Doc. dr. sc. Robertina Zdjelar

Upravljanje rizicima u kontekstu NIS 2 Direktive

Sažetak

Uskladba poslovanja s NIS 2 Direktivom složen je projekt koji podrazumijeva inicijalno implementiranje upravljačkih procesa u različitim aspektima , između ostaloga i upravljanje rizicima. Upravljanje rizicima podrazumijeva standardne aktivnosti o kojima će autorica dati kratak pregled u članku.

Ključne riječi: kibernetička sigurnost, rizik, mjere upravljanja rizicima, NIS 2 Direktiva,

1. Uvod

Kada govorimo o upravljanju rizicima s aspekta kibernetičke sigurnosti i primjene NIS 2 Direktive (EK, 2022) prije svega treba reći da je Recitalom 7. definirano da *„Ključni i važni subjekti u velikoj mjeri snose odgovornost za osiguravanje sigurnosti mrežnih i informacijskih sustava. Trebalo bi* ***promicati i razvijati kulturu upravljanja rizicima****, uključujući procjene rizika i provedbu mjera upravljanja kibersigurnosnim rizicima primjerenih rizicima s kojima se suočava.“*

Recital 59. NIS 2 Direktive kaže: *„Komisija, ENISA i države članice trebale bi* ***nastaviti poticati usklađivanje s međunarodnim normama i postojećim najboljim praksama*** *u industriji u području upravljanja kibersigurnosnim rizicima, na primjer u područjima procjene sigurnosti lanca opskrbe, razmjene informacija i otkrivanja ranjivosti.“*

Članak 21. NIS 2 Direktive govori o ***mjerama upravljanja kibersigurnosnim rizicima.*** Navedeno obvezuje „*Države članice da 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*.“ NIS 2 Direktiva preporuča, ako je primjenjivo, implementirati relevantne europske i međunarodne norme vezane za upravljanje rizicima.

Zakonom o kibernetičkoj sigurnosti („Narodne novine“ 14/24) (dalje u tekstu: Zakon) definirani su pojmovi*: rizik, mjere upravljanja kibernetičkim sigurnosnim rizicima i primjena mjera.*

Prema članku 4. Zakona *„Rizik je mogućnost gubitka ili poremećaja uzrokovana incidentom koji se izražava kao kombinacija opsega takvog gubitka ili poremećaja i vjerojatnosti pojave tog incidenta.*“ .

Člankom 26. Zakona propisano je da su „*Ključni i važni subjekti dužni provoditi odgovarajuće i razmjerne mjere upravljanja kibernetičkim sigurnosnim rizicima. Cilj je primjene mjera upravljanja kibernetičkim sigurnosnim rizicima zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata, uzimajući pritom u obzir sve opasnosti kojima su ti sustavi izloženi.*„.

Nadalje, kada je riječ o mjerama upravljanja kibernetičkim rizicima, prema članku 26. stavku 3. Zakona one obuhvaćaju:

- „*tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ključni i važni subjekti služe u svom poslovanju ili u pružanju svojih usluga te*
- *mjere za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na mrežne i informacijske sustave ključnih i važnih subjekata, primatelje njihovih usluga ili na druge sektore, subjekte i usluge.“*

Nezaobilazan dio metodologije upravljanja rizicima je procjena rizika, odnosno procjena izloženosti subjekta rizicima, veličina subjekta, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni i gospodarski učinak.

Cilj upravljanja rizicima u kontekstu kibernetičke sigurnosti je zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata.

Proces upravljanja rizicima uključuje: a) politike analize rizika i sigurnosti informacijskih sustava; (b) postupanje s incidentima; (c) kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama; (d) sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga; (e) sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući rješavanje ranjivosti i njihovo otkrivanje; (f) politike i postupke za procjenu djelotvornosti mjera upravljanja kibersigurnosnim rizicima; (g) osnovne prakse kiberhigijene i osposobljavanje o kibersigurnosti; (h) politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja; (i) sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom; (j) korištenje višefaktorske provjere autentičnosti ili rješenja kontinuirane provjere autentičnosti, zaštićene glasovne, video i tekstualne komunikacije te sigurnih komunikacijskih sustava u hitnim slučajevima unutar subjekta, prema potrebi.

