Doc. dr. sc. Robertina Zdjelar

Upravljanje krizama izazvanim kibernetičkim napadima u kontekstu NIS 2 Direktive

Sažetak

Širenje primjene digitalnih tehnologija i umjetne inteligencije u globalnim razmjerima, osim pozitivnih učinaka koje očekuju investitori, sa sobom donosi i rizik koji se značajno povećava s povećanjem stupnja ovisnosti o digitalnoj tehnologiji i umjetnoj inteligenciji. Svakodnevne životne navike gotovo su nezamislive bez upotrebe uređaja koji u osnovi ima informacijsko komunikacijsku tehnologiju (IKT). Upravo ta činjenica daje dovoljno snažan uvod koliko je važno biti informiran i spreman u slučaju nastanka krize izazvane kibernetičkim napadom.

Krizna stanja općenito zahtijevaju postupanje po posebnim protokolima iz više razloga. Prije svega kriza je situacija kada je nastali incident poprimio šire razmjere od onih koje bi bio u stanju riješiti jedan poslovni subjekt, jedna regija ili jedna država. U takvim kriznim situacijama teško je očekivati rješenje problema bez koordiniranog djelovanja i upravljanja. Kako je na samom početku rečeno, kibernetički napadi imaju za cilj onesposobiti svakodnevne životne aktivnosti što osim što narušava kvalitetu života čini i značajne štete velikih razmjera (ljudske, financijske, materijalne). U slučaju nastanka takve situacije treba postupati organizirano i koordinirano, zbog čega je potrebno upravljanje. Stoga se u ovom članku daje pregled zahtjeva i preporuka NIS 2 Direktive vezano uz krize izazvane kibernetičkim napadima, preporuke za primjenu standardizirane prakse, a biti će govora i o upravljanju krizama.

Ključne riječi: kibernetička sigurnost, kriza, mreža EU-CyCLONe, NIS 2 Direktiva, upravljanje krizama

1. Uvod

Prema enciklopediji Britannica[1] pojam ***krize*** definiran je kao „teška ili opasna situacija koja zahtijeva ozbiljnu pozornost“ (engl. „a difficult or dangerous situation that needs serious attention“).

Prema međunarodnom standardu ISO 22361:2022 Sigurnost i otpornost – Upravljanje krizama – Upute (engl. Security andresilience — Crisis management — Guidelines) u točki 3.2. definiran je pojam ***krize*** koji podrazumijeva „nenormalan ili izvanredni događaj ili

[1] https://www.britannica.com/dictionary/crisis, pristupljeno 05.11.2024.

situacija koja prijeti organizaciji ili zajednici i zahtijeva strateški, prilagodljiv i pravovremeni odgovor kako bi se očuvala njegova održivost i integritet“.

U povijesti čovječanstva prepoznate su i zabilježene razne krize (humanitarne, financijske, energetske…) od kojih je svaka ostavila posljedice, ali je i potaknula društvene skupine da u budućnosti uvedu mjere kojima se može potencijalne rizike staviti pod kontrolu i umanjiti učinak koji bi oni eventualno mogli imati.

Financijski sektor je kroz povijest svoju otpornost na krize razvijao radi zaštite konkurentnosti i stabilnosti Unije s gospodarskog i bonitetnog aspekta te aspekta ponašanja na tržištu. U Recitalu 5 Uredbe 2022/2554 se spominje da su sigurnost IKT-a i digitalna otpornost dio operativnog rizika, te da im nakon financijske krize nije posvećena prevelika pozornost u regulatornim planovima pa su se razvile samo u nekim područjima političkog i regulatornog okruženja Unije za financijske usluge ili samo u nekoliko država članica. Člankom 3. Uredbe 2022/2554 Europskog parlamenta i vijeća od 14. prosinca 2022. godine **o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011** definirani su pojmovi:

„digitalna operativna otpornost” koji znači „sposobnost financijskog subjekta da izgradi, osigura i preispituje svoju operativnu cjelovitost i pouzdanost tako da upotrebom usluga koje pružaju treće strane pružatelji IKT usluga izravno ili neizravno osigura cijeli raspon IKT sposobnosti potrebnih za sigurnost mrežnih i informacijskih sustava kojima se financijski subjekt koristi i kojima se podupire kontinuirano pružanje financijskih usluga i njihova kvaliteta, među ostalim i tijekom poremećaja“.

