Doc. dr. sc. Robertina Zdjelar

# Kontinuirano poboljšanje stanja kibernetičke sigurnosti - vrijednost koju dobivamo upravljanjem

## Sažetak

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 od nezavisne strane, 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 čine novu poboljšanu praksu.

Provođenje promjena zadnji je korak u Demingovom krugu[1], PDCA (engl. Plan-Do-Check-Act). U ovom članku autorica će dati pregled i razradu područja koja treba pratiti radi usklađenosti s NIS 2 Direktivom te kako postupati (engl. Act) s preporukama i kako ih provesti da bi sustav kojim se upravlja kibernetičkom sigurnošću bio poboljšan.

**Ključne riječi:** kibernetička sigurnost, kontinuirano poboljšanje, NIS 2, samoprocjena, nadzorne mjere

## 1. Uvod

Sustav upravljanja treba osigurati praćenu, nadziranu i kontroliranu provedbu procesa na zadani način što jamči kvalitetu. Svaki propust, bilo koje vrste i značajnosti, kada je uočen, treba biti poticaj da se nepravilnosti u sustavu poboljšaju. Tako svaka revizija, nadzorno tijelo, ima zadatak provjeriti radi li sustav na propisani način (propis može biti zakonski, ali i interni). Ako revizori utvrde nepravilnosti, poželjan (i mudar) odgovor nadziranoga bi mogao biti „Radimo na poboljšanju kontinuirano. I to je sastavni dio redovnog posla.“

Primjena kontinuiranog poboljšanja u osiguranju kibernetičke sigurnosti preuzeto je iz svjetski poznatih upravljačkih doktrina. Jedna od njih je poznati model upravljanja nazvan Kaizen[2]. Spomenuti izvor kaže da je Kaizen japanska riječ koja znači "promjena na bolje". A izvorno značenje japanske riječi "Kaizen" iz Shogakukan rječnika moglo bi se doslovno prevesti kao "Čin poboljšanja loših točaka".

ISO 9001:2015 Sustav upravljanja kvalitetom u točki 10.3. ima propisane zahtjeve za kontinuirano poboljšanje. ISO/IEC 27001:2022 Informacijska sigurnost, kibernetička sigurnosti i zaštita privatnosti – Upravljanje informacijskom sigurnošću u točki 10.1. ima propisane zahtjeve za kontinuirano poboljšanje.

Već spomenuti PDCA je jedan od alata kontinuiranog poboljšanja baziran na procesima.

---

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

[2] What Is Kaizen? The Toyota Way to Continuous Improvement (businessmap.io)

Zakonom o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24) (dalje u tekstu: Zakon) koji je na snazi u Republici Hrvatskoj od veljače 2024. godine predviđa poboljšanje stanja kibernetičke sigurnosti ili smanjenje rizika od kibernetičkih napada **temeljem preporuka utvrđenih nakon provedbe mjera nadzora**. Konkretno, navedeno je utvrđeno u kontekstu poglavlja *Opće nadzorne mjere za ključne i važne subjekte* člankom 79. koji kaže „(1) Nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti ovlašteno je u obavljanju stručnog nadzora…(3) Kada se primjenjuje nadzorna mjera iz stavka 1. podstavka 7. ovoga članka, nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti izrađuje dodatnu analizu kibernetičke sigurnosti na temelju objektivnih, nediskriminirajućih, pravednih i transparentnih kriterija za procjenu rizika, ako je to potrebno u suradnji s nadziranim subjektom, a radi utvrđivanja preporuka za poboljšanje stanja ili smanjenje rizika kojima je subjekt izložen ili može biti izložen.“

Osim vanjskog nazora potrebno je provoditi samoprocjenu i pratiti promjene. U ovom preglednom članku autorica navodi **četiri preporučena područja za praćenje promjena**. Prije svega treba pratiti promjene koje se događaju unutar organizacije. S aspekta kibernetičke sigurnosti važno je biti upućen u te promjene jer svaka od tih promjena može izazvati disbalans u provođenju definiranih politika, procedura usmjerenih na kibernetičku sigurnost.

