dovoljno da osigura sveprisutan utjecaj u velikim organizacijama.

Upravljanje sigurnošću informacija (engl. *information security governance*) objašnjeno je kao proces definiranja, uspostavljanja i održavanja strukture i upravljačkih procesa koji podržavaju usklađivanje sigurnosti informacija s poslovnim ciljevima, istovremeno se pridržavajući primjerenih zakona i propisa. To se ostvaruje usvajanjem politika, kontrola i uspostavom uloga i odgovornosti, koje podržavaju bolje upravljanje rizikom u organizaciji [2]. Proces organiziranja informacijske sigurnosti u organizaciji trebao bi obuhvaćati čimbenike kao što su: misija organizacije, sastav, ovlasti, odgovornosti, uloge, komunikacijske linije, koordinacija i položaj u organizacijskoj strukturi.

Pri definiranju smjernica za upravljanje sigurnošću informacija, Basie von Solms je 2001. godine predstavio 13 dimenzija koje, bez obzira na njihovu organizaciju, trebaju zajedno djelovati da bi stvorile sigurno okruženje [3]:

1. dimenzija korporativne strategije i upravljanja
2. dimenzija organizacije
3. dimenzija politike
4. dimenzija najbolje prakse
5. etička dimenzija
6. dimenzija certificiranja
7. pravna dimenzija
8. dimenzija osiguranja
9. ljudska dimenzija
10. dimenzija svijenosti
11. tehnička dimenzija
12. dimenzija metrike
13. dimenzija revizije.

Stoga, sigurnost informacija treba shvatiti i rješavati kao višedimenzionalno pitanje i ona treba biti obrađena kao odgovornost korporativnog upravljanja i upravljanja općenito. Upravljanje rizicima, izvještavanje i odgovornost voditelja trebaju biti razvijeni tako da osiguravaju odgovarajuću razinu zrelosti i sigurnosti informacija u organizaciji.

Postojanje CISO funkcija unutar organizacija upozorava na to da postoji potreba vodstva koje je odgovorno i posvećeno pitanjima informacijske sigurnosti. U organizacijama nailazimo na funkcije naziva Direktor informacijske sigurnosti, Menadžer informacijske sigurnosti i Voditelj informacijske sigurnosti, no naziv funkcije nije toliko bitan koliko su bitne odgovornosti te funkcije unutar organizacije.

Dok su, naprimjer, funkcije kao Glavni izvrši direktor – CEO (engl. *Chief executive officer*) ili Direktor financija – CFO (engl. *Chief financial officer*) jasno definirane, definicija CISO funkcije još uvijek je u svojevrsnom razvoju. Povijesno gledano, CISO funkcije su većinom bile usredotočene na definiranje standarda tehničke sigurnosti i razvoj politike informacijske sigurnosti. Danas organizacije postaju svjesne da je *cyber* rizik izravno povezan s njihovim strategijama inovacije i rasta. Danas se CISO sve više prepoznaje kao ključni element u definiranju strategije upravljanja rizicima informacija, uz svoje glavne odgovornosti: razvitak, upravljanje i operacionalizacija strategije informacijske sigurnosti; konstantni nadzor

i evaluacija informacijsko-sigurnosne prakse; provođenje revizije i procjene rizika; vođenje, nadzor i trening svojeg odjela; usklađivanje organizacije regulacijom informacijske sigurnosti; razvoj i implementacija plana neprekidnosti poslovanja; zaštita intelektualnog vlasništva organizacije; obuka i podizanje svijesti zaposlenika o rizicima informacijske sigurnosti; upravljanje proračunom za informacijsku sigurnost i izvještavanje Upravnog odbora. Još jedna od glavnih odgovornosti CISO-a jest – biti aktivan član vrhovnog menadžerskog tima.

CISO ima izvršnu ulogu u organizaciji i odgovoran je za uspostavljanje i održavanje vizije, strategije i programa organizacijske informacijske sigurnosti, a koji su usklađeni sa strategijom organizacije.

Ilustrativnim primjerom opisat ćemo položaj Voditelja informacijske sigurnosti i potrebe za njime (u duljenjem tekstu CISO). Odgovornosti je i cilj direktorice financija poduzeća SuperSoft d. o. o., u sklopu godišnje revizije dokazati da je kompanija usklađena sa Sarbanes-Oxley zakonom[1]. Stalna nastojanja internih revizora da pojasne problematiku pričuvne kopije (engl. *backup*) koja predstavlja problem neusklađenosti sa SOX-om, nisu rezultirala rješenjem. Činjenica je da je direktorica financija računovodstvene struke, a ne tehničke. Nastojanje da se prenese problematika tehničkih stručnjaka osobi čija je odgovornost financijsko poslovanje kompanije, rezultirala je nerazumijevanjima; a pokušaj da se putem tehničkih detalja pojasni problematika rezultirao je još većim nerazumijevanjem. Navedeni problem, koji je sve više eskalirao, određeni djelatnik tehničke struke riješio je pomoću alegorijskog metaforičkog primjera. Problem tehničke pričuve rastumačio je opisom vlaka koji prevozi putnike iz stanice A u stanicu B. Objasnio je: „Evo, upravo to je pričuvna kopija, prijenos podataka od naših poslužitelja do pričuvnih traka. Znamo da je vlak stigao na stanicu B, dakle, možemo potvrditi da je pričuvna kopija nastala. No, isto tako ne znamo koliko je putnika stiglo na stanicu B. Dakle, ne možemo tvrditi da smo izradili pričuvnu kopiju svih

[1] SOX je skraćenica za Zakon o zaštiti ulagača u vrijednosne papire (engl. *Sarbanes-Oxley Act*), također poznat kao *SOX Act*. To je američki zakon koji je donesen 2002. godine, kao reakcija na niz financijskih skandala koji su se dogodili krajem devedesetih i početkom 21. stoljeća, poput skandala kompanija *Enron* i *WorldCom*. Cilj SOX-a je poboljšati transparentnost i odgovornost korporacija i zaštititi interese ulagača. Zakon je uveo niz regulatornih zahtjeva i zaštita, kojima se osigurava integritet financijskog izvješćivanja tvrtki. Određeni dio zakona stavlja naglasak na sigurnost podataka, praćenje pokušaja curenja podataka i čuvanje *logova* u svrhu periodičnih nadzora.

informacija, a da bismo bili usklađeni sa SOX-om, moramo biti sigurni u to da su sve informacije sigurnosno pohranjene “.

Direktorica financija je u tom trenutku prvi put zauzela svoj stav i postala svjesna ozbiljnosti situacije. Od tog trenutka ostvaren je pozitivan pomak ka rješenju. Tehničkoj ekspertnoj skupini postavila je pitanje o tome kako planiraju riješiti navedeni problem, na što je ekspertna skupina ponudila nekoliko rješenja te je sastanak završio s konkretnim pomacima.

Metaforički pojednostavljen opis situacije ishodio je rješenje, dok tradicionalni pristup to nije uspio, prenoseći tehnički sigurnosni problem u terminologiju koju je rukovodeća poslovna osoba mogla razumjeti i upamtiti. Ovo ilustrira jednu od ključnih sposobnosti koju bi trebao posjedovati CISO. Potrebno je proširiti doseg informacijske sigurnosti izvan odjela sigurnosti i informatike da bi se ostvarila jasna komunikacija s utjecajnim pojedincima na svim razinama i svih edukacijskih zaleđa.

U nastavku ćemo objasniti neke sposobnosti i osobine koje bi CISO trebao posjedovati da bi obnašao ovu izazovnu funkciju Voditelja informacijske sigurnosti. Prije negoli to opišemo, vratit ćemo se korak unazad i ukratko opisati dinamičnost fokusa informacijske sigurnosti.

Da bi ostalo na tržištu i ostvarilo održiv rezultat, svako poduzeće mora u određenoj mjeri implementirati tehnologiju. Iz navedenog razloga možemo zaključiti da svako poduzeće vremenom postaje tehnološka kompanija. Također, potencijalni utjecaj informacijskog rizika širi se tako da upravljanje sigurnošću i privatnošću postaje kategorija korporativne socijalne odgovornosti. Shodno tome, opseg CISO funkcije bi se trebao proširiti do granica na kojima može pokriti sve rizike vezane za informacijsku sigurnost i njima ovladati. Kod mnogih organizacija to se već događa. CISO preuzima odgovornost za privatnost, usklađenost sa zakonima te sigurnost proizvoda i usluga, što simbolizira promjenu i povećanje važnosti samog položaja unutar organizacije i promjenu u odnosu na tradicionalno shvaćanje IT sigurnosti. Ovakvo je stanje prilika za CISO da zauzme važniju i moćniju funkciju unutar organizacije. Ključne vještine profesionalaca za informacijsku sigurnost su procjena i umanjenje rizika, koji postaju nužnost za umanjivanje novih rizika povezanih sa sigurnošću proizvoda, privatnosti i usklađenosti s regulatornim zahtjevima, uz već tradicionalne vještine vezane za sigurnost IT-a. Ovako opisana proširena funkcija otvara pitanja kao što je potreba promjena naziva same funkcije koja bolje opisuje konvergenciju aktivnosti k procijeni rizika. Tako se u raspravama u vezi s nazivima mogu vidjeti naprimjer, eng. *Chief Trust Officer* ili *Chief Information Risk*

Officer. No nazivi i titule unutar organizacija su jedno, a realne odgovornosti drugo, te su česte diskrepancije. Prihvaćanje funkcije šireg opsega odgovornosti zahtijeva širi pogled i pripadajući skup vještina. Potrebno je komunicirati razumljivo „poslovnim ljudima“ i izgraditi odnose koji omogućuju utjecaj na svim razinama unutar organizacije. Uz tehničke kompetencije potrebne su i menadžerske vještine vođenja i upravljanja ljudima na operativnim i izvršnim funkcijama te sposobnost motiviranja osoba koje su dio proširenog tima upravljanja rizicima. Sposobnost upravljanja punim opsegom rizika povezanih s informacijama je nužnost – ne samo za CISO funkciju, već i za cijelu organizaciju. Ako CISO ne preuzme širi opseg svojih aktivnosti, organizacijama ne preostaje ništa drugo nego da potrebnu stručnost pronađu negdje drugdje. Zbog iznesenih činjenica, zaposlenik koji ima funkciju CISO-a, a nije agilan u prilagodbi potrebama koje navedena funkcija zahtijeva, riskira da postane nebitan i nepotreban. Alternativno, područjima rizika će se upravljati izolirano i fragmentirano, tako da će se organizacija dovesti u situaciju iz koje nikad neće upravljati rizicima na sveobuhvatnoj razini, a kontrole rizika neće biti sveobuhvatne i neisključive. Ako se ovo dogodi, organizacije će sigurno generirati neupravljane rizike za sebe, svoje kupce i društvo.

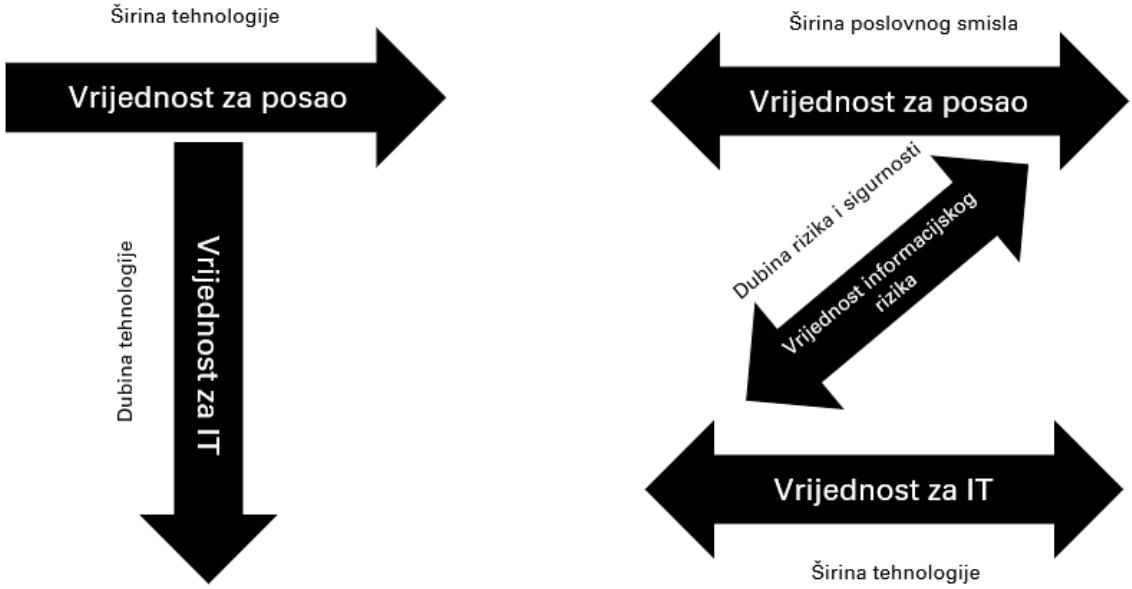
Donedavno je jedan od najzahtjevnijih zadataka CISO funkcije bio dobiti sredstva i odobreni budžet za sigurnosne inicijative unutar organizacije. U današnje vrijeme to nije slučaj, jer učestali i ustrajni sigurnosni incidenti te curenje i krađa podataka velikih razmjera idu u prilog budžetiranju informacijske sigurnosti. No, više osiguranih sredstava ne vodi uvijek nužno većoj razini sigurnosti ili boljem ishodu za organizaciju. Ponekad strah od sigurnosnog incidenta potiče organizacije da ulože velike resurse u kontrole koje proizvode velike restrikcije, ograničavajući sposobnost korisnika i djelatnika da obavljaju svoje poslove. Naprimjer, neke organizacije su uspostavile kontrole koje korisnike sprječavaju da preuzimaju aplikacije ili datoteke i pristupaju određenim mrežnim stranicama. Ove kontrole prijetnja su korisničkoj sposobnosti inoviranja i usporavaju ukupnu poslovnu agilnost. S druge pak strane, to odlučnog korisnika potiče da pronađe načine za zaobilaženje kontrole.

CISO funkcija zahtijeva određenu poslovnu svjesnost procesa i organizacije koje je član, da bi se razumio utjecaj sigurnosnih kontrola na ostale poslovne funkcije. Današnji pristup sigurnosnoj arhitekturi treba započeti s razumijevanjem uspostavljenih kontrola za svladavanje rizika, a uz to je nužna svjesnost o utjecaju te kontrole na druge procese unutar organizacije. Poslovna svjesnost je također neophodna da bi se zaposlenicima koji nisu tehničke struke priopćio rizik tehničke prirode i da bi se razumjelo da je određeni rizik neophodno prihvatiti.

Riskiranje, odnosno prihvaćanje kalkuliranog rizika osnova je svakog poslovnog modela. Bez prihvaćanja rizika, ne mogu se stvoriti dodatne vrijednosti.

Ako ne posjedujemo vještine koje su nužne za CISO-a, moramo ih naučiti i usvojiti. U nastavku ćemo opisati dva modela vještina te karakteristike koje diktiraju trendovi vremena u kojem djelujemo. Profesionalci u IT-u moraju imati poslovnu svjesnost i posjedovati dubinsko razumijevanje IT-a.

Koncept T-oblika (eng. *T-shaped*) pojedinaca primjenjuje se da bi se naglasila ideja o tome da IT profesionalci moraju biti sposobni ponuditi vrijednost horizontalno – među različitim poslovnim odjelima – i vertikalno, na svim razinama unutar odjela IT-a. Navedeni koncepti prikazani su na slici (Sl. 2.1) [4].



Sl. 2.1. IT stručnjak T-oblika i Z-oblika CISO-a [4]

CISO 21. stoljeća mora razumjeti poslovne prioritete i procese dovoljno dobro da bi razumio potiču li sigurnosne kontrole sâm poslovni model organizacije ili ga ograničavaju. Da bi stekao ili stekla dovoljnu razinu razumijevanja, nužno je da ima iskustvo u području na kojem je centralno usmjerenje poslovanja organizacije. To, naravno, varira od organizacije do organizacije, a prvenstveno je predodređeno industrijskim sektorom kojem pripada i strateškim odlukama poslovodstva; naprimjer, CISO je prethodno radio u odjelu proizvodnje ili odjelu poslovnih spajanja i preuzimanja (eng. *mergers and acquisitions*).

CISO također treba imati određenu razinu tehničkih znanja, premda se u literaturi može pročitati dosta rasprava o tome koju razinu tehničkih znanja on treba posjedovati [4]. Na primjeru određenog broja organizacija različitih veličina i kompleksnosti, moguće je primijetiti sljedeće: u manjim organizacijama manje kompleksnosti CISO je više uključen u dubinu tehničkih zahtjeva i upravljanja ljudima, dok je CISO u većim i kompleksnijim organizacijama manje sklon ulaziti u tehničke detalje svakodnevne sigurnosne problematike [2]. Neovisno o navedenome, CISO mora znati dovoljno o tehnologiji da bi mogao odvojiti bitno od nebitnog i rukovodećim ljudima izvan odjela sigurnosti prenijeti sigurnosnu problematiku jasno i nedvosmisleno. To podrazumijeva širok spektar tehničkih znanja – od uređaja do podatkovnih centara. Potrebno je posjedovati razinu tehničkog znanja koja je dovoljna da se može procijeniti sigurnosni rizik, kao i pogodnost konstantno napredujuće i promjenjive tehnologije.

Upravljanje rizicima i vještine u području sigurnosti poveznice su koje upotpunjavaju tzv. Z-oblik (eng. *Z-shape*), odnosno spoj tehnologije i poslovnih procesa. Razumijevanje upravljanja rizicima primjenom procedura, tehničkih i fizičkih kontrola; a u svrhu zadovoljavanja pravnog aspekta, privatnosti i sigurnosnih zahtjeva; glavnina je odgovornosti funkcije CISO-a.

2.1. Osnovne vještine

Postati „pojedinac Z-oblika“ (eng. *Z-shaped individual*) svojevrsni je temelj svake CISO funkcije. Potrebno je uspostaviti kredibilitet diljem organizacije. Kredibilitet je nužan da bi se izgradile kvalitetne veze s voditeljima i specijalistima diljem organizacije, a on se stvara na temelju stručnosti, koja pak dolazi iz razumijevanja posla i tehnologije – uz uvjet da je znanje o sigurnosti na visokoj razini. Postajanjem pojedincem Z-oblika, CISO se postavlja na položaj u kojem utječe na upravljanje rizicima proizvoda ili usluga koje organizacija nudi. Mogućnost da CISO utječe na organizaciju proizlazi iz jasne misije. Jasno iznošenje određenog slučaja moguće je jedino ako CISO ima snažan osjećaj svrhe. Ako je navedeno zadovoljeno, odluke CISO funkcije mogu imati direktan utjecaj i na odluke CFO-a (eng. *chief financial officer*) ili CEO-a (eng. *chief executive officer*), a odjel informacijske sigurnosti može dobiti na važnosti [4].

Ovakva tvrdnja stavlja organizaciju u stratešku poziciju: „zaštiti da bi omogućio“ (eng. *protect to enable*). U današnjoj globalnoj ekonomiji, većina organizacija posluje na kompetitivnom tržištu. Iz perspektive informacijske sigurnosti, zadatak je omogućiti slobodni

tijek informacija i brzu implementaciju novih mogućnosti da bi osigurali uspjeh i dugoročnu kompetitivnu održivost. Uloga CISO-a treba se uklopiti u razinu i karakteristiku organizacije koje je član, posebno u vezi sa stupnjem averzije prema riziku. Misija CISO funkcije uvijek mora biti usklađena s poslovnim prioritetima organizacije. Važno je da misija postane dio onoga što CISO jest i zbog čega postoji u organizaciji. Pruža svrhovitost koja rezultira autentičnošću i konzistentnošću aktivnosti te pomaže u stvaranju kredibiliteta diljem organizacije.

Sigurnost kao takva, uključujući informacijsku sigurnost, može biti poprilično ometajuće zanimanje, s neprekidnim nizom svakodnevnih hitnih situacija i ometanja. Zato je potrebna jasna misija da bismo održali jasan smjer. Opisat ćemo navedenu tvrdnju s pomoću metafore, s ciljem što boljeg prikaza. Poput iskusnih mornara, možemo napredovati prema našem cilju usprkos svakodnevnim ometanjima i skretanjima, čineći stalne prilagodbe i ispravke da bismo ostali na pravom kursu dok vjetrovi mijenjaju smjer [3].

Također je potrebno održavati osjećaj znatiželje. Da bi se povezali s drugima, potrebna je iskrena zainteresiranost za ono što oni rade. Znatiželja potiče mogućnost učenja, što posljedično podiže razinu i širinu kompetencija, a što rezultira povećanjem kredibiliteta.

Dodatan razlog zašto je za funkciju CISO-a potrebno neprestano učenje je taj da ostane ispred zlonamjernih neprijatelja koji narušavaju sigurnost. Takozvani agenti prijetnji uvijek uče jer moraju. Kako se javljaju nove prijetnje, tako se postavljaju nove kontrole. No, kad su jednom te kontrole postavljene, naginju tome da postanu statične. S druge strane, agenti opasnosti svakodnevno inoviraju i pokušavaju osmisliti kako zaobići postavljane kontrole. Upravo zato pojedinci koji obnašaju CISO funkciju moraju dinamički razmišljati i djelovati te moraju svakodnevno učiti da bi bili u stanju zaštititi organizaciju od svakodnevno napredujućih opasnosti.

2.2. Postati pripovjedač

Bez komunikacije s osobama, na njih se ne može se utjecati. Kako se opseg rizika informacija širi, tako je potrebno komunicirati s raznolikim skupinama ljudi unutar organizacije. Takva komunikacija nije uvijek jednostavna. Ako počnemo prenositi tehničke pojedinosti onima koji nisu stručnjaci za tehnologiju, nećemo privući njihov interes. Naprotiv, postoji rizik da postignemo suprotan učinak, kao što je opisano u primjeru na početku ovog poglavlja. Da bi uspješno komunicirao, CISO mora poprimiti sposobnosti kameleona (sposobnost mimikrije),

odnosno mora se uklopiti u različita okruženja. Potrebna je razina znanja o različitim poslovnim područjima organizacije da bi mogli komunicirati jezikom koji djelatnici tih odjela razumiju. Primjera radi, financijski direktori (CFO) često žele čuti sažet pregled, izražen u smislu financijskog utjecaja i povrata ulaganja, što često nije jednostavno kada se raspravlja o sigurnosnim ulaganjima usmjerenima prema teško kvantificiranim prijetnjama. Voditelji proizvoda žele čuti sigurnosna pitanja izražena u terminima koji se odnose na prodaju, marketing i operativnu učinkovitost. Pripovijedanje je nedvojbeno moćan alat za komuniciranje s različitim osobama unutar organizacije. Kada se sigurnosna pitanja predstave kao priče i slike koje ljudi mogu razumjeti, oni se bolje povezuju s tim pitanjima, čak i ako nemaju tehničkih znanja. Moćan alat u komunikaciji su metafore i analogije. Jednostavno se pamte i prevode složene teme u jednostavne pojmove koje svako može razumjeti. Shodno navedenom, citirat ću još jednu metaforu: „Dirigent orkestra ne proizvodi zvuk. Njegova snaga dolazi od buđenja mogućnosti kod drugih. (Zander i Zander, 2000)“. Na isti način, snaga CISO-a dolazi od buđenja svijesti o riziku među ljudima u cijeloj organizaciji, koristeći se pričama zasnovanim na metaforama kako bi stvorio tu svijest. Naprimjer, zaposlenicima je često teško shvatiti opasnosti skrivenih prijetnji jer su neprimjetne. Korisnici često nisu svjesni da u njihovu sustavu postoji problem. Oni i dalje povezuju zlonamjerni softver s očiglednim, iritantnim simptomima poput poruka na zaslonu i rušenja sustava. Stoga, kada im kažemo da smo otkrili opasan softver na njihovom računalu, teško je vjerovati da im je to bitno. Zbog toga se moramo usredotočiti na prevenciju, primjenom kontrola. Ako to ne postignemo kao struka, nastavit ćemo beskonačni ciklus rizika s kojim se danas suočavamo.

Da bismo jasno skrenuli pozornost na opasnost i potrebu za učinkovitim preventivnim kontrolama, korisno je upotrijebiti analogiju. Dobar prikaz stanja daje analogija opasnosti od mrava i opasnosti od termita. Zloćudni softver je nekoć bio poput običnih mrava koji su se vidljivo okupljali oko ostataka hrane u kuhinji. Znate da ste zaraženi kad vidite kako mravi dolaze do vaših ostataka hrane kroz zidove i namještaj. Jednom kad postanete svjesni navedenog, učinit ćete nešto protiv toga. No, u današnje vrijeme sigurnosna opasnost je poput termita koji mogu neprimjetno živjeti u zidovima vaših kuća. Činjenica da ih ne vidimo rezultira time da mislimo da ih jednostavno nema. No, oni čine puno više štete negoli su to obični mravi ikad činili. Termiti mogu narušiti strukturalni integritet cijele kuće, posebno onih montažnih, narušavanjem statike objekta [4]. Iz svakodnevnog poslovnog iskustva mogu potvrditi da uporabom analogije poruka najbrže dolazi do svog cilja, do onog tko bi trebao u vezi s time nešto napraviti, te ljudi jednostavnije shvaćaju da nevidljiva prijetnja može ugroziti cijelu

informatičku infrastrukturu, baš kao što termiti mogu narušiti statiku montažne kuće. Razumijevanje, a samim time i svjesnost, povećava vjerojatnost da djelatnici u nekoj organizaciji prihvate sljedeći korak – uspostavu sigurnosnih kontrola, bile one preventivne ili reaktivne.

Kako bismo raspravljali o upravljanju informacijskim rizikom diljem neke organizacije, korisno je upotrebljavati neki zajednički jezik, koji bi svatko, uključujući netehničke djelatnike, mogao razumjeti. Koristan je okvir za informacijsku sigurnost, NIST[2]. Razvoj navedenog datira od 2013. godine, na temelju naredbe predsjednika Sjedinjenih Američkih Država za poboljšanje sigurnosti kritične infrastrukture. To je rezultiralo jednogodišnjim aktivnostima koje je potaknuo i vodio privatni sektor da bi se razvio dobrovoljan vodič za informacijsku sigurnost.

Okvir stvara zajedničko nazivlje za upravljanje rizikom, olakšavajući komunikaciju sigurnosnim timovima i drugima te potiče suradnju. Osim toga, svaka organizacija može izmjeriti svoju razinu zrelosti upravljanja rizikom u odnosu na okvir. Što se više osoba njime koristi, okvir pomaže u povećavanju općeg razumijevanja informacijskog rizika i načina njegovim upravljanjem.

2.3. Čimbenik straha u informacijskoj sigurnosti

Industrija sigurnosti općenito ima sklonost da se koristi strahom kako bi prodala vlastite proizvode i usluge. Nažalost, ova sklonost odražava činjenicu da mnogi pojedinci u industriji sigurnosti profitiraju od nesigurnosti, što je donekle i paradoks. Prihodi kompanija koje se bave informacijskom sigurnošću rastu kad dođe do učestalijih curenja povjerljivih podataka i kada ima više sigurnosnih incidenata. U internoj situaciji, takvim se okolnostima sigurnosni timovi koriste da bi dobili veće budžete ili resurse. Sigurnosti ne bi bilo bez nesigurnosti, a koju čine opasnosti, ranjivosti i rizici. Fokus na strah koji nije objektivan nipošto nije dobar. U samim

2 NIST (*National Institute of Standards and Technology*) Glavna svrha NIST-a je promicanje industrijske konkurentnosti i inovacija putem razvoja i primjene mjerenja, normi i tehnologije. NIST pruža tehničku podršku za industriju, ažurira i održava standarde i upute i provodi istraživanja koja se odnose na širok spektar znanstvenih i tehničkih područja; uključujući tehnologiju, elektroniku, računarstvo, kemijske i fizikalne znanosti, sigurnost, kibernetiku i druge discipline. NIST također ima važnu ulogu u sigurnosti informacija i kibernetičkoj sigurnosti, pružajući smjernice i izvore za zaštitu informacija i sustava od kibernetičkih prijetnji.

počecima može ponuditi zadovoljstvo te je na neki način i zarazan, no u konačnici, nije objektivan i opravdan te ne ide u prilog ni CISO funkciji, a niti samoj organizaciji.

U kratkom razdoblju, strah može prestrašiti ljude i potaknuti na aktivnosti koje idu u prilog financiranju sigurnosnih projekata. Postavljanje sigurnosti na temelju straha kratkog je vijeka i u konačnici ima suprotan učinak i rezultira time da CISO izgubi na kredibilitetu. Prema određenim izvorima, poslovni model temeljen na strahu doprinosi brzini rotacije CISO funkcija s jedne na drugu organizaciju [4]. Pojedinci koji svoj položaj previše grade na strahu, s vremenom budu zamijenjeni, jer organizacije to u srednjem roku primijete i u konačnici, ne toleriraju.

Strah nije dobar i iz drugih razloga. Većina ljudi ne želi slušati neprestan dotok negativnih informacija. Ako Vas jednom počnu percipirati kao izvor negativnosti, izgubit ćete svoju publiku. Ako Vas promatraju kao odjel s uvijek negativnim odgovorima, s vremenom će Vas početi ignorirati. Ljudi će pronaći načine za zaobići sigurnosne zahtjeve da bi ostvarili poslovnu potrebu i cilj.

Čak i u organizacijama koje se bave sigurnošću, strah može postati poput gravitacijske sile koja privlači svu pozornost i energiju na negativnu stranu sigurnosnih izazova, umjesto da se usredotoči na poslovne izazove. Zato se potrebno usredotočiti na rješenja koja nude tri ključne pogodnosti:

1. dokaziv i održiv nagib na krivulji rizika (umanjenje rizika)
2. sposobnost da se smanji trošak kontrola
3. nisku razinu smetnje kontrola, brzinu i agilnost poslovanja i kupčevo zadovoljstvo.

2.3.1. Naglašavanje pozitivnih aspekata

Pozitivan pristup moguće je zauzeti koncentriranjem na misiju funkcije CISO-a, a to je: „zaštiti da bi omogućio“. Ova misija mijenja naglasak s negativnog na pozitivno. Kako možemo pomoći poduzeću da ostvari vlastite ciljeve rješavanjem informacijskih rizika i sigurnosnih problema?

Misija je usklađena s poslom. Umjesto da je izolirana, temelji se na zajedničkim vrijednostima. Uspostavlja optimistički pristup, a dugoročno, optimizam je puno bolji motivator nego što je to pesimizam. Opasnosti možda i jesu zastrašujuće, ali cilj je vidjeti priliku u

prijetnjama. Ne postoji problem koji ne može biti riješen bez novog okvira [6]. Dakle, ako ne vidimo rješenje koristimo se krivim okvirom. „Zaštiti da bi omogućio“ novi je okvir.

Zamislimo da smo pozvani na određeni sastanak na kojem se raspravlja bi li organizacija trebala započeti s uporabom poslovne aplikacije koja se nalazi u oblaku, a koju održava novi dobavljač. Jasno je da ovaj proizvod predstavlja rizik jer potječe od nepoznatog dobavljača, aplikaciji se pristupa putem interneta te će se osjetljivi podaci spremiti izvan organizacije.

Uzak pogled na sigurnost može nas dovesti u usredotočenost na isključivo određeni rizik. No, upravo takav pogled može nas dovesti u situaciju tzv. „kvake 22“ – da bi umanjila rizike, organizacija ograničava uporabu nove tehnologije. Naprimjer, ta tehnologa može biti rabljena samo za podatke malog rizika ili se njome može koristiti uzak segment djelatnika. Problem u ovom pristupu je taj što ograničenje također ograničava pogodnosti uporabe nove tehnologije, do te razine da granične koristi od tehnologije ne opravdavaju troškove i aktivnosti potrebne za prilagodbu. Dolazi se do zastoja. Da bi tehnologija postala izvediva mogućnost, moramo pokazati poslovnu korist, ali ne možemo je pokazati jer ne dopuštamo punu upotrebu tehnologije.

„Zaštiti kako bi omogućio“ nudi novi okvir koji nas oslobađa opisane dileme. Omogućuje nam koncentriranje na prilike i identificira prednosti koje nadilaze rizike. Naprimjer, izbor novog dobavljača podiže razinu kompetitivnosti kod preostalih, što vodi k uštedama za organizaciju u budućnosti. Ovakva prednost je u skladu s poslovnim ciljevima organizacije te je ono što svi razumiju. Naprimjer, manje intuitivna, ali jednako važna prednost je činjenica da se te uštede mogu iskoristiti za ublažavanje rizika koji su posljedica šire primjene nove tehnologije. U takvoj situaciji prednost novog rješenja nadilazi potencijalno negativne posljedice. S mogućnosti primjene nove tehnologije u širem rasponu, ostvarujemo veću korist od troškova kontrola koje smo uspostavili. Ovakav primjer jasno pokazuje da CISO mora izgraditi smisao za posao. kojim stvara i otkriva prilike za poboljšanje poslovanja, a što mu s druge strane omogućuje pregovaračku moć u budžetiranju sigurnosnih inicijativa.

Opisat ćemo još jedan primjer koji se dogodio u Intel Corporationu. Prije izvjesnog vremena otkriven je zahtjevan i složen računalni crv (eng. *worm*), potpuno aktivan u računalnoj infrastrukturi organizacije. Njegovo otkrivanje zahtijevalo je hitnu intervenciju sigurnosnog tima. Analizom i forenzikom njegovih aktivnosti, uhvaćen je njegov trag i izvor koji je vodio do vanjske računalne infrastrukture izvan perimetra organizacije koja je bila u vlasništvu jednog od zaposlenika Intela.

Odgovor odjela zaduženog za sigurnost organizacije bio je poprilično stereotipan. Ugasili su zaraženu računalnu opremu, poslužitelje i radne stanice. Nakon toga su postrožili sigurnosnu politiku i povezane procedure da bi osigurali stanje u kojem samo radne stanice u vlasništvu organizacije imaju pravo i mogućnost pristupa korporativnoj mreži. Navedeno je provedeno tako da su napravili opsežan popis sve računalne opreme, zatim su skenirali sve unutar mrežnog perimetra te odstranili i ugasili svu opremu koju nisu mogli uskladiti s registrom računalne imovine.

Ovakav odgovor na sigurnosni incident uspješan je u kontekstu smanjenja rizika od zaraze zlućudnim softverom, ali istodobno je doveo do drugih rizika, koji nisu bili predvidljivi. Zabrana pristupa osobnih računala u vlasništvu zaposlenika korporativnoj mreži rezultirao je potrebom da organizacija izda propisano osobno računalo za svakog ugovorenog zaposlenika, uključujući i vanjske suradnike. Njih uvjetno možemo smatrati trećom stranom. Ukratko, puno je ljudi u kratkom vremenu dobilo propisano osobno računalo, kojim je moglo pristupiti korporativnoj mreži. To je pak ishodilo naglo povećanje kapitalnih troškova (eng. CAPEX). Širi utjecaj te odluke eliminirao je sve potencijalne pozitivne utjecaje koji bi mogli proizaći iz toga da zaposlenici rabe svoja osobna računala za svrhu posla.

Nastavno na ovaj sigurnosni incident i rješenje, ovaj slučaj se nakon određenog vremena ponovno vratio na razmatranje, revidiranje i potencijalnu izmjenu odluke. Prvenstveno potaknut zahtjevom zaposlenika, a i sve većom primjenom novih korisničkih uređaja, sigurnosni odjel bio je primoran ispraviti svoju prvobitnu odluku. Ovoga je puta primijenjeno načelo „Zaštiti da bi omogućio“. Pošlo se od pretpostavke toga kako omogućiti uporabu računalnih resursa u osobnom vlasništvu za poslovne svrhe, a da se pri tome umanji sigurnosni rizik. Otkriveno je da je poslovni utjecaj velik i pozitivan. Omogućavanje da zaposlenici međusobno komuniciraju iz bilo kojeg mjesta i u bilo koje vrijeme, može imati pozitivan utjecaj na produktivnost. Također je zapaženo da ta mogućnost čini zaposlenike sretnijima. Zaposlenici se jednostavno vole koristiti svojim privatnim računalnim resursima; kao što su pametni telefoni, osobna računala i tableti, te su cijenili činjenicu da im je to bilo omogućeno. Također je potrebno naglasiti da određena tehnologija nije bila dostupna kad je otkriven sigurnosni incident. Pouka iz ovog primjera je: ako se prvo usredotočimo na prilike, možda se može ponuditi određena razina pristupa uz umanjenje rizika, a uz to, smanjiti utjecaj odluke na kapitalne troškove organizacije.

Naravno da je uloga sigurnosne organizacije i dalje usredotočena na upravljanje rizicima, a to uključuje vječnu raspravu o negativnim posljedicama koje ljudske aktivnosti mogu izazvati. Ako ovu raspravu kontroliramo i strukturiramo, moguće je istodobno informirati bez širenja straha. To je moguće postići tako da se jasno opišu ishod i rješenje, bez dramatiziranja ili apostrofiranja ozbiljnosti i hitnosti određene situacije, a da ozbiljnost sigurnosti bude jasna. Svaka CISO funkcija stvara kontekst unutar kojeg organizacija može donijeti odluku koja je najbolja za poslovanje. Iako CISO funkcija u opisu svojeg posla mora naglašavati neugodan ishod, ne širi se strah dok god se informacija temelji na točnosti i stvarnosti.

