Doc. dr. sc. Robertina Zdjelar

Uskladba poslovanja s NIS 2 Direktivom – ključna područja

Sažetak

Svaki napredak i razvoj sa sobom nosi i negativnu komponentu, rizik, prijetnje, napade, gubitke. Digitalizacija je naročito pogodno područje u kojem se izrazito često govori o rizicima, prijetnjama, napadima i gubicima, stoga je neophodan sustavan pristup kod upravljanja kibernetičkom sigurnosti.

Razvoj svijesti o važnosti kibernetičke sigurnosti krenuo je iz posebno važnih područja kao što su obrana, sigurnost, bankarstvo, financije, a širenjem digitalizacije u druge djelatnosti u zadnjem desetljeću kibernetička sigurnost postala je obvezna prateća funkcija digitalizaciji. Dokaz tome je i uvođenje regulative koja obuhvaća šira geografska područja, pa tako u Europi govorimo o NIS[1](EK, 2016) odnosno sada o NIS 2[2] direktivi (EK, 2022).

U ovom radu cilj je dati pregled ključnih područja koja je važno obuhvatiti kod uskladbe poslovanja s NIS 2 Direktivom (EK, 2022). Slijedom odredbi Direktive NIS 2 (EK, 2022) nacionalna tijela zemalja članica EU obvezna su donijeti nacionalnu regulativu – usklađenu s Direktivom EU te donijeti podzakonske provedbene akte na temu kibernetičke sigurnosti, nacionalnu strategiju kibernetičke sigurnosti i druge politike u cilju postizanja pozitivnih učinaka u području kibernetičke sigurnosti.

U radu se daje praktičan pregled ključnih područja u kojima se zahtijeva proaktivno djelovanje u utvrđivanju, provedbi, praćenju i izvješćivanju o poduzetim mjerama u cilju povećanja razine kibernetičke sigurnosti.

Ključne riječi: kibernetička sigurnost, kontinuitet poslovanja, kontrole, NIS 2 direktiva, upravljanje imovinom, upravljanje krizama, upravljanje rizicima

Uvod

Regulatorni okvir za kibernetičku sigurnost na nivou Europske Unije (EK, 2016), (EK, 2022) i Zakon o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24) prezentirani su od strane nadležnih tijela javnosti. Nadležnosti za pripremu i provedbu uskladbe poslovanja s NIS 2

[1] NIS (EK, 2016) DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[2] NIS 2 (EK, 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)

Direktivom, rokovi za izradu nižih provedbenih akata nastavno na Zakon o kibernetičkoj sigurnosti i rokovi za izvješćivanje propisani su i komunicirani prema javnosti. Uskladba poslovanja s odredbama Direktive NIS 2 opsežan je multidisciplinaran projekt koji treba prije svega biti planiran, vođen, proveden i dokumentiran u skladu s planom i potrebama te u postprovedbenom periodu nadziran, ocijenjen, dokumentiran i revidiran.

Implementacija NIS 2 Direktive zahtijeva posvetiti pažnju na tri ključna područja:

- usvajanje kibernetičke strategije i upravljanje provedbom iste što se očituje kroz osiguranje sigurnosti informacija, promociju kulture o važnosti kibernetičke sigurnosti, razvoj svijesti o važnosti kibernetičke sigurnosti te provođenje primjerenih treninga i uspostavu upravljanja rizicima
- utvrđivanje incidenata i kriza te rješavanje istih pri čemu se osigurava poslovna stabilnost i kontinuitet
- sigurnost infrastrukture i aplikacija kroz implementaciju naprednih mjera sigurnosti, sigurnost aplikacija ugrađenu već kroz razvoj programskih proizvoda, jačanje mehanizama za očuvanje identiteta i kontrolu pristupa te osiguranje od rizika nastalih od strane trećih osoba (poslovni partneri, korisnici).

Projekt uskladbe poslovanja s NIS 2 Direktivom podrazumijeva podršku uprave, posebice u kontekstu osiguranja sredstava i potrebnih resursa za učinkovitu provedbu. Za upravljanje projektom potrebno je imenovati voditelja projekta koji je odgovoran da projekt bude odrađen u skladu s terminskim planom i u zadanim okvirima. Kod planiranja projekta uskladbe poslovanja s NIS 2 Direktivom potrebno je uzeti u obzir sve zainteresirane strane, njihove potrebe i njihovu podršku kod provedbe projekta. Implementacija mjera za uskladbu poslovanja s NIS 2 Direktivom treba biti osmišljena na način da se nove potrebne mjere uklope u već postojeće procese i kulturu u organizaciji. Jednom implementirane mjere nužno je kontinuirano provjeravati i vrednovati s aspekta njihove učinkovitosti, a posebno radi toga jer okruženje u kojem organizacija djeluje je promjenjivo, što može dovesti do novih rizika, promjene intenziteta rizika, promjene vjerojatnosti nastanka rizika. Sve navedeno zahtijeva analizu i evaluaciju te prilagodbu implementiranih mjera na novonastale situacije.

Primjena generičkih modela definiranih normama (npr. ISO, NIST) doprinosi kvaliteti postignutih učinaka jer primjenom određenih standarda i preporuka koje ukazuju na dobru praksu povećava se uspješnost projekta uskladbe poslovanja s NIS 2 Direktivom. Tako primjerice, organizacije koje imaju implementiran sustav:

- ISO/IEC 27001:2022 Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti — Sustavi upravljanja informacijskom sigurnošću — Zahtjevi

i primjenjuju upute i preporuke navedene u

- ISO/IEC 27003:2017 - Informacijska tehnologija — Sigurnosne tehnike — Sustavi upravljanja informacijskom sigurnošću — Smjernice
- ISO/IEC 27100:2020 - Informacijska tehnologija — Kibernetička sigurnost — Pregled i koncepti
- ISO/IEC 27002:2022 - Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti — Kontrole informacijske sigurnosti
- ISO/IEC 27005:2022 - Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti — Smjernice za upravljanje rizicima informacijske sigurnosti

u značajnoj mjeri imaju implementirane mjere važne za kibernetičku sigurnost.

Također ISO 55000:2024 - Upravljanje imovinom — Pregled, načela i terminologija, značajan je za upravljanje imovinom, dok je ISO 31000:2018 - Upravljanje rizicima, praktični vodič značajan za upravljanje rizicima.

Ključna područja za uskladbu poslovanja s NIS 2

Projekt uskladbe poslovanja s NIS 2 Direktivom potrebno je ***planirati*** pri čemu uprava treba donijeti odluku o pokretanju projekta i imenovanju projektnog tima s voditeljem, utvrđivanju rokova provedbe projekta te prava i odgovornosti projektnog tima. Opseg projekta ovisi o organizaciji i kontekstu u kojem ona djeluje. Utvrđivanje postojeće razine zrelosti organizacije u upravljanju kibernetičkom sigurnosti polazna je točka za daljnje usmjeravanje djelovanja. *Postojeća organizacijska struktura i procesi, upravljanje imovinom i upravljanje rizicima* potrebno je proanalizirati te utvrditi pomoću GAP analize kakve mjere treba poduzeti za postizanje napretka do željenog stanja. Naročitu pažnju treba posvetiti *utvrđivanju uloga i odgovornosti svih dionika*, koji mogu utjecati svojim djelovanjem na kibernetičku sigurnost i učinak koji se očekuje od uskladbe poslovanja s NIS 2 Direktivom.

Kada je projekt isplaniran, što podrazumijeva da je utvrđen tim za ***provedbu***, njegove odgovornosti i dinamika provedbe s rokovima, kada su utvrđena stanja upravljanja rizicima, upravljanja imovinom, uloge i odgovornosti svih dionika, potrebno je otpočeti aktivnosti provedbe kontrola predviđenih mjera za osiguranje kibernetičke sigurnosti.

Već spomenuti dionici čije potrebe, uloge i odgovornosti treba u fazi pripreme i planiranja proanalizirati, sada je potrebno regulirati uvođenjem raznih mjera za *upravljanje sigurnošću u lancu isporuke*.

Upravljanje rizicima polazna je osnova za *upravljanje incidentima i upravljanje krizama*. Ako se terminološki rizik definira kao potencijalna prijetnja, tada se

- incidentom smatra stanje u kojem je imovina već ugrožena i nužno je primjenjivati *upravljanje incidentima*,
- krizom smatra situacija u kojoj je stanje ugroze sigurnosti i imovine poprimilo šire razmjere i kada je situacija složena i zahtijeva poseban režim djelovanja pri čemu je nužno aktivirati *upravljanje krizom*.

Sprečavanje nastanka incidenata i kriza ili prevladavanje istih na način da se njima upravlja ako se dogode, ima za cilj osigurati kontinuitet u poslovanju, pri čemu je ključno na pravilan način komunicirati i izvještavati ključne dionike o stanju i poduzimanju ključnih aktivnosti. Za postizanje što boljeg efekta *komunikacije s dionicima* (zaposlenici, kupci, dobavljači, javnost, vlasnici…) potrebno je paralelno tijekom provedbe projekta osmišljavati i provoditi *treninge za razvoj vještina* za prevenciju incidenata te raditi na podizanju svijesti o razumijevanju kibernetičke sigurnosti i važnosti.