Nadalje, velik utjecaj na promjene može imati bilo koja **promjena u tehnologiji** koju koristimo u sustavu. Nove tehnologije potencijalno otvaraju nove rizike i prijetnje, tako da kod primjene novih tehnologija treba biti posebno oprezan i pratiti svaku promjenu koju moramo provesti kroz sustav da bi on i dalje bio siguran i otporan na prijetnje.

**Promjene u okruženju** također mogu biti uzrok novih rizika i prijetnji. Prije svega ovdje treba istaknuti promjene u zakonskoj regulativi, promjene koje se događaju kod dobavljača, poremećaji na tržištu, konkurencija i slično.

Na kraju, sve promjene koje su u prethodna tri preporučena područja spomenuta trebaju biti sagledana i s **aspekta programa kibernetičke sigurnosti**, koji treba biti ažuran u svakom trenutku da bi bio funkcionalan. Kako je aktualna tema usklađenost poslovanja s odredbama NIS 2 Direktive tada treba imati na umu da sva poboljšanja trebaju biti usklađena i s tim propisom.

U nastavku će svako od ova četiri područja biti ukratko opisano uz preporuke na što bi bilo poželjno obratiti pozornost pri aktivnostima koje služe za kontinuirano poboljšanje.

## 2. Organizacijske promjene

Člankom 2. i 3. NIS 2 Direktive (EK, 2022) propisani su kriteriji prema kojima subjekti postaju obveznici primjene iste. Sama činjenica da neka organizacija mijenja ili dopunjuje djelatnost ili joj se mijenja kategorizacija obzirom na veličinu (broj zaposlenih, godišnji promet ili vrijednost imovine) može biti povezana s obveznom da svoje poslovanje uskladi s NIS 2 Direktivom.

Također, kod praćenja promjena treba imati na umu da promjena poslovnih ciljeva može biti razlog da se propita kibernetička sigurnost, politika i program vezan uz nju. Primjerice ako organizacija svoje poslovanje širi na tržište koje ne podliježe obvezi primjene NIS 2 Direktive

(npr. geografski ne pripada području obuhvata primjene NIS 2 Direktive) treba posebno obraditi rizike koje donosi takva odluka s aspekta kibernetičke sigurnosti.

U slučaju da poslovni subjekt uvodi novi proizvod ili uslugu svakako treba provjeriti usklađenost cijelog procesa s NIS 2 Direktivom. Ovisno o vrsti proizvoda ili usluge, no pod pretpostavkom da je riječ o proizvodu ili usluzi koji su povezani s informacijskom i komunikacijskom tehnologijom na bilo koji način, treba sagledati što i kako može biti ugroženo i kakve su štete ako se incident dogodi. Dakle, u tom smislu treba revidirati politiku i program kibernetičke sigurnost.

### 3. Tehnološke promjene

Doba intenzivne digitalizacije i uvođenja pametne tehnologije nosi sa sobom kontinuiranu obavezu propitkivanja utjecaja koji takva promjena može imati za proizvođače i za korisnike. Svaka promjena na bilo kojoj komponenti računalnog sustava, od strojeva, programske podrške, procedura i procesa mora biti popraćena revidiranjem politike i programa kibernetičke sigurnosti.

### 4. Promjene u okruženju

Okruženje u kojem živimo prilično je dinamično i nestabilno, posebice kada je riječ o krizama uzrokovanim političkim čimbenicima i/ili ekonomskim čimbenicima. Promjene u zakonodavstvu koje se odražavaju izravno na organizaciju ili na kupce/korisnike njezinih proizvoda/usluga primarno vode k potrebi revidiranja internih politika i programa kibernetičke sigurnosti.

Promjene u lancu nabave, npr. koje su nastupile kod dobavljača s kojima se ostvaruje kontinuirana komunikacija, mogu prouzročiti promjene i u organizaciji te se treba provesti revidiranje internih politika i programa kibernetičke sigurnosti.

Osim dobavljača treba sagledavati na isti način i konkurenciju, koja također sebi postavlja ciljeve, a koji mogu značajno utjecati i na poslovnu politiku organizacije. Ovo je naročito izraženo u domeni IKT industrije u kojoj je kibernetička sigurnost sastavni dio pri oblikovanju i testiranju proizvoda/usluga koje se razvija i nudi kao nove. Takve promjene mogu biti pokretač promjena u organizaciji i njezinoj politici kibernetičke sigurnosti koju treba u skladu s tim i prilagoditi novim sigurnosnim prijetnjama.

### 5. Promjene programa kibernetičke sigurnosti

Već spomenute promjene u okruženju, u organizaciji, u primijenjenoj tehnologiji, mogu stvoriti potrebu da se revidira program i politika kibernetičke sigurnosti.

Uočeni novi rizici i nove prijetnje uzrokovane promjena moraju biti obrađeni kroz različite scenarije te adekvatno uključeni u mjere za osiguranje kibernetičke sigurnosti kako bi se u narednom razdoblju prilikom kontrola obuhvatilo i ta područja. Važno je imati na umu i vremensku dimenziju cijelog procesa izmjena i ažuriranja. I tu je važan kontinuitet.

Svaki sustav upravljanja kvalitetom bazira se na dokumentiranosti pa je tako i kod upravljanja kibernetičkom sigurnošću. **Svaka promjena koja se uvodi u sustav kibernetičke sigurnosti mora biti dokumentirana na zadani način**. Procedure za postupanje u određenim okolnostima moraju biti ažurirane i dokumentirane s jasnim naznakama od kada su uvedene, tko ih se dužan pridržavati, o čemu pak treba voditi brigu nadzor (engl. audit), najčešće interni.

U članku pod nazivom „Što i kako provjeravati u kontekstu kibernetičke sigurnosti sustava“ autorica je dala okvirne preporuke o tome kako provjeravati uspostavljene mjere kibernetičke sigurnosti u organizaciji. U članku je opisano testiranje kibernetičke sigurnosti, interni nadzor, kontrole putem mjerenja, praćenja i izvješćivanja. Rezultati tih kontrola su dokumentirani, a isti trebaju služiti za podizanje svijesti o uočenim slabostima i propustima te za podizanje sigurnosti sustava na višu razinu. Svaka takva promjena predložena od strane nadzora kao preporuka ili svaka promjena koja je rezultat analize promjena u organizaciji, u okruženju ili tehnologiji, ili kombinaciji svega navedenog, mora biti odobrena od strane odgovorne osobe u organizaciji.

## 6. Što u slučaju utvrđene neusklađenosti s NIS 2 Direktivom?

Usklađenost s NIS 2 Direktivom imperativ je za propisane kategorije ključnih i važnih subjekata, a za što postoje propisani i rokovi. U slučaju da se utvrdi da poslovanje nije usklađeno s NIS 2 Direktivom propisana je i moguća penalizacija u vidu novčanih kazni, a postoji mogućnost i zabrane poslovanja, što je puno veća kazna, sa značajno težim posljedicama (reputacija, zaposlenici). S obzirom na iznose kazni, korisno je svim obveznicima primjene NIS 2 Direktive skrenuti pažnju na odredbe NIS 2 Direktive i Zakona kojima je regulirano to pitanje. Ovdje spomenute kazne su krajnje mjere, ima i blažih. Poput davanja obvezujućih preporuka. No obzirom na iznose svakako je dobro biti upućen u propis.

Kazne za neusklađenost poslovanja s NIS 2 Direktivom za ključne i važne subjekte propisane su člankom 34. NIS 2 Direktive: **Opći uvjeti za izricanje upravnih novčanih kazni ključnim i važnim subjektima koji glasi:**

*„1. Države članice osiguravaju da su upravne novčane kazne izrečene ključnim i važnim subjektima u skladu s ovim člankom u pogledu povreda ove Direktive učinkovite, proporcionalne i odvraćajuće, uzimajući u obzir okolnosti svakog pojedinog slučaja.*

*2. Upravne novčane kazne izriču se dodatno uz sve mjere iz članka 32. stavka 4. točaka od (a) do (h), članka 32. stavka 5. i članka 33. stavka 4. točaka od (a) do (g).*

*3. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu dužna se pažnja u svakom pojedinom slučaju posvećuje barem elementima predviđenima u članku 32. stavku 7.*

*4. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. ključni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 10.000.000EUR ili u najvećem iznosu od najmanje 2 % ukupnog godišnjeg prometa na svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada ključni subjekt, ovisno o tome koji je iznos veći.*

*5. Države članice osiguravaju da u slučaju da povrijede članak 21. ili članak 23. važni subjekti podliježu, u skladu sa stavcima 2. i 3. ovog članka, upravnim novčanim kaznama u najvećem iznosu od najmanje 7.000.000EUR ili u najvećem iznosu od najmanje 1,4 % ukupnog godišnjeg prometa na*

*svjetskoj razini u prethodnoj financijskoj godini poduzeća kojem pripada važni subjekt, ovisno o tome koji je iznos veći.*

*6. Države članice mogu predvidjeti ovlast izricanja periodičnih penala kako bi se ključni ili važni subjekt prisililo da prestane s povredom ove Direktive u skladu s prethodnom odlukom nadležnog tijela.“ (EK, 2022, HR verzija dokumenta)*

Zakon govori o *Novčanim kaznama* u članku 101. *za ključne subjekte* i članku 102. *za važne subjekte.*

*Za **ključne subjekte** propisano je: „(1) Novčanom kaznom u iznosu od 10.000,00 eura do 10.000.000,00 eura ili u iznosu od 0,5 % do najviše 2 % ukupnog godišnjeg prometa dotičnog subjekta na svjetskoj razini ostvarenog u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći, kaznit će se za prekršaj prekršajno odgovoran ključan subjekt“* koji ne provede propisane obveze navedene u članku 101. stavku 1.

*Za **važne subjekte** definirano je da će se: „(1) Novčanom kaznom u iznosu od 5.000,00 eura do 7.000.000,00 eura ili u iznosu od 0,2 % do najviše 1,4 % ukupnog godišnjeg prometa dotičnog subjekta na svjetskoj razini ostvarenog u prethodnoj financijskoj godini, ovisno o tome koji je iznos veći, kaznit će se za prekršaj prekršajno odgovorni važni subjekt”* koji ne provede propisane obveze navedene u članku 102. stavku 1.

Ključni propusti koji se navode u Zakonu kao razlog za izricanje novčanih kazni su:

„- koji ne poduzima, djelomično poduzima ili ne poduzima u roku propisane mjere upravljanja kibernetičkim sigurnosnim rizicima (članak 26. Zakona) (ključni i važni)
- koji se prilikom provedbe mjera upravljanja kibernetičkim sigurnosnim rizicima ne koristi certificiranim IKT proizvodima, IKT uslugama i IKT procesima, ako je takva obveza propisana za subjekta (članak 28. Zakona)
- čije osobe odgovorne za upravljanje mjerama ne odobravaju mjere upravljanja kibernetičkim sigurnosnim rizicima i/ili ne kontroliraju njihovu provedbu odnosno ne osiguravaju provedbu odgovarajućih osposobljavanja u svrhu stjecanja znanja i vještina u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i njihova učinka na usluge koje subjekt pruža odnosno djelatnost koju obavlja (članak 29. Zakona)
- koji ne obavještava o svakom značajnom incidentu ili ne dostavljaju roku obavijesti o značajnim incidentima (članak 37. Zakona)
- koji ne obavještava ili ne obavještava u roku primatelje usluga o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama te o svim mjerama ili pravnim sredstvima koje ti primatelji mogu poduzeti kao odgovor na prijetnju (članak 38. Zakona)
- koji ne provede reviziju kibernetičke sigurnosti najmanje jednom u dvije godine (članak 34. ovoga Zakona) (ključni subjekti) ili koji ne provede samoprocjenu kibernetičke sigurnosti najmanje jednom u dvije godine (članak 35. Zakona) (važni subjekti)
- koji ne dostavi u propisanom roku izvješće o provedenoj reviziji kibernetičke sigurnosti nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 34. Zakona) (ključni subjekti)
- koji onemogućava, ometa ili otežava provedbu revizije kibernetičke sigurnosti ili ne snosi troškove provedbe revizije kibernetičke sigurnosti (članak 34. Zakona) (ključni subjekti)

- koji ne dostavi u propisanom roku izjavu o sukladnosti ili plan daljnjeg postupanja nadležnom tijelu za provedbu zahtjeva kibernetičke sigurnosti (članak 35. Zakona) (važni subjekti)
- koji onemogućava, ometa ili otežava provedbu ciljane revizije kibernetičke sigurnosti ili ne snosi troškove provedbe revizije kibernetičke sigurnosti (članak 34. Zakona) (važni subjekti)
- koji ne surađuje s nadležnim CSIRT-om i s njim ne razmjenjuje potrebne informacije u postupku rješavanja incidenata (članak 68. Zakona)
- koji ne surađuje s nadležnim tijelom pri obavljanju nadzora ili mu ne dostavlja tražene podatke ili dokumentaciju (članci 77. i 79. Zakona)
- koji nadležnim tijelima tijekom stručnog nadzora ne omogući nesmetani pristup prostorima, opremi, sustavima i dokumentaciji nužnima za provođenje nadzora (članak 78. Zakona)
- koji ne postupi ili djelomično postupi ili ne postupi u za to ostavljenom roku po korektivnim mjerama izrečenim u stručnom nadzoru (članak 82. Zakona – važni subjekti) (članci 82. i 83. Zakona – ključni subjekti).“

## 7. Zaključak

Svi modeli upravljanja sadrže aktivnosti kontrole i nadzora. Kontrola i nadzor imaju cilj provjeriti usklađenost sustava s propisima, uočiti slabosti i propuste sustava, dati preporuke za poboljšanja, a to je pak osnova za poboljšanje.

Samoprocjena ili nadzorne mjere provedene od strane vanjskog nadzornog tijela imaju za svrhu provjeriti primjenu odredbi NIS 2 Direktive u praksi nadziranog subjekta. Za utvrđena odstupanja i neusklađenosti trebaju biti date i preporuke koje je potrebno otkloniti u zadanom roku. Svaka preporuka koja je prihvaćena i implementirana treba polučiti očekivano poboljšanje utemeljeno na novo postavljenim ciljevima.

Samoprocjena je poželjna jer se na taj način uzima u obzirom dinamičnost promjena u organizaciji, u tehnologiji koju koristimo, u zakonskoj regulativi, a onda posljedično i u programu kibernetičke sigurnosti. Praćenje promjena osigurava da se pravovremeno počnu provoditi propisane mjere, u slučaju da uočena promjena ima za posljedicu obveznu prilagodbu poslovanja prema NIS 2 Direktivi, jer propisane novčane kazne su značajnih vrijednosti. Razina svijesti svih dionika o važnosti kibernetičke sigurnosti treba se podizati sa svakom promjenom u praksi.

## Reference


1. 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 and Directive (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.
2. „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. u Koprivnici 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 Upravnog odjela za financije, proračun i javnu nabavu, u sastavu kojega je bila i informatika.

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.