„kibernapad” koji znači „zlonamjeran IKT incident uzrokovan pokušajem bilo kojeg aktera prijetnje da uništi, izloži, izmijeni, onemogući, ukrade ili neovlašteno koristi imovinu ili joj neovlašteno pristupi“ .

Iz navedenog je razvidno da je financijski sektor (osim sektora obrane) prepoznao rizik i razvio mjere zaštite od kriza, a na osnovi naučenih lekcija. Upravo temeljem takve prakse, a uvažavajući utjecaj koji IKT ima na svakodnevni život potreba da se u što većem obuhvatu akceptiraju rizici i uvedu mjere zaštite od posljedica kibernetičkih napada razvijena je NIS u prvom izdanju, a sada NIS 2 Direktiva.

Uvodne riječi u Preporuci Europske komisije 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera glase: „Upotreba informacijskih i komunikacijskih tehnologija i ovisnost o njima postali su ključni elementi u svim sektorima gospodarstva, jer su naša poduzeća i građani međusobno povezani i ovisni jedni o drugima u različitim sektorima i preko granica više nego ikada prije.“ (EK, 2017).

Svijest o potencijalnim razmjerima krize izazvane kibernetičkim napadima sve je razvijenija, a tome svakako u značajnoj mjeri doprinosi i obvezujuća primjena aktualne NIS 2 Direktive. NIS 2 Direktivom propisani su zahtjevi i date su preporuke o postupanju u slučaju krize izazvane kibernetičkim napadima, o čemu će biti govora u poglavlju koje slijedi.

2. Pravna regulativa

Recitalom 70. NIS 2 Direktive navedeno je kako „Kibersigurnosni incidenti velikih razmjera i krize na razini Unije zahtijevaju koordinirano djelovanje kako bi se osigurao brz i učinkovit odgovor zbog visokog stupnja međuovisnosti između sektora i država članica. Dostupnost mreža i informacijskih sustava otpornih na kibernapade te dostupnost, povjerljivost i cjelovitost podataka ključni su za sigurnost Unije i zaštitu njezinih građana, poduzeća i institucija od incidenata i kiberprijetnji, kao i za jačanje povjerenja pojedinaca i organizacija u sposobnost Unije da promiče i štiti globalan, otvoren, slobodan, stabilan i siguran kiberprostor utemeljen na ljudskim pravima, temeljnim slobodama, demokraciji i vladavini prava."

Recitalom 71. NIS 2 Direktive opisana je uloga ***mreže EU-CyCLONe*** koja bi „trebala djelovati kao posrednik između tehničke i političke razine tijekom kibersigurnosnih incidenata velikih razmjera i kriza te poboljšati suradnju na operativnoj razini i podupirati donošenje odluka na političkoj razini. U suradnji s Komisijom i s obzirom na njezinu nadležnost u području upravljanja krizama, mreža EU-CyCLONe trebala bi se nadovezati na nalaze mreže CSIRT-ova i koristiti se vlastitim kapacitetima pri izradi analize učinka kibersigurnosnih incidenata velikih razmjera i kriza."

Člankom 9. NIS 2 Direktive opisan je Nacionalni okviri za upravljanje kiberkrizama prema kojem svaka država članica imenuje ili uspostavlja jedno ili više nadležnih tijela odgovornih za upravljanje kibersigurnosnim incidentima velikih razmjera i krizama (tijela za upravljanje kiberkrizama). Države članice osiguravaju da ta tijela imaju odgovarajuće resurse za učinkovito i efikasno obavljanje zadaća koje su im dodijeljene. Države članice osiguravaju koherentnost s postojećim nacionalnim okvirima za opće upravljanje krizama.

Utvrđivanje kapaciteta, sredstava i postupaka koji se mogu primijeniti u slučaju krize za potrebe NIS 2 Direktive u nadležnosti su svake države članice.

