Doc. dr. sc. Robertina Zdjelar

Kibernetička sigurnost u opskrbnom lancu

Sažetak

Zakonom o kibernetičkoj sigurnosti („Narodne novine“ broj 14/24) (dalje u tekstu: Zakon) zakonodavac je u članku 30., stavku 1., podstavku 4. definirao mjere upravljanja kibernetičkim sigurnosnim rizicima koje govore i o ***sigurnosti u opskrbnom lancu***, uključujući sigurnosne aspekte u pogledu odnosa između subjekta i njegovih izravnih dobavljača ili pružatelja usluga. Također, u istom članku stoji odredba da „pri procjeni proporcionalnosti primijenjenih tih mjera ključni i važni subjekti dužni su uzeti u obzir ranjivosti specifične za svakog izravnog dobavljača i pružatelja usluge te opću kvalitetu proizvoda i kibernetičku sigurnosnu praksu svojih dobavljača i pružatelja usluga, kao i rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe informacijsko-komunikacijskim (IKT) uslugama, IKT sustavima ili IKT proizvodima, koje provodi Skupina za suradnju zajedno s Europskom komisijom i ENISA[1]-om“. Prilog IV. Zakona govori da u obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnost (isti je definiran člankom 55. Zakona) treba uključiti razradu politike za rješavanje kibernetičkih sigurnosnih pitanja u opskrbnom lancu za IKT proizvode i IKT usluge kojima se za pružanje svojih usluga odnosno obavljanje svojih djelatnosti koriste subjekti na koje se primjenjuje Zakon.

Ključne riječi: ISO/IEC 29147:2018, ISO/IEC 30111:2019, kibernetička sigurnost, kontrole, NIS 2 direktiva, opskrbni lanac

1. Uvod

Mjere za osiguranje kibernetičke sigurnosti mrežnih i informacijskih sustava (NIS) lako možemo laički opisati kao „imunološki sustav“ u biološkim sustavima. Što je higijena na višoj razini to je veća vjerojatnost da će organizam biti zdrav i otporan. Također, ako biološki sustav ima zdrave uvjete u kojima živi to je vjerojatnost da će se dogoditi napad na imunološki sustav manja. Što je sustav otporniji jer imunološki sustav dobro funkcionira to je razina ranjivosti niža. I tako bismo mogli još sličnosti navesti kako bi približili što je kibernetička sigurnost za tehničke, mrežne i informacijske sustave.

Kako očuvati otpornost? Prije svega na način da svaka jedinka za sebe proaktivno radi na tome, adekvatnim mjerama, ali i „da pazi“ u kakvom okruženju se kreće, gdje se izlaže manjem riziku od ugroze. Upravo takvo djelovanje očekuje se i kod mjera kibernetičke sigurnosti kada je riječ o „kontaktu“ s vanjskim svijetom, odnosno s našim dobavljačima ili pak kupcima.

Obzirom na specifičnost teme za početak treba reći što se podrazumijeva pod pojmom opskrbni lanac.

[1] The European Union Agency for Cybersecurity

Pod pojmom „opskrbni lanac“ (engl. supply chain) u online enciklopediji Britanica[2] stoji: *„Kao pomoć u integraciji vlastitog lanca vrijednosti tvrtke, sustavi za obradu transakcija također mogu poslužiti za integraciju cjelokupnog* ***lanca opskrbe*** *čiji je organizacija dio. To uključuje sve tvrtke uključene u projektiranje, proizvodnju, marketing i isporuku robe i usluga - od sirovina do konačne isporuke proizvoda. Sustav upravljanja lancem opskrbe (engl. Supply chain management - SCM) upravlja protokom proizvoda, podataka, novca i informacija kroz cijeli lanac opskrbe, koji počinje od dobavljača sirovina, prolazi kroz posredničke razine prerađivačkih tvrtki i završava s distributerima i trgovcima. Na primjer, kupnjom artikla u velikoj maloprodajnoj trgovini generira se više od blagajničke potvrde: ona također automatski šalje nalog za obnavljanje zaliha odgovarajućem dobavljaču, koji zauzvrat može zahtijevati narudžbe dobavljačevim dobavljačima. S SCM sustavom, dobavljači također mogu pristupiti bazi podataka o zalihama trgovca putem weba kako bi planirali učinkovito i pravovremeno.“*

Intenzivna razmjena dobara i usluga, a čemu prethodi razmjena informacija o međusobnim aktivnostima dionika u opskrbnom lancu, može potencijalno biti rizik u smislu kibernetičkih napada.