Kibernetička sigurnost u lancu opskrbe obrađen kao zasebna tema.

Kako se NIS 2 Direktiva poziva na poticanje usklađenja poslovanja s međunarodnim normama i postojećim najboljim praksama:

- ISO/IEC 27005:2022 osigurava informacije o upravljanju rizicima vezanim uz informacijsku sigurnost i može se isto tako koristiti u pripremi i provedbi mjera za kibernetičku sigurnost sustava (engl. Information security, cybersecurity and privacy protection - Guidance on managing information security risks).

- ISO/IEC 27001:2022 Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti - zahtjevi (engl. Information security, cybersecurity and privacy protection — Information security management systems — Requirements)

- ISO/IEC TS 27100:2020 Informacijska tehnologija – kibernetička sigurnost – pregled i koncepti (engl. Information technology — Cybersecurity — Overview and concepts)

- ISO 31000:2018 Upravljanje rizicima - upute (engl. Risk management – Guidelines, par. 6.3.3.)

- IEC 31010:2019 – Tehnike procjene rizika (engl. Risk management — Risk assessment techniques)

- osim ISO postoji i NIST okvir za određivanje dosegnute razine upravljanja rizicima (NIST, 2024) (engl. NIST Cybersecurity Framework), s četiri razine implementiranosti upravljanja rizicima.

Kao pomoć pri uspostavi procesa upravljanja rizicima ENISA je u veljači 2023. godine izdala Interoperabilni alat na nivou EU za upravljanje rizicima (ENISA, 2023) (engl. Interoperable EU Risk Management Toolbox). Navedeni alat integrira različite metode upravljanja rizicima te osnovne procese uključujući identifikaciju i kategorizaciju imovine, identifikaciju prijetnji, različite scenarije mogućih napada i procjenu razine izloženosti riziku. Detaljnije o navedenom biti će govora u sljedećem poglavlju.

2. ENISA Alat za upravljanje rizicima

Razvijeni alat predstavlja pregled relevantnih tema iz područja upravljanja rizicima. Koncept se zasniva na definiranu obuhvata i radnog okvira, procjeni rizika, postupanju s rizicima, prihvaćanju rizika, nadziranje i pregled, komuniciranje o rizicima.

Opis obuhvata podrazumijeva opis vanjskog i unutarnjeg okruženja, generiranje konteksta za upravljanje rizicima i formuliranje kriterija za procjenu značaja rizika. Procjena rizika podrazumijeva identifikaciju rizika, analizu relevantnosti prema zadanim mjerilima, evaluaciju. Postupanje s rizicima podrazumijeva utvrđivanje mogućih opcija, razvoj plana djelovanja, potvrdu odnosno odobravanje plana djelovanja, provedbu plana djelovanja i identifikaciju rezidualnih rizika. Ukoliko se neke rizike ne može izbjeći/smanjiti/prenijeti tada je važno osvijestiti informaciju da takve rizike treba prihvatiti i pratiti. S tom činjenicom prije svega mora biti upoznata odgovorna osoba ključnog i važnog subjekta.

3. Aktivnosti upravljanja rizicima

Standardna metodologija upravljanja rizicima prema ISO/IEC 27005:2022 uključuje sljedeće aktivnosti:

- utvrđivanje konteksta organizacije
- identifikaciju rizika
- analizu rizika
- evaluaciju rizika
- djelovanje na rizike
- komunikaciju i konzultacije

- vođenje zapisa o rizicima i izvješćivanje
- praćenje rizika i pregled.

Sažeti opis svake od aktivnosti nalazi se u nastavku članka.