Svaka država članica donosi nacionalni plan za odgovor na kibersigurnosne incidente velikih razmjera i krize u kojem se utvrđuju ciljevi i načini upravljanja kibersigurnosnim incidentima velikih razmjera i krizama. Spomenutim nacionalnim planom, treba utvrditi ciljeve mjera i aktivnosti za nacionalnu pripravnost; utvrditi zadaće i odgovornosti tijela za upravljanje kiberkrizama; postupke upravljanja kiberkrizama, uključujući njihovu integraciju u opći nacionalni okvir za upravljanje krizama, i kanale za razmjenu informacija; nacionalne mjere pripravnosti, uključujući vježbe i aktivnosti osposobljavanja; relevantne javne i privatne dionike i uključenu infrastrukturu. Također, treba definirati i nacionalne postupke i dogovore između relevantnih nacionalnih tijela i drugih tijela kako bi se osiguralo učinkovito sudjelovanje država članica u koordiniranom upravljanju kibersigurnosnim incidentima velikih razmjera i krizama na razini Unije i njihova potpora takvom upravljanju.

Člankom 16. NIS 2 Direktive definirana je Europska mreža organizacija za vezu za kiberkrize (mreža EU-CyCLONe) te je opisana njezina uloga i nadležnosti u upravljanju krizama. Mreža EU-CyCLONe osniva se kako bi se poduprlo koordinirano upravljanje kibersigurnosnim incidentima velikih razmjera i krizama na operativnoj razini i osigurala redovita razmjena

relevantnih informacija među državama članicama te institucijama, tijelima, uredima i agencijama Unije.

Prema stavku 2. članka 16. NIS 2 Direktive „mrežu EU-CyCLONe čine predstavnici tijela država članica za upravljanje kiberkrizama te, u slučajevima kada potencijalni ili aktualni kibersigurnosni incident velikih razmjera ima ili bi mogao imati znatan učinak na usluge i djelatnosti obuhvaćene područjem primjene ove Direktive, Komisija.“.

Mreža EU-CyCLONe ima zadaću povećati razinu pripravnosti za upravljanje incidentima velikih razmjera i krizama izazvanim kibernetičkim napadima i poboljšanje informiranosti. Mreža EU-CyCLONe zadužena je za procjenu posljedica i učinaka koje su izazvali incidenti velikih razmjera i krize te za predlaganje mogućih mjera za ublažavanje posljedica. ***U slučaju kada bi do krize došlo mreža EU-CyCLONe zadužena je koordinirati upravljanjem kibersigurnosnim incidentima velikih razmjera i krizama te pomoći pri odlučivanju na političkoj razini u pogledu takvih incidenata i kriza.***

Upravo na temu spremnosti za postupanja u kriznim situacijama održana je vježba pod nazivom „BlueOlex 2024“[2]u kojoj je EU-CyCLONe testirao svoju spremnost za odgovor na kiberkrize. Cilj vježbe na izvršnoj razini EU-CyCLONe bio je ojačati suradnju među razinama upravljanja u situaciji nastanka kibersigurnosne krize.

Osim same NIS 2 Direktive na snazi su još dva dokumenta na koja se NIS 2 Direktiva poziva.

Države članice trebale bi doprinijeti uspostavi okvira EU-a za odgovor na kiberkrize utvrđenog u Preporuci Komisije (EU) 2017/1584 (EK, 2017) putem postojećih mreža suradnje, posebno Europske mreže organizacija za vezu za kiberkrize (mreža EU-CyCLONe), mreže CSIRT-ova (članak 15. NIS 2 Diretive) i skupine za suradnju. Mreža EU-CyCLONe i mreža CSIRT-ova trebali bi surađivati na temelju postupovnih aranžmana kojima se utvrđuju detalji te suradnje i izbjegavati udvostručavanje zadaća. (Recital 68. NIS 2 Direktive)

Za upravljanje krizama na razini Unije relevantne stranke trebale bi se oslanjati na aranžmane EU-a za integrirani politički odgovor na krizu na temelju Provedbene odluke Vijeća (EU) 2018/1993.(Recital 68. NIS 2 Direktive)

