Doc. dr. sc. ROBERTINA ZDJELAR

USKLADBA POSLOVANJA

S NIS 2 DIREKTIVOM

PLANIRANJE, PROVEDBA, KONTROLA
I KONTINUIRANO POBOLJŠANJE
– UPRAVLJANJE I ORGANIZACIJA

ALINEJA

Doc. dr. sc. Robertina Zdjelar

USKLADBA POSLOVANJA S NIS 2 DIREKTIVOM

PLANIRANJE, PROVEDBA, KONTROLA I KONTINUIRANO POBOLJŠANJE – UPRAVLJANJE I ORGANIZACIJA

NAKLADNIK

Alineja, obrt za edukaciju i savjetovanje
Lojenov prilaz 4, Zagreb

ZA NAKLADNIKA

Biljana Barjaktar

UREDNICA

Biljana Barjaktar

RECENZENTI

Akademik Velimir Srića, profesor emeritus

Doc. dr. sc. Domagoj Frank

Mjesto i godina izdavanja: Zagreb, 2025.

ISBN 978-953-46530-0-5

E-knjiga objavljena je na:
https://alineja.hr/web-trgovina/e-knjige/uskladba-poslovanja-s-nis-2-direktivom-e-izdanje/

Doc. dr. sc. ROBERTINA ZDJELAR

USKLADBA POSLOVANJA

S NIS 2 DIREKTIVOM

PLANIRANJE, PROVEDBA, KONTROLA
I KONTINUIRANO POBOLJŠANJE
– UPRAVLJANJE I ORGANIZACIJA

ALINEJA

Zagreb, 2025.

Sažetak

Svaki napredak i razvoj sa sobom nosi i negativne komponente: rizike, prijetnje, napade i gubitke. Digitalizacija je naročito pogodno područje u kojem se izrazito često govori o rizicima, prijetnjama, napadima i gubicima, stoga je kod upravljanja kibernetičkom sigurnosti nužan sustavan pristup.

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 digitalizacije. Dokaz tome je i uvođenje regulative koja obuhvaća šira geografska područja, pa tako u Europi govorimo o NIS (EK, 2016), odnosno sada o NIS 2 Direktivi (EK, 2022).

Cilj ovog izdanja je dati pregled ključnih područja koja je važno obuhvatiti kod uskladbe poslovanja s NIS 2 Direktivom (EK, 2022). Slijedom odredbi te Direktive nacionalna tijela zemalja članica EU-a obvezna su donijeti nacionalnu regulativu usklađenu s njezinim odredbama 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 knjizi 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. Autorica u knjizi opisuje organizacijski i upravljački pogled na proces uskladbe poslovanja s NIS 2 Direktivom. Uskladba

poslovanja s NIS 2 Direktivom može se sagledavati kao projekt, čije postprovedbene rezultate treba kontinuirano unapređivati.

Zakonom o kibernetičkoj sigurnosti („Narodne novine" broj 14/24, dalje u tekstu: Zakon o kibernetičkoj sigurnosti ili Zakon) propisano je da će u svrhu povećanja spremnosti i otpornosti na kibernetičke napade biti održane vježbe testiranja, a što je dio upravljanja kibernetičkim incidentima velikih razmjera i kibernetičkim krizama (članak 56.). S ciljem dobivanja egzaktnih pokazatelja za utvrđivanje stanja spremnosti i otpornosti u domeni kibernetičke sigurnosti ključnih i važnih subjekata, na nacionalnoj razini, bit će izrađen plan provedbe nacionalnih mjera pripravnosti, uključujući plan aktivnosti osposobljavanja te provedbe vježbi koje su sastavni dio plana iz članka 58. toga Zakona.

Člankom 58. Zakona propisano je da je cilj provođenja vježbi kibernetičke sigurnosti postizanje maksimalne razine pripravnosti na način da se provjeravaju raspoloživi kapaciteti i sposobnosti u području kibernetičke sigurnosti te da se testiraju uspostavljeni komunikacijski mehanizmi. Pri testiranju svakako trebaju biti obuhvaćena znanja, iskustva i prakse koje se primjenjuju u procesima kod ključnih i važnih subjekata vezano za postizanje kibernetičke sigurnosti.

Svakako treba naglasiti da su Zakonom propisane aktivnosti usmjerene na globalnu razinu sigurnosti koja može ovisiti indirektno o razini otpornosti „najslabije karike" u nizu te je, stoga, važno da svaki subjekt, koji može biti žrtva iskorištena kao izvor napada na druge ili može sam biti žrtva napada, podiže razinu spremnosti i svijest o važnosti te teme. Da bi se spriječile ugroze, štete i krize na višoj, nacionalnoj razini, potrebno je osigurati kvalitetan pristup rješavanju pitanja kibernetičke sigurnosti na nižim razinama počevši od razine ključnih i važnih subjekata, koja se može protegnuti sve do razine pojedinca.

U narednim poglavljima daje se pregled što sve organizacije trebaju provjeravati vezano za vlastitu kibernetičku sigurnost.

Nastavno na uvod o ključnim poglavljima vezanim uz kibernetičku sigurnost autorica u poglavlju 3. daje pregled ključnih aktivnosti vezanih za upravljanje imovinom (engl. asset management), s aspekta osiguranja kibernetičke sigurnosti prema NIS 2 Direktivi (EK, 2022). Područje upravljanja imovinom sagledavano je s različitih perspek-

tiva, posebice računovodstvene, financijske i kontrolinške, ali i s perspektive investiranja. S razvojem svijesti o važnosti kibernetičke sigurnosti razvila se i svijest o potrebi vođenja računa o sigurnosti imovine.

Raspolaganje imovinom nužan je preduvjet za ostvarenje vizije, misije i strategije svakoj organizaciji. Što se smatra imovinom, ovisi o konkretnom slučaju. Sagledavanje imovine s aspekta kibernetičke sigurnosti ima za svrhu da uprava i zaposlenici osvijeste koja imovina je ključna za sigurno poslovanje, koja je kritična i ranjiva s aspekta kibernetičkih napada te što je potrebno poduzeti da se rizici od napada spriječe i da moguća šteta, nastala na imovini, bude svedena na minimum.

U poglavlju 3. knjige bit će u kratkim crtama opisana metodologija koju se može primijeniti na upravljanje imovinom, koje su koristi od upravljanja imovinom i koji su to ključni elementi sustava upravljanja imovinom. Također, autorica daje prikaz programa kibernetičke sigurnosti upravljanja imovinom te ukazuje na korake koje je preporučeno provesti za implementaciju programa upravljanja imovinom. Od posebne važnosti, za određene kategorije imovine, može biti pravo pristupa podacima o imovini. Kako postupati s imovinom u trenutku kada zaduženi korisnik više nema osnovano pravo koristiti neku imovinu (umirovljenje, promjena poslodavca...)?

Širenje jedinstvenog digitalnog tržišta na globalnoj razini potaknulo je zakonodavce da utvrde uvjete koje dionici u digitalnom okruženju moraju ispuniti kako bi se osigurala kibernetička sigurnost digitalnog poslovnog i društvenog okruženja. Tako je 2016. godine Europska unija uvela u primjenu Direktivu NIS (engl. Network and Information Systems) (EK, 2016) koja je 2022. godine stavljena izvan snage i zamijenjena NIS 2 Direktivom (EK, 2022). Obvezu primjene NIS 2 Direktive imaju zemlje članice Europske unije (EU-a), no neke odredbe mogu se primjenjivati i na dionike koji nisu s područja članica Europske unije, ali posluju sa subjektima koji imaju sjedišta u EU-u.

Praćenje primjene mjera za osiguranje kibernetičke sigurnosti nužno je radi usmjeravanja pažnje na kritične točke u sustavu zaštite. Što je to europsko tijelo nadležno za statistička istraživanja – EUROSTAT – izvijestilo o stanju u proteklom razdoblju na temu kibernetičke sigurnosti bit će u kratkim crtama prikazano u poglavlju 4.

Svaki implementirani sustav upravljanja očekivano bi trebao dati dodatnu vrijednost, a to je poboljšanje koje je kontinuirano. Kontinuirano poboljšanje (engl. continual improvements) rezultat je ozbiljnog pristupa shvaćanju i prihvaćanju rezultata samoprocjene i evaluacije koju provodi nezavisno tijelo, danih u vidu preporuka. Rezultati samoprocjene i nadzora, koje provode vanjska tijela, trebaju biti korišteni na način da se preporuke razmotre i na najbolji mogući način implementiraju te tako stvaraju novu poboljšanu praksu.

Provođenje promjena zadnji je korak u Demingovom krugu[1], PDCA (engl. Plan-Do-Check-Act). U poglavlju 5. dan je pregled i razrada područja koja treba pratiti radi usklađenosti poslovanja s NIS 2 Direktivom te su pojašnjeni načini postupanja (engl. act) s preporukama za provođenje da bi sustav, kojim se upravlja kibernetičkom sigurnošću, bio poboljšan.

Kibernetička sigurnost u opskrbnom lancu opisana je u poglavlju 6. Zakonodavac je u članku 30. stavku 1. podstavku 4. Zakona 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 Zakona nalazi se odredba prema kojoj *„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[2]-om"*. Prilog IV. Zakona propisuje da u obvezni sadržaj nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnost (koji 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 Zakon primjenjuje.

---

1 https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/1675-william-edwards-deming, pristupljeno 3. kolovoza 2024.

2 The European Union Agency for Cybersecurity

Upravljanje rizicima tema je poglavlja 7. 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 navesti još sličnosti kako bismo pojasnili što je kibernetička sigurnost za tehničke, mrežne i informacijske sustave.

Kako očuvati otpornost? Prije svega tako da svaka jedinka za sebe odgovarajućim mjerama (adekvatnim mjerama za očuvanje otpornosti) proaktivno radi na tome, ali i „da pazi" u kakvom se okruženju 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.

Uskladba poslovanja s NIS 2 Direktivom složen je projekt koji podrazumijeva inicijalno implementiranje upravljačkih procesa u različitim aspektima, između ostalog, i upravljanje rizicima. Upravljanje rizicima podrazumijeva standardne aktivnosti o kojima će autorica dati kratak pregled u poglavlju 7.

Svrha NIS 2 Direktive je uspostaviti okruženje i razviti kulturu o važnosti zaštite od kibernetičkih napada i sprečavanja nastanka kritičnih i rizičnih događaja koji mogu ugroziti povjerljivost, konzistentnost ili dostupnost informacija i imovine. U poglavlju 8. obrađene su teme vezane uz pripremu, prepoznavanje, izvješćivanje o incidentima, procjenu utjecaja incidenata i djelovanju na incidente. Sve navedene aktivnosti opisane su međunarodnim standardima i dobrom praksom pa će u skladu s tim biti navedeni ključni dokumenti kao i regulativa temeljem koje se postavlja obveza upravljanja kibersigurnosnim incidentima.

Širenje primjene digitalnih tehnologija i umjetne inteligencije u globalnim razmjerima, osim pozitivnih učinaka koje očekuju investitori, sa sobom donosi i rizik koji značajno raste s povećanjem stupnja ovisnosti o digitalnoj tehnologiji i umjetnoj inteligenciji. Svakodnevne životne navike gotovo su nezamislive bez upotrebe uređaja koji u osnovi ima informacijsku i komunikacijsku tehnologiju (dalje u tek-

stu: IKT). Upravo ta činjenica dovoljno je snažan argument 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, o čemu je pisano u poglavlju 9. 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 poglavlju daje pregled zahtjeva i preporuka NIS 2 Direktive vezanih uz krize izazvane kibernetičkim napadima, preporuke za primjenu standardizirane prakse, a bit će govora i o upravljanju krizama.

Upravljanje incidentima, incidentima velikih razmjera i krizama podrazumijeva i sprječavanje širenja i saniranja štete i vraćanje sustava u stanje kakvo je bilo prije štetnog događaja ili čak i bolje. U takvim situacijama sve snage treba usmjeriti na uspostavu osnovnih uvjeta za uobičajeno funkcioniranje sustava. Naravno, o tome treba voditi računa puno prije, prije nego nastane štetan događaj. Za osiguranje kontinuiteta poslovanja (engl. business continuity) potrebno je provesti analizu sustava, njegovih procesa i imovine kako bi se utvrdili ključni detalji nužni za brzo djelovanje u slučaju nastanka štetnog događaja. U poglavlju 10. govori se o terminološkom određivanju ključnih pojmova vezanih za osiguranje kontinuiteta poslovanja, o upravljanju kontinuitetom poslovanja, preporukama za oporavak nakon katastrofa i o kategorijama planova koje je potrebno izraditi i primjenjivati ako zatreba. Također, navode se i preporuke temeljene na međunarodnim standardima o procesu uspostave kontinuiteta poslovanja, kao i na dobrim praksama.

Svijest o osobnoj odgovornosti svakog dionika u kibernetičkom prostoru postala je važna jer prema statistikama upravo je ljudski faktor najčešći uzrok počinjenja propusta iz neznanja i nepažnje, koji dovode do incidenata koji mogu prerasti u krizu. Razvoj svijesti treba poticati komuniciranjem o temi, približavanjem konkretnih primjera

iz prakse u kojima dionici prepoznaju sebe kao moguću žrtvu iskorištenu u pokušajima kibernetičkih napada. Prepoznavanje mogućih napada te naučeni i uvježbani načini postupanja u takvim situacijama, omogućavaju dionicima u sustavu da pravilno postupe s ciljem izbjegavanja nastanka štetnog događaja odnosno incidenta. Takvi obrasci ponašanja razvijaju se kroz održavanje praktičnih treninga i vježbi. Stručnjaci koji se po potrebi angažiraju u slučaju nastanka incidenta moraju imati specijalistička znanja za prepoznavanje sumnjivih nakana napadača, procjenu razine ozbiljnosti situacije i otklanjanje posljedica te se trebaju educirati na sustavan i multidisciplinaran način. U poglavlju 11. bit će govora o razvoju kompetencija, širenju znanja i stjecanju praktičnih vještina o čemu govori i NIS 2 Direktiva, ali i nacionalno zakonodavstvo. Rezultati raznih stručnih institucionalnih i individualnih znanstvenih istraživanja također su u sažetom obliku prikazani u tom poglavlju.

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 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 incidentnim i kriznim stanjima ima za cilj unaprijediti i poboljšati temeljne procese za informiranje i komuniciranje među ključnim dionicima, uključujući i javnost. U poglavlju 12. bit će 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. Javno su dostupni radovi i članci o učinkovitoj komunikaciji i informiranju o kibernetičkim događajima i stanjima, iz kojih je moguće sažeti dobre prakse.

Sadržaj