3.1. Utvrđivanje konteksta organizacije

Utvrđivanje konteksta organizacije podrazumijeva sagledavanje vanjskog okruženja i unutarnjeg stanja i činjenica važnih za obuhvat upravljanja rizicima. Vanjski kontekst sagledava se primjenom uobičajenih metoda analize SW**OT**[1] pri čemu se fokusiramo na mogućnosti (engl. Opportunities) i prijetnje (engl. Treats), analize pet Porterovih sila (Gerard, Bruijl, 2019) i/ili PESTLE analize (Ghez, Ghez, 2019). Opis okruženja pomoću spomenutih metoda analize treba osigurati dovoljno informacija koje u kasnijim fazama omogućavaju prepoznavanje mogućih rizika. Svaki ključni i važni subjekt djeluje u okruženju čiji opis treba sagledavati s kulturološkog, društvenog, političkog, zakonodavnog, ekonomskog, tehnološkog aspekta, a što zasigurno ima utjecaj na ciljeve i na njihovo ostvarenje. Uloga vanjskih dionika (konkurencija, kupci, zakonodavstvo) može imati značajan utjecaj na ostvarenje organizacijskih ciljeva te je stoga posebno važno imati saznanja o ciljevima druge strane.

Sagledavanje organizacije s perspektive unutarnjih faktora podrazumijeva analizu vlastitih snaga (engl. Strengths) i slabosti (engl. Weakness), a što je dio **SW**OT analize. Rizici mogu proizlaziti iz upravljačke strukture i upravljanja, organizacijske strukture, uloga i odgovornosti, politika, ciljeva i strategija. Također ključni rizici u ovoj kategoriji mogu proizlaziti iz raspoloživosti ključnih resursa (ljudskih, vremenskih, materijalnih, financijskih, tehnoloških). Kod rizika u kontekstu NIS 2 Direktive obavezno je sagledati i utjecaj informacijskih sustava koji su u upotrebi, tijeka informacija i odlučivanja. U unutarnje faktore koji mogu biti izvor rizika svakako treba spomenuti i organizacijsku kulturu, standarde koji se koriste (ovisno i kako se koriste).

3.2. Identifikacija rizika

Identifikacija rizika podrazumijeva aktivnost kojom se utvrđuju/prepoznaju rizici u opisanom kontekstu iz točke 3.1. Identifikacija uključuje prepoznavanje. Opisivanje rizika neophodno je radi suštinskog razumijevanja i kako bi se organizacija mogla zaštiti od nastanka štete koju može uzrokovati štetni događaj. Osim samog prepoznavanja rizika potrebno je utvrditi imovinu, prijetnje kojima ona može biti izložena, postojeće kontrole ako ih ima, ranjivosti i nositelje koji će biti odgovorni za postupanje s rizicima.

Prema ISO 31000:2018 kod identifikacije rizika važno je razmotriti materijalne i nematerijalne izvore rizika, uzroke i događaje, prijetnje i prilike, ranjivosti i sposobnosti, promjene u vanjskom i unutarnjem okruženju organizacije, pouzdanost informacija na osnovu kojih se donose odluke, neinformiranost, utjecaj koji može imati protek vremena (zastarijevanje informacija na temelju kojih se donose odluke i poduzimaju aktivnosti).

[1] https://onlinelibrary.wiley.com/doi/abs/10.1002/(SICI)1099-1697(199803/04)7:2%3C101::AID-JSC332%3E3.0.CO;2-6, pristupljeno 10.3.2023

Prema ISO/IEC 27005:2022 prepoznavanje sigurnosnih rizika može se temeljiti ***na osnovi događaja*** ili ***na osnovu imovine***. Kod prepoznavanja rizika po događajima važno je sagledati utjecaj koji rizik može imati na ostvarenje ciljeva. Kod prepoznavanja rizika kojima može biti izložena imovina važno je sagledati ranjivosti i prijetnje zbog kojih imovina može biti ugrožena. Kada je riječ o imovini s aspekta informacijske sigurnosti imovina se dijeli na primarne informacije i procese koji su važni za organizaciju i na potpornu imovinu koju čine komponente informacijskog sustava na kojima je poslovna imovina stavljena u funkciju. Primarna informacijska imovina od vitalnog je značaja za ostvarenje misije organizacije. Tu svakako spadaju evidencije o zaposlenima, kupcima/korisnicima usluga, strateški plan organizacije, postavke i parametri mreže, računovodstveni podaci, intelektualno vlasništvo poput patenata i slično. Pod potpornom imovinom se smatra sve što čini resurse nužne da bi se mogli voditi zapisi o primarnoj imovini. U naravi bi u tu kategoriju spadao hardver, programska podrška, računalna mreža, organizacijska struktura i zaposlenici, odnosno njihove vještine rada s informacijsko komunikacijskom tehnologijom (IKT).