Komisija je odgovorna i za dostavljanje analitičkih izvješća za aranžmane za politički odgovor na krizu u skladu s **Provedbenom odlukom (EU) 2018/1993**, među ostalim u pogledu informiranosti o stanju i pripravnosti u području kibersigurnosti, kao i za informiranost o stanju i odgovor na krizu u područjima poljoprivrede, nepovoljnih vremenskih uvjeta, mapiranja i predviđanja sukoba, sustava ranog upozoravanja na prirodne katastrofe, zdravstvenih hitnih stanja, nadzora zaraznih bolesti, zdravlja bilja, kemijskih incidenata, sigurnosti hrane i hrane za životinje, zdravlja životinja, migracija, carina, nuklearnih i radioloških hitnih stanja te energije. (Recital 72. NIS 2 Direktive)

[2]https://www.enisa.europa.eu/news/blueolex-2024-exercise-eu-cyclone-test-its-cyber-crisis-response-preparedness, pristupljeno 10. 11. 2024.

U Republici Hrvatskoj člankom 56. Zakona o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24) propisano je upravljanje kibernetičkim incidentima velikih razmjera i kibernetičkim krizama. Središnje državno tijelo za kibernetičku sigurnost je tijelo odgovorno za upravljanje kibernetičkim incidentima velikih razmjera i kibernetičkim krizama Vlada, na prijedlog tijela odgovornog za upravljanje kibernetičkim krizama, donosi ***Nacionalni program upravljanja kibernetičkim krizama***[3].

3. Međunarodni standardi i dobre prakse

Međunarodni standard ISO 22361:2022 –Sigurnost i otpornost – Upravljanje krizama – Smjernice (engl. Security and resilience — Crisis management — Guidelines) pruža smjernice o upravljanju kriznim situacijama koje pomažu organizacijama da planiraju, uspostave, održavaju, pregledavaju i kontinuirano poboljšavaju sposobnost strateškog upravljanja kriznim situacijama. Navedene Smjernice primjenjive su na najvišu razinu upravljanja sa strateškim odgovornostima za pružanje sposobnosti upravljanja kriznim situacijama u bilo kojoj organizaciji te mogu pomoći svakoj organizaciji da identificira krizu i upravlja njome. Prema ISO 22361:2022 Smjernicama je obuhvaćen:

- kontekst, temeljni koncepti, načela i izazovi (točka 4);
- razvoj sposobnosti organizacije za upravljanje krizama (točka 5);
- krizno vodstvo (točka 6);
- izazovi donošenja odluka i složenosti s kojima se krizni tim suočava u akciji (točka 7);
- krizno komuniciranje (točka 8);
- osposobljavanje, vrjednovanje i učenje iz kriza (točka 9).

Nit koja je zajednička većini definicija pojma 'dobra praksa' podrazumijeva strategije, pristupe i/ili aktivnosti za koje se istraživanjem i evaluacijom pokazalo da su učinkovite, djelotvorne, održive i/ili prenosive te da pouzdano vode do željenog rezultata. (EK, 2021)

Tako je ENISA objavila dokument pod nazivom „Dobra praksa za upravljanje kiberkrizama“ (engl. Best Practices for Cyber Crisis Management) (ENISA, 2024.).U navedenom dokumentu prezentirane su uloge pojedinih tijela/organizacija na strateškoj, operativnoj i tehničkoj razini upravljanja kibernetičkom krizom te je prikazan životni ciklus upravljanja kiberkrizama(ENISA, 2024). Prema dobroj praksi upravljanje kiberkrizama podrazumijeva četiri faze. ***Faza prevencije*** ima za cilj podržati EU i njezine zemlje članice da poboljšaju prevenciju i smanje rizik od nastanka kiberkriza i predvidjeti načine za smanjenje njihovih učinaka. ***Faza pripravnosti*** ima za cilj pripremiti države članice i EU za upravljanje krizama razvojem planova za podršku operacijama odgovora na krizne situacije. ***Faza odgovora*** ima za cilj zaustaviti kibernetičku krizu i spriječiti daljnju štetu. ***Faza oporavka*** ima za cilj omogućiti državama članicama i EU brzi oporavak poduzimanjem mjera, čim kriza prođe, vratiti se na razinu sigurnosti koja je normalna ili čak viša od nje prije krize. (ENISA, 2024.)

Međunarodni standard ISO 22361:2022 opisuje koje to karakteristike ima kriza. Kriza ima nisku vjerojatnost nastanka, veliki učinak ako se dogodi, zahtijeva trenutno i neodgodivo djelovanje, najčešće nema na prvi pogled prepoznatljive uzroke i neizvjesnost učinka

[3] https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=28306#_Toc175835665, pristupljeno 16.11.2024.

postupanja odnosno odgovora na krizu. Zato upravljanje krizama zahtijeva izrazito visoku razinu hitnosti postupanja, brzo odlučivanje i djelovanje, kreativno razmišljanje i motivaciju, a u konačnici treba ovladati kriznim stanjem.

Upravljanje krizama podrazumijeva istraživanje okolnosti u kojima je nastala kriza i procjenu štete, sanaciju posljedica i vraćanje u stanje prije krize te stabilizaciju u cilju izbjegavanja nastanka svakog sličnog štetnog događaja koji može izazvati krizu.

Kako bi se unaprijed pripremili ključni dionici na djelovanje u slučaju nastanka kibernetičke krize potrebno je usvojiti plan upravljanja krizom pomoću kojega tim za upravljanje krizama postupa u očekivanoj situaciji.

4. Preporučene aktivnosti upravljanja krizama

Preporuke ISO 22361:2022 za stvaranje osnovnih preduvjeta učinkovitog postupanja u kriznim situacijama su da je potrebno uspostaviti tim za komunikaciju, definirati plan upravljanja u kriznim situacijama, definirati komunikacijski plan u kriznim situacijama te definirati komunikacijski sustav u žurnim situacijama.

Ključne uloge koje treba definirati pri komunikaciji u krizama prema ISO 22361:2022 točki 8.4. (engl. keyroles) su: ***komunikacijski tim, glasnogovornici i odnosi s medijima***. Uspostavljanje tima za komuniciranje neophodno je iz razloga što komunikacija unutar područja zahvaćenog krizom, ali i prema okruženju mora biti koordinirana i usmjerena na objektivno, jasno i pravovremeno informiranje o kriznoj situaciji. Prema preporuci ISO 22361:2022 točki 8.4.1. uprava mora definirati tim za komuniciranje koji je sposoban djelovati brzo, pripremiti ključne informacije koje treba objaviti, pravilno odabrati način komunikacije i pažljivo oblikovati sadržaj koji se komunicira ovisno o tome kome je informacija namijenjena. Kako u komunikaciji postoje uobičajena pravila i u kontekstu kriznih stanja ista treba poštivati, s pojačanom pažnjom ne izazivanja dodatne panike i straha ili širenja dezinformacija.

Glasnogovornici, komunikološki stručnjaci, trebaju jasno i uvjerljivo prezentirati informacije, prikladno odgovarati na postavljena pitanja i zadržati smirenost tijekom konferencija za medije.

Odnosi s medijima uobičajeno su zahtjevna aktivnost i u svakodnevnom životu gdje je važno prenositi aktualne informacije prema svim medijima jednako, pravovremeno i jasno. Odnos s medijima treba graditi kontinuirano. Od posebnog značaja u kriznim stanjima je važno pratiti prenijete odnosno objavljene informacije i u slučaju kada bi se prenijela kriva informacija ili da je ista krivo interpretirana potrebno je promptno reagirati kako se ne bi proširila dezinformacija i u vezi njom dodatno se zakomplicirala ionako složena situacija.

Tim za upravljanje krizama sastavlja ***plan upravljanja krizama*** kojega usvaja odgovorna osoba ili odgovorno tijelo organizacije na koju se isti odnosi. Svrha donošenja plana upravljanja krizama je da se napravi procjena rizika procjenom vjerojatnosti nastanka nekog

štetnog događaja i učinka koji on može imati na organizaciju. U slučaju da je određeni rizik najvišeg intenziteta tada je potrebno razviti plan djelovanja odnosno postupanja. Plan je potrebno testirati u smislu da se kroz realizaciju osmišljenih scenarija testira djelovanje dionika prema planu u zamišljenim kriznim situacijama. Ukoliko se pokaže da neki dio plana nije u operativnom postupanju dao očekivane rezultate i da nastala kriza nije riješena u očekivanom vremenu, da je imala veći štetan učinak na organizaciju od onoga koji je očekivan ili slično plan upravljanja krizama treba revidirati i ažurirati. Posebno treba voditi računa o „zastarijevanju“ plana upravljanja krizama jer u kibernetičkom svijetu prijetnje i rizici se razvijaju jednakom brzinom kao i IKT proizvodi i usluge te je stoga potrebno kontinuirano usklađivati dokumentaciju sukladno stvarnim prijetnjama.

Što se tiče provođenja vježbi i testiranja, u ovom članku već je spomenut primjer „BlueOlex 2024“ u kojoj je EU-CyCLONe testirao svoju spremnost za odgovor na kiberkrize. Takva praksa poželjna je i na drugim razinama primjereno razmjerima djelovanja koje neki subjekt može provesti. Na taj način širi se svijest o važnosti discipliniranog postupanja u slučajevima kada nastane krizna situacija, o komunikacijskim kanalima i načinu obavješćivanja i sličnim važnim aktivnostima.

Planom komuniciranja u kriznim stanjima treba predvidjeti strategije postupanja, načine na koje se mogu informirati ciljane skupine, definirati odgovornosti za izvršavanje i održavanje plana komunikacije.

Komunikacijski sustav za hitne situacije u kibernetičkim krizama ima posebno važnu ulogu jer vjerojatnost da redovni komunikacijski kanali nisu u funkciji može biti značajna, a i učinak takvog rizika je izrazito velik. Upravo zato je potrebno osigurati dodatne učinkovite i sigurne kanale komuniciranja, koji moraju tijekom testiranja biti isprobani i provjereni.

5. Zaključak

Svaka kriza predstavlja složenu situaciju koja zahtijeva veliku pažnju, postupanje bez odgode, jasne upute i komunikaciju kako bi se što prije zaustavio uzrok krize, a potom da se saniraju štete i da se oštećeni sustav vrati u funkciju.

Organizacija postupanja, odgovornosti i ovlasti institucija u okviru Europske unije, odnosno na nivou zemalja članica EU, uloge i rokovi za postupanje u krizama uzrokovanim kibernetičkim napadima opisani su i propisani NIS 2 Direktivom.

Posebno značajnu ulogu u upravljanju krizama imaju komunikacije i informiranje. Krizne situacije mogu zahvaćati šira geografska područja, pa je u cilju sprečavanja širenja dezinformacija i panike potrebno profesionalno pristupati oblikovanju i pravovremenom prenošenju informacija.

U članku su u kratkim crtama prenijete preporuke ISO za sigurnost i otpornost te dobra praksa u području upravljanja kiberkrizama koju je objavila ENISA.

Krize su posebno zahtjevna i osjetljiva stanja te je ključna preporuka pratiti upute kriznih stožera/timova na višim razinama.

Reference

1. ENISA, (2024). "Best Practices for Cyber Crisis Management", preuzeto https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management, pristupljeno 8. studenoga 2024.
2. Europska Komisija, (2017). Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.)., preuzeto https://eur-lex.europa.eu/eli/reco/2017/1584/oj , pristupljeno 10. studenoga 2024.
3. Europska Komisija, (2021). 'What are good practices?',https://ec.europa.eu/migrant-integration/page/what-are-goodpractices_en., objavljeno 13. listopada 2021., pristupljeno 12. studenoga 2024.
4. Europska Komisija, (2022). DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), preuzeto https://eur-lex.europa.eu/eli/dir/2022/2555/oj, pristupljeno 10. svibnja 2024.
5. ISO 22361:2022 - Security and resilience — Crisis management — Guidelines, preuzeto https://www.iso.org/standard/50267.html, pristupljeno 7. studenoga 2024.
6. Vijeće Europske Unije. (2018). Provedbena odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu (SL L 320, 17.12.2018., str. 28.), preuzeto: https://eurlex.europa.eu/eli/dec_impl/2018/1993/oj, pristupljeno 10. studenoga 2024.
7. Zakon 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 DirectiveLeadImplementer, ISO 27001 interni auditor, ISO 9001 Lead auditor***, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata.