Doc. dr. sc. Robertina Zdjelar

Komuniciranje i informiranje u kontekstu NIS 2 Direktive

Sažetak

Pri stvaranju okruženja otpornog na kibernetičke napade veliku ulogu ima razmjena informacija i komuniciranje kako bi se okruženje pravovremeno upozorilo na moguće opasnosti ili iz njih naučilo kako ubuduće postupati. Pravila postupanja pri razmjeni informacija i u komunikaciji o napadima, incidentima, i o krizama vezana su uz posebne protokole. Ključni i važni subjekti trebaju postaviti komunikacijske ciljeve za obavještavanje prepoznatih ključnih dionika o kibernetičkim prijetnjama, incidentima i krizama. Osmišljavanje i donošenje komunikacijskog plana i odabir strategija komuniciranja ključne su aktivnosti koje treba pravovremeno provesti. Evaluacija provedenih komunikacijskih aktivnosti u incidentnih i kriznim stanjima ima za cilj unaprijediti i poboljšati temeljene procese za informiranje i komuniciranje među ključnim dionicima uključujući i javnost. U članku će biti istaknute odredbe NIS 2 Direktive koje se odnose na informiranje i komuniciranje te odredbe nacionalnih zakonskih i podzakonskih akata iz područja kibernetičke sigurnosti u Republici Hrvatskoj. O učinkovitoj komunikaciji i informiranju o kibernetičkim događajima i stanjima javno su dostupni radovi i članci na temu iz kojih je moguće sažeti dobre prakse, o čemu će također biti govora u ovom članku.

Ključne riječi: komunikacijski tim, komunikacijski plan, prikladnost, transparentnost, NIS 2 Direktiva, usmjerenost, vjerodostojnost

1. Uvod

O kolanju informacija, izvješćivanju, komunikaciji bilo kojeg tipa već je bilo govora u kontekstu NIS 2 Direktive u serijalu objavljenih članaka autorica. Stoga se u nastavku navodi kratak podsjetnik na preporuke međunarodnog standarda ISO 22361:2022 za stvaranje osnovnih preduvjeta učinkovitog postupanja u kriznim situacijama, koje uključuju uspostavu tima za komunikaciju, definiranje komunikacijskog plana (u kriznim situacijama) te definiranje komunikacijskog sustava u žurnim situacijama.

Ključne uloge koje treba definirati pri komunikaciji u krizama prema ISO 22361:2022 Sigurnosti i otpornost – Upravljanje krizama (engl. Security and resilience — Crisis management — Guidelines) u točki 8.4. (engl. key roles) 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 s posebnom pažnjom 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 važno je 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 zakomplicirala ionako složena situacija.

Poseban režim komunikacije i informiranja karakterističan je za krizna stanja, međutim treba imati na umu da i u redovnom informiranju, u cilju širenja svijesti o važnosti kibernetičke sigurnosti jednako tako se treba voditi osnovnim komunikacijskim principima, ako se želi postići očekivani učinak.

O navedenom će detaljnije biti govora u poglavlju posvećenom preporučenim aktivnostima. Također u članku je dat pregled pravne regulative, odnosno odredbi NIS 2 Direktive, hrvatskog Zakona o kibernetičkoj sigurnosti i Uredbe o kibernetičkoj sigurnosti.

Zakonskom regulativom nije propisana obvezna primjena međunarodnih standarda međutim, savjetuje se da standardizacija postupanja u kontekstu kibernetičke sigurnosti, odnosno donošenje procedura, i eventualno certificiranje osigurava nesporno objektivno dokazivanje usklađenosti poslovanja s odredbama NIS 2 Direktive.