U nastavku je naveden još jedan primjer iz Intela. Kupci su se sve više koristili internetom, stoga je marketinški odjel, potaknut tim trendom, htio povećati prisutnost kompanije na internetu. Poslovno logičan pothvat rezultirao je nalogom za izradu više novih mrežnih stranica kompanije. Primjereno proceduri, odjel informacijske sigurnosti započeo je s procjenom rizika i potrebnih kontrola za navedene aktivnosti izrade i objave mrežnih stranica. Velik dio rukovodećih ljudi odjela marketinga nije bio naklonjen navedenim sigurnosnim aktivnostima. Na sve to gledali su isključivo kao na poslovnu priliku, za koju moraju djelovati brzo i efikasno da bi je iskoristili. Smatrali su da imaju svu slobodu odluke o tome kako će komunicirati prema van i da su zahtjevi sigurnosnog odjela samo još jedna administrativna prepreka koja ih usporava. Ono što je uslijedilo bilo je mnogo uvjerljivije od početnih napora odjela sigurnosti da spriječi potencijalne probleme. Nekoliko mrežnih stranica lansirano je bez temeljite kontrole kvalitete. Zlonamjerni hakeri (u nastavku teksta – hakeri) pronašli su slabosti na tim stranicama, ali nisu ih srušili, niti su ukrali informacije. Umjesto toga, ubacili su veze na stranice eksplicitnog sadržaja. Nakon što je ovaj nesretni slučaj otkriven, postao je sinonim i neka vrsta referentnog primjera, koji je poslužio da se iz toga nešto nauči i da se poboljšaju sigurnosne procedure. Tadašnji CISO iskoristio je ovaj primjer jer ga je smatrao dovoljno ilustrativnim i učinkovitim s jedne strane, te dovoljno eksplicitnim da bi bio lako pamtljiv.

2.4. Potrebno iskustvo i pripadajući radni staž CISO funkcije

Prikazat ćemo ilustrativan primjer sposobnosti i iskustva potrebnih za CISO funkciju. Istraživači su zamolili ispitanike da igraju igru u kojoj su mogli maksimizirati svoje dobitke okretanjem karata iz jednog od dvaju špilova. Ispitanici nisu znali da su špilovi već pripremljeni. Mogli su pobijediti odabirom iz jednog špila, dok bi odabir iz drugog špila doveo do gubitka. Nakon otprilike 80 karata, ispitanici su mogli objasniti razliku između špilova. No, već nakon 50 karata imali su osjećaj da nešto nije u redu. Počeli su pokazivati znakove stresa i mijenjati svoje ponašanje čak i ranije, nakon otprilike 10 karata i to dugo prije nego što su na spoznajnoj razini shvatili da postoji razlika.

Osoba na CISO funkciji treba biti na toj razini da kombinacijom svojeg poslovnog – tehničkog iskustva, vještina i cjeloživotnog učenja uspije primijetiti sigurnosnu opasnost prije svih ostalih, uključujući stručnjake unutar njegovog tima. Vrlo često je to kombinacija spoznajnih sposobnosti i iskustva, koja rezultira nekom vrstom „šestog čula“ za sigurnost. Upravo ovakva kombinacija sposobnosti i iskustva je ono što je potrebno u području sigurnosti, u kojem je raspoloživa informacija gotovo uvijek nedorečena ili nepotpuna. Kad opasnost napadne, nema se vremena za provedbu opsežnog istraživanja ili čekanja da se prikupe dokazi. Zato je potrebno djelovati odlučno, na temelju raspoloživih informacija.

Ako se budući rizici identificiraju dovoljno rano, možemo ih u potpunosti spriječiti ili barem umanjiti njihov utjecaj. Preventivni rani postupci mogu smanjiti sveukupne aktivnosti potrebne za kontrolu rizika. Rano djelovanje može izbjeći potrebu za hitnim odgovorom i potencijalno velikim naporima za sanaciju i oporavak od sigurnosnog incidenta.

Sve navedeno o sposobnosti CISO funkcije ima smisla samo onda ako organizacija koje je CISO član, ima sposobnost djelovati brzo. Da bi to bilo moguće, potrebna su dva ključna preduvjeta. Prvo, trebamo hrabrost da se oslonimo na vjeru i poduzmemo korake na temelju onoga u što vjerujemo. Drugi zahtjev je da organizacija brzo reagira kada je obavijestimo o sigurnosnom problemu. Potrebna brza reakcija kompanije moguća je samo ako je CISO funkcija ostvarila i održala kvalitetne odnose s ljudima diljem organizacije. Brze, bezbolne odluke moguće su jer ljudi znaju iz iskustva da su informacije CISO funkcije pouzdane i da je fokus na omogućavanju, a ne širenju straha.

2.5. CISO kao voditelj

Prije svega, CISO današnjice mora postati učinkovit voditelj, koji potiče i motivira svoj tim stručnjaka da bi učinkovito zaštitio organizaciju. Iskustveno, tijekom dugog niza godina bavljenja pitanjima sigurnosti, identificirane su tri ključne teme – svi članovi tima odgovornog za sigurnost [7]:

1. moraju vjerovati u misiju tima
2. moraju osjećati pripadnost
3. moraju imati osjećaj da su važni.

Ako iz menadžerske i voditeljske perspektive možemo učiniti to da ljudi osjećaju da vjeruju, da pripadaju i da su važni, uhvatit će se rješavanja bilo kakvog izazova. Ako ljudi razumiju viši cilj, mogu ostvariti emocionalnu povezanost koja upravlja njihovim svakodnevnim aktivnostima. Ovo je jedan od ključnih razloga zašto je potrebno puno vremena posvetiti definiranju misije. Uz to, potrebno je uložiti vrijeme da bi se približilo i stvorilo razumijevanje kod članova odjela informacijske sigurnosti, da su njihovo radno mjesto i opis posla itekako povezani s poslovnim ciljevima organizacije.

Kao primjer, operativni cilj može biti instalacija sigurnosnih zakrpa (eng. *patch*) unutar tjedan dana od dana izlaska nove inačice softvera. Cilj je tim više smislen ako uspostavimo vezu s poduzećem koristeći se premisom „ja vjerujem, ja pripadam i ja sam bitan“. Vjeruju u misiju „Zaštiti da bi omogućio“, odnosno da nisu štitili da bi omogućili, ostali zaposlenici organizacije ne bi mogli obavljati svoj posao, a organizacija ne bi ispunjavala svoje rezultate i svoju svrhu. Brza ugradnja sigurnosnih zakrpi bitna je zato što pomaže našim korisnicima da rade svoj posao, što pak organizaciji omogućuje da ispuni svoje ciljeve.

2.6. Učenje od drugi poslovnih voditelja

Voditelj na CISO funkciji može puno naučiti od ostalih poslovnih voditelja. Danas se rukovoditeljske funkcije sve više odmiču od rada po principu „zapovijedaj i kontroliraj“ (eng. *command and control*) i pristupaju suradnji koja se koristi prednostima različitosti ideja zaposlenika. Ovaj princip nije sporazum koji vodi u beskonačne debate i nedonošenje odluka. Cilj voditelja je da osigura usklađenost sa zajedničkom misijom i da ubrza donošenje odluka.

Unutar opisanog okvira, različiti pogledi i rasprave potiču kreativnost, stvaraju nove ideje i produktivne tenzije koje mogu potaknuti rezultat.

Zbog toga što sigurnost može biti frustrirajuća, čak i zastrašujuća, važno je otkriti kako pomoći zaposlenicima da ostanu motivirani. Važno im je pomoći da osjete da napreduju – ne samo kada postignu velike ciljeve, već i kada rješavaju manje probleme, s kojima se svakodnevno susreću.

Prilike za vođenjem neprestano se ukazuju, u svakoj interakciji unutar tima, s drugim djelatnicima IT odjela i s ostalim poslovnim partnerima. Pitanje koje je ovdje potrebno postaviti jest – koristimo li se svakom prilikom da nametnemo svoju misiju i time pomognemo organizaciji da ostvari uspjeh.

Na tehničkim pozicijama ili u organizacijama tehničkog sektora, često je fokus na tehničkim pitanjima dok čovjek pada u drugi plan. Iz iskustva, smatram da je potrebno održavati međuljudski kontakt, koji potiče osjećaj pripadnosti. Ako znamo više jedni o drugima, više nam je stalo. Svaka je interakcija prilika za uzajamno učenje i povećanje kompetencija. Zadnji i najvažniji kriterij za učinkovito vodstvo je sposobnost da razvijemo druge vođe unutar odjela sigurnosti. U protivnom, snaga tima da upravlja rizicima bit će prisutna samo dok je tu i aktualni CISO. Razvojem kompetencija u dubinu, CISO može osigurati da organizacija isporuči održiv rezultat tijekom vremena.

Tablica 2.1 prikazuje istraživanje izvršne agencije za pretraživanje, Korn Ferry – koje sugerira da vođe u području kibernetičke sigurnosti trebaju posjedovati jedinstven skup osobina, uključujući sposobnost razmišljanja izvan okvira, duboko pronicanje u probleme, primjenu prosudbe na razini upravnog odbora te moraju biti vjerodostojan poslovni partner.

Tablica 2.1 Karakteristike voditelja u području kibernetičke sigurnosti

Ključne karakteristike za izvršne direktore u području kibernetičke sigurnosti			
Stručnosti	**Iskustvo**	**Osobine**	**Pokretači**
Strateški, globalno usmjeren mislilac (sposoban sagledati širu sliku)	Dubina tehničkog iskustva	Brzo učenje (prilagodljivost novom i drugačijem)	Traži uloge visoke vidljivosti i odgovornosti
Mislilac izvan okvira	Razumije pravne i regulatorne okvire	Fleksibilan	Nastoji biti agent promjene (umjesto „ne“ agent)
Analitički (zadire duboko u probleme)	Uspješno se nosi sa sigurnosnim incidentima u prošlosti	Razumijevanje i tolerancija za dvosmislenost	Mora „proći kroz iglene uši“ da bi uravnotežio vođenje promjena s upravljanjem rizicima poduzeća
Posjeduje poslovnu vještinu (razumije kako se informacije primjenjuju u svakodnevnim operacijama)		Intelektualno radoznao	Traži blisku suradnju s poslovnim liderima (radi na dodavanju poslovne vrijednosti)
Balansira suprotstavljene prioritete			
Komunicira i utječe na široko područje (upravni odbor, vrhovni menadžment).			
Privlači, gradi i koristi se talentima.			

Kako se tehnološko okruženje nastavlja razvijati, mnogi ljudi vjeruju da se pomičemo k budućnosti u kojoj će organizacije većinu svojih IT potreba i aktivnosti ugovarati s trećim stranama (engl. *outsourcing*). Ako se takav trend i dalje nastavi, pitanje je kakav to ima utjecaj na CISO funkciju ?

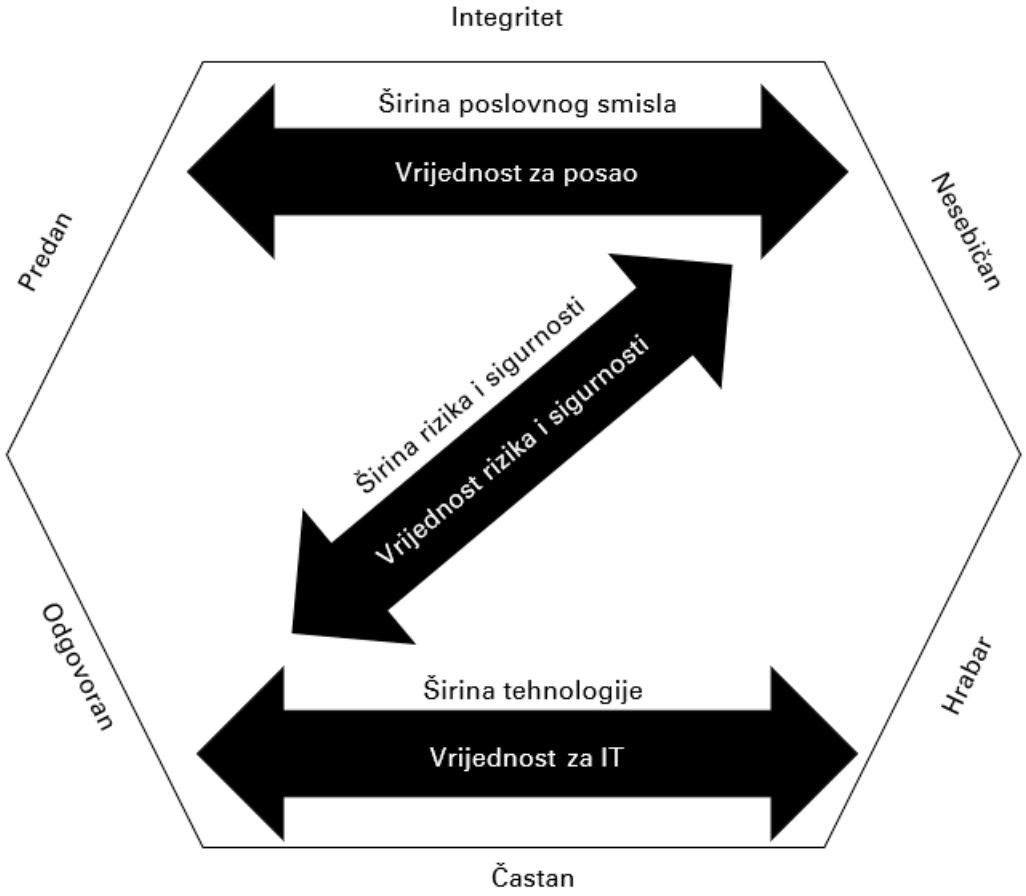
U ovom pogledu na budućnost, organizacija se udaljava od implementacije IT-a prema nabavi i upravljanju dobavljačima i uslugama, istovremeno postavljajući smjer i uspostavljajući cjelokupnu IT arhitekturu.

Osim toga, organizacija će morati zadržati ključnu stručnost odjela zaduženog za sigurnost, a to je upravljanje rizikom informacija. Organizacije ne mogu u potpunosti prenijeti rizik na druge. Mogu se unajmiti organizacije koje će isporučivati poslovne sustave, ali i dalje odgovornost za usklađenost s propisima poput SOX-a i HIPAA, GDPR-a ostaje na organizaciji. Ako povreda podataka rezultira curenjem osobnih podataka ili podataka intelektualnog vlasništva, organizacija je i dalje odgovora za izvještavanje i prijavu sigurnosnog incidenta. Dodatno, organizacije često snose posljedice šteta od incidenta koji se često odražava na umanjenje vrijednosti brenda, premda su vektor napada i razlog dolaska do sigurnosnog incidenta nedostatak i ranjivost u sustavu dobavljača. S obzirom na sve veći broj propisa i činjenicu da se sve više osobnih podataka pohranjuje u poslovnim sustavima, rizici mogu samo rasti. Prema tome, sposobnosti CISO funkcije će ostati bitne, čak i ako se promijeni naziv poslovne funkcije unutar organizacije. Dok god je CISO funkcija sposobna pružati traženu kompetenciju u stalno promjenjivom okruženju organizacije, tako da se vodi misijom „Zaštiti da bi omogućio“, taj doprinos poslovanju svake organizacije nije zanemariv. Pitanje i odluka svake organizacije jest postoji li svjesnost, volja ili regulatorna obveza da sistematizira takvu poslovnu funkciju u vidu radnog mjesta. Hoće li to radno mjesto i funkcija imati isključivu odgovornost za informacijsku sigurnost, stvar je regulacije, odluke uprave organizacije i u konačnici, sposobnostima pojedinca koji upotpunjava to radno mjesto.

Očito je da vođenje podrazumijeva preuzimanje odgovornosti. Ipak, čini se da neki CISO-i, barem povremeno, zaboravljaju tu tvrdnju. Tipična situacija iz prakse ide otprilike ovako: CISO je upozorio na sigurnosni problem, ali nije mogao dobiti proračun ili resurse za njegovo rješavanje. Stoga je odustao od odgovornosti, jer je netko drugi donio odluku da neće financirati rješenje. Autor ovog rada ima drugačije mišljenje – čak i ako se ne slažemo s odlukom, trebamo se potruditi izraziti svoje vrijednosti. Moramo artikulirati potencijalni utjecaj na organizaciju, naše kupce i na društvo.

Kao partner u strategiji organizacije, CISO bi se trebao obvezati na donesenu odluku i dijeliti potpunu odgovornost i odgovornost prema kolegama. Da bi navedeno bilo ostvarivo, potrebno je jasno izraziti osobne vrijednosti i ostati dosljedan vlastitim principima. Pridržavanje osobnih vrijednosti može značiti preuzimanje rizika za vlastitu karijeru. Stoga je ključno da si pojedinac koji obnaša CISO funkciju uzme vremena za razmišljanje o načelima i vrijednostima koje zaista slijedi. Neka vrsta osobnog propitivanja koju svaki CISO treba proći dodaje još

jednu dimenziju konceptu pojedinca Z-oblika – dimenziju vrijednosti – kao što je prikazano na (Sl. 2.2).



Sl. 2.2 Dodatna dimenzija pojedinca Z-oblika: osobne vrijednosti koje diktiraju naše aktivnosti [4]

3. Poslovi i odgovornosti CISO funkcije

3.1. Podrška i odgovornost za standardizaciju

U ovom dijelu rada opisat ćemo najčešće certifikacijske standarde, za čije je certificiranje, održavanje i recertificiranje odgovoran CISO.

Razvoj standarda za informacijsku sigurnost na međunarodnoj razini uključuje Međunarodnu organizaciju za standardizaciju, ISO (engl. *International Organization for Standardization*), Međunarodni elektronički konzorcij i IEC (engl. *International Electronics Consortium*). Druge organizacije pružaju specifične standarde za određene sektore, a često se temelje na „ISO“ standardima (obično nazvane ISO/IEC) ili se na njih referiraju. U Sjedinjenim Američkim Državama ovim radom upravljaju Američki nacionalni institut za standarde (ANSI) i Međunarodni odbor za standarde informacijske tehnologije (INCITS). Skupina izravno odgovorna za razvoj, doprinos i upravljanje ovim radom je INCITS CS/1, kibernetička sigurnost. Ova grupa, CS/1, također je odgovorna za standardizaciju područja informacijske tehnologije (IT), sigurnosti, privatnosti, upravljanja identitetom i biometrijsku sigurnost. Jedno od glavnih područja fokusa za CS/1 uključuje standarde informacijske sigurnosti poznate kao ISO/IEC 27001:2013 (zahtjevi za upravljanje informacijskom sigurnošću – sustav upravljanja informacijskom sigurnošću) i ISO/IEC 27002:2013 (specifikacija za upravljanje informacijskom sigurnošću). Radi jednostavnosti, ovi će se standardi od sada nazivati „ISO 27002“ i „ISO 27001“. Također je važno napomenuti da je od travnja 2007. ISO 17799 prošao promjenu označavanja i preimenovan je u ISO 27002. Nakon toga, 2013. provedene su izmjene i revizije obaju standarda, dok je posljednja izmjena standarda ISO 27001 provedena u 2022. godini.

Ovi standardi, ISO 27001 i ISO 27002 (ranije poznat kao ISO 17799) odnose se na područje informacijske sigurnosti. ISO 27001 je standard za sustav upravljanja informacijskom sigurnošću (ISMS), dok je ISO 27002 najbolja praksa za informacijsku sigurnost. Iako na prvi pogled može biti zbunjujuć, njihov odnos nije teško razumjeti. Mnogi ljudi zamjenjuju ISO 27001 i ISO 27002 s britanskim standardom (BS) 7799, ali – iako su slični, nisu isti. Važno je napomenuti da je veći dio rada u ovom području započeo i razvio se na temelju BS-a 7799, prije nego što je bio izmijenjen i odobren kao ISO standard. Ono što danas imamo rezultat je tog početnog rada u kombinaciji s doprinosom i sudjelovanjem više zemalja.

ISO/IEC 27001 je međunarodni standard koji postavlja zahtjeve za stvaranje, strukturu i upravljanje ISMS-om (sustavom upravljanja informacijskom sigurnošću). Ovaj je standard jedna od bitnijih odgovornosti CISO funkcije jer održavanje, provedba, certificiranje i recertificiranje aktivnosti su u koje je uključen CISO, često kao glavni odgovorni ili kao medijator između, naprimjer, vanjskog društva za certificiranje i organizacije.

ISO 27001 sadrži pet glavnih područja, koja se često nazivaju „odjeljci 4 do 8“. Ta područja obuhvaćaju ISMS, odgovornost menadžmenta, interne revizije ISMS-a, pregled ISMS-a koji obavlja menadžment i poboljšanje ISMS-a. Ta četiri odjeljka organizaciji omogućuju da stvori strukturu programa, odnosno ISMS. Većina je stručnjaka za informacijsku sigurnost upoznata s ISO-m 9001, koji se bavi sustavima upravljanja kvalitetom. ISO 27001 može se zamisliti kao slična struktura, ali u kontekstu informacijske sigurnosti. To se može vizualizirati poput kišobrana. ISO 27001 pruža gornji sloj definiranja načina dokumentiranja, organiziranja, osnaživanja, revizije, upravljanja i poboljšanja Vašeg programa informacijske sigurnosti. Drugim riječima, ISMS je struktura organizacije za upravljanje ljudima, procesima i tehnologijom. Ovo poglavlje će Vam pružiti informacije o standardima, ali neće se detaljno baviti opisima redova ili popisom ciljeva kontrole.

ISO 27002 pruža ciljeve kontrole s relevantnim pravnim, regulatornim ili poslovnim zahtjevima koji se odnose na organizaciju informacijske sigurnosti. Postoji deset različitih područja koja ISO 27002 pokriva [8]:

1. sigurnosna politika
2. organizacija sigurnosti
3. klasifikacija imovine i kontrola
4. sigurnost osoblja
5. fizička i okolišna kontrola
6. upravljanje komunikacijama i operacijama
7. kontrola pristupa
8. razvoj i održavanje sustava
9. upravljanje kontinuitetom poslovanja
10. usklađenosti.

Uz pravne, regulatorne i poslovne zahtjeve organizacije, ovi ciljevi kontrole pružaju temelj za ISO 27001 ISMS (sustav upravljanja informacijskom sigurnošću). Ako promotrite Prilog A standarda ISO 27001, primijetit ćete da su ciljevi kontrole iz standarda ISO 27002 tamo ponovljeni. Kada voditelj sigurnosti, ili praktičar, želi certificirati program svoje organizacije kao program usklađen s ISO-m 27002, to se zapravo postiže certifikacijom prema kriterijima definiranima u ISO 27001. To može izgledati zbunjujuće, ali treba razumjeti da je cilj dokazati provedbu primjenjivih kontrola iz ISO-a 27002 (također Prilog A standarda ISO 27001), a ISMS razvijen prema ISO-u 27001 (opći zahtjevi) pruža način za postizanje toga.

Odjeljak 4 obuhvaća zahtjeve za razvoj, implementaciju, upravljanje i poboljšanje ISMS-a. Jedan od prvih koraka u razvoju ISMS-a je definiranje opsega. Taj opseg može se temeljiti na fizičkoj lokaciji, funkciji, organizacijskoj kulturi, okruženju ili logičkim granicama. Radi pojednostavljenja, mnoge se organizacije koriste fizičkim ili logičkim granicama. Opseg uključuje fizičke, tehničke, informacijske i programske elemente te ljudske resurse. Ovdje ćemo malo dublje razmotriti koncept opsega, jer to je ključni koncept u informacijskoj sigurnosti i reviziji.

Kada razvijate program informacijske sigurnosti temeljen na ISO-u 27001, bez cilja certifikacije, vaš će opseg biti na mjestu za koje ste odredili da je vaš program informacijske sigurnosti primjenjiv. Naprimjer, možda radite za poduzeće s više divizija. Vaš opseg može obuhvaćati samo diviziju za koju ste odgovorni, ali ne i ostale, niti nadređenu korporativnu strukturu. Razmislite o opsegu u smislu dosega kontrole, što je ključno za uspješnost bilo kojeg programa. Možete odlučiti iskoristiti izgradnju programa temeljenog na ISO-u 27001 da biste proširili postojeće kontrole radi postizanja dosljednosti ili upravljanja rizicima.

Ako stvarate opseg u svrhu certifikacije, postoji nekoliko važnih stvari koje treba uzeti u obzir:

1. Koja je vrijednost sadržaja domene definirane opsegom organizacije?
2. Imate li raspon kontrola na toj domeni?
3. Koje su uloge i odgovornosti osoba povezanih s tom domenom?
4. Koje se logičke i fizičke granice mogu primijeniti za definiranje domene?
5. Koje iznimke postoje?
6. Je li željeni opseg razuman za certifikaciju?

Kada određujete vrijednost sadržaja, dostupne su vam mnoge formule kojima se možete koristiti. Neke se temelje na mjerljivim vrijednostima, poput novčane vrijednosti opreme.

Druge se temelje na riziku ili poslovnom utjecaju (mogućnost velikih poremećaja u poslovanju zbog nedostupnosti, itd.). Često se kombinacija ovih pristupa pokazuje najuspješnijom.

Raspon kontrole je ključni koncept koji se odnosi na uspješno određivanje opsega. Treba analizirati nad čime postoji izravna kontrola, na što se može utjecati ili nad čime nema utjecaja. Opsezi certifikacije obično se bave područjima nad kojima nemate kontrolu ili imate ograničen utjecaj putem sporazuma o razini usluge (eng. *service level agreement*), memoranduma o razumijevanju, dokumenta odgovornosti ili drugih metoda. Pokušaj stvaranja opsega s malo ili nimalo kontrole možda nije mudra ideja i može uzrokovati frustraciju zbog neučinkovitog programa ili neuspješnog pokušaja certifikacije.

Unutar opsega postoje uloge i odgovornosti koje trebaju biti objašnjene i razumljive da bi se izbjeglo preklapanje i dupliciranje. Odgovornost za upravljanje ISMS-om treba biti zadana, kao i odgovornost za aktivnosti koje čine svakodnevno funkcioniranje sustava. Uporaba RACI dijagrama (u kojima se zadaci dijele na četiri vrste uloga: Odgovoran, Odgovorni, Konzultiran, Informiran), ili matrica odgovornosti odličan je način da se sve te informacije jasno prikažu.

Fizičke i logičke granice mogu se primijeniti da bi se definiralo gdje postoji opseg i također mogu pomoći u razjašnjavanju raspona kontrole. Te granice mogu biti zidovi, podovi, ograde, itd. (fizičke granice) ili virtualne lokalne mreže, segmenti ili filtrirani portovi (logičke granice). To je posebno važno u pripremi opsega za podatkovni centar. Ulazne i izlazne točke, kako fizičke tako i logičke, mogu se identificirati i trebaju se ispitati i dokumentirati.

Još jedan važan korak pri izradi opsega je dokumentiranje iznimki. Izmjene su sve što nije primjenjivo prema kontrolnim ciljevima u Prilogu A. Zahtjevi u Sekcijama 4 do 8 su upravo to – obvezni. Za ta se područja ne mogu dokumentirati iznimke. Jedan način za rješavanje navedenoga je stvaranje liste napretka ili primjena procesa koji organizira te iznimke. Moguće se dovesti u situaciju u kojoj je potrebno obraniti svoje razloge za iznimke tijekom revizije.

Najvažnije pitanje na koje treba odgovoriti jest posljednje pitanje koje je ranije postavljeno: je li opseg razuman za pokušaj certifikacijske revizije? Mnoge organizacije, kada prvi put odluče krenuti tim putem, odluče certificirati cijelu organizaciju. Iako to može biti uspješno u manjim organizacijama s jakom kontrolom, za većinu organizacija nije razumno. Iskustvo je pokazalo da se uspješna certifikacija temelji na programu koji je dizajniran i implementiran na razini poduzeća, ali u kojem se posebnosti certifikacije primjenjuju na resurse koji imaju najveću vrijednost za organizaciju. Ishod je situacija u kojoj organizacija može imati

koristi od programa za informacijsku sigurnost koji ste razvili (Vaš ISMS) i od certifikacije koja je međunarodno priznata i primijenjena na Vaše najvrjednije resurse ili usluge. Najbolja praksa je razmotriti onaj opseg certifikacije koji ima smisla. Neka od pitanja koja nas mogu usmjeriti su: je li organizacija pružatelj usluga? (razmislite o certifikaciji dijelova vaše organizacije koji pružaju te usluge vašim klijentima), je li organizacija financijska institucija? (razmislite o certifikaciji usluga ili centara u kojima se pohranjuju, upotrebljavaju i zadržavaju informacije o klijentima). Ako se želi certificirati na razini poduzeća, preporučljivo je podijeliti svoje napore na upravljive domene i na njih primijeniti isti proces određivanja opsega.

Definiranje politike ISMS-a znači upravo to, pisanje politike. Predlošci politika su popularni polazni bodovi, ali treba biti oprezan pri uporabi gotovog dokumenta – ako se cilja na certifikaciju ili izgradnju učinkovitog programa. Svaka dobra politika trebala bi biti temeljito promišljena. Prečesto se u politiku stavljaju komponente specifikacija (npr. minimalne 128-bitne enkripcije), a to sprječava mogućnost upravljanja. Nitko ne želi svaki put ići pred upravni odbor kada treba ažurirati tehničke postavke. Najbolja praksa je kada Vaša „politika“ odgovara kulturi i okruženju Vaše organizacije. Potrebno je posvetiti vrijeme da biste bili sigurni da se ne stvara nerealan politički okvir, kojemu ne možete udovoljiti, a čime organizaciju osuđujete na neuspjeh.

Upravljanje rizicima simbolizira različite stvari različitim ljudima, ali svatko bi trebao cijeniti fleksibilnost i poslovno prihvatljiv pristup koji nude ISO standardi. Iz perspektive ISO standarda, veća je zabrinutost da imate organizacijski pristup riziku, kriterije ili pragove te ponovljivu metodologiju. Postoje informativne reference (opcionalne, informativne) koje su izravno primjenjive. Dvije od njih su:

1. ISO/IEC 27005 *Information Technology – Security Techniques – Information Security Risk Management*
2. ISO/IEC TR 13335-3, *Information Technology – Guidelines for the Management of IT Security – Techniques for the Management of IT Security*.

Preporučljiva je primjena tih dokumenata kao izvora informacija. Nakon provedene temeljite procjene rizika, trebali bismo imati vrlo dobru predodžbu o tome gdje se nalaze važni rizici, koje kontrole postoje i koji je preostali rizik. Prihvaćanje ili prijenos također su odobrene metode za upravljanje rizikom.

Praćenje i održavanje ISMS-a – ovi zahtjevi osiguravaju da aktivno upravljate ISMS-om. Nije dovoljno samo razumjeti što imate, već to morate i redovito pregledavati. Potrebno je provjeravati pogreške ili sigurnosne događaje, pregledavati učinkovitost i provjeravati jeste li i dalje usklađeni s ciljevima. Potrebno je posvetiti određeno vrijeme da bi se poboljšao ISMS, istovremeno osiguravajući da se rješavaju identificirani problemi ili nedostaci.

Potrebno je održavati dokumente i zapise, kako je navedeno u preostalim zahtjevima iz Odjeljka 4. Za to su navedeni određeni tipovi dokumenata i zahtjevi za kontrolu dokumenata. Sva važna dokumentacija treba biti pohranjena na lako dostupnom mjestu, uz održavanje integriteta tih informacija. U tu svrhu često se upotrebljava sustav upravljanja sadržajem, portal ili mrežni poslužitelj. Međutim, nema zahtjeva koji nalaže da ti zapisi moraju biti elektronički. U certifikaciji obratite pozornost na Odjeljak 4.3.1, jer ćete te stavke morati imati u blizini i spremne za revizore. To su osnovne kategorije stvarnih dokumenata koji čine ISMS.

Unutarnja revizija još je jedna obavezna funkcija, a zahtjevi su opisani u Odjeljku 6. To je funkcija koja provjerava je li Vaš ISMS u skladu s vašim zahtjevima. Ovdje su obuhvaćeni očekivani aspekti vezani za pregled; uključujući raspored, izvedbu i zahtjeve za otklanjanje nedostataka. Unutarnji pregled važan je postupak jer omogućuje identifikaciju i rješavanje problema među ciklusima revizije certifikacijskog tijela. Ako pronađete problem, možete ga popraviti, ali ozbiljni problemi ili neusuglašenosti moraju se prijaviti.

Pregled upravljanja je tema Odjeljka 7. Ovaj odjeljak izravno je povezan s PDCA (Planiraj, Realiziraj, Provjeri, Djeluj) modelom, koji je temelj za sve ISO standarde ISMS-a. Ovdje se pregledavaju Vaše radnje, promjene u okruženju, mjerenja i ostalo. Sastoji se od dva dijela, jedan koji se bavi „ulazima“ i drugi, koji se bavi „izlazima“. Dio za „izlaz“ pomaže dokumentirati Vaše radnje, razmatranja i rezultate. Ti su tipovi zapisa važni za prikaz aktivnog upravljanja ISMS-om.

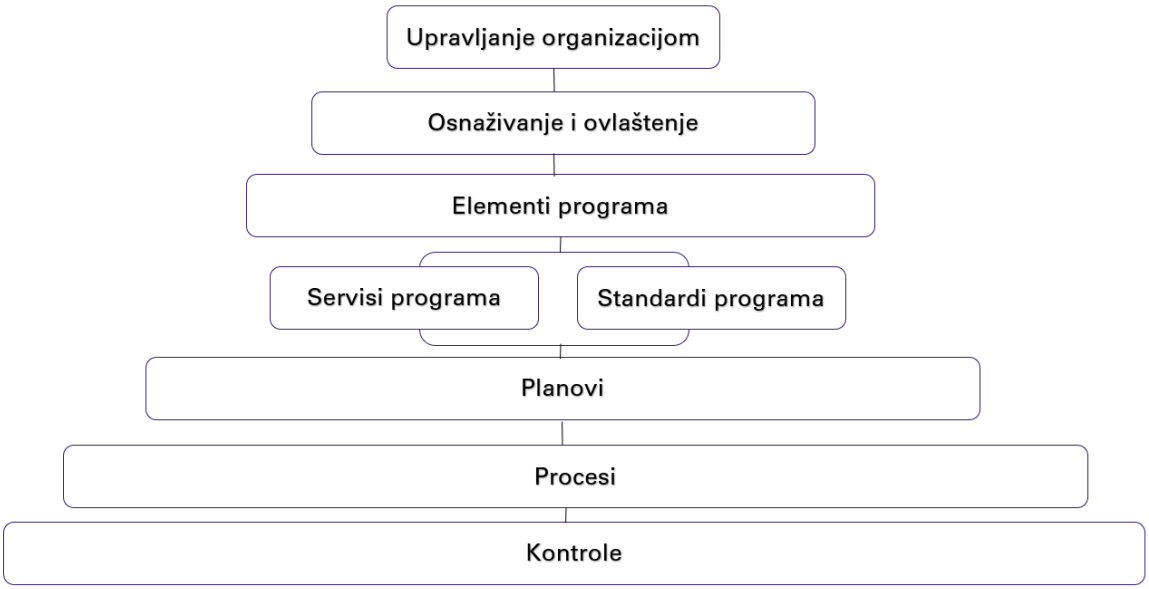
Posljednji odjeljak, Odjeljak 8, bavi se poboljšanjem ISMS-a. Često se uspoređuje sa sustavnim poboljšanjem procesa, što on u osnovi i jest. Odjeljak 8 može se pojednostaviti na sljedeći način: ispravljujuće radnje, koje se usredotočuju na identificirane probleme i preventivne radnje, poduzete da bi se izbjegli negativni događaji i utjecaji. Često su ove preventivne radnje posljedica pregleda ispravljajućih radnji.

To bi trebalo pružiti osnovno razumijevanje onoga što se obuhvaća općim zahtjevima ISO-a 27001. Kao što je vidljivo, postoje različiti standardi i dokumenti koji zajedno doprinose učinkovitosti ISMS-a.

U kontekstu aktivnosti CISO-a, ISO 27000 grupa standarda najčešće pripada aktivnostima i odgovornostima koje se pripisuju toj funkciji unutar neke organizacije. Standardi ISO 27001 grupe podložni su neprestanoj izmjeni i dopuni, shodno dinamici današnjice. ISO 27000 je standard dizajniran da bi poučio i obavijestio o tome što je grupa dokumenata 27000 i kako su oni međusobno povezani. Također sadrži terminologiju koja je svojevrsna ovoj grupi ISO standarda.

1. ISO 27002 (od travnja 2007.) trenutačno poznat kao ISO 17799.
2. ISO 27003 smjernica je za implementaciju ISO-a 27001, usmjeravajući se na opće zahtjeve (odjeljci 4 do 8).
3. ISO 27004 prikuplja mjerenja i metrike iz ISMS-a (Sustava upravljanja informacijskom sigurnošću).
4. ISO 27005 pokriva upravljanje rizikom u vezi s ISO-om 27001 i ISMS-om.
5. ISO 27006 bavi se zahtjevima za akreditacijska tijela (osobe koje obavljaju certifikacijske revizije).

Dodatni standardi u grupi 27000 bit će dodani prema potrebi kako bi podržali ukupne standarde sustava upravljanja informacijskom sigurnošću. Na slici (Sl.3.1) opisani su odnosi i funkcije standarda.



Sl. 3.1 Referentni model upravljanja informacijskom sigurnošću

Iako ti standardi pokrivaju informacijsku sigurnost, ne opstaju odvojeni od drugih. Postoji popriličan broj drugih standarda koji su komplementarni s ovom grupom, naprimjer ISO 20000 (upravljanje IT uslugama) je komplementaran i presijeca se s ISO-m 27001 i ISO-m 27002.

CISO-i se često se pitaju kako se standardi poput COBIT-a (Ciljevi kontrole za informacije i povezanu tehnologiju) i standarda Nacionalnog instituta za standarde i tehnologiju (NIST) odnose prema ISO standardima. Iako ISO 27001 neće izravno propisati blokiranje određenog porta na vatrozidu, zahtijevat će razumijevanje okoline rizika i primjenu odgovarajuće kontrole, to jest, sugestivno će dovesti do zaključka da je blokiranje tog porta poželjno. Važno je razumjeti da su standardi više operativni, ISO standardi bave se pitanjima kako sigurnosni menadžeri (pa tako i CISO-i) zapravo upravljaju informacijskom sigurnošću. To pomaže na taktičkoj i strateškoj razini, oblikujući procese za donošenje odluka koje utječu na operativnu razinu. Operativni zahtjevi proizlaze iz zakonskih, regulatornih ili poslovnih zahtjeva. Kada se ovi elementi pravilno kombiniraju, rezultat je sveobuhvatni program informacijske sigurnosti.

Nadalje, svaki CISO mora razumjeti i razdvojiti potrebu od dobrovoljne odluke uprave neke organizacije da odredi potrebu za certificiranjem na osnovi informacije sigurnosti.

Ovi razlozi uključuju traženje načina za pružanje dokaza o aktivnostima, potrebnu pozornost, odgovornost i usklađenost s regulativama. ISMS, prema ISO-u 27001, jasno udovoljava zahtjevima Zakona Sarbanes-Oxley i drugih sličnih zakonodavstava u Sjedinjenim Američkim Državama ili diljem svijeta, putem procesa identifikacije i ispunjavanja zahtjeva. Drugi to vide kao putokaz u budućnost, razumijevajući gdje će se budući zahtjevi moći lakše ispuniti, uz postojeću dokazanu i prilagodljivu strukturu.

S uspostavljenim ISO 27001 ISMS-om, organizacije dobivaju temeljnu strukturu za upravljanje informacijskom sigurnošću, koja se može prilagoditi budućim zahtjevima. Ova dokazana i prilagodljiva struktura organizacijama omogućuje da se lakše prilagode promjenjivim zahtjevima u području informacijske sigurnosti i da uspješno ispune buduće zahtjeve. Budući da se informacijska sigurnost neprestano razvija i mijenja, organizacije koje imaju implementiran ISO 27001 ISMS imaju prednost, jer već imaju strukturiran i testiran okvir. Ova struktura organizacijama pomaže da brže i učinkovitije reagiraju na nove zahtjeve, jer već imaju procese, kontrole i prakse koje se mogu prilagoditi i primijeniti na nove scenarije.

Osim toga, ISO 27001 ISMS pruža okvir za stalno poboljšanje. Procesom praćenja i revizije, organizacije mogu identificirati nedostatke, rizike i nove zahtjeve te ih adresirati u skladu s ciljevima poboljšanja informacijske sigurnosti. Tako ISO 27001 ISMS djeluje kao putokaz u budućnost, omogućujući organizacijama da budu spremne za promjene i razvijaju sigurnosne prakse da bi se na najbolji mogući način susrele s budućim zahtjevima.

Jasan primjer vodstva u industriji pokazuju organizacije poput Fujitsua, Premier Bankcarda i Federal Reserve Banke New Yorka, koje su među prvima u svijetu certificirale svoje sustave upravljanja informacijskom sigurnošću prema ISO-u 27001, kada je standard objavljen u studenom 2005. godine. Različite organizacije iskoristile su napore u implementaciji ISMS-a da bi ubrzale sazrijevanje u svom poslovanju, istovremeno zadržavajući fleksibilnost. Certifikacija prema ISO-u 27001 pruža organizacijama priznanje za njihovu posvećenost i usklađenost s međunarodno priznatim standardima informacijske sigurnosti. Organizacije koje su među prvima certificirale svoje sustave upravljanja informacijskom sigurnošću prema ISO-u 27001 pokazuju proaktivnost u industriji i posvećenost osiguravanju visoke razine sigurnosti informacija.

Implementacija ISMS-a prema ISO-u 27001 organizacijama omogućuje da uspostave sveobuhvatan okvir za upravljanje rizicima – identificirajući sigurnosne prijetnje, procjenjujući

ih i upravljajući njima. Ovaj okvir pomaže organizacijama u izgradnji kulture informacijske sigurnosti i stalnom poboljšanju.

Certifikacija prema ISO-u 27001 također pokazuje da organizacija ozbiljno pristupa zaštiti informacija i da ima sustavni pristup upravljanju sigurnošću informacija. Ovo može pružiti povjerenje dionicima, klijentima i partnerima; pokazujući da organizacija primjenjuje najbolje prakse u području informacijske sigurnosti.

Iskorištavanje napora u implementaciji ISMS-a omogućuje organizacijama da ubrzaju sazrijevanje u području informacijske sigurnosti, primjenjujući dokazane smjernice i prakse koje su dio ISO 27001 standarda. Istovremeno, organizacije zadržavaju fleksibilnost te mogu prilagoditi svoje pristupe prema svojim specifičnim potrebama i uvjetima poslovanja.

Ukupno gledajući, ISO 27001 certifikacija pruža organizacijama prednosti u smislu priznavanja njihove posvećenosti sigurnosti informacija, poboljšanja poslovnog ugleda i stjecanja povjerenja dionika. Certifikacija također podržava organizacije u razvoju sazrelih praksi upravljanja informacijskom sigurnošću, što je ključno za uspjeh u suvremenom digitalnom okruženju.

Jedan od ključnih razloga zašto je ISO 27001 standard koji je sklon poslovnom modelu organizacije jest činjenica da je utemeljen na rizicima i samim time nema rigidnost koja bi mogla biti paralizirajuća za poslovanje. CISO može odabrati koje ciljeve želi ostvariti, ovisno o riziku, zakonu i regulatornim zahtjevima.

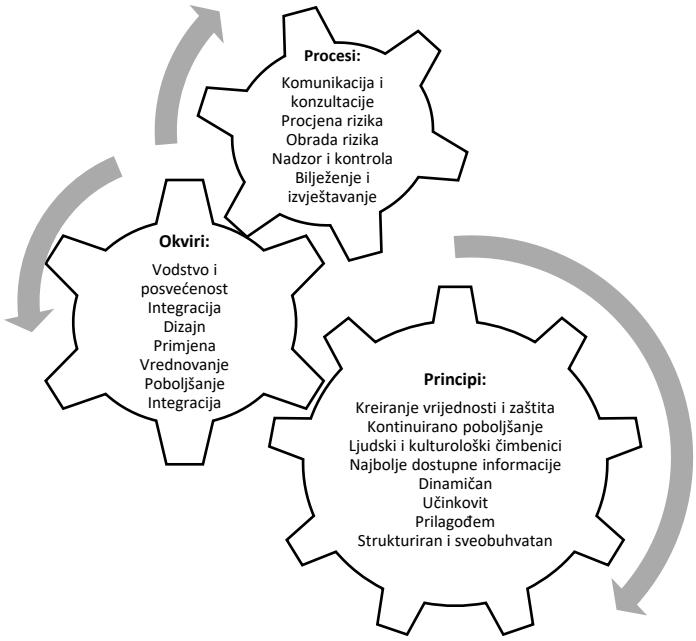
3.2. Upravljanje rizikom informacijske sigurnosti u skladu s normom ISO/IEC 31000

Kako je navedeno u prethodnim poglavljima, upravljanje rizicima jedan je od ključnih zadataka i odgovornosti svake CISO funkcije. Upravljanje rizicima, tj. procjenama rizika informacijske sigurnosti je među obveznim aktivnostima za uspješno certificiranje prema ISO 27001 standardu te ga je obvezno provoditi.

Rizik informacijske sigurnosti je kombinacija vjerojatnosti pojavljivanja nekog neželjenog događaja, odnosno prijetnje koja se koristi ranjivosti informacijske imovine i negativnih posljedica tog događa na povjerljivost, cjelovitost i raspoloživost podataka. Informacijska imovina, tj. resurs, sva su sredstva kojima se organizacija koristi u svrhu ostvarivanja svojih poslovnih ciljeva, kao što su: infrastruktura, hardver, softver i podaci. Upravljanje rizikom bilo

koje vrste provodi se učestalo i interaktivno, a služi kao pomoć upravljačkoj strukturi organizacije u donošenju strategije, postizanju ciljeva i donošenju argumentiranih odluka.

Prema standardu, da bi se rizikom upravljalo učinkovito i dosljedno, postupak se mora sastojati od zadanih međuovisnih principa, okvira i procesa [9]. Na slici (Sl. 3.2) je prikazana sveobuhvatnost.



Sl. 3.2 Prikaz principa, okvira i procesa upravljanja rizikom u skladu s normom *ISO/IEC 31000*

Upravljanje rizikom informacijske sigurnosti sveobuhvatan je postupak, kojim se potvrđuje poslovna opravdanost odabira propisanih mjera i standarda s ciljem osiguranja dovoljne razine sigurnosti. Naprimjer, tijela i pravne osobe koje postupaju s klasificiranim podacima dužne su upravljati rizikom informacijske sigurnosti, trajnim procjenjivanjem i odabirom rizika u skladu s međunarodnim standardima i normama, kao što su *ISO/IEC 27005, ISO/IEC 31000, COSO* i dr., a radi sprječavanja njihovog neovlaštenog otkrivanja ili gubitka [10].

Proces upravljanja rizikom informacijske sigurnosti prema normi *ISO/IEC 31000,* sastoji se o sljedećih aktivnosti:

1. komunikacija i konzultacija (engl. *communication and consulting*),
2. određivanja opsega, konteksta i kriterija (engl. *scope, context and criteria*),
3. procjene rizika (engl. *risk assessment*)

a. identifikacija rizika (engl. *risk identification*),
b. analiza rizika (engl. *risk analysis*)
c. vrednovanje rizika (engl. *risk evaluation*)

4. obrade rizika (engl. risk treatment),
5. nadzora i kontrole (engl. *monitoring & review*),
6. bilježenja i izvještavanja (engl. *recording & reporting*).

3.2.1. Komunikacija i konzultacije

Ova aktivnost pomaže svim glavnim vanjskim i unutarnjim dionicima tijela ili pravne osobe u razumijevanju rizika, osnovi za donošenje odluka i razlozima zbog kojih je potrebno provesti određene aktivnosti. Glavni cilj je osigurati različite poglede i stručna znanja pri određivanju kriterija vrednovanja rizika. Razmjena podataka u komunikaciji i pri konzultacijama mora biti temeljena na činjenicama, pravovremena, relevantna, točna i razumljiva te stalna tijekom svih aktivnosti procesa upravljanja rizikom.

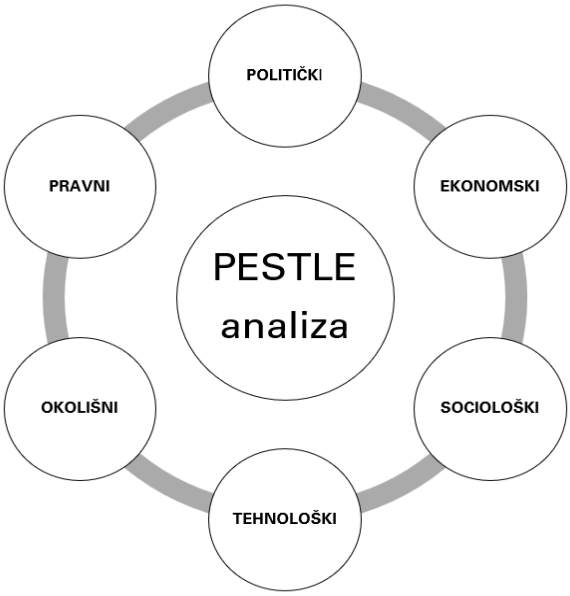
Na početku procesa upravljanja rizikom nužno je postaviti opseg aktivnosti koje je potrebno provesti i uskladiti ciljeve procesa s ciljevima tijela ili pravne osobe, uz razumijevanje konteksta u kojem tijelo ili pravna osoba djeluje.

3.2.2. Opseg, kontekst i kriterij

Svrha ove aktivnosti je prilagodba procesa upravljanja rizikom osobitostima tijela ili pravne osobe da bi se procjena rizika provela djelotvorno, a rizik obradio na odgovarajući način. Na početku samog procesa upravljanja rizicima potrebno je objasniti opseg aktivnosti koje je potrebno provesti i uskladiti ciljeve procesa s ciljevima organizacije, ali u kontekstu u kojem organizacija posluje. Da bi se postiglo razumijevanje konteksta, potrebno je prepoznati, analizirati i u obzir uzeti vanjske i unutarnje čimbenike, odnosno tržište u kojem organizacija posluje. Potrebno je prepoznati kako se oni odnose prema aktivnostima i procesima upravljanja

rizikom. U prepoznavanju vanjskih čimbenika primjenjuje se PESTLE[3] analiza, a pri prepoznavanju unutarnjih utjecaja, SWOT[4] analiza [11] [12].

PESTLE analiza, prikazana na (Sl. 3.3) razmatra političke, ekonomske, sociološke, tehnološke, pravne i okolišne čimbenike; neovisno o tome razmatramo li organizaciju na međunarodnoj, regionalnoj ili lokalnoj razini. Osim opisanih čimbenika, vanjski se utjecaji mogu odnositi i na ugovorne obveze, percepciju ključnih dionika ili organizacije te trendove i slično.



Sl. 3.3 Faktori PESTLE analize [13]

Jedna od najpoznatijih, a ujedno osnovna tehnika strateške analize, predstavljena još 1969. u domeni poslovne znanosti je SWOT analiza, odnosno SWOT matrica. U svrhu spoznaje

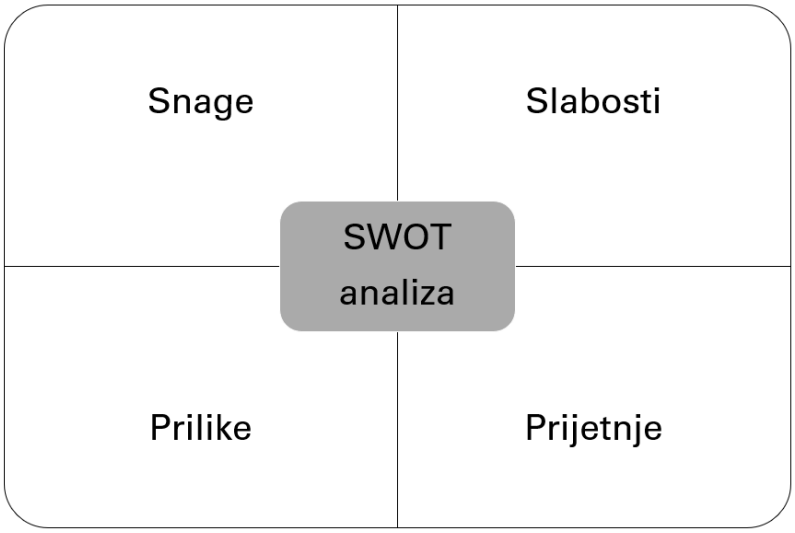
[3] PESTLE, odnosno PEST analiza predstavljena je 1967. godine, kao metoda za otkrivanje i kvantificiranje čimbenika koji su izvan kontrole poduzeća, a utječu na njegovo poslovanje. Riječ *PESTLE* akronim je početnih slova riječi, koje na engleskom jeziku označavaju političke (engl. *Political*), ekonomske (engl. *Economic*), sociološke (engl. *Social*), tehnološke (engl. *Technological*), pravne (engl. *Legal*) i čimbenike okoliša (engl. *Environmental*).

[4] SWOT analiza, odnosno SWOT matrica, jedna je od najpoznatijih i osnovnih tehnika strateške analize iz područja poslovnih znanosti, predstavljena 1969. godine. Da bi se došlo do strateških saznanja i poduzele pravilne mjere i aktivnosti za postizanje poslovnih i drugih ciljeva poduzeća, analiziraju se i identificiraju njegova četiri aspekta: snage (S, kratica od engl. *Strengths*), slabosti (W, kratica od engl. *Weaknesses*), prilike (O, kratica od engl. *Opportunities*) i prijetnje (T, kratica od engl. *Threats*).

strateških saznanja, da bi se mogle poduzeti pravilne mjere i aktivnosti za postizanje poslovnih i drugih ciljeva organizacije, analiziraju se četiri aspekta:

1. snage (S, kratica od engl. *Strengths*),
2. slabosti (W, kratica od engl. *Weaknesses*),
3. prilike (O, kratica od engl. *Opportunities*),
4. prijetnje (T, kratica od engl. *Threats*).

Uz to se za organizaciju analiziraju vizija, misija, vrijednosti (ljudski resursi, tehnologije, podaci, informacijski sustav i dr.), način kruženja podataka, organizacijska struktura i kultura, strategija, ciljevi, politike, standardi i preporuke koje je organizacija usvojila. SWOT analiza se može upotrijebiti za prepoznavanje vanjskih i unutarnjih utjecaja. U toj se situaciji snage i slabosti organizacije svrstavaju u unutarnje utjecaje, dok se prilike i prijetnje svrstavaju u vanjske utjecaje [14]. Na (Sl. 3.4), prikazan je aspekt SWOT analize.



Sl. 3.4 SWOT analiza

Na kraju ove aktivnosti potrebno je odrediti kriterije, odnosno vrijednosti rizika, koji su u kontekstu ciljeva prihvatljivi odnosno neprihvatljivi za organizaciju. Osim samih ciljeva, pri određivanju kriterija potrebno je u obzir uzeti vrijednosti, postojeće politike, obveze i mišljenja ključnih dionika te tehniku koja će se primjenjivati pri procjeni vrijednosti razine rizika.
Premda se određuju na početku procesa upravljanja rizikom, mjerila je potrebno sustavno revidirati i po potrebi, mijenjati za vrijeme trajanja procesa. Prema zadanim mjerilima se, u konačnici, za svaki pojedini rizik donosi odluka o načinu njegove obrade. Primjer zadanih

mjerila i raspona vrijednosti dobivenih modificirano-kvantitativnom tehnikom prikazan je u Tablici 3.1.

Tablica 3.1 Primjer mjerila za prihvaćanje rizika informacijske sigurnosti

Raspon vrijednosti	Razina rizika	Opis rizika
1 – 20	NIZAK	Rizik je dovoljno malen, da nije potrebno primjenjivati dodatne kontrole za male ili zanemarive štete odnosno vjerojatnost realizacije prijetnje.
21 – 45	SREDNJI	Rizik je srednje razine, potrebno je planirati način obrade za znatne štete odnosno vjerojatnosti realizacije prijetnje.
46 – 75	VISOK	Rizik je visoke (kritične) razine, potencijalna šteta može ugroziti poslovanje Društvo, odnosno realizacija prijetnje je gotovo sigurna tijekom razdoblja od godine dana.

3.2.3. Procjena rizika

U kontekst informacijske sigurnosti, rizik za pojedini resurs odnosno imovinu procjenjuje se uzimajući u obzir njegovu vrijednosti (engl. *Assets Value* – AV), ranjivost tog resursa engl. *Vulnerability* – V), prijetnje koje mogu iskoristiti tu ranjivost (engl. *Threat* – T), vjerojatnosti ostvarenja prijetnji (engl. *Probability* – P) i posljedice (engl. *Impact* – I) koje se mogu dogoditi ako se određena prijetnja ostvari. Matematički rizik predstavlja funkciju navedenih varijabli:

$$R = f(AV, V, T, P, I) \text{ [15]} \qquad (1)$$

Da bi rezultate procjene rizika mogli smatrati valjanima, sam postupak mora zadovoljiti sljedeće kriterije [15]:

1. jednoznačnost
2. pouzdanost
3. objektivnost
4. ponovljivost.

Procjena rizika je najvažniji, najosjetljiviji i najduži dio procesa upravljanja rizikom, koji sadrži tri aktivnosti: identifikaciju, analizu i vrednovanje rizika.

Identifikacija rizika provodi se pronalaženjem, prepoznavanjem i opisivanjem svih mogućih rizika koji bi u negativnom smislu mogli utjecati na ostvarivanje ciljeva organizacije i njihovih izvora, tj. ranjivosti i prijetnji vezanih za pojedinu ranjivost, bilo da su pod njezinim direktnim utjecajem ili ne. Bitno je identificirati sve moguće izvore rizika, jer one ranjivosti i prijetnje koje se ne identificiraju, bit će isključene iz daljnjeg procesa upravljanja rizikom. Pri identifikaciji, organizacija može primijeniti razne alate i tehnike, kao što su: pregled sustava, analiza dokumentacije, intervjui, upitnici, sigurnosno testiranje, penetracijsko testiranje i slično – prilagođene vlastitim ciljevima i uvjetima – te se koristiti ranijim iskustvom s rizicima koji su se već ostvarili [15]. Za identifikaciju ranjivosti i prijetnji bitno je da su prikupljene informacije relevantne i ažurne. U ovu aktivnost potrebno je uključiti sve ključne sudionike koji su adekvatni u poznavanju područja za koje se ona provodi.

Nakon završene faze identifikacije rizika i njihovih izvora slijedi postupak analize rizika sa svrhom stjecanja razumijevanja prirode i karakteristika identificiranih rizika. Postupak uključuje identifikaciju, dodjelu ili procjenu [17]:

1. grupa imovine
2. vrijednosti razine rizika
3. razine ranjivosti imovine
4. vlasništva nad imovinom
5. učinkovitosti ranije primijenjenih mjera
6. vrijednosti imovine
7. vjerojatnosti pojavljivanja prijetnji.

U praksi se imovina često grupira prema postojanju istih ili sličnih karakteristika i zahtjeva na informacijsku sigurnost i djelovanja sličnih tipova prijetnji. U Tablici 3.2 prikazano je jedno takvo grupiranje, a izraz „vlasnik“ u ovom je kontekstu potrebno shvatiti kao onog koji ima odgovornost za uporabu, razvoj i održavanje sigurnosti i imovine, a ne kao nekog tko ima vlasnička prava. U ovoj fazi također je bitno identificirati primijenjene mjere. Identifikacija mjera pomaže u procjeni učinkovitosti i optimizaciji postojećih mjera. Procjena učinkovitosti uspostavljenih mjera provodi se tako da se analizira postupak za koji one umanjuju razinu ranjivosti imovine ili vjerojatnost ostvarivanja prijetnje.

Tablica 3.2 Primjer kataloga imovine s ranjivostima i prijetnjama

Grupa imovine	Ranjivost	Prijetnja
Hardver i infrastruktura	Uporaba opreme bez odgovarajuće TEMPEST zaštite	Špijunaža i prisluškivanje
	Neodgovarajući smještaj i fizička zaštita	Fizičke manipulacije ili krađa imovine
	Neodgovarajući klimatizacijski uređaj i/ili napajanje	Kvarovi, neispravnost ili uništenje hardvera i nepostojanje servisa
	Neodgovarajuće održavanje uz neodvajanje testne i produkcijske okoline	
	Neodgovarajući kapacitet (engl. *singl point of failure*)	Nefunkcionalnost ili preopterećenost servisa
		Gubitak podataka
Softver	Neodgovarajuće upravljanje zakrpama nadogradnji ili neodržavanje	Kvarovi, neispravnost i neraspoloživost servisa
		Poznate ranjivosti, zloćudni softver
		Privremena nedostupnost ili trajni gubitak podatka zbog djelovanja ucjenjivačkog softvera
	Neodvajanje testne i produkcijske okoline	Kvarovi, neispravnost i neraspoloživost servisa
		Privremena nedostupnost ili trajni gubitak podataka zbog djelovanja ucjenjivačkog softvera
	Ne postoji antivirusni softver ili se antivirusne definicije ne ažuriraju redovito	Poznate ranjivosti, maliciozni softver
		Privremena nedostupnost ili trajni gubitak podatka zbog djelovanja ucjenjivačkog softvera
	Neodgovarajuća kontrola i nadzor uporabe	Neovlaštene radnje
	Neodgovarajuća konfiguracija	
	Neodgovarajuće upravljanje autorizacijama	Neovlašteni pristup i curenje podataka
Usluge i procesi	Neodgovarajuće upravljanje	Nedostupnost ili neučinkovitost
	Neodgovarajuća dokumentacija	Pogrešno formulirani ili obavljeni postupci

Grupa imovine	Ranjivost	Prijetnja
Podaci	Izostanak izrade sigurnosnih kopija podataka	Gubitak podataka
	Neadekvatna pohrana sigurnosnih kopija podataka	
	Neodgovarajuća razmjena ili distribucija podataka	Gubitak, curenje ili manipulacija podacima
	Mogućnost iznosa podataka	
	Nepravilno uništavanje ili brisanje podataka	
	Izostanak enkripcije sigurnosno osjetljivih podataka	Prisluškivanje ili odavanje informacija
	Nekontrolirano izlaganje ispisanih sigurnosno osjetljivih dokumenata	Neovlašteni pristup podacima
		Curenje podataka
	Izlaganje podataka na zaslonu računala	Neovlašteni pristup podacima
Prostorni resursi	Neodgovarajuća zaštita prostora od neželjenog elektromagnetskog zračenja (TEMPEST)	Špijunaža i prisluškivanje
	Neodgovarajući nadzor prostora	Fizičke manipulacije ili otuđenje imovine
	Neodgovarajuća kontrola pristupa prostorima	Neovlašteni pristup
		Gubitak ili curenje podataka
		Špijunaža ili prisluškivanje
	Neodgovarajuća zaštita prostora od provale	Provala
	Neodgovarajuća zaštita prostora od požara	Požar
	Osjetljivost objekta na vanjske uvjete	Viša sila (vremenske nepogode, udar groma, poplava, potres)
Ljudski resursi	Neodgovarajuće upravljanje	Neraspoloživost ili gubitak osoblja
	Neodgovarajuće ili neobučeno osoblje	Greške u radu i neodgovornost
	Nedovoljna provjera ili informiranost/izobrazba u području informacijske sigurnosti	Socijalni inženjering i špijunaža
	Nezadovoljno ili nepouzdano osoblje	Otuđenje ili zlonamjerno uništavanje imovine
		Širenje netočnih informacija

	Neodgovarajuća zaštita identiteta i vjerodajnica	Otuđenje identiteta i neovlašten pristup servisima
	Neodgovarajuće rukovanje imovinom	Otuđenje imovine
		Gubitak ili curenje podataka
	Pristup imovini osoblja trećih strana	Zlouporaba prava pristupa
		Gubitak ili curenje podataka
		Narušavanje integriteta informacijskog sustava

Najčešći način za određivanje vrijednosti imovine temelji se na parametrima kao što su:

1. nabavna vrijednost, trošak zamijene ili ponovnog stvaranja imovine
2. trošak koji bi nastao zbog gubitka povjerljivosti, cjelovitosti i raspoloživosti imovine
3. reputacijski gubitak.

Odabirom jednog ili više parametara imovini se dodjeljuju odgovarajuće numeričke vrijednosti temeljem procjena vlasnika informacijske imovine, angažiranih procjenitelja ili intervjua s korisnicima i administratorima sustava. Nakon toga slijedi odluka o tome ulazi li imovina dalje u postupak procjene rizika ili ne, a donosi se na temelju dodijeljene joj numeričke vrijednosti. Primjer vrednovanja podataka na temelju troška ili nastale štete zbog gubitka, povjerljivosti, cjelovitosti i raspoloživosti prikazan je u Tablici 3.3.

Tablica 3.3 Primjer određivanja vrijednosti podatka temeljem parametara CIA-e

Numerička vrijednost	Oznaka	Opis		
		Povjerljivost	Cjelovitost	Raspoloživost
1	Vrlo niska	Javno dostupne informacije	Izmjena koja ne uzrokuje dodatni posao ili zaostatke u radu	Nedostupnost koja ne uzrokuje gomilanje posla
2	Niska	Informacije dostupne svim zaposlenicima	Izmjena uzrokuje dodatni posao ili zaostatke u radu	Nedostupnost koja uzrokuje gomilanje posla i zaostatke u radu
3	Srednja	Interne informacije za koje je potrebna ovlast	Izmjena uzrokuje zaostatke u radu i mogući financijski gubitak	Nedostupnost koja uzrokuje znatne probleme u radu i mogući financijski gubitak
4	Visoka	Informacije o poslovnim partnerima	Izmjena uzrokuje sigurni financijski gubitak	Nedostupnost koja uzrokuje sigurni financijski gubitak
5	Vrlo visoka	Poslovna tajna	Izmjena uzrokuje dodatni posao ili zaostatke u radu	Nedostupnost koja uzrokuje znatne probleme i predstavlja mogući financijski gubitak

Vrijednost rizika može se procijeniti kvalitativnim i kvantitativnim metodama. Svaka od metoda, neovisno o kategorizaciji, zbog svojih nedostataka nije prikladna za upravljanje rizikom informacijske sigurnosti, zbog čega se predlaže njihova kombinacija u modificiranu kvalitativnu tehniku [15].

Modificirana kvalitativna tehnika temelji se na određenim pretpostavkama, a one su [15]:

1. svaka imovina ima svoju vrijednost
2. za pojedinu imovinu ranjivost može ili ne mora postojati (ako je uspostavljena jaka zaštita i kontrola)
3. ranjivost i prijetnje su međusobno ovisne (ako postoji ranjivost, postoji i prijetnja, a ako postoji prijetnja, postoji i ranjivost)
4. prijetnja ima vjerojatnost koja ovisi o okolnostima
5. prijetnja ima moguće posljedice, čija veličina ovisi o okolnostima.

Ako uzmemo u obzir sve navedene pretpostavke, procjena rizika modificiranom kvalitativnom metodom može se prikazati kao umnožak vrijednosti imovine, vjerojatnosti nastanka prijetnje i ranjivosti imovine:

$$R = AV * P * V \text{ [15]} \quad (2)$$

Raspon vrijednosti koji svaki od navedenih parametara može poprimiti, proizvoljan je. Primjer raspona vrijednosti imovine prikazan je u Tablici 3.4, primjer raspona vrijednosti vjerojatnosti ostvarivanja prijetnje prikazan je u Tablici 3.5, a primjer raspona vrijednosti ranjivosti imovine dan je u Tablici 3.6.

Tablica 3.4 Primjer raspona vrijednosti imovine

	Razina	Oznaka	Opis
Vrijednost imovine	1	Vrlo niska	Vrlo niska vrijednost
	2	Niska	Niska vrijednost
	3	Srednja	Srednja vrijednost
	4	Visoka	Visoka vrijednost
	5	Vrlo visoka	Vrlo visoka vrijednost

Tablica 3.5 Primjer raspona vrijednosti vjerojatnosti ostvarivanja prijetnje

	Razina	Oznaka	Opis
Raspon vrijednosti vjerojatnosti ostvarivanja prijetnje	1	Vrlo niska	Vrlo niska vjerojatnost pojavljivanja prijetnje
	2	Niska	Niska vjerojatnosti pojavljivanja prijetnje
	3	Srednja	Srednja vjerojatnost pojavljivanja prijetnje
	4	Visoka	Visoka vjerojatnost pojavljivanja prijetnje
	5	Vrlo visoka	Vrlo visoka vjerojatnost pojavljivanja prijetnje

Tablica 3.6 Primjer raspona vrijednosti ranjivosti imovine

	Razina	Oznaka	Opis
Raspon vrijednosti ranjivosti imovine	1	Niska	Vrlo niska vjerojatnost pojavljivanja prijetnje
	2	Srednja	Niska vjerojatnost pojavljivanja prijetnje
	3	Visoka	Srednja vjerojatnost pojavljivanja prijetnje

Na temelju jednadžbe (2) i vrijednosti iz tablica 3.3, 3.4 i 3.5 može se izračunati da je najmanja procijenjena vrijednost rizika R_{min} jednaka 1, maksimalna vrijednost procijenjenog rizika R_{max} jednaka je 125. U Tablici 3.7 prikazana je modificirana matrica za procjenu vrijednosti rizika s primijenjenim kriterijima za prihvaćanje rizika iz Tablice 3.1.

Tablica 3.7 Modificirana matrica za procjenu vrijednosti razine rizika

Prijetnja i ranjivost imovine	Razina vjerojatnosti ostvarivanja prijetnje	1			2			3			4			5		
	Razina ranjivosti imovine	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Vrijednost imovine	1	1	2	3	2	4	6	3	6	9	4	8	12	5	10	15
	2	2	4	6	4	8	12	6	12	18	8	16	24	10	20	30
	3	3	6	9	6	12	18	9	18	27	12	24	36	15	30	45
	4	4	8	12	8	16	24	12	24	36	16	32	48	20	40	60
	5	5	10	15	10	20	30	15	30	45	20	40	60	25	50	75

Na temelju podataka koji su proizašli iz provedene analize rizika, provodi se vrednovanje rizika s ciljem donošenja odluka o daljnjim aktivnostima. Odluke se donose na temelju usporedbe razina procijenjenih vrijednosti rizika s kriterijima prihvaćanja rizika organizacije [9]. Odluke mogu rezultirati time da se za pojedine rizike ne poduzimaju daljnje aktivnosti, da se razmatraju mogućnosti obrade, poduzmu daljnje aktivnosti, provedu dodatne analize radi boljeg razumijevanja rizika, zadrže primijenjene mjere ili preispitaju ciljevi organizacije.

3.2.4. Obrada rizika

Obrada rizika je iterativni postupak koji obuhvaća odabir, planiranje i primjenu novih mjera, procjenu učinkovitosti primijenjenih mjera, donošenje odluke o prihvatljivosti preostalog

rizika. Uz to, obuhvaća poduzimanje daljnjih koraka za slučaj da odabrane i primijenjene mjere nisu postigle željeni učinak [9].

Prema [10], obrada rizika je postupak u kojem se za svaki procijenjeni rizik utvrđuje stupanj prihvatljivosti rizika, radi njegovog prihvaćanja, smanjenja ili izbjegavanja.

3. Rizik bi se mogao prihvatiti ako bi nastala šteta bila manja od štete koja bi nastala zbog neprovođenja određene aktivnosti.
4. Smanjivanje rizika provodi se primjenom sigurnosnih mjera, radi sprečavanja uništenja, otuđenja, gubitka i neovlaštenog pristupa klasificiranim podacima.
5. Izbjegavanje rizika podrazumijeva poduzimanje organizacijskih mjera, u cilju izbjegavanja radnji koje bi mogle izazvati rizik.

Odluku o postupanju s preostalim rizikom, nakon obrade rizika donosi glavni i odgovorni za upravljanje organizacijom [10]. Kod poslovnih subjekata iz korporativnog svijeta, to je najčešće izvršni direktor, predsjednik uprave (CEO, engl. *chief executive officer*), dok je u javnom sektoru to najčešće ravnatelj određene institucije.

Uz navedeno, rizik se može prenijeti na treću stranu, naprimjer osiguravajuće društvo ili dobavljača, to jest treću stranu [9].

Pri odabiru strategije obrade rizika potrebno se pobrinuti o učinkovitosti mjera u postizanju ciljeva organizacije u odnosu na troškove i zalaganje koje je potrebno poduzeti pri njihovoj primjeni. Osim ekonomske računice, potrebno se brinuti i o ranije preuzetim obavezama i mišljenju ključnih dionika tijela ili pravne osobe. Također, odabir mora biti usklađen i s ranije određenim kriterijima za prihvaćanje rizika te s resursima s kojima tijelo ili pravna osobe raspolaže.

Preostali (rezidualni) rizik je onaj koji podrazumijeva sve one ranjivosti i prijetnje za koje se smatra da ne zahtijevaju dodatnu obradu u pogledu njihovog smanjivanja, a za koje je ustanovljeno da troškovi implementacije eventualnih mjera nisu isplativi i za koje trenutačno ne postoji odgovarajuća mogućnost obrade ili za koje obrada nije postigla željeni učinak. Takav je rizik potrebno dokumentirati, mora ga formalno prihvatiti čelnik tijela ili pravna osoba i mora postati predmet daljnjeg nadzora i kontrole.

Ishodi ove aktivnosti se obično objedinjavaju u Planu postupanja s rizicima, temeljnom dokumentu koji omogućava provedbu upravljanja rizicima informacijskog sustava i u kojem se određuje kako, kojim redoslijedom i u kojem će se roku odabrane mjere primijeniti [16].

Takav plan mora biti integriran u upravljačke dokumente organizacije i priopćen svim zainteresiranim dionicima, a između ostalog, treba obuhvatiti [9]:

1. rizike koji će se obrađivati
2. prvenstva obrade
3. odabrane mjere za pojedine rizike
4. odgovorne osobe za implementaciju odabranih mjera
5. resurse potrebne za implementaciju mjera
6. ograničenja
7. termine početka i roka završetka implementacije odabranih mjera.

3.2.5. Nadzor i kontrola

Može se dogoditi da postupak obrade rizika ne postigne željene učinke i izazove, neplanirane i neželjene posljedice neovisno o planiranju i dizajniranju samog procesa. Stalni nadzor i izmjenična kontrola procesa upravljanja rizikom i iz njega proizašlih rezultata trebali bi biti dio samog postupka i provoditi se u svim njegovim fazama, a pogotovo tijekom obrade rizika, jer obrada pojedinog rizika može uzrokovati novi rizik, koji je potrebno identificirati i obraditi na odgovarajući način [9].

3.2.6. Bilježenje i izvještavanje

Postupak upravljanja rizikom i same rezultate tog postupka potrebno je sustavno bilježiti i o njima izmjenično izvještavati. Cilj izvještavanja je taj da svi zainteresirani dionici organizacije u bilo kojem trenutku budu upućeni o bitnim činjenicama i pomognu u davanju podataka potrebnih za donošenje odluka. Odluke koje se mogu donijeti na temelju rezultata procjene rizika informacijske sigurnosti mogu imati znatne posljedice za sve postupke u organizaciji, uključujući i one poslovno vitalne. Bilježenje, dokumentiranje i jasno izvještavanje potrebno je za učinkovito upravljanje rizicima informacijskog sustava.

4. Relevantna legislativa za informacijsku sigurnost unutar Republike Hrvatske i EU-a

Punopravnim članstvom Republike Hrvatske u EU-u te posljedičnim daljnjim integracijskim procesima, kao što je ulazak u Eurozonu i Schengen, odluke Europskog parlamenta i ostalih zakonodavnih i regulatornih tijela Europske unije, postaju i dio legislative Republike Hrvatske. Ovdje ćemo istaknuti neke od važnih zakona i njihov utjecaj na potrebu za CISO funkcijom, kao i na njezine odgovornosti i aktivnosti.

Neki od važnih zakona, odluka i akata su:

1. Zakon o kritičnim infrastrukturama, koji je na snazi od 1. 1. 2023.
2. Odluka o primjerenom upravljanju informacijskim sustavom, na snazi od 23. 9. 2022.
3. Smjernice za primjereno upravljanje rizicima informacijskog sustava subjekta nadzora, na snazi od 21. 12. 2022.
4. Zakon o informacijskoj sigurnosti, 13. 7. 2007.
5. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, od 26. 7. 2018.
6. Kazneni zakon, na snazi od 1. 1. 2023.
7. Zakon o elektroničkim komunikacijama, na snazi od 12. 7. 2022.
8. Zakon o provedbi opće uredbe o zaštiti podataka, 3. 5. 2018.

Ovaj rad opisuje relevantnu legislativu koliko je to potrebno da bi se pojasnila i opisala potreba za CISO funkcijom u organizacijama različitih sektora i poslovnih ciljeva. Neovisno o činjenici što veće i ozbiljnije organizacije u svojoj strukturi imaju pravne odjele, u kojima postoje stručnjaci specijalizirani u navedenoj legislativi; CISO funkcija, koja nije dio pravne službe, treba imati svjesnost i određeno razumijevanje navedenih zakona i odluka.

4.1. Zakon o kritičnim infrastrukturama

Ovim zakonom uređuju se nacionalne i europske kritične infrastrukture, sektori nacionalnih kritičnih infrastruktura, upravljanje kritičnim infrastrukturama, izrada analize rizika, sigurnosni

plan vlasnika, sigurnosni koordinatori za kritičnu infrastrukturu, postupanje s osjetljivim i klasificiranim podacima i nadzor nad provedbom zakona [18].

Ovim se zakonom u zakonodavstvo Republike Hrvatske preuzima pravna stečevina Europske unije sadržana u Direktivi Vijeća 2008/114/EC, o identifikaciji europskih kritičnih infrastruktura i procjeni potrebe za unaprjeđenjem njihove zaštite [18].

Zakon određuje **sigurnosnog koordinatora za kritičnu infrastrukturu**, kao osobu koja djeluje vezano za zaštitu kritične infrastrukture između vlasnika/upravitelja i središnjih tijela državne uprave odgovornih za pojedini sektor kritične infrastrukture [18]. U ovoj definiciji nedvojbeno je objašnjena CISO funkcija.

Središnja tijela državne uprave određuju sigurnosnog koordinatora za kritičnu infrastrukturu i njegova zamjenika za svaki sektor kritične infrastrukture iz svog djelokruga.

Nacionalne kritične infrastrukture su sustavi, mreže i objekti od nacionalne važnosti, čiji bi prekid u djelovanju ili u isporuci robe ili usluga mogao imati ozbiljne posljedice na nacionalnu sigurnosti, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti.

Sektori koji mogu sadržavati sektore kritične infrastrukture:

Energetika

- proizvodnja
- akumulacije i brane
- prijenos
- skladištenje
- transport energenta i energije
- sustav za distribuciju.

Komunikacijska i informacijska tehnologija

- elektroničke komunikacije
- prijenos podataka,
- informacijski sustavi
- pružanje audio i audiovizualnih medijskih usluga.

Promet

- cestovni
- željeznički
- zračni

- pomorski i promet unutarnjim plovnim putovima.

Zdravstvo

- zdravstvena zaštita
- proizvodnja
- promet i nadzor nad lijekovima.

Vodno gospodarstvo

- regulacijske i zaštitne vodne građevine i komunalne vodne građevine

Hrana

- proizvodnja hrane i opskrba njome
- sustav sigurnosti hrane
- robne zalihe.

Financije

- bankarstvo
- burze
- investicije
- sustavi osiguranja i plaćanja.

Proizvodnja, skladištenje i prijevoz opasnih tvari

- kemijskih
- bioloških
- radioloških
- nuklearnih materijala.

Javne službe

- osiguranje javnog reda i mira
- zaštita i spašavanje
- hitna medicinska pomoć.

Nacionalni spomenici i vrijednosti.

Vlada Republike Hrvatske (u daljnjem tekstu Vlada) može odlukom odrediti kritične infrastrukture i iz drugih sektora. Vlada posebnom odlukom određuje sektore iz kojih središnja tijela državne uprave identificiraju pojedine nacionalne kritične infrastrukture. Također određuje popis redoslijeda sektora kritične infrastrukture zbog njihova značaja za opće funkcioniranje zemlje.

U zakonu je također definiran pojam **Vlasnik/Upravitelj kritičnom infrastrukturom**, kao pravna osoba odgovorna za upravljanje kritičnom infrastrukturom [18].

Vlasnici/Upravitelji kritične infrastrukture dužni su odrediti sigurnosnog koordinatora za kritičnu infrastrukturu, koji je u provedbi zaštite kritične infrastrukture odgovoran za

komunikaciju o sigurnosnim pitanjima između vlasnika i mjerodavnog središnjeg državnog tijela državne uprave u čijem je djelokrugu kritična infrastruktura [18].

Iz ovog zakona potrebno je istaknuti pojam Europske kritične infrastrukture. To su infrastrukture koje su u interesu najmanje dvjema državama članicama ili jednoj državi članici koja se nalazi na teritoriju druge države članice [18]. Europske kritične infrastrukture mogu se odrediti u sektorima koje određuje Europska komisija.

Podaci vezani za određivanje pojedine kritične infrastrukture europskom kritičnom infrastrukturom klasificirani su podatak. Kriterij za određivanje stupnja tajnosti tih podataka propisuje Vlada, svojom odlukom. Ako se kritična infrastruktura važna za Republiku Hrvatsku nalazi na području druge države članice Europske unije, Vlada predlaže mjerodavnom tijelu te države određivanje europske kritične infrastrukture. U slučaju da država članica na čijem se teritoriju nalazi kritična infrastruktura ne prihvati prijedlog Vlade, Vlada o tome obavještava Europsku komisiju i traži njezino uključivanje. Europska kritična infrastruktura na području Republike Hrvatske štiti se jednako kao nacionalna kritična infrastruktura, osim ako je uredbama Europske unije to pitanje drugačije uređeno.

Vlada jednom godišnje usvaja izvještaj o broju europskih kritičnih infrastruktura po sektoru i broju zainteresiranih država koje ovise o svakoj određenoj kritičnoj infrastrukturi. Taj prijedlog dostavlja središnje tijelo državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja. Ovaj se izvještaj dostavlja Europskoj komisiji i zainteresiranim državama članicama koje ovise o toj infrastrukturi.

Vlada svake dvije godine Europskoj komisiji dostavlja sažetak općih podataka o vrstama opasnosti, prijetnjama i slabostima utvrđenima u svakom sektoru u kojem Republika Hrvatska ima europsku kritičnu infrastrukturu [18].

Zakonima je također određena kontaktna točka za potrebe razmjene podataka i koordiniranje aktivnosti u vezi s europskim kritičnim infrastrukturama s drugim državama članicama i tijelima Europske unije, a to je središnje tijelo državne uprave u čijem su djelokrugu poslovi zaštite i spašavanja.

Uz to, predviđen je i nadzor, tj. inspekcijski nadzor nad provedbom ovog Zakona kod vlasnika/upravitelja kritičnih infrastruktura, koji provode središnja državna tijela državne uprave u čujem su djelokrugu pojedine kritične infrastrukture i mjerodavne regulatorne agencije. Upravo u ovakvom procesu poželjno je da organizacija koja je vlasnik/upravitelj

kritične infrastrukture ima kompetentnu i stručnu osobu koja vlada potrebnim znanjem, koje može iskoristi u korespondenciji i dokazivanju usklađenosti sa Zakonom te poboljšanju razine informacijske sigurnosti. Takve funkcije unutar organizacije mogu biti upotpunjenje CISO funkcijom.

Također, Zakon za organizacije koje su vlasnici/upravitelji kritične infrastrukture, propisuje prekršajne odredbe. Tako će novčanom kaznom od 66.360 do 132.720 EUR biti kažnjeni vlasnici/upravitelji kritične infrastrukture ako [18]:

1. ne izrade Analizu rizika, kao podlogu sigurnosnog plana
2. ne odrede sigurnosnog koordinatora za kritičnu infrastrukturu.

Dodatno, kaznit će se i odgovorna osoba vlasnika/upravitelja kritičnih infrastruktura – od 1.320 do 6.630 EUR.

U Zakonu je određena funkcija CISO-a putem pojma i opisa aktivnosti koordinatora za kritičnu infrastrukturu i propisana kaznena odredba ako se ne odredi. Također, ovim Zakonom nije određen oblik u kojem CISO funkcija mora izvršavati aktivnosti i preuzeti odgovornost koordinatora za kritičnu infrastrukturu.

4.2. Odluka o primjerenom upravljanju informacijskim sustavom

Na temelju članka 101. stavka 2. točke 1. Zakona o kreditnim institucijama i članka 43. stavka 2. točke 10. Zakona o Hrvatskoj narodnoj banci, guverner Hrvatske narodne banke donio je Odluku o primjerenom upravljanju informacijskim sustavom (u daljnjem tekstu Odluka).

Tom Odlukom pobliže se propisuju obveze kreditne institucije koje se odnose na upravljanje informacijskim sustavom te upravljanje rizicima informacijske i komunikacijske tehnologije. Odredbe ove Odluke primjenjuju se na kreditnu instituciju sa sjedištem u Republici Hrvatskoj, koja je od Hrvatske narodne banke dobila odobrenje za rad. Također, odredbe ove Odluke na odgovarajući način primjenjuju se na podružnicu kreditne institucije iz treće zemlje koja je od Hrvatske narodne banke dobila odobrenje za osnivanje podružnice kreditne institucije iz treće zemlje. Odlukom su objašnjeni određeni pojmovi, među kojima su i pojmovi CIA akronima (C kratica od engl. *Confidentiality*, I kratica od engl. *Integrity*, A kratica od engl.

Availability) te IKT-a (informacijska i komunikacijska tehnologija), operativni i sigurnosni incident, kibernetički napad i drugi.

Stavka 4 ovog Zakona odnosi se na informacijsku sigurnost, u kojoj su objašnjeni i propisani svi bitni elementi informacijske sigurnosti kreditne institucije. Tako je kreditna institucija dužna izraditi i dokumentirati politiku informacijske sigurnosti kojom se određuju načela i pravila za zaštitu povjerljivosti, cjelovitosti i dostupnosti podataka kreditne institucije i njezinih klijenata. Politika informacijske sigurnosti mora biti u skladu s ciljevima kreditne institucije glede informacijske sigurnosti i temeljiti se na relevantnim rezultatima procjene rizika, a uprava kreditne institucije dužna je tu politiku odobriti [19]. Politika mora sadržavati opis glavnih uloga i odgovornosti upravljanja informacijskom sigurnošću, a uz to, kreditna institucija dužna je osigurati da svi radnici i treće strane na odgovarajući način budu upoznati s politikom informacijske sigurnosti.

Na temelju politike informacijske sigurnosti, kreditna institucija dužna je uspostaviti i provoditi sigurnosne mjere za ovladavanje IKT rizicima, a to obuhvaća sljedeće [19]:

1. upravljačke kontrole
2. logičke kontrole
3. fizičke kontrole
4. sigurnosti IKT operacija
5. praćenje sigurnosti
6. provjeru, ocjenjivanje i testiranje informacijske sigurnosti
7. osposobljavanje i podizanje svijesti o informacijskoj sigurnosti.

Odluka u članku 12 određuje da je uprava kreditne institucije dužna uspostaviti funkciju voditelja informacijske sigurnosti, neovisno o funkciji voditelja organizacijske jedinice IKT-a, te postaviti njegov djelokrug, ovlasti i odgovornosti. S obzirom na to da je iz članka 12 ove Odluke jasno vidljivo da je uprava ta koja određuje djelokrug i odgovornost CISO funkcije, ova odluka upravi daje slobodu da odredi sistematizaciju radnog mjesta, stručnost i iskustvo koje adekvatan kadar treba posjedovati.

Dalje je Odlukom određena logička sigurnost prema kojoj je kreditna institucija dužna objasniti, dokumentirati, provoditi, pratiti i redovito preispitivati postupke za logičku kontrolu pristupa. Uz logičku sigurnost, određena je i fizička sigurnost, prema kojoj je kreditna institucija dužna objasniti, dokumentirati i provoditi mjere fizičke sigurnosti radi zaštite vlastitih

prostorija, podatkovnih centara i ostalih osjetljivih područja od neovlaštenog pristupa i štetnih utjecaja iz okruženja.

Praćenje sigurnosti Ovom je Odlukom propisano u članku 16, a odlukom uprave kreditne institucije može postati direktna odgovornost CSIO funkcije. Odluka nalaže da je kreditna institucija dužna uspostaviti proces i provoditi postupke za otklanjanje neuobičajenih aktivnosti koje bi mogle narušiti informacijsku sigurnost i odgovarajuće odgovoriti na te događaje. Kao dio stalnog praćenja, kreditna institucija dužna je uvesti primjerene i učinkovite mehanizme za otkrivanje fizičkih i logičkih upada te povreda povjerljivosti, cjelovitosti i dostupnosti informacijske imovine. Uz navedeno, dužna je uspostaviti i provoditi postupke za utvrđivanje i neprekidno praćenje sigurnosnih i operativnih prijetnji koje bi mogle znatno utjecati na sposobnost pružanja njezinih usluga. To podrazumijeva aktivno praćenje tehnoloških kretanja da bi bila upoznata sa sigurnosnim rizicima. Sve se navedeno odlukom uprave lako može svrstati u odgovornost potrebnih aktivnosti koje su u ingerenciji CISO funkcije [19].

Nadalje, propisana je provjera, procjenjivanje i testiranje informacijske sigurnosti, prema kojima je kreditna institucija dužna provjeravati, procjenjivati i testirati informacijsku sigurnost da bi osigurala učinkovito utvrđivanje ranjivosti u IKT sustavima i uslugama. Potrebno je uspostaviti primjereni okvir za testiranje informacijske sigurnosti, koji će uzeti u obzir prijetnje i ranjivosti utvrđene postupcima praćenja prijetnji i procjene IKT rizika [19].

Kreditna institucija je također dužna okvirom za testiranje informacijske sigurnosti osigurati da testiranja:

1. provode neovisne osobe s dovoljno znanja, vještina i stručnosti u testiranju mjera informacijske sigurnosti, koje nisu uključene u razvoj mjera informacijske sigurnosti koje se testiraju
2. uključuju ispitivanje ranjivosti i penetracijska testiranja koja su razmjerna razini rizika utvrđenog u poslovnim procesima i IKT sustavima.

Uz navedeno, kreditna institucija dužna je sustavno testirati sigurnosne mjere, što obuhvaća sljedeće [19]:

1. za sve kritične IKT sustave provoditi testiranje barem jedanput godišnje
2. za IKT sustave koji nisu kritični, razmjerno rizicima, barem jedanput svake tri godine provoditi testiranje.

U vrijeme pisanja ovog rada, tehnologija je i dalje sve dominantniji faktor u ljudskoj svakodnevici, pa tako i u primjeni u organizacijama. Geopolitičke okolnosti idu u prilog sve učestalijim i brojnijim sigurnosnim incidentima. Ova Odluka u članku 20. upravo upućuje na

navedeni izazov propisivanjem toga da je kreditna institucija dužna uspostaviti odgovarajuće postupke i organizacijske strukture radi osiguravanja dosljedne i cjelovite kontrole incidenta i problema, postupanja s njima te njihovog daljnjeg praćenja. Upravljanjem incidentima i problemima, kreditna institucija dužna je obuhvatiti sljedeće [19]:

1. postupke za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju incidenata u skladu s prvenstvom kritičnosti poslovanja
2. uloge i odgovornosti za različite scenarije incidenta (npr. pogreške, neispravan rad, kibernetički napadi)
3. postupke upravljanja problemima, što uključuje utvrđivanje, analizu i rješavanje glavnih uzroka jednog ili više incidenata, da bi se spriječilo njihovo ponavljanje
4. postupke odgovora na incidente da bi se ublažili učinci povezani s njima i da bi se osiguralo da usluga pravodobno postane operativna i sigurna
5. učinkovite interne komunikacijske planove, uključujući postupke obavješćivanja o incidentima i postupcima eskalacije
6. posebne komunikacijske planove za kritične poslovne funkcije i postupke, u svrhu suradnje s relevantnim dionicima i pružanja pravodobnih informacija vanjskim stranama.

Kreditna institucija dužna je u slučaju značajnih IKT incidentata u primjerenom roku od nastanka incidenta, o njemu, njegovim učincima i poduzetim mjerama obavijestiti Hrvatsku narodnu banku.

Sve izneseno u ovoj Odluci, uključujući članak 19, koji eksplicitno zahtijeva postojanje voditelja informacijske sigurnosti i činjenicu da odgovornosti i aktivnosti odredi uprava kreditne institucije, gotovo u svakom dijelu i članku Odluke postoje aktivnosti koje se mogu dodijeliti voditelju informacijske sigurnosti. U preostalom dijelu ove Odluke, koji nije opisan u ovom radu, a odnosi se na upravljanje IKT projektima i promjenama, upravljanje kontinuitetom poslovanja, analizu utjecaja na poslovanje i kriznu komunikaciju, CISO funkcija također ima aktivnosti i potencijalne odgovornosti.

4.3. Smjernice za primjereno upravljanje rizicima informacijskog sustava subjekta nadzora

Subjekti nadzora su sve pravne i fizičke osobe koje se bave pružanjem financijskih usluga, savjetovanjem na financijskom tržištu, prodajom, posredovanjem ili upravljanjem imovinom korisnika financijskih usluga [20].

Premda smjernice eksplicitno ne propisuju potrebu da organizacija mora imati određenu i sistematiziranu CISO funkciju; zahtjeve ove smjernice, objašnjene pojmova i postupak nadzora olakšalo bi postojanje CISO funkcije – funkcija koja bi mogla preuzeti aktivnosti i odgovornost za to da je organizacija usklađena sa smjernicama regulatornog tijela, kao što je HANFA (Hrvatska agencija za nadzor financijskih usluga).

Iz same smjernice proizlazi da HANFA želi ostvariti sljedeće ciljeve [20]:

- razvoj svijesti subjekta o rizicima informacijskog sustava, s osobitim naglaskom na rizike vezane za uporabu IT-a
- upoznavanje subjekta nadzora s dobrim praksama ublažavanja rizika informacijskog sustava.

HANFA očekuje da će razumijevanje i primjena mjera i postupaka opisanih u smjernicama doprinijeti kvaliteti upravljanja rizicima IS subjekata i tako umanjiti izloženost subjekata rizicima poslovanja u cjelini.

Smjernicama su obuhvaćeni ključni oblici upravljanja rizicima informacijskog sustava, koji se sastoje od [20]:

- osnovnih načela
- identifikacije, procjene i postupanja s rizicima informacijskog sustava
- zaštite od kibernetičkih prijetnji i rizika.

Smjernice također obuhvaćaju mjere i postupke za smanjenje rizika informacijskog sustava [20]:

- organizaciju i upravljanje
- razvoj i održavanje
- unutarnje kontrole i revizije
- upravljanje promjenama

- izdvajanje procesa
- neprekinutost poslovanja i oporavak nakon katastrofe
- fizičku i okolišnu sigurnost
- logičke kontrole pristupa
- sigurnost računalnih mreža
- sigurnost prijenosnih uređaja i medija za pohranu podataka
- podizanje razine svijesti o sigurnosti
- upravljanje incidentima
- upravljanje operativnim i sistemskim zapisima
- zaštitu od malicioznog koda.

Kao i u prethodnim legislativnim aktima, u smjernicama se dalje razrađuju načela iz CIA akronima, postupak i način upravljanja procjenom rizika informacijskog sustava.

Iz smjernica se, kao i u navedenim aktima, može pročitati da funkcioniranje informacijskog sustava organizacije znatno ovisi o podršci uprave subjekta. Uprava je odgovorna za organizaciju, strateško odlučivanje, dodjelu resursa i donošenje pravila i procedura u kontekstu upravljanja IS-a, što obuhvaća i postupke izdvojene vanjskim pružateljima usluga. Ako uprava organizacije nije primjereno uključena u upravljanje informacijskim sustavom, subjekt se može izložiti rizicima kao što je neusklađenost strategije poslovnog razvoja i razvoja informacijskog sustava, te neučinkovito trošenje sredstava za razvoj i održavanje [20].

Također se usmjerava k tome da sukladno vlastitoj procjeni rizika, uprava organizacije može dodatno primijeniti sljedeće mjere i postupke [20]:

- Formiranje odbora za upravljanje informacijskim sustavom. Uobičajena praksa je da u radu odbora za upravljanje sudjeluju odgovorne osobe poslovnih organizacijskih jedinica i sustava unutarnjih kontrola, uz članove uprave i osobe odgovorne za sigurnost i funkcionalnost. Rad odbora manifestira se putem zajedničkih sjednica, na kojima se raspravlja o ključnim pitanjima funkcionalnosti i sigurnosti informacijskog sustava. Tako se olakšava komunikacija među sudionicima, rješavaju problemi u suradnji i unaprjeđuje se usklađenost djelovanja organizacijskih jedinica zaduženih za osiguranje funkcionalnosti i sigurnosti i ostalih organizacijskih jedinica.

- Funkcije upravljanja sigurnošću u nekim situacijama mogu biti u suprotnosti s drugim zaduženjima vezanima za sigurnosne i funkcionalne ciljeve, stoga je prisutna praksa razdvajanja tih funkcija njihovom dodjelom različitim osobama.
- Razdvajanje međusobno neusklađenih dužnosti u procesu upravljanja IT-om, na primjer, sistemskog administratora od programera aplikacija do administratora baze podataka, sistemskog administratora od mrežnog administratora i drugo. Dodjelom tih funkcija različitim djelatnicima omogućava se njihova veća usredotočenost na dužnosti za koje su specijalizirani, ali se istovremeno ograničava moguća šteta koja bi mogla nastati namjernim štetnim djelovanjem nekog od zaposlenika navedenih u primjeru.
- Oformljivanje sustava unutarnjih kontrola informacijskog sustava. Unutarnje kontrole, u obliku funkcija unutarnje revizije, procjene rizika ili usklađenosti, a koje su neovisne od ostalih zaduženja vezanih za funkcionalnost ili sigurnost informacijskog sustava, mogu doprinijeti kvalitetnijem upravljanju rizicima.
- Dokumentiranje i usvajanje politika, pravila, standarda, smjernica, uputa i radnih procedura.

Ovdje bi trebalo istaknuti da se nalaže razdvajanje funkcije upravljanja sigurnošću od drugih zaduženja, što ide u prilog tome da CISO funkcija unutar ovakve organizacije treba biti neovisna i nepristrana, pod izravnim ovlaštenjem uprave organizacije. U daljnjim poglavljima opisane su smjernice kao što su razvoji i održavanje informacijskog sustava, upravljanje promjenama, neprekinutost poslovanja i oporavak nakon katastrofe, fizička i okolišna sigurnost, logičke kontrole, sigurnost računalnih mreža i upravljanje incidentima. Također su opisani zahtjevi i aktivnosti koje bi CISO funkcija mogla preuzeti i staviti pod svoju odgovornost.

4.4. Zakon o informacijskoj sigurnosti

Ovim se Zakonom (u daljnjem tekstu ovog poglavlja Zakon) utvrđuje pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, te mjerodavna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje se u svom djelokrugu koriste klasificiranim i neklasificiranim podatcima, a primjenjuje se i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima [21].

Zakon određuje informacijsku sigurnost kao stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

U članku 8 definirano je područje informacijske sigurnosti za koje se propisuju standardi informacijske sigurnosti, a to su [21]:

- sigurnosna provjera
- fizička sigurnost
- sigurnost podataka
- sigurnost informacijskog sustava
- sigurnost poslovne suradnje.

Sigurnost informacijskog sustava opisuje se kao područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava [21].

Zakon propisuje da je Ured Vijeća za nacionalnu sigurnost središnje državno tijelo za informacijsku sigurnost, koje koordinira i usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj i u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. Navedeni je Ured također nadležan za donošenje pravilnika o informacijskoj sigurnosti, koji su obvezni za javna tijela.

Dodatno je propisano da je Zavod za sigurnost informacijskih sustava središnje državno tijelo za tehnička područja sigurnosti informacijskih sustava u tijelima i pravnim osobama u većinskom vlasništvu Republike Hrvatske.

Tehnička područja su [21]:

- standardi sigurnosti informacijskog sustava
- sigurnosne akreditacije informacijskog sustava
- upravljanje kriptomaterijalima koji se primjenjuju u razmijeni klasificiranih podataka
- koordinacija prevencija i odgovor na računalne ugroze sigurnosti informacijskog sustava.

U odjeljku 5 objašnjen je nacionalni CERT, kao tijelo za zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. Propisano je da CERT i Zavod za sigurnost informacijskih sustava surađuju na sprječavanju i zaštiti od računalnih ugroza sigurnosti informacijskih sustava. Također sudjeluju u izradi preporuka i normi u Republici Hrvatskoj, iz područja sigurnosti informacijskih sustava.

U člancima 25. i 26. ovog Zakona propisan je nadzor informacijske sigurnosti te Savjetnik za informacijsku sigurnost, dakle, propisano je da poslove nadzora provode savjetnici za informacijsku sigurnost. Ured Vijeća za nacionalnu sigurnost pravilnikom propisuje kriterije za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost, a savjetnik podnosi izvještaj o rezultatima provedenog nadzora čelniku tijela ili pravne osobe i Uredu Vijeća za nacionalnu sigurnost.

CISO funkcija u ovakvom obliku organizacije od javnog je interesa te kriterije u kojima bismo CISO funkciju / voditelja informacijske sigurnosti mogli poistovjetiti s pozicijom Savjetnika za informacijsku sigurnost, donosi isključivo Ured Vijeća za nacionalnu sigurnost.

4.5. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

Iako sâm Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (u daljnjem tekstu ovog poglavlja Zakon) eksplicitno ne propisuje obvezu formiranja CISO funkcije odnosno voditelja informacijske sigurnosti, on ne isključuje potencijalnu potrebu organizacije, za koju je Zakon obvezan, da je ustroji.

Ovim se Zakonom uređuju postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, mjerodavnosti i ovlasti odgovornih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela odgovornih za sprječavanje i zaštitu od incidenata (u daljnjem tekstu: odgovorni CSIRT ili CERT) i tehničkog tijela za ocjenu sukladnosti, te nadzor nad operatorima ključnih usluga i davateljima digitalnih usluga u provedbi ovog Zakona i prekršajne odredbe [22].

Cilj Zakona je osigurati provedbu propisanih mjera sa zadatkom postizanja visoke razine kibernetičke sigurnosti. Cilj je također osigurati nesmetano davanje usluga koje su posebno važne za održavanje ključnih društvenih i gospodarskih aktivnosti. U prilogu ovog Zakona nalaze se [22]:

- popis ključnih usluga s kriterijima i prigovorima za donošenje ocjene o važnosti negativnih učinaka incidenta
- popis digitalnih usluga
- popis mjerodavnih tijela.

Zakonom je u hrvatsko zakonodavstvo preuzeta Direktiva 2016/1148 Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava diljem EU-a. Ovaj Zakon također osigurava provedbu Provedbene uredbe Komisije (EU) 2018/151 iz 2018., o utvrđivanju pravila za primjenu navedene Direktive u odnosu na dodatne specifikacije elemenata koje pružatelji digitalnih usluga moraju uzeti u obzir – naprimjer, u upravljanju rizicima kojima je izložena sigurnost njihovih mrežnih i informacijskih sustava i parametara za utvrđivanje ima li incident značajan učinak.

Zakon se primjenjuje na operatore ključnih usluga, neovisno o tome jesu li u pitanju javni ili privatni subjekti, neovisno o državi njihova sjedišta, njihovoj veličini, ustroju i vlasništvu.

Bili javni ili privatni, pojedini subjekti će se kategorizirati kao operator ključnih usluga ako [22]:

- subjekt pruža neku od ključnih usluga prikazanih u Tablici 4.1
- pružanje ključnih usluga kod tog subjekta ovisi o mrežnim i informacijskim sustavima
- bi incident imao znatan negativan učinak na pružanje ključne usluge.

Tablica 4.1 Popis ključnih usluga prema sektorskoj i podsektorskoj podjeli

Sektor	Podsektor	Ključna usluga
Energetika	Električna energija	Proizvodnja električne energije
		Prijenos električne energije
		Distribucija električne energije
	Nafta	Transport nafte naftovodima
		Proizvodnja nafte
		Proizvodnja naftnih derivata
		Skladištenje nafte i naftnih derivata
	Plin	Distribucija plina
		Transport plina
		Skladištenje plina
		Prihvat i otprema UPP-a
		Proizvodnja prirodnog plina

Prijevoz	Zračni promet	Zračni prijevoz putnika i tereta
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke
		Kontrola zračnog prometa
	Željeznički promet	Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom
		Usluge prijevoza robe i/ili putnika željeznicom
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom
	Vodni prijevoz	Nadzor kretanja brodova (VTS usluga)
		Obavljanje poslova pomorske radijske službe
		Održavanje objekata sigurnosti plovidbe
		Prijevoz putnika u međunarodnom i/ili domaćem prometu
		Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu
		Prijevoz putnika, tereta i vozila u unutarnjim morskim vodama i teritorijalnom moru Republike Hrvatske, koji se obavlja na unaprijed utvrđenim linijama prema objavljenim uvjetima reda plovidbe i cjeniku usluga
		Praćenje i lociranje plovila u unutarnjoj plovidbi
		Obavijesti brodarstvu u unutarnjoj plovidbi
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi
		Baza podataka o trupu plovila u unutarnjoj plovidbi
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi
Sektor	**Podsektor**	**Ključna usluga**
	Cestovni prijevoz	Javni prijevoz putnika
		Uporaba cestovne infrastrukture
		Upravljanje prometnim tokovima ili informiranje vozača (ITS)
Bankarstvo		Platne usluge
Infrastrukture financijskog tržišta		Usluge mjesta trgovanja
		Usluge središnjih drugih ugovornih strana (CCP)
Zdravstveni sektor		Primarna zdravstvena zaštita
		Sekundarna zdravstvena zaštita
		Tercijarna zdravstvena zaštita
		Transfuzijska medicina i transplantacija organa
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita
		Sigurnost hrane
		Zaštita od opasnih kemikalija

	Distribucija i sigurnost lijekova i medicinskih proizvoda Nadzor nad zdravstvenim stanjem stanovništva i ljudskim resursima u zdravstvu vođenjem javnozdravstvenih registara
Opskrba vodom za piće i njezina distribucija	Opskrba krajnjih korisnika
Digitalna infrastruktura	DNS usluga za .hr TLD Registar naziva domena za .hr TLD Sustav za registriranje i administriranje sekundarne domene Usluga IXP
Poslovne usluge za državna tijela	Usluge u sustavu e-Građani Poslovne usluge za korisnike državnog proračuna

Mjerodavna sektorska tijela provode postupak identifikacije operatora ključnih usluga po sektorima, prema Tablici 4.1. Taj postupak svodi se na izrađivanje popisa svih subjekata koji pružaju ključnu Zatim je propisano da je mjerodavno sektorsko tijelo dužno postupak identifikacije operatora ključnih usluga provoditi redovito, sukladno tržišnim promjenama u sektoru, a najmanje jednom u dvije godine [22].

Prema Zakonu, operatori ključnih usluga i davatelji digitalnih usluga dužni su, radi osiguranja neprekidnosti u davanju tih usluga, poduzeti određene mjere sa svrhom održavanja kibernetičke sigurnosti. Te mjere su [22]:

- tehničke i organizacijske mjere za upravljanje rizicima, uzimajući pri tome u obzir najnovija tehnička dostignuća koja se upotrebljavaju u okviru najbolje sigurnosne prakse u području kibernetičke sigurnosti
- mjera za sprječavanje i ublažavanje učinaka incidenata na sigurnost mrežnih i informacijskih sustava.

Odgovornost za primjenu mjera je na operatoru ključnih usluga i davatelju digitalnih usluga, koji su dužni provoditi mjere za postizanje visoke razine kibernetičke sigurnosti bez obzira na to upravljaju li i/ili održavaju svoje mrežne i informacijske sustave sami ili za to angažiraju vanjskog partnera.

Iz ovog dijela Zakona jasno je vidljiva situacija u kojoj vanjski partner može održavati mreže i informacijske sustave u sklopu kojih ugovorno održavanje može sadržavati sve što doprinosi poboljšavanju kibernetičke sigurnosti, a to može uključivati i uslugu vanjskog voditelja

informacijske sigurnosti, u kontekstu ovog rada vanjsku CISO funkciju (prema modelu, engl., *CISO as a service*).

Mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga i način njihove provedbe pobliže se propisuje uredbom koju donosi Vlada Republike Hrvatske [22].

Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga propisuje okvir upravljanja, načela sigurnosti, uspostavu i dokumentiranje politike upravljanja, provedbu internih nadzora, upravljanje rizicima; uključujući procjenu rizika, upravljanje eksternalizacijom, organizacijsku strukturu i dodatne elemente bitne za provedbu i uspostavu mjera kibernetičke sigurnosti [23].

Ne ulazeći u cjelokupnu analizu ove Uredbe, velik dio propisanih aktivnosti i zahtjeva mogla bi preuzeti CISO funkcija s adekvatnim kompetencijama i iskustvom.

U članku 7. ove Uredbe propisana je organizacijska struktura, prema kojoj su operatori ključnih usluga dužni odrediti osobu s najvišim rukovodnim ovlastima, odgovornu za uspostavu i upravljanje sigurnošću ključnih sustava. Nadalje, operatori ključnih usluga dužni su uspostaviti organizacijsku strukturu s formalnom raspodjelom zadaća, ovlasti i odgovornosti kojom će se osigurati primjerno upravljanje sigurnošću ključnih sustava [23].

Ovim dijelom unutar Uredbe na koju se poziva Zakon otvara se jasna potreba za uspostavljanje CISO funkcije / voditelja informacijske sigurnosti koji – da bi navedene zahtjeve ispunio i mogao preuzeti pripadajuće odgovornosti, a prvenstveno odgovornosti uspostave i upravljanja kibernetičkom sigurnošću (uvjetno rečeno, podskupom informacijske sigurnosti) – treba imati adekvatnu stručnost i iskustvo. Stručnost se stječe adekvatnom naobrazbom i radom, a iskustvo isključivo praksom i radom u području informacijske sigurnosti.

Zakonom se zatim propisuje obavješćivanje o incidentima, u sklopu čega je opisana obveza obavješćivanja. Konkretnije, operatori ključnih usluga i davatelji digitalnih usluga dužni su odgovorni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na neprekidnost usluga koje pružaju. Ako je incident na mrežnom i informacijskom sustavu davatelja digitalne usluge imao znatan učinak na pružanje neke ključne usluge, operator ključne usluge dužan je o tom incidentu obavijestiti odgovorni CSIRT [23]. Također, propisani su određeni kriteriji, o kojima možete više pročitati u članku 22. Zakona.

U vrijeme pisanja ovog rada izrazito je zanimljiv i vrlo aktualan članak 24., koji propisuje informiranje javnosti o incidentu. Konkretnije, odgovorni CSIRT može, po prethodno

provedenom savjetovanju s operatorom ključne usluge i mjerodavnim sektorskim tijelom, obavijestiti javnost o pojedinačnim incidentima koji imaju znatan učinak na neprekidnost usluge koju operator pruža, ako je osviještenost javnosti nužna za sprječavanje širenja i jačanja učinka incidenta ili za rješavanje incidenta koji je u tijeku [23].

Također, odgovorni CSIRT i prema potrebi, CSIRT-ovi drugih pogođenih država članica, mogu javnost obavijestiti o pojedinačnim incidentima koji imaju znatan učinak na neprekidnost pojedine digitalne usluge ili od davatelja digitalnih usluga zatražiti da to učini, ako je objavljivanje obavijesti o incidentu u javnome interesu, a osobito ako je to potrebno radi sprječavanja širenja i jačanja učinka incidenta ili rješavanja incidenta koji je u tijeku.

Zatim je propisan nadzor nad operatorom ključnih usluga, koji se provodi jednom u dvije godine. No, nadzor se može provesti i prije ako mjerodavno sektorsko tijelo utvrdi ili zaprimi informacije koje upozoravaju na to da operator ne izvršava svoj obveze iz ovog Zakona, dok se nadzor nad davateljem digitalnih usluga provodi isključivo nakon što mjerodavno sektorsko tijelo zaprimi informacije koje upozoravaju na to da davatelj digitalne usluge ne postupa sukladno ovom Zakonu. Sam nadzor pružatelja digitalnih usluga provodi mjerodavno sektorsko tijelo uz podršku mjerodavnog tijela za ocjenu sukladnosti i odgovornog CSIRT-a [23].

Zatim su propisane zadaće odgovornog CSIRT-a, a one glase da je CSIRT odgovoran na sektorskoj razini, prema Tablici 4.2, a obavlja sljedeće poslove [23]:

- prati incidente
- pruža rana upozorenja i najave i obavještava o rizicima i incidentima
- provodi dinamičku analizu rizika i incidenata i izrađuje pregled situacije u sektoru
- provodi redovite provjere ranjivosti mrežnih i informacijskih sustava operatora ključnih usluga, odnosno davatelja digitalnih usluga
- prima obavijesti o incidentima
- na zahtjev operatora ključnih usluga, odnosno davatelja digitalnih usluga, analizira i odgovara na incidente
- ako to dopuštaju okolnosti, nakon primitka obavijesti o incidentu operatoru ključnih usluga dostavlja važne podatke u pogledu daljnjeg postupanja po njegovoj obavijesti, a osobito podatke koji bi mogli pridonijeti djelotvornom rješavanju incidenta
- donosi smjernice za ujednačavanje i unaprjeđenje stanja provedbe obveze obavješćivanja o incidentima

- informira mjerodavno sektorsko tijelo o incidentima
- u suradnji s mjerodavnim sektorskim tijelom, određuje prekogranične utjecaje incidenata
- jedinstvenu nacionalnu kontaktnu točku obavještava o incidentima, sukladno njezinim smjernicama
- jedinstvenoj nacionalnoj kontaktnoj točki dostavlja podatke o glavnim elementima postupaka rješavanja incidenata koje provodi
- obavješćuje odgovorni CSIRT druge pogođene države članice ili više njih o incidentu na mrežnom i informacijskom sustavu operatora ključnih usluga – ako incident ima znatan učinak na neprekidnost ključnih usluga u toj državi članici
- obavješćuje nadležni CSIRT druge pogođene države članice ili više njih o incidentu na mrežnom i informacijskom sustavu pružatelja digitalnih usluga ako se incident odnosi na dvije ili više država članica
- surađuje s drugim CSIRT-ovima na nacionalnoj i međunarodnoj razini
- sudjeluje u mreži CSIRT-ova na razini Europske unije, koja je osnovana s ciljem razvoja povjerenja i pouzdanja među državama članicama te promicanja brze i učinkovite operativne suradnje
- promiče usvajanje i primjenu zajedničkih ili normiranih praksi za postupke rješavanja incidenata i rizika te planove za klasifikaciju incidenata, rizika i informacija.

Također je propisano da je operator ključnih usluga i davatelj digitalnih usluga dužan surađivati s odgovornim CSIRT-om i s njim razmjenjivati potrebne informacije.

Tablica 4.2. Popis nadležnih tijela [23]

Sektor ključnih usluga	**Mjerodavno sektorsko tijelo**	**CSIRT**	**Tehničko tijelo za ocjenu sukladnosti**
Energetika	tijelo državne uprave odgovorno za energetiku	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Prijevoz	tijelo državne uprave odgovorno za promet	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Bankarstvo	Hrvatska narodna banka	Nacionalni CERT	–
Infrastrukture financijskog tržišta	Hrvatska agencija za nadzor financijskih usluga	Nacionalni CERT	–
Zdravstveni sektor	tijelo državne uprave odgovorno za zdravstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Opskrba vodom za piće i njezina distribucija	tijelo državne uprave odgovorno za vodno gospodarstvo	Zavod za sigurnost informacijskih sustava	Zavod za sigurnost informacijskih sustava
Digitalna infrastruktura	Središnji državni ured za razvoj digitalnog društva	Nacionalni CERT	Hrvatska akademska i istraživačka mreža – CARNET

Poslovne usluge za državna tijela	Središnji državni ured za razvoj digitalnog društva	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT*	Zavod za sigurnost informacijskih sustava ili Nacionalni CERT**

Zatim je propisana zaštita podataka, prema kojoj se popisi operatora ključnih usluga, kao i svi drugi podatci koji nastaju u okviru provedbe ovog Zakona, upotrebljavaju isključivo u svrhu izvršavanja zahtjeva iz ovog Zakona. Također se nalaže da su se mjerodavna tijela pri razmjeni podataka dužna brinuti o potrebi ograničavanja pristupa podatcima, kada je to potrebno u svrhu sprječavanja, otklanjanja, provođenja istraživanja i vođenja kaznenog postupka. Na kraju, Zakon propisuje i kaznene odredbe. Više o kaznenim odredbama pročitajte u samom Zakonu. Kao što je i navedeno, ovaj Zakon ne propisuje eksplicitno ustrojenje funkcije CISO-a / voditelja informacijske sigurnosti, no, pozivajući se na Uredbu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, indirektno se propisuje organizacijska struktura u kojoj mora postojati funkcija koja će imati odgovornosti i upraviteljska prava CISO funkcija, a sam Zakon ne isključuje njegovo postojanje.

4.6. Kazneni zakon

Ovaj Zakon ne propisuje eksplicitno pojam voditelja informacijske sigurnosti, no predstavlja Zakon s kojim bi, poželjno, trebala biti upoznata svaka CISO funkcija u organizaciji koja djeluje na području Republike Hrvatske ili u jednoj od članica EU-a, jer svaki CISO neke organizacije – uz to što mora biti upoznat s internim pravilnicima, a posebno onima koji pokrivaju informacijsku sigurnost, poput Politike informacijske sigurnosti – mora biti upoznat i sa zakonima Republike Hrvatske koji utječu ili se preklapaju s aktivnostima povezanima s informacijskom sigurnošću.

Opisat ćemo direktno primjenjivi dijelovi Kaznenog zakona (u daljnjem tekstu ovog poglavlja Zakon). Zakon u članku 71. Zabrana obavljanja određene dužnosti ili djelatnosti propisuje sljedeće. Tamo gdje je propisano da sigurnosnu mjeru zabrane potpunog ili djelomičnog obavljanja određene dužnosti ili djelatnosti, sud će kaznu izreći počinitelju koji je kazneno djelo počinio u obavljanju dužnosti ili djelatnosti ako postoji opasnost da će zlouporabom te dužnosti ili djelatnosti ponovno počiniti kazneno djelo [24].

U kontekstu informacijske sigurnosti, dalje je u članku 75. propisana sigurnosna mjera zabrane pristupa internetu, koju će sud izreći počinitelju koji je kazneno djelo počinio putem interneta ako postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo [24].

Od članka 266. do članka 273. (uključujući i njega) propisane su stavke vezane za računalni kriminal koji utječe na informacijsku sigurnost.

Naprimjer, propisano je da će se onaj koji neovlašteno pristupi računalnom sustavu ili nekom njegovom dijelu ili računalnim podatcima, kazniti kaznom zatvora do dvije godine. Onaj koji kazneno djelo ovog tipa počini u odnosu na računalni sustav ili računalne podatke tijela vlasti, Ustavnog suda Republike Hrvatske ili ostalih javnih tijela, kaznit će se kaznom zatvora od tri godine. Također, zbog pokušaja ovakvog kaznenog djela, počinitelj će se kazniti i prema prijedlogu suda te je propisana mogućnost progona počinitelja. Isto vrijedi i za počinjenje aktivnosti [24]:

- ometanja rada računalnog sustava
- oštećenja računalnih podataka
- neovlaštenog zaustavljanja računalnih podataka
- računalnog krivotvorenja.

Računalna prijevara tretira se drugačije. Naprimjer, onaj koji s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, prenese, izmijeni, izbriše, prikrije, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa ili sprječava rad računalnog sustava i tako prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina [24].

U slučaju da je kaznenim djelom pribavljena znatna imovinska korist ili prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od jedne do osam godina, a podatci koji su nastali počinjenjem kaznenog djela će se uništiti [24].

Onaj koji izradi, nabavi, proda, posjeduje, distribuira ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje navedenih kaznenih djela, kaznit će se kaznom zatvora do tri godine.

Onaj tko nabavi, proda, posjeduje, distribuira ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu, a s ciljem da ih se upotrijebi za počinjenje svih navedenih kaznenih djela, kaznit će se zatvorom do dvije godine [24]. Takve će se posebne naprave i programi oduzeti, a podatci će se uništiti.

U Zakonu su također propisana teška kaznena djela protiv računalnih sustava, programa i podataka. Naprimjer, onaj koji navedena kaznena djela počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, Ustavnog suda Republike Hrvatske i međunarodne organizacije koje je Republika Hrvatska član, tijela jedinica lokalne ili područne samouprave

ili neke javne ustanove kaznit će se zatvorom od šest mjeseci do pet godina, a u slučaju da počinitelj počini napad na više računalnih sustava ili na one kojima je prouzročena šteta, kaznit će se zatvorom od jedne do osam godina [24].

4.7. Zakon o elektroničkim komunikacijama

Ovim se Zakonom (u daljnjem tekstu ovog poglavlja Zakon) uređuje područje elektroničkih komunikacija i to: pružanje elektroničkih komunikacijskih mreža i usluga, pružanje univerzalnih usluga i zaštite prava korisnika, gradnju, postavljanje, održavanje i uporabu elektroničke komunikacijske infrastrukture; povezane opreme; povezanih usluga i određenih značajki terminalne opreme, uvjete tržišnog natjecanja te prava i obveze sudionika na tržištu elektroničkih komunikacijskih mreža i usluga. Također, Zakonom je propisano djelotvorno upravljanje radiofrekvencijskim spektrom te adresnim i brojevnim prostorom; digitalni radio i televizija; zaštita podataka; sigurnost elektroničkih komunikacijskih mreža i usluga te obavljanje inspekcijskog nadzora i kontrole u elektroničkim komunikacijama. Uz to, propisan je i postupak donošenja odluka i rješavanja sporova u elektroničkim komunikacijama, kao i ustrojstvo, djelokrug i odgovornost nacionalnog regulatornog tijela za elektroničke komunikacije, poštanske usluge i željezničke usluge [25].

U kontekstu ovog rada opisan je dio zakona koji se tiče zaštite podataka, sigurnosti elektroničkih komunikacijskih mreža i usluga te obavljanje inspekcijskog nadzora. S navedenim dijelovima Zakona trebala bi biti upoznata svaka osoba koja obavlja CISO funkciju u organizaciji koja je registrirana u Republici Hrvatskoj. Kako je ovim Zakonom prenesena legislativa EU-a u legislativu Republike Hrvatske putem Direktiva, Uredba i Odluka Europskog parlamenta i Vijeća, tako je dobar dio Zakona primjenjiv i za CISO funkcije izvan Republike Hrvatske, a u nekoj od zemlja članica EU-a.

Tako je Zakonom definirano značenje pojma povreda osobnih podataka, kao povreda sigurnosti koje uzrokuju slučajno ili nezakonito uništenje, gubitke, izmjenu, neovlašteno razlikovanje ili pristup osobnim podacima koji se prenose, pohranjuju ili drugačije obrađuju u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga EU-a [25].

Hrvatska regulatorna agencija za mrežne djelatnosti (u daljnjem tekstu ovog poglavlja HAKOM) nacionalno je regulatorno tijelo za obavljanje regulatornih i drugih aktivnosti propisanih ovim Zakonom. HAKOM je u načelu neprofitna i neovisna pravna osoba s javnim

ovlastima propisanih ovim Zakonom i posebnih zakona koji se tiču poštanskih usluga i regulacija tržišta željezničkih usluga. HAKOM odgovara Hrvatskom saboru.

U kontekstu ovog rada, u članku 16. propisano je da je mjerodavnost HAKOM-a u stavki 23. – donošenje odluke u vezi s izvođenjem u zoni elektroničke komunikacije te zaštita ili premještaj elektroničke komunikacijske infrastrukture i druge opreme.

Uz to, u člancima 24. i 25. propisana je mjerodavnost osiguranja usklađenosti poslovanja operatora elektroničkih komunikacijskih mreža i/ili usluga s odredbama Zakona o sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga te zaštita podataka i inspekcijski nadzor nad primjenom ovog Zakona [25].

Zakonom je također propisana suradnja HAKOM-a s drugim tijelima, gdje se nalaže suradnja s tijelom za zaštitu osobnih podatka i tijelom odgovornim za usklađivanje sprječavanja i zaštite računalnih ugroza sigurnosti informacijskih sustava, u skladu sa zakonom kojim se uređuje informacijska sigurnost i preporukama ENISA-e. Uz to, propisana je i suradnja s tijelom odgovornim za nacionalnu sigurnost.

Od članka 41., pa do 54. propisana je zaštita podataka i sigurnost elektroničkih komunikacija. U tom dijelu Zakona propisano je da operatori javnih elektroničkih komunikacijskih mreža i usluga te mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastruktura, moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere da bi se zaštitila sigurnost njihovih mreža i usluga. Propisano je da poduzete mjere moraju garantirati sigurnost koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga. Osobito je potrebno poduzeti mjere koje uključuju i kodiranje (enkripciju), kada je to primjereno [25].

Nadalje u stavki (2) članka 41. propisuje se da su operatori obvezni odrediti odgovornu osobu za provedbu mjere tog članka. Ovim se dijelom otvara zakonska obveza sistematizacije radnog mjesta unutar operatora, na kojem bi pojedinac bio odgovoran za informacijsku sigurnost. Taj pojedinac iz organizacijske perspektive može i ne mora imati vlastiti tim stručnjaka koji osiguravaju primjenu ovim Zakonom traženih mjera, no mjere moraju biti primijenjene. Mjere su [25]:

1. osigurati da osobnim podacima mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe

2. štititi prenošene ili pohranjene osobne podatke od slučajnog ili nezakonitog uništenja, slučajnog gubitka ili izmjene te neovlaštene ili nezakonite pohrane, obrade, pristupa ili razotkrivanja
3. osigurati primjenu sigurnosne politike u odnosu na obradu osobnih podataka
4. osigurati odgovarajuću razinu kibernetičke sigurnosti, u skladu s ishodom revizije, da bi se u najvećoj mogućoj mjeri spriječili sigurnosni incidenti.

Zatim je propisano da su operatori obvezni prijaviti sigurnosni incident HAKOM-u, a on će, između ostalog, izvijestiti i ENIS i mjerodavna nacionalna regulatorna tijela drugih država članica EU-a.

Organizacijsko tijelo unutar HAKOM-a, naziva Vijeće, pravilnikom propisuje mjere za ispunjavanje obveza operatora i mjerila za sprječavanje i prijavu sigurnosnih incidenata, uzimajući u obzir sljedeće [25]:

- broj korisnika
- trajanje sigurnosnog incidenta
- zemljopisni obuhvat područja na koje sigurnosni incident utječe
- mjeru u kojoj sigurnosni incident utječe na rad mreže ili pružanje usluge
- opseg utjecaja na gospodarstvo i društveno djelovanje.

HAKOM u svrhu provedbe opisanog članka 41. ima ovlasti zatražiti i dobiti pomoć nacionalnog tijela odgovornog za sprječavanje i zaštitu od računalno-sigurnosnog incidenta (CERT), te nacionalnog tijela odgovornog za upravljanje kibernetičkim krizama.

Nadalje, propisana je i situacija u kojoj dolazi do povrede osobnih podataka, a ako do nje dođe, operator je obvezan bez odgode obavijestiti tijelo odgovorno za zaštitu osobnih podataka, konkretnije Agenciju za zaštitu osobnih podataka (AZOP). U Zakonu je također određeno da HAKOM i AZOP mogu, u skladu sa svojim ovlastima, po službenoj dužnosti ili na zahtjev zainteresirane strane odlukom narediti prestanak povreda članaka 41. do 50. ovog Zakona, odnosno upravo onih članaka koji se tiču informacijske sigurnosti.

4.8. Zakon o provedbi opće uredbe o zaštiti podataka

Ovim Zakonom o provedbi opće uredbe o zaštiti podataka (u daljnjem tekstu ovog poglavlja Zakon) osigurava se provedba Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom

kretanju takvih podataka. Uz to, stavlja izvan snage Direktivu 95/46/EZ (Opća uredba o zaštiti podataka) [26].

Ovaj se Zakon ne odnosi na obradu osobnih podataka koju obavljaju mjerodavna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovog sprečavanja; kao ni na područje nacionalne sigurnosti i obrane [26].

Neovisno o tome što veće i ozbiljnije organizacije u svojoj strukturi imaju pravne odjele u kojima rade pravni stručnjaci sa specijalizacijom u navedenom području, ovaj Zakon pokriva teme i dio odgovornosti CISO funkcije [26]. U Zakonu je također propisano da je nadzorno tijelo Opće uredbe o zaštiti podataka Agencija za zaštitu osobnih podataka (u daljnjem tekstu AZOP). AZOP je neovisno državno tijelo, koje za svoj rad odgovara isključivo Hrvatskom saboru. Obavlja sljedeće poslove [26]:

- kada je to propisano posebnim zakonom, može pokrenuti i ima pravo sudjelovati u kaznenim, prekršajnim, upravnim i drugim sudskim i izvansudskim postupcima zbog povrede Opće uredbe o zaštiti podataka i ovoga Zakona
- donosi kriterije za određivanje visine naknade administrativnih troškova
- objavljuje pojedinačne odluke
- pokreće i vodi odgovarajuće postupke protiv odgovornih osoba zbog povrede Opće uredbe o zaštiti podataka
- obavlja poslove neovisnog nadzornog tijela za praćenje primjene EU direktive
- obavlja druge Zakonom propisane poslove, uključujući nadzor nad provedbom ovog Zakona.

Kako ovaj Zakon propisuje i poziva se na Uredbu, u njoj su propisani svi detalji. U kontekstu ovog rada, CISO funkcija treba biti svjesna obveza koje proizlaze iz sigurnosti osobnih podataka. Tako, naprimjer, sukladno članku 37. Opće uredbe o zaštiti podataka, voditelj obrade i izvršitelj obrade imenuju službenika za zaštitu podataka (DPO, engl. *Data protection officer*) u svakom slučaju u kojem:

- obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske mjerodavnosti

- se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od postupaka obrade, koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri
- se osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka.

CISO funkcija u organizaciji treba u svojoj domeni odgovornosti imati i aktivnosti za koje je odgovoran i koje izvršava DPO.

5. Opis aktivnosti i odgovornosti voditelja informacijske sigurnosti

U ovom dijelu rada dan je pregled studija slučaja na primjeru više različitih angažmana voditelja informacijske sigurnosti u organizacijama na području Republike Hrvatske, koje pripadaju različitim sektorima privrede. Studije slučaja su primjeri i opisi aktivnosti i odgovornosti unazad pet godina od trenutka pisanja ovog rada. Vrijeme i aktualnost primjera bitan je parametar za prikazivanje optimalnog pregleda, jer su tehnologija, informacije i informacijska sigurnost dinamični i vrlo promjenjivi. Razvoj nove tehnologije stalan je postupak, koji legislativu, a onda i regulaciju, stavlja u poziciju u kojoj neprestano kasni, ali se i stalno mijena i prilagođava novonastalom stupnju razvoja. Upravo ovako opisana uzajamno-posljedična dinamika čini aktivnosti i odgovornosti voditelja informacijske sigurnosti dinamičnima.

5.1. Voditelj informacijske sigurnosti u tehnološkim kompanijama u Republici Hrvatskoj

Postoje brojni čimbenici koji bi se mogli navesti, a idu u prilog tome zašto su tehnološke kompanije u svojoj organizacijskoj strukturi ustrojile funkciju voditelja informacijske sigurnosti. Dva dominantna čimbenika su:

1. rastući trend broja, kompleksnosti i potencijalne štete napada na informacijski sustav
2. regulacija, kao odgovor na trendove i liberalizaciju određenih sektora poput platnog prometa.

PSD direktiva i posebno njezina revidirana verzija, PSD2 – donijele su nove mogućnosti, koje su tehnološke kompanije koje se bave razvojem softvera vidjele kao priliku za razvoj aplikacija za uvid u financijsko stanje ili za plaćanje.

5.1.1. Revidirana Direktiva o platnim uslugama

Revidirana Direktiva o platnim uslugama (PSD2, engl *Payment Services Directive*) temelji se na podacima i tehnologiji, a njezin je cilj povećati tržišno natjecanje, inovacije i

transparentnost na cijelom europskom tržištu plaćanja, uz istodobno unaprjeđenje sigurnosti internetskog plaćanja i pristupa računu.

Između ostalog, u Direktivi su propisana pravila o novim uslugama koje pružaju treći pružatelji platnih usluga (TTP, engl. *Third Party Payment Service Provider*) u ime korisnika platnih usluga (PSU, engl. *Payment Service User*).

Usluge su sljedeće [27]:

- usluga iniciranja plaćanja (PIS, engl. *Payment Initiation Service Provider*), koju pruža TPP, pružatelj usluge iniciranja plaćanja (PISP, engl. *Payment Initiation Service Provider,*), kako je propisano člankom 66.
- usluga informiranja o računu (AIS, engl. *Account Information Service*), koju pruža TPP, pružatelj usluga informiranja o računu (AISP, engl. *Account Information Service Provider*), kako je propisano člankom 67.
- usluga potvrde raspoloživosti sredstava (CFS, engl. *Confirmation on the Availability of Funds Service*), koju pruža TPP, pružatelj usluge izdavanja platnog instrumenta (PISP, engl. *Payment Initiation Service Provider*), kako je propisano člankom 65.

Da bi se navedene usluge mogle provesti, uz suglasnost korisnika platnih usluga (PSU), treći pružatelj platnih usluga (TPP) treba imati pristup računu PSU-a. Račun najčešće vodi drugi pružatelj platnih usluga (PSP), odnosno pružatelj platnih usluga koji vodi račun (ASPSP, engl. *Payment Initiation Service Provider*). U Republici Hrvatskoj to su još uvijek najčešće banke. Da bi podržao TTP u pristupu računima koje vodi ASPSP (u Hrvatskoj najčešće banka), svaki ASPSP mora osigurati XS2A sučelje[5] (XS2A, engl. *Access to Account*) za pristup računu. Ukratko, XS2A sučelje omogućuje otvaranje tržišta i inovacija u financijskom sektoru,

[5] XS2A sučelje je tehnološki standard koji omogućuje trećim stranama, poput *fintech* poduzeća ili drugih financijskih institucija, da pristupe podacima o računu korisnika iz banke ili drugih pružatelja financijskih usluga. Sučelje XS2A korisnicima omogućuje da daju pristanak trećim stranama za pristup njihovim financijskim podacima i izvršavanje transakcija s njihovih računa. Ovo pruža mogućnost otvaranja novih usluga, poput agregacije računa (prikaz svih računa na jednom mjestu), upravljanja financijama, inovativnih mobilnih plaćanja i drugih financijskih usluga. Putem XS2A sučelja, treće strane mogu pristupiti podatcima o stanju računa, transakcijskoj povijesti i drugim financijskim podatcima korisnika. Važno je napomenuti da korisnik mora izričito dati pristanak za pristup i dijeljenje tih podataka.

pružajući korisnicima veću kontrolu nad svojim financijskim podacima i omogućujući im pristup novim i naprednim financijskim uslugama.

Pitanja u vezi odgovornosti i prava TPP-a i ASPS-a koja se odnose na interakcije putem XS2A sučelja, određene su i uređene samom PSD2 uredbom. Detaljni zahtjevi za provedbu i rad XS2A sučelja određeni su tehničkim regulatornim standardom Europskog nadzornog tijela za bankarstvo EBA-RTS[6].

Ključni ciljevi Direktive [28]:

- doprinos integriranjem i učinkovitijem europskom tržištu plaćanja
- poboljšanje jednakih uvjeta tržišnog natjecanja za pružatelje platnih usluga (uključujući nove sudionike na tržištu)
- povećanje sigurnosti i zaštite plaćanja
- zaštita potrošača
- poticanje nižih cijena za plaćanje.

S druge strane, uspostavljena je osnova regulatornih zahtjeva, koju čine sljedeći dokumenti [28]:

- PSD2 – Direktiva (EU) 2015/2366
- regulatorni tehnički standardi za pouzdanu autentifikaciju klijenata (SCA) i zajedničke i sigurne otvorene standarde komunikacije (CSC)
- lokalni zakoni kojima se direktiva prenosi u zakonodavstvo: „Zakon o platnom prometu" (ZPP), objavljen u Narodnim novinama br. 66/2018 od 20. srpnja 2018.

Iako PSD2 i EBA-RTS regulative ne nalažu izričito postojanje i ustrojenje funkcije Voditelja informacijske sigurnosti u organizaciji, cilj im je promicanje visokih standarda sigurnosti u kontekstu pružanja platnih usluga, a financijske institucije i pružatelji usluga plaćanja koji posluju u skladu s Direktivom PSD2 obvezni su osigurati adekvatne sigurnosne mjere za zaštitu podataka korisnika i prevenciju zloupotrebe.

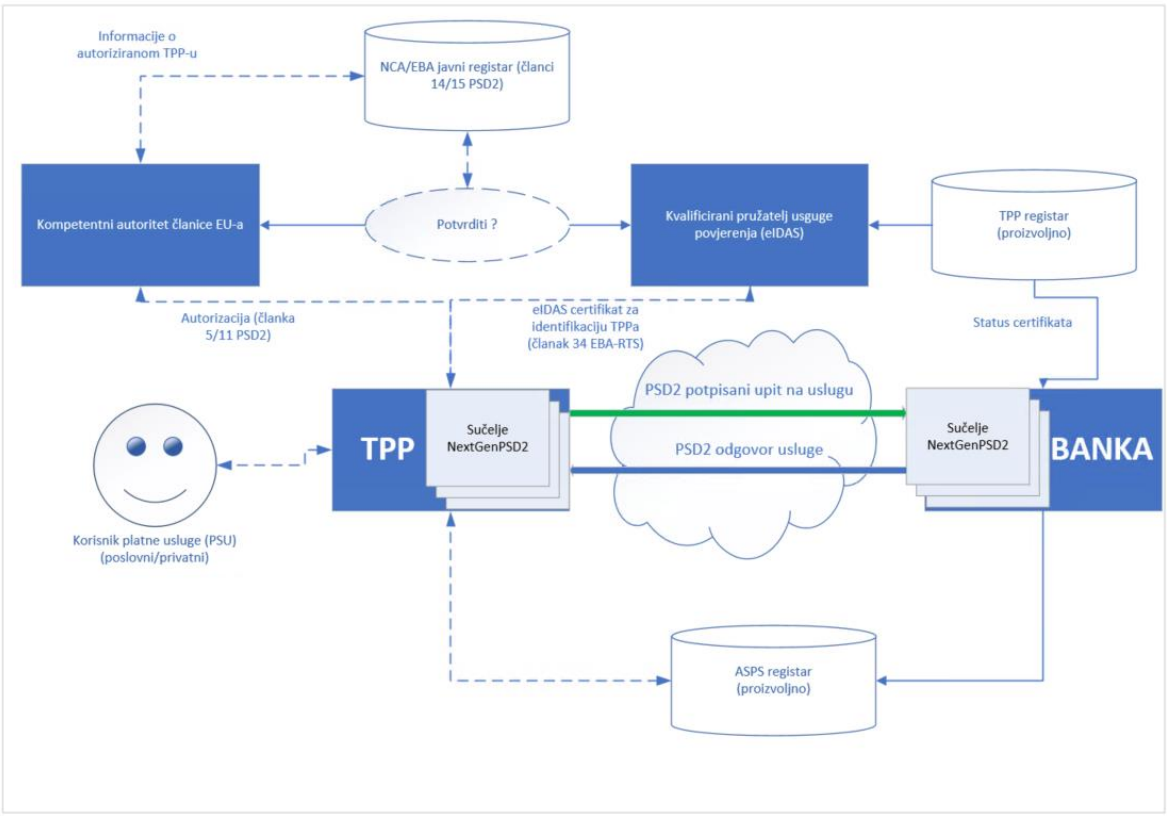
[6] EBA-RTS (engl. *European Banking Authority Regulatory Technical Standards*) tehnički su standardi koje je razvila Europska bankarska agencija (EBA) u skladu s Direktivom o platnim uslugama PSD2. Oni postavljaju pravila i standarde za sigurnost i interoperabilnost u vezi s pristupom računu i izvršavanjem elektroničkih plaćanja, osiguravaju zaštitu korisničkih podataka i usklađenost s propisima Direktive PSD2.

5.1.2. Inicijativa NextGenPSD2 Berlinske skupine

NextGenPSD2 inicijativa posebna je radna skupina unutar Berlinske skupine[7], s ciljem stvaranja zajedničkog, otvorenog i usklađenog europskog standarda za sučelje namjenskih programa (API, *engl*. *Application Programming Interface*) kojima se trećim pružateljima usluga (TPP-ovi) omogućuje pristup bankovnim računima u skladu s Direktivom PSD2. U određenom obliku jedinstvenog partnerstva, sudionici u inicijativi NextGenPSD2 zajedno rade na ostvarivanju vizije otvorenih i usklađenih standrada PSD2 i XS2A sučelja za postupke, podatke i infrastrukture nužne sastavnice otvorenog i interoperabilnog tržišta. Stvarna interoperabilnost ključna je komponenta konkurentnih paneuropskih PSD2 XS2A usluga, kojom će se pridonijeti daljnjem napretku prema jedinstvenom EU tržištu. Uz to, želi se ostvariti korist cijele industrije platnih usluga s naglaskom na europske potrošače i poduzeća [28].

Dok je usklađeno XS2A sučelje nužno za omogućavanje razvoja XS2A usluga u njihovom obujmu i za relativno niske troškove, cjeloviti PSD2 XS2A ekosustav obuhvaća i ostala tehnička, funkcionalna, operativna i upravljačka područja s (ponekad izbornim) komplementarnim uslugama, kako je prikazano na slici (Sl. 5.1).

[7] Berlinska skupina je europska inicijativa koja okuplja financijske institucije, pružatelje platnih usluga i tehnološke kompanije, s ciljem razvoja i promocije standarda i tehničkih rješenja za otvorene bankarske usluge. Berlinska skupina osnovana je 2002. godine, s prvobitnim usmjerenjem na razvoj standarda za SEPA-u (Jedinstveno euro platno područje). Međutim, ulaskom u snagu Direktive o platnim uslugama PSD2 (*Payment Services Directive 2*) u Europu, Berlinska se skupina također angažirala u razvoju tehničkih standarda za pristup računu (XS2A) i izvršavanje elektroničkih plaćanja.



Sl. 5.1 PSD2 i XS2A okruženje

Ključne karakteristike i komponente su [28]:

- moderni „RESTful" API set koji upotrebljava HTTP/1.1 uz TLS 1.2 (ili viši) kao protokol za prijenos podataka
- integriranje povratnih informacija iz javnog savjetovanja u prvoj verziji nacrta
- identifikacija TPP-a putem ETSI viii – definiranih eIDAS certifikata; QWACS je obvezan (jednostavna mjera zaštite od, naprimjer, DDOS napada), a QSEALS izboran za banke (TPP prati upute banke)
- podržava sve PSD2-om zahtijevane slučajeve pružanja usluga iniciranja plaćanja, usluga informiranja o računu i usluga potvrde raspoloživosti sredstava, dok su buduća, višestruka/skupna i povremena plaćanja izborna (ovisno o podršci u okviru *online* bankarstva ili nacionalnog zakonodavstva)
- potpuna viševalutna podrška računa
- četiri modela arhitekture za pouzdanu autentifikaciju klijenta (SCA); preusmjeravanje, OAuth2, odvojeno i „ugrađeno", s utjecajem TPP-a na prednost preusmjeravanja

- višerazinski SCA pristup za poduzeća, npr. podupiranje načela dvostruke provjere („u četiri oka“)
- podržava račune za namirenje kartičnih transakcija
- upotrebljava „košarice“ za potpisivanje, kao instrument za potpisivanje grupiranih transakcija (umjesto funkcija višestrukog plaćanja)
- transparentna struktura resursa (omogućava TPP-ovima pregled čak i u složenim poslovnim postupcima)
- posebna suglasnost za API, čime se obrada suglasnosti odvaja od pristupa računu, pri čemu se poštuju zahtjevi PSD2-a i GDPR-a
- izborna podrška tijekom sesije (skupa uzastopno izvršenih transakcija), podložno odgovarajućoj suglasnosti klijenta
- podatkovne strukture, ovisno o zahtjevima maloprodaje
- JSON s podatkovnim modelom koji se temelji na ISO-u 20022 ili
- XML s pain.001 za PISP-ove i camt.05x za AISP-ove
- integrirani formalni i transparentan postupak upravljanja promjenama i izrade verzija
- mogućnost dodatnih proširenja koja omogućavaju izgradnju („non-core“ PSD2) usluga s dodanom vrijednošću.

5.1.3. Organizacijska struktura i aktivnosti te odgovornosti voditelja informacijske sigurnosti

Zahtjeve za usklađenošću s PSD2 Direktivom u Republici Hrvatskoj i *Registar pružatelja platnih usluga i izdavatelja elektroničkog novca*, prati i vodi Hrvatska narodna banka putem Zakona o platnom prometu, u koji je integrirana PSD2 direktiva. HNB prati usklađenost i nadzire informacijsku sigurnost. Jednom zavedeni poslovni subjekti koji su u registru pružatelja platnih usluga, obvezni su se uskladiti s Direktivom i izvještavati HNB na zahtjev. Obvezni su provoditi procjenu rizika među kojima je i procjena rizika vezana za IKT (informacijsko-komunikacijsku tehnologiju) te su obvezni provesti reviziju informacijsko-komunikacijske tehnologije jednom godišnje.

U registru pružatelja platnih usluga i izdavanja elektroničkog novca, prvi su se put našli poslovni subjekti koji su klasificirani u tehnološki sektor i čija je primarna djelatnost razvoj softverskog rješenja. Zbog specijalizacije i orijentacije na primarne aktivnosti kao što je razvoj softvera, neke od takvih organizacija uspostavile su funkciju voditelja informacijske sigurnosti

između internih djelatnika, a neke od njih pronašle su rješenje u uporabi usluge vanjskog voditelja informacijske sigurnosti. U ovakvoj situaciji pojavila se usluga vanjskog voditelja informacijske sigurnosti FaaS (eng. *Functions as a Service*). Navedeno je i formalno moguće uz dubinsku procjenu rizika treće strane (pružatelja usluge vanjskog CISO-a) nakon što je pošalje i odobri HNB.

Većina aktivnosti koju tako ugovoreni voditelj informacijske sigurnosti provodi, ovisi o modelu na koji se tehnološko poduzeće odlučilo. Ako je to interni djelatnik, on je vrlo često primarno zadužen za neke druge aktivnosti razvoja softvera, sistemskog i mrežnog održavanja, a ponekad i financija, te su mu aktivnosti vezane za informacijsku sigurnost samo dodatna odgovornost i posao.

Kod modela eksternalizacije funkcije voditelja informacijske sigurnosti (FaaS model) moguće je dobiti određenog pojedinca s višom razinom kompetencija negoli ga posjeduje postojeći interni kadar. CISO, kao usluga i pojedinac koji je izvršava može imati timove i odjele unutar organizacije gdje je zaposlen, koji su specijalizirani u određenim segmentima informacijske sigurnosti. Tako može ponuditi dodatnu vrijednost na svoju uslugu, a organizacija koja se odluči na takav model može u tome vidjeti dodatnu vrijednost.

Aktivnosti koje takav voditelj informacijske sigurnosti provodi najčešće su: procjena IKT rizika, korespondencija s regulatorom, revizije informacijskog sustava, rješavanje sigurnosnog incidenta, izvještavanje uprave i regulatora, održavanje ISMS (ISO 27001) dokumentacije te podrška i koordinacija procesa certifikacije i recertifikacije informacijske sigurnosti. Uz navedeno, svaki standard informacijske sigurnosti ima svoj zahtjev, a ispunjavanje tih zahtjeva i usklađivanje sa standardom, odgovornost je voditelja informacijske sigurnosti.

5.1.4. Aktivnosti i odgovornosti voditelja informacijske sigurnosti u tehnološkoj kompaniji InfoSoft d.o.o.

Autor ovog rada je eksternalizirani voditelj informacijske sigurnosti (u nastavku ovog poglavlja Voditelj) u tehnološkoj kompaniji koja se bavi razvojem aplikacija. Liberalizacija određenih tržišnih niša kao što je naprimjer platni promet, potaknut PSD i PSD2 direktivama, otvorila je mogućnost InfoSoftu da razvije financijsku aplikaciju SmartFIN. Cilj aplikacije je korisnicima, koji su fizičke osobe i rezidenti neke od članica EU-a, ponuditi naprednu analitiku i projekciju njihove platežne sposobnosti. SmartFIN na temelju podataka o platnim transakcijama i trenutno raspoloživom saldu korisnikovih bankovnih računa, koristeći se strojnim učenjem i naprednim algoritmima, nudi projekciju platne sposobnosti korisnika. Točnost i korisnost aplikacije ovisi o količini i kvaliteti podataka koji su dostupni prediktivnim algoritmima. Prediktivni modeli se, uvjetno rečeno, treniraju na podacima koji su im dostupni u bazi. Što je više stvarnih podataka na kojima se modeli treniraju, to su projekcije točnije.

SmartFIN se instalira na mobilni uređaj korisnika, a uz njegovo formalno odobrenje, koristi se namjenskim API-jem kojim se povezuje na bankovno sučelje ili više njih, gdje korisnik aplikacije ima otvorene račune. Navedeno je omogućila PSD2 direktiva, prema kojoj se trećim stranama, u ovom kontekstu InfoSoftu, dozvoljava nuđenje usluge informiranja o računu, tzv. AISP-u. Da bi usluga bila moguća i da bi se komercijalno mogla ponuditi tržištu, potrebno je formalno odobrenje regulatora platnog prometa zemlje članice EU-a u kojoj je registrirana djelatnost InfoSofta. Za InfoSoft, to je Hrvatska narodna banka. Hrvatska narodna banka izdaje rješenje o upisu u registar pružatelja platnih usluga i izdavatelja elektroničkog novca, ako na osnovi zahtjeva i dostavljene dokumentacije ocijeni da su ispunjeni svi uvjeti propisani Zakonom o platnom prometu.

InfoSoft d. o. o. dobio je rješenje kojim se odobrava upis u registar pružatelja AISP usluge. Za InfoSoft je navedeno rješenje otvorilo potrebu za podizanjem razine informacijske sigurnosti u cijeloj organizaciji, a to je jedan od glavnih zadataka i odgovornosti voditelja informacijske sigurnosti. Organizacijska struktura u kojoj je djelatnik InfoSofta, do HNB-ovog odobrenja, uz svoju primarnu funkciju voditelja sistemske podrške obnašao i funkciju voditelja informacijske sigurnosti, postala je neodgovarajuće rješenje. Stvorili su se uvjeti i regulatorni zahtjevi za formiranjem dedicirane funkcije voditelja informacijske sigurnosti.

Jedan od prvih zadataka voditelja nakon dobivanja AISP odobrenja, bio je provesti tzv. *gap* analizu, odnosno analizu usklađenosti InfoSofta s tada novim i promijenjenim smjernicama: *Smjernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima* (u daljnjem tekstu ovog odlomka Smjernice). Voditelj je proveo *gap* analizu, u kojoj je ustanovio da su smjernice pisane tako da se usmjere veliki financijski sustavi koji nude uslugu platnog prometa, a to su u Republici Hrvatskoj većinom banke. Neovisno o tome za koga je smjernica indirektno pisana, donesen je zaključak. Smjernice se velikim dijelom oslanjaju na kontrole iz ISO 27002:2013 standarda. Uspostavom i implementacijom svih obveznih kontrola iz ISO-a 27002 i certifikacijom u odnosu na ISO 27001 standard, riješila bi se sva neusklađenosti InfoSofta u odnosu na smjernice. Voditelj je navedeni zaključak naglasio u *gap* analizi te je isti prezentirao upravi InfoSofta. Uprava je formalno donijela odluku o pokretanju certifikacije u odnosu na ISO 27001:2013 standard. Za voditelja projekta izabran je Voditelj informacijske sigurnosti. Navedeno je rezultiralo mijenjanjem Politike informacijske sigurnosti, u kojoj se proširio opseg primjenjivosti na sva povezana poduzeća u kojima InfoSoft ima većinski vlasnički udio. Voditelj informacijske sigurnosti je Politiku informacijske sigurnosti unaprijedio tako da se kroz nju pozvalo na određene pravilnike i procedure koje je tek trebalo napisati i koje je u konačnici, trebala usvojiti uprava.

Projekt certifikacije po osnovi ISO 27001 standarda, kojim bi se osigurala usklađenost s navedenim smjernicama, voditelj je podijelio u četiri osnovne faze, a to su:

- Faza 1 – stvaranje i usvajanje dokumentacije vezane za informacijsku sigurnost
- Faza 2 – implementiranje onog što je propisano dokumentacijom
- Faza 3 – interna revizija svega proizišlog iz prethodnih dviju faza
- Faza 4 – pismo uprave s naglašenim bitnim rezultatima svih prethodnih faza.

U prvoj je fazi voditelj informacijske sigurnosti stvorio, a uprava usvojila sljedeće dokumente:

- Pravilnik o upravljanju pristupnim pravima
- Pravilnik o upravljanju fizičkom sigurnošću
- Pravilnik o upravljanju enkripcijom
- Pravilnik o upravljanju resursima informacijskog sustava
- Pravilnik o upravljanju lozinkama
- Pravilnik o procjeni učinkovitosti sigurnosnih kontrola

- Pravilnik o ulogama i odgovornostima za informacijsku sigurnost
- Pravilnik o eksternalizaciji
- Pravilnik o upravljanju promjenama informacijskog sustava
- Pravilnik o upravljanju ranjivostima
- Pravilnik o upravljanju incidentima
- Pravilnik o upravljanju pričuvnom pohranom
- Pravilnik o upravljanju operativnim i sistemskim zapisima
- Pravilnik o praćenju usklađenosti
- Pravilnik o klasifikaciji informacija
- Pravilnik o upravljanju promjenama informacijskog sustava
- Pravilnik o primjerenom korištenju informacijskog sustava
- Plan kontinuiteta poslovanja
- Politiku upravljanja kontinuitetom poslovanja
- Proceduru procjene rizika i prilika
- Proceduru o upravljanju ljudskim resursima.

U ovoj je fazi, za voditelja glavni izazov bio prenijeti važnost razumijevanja i usvajanja politika, pravilnika, procedura i planova članovima uprave. U InfoSoftu uprava se sastoji od triju članova, od kojih je jedan član izvršni direktor, jedan tehnički direktor i jedan direktor financija. Neovisno o donesenoj odluci uprave za podizanjem razine informacijske sigurnosti, putem certifikacije i time usklađivanjem sa smjernicama, nedostajalo je razumijevanja i svjesnosti o njezinom značenju. Nedostajalo je razumijevanja, što za kompaniju znači usklađivanja i u konačnici, uspostave sustava upravljanja informacijskom sigurnošću. U ovoj fazi voditelj informacijske sigurnosti trebao je naći način za to kako se postaviti i kako jasno i nedvosmisleno komunicirati s upravom s ciljem stvaranja razumijevanja. Formalni dopis HNB-a kojim je istaknuta potreba za dostavom određene dokumentacije kao što je Politika informacijske sigurnosti, rezultati provedene interne revizije i u konačnici, procjena IKT rizika te stručan i iskusan voditelj informacijske sigurnosti – polako su stvorili svijest kod izvršnog direktora, za usvajanjem i implementacijom opisanih dokumenta.

Nakon usvojene dokumentacije, voditelj informacijske sigurnosti pokrenuo je izradu potpunog i sveobuhvatnog registra informacijsko-komunikacijske imovine, među kojom su i podaci u vlasništvu kompanije. Točan i sveobuhvatan registar imovine bio je glavni preduvjet za smislenu procjenu IKT rizika. Da bi registar bi potpun, prolazilo se po iteracijama stvaranja

i nadopunjavanja, kao i kontrole samog registra. Te su se iteracije svodile na to da je voditelj informacijske sigurnosti tijekom dvosatnih radionica s vlasnicima poslovnih procesa koji su koristili određenu IKT imovinu, prolazio njihove poslovne procese i nastojao ih što je moguće bolje povezati na korištenu IKT imovinu. Nakon povezivanja poslovnog procesa i IKT imovine, djelatnicima InfoSofta dodijeljeno je vlasništvo i odgovornost nad procesom i imovinom. Nakon toga, imovna je podijeljena u logičke grupe.

Putem iteracija, Voditelj je odredio prijetnju i ranjivost za svaku grupu imovine te je izračunao kvantitativni pokazatelj kritičnosti. Uz navedeno, za svaku je grupu naveo postojeće i planirane mjere kontrole.

Nakon ove faze procjene rizika, u sam je projekt unio određeni kaos detektirani i uspješno riješen sigurnosni incident, koji se nalazio unutar perimetra sistemske infrastrukture InfoSofta. Ovo je na neki način bio prijelomni trenutak, u kojem su i preostala dva člana uprave informacijsku sigurnost pribrojili u prioritetne ciljeve kompanije. Da se djelovalo brže i preventivno, do sigurnosnog incidenta ne bi ni došlo. Postojanje određenih sigurnosnih kontrola i voditelja informacijske sigurnosti rezultiralo je time da je uzrok i razlog incidenta detektiran, izoliran i u konačnici otklonjen.

Od već nabrojanih dokumenata, tri su dobila na posebnom značaju te su se pokazali korisnima i potrebnim. To su bili: Pravilnik o upravljanju ranjivostima, Pravilnik o upravljanju incidentima i nešto manje, Pravilnik o upravljanju pričuvnom pohranom.

U Pravilniku o upravljanju incidentima je između ostalog određena i faza pripreme, kojom su obuhvaćene aktivnosti:

- uspostave i redovnog ažuriranja internih akata za upravljanje incidentima
- uspostave i redovnog ažuriranja kataloga imovine unutar kojeg su definirani Vlasnici pojedinih sustava i njihova kritičnost
- uspostave funkcionalnog sustava upravljanja pričuvnim kopijama prema poslovnim potrebama InfoSofta
- instalacije, konfiguracije i redovitog održavanja sustava i alata koji se rabe u svrhu identifikacija i odgovora na incidente.

Analiza logova uspostavljenog SIEM rješenja upozorila je na postojanje sigurnosnog incidenta, čije je rješavanje preuzeo Voditelj. U Pravilniku je člankom propisana faza identifikacije, u

kojoj stoji da je za identifikaciju sigurnosnog incidenta potrebno pažljivo pratiti sljedeće kriterije:

- neuobičajene procese koji se izvode na pojedinim sustavima
- neuobičajene datoteke ili *Registry Key* vrijednosti
- indikatore prisustva aktivnog malicioznog softvera
- velike količine kriptiranog mrežnog prometa koji izlazi iz mreže InfoSofta prema sumnjivim odredištima
- nove (nepoznate) korisničke račune
- neuobičajen izlazni mrežni promet
- anomalije u aktivnostima privilegiranih korisničkih računa
- geografske neuobičajenosti
- sumnjive pokušaje prijave u sustav
- anomalije DNS prometa.

Voditelj je putem dnevnog automatskog izvještaja iz SIEM rješenja u kojem je postavljeno automatsko pravilo (engl. *rule*) koje kombinira varijablu neuobičajenog procesa na pojedinom poslužitelju, nedvojbeno identificirao anomaliju DNS prometa i geografsku neuobičajenost te instaliranu nedozvoljenu aplikaciju, točnije tzv. *crypto miner*. U samom pravilniku propisana je faza uklanjanja i oporavka te izvještavanja. Voditelj je uz pomoć administratora tog poslužitelja uklonio i oporavio sve tehničke i poslovne procese te napisao i prikazao izvještaj o sigurnosnom incidentu upravi. S jedne strane, opasna i neugodna situacija za InfoSoft rezultirala je naučenom lekcijom i jasnim stavom cijele uprave o važnosti informacijske sigurnosti. Od tog trenutka nadalje, Faza 1 i Faza 2 opisanog projekta za Voditelja započele su brže, jasnije i konkretnije. Otpora zaposlenika na operativnim razinama i srednjeg menadžmenta, gotovo da nije bilo. Pri kraju Faze 2 voditelj je stvorio sljedeće dokumente:

- Katalog rizika
- Katalog trećih strana
- Katalog rizika i prilika
- ISMS Opseg
- Izvješće analize utjecaja na poslovanje
- Izvješće procjene rizika
- Izvješće procjene učinkovitosti sigurnosnih kontrola.

Zadnja tri dokumenta svodila su se na izvještaje u kojima je voditelj upravi predstavio procjenu rizika i izvještaj o procjeni učinkovitosti sigurnosnih kontrola, čime je završena Faza 3 opisanog projekta.

U zadnjoj fazi prije same certifikacije voditelj je stvorio dokument u kojem je sažeo sve ono bitno za cjelokupni proces i informacijsku sigurnost InfoSofta. Dokument koji je formalno nazvan Upravljanje informacijskom sigurnošću – ocjena uprave, u sebi sadrži rezultate interne revizije, nesukladnosti u odnosu na zahtjeve norme, nalaze, rizike i preporuke, povratne informacije od zainteresiranih strana, prijedloge i poboljšanje učinkovitosti ISMS sustava, status i ispunjavanje ISMS ciljeva, rezultate mjerenja učinkovitosti sigurnosnih kontrola i prijedloge za unaprjeđenje ISMS-a. U Tablici 5.1 prikazane su sve uspostavljene sigurnosne kontrole koje je voditelj podijelio na organizacijske i tehničke, a u Tablici 5.2 prikazani su ciljevi sustava upravljanja informacijskom sigurnošću.

Tablica 5.1 Organizacijske sigurnosne kontrole

#	Kontrola	Razina povezanog rizika
ORGANIZACIJSKE SIGURNOSNE KONTROLE		
KO-01	ISMS dokumentacija - izrada i dopuna internih akata (politike, pravilnici, procedure, katalozi) na način adresiranja regulatornih zahtjeva (ISO 27001 norma, HNB/EBA smjernice, GDPR)	VISOKA
KO-02	Edukacija ključnih zaposlenika o informacijskoj sigurnosti – formalna edukacija za ISO 27001 internog auditora	VISOKA
KO-03	LMS - nabava i implementacija sustava za edukaciju i podizanje svijesti zaposlenika o informacijskoj sigurnosti	VISOKA
KO-04	Revizija dodijeljenih pristupnih prava – na svim sustavima	SREDNJA
KO-05	Prilagodba korisničkih grupa	SREDNJA
KO-06	Ažurno evidentiranje promjena u aplikaciji	SREDNJA
KO-07	Automatizirana provedba testiranja aplikacija nakon promjena	SREDNJA
KO-08	Razmjena znanja	SREDNJA
KO-09	Rotacija dužnosti unutar organizacije	SREDNJA
KO-10	Unaprjeđenje razine brige o zaposlenicima – provođenje ankete o zadovoljstvu zaposlenika i prikupljanje prijedloga za unaprjeđenjem	SREDNJA
TEHNIČKE SIGURNOSNE KONTROLE		
KT-01	Implementacija novog alata za pričuvnu kopiju	SREDNJA
KT-02	Enkripcija tvrdih diskova – radne stanice	VISOKA
KT-03	Proširenje opsega primjene sustava za procjenu ranjivosti – obuhvatiti čitav ISMS	SREDNJA
KT-04	Implementacija 2FA za kontrolu pristupa na ključne sustave	SREDNJA
KT-05	Implementacija naprednih alata za testiranje aplikacija	SREDNJA

Tablica 5.2 Ciljevi sustava upravljanja informacijskom sigurnošću

#	ISMS ciljevi	Opis	Status
1	ISO 27001:2013 certifikacija	Uspješno dovršenje ISO 27001:2013 certifikacije	Realizacija je u tijeku.
2	Puno usvajanje ISMS-a na nivou InfoSofta	Svi zaposlenici pročitali su i usvojili Politiku informacijske sigurnosti i prateće ISMS dokumente, kao i svoje uloge i odgovornosti u ISMS sustavu.	Realizacija je u tijeku.
3	Uspješno ispunjavanje i pozitivan odgovor na sve zahtjeve za ocjenu sukladnosti	InfoSoft bi trebao uspješno ispuniti i odgovoriti na sve zahtjeve za ocjenu sukladnosti na koje upućuju klijenti ili regulatori.	Realizacija je u tijeku (sustavno provođenje).
4	Program podizanja svijesti o informacijskoj sigurnosti za sve zaposlenike	Uspostava programa podizanja svijesti o informacijskoj sigurnosti, koji pohađaju svi zaposlenici.	Redovno informiranje svih zaposlenika mjesečnim *InfoSec Newsletterom*. Implementacija LMS sustava je u tijeku.
5	Sigurnost trećih strana	Razviti i implementirati upitnik za procjenu sigurnosti treće strane kao dio postupka dubinske analize.	Realizirano
6	Implementacija kritičnih sigurnosnih kontrola identificiranih tijekom godišnjeg postupka procjene rizika	Implementacija sigurnosnih kontrola koje su identificirane i formalno prihvaćene putem postupka upravljanja rizicima.	Realizacija je u tijeku.

Predstavljanjem i nakon toga usvajanjem dokumenta ISMS Ocjena uprave, voditelj je stvorio sve preduvjete za angažiranje akreditiranog društva za formalno certificiranje InfoSofta po osnovi ISO-a 27001. Nakon toga voditelj je ugovorio proces certifikacije, dobio formalni termin za nju i organizirao sâm postupak u kojem su ovlašteni revizori vanjske akreditirajuće kuće proveli certifikaciju. Voditelj je bio onaj tko je odgovarao na pitanja i dostavljao dokaze.

Pitanja su se svodila na to postoje li određeni dokumenti koje standard zahtijeva te jesu li propisani postupci i procedure zaista implementirani. Jedno od vrlo čestih pitanja za koje je potrebno dostaviti dokaze svodi se na duljinu i kompleksnost lozinke koja je propisana *Pravilnikom o upravljanju lozinkama*.

U pravilniku je voditelj propisao, a uprava usvojila, da sve aplikacije; uključujući i direktorij-servise poput Active directoryja, u kojima su kreirani korisnički računi, sljedeće: za račune s običnim pravima, lozinke moraju imati minimalno 12 znakova, među kojima je uz alfanumeričke znakove potrebno ubaciti barem jedan poseban znak. Svi računi s povlaštenim pravima, kao što su servisni računi, administratorski računi i računi vanjskih partnera moraju imati lozinke minimalne duljine 14 znakova te uz alfanumeričke znakove moraju sadržavati barem jedan posebni znak. Dodatno je propisano da se sve lozinke moraju promijeniti minimalno svaka tri mjeseca. Voditelj je navedene zahtjeve iz pravilnika uspio implementirati uz pomoć primoravanja vlasnika i administratora svih aplikacija i sustava. Proces revizije navedenog sveo se na to da je revizor od voditelja zatražio popis svih računa na ključnim sustavima kompanije. Paralelno je iz kadrovske službe zatražio trenutačni popis svih

zaposlenika, te je od voditelja komunikacije s dobavljačima zatražio popis svih dobavljača s kontaktnom osobom. Prvo je usporedio broj zaposlenika InfoSofta s brojem računa na Active directoryju, te je na temelju nasumičnog uzorka provjerio sigurnosne postavke lozinke za korisnički račun s običnim pravima i za korisnički račun s povlaštenim pravima.

Nakon toga je isto napravio za korisničke račune vanjskih partnera koji imaju pravo pristupa sustavima InfoSofta. Sve navedeno provjerio je na temelju nasumičnog i reprezentativnog uzorka. Reprezentativnost, pa samim time i točnost navedenog revizorskog procesa upitna je, no dozvoljena samim standardom. Za reviziju i u konačnici, zahtjeve standarda, provedeno je bilo zadovoljavajuće. Navedeno nije bilo zadovoljavajuće za interne zahtjeve voditelja, koji je sâm pokrenuo sveobuhvatnu internu reviziju svih korisničkih računa, a koju nije proveo na temelju uzorka već na temelju uvida u sve račune i njihove sigurnosne postavke vezane za kompleksnost, duljinu i trajanje pristupne lozinke. Ti nalazi pokazali su pravo stanje i upozorili na neusklađenosti s pravilnikom i kršenje sigurnosnih mjera, dok certificirajuća revizija ovdje nije otkrila neusklađenost sa standardom. Interna revizija koju je inicirao voditelj, pronašla je popriličan broj neusklađenost s pravilnikom i kršenja njegovih zahtjeva. Interni nalazi ishodili su pokretanje korektivnih aktivnosti, a nadzor provedbe korektivnih aktivnosti preuzeo je voditelj informacijske sigurnosti.

Projekt certifikacije InfoSofta po osnovi ISO 27001 standarda uspješno je proveden uz obvezu provođenja određenih korektivnih radnji i preporuka do sljedećeg ciklusa certifikacije.

Uz navedenu interno pokrenutu reviziju (pokrenuo ju je voditelj), otkriven je prostor za poboljšanjem informacijske sigurnosti. Neke od preporuka su: gašenje određenog broja AD računa koji su pripadali bivšim djelatnicima, zahtjev za podizanjem na noviju verziju određenih operacijskih sustava na određenim poslužiteljskim računalima, podizanje svjesnosti i znanja o informacijskoj sigurnosti kod svih djelatnika i uspostava dvostruke autentifikacije za interno razvijeno rješenje u kojem se nalaze sve bitne poslovne aplikacije.

Svi ciljevi održavanja sustava upravljanja informacijskom sigurnošću i provođenje uspostavljenih kontrola prikazanih u Tablici 5.1, postale su glavne aktivnosti i odgovornosti voditelja.

5.2. Voditelj informacijske sigurnosti u javnom sektoru

Prema iskustvu autora ovog rada, obnašatelj funkcije voditelja informacijske sigurnosti velikim dijelom ovisi o tome je li organizacija u kojoj je ta funkcija odgovorna za informacijsku sigurnost dio kritične nacionalne infrastrukture ili nije. Ako jest, organizacija je obvezna uskladiti svoje aktivnosti i odgovornost sa Zakonom o kritičnoj infrastrukturi. Kako je opisano u poglavlju 3.2, Zakon o kritičnim infrastrukturama je tekovina europske legislative spuštene u nacionalne zakone zemalja članica, među kojima je i Republika Hrvatska. Organizacija tada mora biti usklađena sa Zakonom o kritičnoj infrastrukturi, a oformljivanje, izbor i aktivnosti voditelja informacijske sigurnosti jasno su propisane Zakonom.

Ako javno tijelo nije dio kritične infrastrukture, sloboda i sistematizacija funkcije voditelja informacijske sigurnosti je na upravi i/ili ravnateljstvu tog tijela. U primjeru ovog rada je organizacija koju zbog prirode svih aktivnosti i vlasničke strukture možemo smatrati tijelom javnog sektora. Prije deset godina prepoznala je važnost i vrijednost informacijske sigurnosti. Razlog i odluku da se pokrenu aktivnosti vezane za uspostavu određene razine informacijske sigurnosti možemo samo nagađati te iz zapisnika sjednice uprave možemo zaključiti da je razlog bio predviđanje sve veće prijetnje na informacijsku sigurnost. S obzirom na to da je organizacija kombinacija isprepletenih komercijalnih aktivnosti i aktivnosti koje možemo svrstati u domenu javnog dobra i usluge, uspostava i održavanje informacijske sigurnosti kompleksan je posao.

Uspostavom informacijske sigurnosti krenulo se kroz pripremu za certificiranje prema međunarodnom standardu za informacijsku sigurnost ISO 27001:2013. Formalno, razvojem skupa osnovne dokumentacije uspostavljen je ISMS (engl. *Information Security Management System*). Kombinacija je to u kojoj je direktor odjela informatike uz angažman treće strane pružatelja usluge razvio, a potom od uprave usvojio osnovni skup dokumenta kao što su:

- **Politike**
    - Politika informacijske sigurnosti
    - Politika kontrole pristupnih prava
    - Politika uporabe interneta i e-pošte
    - Politika uporabe prijenosnih računala i prijenosne opreme
    - Politika kriptografskih kontrola
    - Politika nabave razvoja i održavanja informacijskih sustava

- Politika praznog stola i praznog zaslona
- Politika sukladnosti
- Politika upravljanja imovinom
- Politika upravljanja kapacitetom, planiranjem i prihvaćanjem sustava
- Politika zaporki

- **Postupci i procedure**
  - Zahtjev dobavljaču za promjenom
  - Postupak interne provjere
  - Postupak izrade kataloga i klasifikacije imovine
  - Postupak izrade sigurnosne kopije
  - Postupak korektivne radnje
  - Postupak mjerenja djelotvornosti kontrola ISMS-a
  - Postupak nadzora antivirusnog sustava
  - Postupak nadzora uporabe sustava
  - Postupak preuzimanja računala od korisnika
  - Postupak preventivne radnje
  - Postupak prihvata isporuka dobavljača
  - Postupak primjerenog rukovanja povjerljivim informacijama
  - Postupak rada u sistemskim prostorima
  - Postupak upravljanja dokumentima i zapisima
  - Postupak upravljanja korisničkim i privilegiranim pravima
  - Postupak upravljanja promjenama
  - Postupak upravljanja sigurnošću djelatnika
  - Postupak upravljanja sigurnosnim slabostima i incidentima
  - Sigurnost i kontrole pristupa mreži operativnim sustavima i aplikacijama
  - Smjernice izrade korisničkog imena
  - Upravljanje uslugom treće strane
- **Obrada i analiza rizika**
  - Katalog i klasifikacija imovine
  - Plan obrade rizika
  - Izvještaj procjene rizika
  - Metodologija procjene i kriterij obrade rizika
- **Registar sigurnosnih incidenta**

- **Izvještaji i odluke**
    - CISO izvještaj
    - Ocjena uprave
    - Program internih provjera i izvještaj internih provjera
    - Strategija informacijske sigurnosti.

Navedeni skup dokumenata među kojima su interne politike, pravilnici i procedure te sveobuhvatna procjena rizika informacijske sigurnosti, provedeni su prema ISO 27005 standardu.

ISO 27005 opisao je postupak upravljanja rizicima informacijske sigurnosti koristeći se pristupom utemeljenim na analizi rizika. Ovaj je pristup unutar organizacije pokrenuo postupak za identifikaciju i procjenu rizika, odabir odgovarajućih mjera za upravljanje rizicima te praćenje i reviziju tih mjera.

Ovime se uspio uspostaviti okvir za upravljanje rizicima informacijske sigurnosti i uspjeli su se identificirati i procijeniti rizici povezani s informacijskom sigurnošću te odabrati i primijeniti kontrole i mjere za upravljanje rizicima.

Identifikacija i procjena rizika svela se na sveobuhvatan popis imovine informacijsko-komunikacijske tehnologije. U ovoj se fazi prvi put unutar organizacije profilirao djelatnik koji je bio odgovoran i dovoljno kompetentan da ga se promakne u specijalista za informacijsku sigurnost. Uz pomoć treće strane i uz suradnju odjela financija i računovodstva, kontrolinga i drugih s odjelima informatike, stvorena je dokumentacija, kao i procedure s ciljem održavanja i poboljšanja informacijske sigurnosti. U konačnici, odjel informatike unutar ovdje opisane organizacije je uspješno certificirala akreditirana međunarodna certifikacijska kuća. Time je ostvarena svijest kod uprave te svijest i obveza djelatnika u vezi informacijskom sigurnosti.

Nakon uspješne certifikacije stvorena je svijet o potrebi ulaganja u informacijsku sigurnost, a kao posljedica toga – ugovorena je usluga vanjskog voditelja informacijske sigurnosti. Uz održavanje osnovnog skupa opisane dokumentacije, voditelj informacijske sigurnosti odgovoran je za implementaciju svih mjera koje su propisane u ISMS dokumentaciji. Uz navedeno, on je zadužen za podučavanje djelatnika, stvaranje svijesti u pisanju mjesečnih izvještaja o aktualnim temama; kao što su nove ranjivosti, novi oblici hakerskih napada i ranjivosti u staroj i novoj tehnologiji. Uz navedeno, ima savjetodavnu ulogu za odjel sistemske podrške, odjel mrežnih tehnologija i aplikativne potpore.

Neke od aktivnost su: revizija konfiguracije vatrozida i pravila i sugestije za njihova poboljšanja, revizija topologije mreže, segmentiranje mreže i definiranje pristupnih listi, organiziranje i koordiniranje penetracijskog testiranja, tretiranje i uklanjanje nalaza penetracijskog testiranja, tretiranje i uklanjanje nalaza interne i eksterne revizije, odgovor na sigurnosni incident, održavanje ciklusa recertifikacije, praćenje i predlaganje novih rješenja i/ili unapređenje postojećih te izvještavanje uprave o svojem radu i stanju informacijske sigurnosti u organizaciji. Uz navedeno, voditelj informacijske sigurnosti mora pratiti regulativu i sve zakone koji se tiču informacijske sigurnosti, a utječu na organizaciju. Iz svega opisanog može se primijetiti širina aktivnosti koja iziskuje stručnost, iskustvo i neprestano učenje za pojedinca koji obavlja navedenu funkciju voditelja informacijske sigurnosti. U ovdje opisanoj studiji slučaja, voditelj informacijske sigurnosti je vanjski suradnik koji je specijaliziran za informacijsku sigurnost i koji ima na raspolaganju osobe specijalizirane u različitim poljima informacijske sigurnosti – od penetracijskog testiranja, nadzora mrežnog prometa, upravljanja incidentima do računalne forenzike i ostalog. Baš zbog ovakve situacije može potražiti savjet kolega koji su stručniji od njega u određenom području, te model FaaS pružanja usluge vanjskog voditelja informacijske sigurnosti ovdje ima dodatnu vrijednost. S druge pak strane, ovakav model ugovoren je određenom satnicom, koja je ujedno zapreka – kako vremenska, tako i troškovna.

5.3. Voditelj informacijske sigurnosti u organizacijama za kartično plaćanje

Organizacija u ovom sektoru je ona koja nije dio banke ili bankarske grupacije, te je kao takva na području Republike Hrvatske. Osnovni zakon koji propisuje ključne parametre poslovanja je Zakon o platnom prometu, a ključan standard je PCI DSS[8] (engl. *Payment Card Industry*

[8] PCI DSS (engl. *Payment Card Industry Data Security Standard*) sigurnosni je standard koji se primjenjuje u industriji plaćanja kreditnim karticama. PCI DSS razvilo je Vijeće za sigurnost plaćanja (engl. *Payment Card Industry Security Standards Council*) s ciljem zaštite podataka o karticama i smanjenja rizika od krađe ili zloupotrebe podataka kreditnih kartica. Standard definira sigurnosne zahtjeve i preporuke koje moraju zadovoljiti organizacije, koje obrađuju, pohranjuju ili prenose podatke o kreditnim karticama. To uključuje trgovce, procesore plaćanja, kritičare, banke i druge uključene u lanac obrade kartičnih transakcija.

Data Security Standards). Aktivnosti voditelja informacijske sigurnosti su većinom povezane sa zahtjevima ovog sigurnosnog standarda i područjem

njegove primjene. U ovom dijelu rada prikazana je studija slučaja s naglaskom na aktivnosti upravljanja ranjivostima (engl. *vulnerability management*). U Tablici 5.3 to su točke 5. i 6.

Tablica 5.3 Osnovni PCI DSS zahtjevi [29]

PCI standard sigurnosti podataka - pregled zahtjeva	
Izgradi i održavaj siguran mrežni sustav!	1. Instaliraj i održavaj sigurnosne kontrole mreže! 2. Primijeni sigurne konfiguracije na sve sistemske komponente!
Zaštiti podatke računa!	3. Zaštiti spremljene podatke računa! 4. Zaštiti podatke vlasnika kartica jakim kriptiranjem za vrijeme prijenosa javno dostupnim mrežama!
Održavaj proces upravljanja ranjivostima!	5. Zaštiti sve sustave i mreže od zlonamjernog softvera! 6. Razvij i održavaj siguran sustav i softver!
Uspostavi jak proces upravljanja pristupnim pravima!	7. Ograniči pristup dijelovima sustava i podatcima nositelja kartice po principu potrebe za poslovnu svrhu! 8. Identificiraj korisnike i ovjeri pristup dijelovima sustava! 9. Ograniči fizički pristup podatcima nositelja kartica!
Učestalo nadziri i testiraj mrežu!	10. Nadziri sve logove pristupa sustavu i podatcima nositelja kartica! 11. Redovito testiraj sigurnost sustava i mreže!
Održavaj Politiku informacijske sigurnosti!	12. Potakni informacijsku sigurnost organizacijskim politikama i programima!

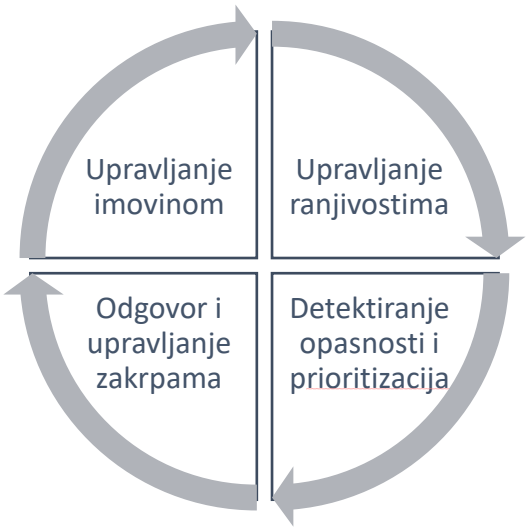
Da bi se zadovoljio standard, uspostavljen je sustav upravljanja ranjivostima; diljem sistemske i mrežne infrastrukture te unutar i izvan mrežnog perimetra, uspostavljen je sustav automatskog skeniranja ranjivosti, primjenom gotovih komercijalnih riješena.

Za automatsko skeniranje ranjivosti upotrebljava se *Qualys*[9], koji je integriran s platformom *ServiceNow*[10]. Uz automatsko skeniranje i primjenu baza znanja, u paketu usluga

[9] *Qualys* je sigurnosna platforma temeljena na oblaku, koju pruža istoimena tvrtka. To je sveobuhvatno rješenje za upravljanje sigurnošću, koje organizacijama omogućuje identificiranje, procjenu i upravljanje ranjivostima u njihovim informacijskim sustavima, mrežama, uređajima i aplikacijama.

[10] *ServiceNow* je platforma temeljena na oblaku, koja služi za upravljanje radnim postupcima i organizacijama omogućuje automatizaciju, standardizaciju i upravljanje raznim poslovnim procesima i uslugama. To je

koje nudi licenca *Qualysa* primjenjuje se modul VMDR, tj. modul koji je razvijen za upravljanje ranjivostima. Na slici (Sl. 5.2) prikazane sve faze upravljanja ranjivostima unutar VMDR modula.



Sl. 5.2 VMDR modul *Qualysa* [30]

Proces upravljanja ranjivostima pod direktnom je odgovornošću voditelja informacijske sigurnosti. Organizacija je globalno prisutna i rasprostranjena, a aktivnosti i platna mreža, s cjelokupnom pripadajućom infrastrukturom, imaju globalne razmjere s regionalnim posebnostima. Razlog regionalne posebnosti je djelomično zakonske, a djelomično tehničke prirode jer nemaju sve regije jednaku legislativu, niti jednako razvijenu tehničku infrastrukturu i regulaciju, koja je preduvjet povezivanja na platni sustav regije gdje je organizacija prisutna. Uz sve navedeno, karakteristika ovog podsektora financijskog sustava je ta da je regulacija striktna i prisutna kod više regulatornih tijela istovremeno. Tako je naprimjer, u Republici Hrvatskoj to s jedne strane Hrvatska narodna banka, a s druge Hrvatska agencija za regulaciju financijskih usluga. One su mjerodavne za Republiku Hrvatsku, ali moraju komunicirati i provoditi direktive i uredbe europskih regulatornih tijela. Dodatna specifičnost kartično-platne industrije je ta da je stalno prisutna kupnja i prodaja organizacija ili određenih dijelova drugih poslovnih subjekata (M&A transakcije, engl. *mergers and acquisitions*). U takvoj organizaciji, svjesnost navedenih činjenica poželjna je kod voditelja informacijske sigurnosti, jer sve to

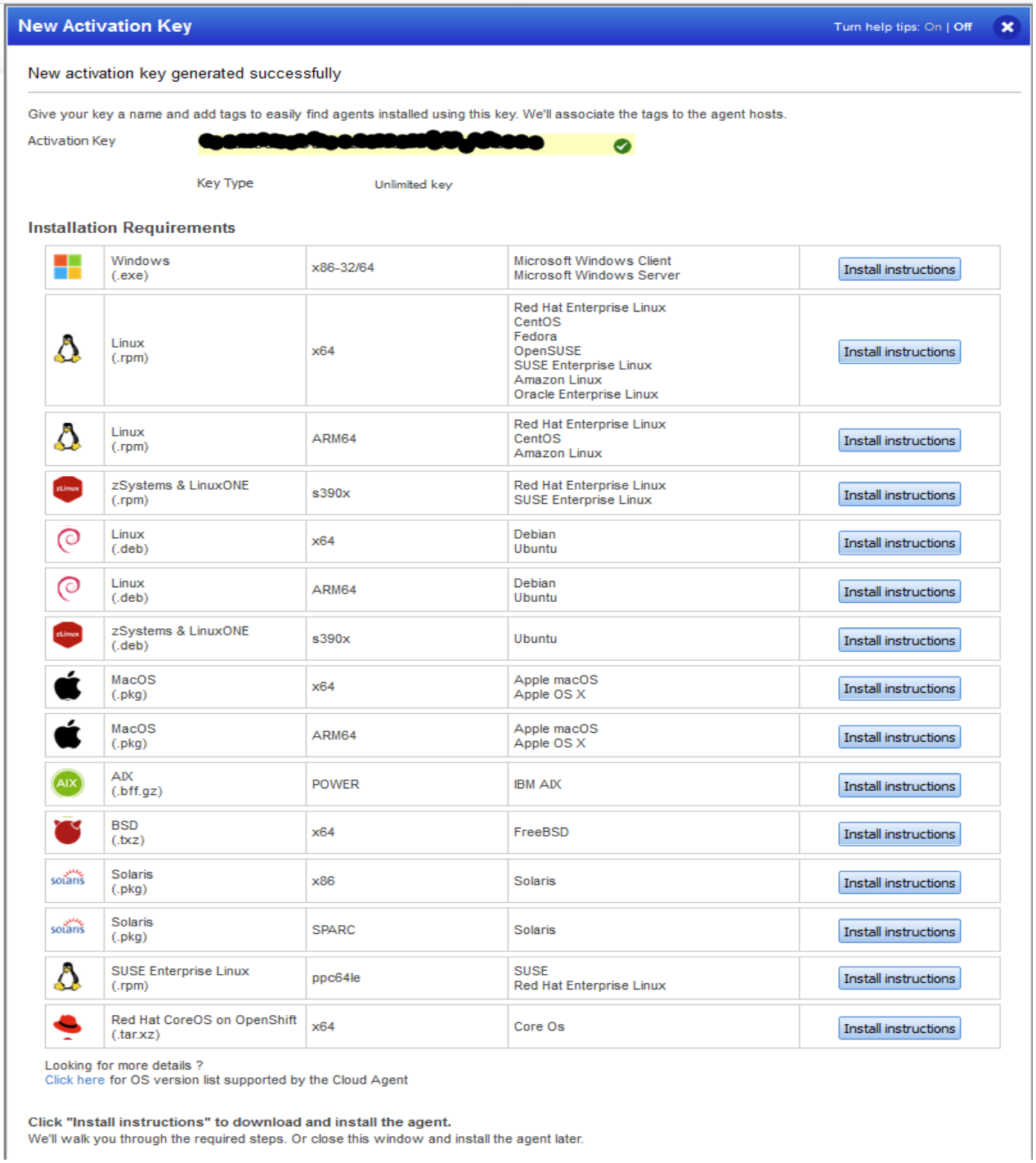
sveobuhvatna platforma, koja objedinjuje različite funkcionalnosti da bi podržala različite aspekte upravljanja poslovnim operacijama.

utječe na njegove aktivnosti, koje nisu samo upravljanje ranjivostima. U ovoj studiji slučaja opisana je isključivo aktivnost upravljanja ranjivostima.

5.3.1. Skeniranje ranjivosti

Postupak upravljanja ranjivostima svodi se na definiranje raspona internih IP adresa i podmreža (engl. *subnet*), u kojima su računala i mrežni uređaji s pripadajućim internim IP adresama i DNS imenima. U prvoj fazi uspostave, nakon što je određen opseg, počinje instalacija *Qualys* agenata na računala i mrežne uređaje. Postupak instalacije ovisi o operacijskom sustavu koji je instaliran na određenom poslužiteljskom ili klijentskom računalu.

Na slici (Sl. 5.3.) je prikazan postupak generiranja aktivacijskog ključa, kao i ponuđeni operacijski sustavi. Ovisno o operacijskom sustavu, u daljnjem koraku instalacije, koji je prikazan u nastavku, nekoliko je linija naredbi koje je potrebno upisati u terminal na stroju na kojem se želi instalirati agent.



Sl. 5.3 Generiranje aktivacijskog ključa *Qualys* agenta

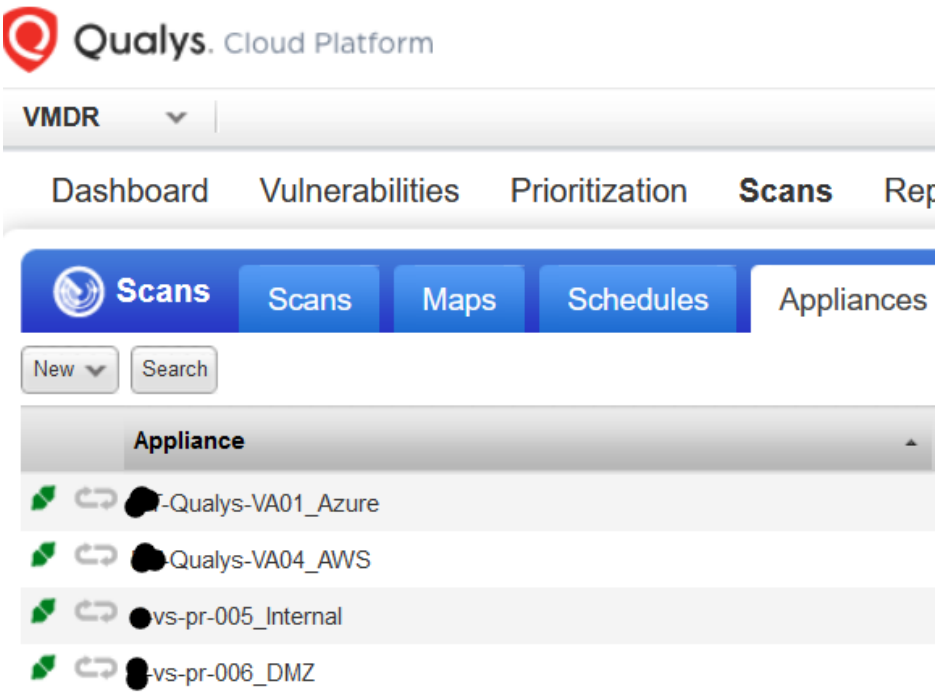
Instalacijska naredba za terminal na kojem je Windows operativni sustav:

```
QualysCloudAgent.exe CustomerId={XXXX-XXXX-XXXX}
ActivationId={XXXX-XXXX-XXX-XXXX}
WebServiceUri=https://qagpublic.qg1.apps.qualys.eu/CloudAgent/
```

Instalacijska naredba za terminal na kojem je Linux operativni sustav:

```
sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId=XXXX-XXXX-XXXX-XXXX-XXXX
CustomerId=XXXX-XXXX-XXXX-XXXX-XXXX
```

Nakon uspješno provedene instalacije pokreće se proces automatskog skeniranja za inicijalnu svrhu mapiranja svih instaliranih i aktiviranih agenata. U ovoj fazi nakon aktivacije agenta, koja se odrađuje preko centraliziranog mrežnog sučelja, ostvaruje se prva veza agenta sa skenerom koji je smješten u oblaku (engl. *virtual scanner appliance*). Skeneri su regionalno dedicirani, tj. smješteni su u podatkovne centre diljem svijeta, te se aktivni agent inicijalno pokušava povezati sa svim raspoloživim skenerima u regiji gdje je smješten stroj na kojem je instaliran. Na slici (Sl. 5.4) su prikazani skeneri raspoloživi aktivnom *Qualys* agentu.



Sl. 5.4 *Qualys* skeneri

Nakon odabira skenera i provedenog inicijalnog mapiranja zakazuju se automatska ili ručna skeniranja, ovisno o dogovoru unutar organizacije i prema zahtjevima PCI DSS standarda. Glavna podjela skeniranja uz način zakazivanja je podjela na autentificirana i neautentificirana skeniranja.

Neautentificirano skeniranje: U ovakvom se skeniranju *Qualys* koristi metodom u kojoj se ne zahtijevaju pristupni parametri ili vjerodajnice za pristup ciljnom sustavu. To znači da *Qualys* skenira sustav s vanjske mreže, koristeći se dostupnim podatcima i tehnikom skeniranja da bi identificirao ranjivosti. Neautentificirano skeniranje brže je i jednostavnije jer ne zahtijeva autentifikaciju na ciljnom sustavu, ali u pravilu pruža manje detalja o ranjivostima i ograničeno je u otkrivanju određenih vrsta problema [30].

Autentificirano skeniranje: Da bi se autentificirao na ciljnom sustavu, u ovakvom se skeniranju *Qualys* koristi pristupnim podatcima i vjerodajnicama koje su unaprijed dostavljene. Ova metoda skeniranja *Qualysu* omogućuje da pristupi dubljim razinama sustava kao što su: instalirani softver, konfiguracijske postavke i datoteke sustava. Autentificirano skeniranje pruža detaljnije podatke o ranjivostima i bolje razumijevanje ukupnog sigurnosnog stanja ciljnog sustava, ali zahtijeva pristupne podatke i duže vrijeme za izvršavanje [30].

U redovne aktivnosti koje provodi voditelj informacijske sigurnosti ove organizacije ubraja se zakazivano autentificirano skeniranje po svih 65536 portova, u definiranom opsegu i prema geolokacijama, te po rasponima internih IP adresa.

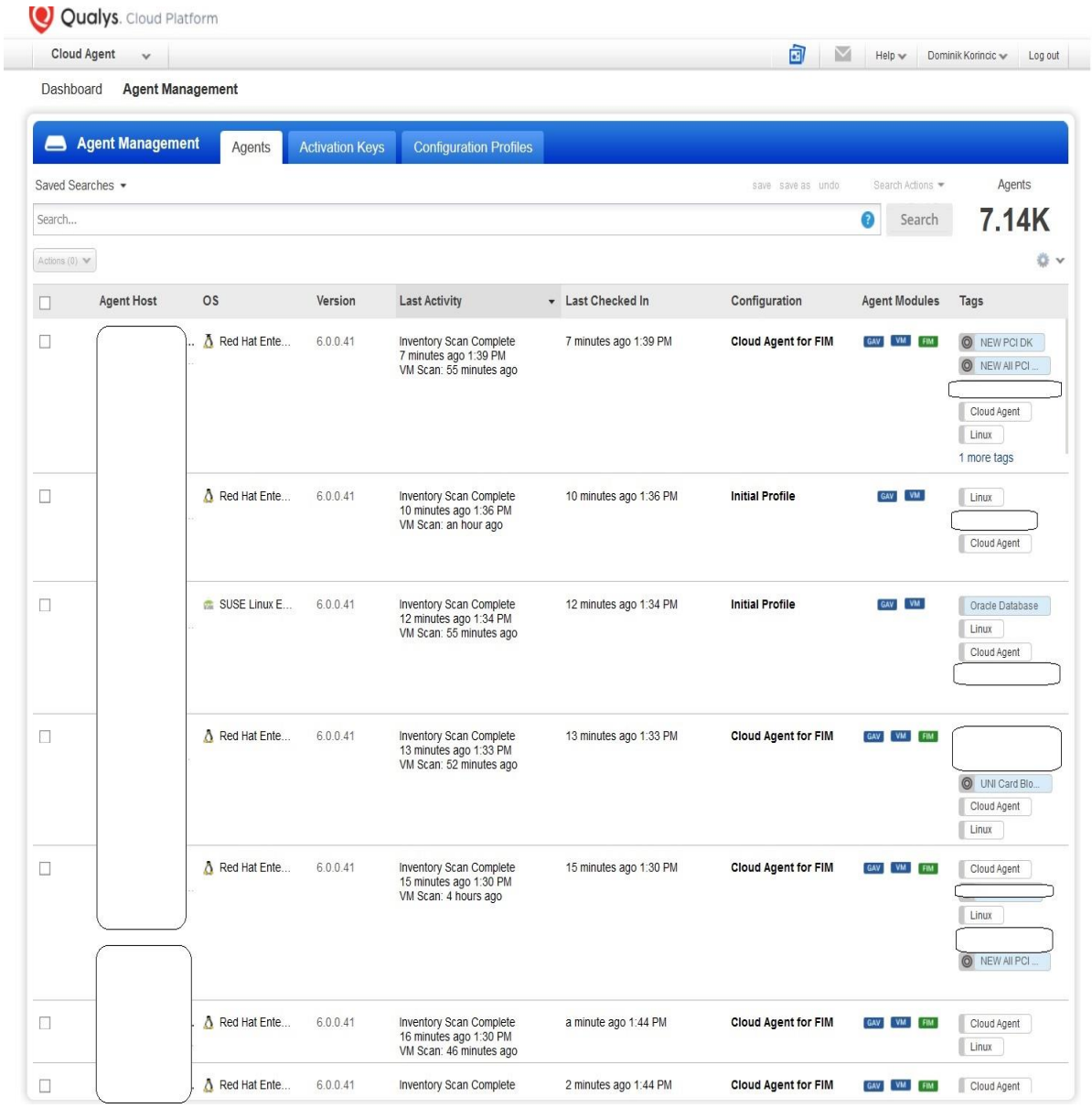
Jednom uspostavljenim aktivnim *Qualys* agentima upravlja se ili putem centraliziranog mrežnog sučelja ili izravnim spajanjem na terminal određenog stroja – bio on fizički ili virtualni. U ovoj organizaciji *Qualys* agenti su instalirani na sve strojeve, a što uključuje klijentska računala, poslužiteljska računala i određenu mrežnu opremu. Klijenti su odlukom voditelja informacijske sigurnosti konfigurirani da se povezuju na centralni poslužitelj svakih 15 minuta, pri čemu istom dinamikom skidaju deltu (odnosno razliku) u poznatim ranjivostima u odnosu na prethodno povezivanje.

Neautentificirano skeniranje provodi se samo u trenutcima dodavanja novih raspona IP adresa na kojima su strojevi i mrežna oprema. To je najčešće usklađeno s ranije iznesenom činjenicom da je za ovaj sektor karakteristično često preuzimanje i prodaja drugih kompanija iste branše. Neautentificirano skeniranje, koje je brže, samo je prijelazna faza prije negoli se mapiraju svi novi strojevi i uspostavi procedura i dinamika skeniranja te upravljanje ranjivostima.

5.3.2. Pregled skeniranih ranjivosti

Na slici (Sl. 5.5) prikazan primjer centraliziranog sučelja za upravljanje agentima.

Sl. 5.5 *Qualys* sučelje

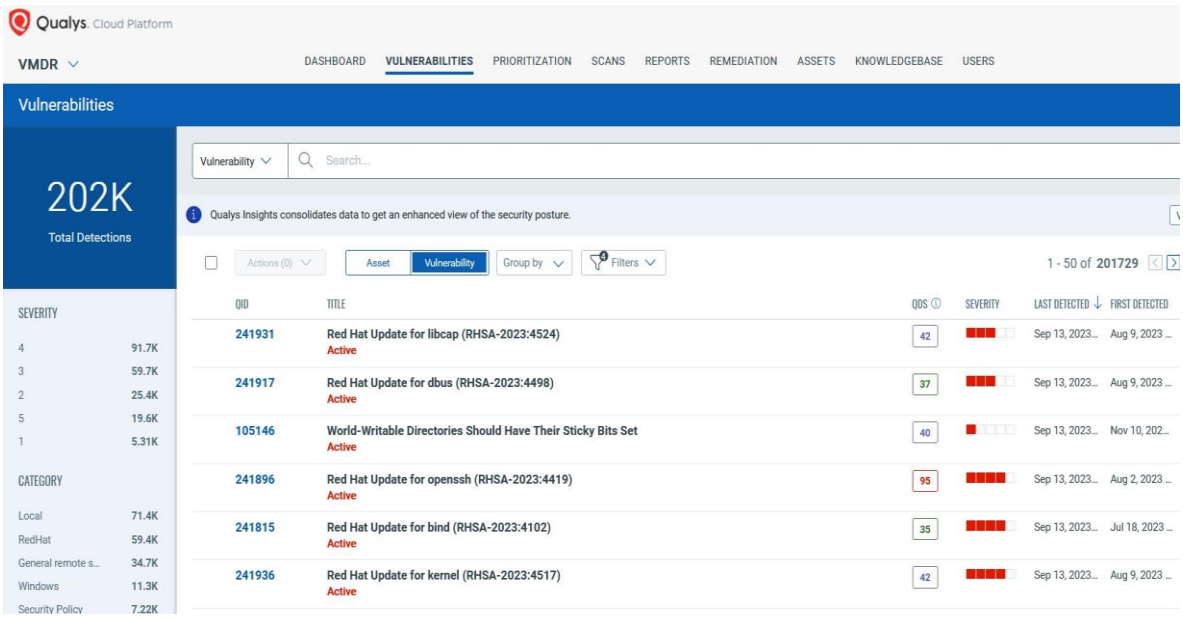


Pregled svih ranjivosti na definiranom rasponu IP adresa prati se putem QID[11] markera. Na slici (Sl. 5.6) je prikazan pregled svih ranjivosti koje su otkrivene na strojevima unutar mrežnog

[11] *Qualys QID* (*Qualys ID*) identifikacijski je broj koji se primjenjuje u okviru *Qualys* platforme za identifikaciju specifičnih ranjivosti ili sigurnosnih problema. QID je jedinstveni identifikator koji Qualys dodjeljuje svakoj pojedinoj ranjivosti koju otkrije ili prati u sustavu.

perimetra. O svakom QID-u mogu se pročitati detalji, kao i način uklanjanja ranjivosti te status. Dinamični su i aktualni prema postavljenoj konfiguraciji [30].

Glavni parametar prema kojem se određuje brzina i način tretiranja ranjivosti je kritičnost (engl. *severity*), no s obzirom na to da je *Qualys* prva razina upravljanja ranjivostima koja se isključivo tiče skeniranja, ovom se tehnologijom ne rješavaju ranjivosti, iako postoji modul koji to omogućuje. Detektirana ranjivost tretira se u daljnjem postupku, koji je integriran sa sustavom *ServiceNow*.



Sl. 5.6 Pregled ranjivosti s *Qualys* strane

U *Qualysu* se nakon provedenih skeniranja mogu automatski konfigurirati, generirati i slati izvještaji o pronađenim ranjivostima. Voditelj informacijske sigurnosti konfigurira izvještaje o ranjivostima i šalje izvještaj vlasnicima strojeva na kojima su pronađene ranjivosti. Vlasnika strojeva u ovoj organizaciji ima više jer su sve ranjivosti na stroju podijeljene prema sloju kojeg ranjivost obuhvaća. Primarno se referiramo na TCI/IP model[12], ali ne uvijek. Naprimjer, na aplikacijskom sloju je i operacijski sustav, a i određena aplikacija. Internom odlukom vlasnik,

[12] TCP/IP model je referentni model za arhitekturu mrežnih protokola koji se primjenjuju za prijenos podataka putem mreža. Sastoji se od četiri sloja: sloja mrežnog pristupa, internetskog sloja, transportnog sloja i aplikacijskog sloja. Svaki sloj ima svoje funkcije i odgovornosti u prijenosu podataka. TCP/IP model je temelj internetskog protokola i omogućuje komunikaciju između računalnih sustava u mreži.

tj. odgovorna osoba za sigurnost operacijskog sustava i određene aplikacije na tom aplikacijskom sustavu, nisu ista osoba odnosno funkcija u organizaciji; nego dvije, a to su: voditelj poslužitelja, koji na sebi ima instalaciju Windows OS-a[13] i naprimjer voditelj odjela, zadužen za aplikaciju autorizacije izvršenja neke transakcije. Na voditelju informacijske sigurnosti je odgovornost da alocira i pošalje izvještaj o ranjivostima na odgovornu osobu za tu ranjivost. Odgovorna osoba, tj. vlasnik te informacijske imovine, u određenom razdoblju odgovoran je za uklanjanje ranjivosti ili, uz adekvatnu argumentaciju, prihvaćanje sigurnosnog rizika.

5.3.3. Upravljanje ranjivostima

U ovog fazi primjenjuje se *ServiceNow*, koji je integriran s *Qualysom*. Svi nalazi i podatci o ranjivostima se putem CMDB[14] baze prenose u *ServiceNow* aplikaciju. Primjer rezultata takve integracije ovih dvaju rješenja je pregled svih pronađenih i mapiranih ranjivosti, prikazan na slici (Sl. 5.7).

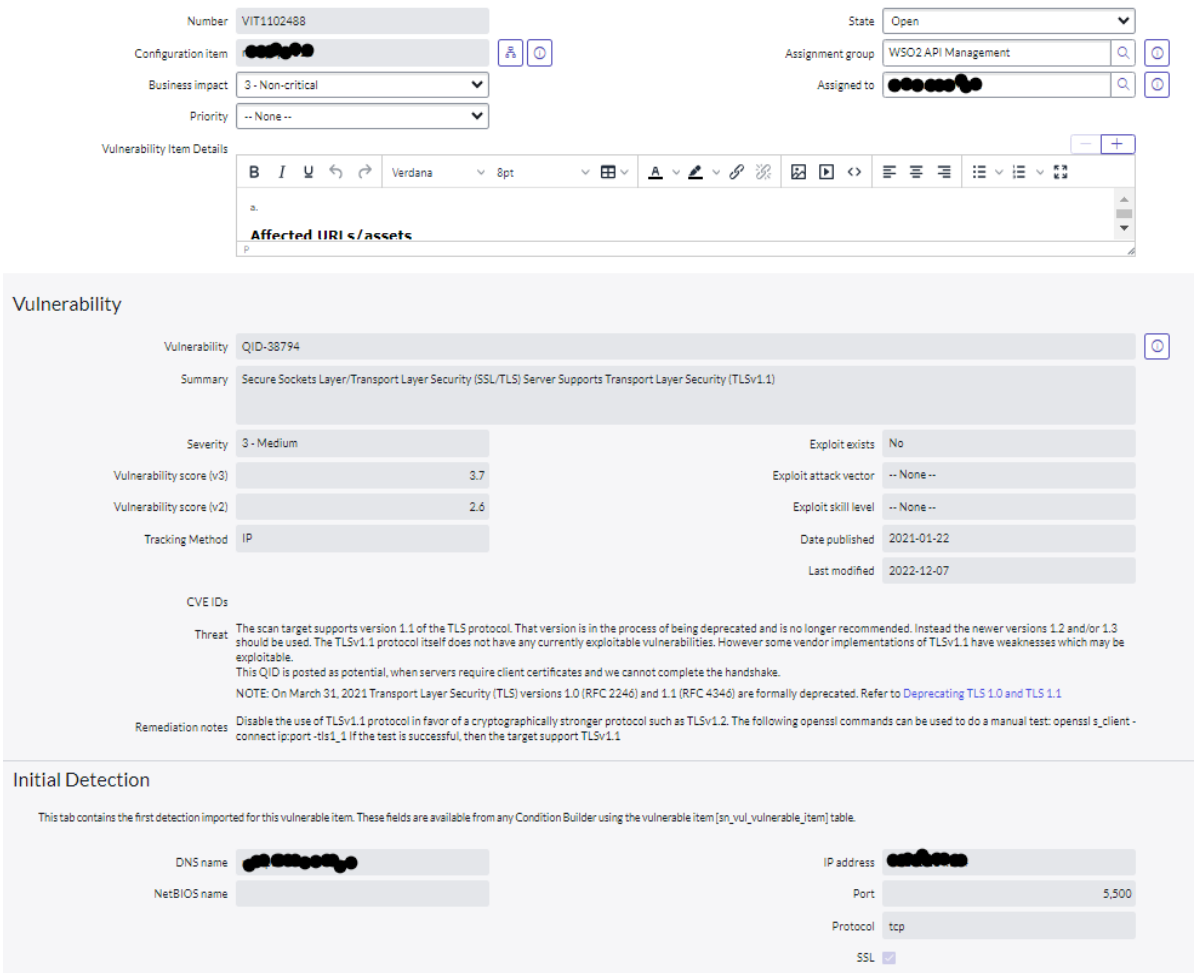
[13] Windows OS je obitelj popularnih operativnih sustava koje je razvio i distribuirao Microsoft Corporation. To je široko primjenjivan operativni sustav na različitim platformama, uključujući računala, prijenosna računala, poslužitelje i mobilne uređaje. Windows OS pruža korisničko sučelje, podršku za aplikacije, upravljanje datotekama, mrežno povezivanje i druge funkcionalnosti. Dolazi u različitim izdanjima, poput Windowsa 10, Windowsa 8 i Windowsa 7, s različitim značajkama i prilagođenim verzijama.

[14] CMDB (engl. *Configuration Management Database*) baza je podataka koja sadrži sve informacije o hardverskim i softverskim komponentama kojima se koristimo za IT usluge kompanije. Odnosi između tih komponenti su u CMDB-u također fiksni. CMDB nudi jasan pregled konfiguracijskih podataka i način njihovog pregleda iz željene perspektive [31].

Number	State	Opened	Last found	Proof
Search	Search	Search	Search	Search
VIT0109286	Closed	2019-10-31 00:00	2023-06-14	EOL Software:jQuery Version 1.x or 2.x Detected. jquery-1.12.4.min.js
VIT1089166	Closed	2022-11-02 00:00	2022-11-02	
VIT1218939	Open	2023-06-04 00:00	2023-09-12	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/bin/java 1.8.0_231-b34 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/jre/bin/java 1.8.0_231-b34 Enhanced
VIT0288188	Closed	2019-11-11 00:00	2023-09-12	intclr 5810 0.4 0.6 11054476 1277168 ? Sl Aug 18 02:29:13 java -Djava.io.tmpdir=/opt/intclr/jetty_tmp -Dfile.encoding=UTF-8 -Duser.timezone=UTC -Xms256m -Xmx1024m -Dprocess.name=reachable-participant-app -Djava.security.egd=file:///dev/urandom -XX:+HeapDumpOnOutOfMemoryError -Dsun.net.inetaddr.ttl=30 -Djdk.security.allowNonCaAnchor=true -Xdebug -Xnoagent -Djava.compiler=NONE -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=*:7007 -jar curr/reachable-participant-app.jar debug --spring.config.location=./etc/,optional:./secure/secure-environment.properties
VIT1218872	Open	2023-06-04 00:00	2023-09-13	Vulnerable version of OpenSSH Detected: OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017
VIT0625682	Closed	2020-12-11 00:00	2023-09-11	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.2.0.0.0/oracle_common/jdk/jre/bin/java 1.7.0_111-b13 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.2.0.0.0/oracle_common/jdk/bin/java 1.7.0_111-b13 Enhanced
VIT0134837	Closed	2019-11-11 00:00	2023-06-18	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\RebootPending exists
VIT1079599	Closed	2022-10-18 00:00	2022-10-18	
VIT1218981	Open	2023-06-04 00:00	2023-09-13	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/bin/java 1.8.0_231-b34 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/jre/bin/java 1.8.0_231-b34 Enhanced

Sl. 5.7 Baza svih ranjivosti organizacije

U sustavu *ServiceNow* svaka ranjivost dobiva svoj marker RII-a (ranjivosti identificirane imovine) prema QID i IP adresi stroja. U toj fazi mapiranja svaki RII dobiva određene nužne parametre za daljnje upravljanje ovom ranjivosti. Primjer jednog takvog RII-a prikazan je na slici (Sl. 5.8).



Sl. 5.8 Detalji RII-a i potrebni parametri

Ranjivost dalje dolazi do voditelja informacijske sigurnosti, koji određenom RII-u dodjeljuje odgovorni odjel i voditelja, koji je u konačnici odgovoran da u određenom vremenu, koje ovisi o kritičnosti same ranjivosti, postupi na sljedeći način:

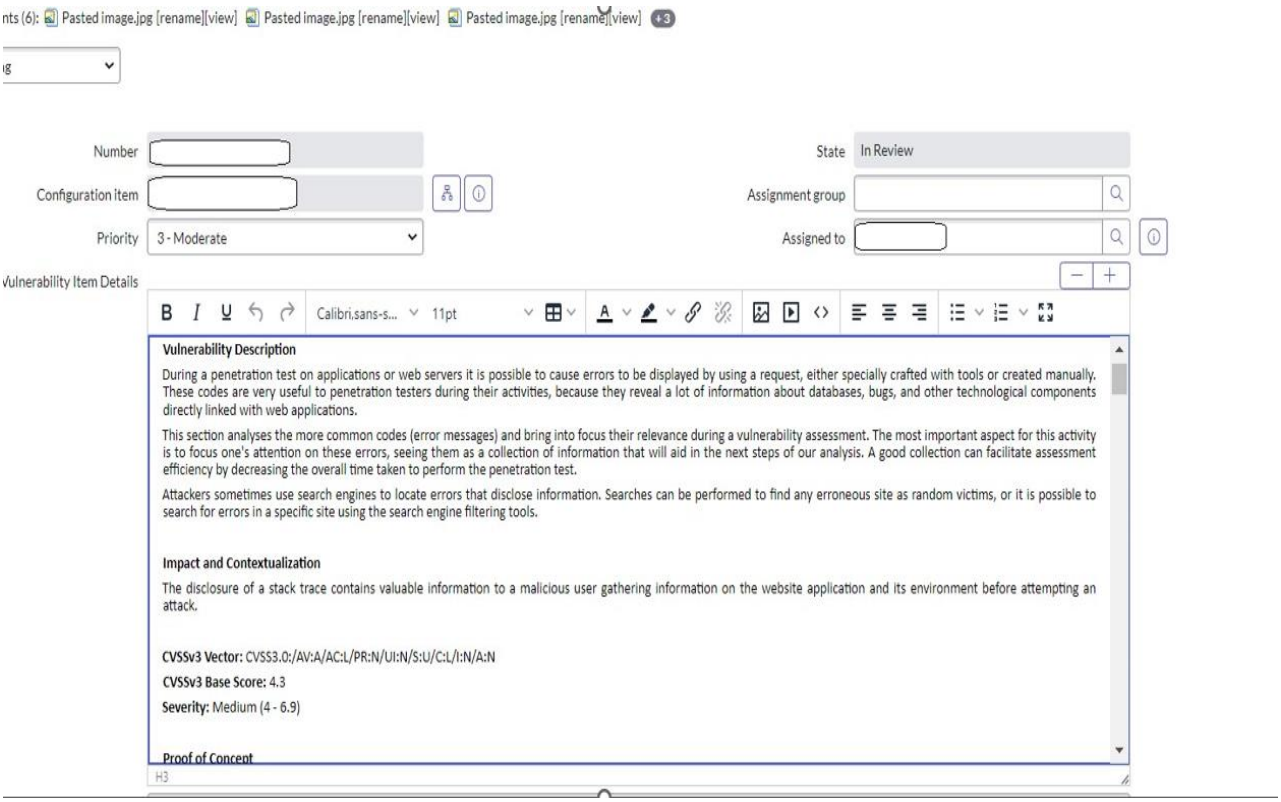
1. ukloni ranjivost
2. prihvati rizik uz valjanu argumentaciju
3. prenese odgovornost na drugi odjel, uz valjanju argumentaciju.

Za 1. rješenje voditelj informacijske sigurnosti pri daljnjem skeniranju dobiva informaciju je li ranjivost riješena ili ne. Za 2. ili 3. rješenje, da bi se ona odobrila, potrebno je da voditelj informacijske sigurnosti potvrdi uneseni odabir u sustav *ServiceNow*.

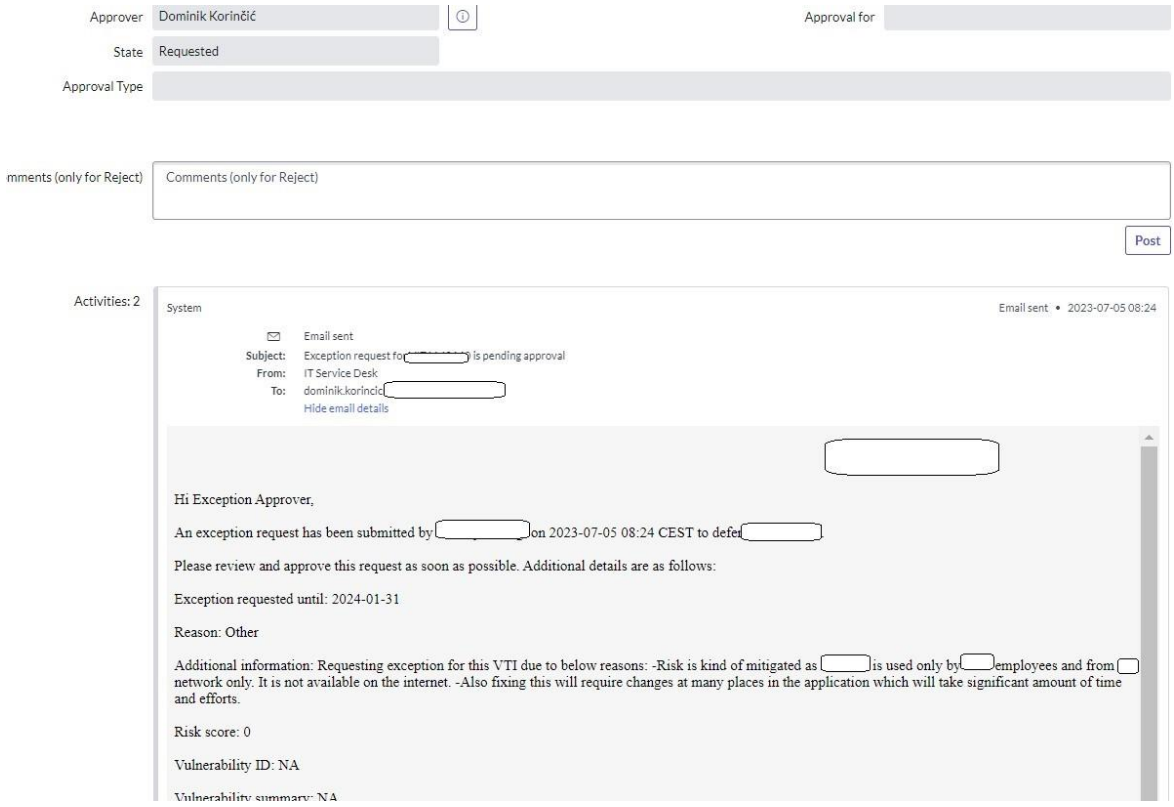
Bitan čimbenik upravljanja ranjivostima jest i pitanje je li neki raspon IP-a u opsegu PCI DSS certifikacije ili nije. Onaj koji jest, ujedno je kritična imovina za poslovanje kartičarske organizacije i prioritet u poduzimanju aktivnosti zaštite.

Uz automatsko pronalaženje ranjivosti skeniranjem pomoću *Qualys* rješenja, PCI DSS standard u odjeljku 11.4.2 i 11.4.3 zahtijeva od stručnih i kvalificiranih pojedinaca da najmanje jednom godišnje, te nakon svake značajne promjene u infrastrukturi, provedu interni i eksterni penetracijski test [29]. Penetracijska su testiranja obvezna na infrastrukturi koja je u opsegu samog standarda i na svemu što se klasificira kao kritična infrastruktura nužna za rad.

Rezultati penetracijskih testiranja istodobno se predaju voditelju odjela, koji je vlasnik ranjivog informacijskog resursa i voditelju informacijske sigurnosti. Voditelj informacijske sigurnosti, na primjeru ove organizacije, ima cijeli tim ljudi specijaliziranih za određeno područje u informacijskoj sigurnosti. Ovisno o kritičnosti ranjivosti pronađene penetracijskim testom i o tome je li ona na informacijskoj imovini koja je pokrivena sigurnosnim standardom, s njome se postupa prema proceduri. Procedura je propisana Pravilnikom o upravljanju ranjivostima te je obvezna za sve djelatnike organizacije. U konačnici, sve ranjivosti koje su na imovini koja je pokrivena PCI DSS standardom, moraju biti uklonjene. U slučaju ranjivosti koje nisu na imovini koja je pod standardom, vlasnik te imovine mora odlučiti prihvaća li rizik te ranjivosti ili poduzima potrebne korake da je ukloni. Ako i prihvati rizik ranjivosti, to prihvaćanje ne može biti dulje od godine dana, nakon čega je dužan ukloniti ranjivost ili ponuditi alternativno rješenje. Neovisno o odluci, cijeli proces u konačnici završava time da voditelj informacijske sigurnosti odobri ili ne odobri traženi zahtjev vlasnika resursa na kojem je ranjivost (vlasnika ranjivosti). Primjer jednog takvog zahtjeva za odobravanjem nalaza ranjivosti penetracijskog testiranja prikazan je na slici (Sl. 5.9), a opis ranjivosti prikazan je na slici (Sl. 5.10).



Sl. 5.9 Opis nalaza penetracijskog testa



Sl. 5.10 Zahtjev za odobravanje tretiranja ranjivosti

5.4. Vanjski voditelj informacijske sigurnosti

Uz opisane primjere voditelja informacijske sigurnosti, u Republici Hrvatskoj takve se funkcije najčešće nalaze u bankama, osiguravajućim kućama i telekomima. Neovisno o tome postoji li zakonska obveza oformljivanja takve funkcije, funkcija voditelja informacijske sigurnosti / CISO-a postoji u organizacijama iz navedenih sektora. Organizacije su; posljedično trendovima, regulatornim zahtjevima i zahtjevima njihovih klijenata osvijestile da su zahtjevi za informacijskom sigurnošću sve učestaliji, važniji i da se konstantno mijenjaju. Jedan od navedenih argumenta bio je dovoljan da se odredi osoba koja je odgovorna za informacijsku sigurnost, a to je upravo CISO. Od organizacije do organizacije njegova sistematizacija unutar organigrama organizacije varira te je podložna promjenama, ali i različitim stavovima i odlukama uprave, iz čega je jasan stav uprave prema voditelju informacijske sigurnosti. Stav uprave prema informacijskoj sigurnosti upravo se može odrediti u odnosu prema voditelju informacijske sigurnosti. U korporativnom svijetu određene veće organizacije često imaju i voditelja sigurnosti organizacije (CSO, *engl. chief security officer*) koji je nadležan CISO-u, te je on pred upravom onaj koji je odgovoran i za informacijsku sigurnost. No, zbog složenosti same tematike i važnosti informacijske sigurnosti, je li CISO član uprave ili ne ovisi o tome koliko je informacijska sigurnost važna za tu organizaciju.

Još jedan čimbenik koji utječe na to je li u organizaciji sistematizirana funkcija voditelja informacijske sigurnosti je iskustvo sa sigurnosnim incidentima. Ako je organizacija imala sigurnosni incident čije su se posljedice financijski odrazile na poslovanje organizacije, vjerojatnost uspostave voditelja informacijske sigurnosti velika je. U toj situaciji CISO je i vrlo operativna funkcija, koja ulazi u sve poslovne i tehničke procese organizacije.

Situacija u kojoj regulacija i kupci traže sve više, pa tako i po pitanju informacijske sigurnosti, stvara dodatne aktivnosti i posao za postojeće zaposlenike koji često nemaju potrebne kompetencije ni iskustvo u pitanjima informacijske sigurnosti kao što su: procjena rizika informacijskog sustava, upravljanje ranjivostima, penetracijska testiranja i rješavanje sigurnosnih incidenata. To otvara potrebu za funkcijom voditelja informacijske sigurnosti koja nije pro forma položaj, već osoba koja može preuzeti odgovornost i nositi se s opasnostima. U vrijeme pisanja ovog rada, pojedinaca koji posjeduju sve tražene kompetencije na tržištu ima jako malo, a oni koji ih imaju, već imaju poslove s natprosječnim uvjetima. Pronaći i privući adekvatnog stručnjaka nije lako. Kao odgovor na nedostatak stručnjaka i/ili nemogućnost organizacije da ponudi adekvatnu kompenzaciju takvom zaposleniku, moguće je ugovoriti

vanjskog voditelja informacijske sigurnosti po modelu FaaS. Ugovor o eksternalizaciji takve funkcije mora proći dubinsko snimanje kod regulatora, zatim mora zadovoljiti stručne kriterije – iskustva, relevantnog obrazovanja i certifikacije. Kada je to zadovoljeno moguće je imati ugovorenu funkciju voditelja informacijske sigurnosti, koji uz primjerenu mjesečnu satnicu može zadovoljiti određenim regulatornim i sigurnosnim zahtjevima. Prednost takvog oblika je ta da takav pojedinac može dolaziti iz organizacije koja je specijalizirana za informacijsku sigurnosti i ima na raspolaganju više stručnjaka iz različitih područja informacijske sigurnosti. Nedostatak je činjenica da satnica takvog pojedinca može biti ograničena i da poznavanje internih organizacijskih procesa i tehnologija može biti na manjoj razini negoli je to u situaciji internog zapošljavanja i sistematizacije funkcije voditelja informacijske sigurnosti.

6. Trendovi u informacijskoj sigurnosti

Trendovi informacijske sigurnosti u kontekstu funkcije voditelja informacijske sigurnosti se tijekom 2022. i u prvoj polovici 2023. godine mogu opisati kao više svega – više rizika, više prilika i više materijalnih kompenzacija. Na globalnoj razini, funkcija voditelja informacijske sigurnosti sazrijeva u skladu s tehnološkim potrebama organizacije i pripadajućih rizika, a to stavlja u fokus informacijsku sigurnost. Organizacije i voditelji tih organizacija moraju gledati u budućnost funkcije voditelja informacijske sigurnosti da bi se osigurao uspjeh i konstantna organizacijska održivost. Da bi navedeno bilo moguće, potrebno je ulagati u razvoj CISO funkcije, tako da se uloži u povećavanje znanju i ekspertizi, voditeljskim sposobnostima i adekvatnoj kompenzaciji.

Prema istraživanju provedenom 2023., voditelji informacijske sigurnosti istaknuli su sljedeće rizike [32]:

- napredak umjetne inteligencije i strojnog učenja
- geopolitičke rizike vezane za ratne sukobe
- hakerske napade, državno sponzorirane i one kriminalnih skupina.

Neki od zaključaka su sljedeći: može se očekivati da će se opasnosti za informacijsku sigurnost nastaviti razvijati brzim tempom, koji je često nepredvidiv i neočekivan. Smatraju da će se sistematski rizik nastaviti povećavati zbog ovisnosti o svega nekoliko proizvođača. Trend u kojem se sve više infrastrukture prebacuje na pružatelje usluge oblaka, a uz to, primjetan je nedostatak vještina u primjeni rješenja u oblaku, što je u konačnici rizik [32].

Znanje i stručnost sve su važniji, ne samo na operativnim razinama, nego i na razini uprave organizacija. Potreba za visokom razinom stručnosti za sobom povlači rizik – rizik talenta. Povelikih 41 % ispitanika potvrdilo je da njihove organizacije nemaju razrađen plan za zamjenu voditelja informacijske sigurnosti. Organizacije bi se trebale pripremiti za situaciju u kojoj postojeći voditelj informacijske sigurnosti napušta organizaciju [32].

U 2023. godini, u odnosu na isto razdoblje protekle godine, udio se voditelja informacijske sigurnosti koji su članovi uprave udvostručio, no i dalje je to mali udio, što dokazuje činjenicu da je u upravama organizacija udio članova koji razumiju i/ili imaju vještine potrebne za informacijsku sigurnost malen [32]. U Sjedinjenim Američkim Državama, SEC (engl. *Securities and Exchange Commission*) je po prvi puta objavio smjernice prema kojima bi uskoro

sve organizacije koje kotiraju na burzi, trebale objaviti koji član uprave, ako takav postoji, ima adekvatna znanja o informacijskoj sigurnosti [32]. Navedeno predstavlja dodatni prostor za napredak funkcije voditelja informacijske sigurnosti, no s druge pak strane, otvara složena pitanja, poput toga što je adekvatna razina kompetencije o informacijskoj sigurnosti za člana uprave jedne takve organizacije?

6.1. Rezultati istraživanja

Ključni pokazatelji istraživanja dani su u Tablici 6.1

Tablica 6.1 Trendovi CISO funkcije [32]

Struktura organizacije i rizici	Kompenzacija
41 % ispitanika koji obavljaju funkciju CISO-a u organizaciji, potvrdilo je da njihova organizacija ne posjeduje plan zamijene CISO-a, a 13 % njih potvrdio je da organizacija to nema ni u planu.	CISO u Sjedinjenim Američkim Državama ubraja se među najplaćenije stručnjake u IT-u s medijalnim bruto godišnjim primanjima od 620.000 američkih dolara, s dodatnim beneficijama u opcijama i dionicama kompanije od 1.100.000 američkih dolara. Navedeno predstavlja rast od 6 % u odnosu na 2022.
Navedeno je zabrinjavajuće ako uzmemo u obzir važnost te funkcije. Prema istraživanju, od svih ispitanih, njih 76 % potvrdilo je da je unutar sljedeće tri godine potpuno otvoreno za promjene poslodavca. Nedostatak plana zamijene predstavlja organizacijski rizik.	Isti pokazatelji za EU + Ujedinjeno Kraljevstvo su 457.000 američkih dolara bruto primanja, te 552.000 američkih dolara u opcijama i dionicama. Za Republiku Hrvatsku ne postoje pouzdani podaci, no dio je EU-a, te bi trendovi i konvergencija u razvijenijim sredinama trebale potaknuti i trendove u Hrvatskoj.
Ne iznenađuje da je umjetna inteligencija proglašena najvećom prijetnjom u sljedećih pet godina. Ova opasnost iziskuje evoluciju i sustavan razvoj CISO funkcije i traženih vještina. Navedeno ide u prilog činjenici i trendu da CISO funkcija postaje sve više tehnička funkcija. Primjetan je zahtjev da CISO razumije softversko inženjerstvo i sigurnost računarstva u oblaku. Općenito, od CISO-a su tražene tehničke sposobnosti.	U Australiji su navedeni indikatori primanja od 368.000 američkih dolara i 586.000 u opcijama i dionicama.
Ohrabruje činjenica da je 80 % ispitanika potvrdilo da je sposobno ulagati u vodstvo i razvoj da bi podigli razinu stručnosti u timu.	Globalno gledano, najplaćeniji CISO-i su u financijskom sektoru, dok oni s najvišim beneficijama u opcijama i dionicama dolaze iz tehnološkog i uslužnog sektora gospodarstva.
Sveukupno, polovica ispitanika potvrdila je da misli da uprava djelomično ili uopće ne razumije nalaze koji su im je predstavio CISO, dok je istovremeno 30 % njih dio uprave u organizaciji, u odnosu na 14 % u 2022. god.	

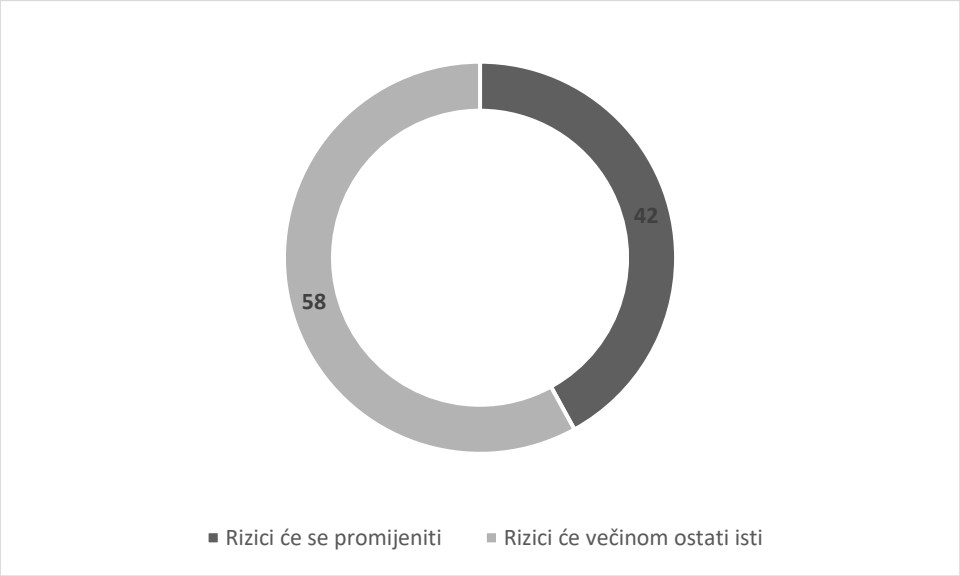
Činjenica da je 41 % ispitanika potvrdio da ne postoji plan u organizaciji za zamjenu trenutačnog voditelja informacijske sigurnosti, ozbiljan je problem jer si organizacije ne mogu

priuštiti da imaju otvoren položaj voditelja informacijske sigurnosti, iz više razloga, među kojima su:

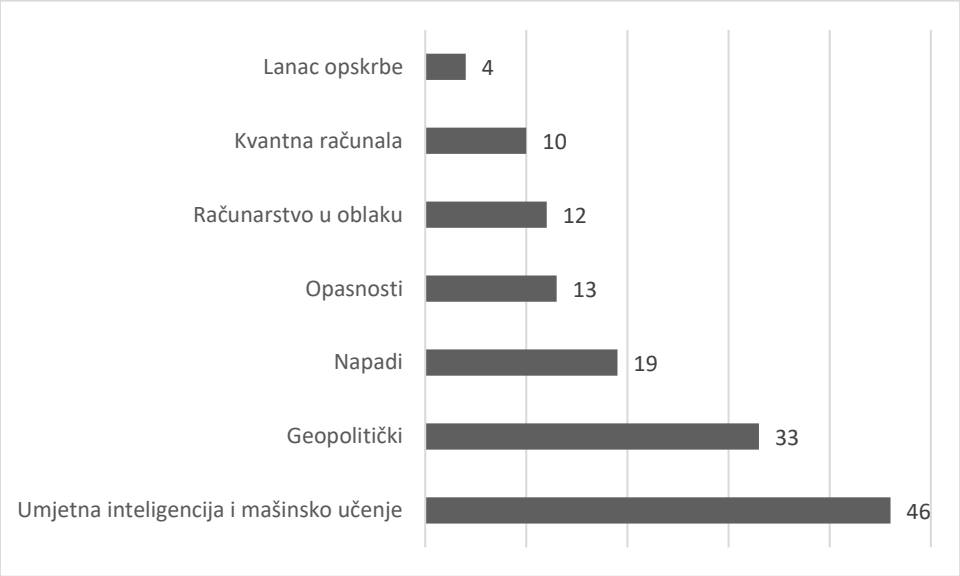
- **Prijetnja –** sigurnosne prijetnje s kojima se danas susreću organizacije rezultira time da nepostojanje plana zamjene voditelja informacijske sigurnosti nije samo problem kadrovske službe, već poslovni problem za cijelu organizaciju.
- **Regulacija –** rizik informacijske sigurnosti je rizik na razini uprave poduzeća reguliranog sektora. Ovo je primjetno i na strani regulatornih tijela, koja postojanje i nepostojanje voditelja informacijske sigurnosti tretiraju kao ključni pokazatelj spremnosti na sigurnosni incident, gdje je za određene sektore regulator propisao nužnost postojanje voditelja informacijske sigurnosti. U Hrvatskoj su to subjekti koji se ubrajaju u kritičnu infrastrukturu.
- **Dostupnost –** stručnjaci koji obavljaju funkciju CISO-a teško mogu biti shvaćeni izvan domene svojeg djelovanja, te je u slučaju promjene poslodavca najizglednija promjena na istu funkciju. Da bi se pronašla adekvatna zamjena, također je potreban znatan broj resursa, kao što su vrijeme, novac i trud.

Navedeno otvara pitanje: Kako pronaći voditelja informacijske sigurnosti? To pitanje u sebi sadrži niz čimbenika kao što su sadašnja i buduća poslovna strategija, regulatorni zahtjevi, korporativna kultura i tržišni trendovi. Iz navedenih je razloga potrebno da organizacija ima razrađen plan zamjene voditelja informacijske sigurnosti.

Važnost voditelja informacijske sigurnosti u 2023. godini nastavlja dobivati na značaju, prvenstveno zbog razvoja umjetne inteligencije te posebno zbog bojazni prema hakerskim napadima (engl. *ransomware*). Prema ispitivanju, rezultati koji su prikazani na slici (Sl. 6.1 Rizici informacijske sigurnosti u sljedećih pet godina [32]) i (Sl. 6.2 Glavni čimbenici rizika [32]) prikazuju da većina voditelja misli da su umjetna inteligencija i strojno učenje, zatim geopolitički rizik i hakerski napadi glavni rizici. Također, u 2023. godini više od polovne ispitanika misli da će ti rizici za informacijsku sigurnost biti dominanti i za pet godina.



Sl. 6.1 Rizici informacijske sigurnosti u sljedećih pet godina [32]



Sl. 6.2 Glavni čimbenici rizika [32]

Na pitanje o tome što je za voditelje informacijske sigurnosti najveći rizik na osobnoj razini, uz odgovor su zabilježeni i komentari kao što su [32]:

Nastavit će se utrka oko automatizacije aktivnosti.

Sve učestaliji napadi iziskuju sve brže odgovore.

Napadi postaju sve brži, do razine automatizacije, dok su odgovori ostali na razini ljudske sposobnosti.

Razvoj kompetencija potrebnih za odgovor na sigurnosni incident ne prati brzinu razvoja metoda napada.

Prema istraživanju, stres, izgaranje i zasićenje najveće su izazovi i problemi većini voditelja informacijske sigurnosti, u nešto većoj mjeri negoli je to bilo u 2022. godini [32].

U 2023. za sektore zdravstva i financija sigurnosni incidenti su najveći izazov, prvenstveno zato što upravo ovi sektori prolaze kroz brzi postupak digitalizacije procesa i aktivnosti [32]. Poticanje digitalizacije procesa i postojećih aktivnosti komplicira pitanje sigurnosti. 89 % voditelja informacijske sigurnosti slaže se s činjenicom da prebrza digitalizacija omogućuje pojavljivanje nepredvidivih rizika za podatke tih organizacija [33]. 47 % voditelja informacijske sigurnosti smatra da zdravstveni sektor ima najviše problema sa sigurnosnim incidentima, dok 42 % njih misli da je to sektor financija [33].

Navedeno je posljedica činjenice da bi organizacije u zdravstvenom i financijskom sektoru ostale konkurente, a u zadovoljavanju očekivanja svojih klijenata primorane su ubrzati procese digitalizacije svojih usluga. Brzina vrlo često isključuje adekvatnu sigurnost i otvara priliku koju zlonamjernici mogu iskoristiti. Paradoksalan ovom rezultatu je i rezultat ispitivanja koji upozorava na to da su sektori zdravstva i financija upravo oni sektori u kojima je najteže opravdati budžete za informacijsku sigurnost [33]. Sve navedeno pokazuje da u zdravstvu i financijama voditeljima informacijske sigurnosti nipošto nije lako.

Gotovo polovica ispitanih voditelja informacijske sigurnosti zabrinuta je da sigurnosni proboj i incident može rezultirati njihovom osobnom odgovornošću, koja povlači krivične sudske procese i kazne za njih. 99 % ispitanika priznaje osobni izazov koji proizlazi iz njihovog posla, od čega se 48 % odnosi na zabrinutost za sudske procese, a 45 % odnosi se na povećanu osobnu odgovornost [33]. Da bi se ovaj izazov umanjio, organizacije trebaju ponuditi adekvatne sigurnosne procese i alate koji voditelju informacijske sigurnosti daju zadovoljavajući pogled na sve sigurnosne rizike. Tek iz tog položaja, pojedinac koji je odgovoran može zatvoriti sve neusklađenosti sigurnosnih kontrola i stanja informacijske infrastrukture. Ovako se može smanjiti strah za osobnu odgovornost. U današnje vrijeme, u kojem voditelj informacijske sigurnosti postaje sve važnija funkcija u organizaciji, rukovodstvo te iste organizacije si ne može dopustiti rizik odlaska CISO-a zbog straha od osobne odgovornosti.

Sigurnost API-a je 78 % CISO-a naglasilo kao jednu od prioritetnih aktivnosti, a 95 % njih potvrdilo je da se revizija sigurnosti postojećih API-ja mora provesti u predstojeće dvije godine. Shodno tržišnim trendovima, u posljednje dvije godine, korištenje API-a – bilo ono

direktno ili indirektno – utječe na sigurnosne neusklađenosti u odnosu na preporučenu sigurnosnu praksu. API-ji imaju najveći potencijal utjecati na uspješnost digitalne transformacije organizacije, s obzirom na to da su integrirani u većinu današnjih aplikacija. U vezi s tim, glavni izazov CISO-a su API-ji koji se primjenjuju u postupku opskrbe organizacije. Integrirali su dio aplikacija koje komuniciraju s aplikacijama trećih strana, te je povećavanje njihove sigurnosti prioritet i jedna od glavnih aktivnosti voditelja informacijske sigurnosti [33].

7. Zaključak

Kao posljedica stalnih promjena, bilo kroz tehnološki razvoj ili društveno donesene odluke, okruženje u kojem posluju današnje organizacije – poslovne ili ne, javne ili privatne, profitne ili neprofitne – sve one imaju svoju svrhu i cilj, koji ovise o tim promjenama. Shodno tome, sigurnost kao čimbenik u ostvarivanju ciljeva sa svojim, uvjetno rečeno – podskupom informacijske sigurnosti, postaje sve vidljiviji čimbenik na razinama pojedinaca koji donose odluke koje utječu na organizacije, a posljedično i na sve one koji o njima ovise. Sigurnosni incidenti koji su manifestacija hakerskih napada, u kojima je vektor napada tehnologija povezana na poslovne procese napadnute organizacije, sve češće su popraćeni i medijskim natpisima. Uz financijsku štetu rezultiraju i reputacijskom štetom, a nakon samog incidenta često slijede promjene u organizaciji koje utječu na sve članove/djelatnike organizacije. Da bi se smanjio rizik nastajanja incidenta, potrebna je svijest i kompetencija. Ovim je radom opisano rješenje navedenih izazova tako da organizacije sistematiziraju funkcije voditelja informacijske sigurnosti, tj. CISO-a, ili ugovore navedenu funkciju s vanjskim partnerom. Dan je teorijski koncept, kao i karakteristike i potrebne vrline te vještine koje su rezultat višegodišnjeg iskustva relevantnih pojedinaca, iz čega je jasno vidljivo da voditelj informacijske sigurnosti uz tehničke vještine, mora biti svjestan poslovnih procesa i posjedovati sposobnosti rukovođenja. Jedna od glavnih aktivnosti i odgovornosti voditelja informacijske sigurnosti je procjena rizika povezanih za informacijsko-komunikacijske tehnologije. Ovo je ključna aktivnost i preduvjet uspostave ISMS-a i svih potrebnih politika i procedura za upravljanjem informacijskom sigurnosti. Cjelovit registar informacijske imovine s jasnim i realnim prijetnjama i ranjivostima temelj je za uspostavu kontrola za umanjenje rizika, implementaciju procedura, certifikaciju u vezi s informacijskom sigurnosti, te zadovoljavanje zahtjeva regulatora i klijenta.

U danom pregledu legislative Republike Hrvatske, s usvojenim EU direktivama, može se zaključiti da postoji pravno uporište za uspostavu funkcije voditelja informacijske sigurnosti. Kod određenih je zakona to eksplicitno navedeno, a kod ostalih je indirektno otvorena mogućnost prijeko potrebnih aktivnosti, a da nije eksplicitno zabranjena uspostava same funkcije voditelja informacijske sigurnosti.

U studijama slučaja u kojima su opisane aktivnosti voditelja informacijske sigurnosti u različitim organizacijama u Republici Hrvatskoj, može se zaključiti da je CISO funkcija poznata i tražena, a same aktivnosti i odgovornosti znatno ovise o sektoru kojem organizacija pripada

te samoj veličini i strukturi organizacije. Trendovi koje diktiraju razvijenija tržišta prelijevaju se preko ogranka multinacionalnih korporacija i na područje Republike Hrvatske, dok trendovi i noviteti u području opasnosti ionako imaju globalni karakter. Organizacije u Republici Hrvatskoj nisu izolirane, a globalno prisutne prijetnje za informacijsku sigurnost prisutne su i u Republici Hrvatskoj.

Voditelj informacijske sigurnosti trebao bi pokrivati širok spektar aktivnosti, imati znanje i iskustvo, kao i karakter koji se može uklopiti u organizaciju. Uz navedeno, treba posjedovati znatiželju i volju za konstantnim i cjeloživotnim obrazovanjem i učenjem o tehnologiji i informacijskoj sigurnosti. Globalni zahtjevi, radni uvjeti i beneficije te nedostatak stručnjaka informacijske sigurnosti, koji uz to imaju sve prije navedene karakteristike, čini voditelje informacijske sigurnosti vrlo traženim i deficitarnim kadrom – globalno i u Republici Hrvatskoj. Glavni komparativni nedostatak Republike Hrvatske je taj da organizacija na svojem teritoriju ne može ponuditi radne uvijete koji su konkurentni nekom razvijenijem okruženju – kako u EU-u, tako i šire.

Kao što je već navedeno, jedno od ponuđenih rješenja je i ugovaranje usluge vanjskog voditelja informacijske sigurnosti po principu FaaS, koji ima svoje prednosti i nedostatke. Prednost je širi doseg različitih ekspertiza u području informacijske sigurnosti, a nedostatak je ograničena satnica, nedovoljno poznavanje unutarnjih procesa, rizik treće strane i odgovornost. Iz istraživanja provedenih u 2023. jasno se može zaključiti koji je najčešći razlog odlaska voditelja informacijske sigurnosti i koji je problem nepostojanja plana zamijene tih ljudi. Ugovaranje vanjskog CISO-a po principu FaaS, uz neprestanu kontrolu njegova angažmana i doprinosa, rješenje je tih izazova.

Prema svemu izloženom u ovom radu, nove regulacije i trendovi će funkciju voditelja informacijske sigurnosti činiti sve bitnijom – kako globalno, tako i u Republici Hrvatskoj.

8. Literatura

[1] ISACA, 2012. - Fundamental Concepts of IT Security Assurance, https://www.isaca.org/resources/isaca-journal/past-issues/2012/fundamental-concepts-of-it-security-assurance, 5.6.2023.

[2] International Organization for Standardization – ISO: ISO 27000:201*8* *Information technology — Security techniques — Information security management systems — Overview and vocabulary* https://www.iso.org/standard/73906.html, 11. 6. 2023.

[3] Pedro Monzelo and Sergio Nunes: „*The Role of the Chief Information Security Officer (CISO) in Organizations*“, University of Lisbon, Lisbon, 2019. https://www.researchgate.net/publication/338833079 15.5.2023.

[4] Malcolm W. Harkins: „*Managing Risk and Information Security, Protect to Enable*“, 2. izdanje, Folsom, Kalifornia, Sjedinjene Američke Države, 2016.

[5] James S. Tiller: „*CISO's Guide to Penetration Testing*“, Boca Raton, Florida, Sjedinjene Američke Države, 2011.

[6] Marco Morana and co-autors: „ Application Security Guide For CISOs“, OWASP, 1.0 verzija, 2013. https://owasp.org/www-pdf-archive/Owasp-ciso-guide.pdf

[7] Harold F. Tipton and Micki Krause: „*Information Security Mangment Handbook*“, 6. izdanje, Boca Raton, Florida, Sjedinjene Američke Države, 2007.

[8] David Kim and Michael G. Solomon: „*Fundamentals of Information Systems Security*“ Burlington, Sjedinjene Američke Države, 2018.

[9] *International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines*, s interneta, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18. 6. 2023.

[10] Vlada Republike Hrvatske: „*Uredba o mjerama informacijske sigurnosti*“, Narodne novine 46/2008 broj dokumenta u izdanju 1547, Zagreb, 2008.

[11] City University of Seattle: Business & Management, s interneta, https://library.cityu.edu/researchguides/business/swot, 21. 6. 2023.

[12] Ekonomski fakultet Zagreb: *Studijska analiza makro okoline i analiza korporativnoga upravljanja*, s internata, https://www.efzg.unizg.hr/UserDocsImages/OIM/dhruska/2014-2-%20Situacijska%20analiza%20-%20okolina%20i%20SWOT.pdf, 21. 6. 2023.

[13] de Bruin, Lars: Scanning the Environment: PESTEL Analysis, s interneta, https://www.business-to-you.com/scanning-the-environment-pestel-analysis/, 21. 6. 2023.

[14] Schoenbeck, Dave: Essential Ingredients of a Small Business SWOT Analysis, s interneta, https://daveschoenbeck.com/essential-ingredients-small-business swotanalysis/, 21. 6. 2023.

[15] Šegudović, Hrvoje: „Prednosti i nedostaci metoda za kvalitativnu analizu rizika“,Infigo IS d.o.o., Zagreb, 2006.

[16] *International Organization for Standardization – ISO: ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*, s interneta, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 18. 6. 2023.

[17] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks* https://www.iso.org/standard/80585.html, 18. 6. 2023

[18] ZAKON HR: Zakon o kritičnim infrastrukturama,https://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, 26. 6. 2023.

[19] ZAKON HR: Odluka o primjerenom upravljanju informacijskim sustavom, https://www.zakon.hr/cms.htm?id=53755, 27. 6. 2023.

[20] HANFA: 3.3. Smjernice za primjereno upravljanje rizicima informacijskog sustava subjekta nadzora, https://www.hanfa.hr/media/8581/26-uis-04-smjernice-za-primjereno-upravljanje-rizicima-is-subjekata-nadzora.pdf, 27. 6. 2023.

[21] ZAKON HR: Zakon o informacijskoj sigurnosti,

https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, 28. 6. 2023.

[22] ZAKON HR: Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, https://www.zakon.hr/z/1041/Zakon-o-kiberneti%C4%8Dkoj-sigurnosti-operatora-klju%C4%8Dnih-usluga-i-davatelja-digitalnih-usluga, 30. 6. 2023.

[23] ZAKON HR: Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, https://www.zakon.hr/cms.htm?id=31285, 1. 7. 2023.

[24] ZAKON HR: Kazneni zakon, https://www.zakon.hr/z/98/Kazneni-zakon, 1. 7. 2023.

[25] ZAKON HR: Zakon o elektroničkim komunikacijama, https://www.zakon.hr/z/182/Zakon-o-elektroni%C4%8Dkim-komunikacijama, 3. 7. 2023.

[26] ZAKON HR: Zakon o provedbi Opće uredbe o zaštiti podataka, https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka, 6. 7. 2023.

[27] EUR-Lex: Direktiva (EU) 2015/2236 Europskog parlamenta i vijeća do 25. studenog 2015. o platnim uslugama na unutarnjem tržištu, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32015L2366, 8. 7. 2023.

[28] *Hrvatska udruga banaka: PSD2 Open API,* s interneta, https://www.hub.hr/hr/PSD2-Open-Api-hr, 8. 7. 2023.

[29] *Security Standards Council, LLC : Payment Card Industry Data Security Standard: Requirements and Testing Procedures v4.0, https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf*, 11. 7. 2023.

[30] Qualys, Inc.: Qualys Vulnerability Management (VMDR), https://www.qualys.com/apps/vulnerability-management-detection-response/, 12. 7. 2023.

[31] ITpedia: CMDB - Baza podataka za upravljanje konfiguracijom, https://bs.itpedia.nl/2018/08/24/cmdb-configuration-management-database/,

11. 7. 2023.

[32] Hedrick & Struggles: „ *2023 Global Chief Information Security Officer Survey*“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey, 10.7.2023.

[33] Salt Security: „*State of the CISO, A global report on priorities, pain points, and security gaps 2023*“, https://content.salt.security/global-state-ciso-report-2023.html, 11.7.2023.

Kazalo pojmova

AD	Active directory	direktorij servis
AIS	Account Information Service	usluga informiranja o stanju računa
AISP	Account Information Service Providers	pružatelj usluge o stanju računa
API	Application Programming Interface	pristupno sučelje
ASPSP	Payment Initiation Service Provider	akreditirani pružatelj usluge plaćanja
AZOP	Agencija za zaštitu osobnih podataka	agencija
CAPEX	Capital Expenditure	
CIA	Confidentiality Integrity Availability	akronim
CISO	Chief information security officer	Voditelj informacijske sigurnosti
CEO	Chief executive officer	Glavni izvršni direktor
CERT	Computer Emergency Response Team	organizacija zadužena za incidente
CFO	Chief financial officer	Direktor financija
CMDB	Configuration Management Database	baza podataka konfiguracija
COBIT	Control Objectives for Information and Related Technologies	sigurnosni okvir
CSO	Chief security officer	Direktor sigurnosti
CSIRT	Computer Security Incident Response Team	organizacija zadužena za incidente
DNS	Domain name system	sustav upravljanja domenskim imenima
DPO	Data protection officer	Voditelj za zaštitu osobnih podataka
DDOS	Distributed Denial of Service	vrsta sigurnosnog napada
EBA-RTS	European Banking Authority Regulatory Technical Standards	europsko regulatorno tijelo za tehničke standarde
ENISA	The European Union Agency for Cybersecurity	europska agencija
EU	European Union	Europska unija
FaaS	Function as a service	modalitet ponuđene usluge
GDPR	General Data Protection Regulation	Direktiva o zaštiti osobnih podataka
HNB	Hrvatska narodna banka	regulator
HANFA	Hrvatska agencija za nadzor financijskih usluga	regulator
HAKOM	Hrvatska regulatorna agencija za mrežne djelatnosti	regulator
HERA	Hrvatska energetska regulatorna agencija	regulator
HIPPA	Health Insurance Portability and Accountability Act	zakon o zaštiti medicinski podataka
HTTP	Hypertext Transfer Protocol	mrežni protokol na web-u

IEC	International electronic consortium	međunarodno elektroničko udruženje
ISMS	Information Security Management System	sistem za upravljanje sigurnošću
ISO	International Organization for Standardization	organizacija za standardizaciju
IKT	Informacijska i komunikacijska tehnologija	akronim
IT	Information tehnology	informacijska tehnologija
JSON	JavaScript Object Notation	format datoteke
M&A	Mergers and acquisitions	transakcija preuzimanja poduzeća
NIST	National Institute of Standards and Technology	nacionalni institut za standarde i tehnologiju
PCI DSS	Payment Card Industry Data Security Standard	Sigurnosni standard
PDCA	Plan Do Check Act	akronim
PESTLE	Political, Economic, Social, Technological, Legal and Environmental factors,	okvir za analizu
PSD2	Payment Services Directive	direktiva o platnim uslugama
PSU	Payment Service User	korisnik usluge platnog sustava
PISP	Payment Initiation Service Provider	pružatelj platne usluge
RACI	Responsible, Accountable, Consulted, Informed	dijagram odgovornosti
RII		Ranjivost identificirane imovine
SaaS	Software as a service	modalitet usluge u oblaku
SIEM	Security information and event management	nadzorni sustav sigurnosti
SEC	Securities and Exchange Commission	regulator
SWOT	Strengths, Weaknesses, Opportunities, and Threats	okvir za analizu
SOX	Sarbanes-Oxley Act	zakon o zaštiti ulagača
TLS	Transport Layer Security	mrežni protokol za enkripciju
TTP	Third Party Payment Service Provider	pružatelj usluge plaćanja koji nije banka
TCI/IP	Transmission Control Protocol/Internet Protoco	skup mrežnih protokola
VMDR	Vulnerability Management, Detection, and Response	modul upravljanja ranjivostima
XML	eXtensible Markup Language	format datoteke
XS2A	Access to Account	pristup računu
QID	Qualys ID	identifikacija ranjivosti

Životopis

Dominik Korinčić rođen je 10. 12. 1986. godine u Zagrebu. Nakon završetka XV. Prirodoslovno-matematičke gimnazije u Zagrebu 2006., započinje svoju poslovnu karijeru i paralelno upisuje Ekonomski Fakultet u Zagrebu. Nakon završenog prvostupanjskog obrazovanja iz poslovne ekonomije, stječe titulu *univ. bacc. oec*., nakon čega upisuje diplomski, smjer računovodstva i revizije, koji završava te stječe titulu *mag. oec*. Za vrijeme i nakon studija radi u revizorskim poduzećima, među kojima su Deloitte i PwC, zatim radi u sektorima investicijskih fondova, proizvodnje te u multinacionalnoj energetskoj kompaniji E.ON. Tijekom poslovne prakse upoznaje se s informacijskom sigurnošću i postaje svjestan potencijala i potrebe za njome. Godine 2020. u Zagrebu na Fakultetu elektrotehnike i računarstva upisuje poslijediplomski specijalistički studij Informacijske sigurnosti te nastavlja svoju karijeru u tvrtki INFIO IS d. o. o., na položaju stručnjaka za informacijsku sigurnost – konzultant.

Biography

Dominik Korinčić was born on December 10th, 1986. in Zagreb. After finishing the XV. natural science and mathematics high school in Zagreb, in 2006 he started his business career and simultaneously enrolled in the Faculty of Economics in Zagreb. After completing his undergraduate education in business economics, he obtained the title univ. bacc.oec., after which he enrolled in the audit and accounting major, which he completed and obtained the title M.Sc.oec. During and after his studies, he worked in auditing companies, including Deloitte and PwC. After that, he worked in the sectors of investment funds, production, and a multinational energy company E.ON. Through business practice, he became familiar with information security and aware of the potential and need for it. In 2020, he enrolled in a postgraduate specialist study of Information Security at the Faculty of Electrical Engineering and Computer Science in Zagreb and continued his career at INFIO IS d.o.o. on the position of information security specialist-consultant.