Uvedene mjere za podizanje razine kibernetičke sigurnosti na željenu/potrebnu razinu treba kontinuirano provjeravati u smislu njihovog obuhvata i učinkovitosti, s obzirom da se okruženje u kojem organizacija djeluje dinamički mijenja. Uvedene *mjere za osiguranje kibernetičke sigurnosti treba testirati* i ovisno o rezultatima provedenih provjera poduzimati mjera za daljnji razvoj i unapređenje. *Interna kontrola* (audit) također služi za kontinuirano praćenje pravilne primjene definiranih i implementiranih mjera za osiguranje potrebne razine kibernetičke sigurnosti. Sve kontrole, testiranja moraju biti dokumentirane i dokazive, a o rezultatima kontrola treba biti obaviještena (*izvještaj*) uprava odnosno odgovorna osoba u organizaciji koja je odobrila provedbu projekta. Sve utvrđene nesukladnosti i propusti trebaju se dokumentirati i

analizirati, kako bi se pravovremeno uz nikakvu ili minimalnu štetu uvele nove efikasnije mjere sigurnosti.

Proces koji slijedi nakon provedenih provjera, testiranja i kontrola treba usmjerava resurse na poboljšanja implementiranih mjera kibernetičke sigurnosti. Suština procesa upravljanja je osiguranje *kontinuiranog poboljšanja*.

Diskusija

Pod utjecajem medija javnost je osviještena o važnosti kibernetičke sigurnosti u organizaciji. Svaki pojedinac kroz razne uloge, bilo kao zaposlenik, kao donositelj odluka, kao korisnik pojedinih usluga, kao isporučitelj roba i usluga može svojim aktivnostima doprinijeti povećanju razine kibernetičke sigurnosti.

O važnosti kibernetičke sigurnosti i štetnim utjecajima incidenata i kriza na kvalitetu života svakodnevno treba učestalo informirati građane, posebice putem medija dostupnih najširem mogućem broju građana. Jedan od ključnih razloga za digitalni jaz je nedovoljno znanje i vještine za korištenje informacijske i komunikacijske tehnologije (IKT). Koliko je rizično za kibernetičku sigurnost nedovoljna digitalna pismenost korisnika IKTa u doba digitalne transformacije pitanje je kojem bi trebalo posvetiti detaljnije istraživanje? Koliko incidenata nastane kojima se ugrozi kibernetička sigurnost radi neznanja i radi nepažnje korisnika?

Zaključak

Kibernetička sigurnost je imperativ, koji nema prikladnu alternativu u digitalnom društvu. Cjelovito sagledavanje kibernetičke sigurnosti temeljene na odredbama NIS 2 Direktive zahtijeva sustavan projektni pristup od planiranja, provedbe, kontrole do unapređenja.

Direktivom NIS 2 (EK, 2022) utvrđen je značajan broj obveznika primjene iste, što s obzirom na kriterij djelatnosti ili pak s obzirom na važnost subjekata zbog njihove veličine (broj zaposlenih, godišnji prihodi, vrijednosti imovine). Preporuke za uskladbu poslovanja s NIS 2 Direktivom temelje se na brojnim, već poznatim područjima upravljanja. Mjere za osiguranje kibernetičke sigurnosti je potrebno dimenzionirati u skladu s kontekstom u kojem organizacija djeluje, u skladu s rizicima i prijetnjama, te prepoznatim slabostima. Mjere je potrebno uvesti, primjenjivati i kontrolirati njihovu primjenu kontinuirano. Jednom uspostavljen sustav upravljanja kibernetičkom sigurnošću treba kontinuirano evaluirati jer okruženje se dinamički mijenja, što utječe na pojavu novih rizika od kojih se treba zaštiti i ranjivosti koje treba preventivnim mjerama ukloniti.

Reference

1. Europska Komisija, (2016), DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, preuzeto https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1692602453659, pristupljeno 10. svibnja 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 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.

3. ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, preuzeto https://www.iso.org/standard/27001 , pristupljeno 13. svibnja 2024.

4. ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, preuzeto https://www.iso.org/standard/75652.html, pristupljeno 13. svibnja 2024

5. ISO/IEC 27003:2017, Information technology — Security techniques — Information security management systems — Guidance, preuzeto https://www.iso.org/standard/63417.html, pristupljeno 10. srpnja 2024.

6. 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 13. svibnja 2024

7. ISO/IEC 27100:2020, Information technology — Cybersecurity — Overview and concepts, preuzeto https://www.iso.org/standard/72434.html, pristupljeno 13. svibnja 2024.

8. ISO 31000:2018, Risk management, A practical guide, preuzeto https://www.iso.org/publication/PUB100464.html, pristupljeno 10. srpnja 2024.

9. ISO 55000:2024, Asset management — Overview, principles and terminology, preuzeto https://www.iso.org/standard/55088.html, pristupljeno 20. srpnja 2024.

10. „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.

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 dvadesetgodišnje 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 ISO 27001 interni auditor, ISO 9001 interni auditor, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata. U postupku je stjecanja certifikata za vodećeg implementera NIS 2 direktive. Svoje radno iskustvo koristi kao izvor ideja za znanstvene i stručne radove.