2. Pravna regulativa

Recital 103. NIS 2 Direktive kaže „*Ako je to primjenjivo, ključni i važni subjekti bi trebali bez nepotrebnog odgađanja obavijestiti svoje primatelje usluga o svim mjerama ili pravnim sredstvima koje mogu poduzeti kako bi ublažili rizike koji proizlaze iz ozbiljne kiberprijetnje.* ***Ti subjekti bi trebali, prema potrebi, a posebno ako je vjerojatno da će se ozbiljna kiberprijetnja ostvariti, svoje primatelje usluga obavijestiti i o samoj prijetnji.*** *Zahtjev za izvješćivanje tih primatelja usluga o ozbiljnim kiberprijetnjama trebao bi se ispuniti u najvećoj mogućoj mjeri, ali ne bi smio podrazumijevati oslobađanje tih subjekata od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mjere kako bi se spriječile ili uklonile sve takve prijetnje i ponovno uspostavila normalna sigurnosna razina usluge.* ***Pružanje takvih informacija o ozbiljnim kiberprijetnjama trebalo bi biti besplatno za primatelje usluga i sastavljeno na lako razumljivom jeziku.****”.*

Recital 119. NIS 2 Direktive kaže „S obzirom na to da kiberprijetnje postaju sve složenije i sofisticiranije, dobre mjere njihova otkrivanja i sprečavanja uvelike ovise o redovitoj razmjeni informacija o prijetnjama i ranjivostima među subjektima. ***Razmjena informacija doprinosi boljoj informiranosti o kiberprijetnjama, što pak povećava kapacitet subjekata da spriječe***

<u>da se prijetnje pretvore u incidente te omogućuje subjektima da bolje ograniče učinke incidenata i učinkovitije se oporave od njih.</u> U nedostatku smjernica na razini Unije čini se da su razni čimbenici spriječili takvu razmjenu informacija, a osobito nesigurnost u pogledu usklađenosti s pravilima o tržišnom natjecanju i odgovornosti.".

Člankom 29. NIS 2 Direktive propisani su mehanizmi za razmjenu informacija o kibersigurnosti.

Države članice EU osiguravaju da subjekti koji su obveznici primjene NIS 2 Direktive, ali i drugi subjekti mogu „međusobno ***dobrovoljno*** razmjenjivati relevantne informacije o kibersigurnosti, uključujući informacije koje se odnose na kibernetičke prijetnje, izbjegnute incidente, ranjivosti, tehnike i postupke, pokazatelje ugroženosti, neprijateljske taktike, informacije o počinitelju prijetnje, kibersigurnosna upozorenja i preporuke o konfiguraciji kibersigurnosnih alata za otkrivanje kibernetičkih napada" uz uvjete da „takva razmjena informacija:

a) ima za cilj sprečavanje ili otkrivanje incidenata, odgovaranje na njih, oporavljanje od incidenata ili ublažavanje njihova učinka;
b) povećava razinu kibersigurnosti, posebno povećanjem informiranosti o kiberprijetnjama, ograničavanjem ili ometanjem mogućnosti širenja takvih prijetnji, podupiranjem niza obrambenih sposobnosti, otklanjanjem i otkrivanjem ranjivosti, tehnikama otkrivanja, zaustavljanja i sprečavanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka ili promicanjem suradničkog istraživanja kiberprijetnji između javnih i privatnih subjekata."

Također čl. 29. st. 2. NIS 2 Direktive govori da „Države članice osiguravaju da se razmjena informacija odvija unutar zajednica ključnih i važnih subjekata te, prema potrebi, njihovih dobavljača ili pružatelja usluga. S obzirom na potencijalno osjetljivu prirodu informacija koje se razmjenjuju, takva se razmjena provodi putem mehanizama za razmjenu informacija o kibersigurnosti.".

Članak 29. st. 3. NIS 2 Direktive govori da „Države članice olakšavaju uspostavu mehanizama za dijeljenje informacija o kibersigurnosti iz stavka 2. ovog članka. Takvim mehanizmima mogu se utvrditi operativni elementi, među ostalim upotreba namjenskih IKT platformi i alata za automatizaciju, sadržaj i uvjeti mehanizama za razmjenu informacija. Utvrđivanjem pojedinosti o sudjelovanju tijela javne vlasti u takvim mehanizmima države članice mogu odrediti uvjete za informacije koje nadležna tijela ili CSIRT-ovi stavljaju na raspolaganje.".

Članak 29. st. 4. NIS 2 Direktive govori da „Države članice osiguravaju da ključni i važni subjekti obavješćuju nadležna tijela o svojem sudjelovanju u mehanizmima za razmjenu informacija o kibersigurnosti iz stavka 2. nakon početka sudjelovanja u takvim mehanizmima ili, ako je primjenjivo, o svojem povlačenju iz takvih mehanizama nakon što povlačenje stupi na snagu.".

Članak 29. st. 5. NIS 2 Direktive govori da „ENISA pruža potporu uspostavi mehanizama za razmjenu informacija o kibersigurnosti iz stavka 2. razmjenom najboljih praksi i pružanjem smjernica.“.

Članak 30. NIS 2 Direktive govori o **dobrovoljnom obavješćivanju o relevantnim informacijama, a što se odnosi na obvezu država članica koje osiguravaju da, „**uz obvezu obavješćivanja iz članka 23. NIS 2 Direktive, CSIRT-ovima ili, ako je to primjenjivo, nadležnim tijelima obavijesti mogu dobrovoljno podnositi:

a) ključni i važni subjekti u pogledu incidenata, kiberprijetnji i izbjegnutih incidenata;
b) subjekti koji nisu subjekti iz točke (a), neovisno o tome jesu li obuhvaćeni područjem primjene ove Direktive, u pogledu značajnih incidenata, kiberprijetnji ili izbjegnutih incidenata.“.

Važno je znati da ako je neki subjekt uključen u dobrovoljno izvješćivanje, ono ne smije dovesti do nametanja dodanih obveza takvom subjektu, kojima ne bi podlijegao da nije podnio obavijest. (članak 30. st. 2. NIS 2 Direktive).

3. Međunarodni standardi i dobre prakse

Osim već opisanih zahtjeva ISO 22361:2022 za stvaranje osnovnih preduvjeta učinkovitog postupanja u kriznim situacijama, koje uključuju uspostavu tima za komunikaciju, definiranje komunikacijskog plana (u kriznim situacijama) te definiranje komunikacijskog sustava u žurnim situacijama u kontekstu komunikacija postoji i ISO/IEC 27003:2017 Informacijska tehnologija – sigurnosne tehnike – Sustav upravljanja informacijskom sigurnosti - Smjernice (engl. Information technology — Security techniques — Information security management systems — Guidance). Smjernicama su opisana tri ključna elementa komunikacije: procesi, komunikacijski kanali i protokoli komunikacije. Odabir svakog od tri elementa i kombiniranje različitih pristupa čini strategiju komuniciranja i informiranja zainteresiranih strana.

Obzirom na osjetljivost informacija treba posebno dodijeliti ovlaštenja već ranije spomenutim komunikacijskim ulogama kako bi se utvrdilo tko je ovlašten davati informacije unutar ili izvan subjekta o napadima, incidentima i krizama i kome ih smije prenositi.

ENISA je objavila studiju s prijedlozima rješenja za razmjenu informacija između CSIRT-ova i agencije za provođenje zakona (LEA) u obliku plana i zajedničke taksonomije, na kojoj se temelji mehanizam za razmjenu informacija. Predložen je i model ažuriranja taksonomija novim vrstama napada ili novih vrstama ranjivosti (ENISA, 2015).

Razmjena informacija u području kibernetičke sigurnosti tema je brojnih znanstvenih istraživanja u kojima se proces informiranja i komunikacije sagledava iz različitih perspektiva, o čemu su pregledni rad objavili Pala i Zhuang (Pala, Zhuang, 2019). U razmatranje su uzeta 82 rada na temu razmjene informacija o kibernetičkoj sigurnosti. Prema navedenim izvorima dvije su grupe informacija koje treba podijeliti: Indikatori kibernetičkog napada: incidenti, slabosti, prijetnje, i obrambene mjere: kako izbjeći napad, svijest o napadu, dobre prakse i strateška analiza. Prednosti razmjene informacija u analiziranim izvorima očituju se kroz koordinaciju i suradnju te jačanje sposobnosti ublažavanja kibernetičkih

napada i odgovora. Autori preglednog rada zaključuju da se razmjenom informacija povećava kolektivno znanje i učinkovita suradnja, da se omogućuje bolje razumijevanje prijetnji i budućih rizika, omogućuje identifikacija budućih napada, povećava mogućnost otkrivanja napada, smanjuje ulaganje u kibernetičku sigurnost, te analiziraju buduće investicijske strategije (Pala, Zhuang, 2019).

Temeljem praktičnih iskustava istraživači Chang i Huang (Chang, K., & Huang, H., 2023.) su dali sažetak pravila u uporabi koja utječu na dijeljenje i uskraćivanje informacija u kontekstu očuvanja kibernetičke sigurnosti (Chang, K., & Huang, H., 2023., Table 1., stranica 11.). Autori u spomenutom radu na, primjeru Tajvana, govore o tome zašto i kako članovi Centra za razmjenu i analizu informacija (engl. ISAC) dijele informacije o kibernetičkoj sigurnosti za sprječavanje kibernetičkih prijetnji i o čimbenicima koji to potiču ili obeshrabruju. Autori su kroz istraživanje proanalizirali literaturu o dijeljenju informacija te su zaključili da se u literaturi tradicionalno naglašavaju motivi za dijeljenje informacija i/ili strukturu platforme/mreže za dijeljenje istih, no temeljem istražene literature nije razvidno kako je formalna i neformalna pravila mreže oblikuju niti kako utječu na razmjenu informacija. Istraživanjem su obuhvaćeni tajvanski regionalni i sektorski centri za razmjenu i analizu informacija. Provedeno je 40 intervjua u institucijama središnje/lokalne vlasti, u privatnim i poduzećima u državnom vlasništvu i nevladinim organizacijama. Na bazi dubinske kvalitativne analize podataka prikupljenih kroz intervjue autori analiziraju institucionalna pravila u primjeni na operativnoj, društvenoj i državnoj razini. Prema dobivenim informacijama neformalna pravila u uporabi na operativnoj razini uključuju „učenje kako spriječiti" i "provođenje mjera prevencije u stvarnom vremenu", koje se mogu smatrati opće primjenjivima čime se mogu steći znanje i iskustvo te osnažiti i poboljšati obrambene sposobnosti.

4. Preporučene aktivnosti za efikasnu komunikaciju

U prethodnim poglavljima već su ukratko opisane osnovne informacije vezane uz proces informiranja i komuniciranja u kontekstu uskladbe poslovanja s NIS 2 Direktivom pa će u ovom poglavlju biti dodatno opisane posebnosti kojima se informiranje i komuniciranje može učiniti efikasnijim.

Efikasan komunikacijski plan obuhvaća osvrt prema unutarnjim i vanjskim zainteresiranim stranama za koje je potrebno posebno osmisliti komunikacijsku strategiju, odnosno pristup za oblikovanje i prijenos informacija. Tako od zainteresiranih strana treba svakako u plan uključiti medije, vlasnike, investitore, dobavljače, kupce/korisnike usluga, zaposlenike i širu zajednicu. Svaka od navedenih zainteresiranih strana ima svoje interese, očekivanja i potrebe za dobivanjem informacija. Oblikovanje informacija i komuniciranje o incidentima i/ili o kriznim stanjima ima velik utjecaj na imidž subjekta stoga se zahtijeva visoka razina profesionalnosti u ovim aktivnostima.

Proces komunikacije podrazumijeva klasične kanale komuniciranja danas dostupne, od objavljivanja izvještaja, obavijesti putem elektroničke pošte, novinskih članaka, medijskih propagandnih uradaka. Ovisno o očekivanom učinku razmjena informacija o napadima, incidentima, krizama, može biti provedena kroz stručne fokus grupe, radionice i konferencije,

prezentacije, što osim širenja znanja ima za cilj i dodatne analize i rasprave kojima se osigurava kvalitetna podloga za unapređenje stanja.

Pravila efikasne komunikacije su ***prikladnost, transparentnost, vjerodostojnost, usmjerenost i razumljivost, jasnoća informacija***. Pravila efikasne komunikacije nalažu da je oblikovanje i način prijenosa informacija potrebno prilagoditi ciljanoj skupini, onome što se želi prenijeti kao ključni sadržaj. Potrebno je koristiti primjeren jezik i način izražavanja prihvatljiv ciljanoj skupini kojoj su informacije namijenjene. Konzistentnost u oblikovanju i prenošenju informacija također je pravilo koje se mora poštovati kako bi se postiglo objektivno informiranje svih ciljanih skupina.

Proces komuniciranja i informiranja osmišljava se i prikazuje u obliku komunikacijskog plana i komunikacijske strategije koje se primjenjuju u predviđenim situacijama (napad, incident, kriza). Provedba procesa i kontrola odrađenih aktivnosti te evaluacija učinaka tako postavljenog komunikacijskog plana i strategije daje osnovne informacije koje trebaju osigurati unapređenje i poboljšanje procesa komuniciranja i informiranja u narednom razdoblju. Kod evaluacije učinkovitosti komunikacije primarno treba proanalizirati jesu li zainteresirane strane dobile informacije koje su im bile korisne, jesu li objavljene informacije bile pravovremene, objektivne, razumljive, jasne i korisne.

5. Zaključak

Komuniciranje i informiranje općenito govoreći je alat kojim se osigurava da pravovremenim prijenosom objektivnih činjenica (informacija) dvije strane koje sudjeluju u procesu mogu imati kvalitetnu interakciju.

Kada je riječ o situacijama u kojima biti pravovremeno informiran može značiti izbjegavanje potencijalne štete prouzročene kibernetičkim napadom, izbjegavanje uključenosti u incident ili u krizu tada je od neprocjenjive važnosti sudjelovati i biti aktivan u mehanizmima za dijeljenje informacija o kibersigurnosti (članak 29. st. NIS 2 Direktive) koji služi za razmjenu takvih informacija.

Procjena što je od informacija, kada i kome potrebno prenijeti sigurno ovisi od slučaja do slučaja, no u svakom slučaju kao podrška u smislu kritičnosti i važnosti informacija uvijek je moguće konzultirati kontaktnu točku na nacionalnoj razini koja ima šira saznanja o razmjerima i mogućem utjecaju potencijalnih neželjenih događaja (napada, incidenata i prijetnji).

Reference

1. Chang, K., & Huang, H. (2023). Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government Information Quarterly*, *40*(4), 101870.
2. ENISA (2015). Information sharing and common taxonomies between CSIRTs and Law Enforcement, dostupno na

https://www.enisa.europa.eu/sites/default/files/publications/Report%20on%20information%20sharing%20and%20common%20taxonomies%20between%20CERTs%20and%20Law%20Enforcement.pdf, pristupljeno 1. prosinca 2024.
3. 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.
4. ISO 22361:2022 - Security and resilience — Crisis management — Guidelines, preuzeto https://www.iso.org/standard/50267.html, pristupljeno 7. studenoga 2024.**ISO/**
5. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance, preuzeto https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en, pristupljeno 10.12.2024
6. Pala, A., & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis*, *16*(3), 172-196.
7. Uredba o kibernetičkoj sigurnosti („Narodne novine“ br. 135/24)
8. 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.