Prepoznavanje prijetnji važno je radi pravovremenog definiranja postupanja u slučaju nastanka istih, što podrazumijeva donošenje odluke o aktivnostima koje su odgovor na prijetnje. Prijetnje treba kontinuirano prepoznavati jer svaka promjena u vanjskom ili unutarnjem okruženju može stvoriti situaciju iz koje može nastati ranjivost. Kontinuirano je potrebno nadzirati postojeće kontrole, jesu li dovoljno učinkovite u odnosu na moguće nove scenarije.

Izvori prijetnji mogu se grupirati na: zaposlenike (nepažnja, neprepoznavanje lažnog predstavljanja, ljudska pogreška), konfiguraciju sustavu i okruženja (imovina implementirana u nezaštićenom području, otvorenost sustava koji razmjenjuje podatke putem javne IKT mreže), infrastrukturu (ovisnost o napajanju samo iz vanjske energetske mreže), dobavljače i IKT dobavni lanac.

Postojeće sigurnosne kontrole moraju biti uspostavljene na način da sustav kontrole bude učinkovit i djelotvoran, da uloge i odgovornosti budu jasno definirane, da odredi vremenski plan provođenja kontrola. Prepoznavanje ranjivosti pomoću automatiziranih alata, penetracijski testovi i testiranje koda samo su neki od načina ovladavanja ranjivostima sigurnosti sustava.

3.3. Analiza rizika

Analizu rizika treba provesti sagledavajući različite aspekte ugroza. Posebno je važno utvrditi vjerojatnost nastanka događaja i težinu posljedica koje isti može imati po kibernetičku sigurnost sustava. Važno je sagledati prirodu posljedica i njihov utjecaj na sigurnost.

Analiza rizika aktivnost je u kojoj se na različitim razinama detaljnosti rizici mogu sagledavati. Dostupnost informacija o nekom riziku i vjerodostojnost nastanka štetnog događaja ključne su za kvalitetu rezultata analize.

Rezultati analize potrebni su za evaluaciju i donošenje odluke o djelovanju na rizike (prioriteti) i o načinu na koji će se djelovati. Ujedno daljnji postupak podrazumijeva donošenje strategije postupanja s rizicima i metode koje se pri tome koriste.

Procjena potencijalnih posljedica potrebna je zbog sigurnosti informacija koja može biti narušena. ***Sigurnost informacija očituje se kroz osiguranje i zaštitu povjerljivih informacija, integritet informacija i dostupnost***. Gubitak bilo kojeg od svojstava ili šteta zbog gubitka može ugroziti ugled ključnog i važnog subjekta ili onemogućiti ga u ostvarenju ciljeva. Kod analize potencijalnih posljedica ugroze informacijske sigurnosti treba utvrditi što će se dogoditi ako nastupi štetni događaj i bude ugrožena povjerljivost, integritet ili dostupnost informacije, a tu procjenu može sveobuhvatno provesti osoba koja se smatra „imateljem“ rizika (engl. risk owner). Kod procjene treba sagledavati i po mogućnosti vrijednosno iskazati štetu koja nastaje uslijed štetnog događaja i svakako procijeniti troškove koji mogu biti neophodni za vraćanje sustava u prvobitno stanje.

Procjena vjerojatnosti nastanka štetnog događaja podrazumijeva utvrđivanje mogućnosti nastanka nekog rizičnog scenarija na osnovi iskustva, prema izvoru ugroze, prema prepoznatim slabostima ili ranjivosti vlastitog sustava ili s obzirom na razinu sigurnosti koju osiguravaju postojeće kontrole.

Rezultati procjene posljedica i procjene vjerojatnosti nastanka rizičnog događaja zajedno daju razinu rizika (matrica). ENISA je dala preporuku za određivanje stupnjeva/razina vjerojatnosti i posljedica temeljem čega se definira matrica rizika po kojoj se dalje radi evaluacija. Primjerice matrica 5×5 daje kategorije (ukupno 25 mogućih):

a) za vjerojatnost: od sigurno (najviši stupanj), vrlo vjerojatno, vjerojatno, manje vjerojatno, nije moguće (najniži stupanj)

b) za kriterij utjecaja odnosno posljedica raspon ide od: katastrofa (najveća moguća šteta), kritično, ozbiljno, značajno, nebitno (gotovo da nema štete).

3.4. Evaluacija rizika

Evaluacijom se rizici ocjenjuju prema gore opisana dva kriterija: vjerojatnost nastanka štetnog događaja i utjecaj koji štetni događaj može imati. Svrha evaluacije rizika je utvrđivanje razine važnosti (prioriteti) prepoznatih rizika radi donošenja daljnjih odluka o djelovanju na rizike.

Na evaluaciji rizika provode osim osobe koja je zadužena za pojedini rizik („imatelj“, engl.. owner) rade i drugi poslovni i tehnički specijalisti kako bi se evaluacija provela sagledavajući širi aspekt te kako bi rizici bili rangirani što realnije.

Prioritet za rješavanje svakako trebaju imati rizici koji imaju značajan utjecaj odnosno štetne posljedice većih razmjera po zaštitu povjerljivosti, integriteta, dostupnosti informacija i imovine te kod kojih je vjerojatnost nastanka događaja visoka.

Uvođenje mjera osiguranja informacijske sigurnost, ali i kibernetičke sigurnosti sustava u cjelini od rizika visokog prioriteta zahtijeva angažman dodatnih resursa (ljudskih, financijskih, tehničkih).

3.5. Djelovanje na rizike

Djelovanje na prepoznate i evaluirane rizike može biti usmjereno u više pravaca. Postavlja se pitanje kako postupati s rizicima, odnosno koja je razina postupanja optimalna? Nekoliko je mogućih načina postupanja s rizicima: a) izbjegavanje rizika; b) smanjenje rizika; c) dijeljenje rizika i d) prihvaćanje rizika.

Izbjegavanje rizika moguće je postići na način da se aktivnosti koje potencijalno dovode do rizičnog događaja prestanu provoditi ili da se način provođenja aktivnosti promijeni/poboljša. Smanjenje rizika podrazumijeva uvođenje/provođenje kontrola nakon čega ostaje samo rezidualni rizik koji je u granici prihvatljivog. Dijeljenje rizika podrazumijeva scenario u kojem pronalazimo partnera s kojim bi se mogao rizik podijeliti (npr. dijeljene usluge, osiguranje i sl). Naposljetku prihvaćanje rizika je scenario u kojem najčešće nema druge mogućnosti da se rizik izbjegne, smanji ili prenese, pa je u tom slučaju najbitnije odgovorne osobe osvijestiti o postojanju rizika i značenju prihvaćanja istoga.

Za postupanje s rizicima osim definiranja optimalnog scenarija za postupanje za svaki od rizika potrebno je usvojiti Plan postupanja s rizicima. U Plan se uključuju oni rizici koji su visoko na listi prioriteta (vjerojatnost nastanka i utjecaj koji mogu imati). Planom treba za svaki rizik biti utvrđeno koje kontrole će biti ključne za smanjenje ili izbjegavanje rizika i kako su odabrane kontrole povezane s okruženjem u koje se moraju implementirati. Kontrole mogu biti preventivne, korektivne ili detektivne. Postupanje s rizicima zahtijeva resurse (ljudske, vrijeme, materijalne) bez čega implementacija kontrole nije provediva. O tom segmentu također treba voditi računa kod kreiranja i odobrenja Plana postupanja s rizicima. Mjerljivost razine rizika očituje se kroz mjerljive indikatore čije vrijednosti treba pratiti prije i nakon uvođenja kontrolnih aktivnosti.

Plan postupanja s rizicima treba biti potvrđen s osobama koje su prepoznate kao odgovorne za konkretan rizik. Osim opisa rizika u planu postupanja treba iskazati razinu rizika, prioritet, način postupanja, mjereni pokazatelj, potrebne resurse, odgovornosti, početni i završni rok za postupanje te po potrebi ažuriranje statusa nakon pregleda.

Već spomenuti rezidualni rizik predstavlja rizik koji ostaje nakon svih odrađenih kontrola, kojega nije moguće otkloniti provedenim aktivnostima, a o čemu trebaju biti informirane i osviještene odgovorne osobe ključnih i važnih subjekata.

3.6. Komunikacija i konzultacije

Komunikacija unutar subjekta vezano za upravljanje rizicima treba biti kontinuirana i pravovremena. Nastavno na već opisane aktivnosti u procesu upravljanja rizicima jasno je da u razmjeni informacija trebaju sudjelovati svi ključni dionici, od onih u čijoj domeni djelovanja se rizici procjenjuju, analiziraju i evaluiraju, do osobe koja je zadužena za proces upravljanja rizicima (eng. Risk manager) te uprava odnosno odgovorna osoba koja odgovara za poslovanje ključnog i važnog subjekta i ostvarenje ciljeva istoga.

Podizanje razine svijesti o postojanju rizika prvi je korak u cilju rješavanja istih i sprječavanja nastanka rizičnih situacija u kojima mogu zbog štetnih događaja biti ugroženi ljudi i imovina.

Direktna komunikacija putem radnih sastanaka i internih konzultacija omogućava neposrednu razmjenu ključnih informacija, koje često nisu i ne moraju biti dostupne širem krugu dionika, ovisno o konkretnom procesu/aktivnosti, imovini ili događaju kojeg se treba zaštititi.

Vrlo često, uslijed promjena unutarnjih i vanjskih faktora, dolazi do promjena ključnih informacija o rizicima (utjecaj, vjerojatnost, status, kontrole i sve ostalo spomenuto uz djelovanje) te je stoga važno svaku takvu promjenu pravovremeno komunicirati. Naročito je važno, biti ažuran u protoku informacija koje su vezane uz nove rizike.

Komunikacijskim planom definiraju se ključni dionici u procesu razmjene informacija, dodjeljuju se ovlaštenja tko, kada, prema kome, na koji način komunicira o rizicima. Treba imati na umu da je tema upravljanja rizicima uglavnom internog karaktera i zbog toga u komunikaciji treba biti izrazito oprezan.

3.7. Zapisi o rizicima i izvješćivanje

Kada je riječ o procesu upravljanja rizicima rezultate treba moći dokumentirati za što je neophodno vođenje zapisa i izvješćivanje. Što su rezultati procesa upravljanja rizicima i koji su njegovi učinci? U rezultate aktivnosti koje spadaju u proces upravljanja rizicima svakako su registar rizika, plan postupanja s rizicima i komunikacijski plan te dokumentacija kojom se potvrđuje odrađivanja aktivnosti postupanja s rizicima, prijenos informacija ključnih za rezidualne rizike.

U dokumentirane informacije o procesu upravljanja rizicima spada i definiranje kriterija za procjenu rizika te kriterija za utvrđivanje rizika koji su prihvatljivi. Metode prepoznavanja i analize rizika također je važno dokumentirati i opisati.

Učinak procesa upravljanja rizicima ukratko možemo opisati razinom stabilnosti poslovanja ključnog i važnog subjekta u ostvarenju njegovih ciljeva te sigurnost ljudi i imovine. Pravovremeno prepoznavanje rizika i određivanje prioriteta istoga nužne su pretpostavke za djelovanje. Odrađene mjere moraju biti dokumentirane kako bi se mogao pratiti napredak i poboljšanja u području stabilnosti i sigurnosti poslovanja.

3.8. Pregled i praćenje

Pregled dokumentiranih zapisa i praćenje stanja osiguravaju poboljšanja i napredak u postizanju željene razine sigurnosti/informacijske sigurnosti. Pregled i praćenje provodi se kontinuirano u svim aktivnostima uključenim u proces upravljanja rizicima, jer rizici nisu statični kao niti okruženje u kojem subjekt djeluje. Već je spomenuto u uvodu da je ključno sagledavati rizike kontinuirano, da je potrebno sagledavati rizike koji proizlaze iz unutarnjih (organizacijske, tehnološke, procesne) i vanjskih promjena (regulatorne, tržišne, političke i sl.). Kontinuirano praćenje učinaka uspostavljenih sigurnosnih mjera osigurava kvalitetu u upravljanju rizicima. Upravljanje rizicima može se smatrati preventivom za sigurnost sustava.

Zaključak

Za kraj, moglo bi se reći nakon opisane metodologije upravljanja rizicima da je glavni moto „bolje spriječiti nego liječiti“.

NIS 2 Direktivom propisano je da države članice EU imaju obvezu osigurati da subjekti, ključni i važni, implementiraju upravljanje rizicima radi osiguranja stabilnosti poslovanja i sigurnosti ljudi i imovine od kibernetičkih napada i drugih štetnih događaja.

ENISA je učinila dostupnim za korištenje alat za procjenu i upravljanje rizicima, koji se zasniva na definiranu obuhvata i radnog okvira, procjeni rizika, postupanju s rizicima, prihvaćanju rizika, nadziranje i pregled, komuniciranje o rizicima. Sve navedeno je sastavni dio osnovne metodologije za upravljanje rizicima.

Upravljanje rizicima u cjelokupnom projektu osiguranja kibernetičke sigurnosti temelj je za sljedeće faze procesa uskladbe poslovanja s NIS 2 Direktivom, pri čemu se svakako misli na upravljanje incidentima i upravljanje krizama, ako do štetnih događaja ipak dođe.

Reference

1. ENISA, (2023). ‘The Interoperabile EU risk management toolbox’, preuzeto https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox, pristupljeno 12. kolovoza 2024. godine
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. Gerard, H., Bruijl, T. (2019). The relevance of Porter's five forces in today's innovative and changing business environment. SSRN.
4. Ghez, J., Ghez, J. (2019). The Power of Analysis. Architects of Change: Designing Strategies for a Turbulent Business Environment, 95-109.
5. ISO 31000:2018 Upravljanje rizicima - upute, preuzeto https://www.iso.org/standard/65694.html?utm_source=google&utm_medium=ppc_paid_social&utm_campaign=iso31000&utm_content=gads01&gad_source=1&gclid=Cj0KCQjwj4K5BhDYARIsAD1Ly2r0Lv6pg0lFxdOwAThIjd36eYW_z7z3U7qJVRx2sNI5E4mvMr9Z2UwaAteEALw_wcB, pristupljeno 10. svibnja 2024.
6. IEC 31010:2019 Risk management — Risk assessment techniques, preuzeto https://www.iso.org/standard/72140.html, pristupljeno 10. svibnja 2024
7. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, preuzeto https://www.iso.org/standard/27001, pristupljeno 10. svibnja 2024.
8. ISO/IEC TS 27100:2020 Information technology — Cybersecurity — Overview and concepts, preuzeto https://www.iso.org/standard/72434.html, pristupljeno 10. svibnja 2024.
9. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks, preuzeto https://www.iso.org/standard/80585.html, pristupljeno 10. svibnja 2024.
10. National Institute of Standards and Technology (2024). Cybersecurity Framework, dostupno na https://www.nist.gov/cyberframework, February 26, 2024, pristupljeno 10. svibnja 2024.
11. Zakonom o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24)

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 i računovodstva. 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 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.