U nastavku se daje pregled recitala i članaka NIS 2 Direktive o kibernetičkoj sigurnosti u opskrbnom lancu.

NIS 2 Direktiva u **recitalu 56.** kaže *„..Mala i srednja poduzeća sve više postaju meta napada u lancu opskrbe zbog svojih manje strogih mjera upravljanja kibersigurnosnim rizicima i upravljanja napadima te činjenice da imaju ograničene resurse za sigurnost. Takvi napadi u lancu opskrbe ne utječu samo na mala i srednja poduzeća i njihovo poslovanje, već mogu imati i kaskadni učinak na veće napade na subjekte kojima isporučuju robu. Države članice trebale bi kroz svoje nacionalne strategije za kibersigurnost pomoći malim i srednjim poduzećima u rješavanju izazova s kojima se suočavaju u svojim lancima opskrbe..“*

Recital 85. NIS 2 Direktive govori „*Suzbijanje rizika koji proizlaze iz lanca opskrbe subjekta i njegova odnosa s dobavljačima, kao što su pružatelji usluga pohrane i obrade podataka ili pružatelji upravljanih sigurnosnih usluga i proizvođači softvera, posebno je važno s obzirom na učestalost incidenata u kojima su subjekti postali žrtve kibernapada i u kojima su zlonamjerni počinitelji mogli ugroziti sigurnost mrežnih i informacijskih sustava subjekta iskorištavanjem ranjivosti koje utječu na proizvode i usluge trećih strana. Ključni i važni subjekti bi stoga trebali procijeniti i uzeti u obzir ukupnu kvalitetu i otpornost proizvoda i usluga, mjera upravljanja kibersigurnosnim rizicima koje su ugrađene u njih, i kibersigurnosnih praksi svojih dobavljača i pružatelja usluga, uključujući njihove sigurne razvojne postupke. Ključne i važne subjekte bi trebalo posebno poticati da uključe mjere upravljanja kibersigurnosnim rizicima u ugovorne aranžmane sa svojim izravnim dobavljačima i pružateljima usluga. Ti subjekti bi mogli razmotriti rizike koji proizlaze iz drugih razina dobavljača i pružatelja usluga“*

[2]Britannica, „Along with helping to integrate a firm’s own value chain, transaction processing systems can also serve to integrate the overall supply chain of which the organization is a part. This includes all firms involved in designing, producing, marketing, and delivering the goods and services—from raw materials to the final delivery of the product. A supply chain management (SCM) system manages the flow of products, data, money, and information throughout the entire supply chain, which starts with the suppliers of raw materials, runs through the intermediate tiers of the processing companies, and ends with the distributors and retailers. For example, purchasing an item at a major retail store generates more than a cash register receipt: it also automatically sends a restocking order to the appropriate supplier, which in turn may call for orders to the supplier’s suppliers. With an SCM system, suppliers can also access a retailer’s inventory database over the Web to schedule efficient and timely deliveries in appropriate quantities.“ preuzeto s https://www.britannica.com/topic/supply-chain-management, pristupljeno 8. kolovoza 2024.

Recital 90. NIS 2 Direktive govori *„Kako bi se dodatno suzbili ključni rizici u lancu opskrbe i pomoglo ključnim i važnim subjektima koji djeluju u sektorima obuhvaćenima ovom Direktivom da na odgovarajući način upravljaju rizicima u lancu opskrbe i rizicima povezanima s dobavljačima, skupina za suradnju, u suradnji s Komisijom i ENISA-om te, prema potrebi, nakon savjetovanja s relevantnim dionicima, među ostalim iz industrije, trebala bi provoditi koordinirane procjene sigurnosnih rizika kritičnih lanaca opskrbe, kao što je učinjeno za 5G mreže u skladu s Preporukom Komisije (EU) 2019/534(19), u cilju utvrđivanja ključnih IKT usluga, IKT sustava ili IKT proizvoda, relevantnih prijetnji i ranjivosti za pojedini sektor.“*

Članak 7. NIS 2 Direktive govori: „2. *U okviru nacionalne strategije za kibersigurnost države članice posebno donose politike: (a) za rješavanje kibersigurnosnih pitanja u lancu opskrbe za IKT proizvode i IKT usluge kojima se koriste subjekti za pružanje svojih usluga.“*

Članak 21. NIS 2 Direktive govori: *„1. Države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge.*

2. Mjere iz stavka 1. temelje se na pristupu kojim se ***uzimaju u obzir sve opasnosti*** *i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata te uključuju najmanje sljedeće:*

...(d) sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga;...“

Iz priloženog je vidljivo da NIS 2 Direktiva ne propisuje načine kako provesti mjere i koje točno mjere treba provesti. Niti međunarodni standardi (ISO, NIST) ne daju konkretne mjere što je potrebno učiniti. No, moguće je osloniti se na preporuke, što je u ovako izazovnom području itekako od pomoći jer su preporuke nastale na temelju provjerene dobre prakse. Primjerice **ISO/IEC 30111:2019** *Information technology — Security techniques — Vulnerability handling processes* daje preporuke što je moguće poduzimati kod rješavanja ranjivosti i **ISO/IEC 29147:2018** *Information technology — Security techniques — Vulnerability disclosure* daje preporuke što je moguće poduzimati za otkrivanje ranjivosti. Područje informacijske sigurnosti pokriveno je ***ISO/IEC 27002:2022*** *Information security, cybersecurity and privacy protection — Information security controls. U okviru spomenutih dokumenata* obrađena su pitanja informacijske sigurnosti u vezi dobavljača (5.19), definiranje informacijske sigurnosti u ugovorima s isporučiteljem (5.20), upravljanje informacijskom sigurnosti u IKT opskrbnom lancu (5.21), upravljanje praćenjem, pregledom i promjenom usluga isporučitelja (5.22), informacijska sigurnost pri korištenju „usluga u oblaku“ (5.23), razvoj povjeren vanjskim suradnicima (engl. outsourcing) (8.30).

2. Upravljanje rizicima u opskrbnom lancu

Za učinkovito upravljanje rizicima u opskrbnom lancu potrebno je uspostaviti procedure kojima se ublažavaju rizici. Procedure se provode timski. Dakle, formiranje tima za

upravljanje rizicima u opskrbnom lancu bio bi prvi korak. Kao i svaka upravljačka aktivnost tako i ova nužno zahtijeva raspoložive resurse i dobru organizaciju radnih aktivnosti. U ovom segmentu djelovanja na rizike značajnu ulogu imaju iskusni menadžeri, koji su prema RASCI (engl. **Responsible, Accountable, Supportive, Consulted, and Informed)** matrici dostupni, na pomoć timu, da savjetuju oko kritičnih točaka u procesima i općenito u poslovanju.

Utvrđivanje ključnih dobavljača sljedeći je korak. Taj korak ima ulogu da se utvrdi koji su dobavljači prema važnim kriterijima bitni za poslovanje, s kojima od njih radimo često, bez čije podrške nikako ne bismo mogli funkcionirati, za koje od njih obavezno treba imati „u pripremi plan B“ za slučaj da nisu u mogućnosti dobaviti nam robu/uslugu koju od njih nabavljamo.

Potrebno je utvrditi rizike koji su povezani sa svakim od utvrđenih dobavljača te razmotriti ranjivosti sustava, koje mogu nastati i biti iskorištene na našu štetu.

Na kraju nužno je utvrditi kojim aktivnostima možemo smanjiti/izbjeći rizike ili njihov učinak. Primjerice neke od aktivnosti kojima se može zaobići prepoznate rizike i slabosti je pripremiti plan diverzificiranja dobavljača, predvidjeti planove za nepredviđene situacije za ključne poslovne procese, prilikom ugovaranja poslova s dobavljačem pravovremeno dogovoriti pravila postupanja za osiguranje kontinuiteta poslovanja (engl. business continuity).

3. Rješavanje ranjivosti

Proces rješavanja ranjivosti nije definiran NIS 2 Direktivom, propisana je samo obaveza da se ranjivosti trebaju rješavati. Kao pomoć u pronalaženju adekvatnih rješenja trebaju poslužiti potvrđene dobre prakse i rezultati istraživanja u tom području. Istraživanja provode najčešće nadležna tijela (npr. ENISA) i eminentnih stručnjaka. U nastavku će biti ukratko predstavljena dva aktualna izvora u kojima su sadržane korisne informacije o rezultatima istraživanja – u izdanju ENISA-e.

ENISA je 2021. godine objavila publikaciju (ENISA, 2021) u kojoj se daje pregled prijetnji za napade na lanac opskrbe. U cilju što bolje komunikacije s dionicima u području kibernetičke sigurnosti opisani su tipovi prijetnji za napade na lanac opskrbe (ENISA, 2021). U navedenom dokumentu opisana je taksonomija za napade na opskrbni lanac. Taksonomija se sastoji od četiri dijela: (i) tehnike napada na dobavljača, (ii) napadnuta imovina dobavljača, (iii) tehnike napada na kupca, (iv) napadnuta imovina kupca.

Dobavljač		Kupac	
tehnike napada	napadnuta imovina	tehnike napada	napadnuta imovina
Infekcija zlonamjernim softverom	Postojeći softver	Odnos od povjerenja	Podaci
Društveni inženjering	Softverske knjižnice	Zasnovanost na kompromisu	Osobni podaci
Napad grubom silom	Kôd	Krađa identiteta	Intelektualno vlasništvo
Iskorištavanje ranjivosti softvera	Konfiguracije	Infekcija zlonamjernim softverom	Softver
Iskorištavanje ranjivosti konfiguracije	Podaci	Fizički napad ili modifikacija	Procesi
Inteligencija otvorenog kôda	Procesi	Krivotvorina	Širokopojasni pristup
	Hardver		Financije
	Zaposlenici		Zaposlenici
	Dobavljač		

Izvor: ENISA (2021), Tablica 1, stranica 7.

Tehnike napada odnose se na "kako" se napad dogodio, a ne na "što" je korišteno za napad. U nastavku su navedeni i primjeri za pojedine tehnike napada.

Tehnike napada na dobavljača	Primjer
Infekcija zlonamjernim softverom	Špijunski softver koji se koristi za krađu vjerodajnica od zaposlenika
Društveni inženjering	Krađa identiteta, lažne aplikacije, tipkarske greške, lažno predstavljanje putem Wi-Fi mreže, uvjeravanje dobavljača da nešto učini
Napad grubom silom	Pogađanje SSH lozinke, pogađanje web prijave
Iskorištavanje ranjivosti softvera	Iskorištavanje SQL ubacivanja ili prekoračenja međuspremnika u aplikaciji.
Iskorištavanje ranjivosti konfiguracije	Iskorištavanje problema u konfiguraciji uređaja
Inteligencija otvorenog kôda	Pretraživanje vjerodajnica na mreži, API ključeva, korisničkih imena.
Fizički napad ili modifikacija	Modificirati hardver, fizički upad
Krivotvorina	Imitacija USB-a u zlonamjerne svrhe

Izvor: ENISA (2021), Tablica 2, stranica 8.-9.

Napadnuta imovina dobavljača	Primjer
Postojeći softver	Softver koji koristi dobavljač, web poslužitelji, aplikacije, baze podataka, sustavi za nadzor, aplikacije u oblaku, firmware. Ne uključuje softverske biblioteke
Softverske knjižnice	Biblioteke trećih strana, softverski paketi instalirani od trećih strana kao što su npm, ruby itd
Kôd	Izvorni kod ili softver koji proizvodi dobavljač
Konfiguracije	Lozinke, API ključevi, pravila vatrozida, URL-ovi
Podaci	Podaci o dobavljaču, vrijednosti sa senzora, certifikati, osobni podaci kupaca ili samih dobavljača, osobni podaci
Procesi	Ažuriranja, sigurnosne kopije ili procesi provjere valjanosti, procesi potpisivanja certifikata
Hardver	Hardver proizveden od strane dobavljača, čipovi, USB
Zaposlenici	Ciljane pojedince s pristupom podacima, infrastrukturi ili drugim ljudima.

Izvor: ENISA (2021), Tablica 3, stranica 9.

Tehnike napada na kupca	Primjer
Odnos od povjerenja	vjerujte certifikatu, vjerujte automatskom ažuriranju, vjerujte automatskom sigurnosnom kopiranju.
Zasnovanost na kompromisu	zlonamjerne skripte na web stranici za zarazu korisnika zlonamjernim softverom
Krađa identiteta	poruke koje lažno predstavljaju dobavljača, lažne obavijesti o ažuriranju
Infekcija zlonamjernim softverom	Trojanski konj s udaljenim pristupom (RAT)..
Fizički napad ili modifikacija	modificirati hardver, fizički upad
Krivotvorina	stvoriti lažni USB, modificirati matičnu ploču, lažno predstavljanje osoblja dobavljača

Izvor: ENISA (2021), Tablica 4, stranica 9.

Napadnuta imovina kupca	Primjer
Podaci	podaci o plaćanju, video izvori, dokumenti, e-pošta, planovi leta, podaci o prodaji i financijski podaci, intelektualno vlasništvo
Osobni podaci	podaci o kupcima, evidencija zaposlenika, vjerodajnice
Intelektualno vlasništvo	
Softver	pristup izvornom kodu proizvoda kupca, izmjena softvera kupca
Procesi	dokumentacija internih procesa rada i konfiguracija, umetanje novih zlonamjernih procesa, dokumenti shema
Širokopojasni pristup	koristiti širinu pojasa za Distributed Denial of Service (DDoS), slati SPAM ili zaraziti druge u velikim razmjerima
Financije	ukrasti kriptovalute, oteti bankovne račune, transfere novca
Zaposlenici	ciljani pojedinci zbog svog položaja ili znanja

Izvor: ENISA (2021), Tablica 5, stranica 10.

Preporuke za kontrolu kibernetičke sigurnosti temeljene na standardima ISO/IEC 27002, ISO 9001 i ISO 31000, prema ENISA (2021) za kupce su:

- identificirati i dokumentirati vrste dobavljača i pružatelja usluga,
- definirati kriterije rizika za različite vrste dobavljača i usluga (npr. važne ovisnosti o dobavljačima i kupcima, kritične ovisnosti o softveru, pojedinačne točke kvara),
- procijeniti rizike opskrbnog lanca prema vlastitim procjenama i zahtjevima utjecaja na kontinuitet poslovanja,
- definirati mjere za tretman rizika na temelju dobre prakse,
- nadzirati rizike i prijetnje lanca opskrbe, na temelju unutarnjih i vanjskih izvora informacija i na temelju rezultata praćenja i pregleda učinka dobavljača,
- svoje osoblje upoznati s rizikom.

S druge strane prema ENISA (2021), dobavljačima se preporuča:

- osigurati da infrastruktura koja se koristi za projektiranje, razvoj, proizvodnju i isporuku proizvoda, komponenti i usluga slijedi prakse kibernetičke sigurnosti prema ISO/IEC 27001,
- implementirati proces razvoja proizvoda, održavanja i podrške koji je u skladu s općenito prihvaćenim procesima razvoja proizvoda,
- implementirati proces sigurnog inženjeringa koji je u skladu s općenito prihvaćenim sigurnosnim praksama,
- razmotriti primjenjivost tehničkih zahtjeva na temelju kategorije proizvoda i rizika,
- nuđenje Izjava o sukladnosti kupcima za poznate standarde (ISO/IEC 27001 i druge) i osiguravanje i potvrđivanje, u mjeri u kojoj je to moguće, integriteta i podrijetla softvera otvorenog kôda, koji se koristi unutar bilo kojeg dijela proizvoda,
- definirati ciljeve kvalitete kao što je broj nedostataka ili eksterno identificiranih ranjivosti ili eksterno prijavljenih sigurnosnih problema i koristiti ih kao instrument za poboljšanje ukupne kvalitete,
- održavati točne i ažurne podatke o podrijetlu softverskog kôda ili komponenti, te o kontrolama primijenjenim na interne i softverske komponente, alate i usluge trećih strana prisutnih u procesima razvoja softvera,
- provoditi redovite revizije kako bi se osiguralo da su gore navedene mjere ispunjene.

Drugi praktično primjenjiv izvor je publikacija autora Papaphilippou, Konstantinos i Marianthi (2023) koji su izradili priručnik u kojem je opisana dobra praksa za kibernetičku sigurnost u dobavnom lancu, a isti je objavljen od strane ENISA-e. U nastavku autorica prenosi nekoliko navoda autora spomenute publikacije:

a) autori su u publikaciji objavili rezultate istraživanja provedenog u razdoblju od travnja do lipnja 2022. godine. Istraživanjem je obuhvaćeno najmanje 40 poduzeća (raznih veličina prema kriteriju broja zaposlenih) iz svake zemlje članice EU,
b) anketirana poduzeća bave se bankarstvom, digitalnom infrastrukturom, opskrbom i distribucijom pitke vode, energijom, infrastrukturom financijskog tržišta, zdravstvom, prometom ili su pružatelji digitalnih usluga (računalstvo u oblaku, internetska tržišta, internetske tražilice),
c) rezultati istraživanja pokazali su da 86% ispitanih poduzeća ima odobrene IKT/OT (engl. Operational Technology) politike upravljanja rizikom kibernetičke sigurnosti u opskrbnom lancu na snazi,
d) samo 47 % anketiranih organizacija u EU-u planiralo je financijska sredstva za kibersigurnost IKT/OT lanca opskrbe, dok većina anketiranih organizacija (53%) nema odobrena financijska sredstva za takva pitanja,
e) poduzeća bi trebala biti svjesna da implementacija praksi i kontrola kibernetičke sigurnosti lanca opskrbe IKT/OT-a zahtijeva dodatne financijske i ljudske resurse,
f) istraživanjem je utvrđeno da samo 24% anketiranih organizacija ima definirane uloge i odgovornosti za kibersigurnost IKT/OT lanca opskrbe. Većina ispitanih organizacija (76%) nema za predmetna pitanja osigurane ekvivalente punog radnog vremena (engl. full-time equivalents FTE). Također, 59% anketiranih organizacija koje imaju upravljanje rizikom treće strane (engl. third party risk management TRM) politike također imaju namjenski proračun ili proračunsku liniju za sigurnost opskrbnog lanca,
g) na pitanje koje su tehnike za smanjenje rizika kibernetičke sigurnosti u lancu opskrbe IKT/OT-a usvojene, 61% ispitanih organizacija dalo je prednost sigurnosnim certifikatima, a odmah nakon njih slijede usluge ocjenjivanja sigurnosnog rizika (43%) i dužna pažnja ili procjene rizika (37%). Samo 9% ispitanih organizacija navodi da ni na koji način ne procjenjuju sigurnosne rizike u lancu opskrbe,
h) na pitanje o normalnom trajanju otklanjanja kritičnih ranjivosti na IKT imovini, 46% ispitanih je navelo da su ih otklonili unutar manje od 1 mjeseca, dok je drugih 46% navelo da su otklonili unutar 6 mjeseci.

Temeljem rezultata istraživanja (Papaphilippou, Konstantinos i Marianthi, 2023) zaključeno je da su ispitane organizacije svjesne važnosti kibersigurnosti u opskrbnom lancu no ne izdvajaju financijske resurse u dovoljnoj mjeri za rješavanje tog pitanja. Također, bankarstvo kao djelatnost je najdalje dosegnula praktičnu primjenu mjera kibernetičke sigurnosti, a što u značajnoj mjeri potvrđuje i činjenica da je donošenjem NIS 2 Direktive bankarstvo ostalo u obvezi primjenjivati odredbe Digital Operational Resilience Act[3] (DORA) koji je namijenjen financijskom sektoru. Zanimljivo je i to da su se brojni ispitanici izjasnili da se oslanjaju na

[3] REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

certifikate kao najpoželjniji način za praćenje kibernetičke sigurnosti dobavljača, no to zahtijeva značajna financijska sredstva. Većina anketiranih organizacija izjasnila se da nema sustav upravljanja ranjivostima koji pokriva svu organizacijsku imovinu. Ispitanici su osviješteni da upravljanje ranjivostima i testiranje proizvoda doprinose boljoj kibersigurnosti IKT/OT lanca opskrbe.

4. Zaključak

Dinamično okruženje, digitalizacija B2B (engl. Business to Business) poslovnih procesa, interoperabilnost donose sa sobom pojačani rizik od kibernetičkih napada kojima se iskorištavaju ranjivosti pojedinih komponenti sustava. Opskrbni lanci podrazumijevaju isprepletenost svih mogućih kategorija poslovnih subjekata, a na kraju uključuju i fizičke osobe - kupce. Kibernetički napadi na dobavljače i kupce, opisani tehnikama i primjerima u ovom članku, najčešći su do sada zabilježeni oblici napada. Treba imati na umu da je područje kibernetičke sigurnosti vrlo dinamično te da je posebno važno održati kontinuitet u posvećenosti sigurnosnim mjerama, njihovoj primjeni i očekivanim učincima.

Očuvanjem kibernetičke sigurnosti unutar vlastitog sustava doprinosi se i očuvanju sigurnosti okruženja u kojem djelujemo.

Reference

1. ENISA (2021), 'Threat landscape for supply chain attacks', preuzeto https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, pristupljeno 2. kolovoza 2024.
2. Europska Komisija, (2022), DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a highcommonlevelofcybersecurityacrossthe Union, amendingRegulation (EU) No 910/2014 andDirective (EU) 2018/1972, andrepealingDirective (EU) 2016/1148 (NIS 2 Directive), preuzeto https://eur-lex.europa.eu/eli/dir/2022/2555/oj, pristupljeno 10. svibnja 2024.
3. ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure, preuzeto https://www.iso.org/standard/72311.html, pristupljeno 4. kolovoza 2024.
4. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, preuzeto https://www.iso.org/standard/75652.html, pristupljeno 4. kolovoza 2024.
5. ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes, preuzeto https://www.iso.org/standard/69725.html, pristupljeno 4. kolovoza 2024.
6. „Narodne novine" br. 14/24, Zakon o kibernetičkoj sigurnosti, preuzeto https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html, pristupljeno 12. lipnja 2024.
7. Papaphilippou, M., Konstantinos, M. and Marianthi, T. (2023). "Good Practices For Supply Chain Cybersecurity." ENISA, June 2023., preuzeto s https://www.enisa.europa.eu/publications/good-practices-for-supplychain-Cybersecurity, pristupljeno 8. kolovoza 2024.

O autorici

Doc. dr. sc. Robertina Zdjelar doktorirala je u području društvenih znanosti, polje informacijske i komunikacijske znanosti 2022. godine. Tijekom 2024. godine autorica je izabrana u znanstveno-nastavno zvanje naslovni docent. Bavi se istraživanjem u području informacijskih i komunikacijskih znanosti, stručnim radovima u području javnih politika, financija, računovodstva i kontrolinga. Angažirana je kao vanjski suradnik na Sveučilištu u Zagrebu na Fakultetu organizacije i informatike Varaždin te na Pravnom fakultetu u Zagrebu te na Geotehničkom fakultetu u Varaždinu. Djelovanje na Fakultetu organizacije i informatike odnosi se na upravljanje kvalitetom u informatici, kvalitetu i mjerenja u informatici, upravljanje primjenom informacijske tehnologije u poslovanju, odgovornost, inkluzija i održivost u informatici. Na Pravom fakultetu u Zagrebu autorica je održala nekoliko predavanja na temu upravljanja projektima. Na Geotehničkom fakultetu u Varaždinu održala je tribinu pod naslovom "Umjetna inteligencija i gospodarenje otpadom".

U poslovnom okruženju autorica je zaposlenik Gradskog komunalnog poduzeća Komunalac d.o.o. kao direktorica Sektora financija, računovodstva, kontrolinga i EU projekata, a u okviru kojega se nalaze i druge poslovne funkcije važne za poslovanje društva. Zadnjih osam godina zaposlena je u društvu Komunalac, čemu je prethodilo dvadeset godišnje radno iskustvo u Koprivničko-križevačkoj županiji na raznim pozicijama, od pripravnika, suradnika do pročelnice za financije, proračun i javnu nabavu.

Autorica posjeduje brojne stručne certifikate od kojih treba istaknuti ***NIS2 Directive Lead Implementer, ISO 27001 interni auditor, ISO 9001 Lead auditor***, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata.