Doc. dr. sc. Robertina Zdjelar

Što i kako provjeravati u kontekstu kibernetičke sigurnosti sustava?

Sažetak

Zakonom o kibernetičkoj sigurnosti („Narodne novine“ broj 14/2024) (dalje u tekstu: 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 biti će izrađen plan provedbe nacionalnih mjera pripravnosti, uključujući plan aktivnosti osposobljavanja te provedbe vježbi koje su sastavni dio plana iz članka 58. ovoga Zakona.

Člankom 58. Zakona zakonodavac navodi kako 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 sama može biti žrtva napada, podiže razinu spremnosti i svijest o važnosti te teme. Upravo zato, da bi se spriječile ugroze, štete i krize na višoj, nacionalnoj razini, potrebno je osigurati kvalitetan pristup rješavanju pitanja kibernetičke sigurnosti na nižim razinama – razina ključnih i važnih subjekata, što pak u nekim pojedinostima seže do razine pojedinca, fizičke osobe.

U članku se daje pregled o tome što organizacije mogu/ trebaju provjeravati vezano za vlastitu kibernetičku sigurnost.

Ključne riječi: interni nadzor, kibernetička sigurnost, kontrole, NIS 2 direktiva, testiranje

1. Uvod

U uvodnom članku pod nazivom „Uskladba poslovanja s NIS 2 Direktivom – ključna područja“ opisane su faze u životnom ciklusu projekta uskladbe poslovanja s NIS 2 Direktivom. Ukratko, životni ciklus projekta uskladbe poslovanja s NIS 2 Direktivom, baziran na Demingovom krugu[1], sastoji se od faze planiranja, provedbe, ***provjere*** i djelovanja s ciljem kontinuiranog poboljšanja. Sigurnost je najvažnija.

Zamislite stanje sigurnosti u putničkom zrakoplovu na prekooceanskom letu i odgovornost posade da preveze putnike od točke A do točke B na siguran način. Što sve posada zrakoplova

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

mora imati pod kontrolom, a koliko potencijalnih rizika stoji oko njih u svakom trenutku. Što posada radi? Posada ***surađuje*** s timom koji prije polijetanja provjera zrakoplov, ispravnost komunikacijskog sustava i općenito tehničku ispravnost zrakoplova za siguran let, razinu goriva u spremnicima, signalizaciju te se posada pouzdaje u njihovu pedantnost pri obavljanju posla. Također, posada zrakoplova ***surađuje*** s timom koji provjerava putnike i sve što ulazi u zrakoplov u teretni prostor i putnički prostor te se posada pouzdaje u njihovu pedantnost pri obavljanju posla. Oba tima za podršku koji rade na pripremi zrakoplova i putnika imaju ***zadane procedure*** za postupanje. Također, imaju kontrolu leta koja isto tako svoj posao mora raditi pedantno i prema propisanoj proceduri. Svaki putnik dobiva ***jasne upute o pravilima i ponašanju*** za vrijeme leta te o tome što je dozvoljeno unositi u zrakoplov. I na kraju, kada posada zatvara vrata zrakoplova i priprema se za polijetanje – fokusiraju se na stanje pokazatelja na nadzornoj ploči u kokpitu zrakoplova. Prati se brzina kojom zrakoplov leti, visina na kojoj leti, raspoloživa količina goriva, brzina strujanja zraka i vremenske prilike, ima li koga od drugih letećih objekata u blizini te se mjeri udaljenost do cilja i kontaktiraju se kontrolne točke na zemlji radi potvrđivanja smjera i ostalih uvjeta. Svi ostali parametri na kontrolnoj ploči također se prate, no ako su timovi prije preuzimanja zrakoplova od strane posade odradili sigurnosne i tehničke procedure kako treba, velika je ***vjerojatnost*** da će posada sigurno prevesti putnike od točke A od točke B. Naglasak u ovom primjeru treba biti na tome da svaki član svakog tima treba usmjeriti maksimalnu pažnju na ono što je njegov dio zadatka (Kaplan, Norton, 1996). ***Učinak*** koji na sigurnost može imati samo jedna pogreška ili propust je u ovom slučaju velik, što dovodi do ***štete*** velikih razmjera.

Opisani primjer se može preslikati i na sustav kibernetičke sigurnosti u nekom sustavu. Ono što kibernetičku sigurnost čini posebnom, u odnosu na navedeni primjer, je to što je okruženje dinamično (ali i zrakoplov leti u vremenskim uvjetima koji nisu u 100% slučajeva predvidivi i baziraju se samo na prognozama; političke situacije koje mogu potaknuti organiziranje otmice i sl.) i što se rizici iz dana u dan mijenjaju, što rizici mogu biti unutarnji i vanjski. No, zato postoje stručni timovi koji o tome kontinuirano vode brigu. Osim profesionalaca i korisnici računalnih sustava, u najširem smislu riječi, imaju važnu ulogu u kibernetičkoj sigurnosti, kao i putnici u zrakoplovnom prometu jer njihovo ponašanje može dovesti u rizik cijeli sustav. O tome koliko često je dovođenje sustava u rizik iz neznanja ili namjerno od strane korisnika može se nagađati, zato treba osmišljavati i provoditi preventivne mjere podizanja svijesti (edukacije, treninzi) o važnosti sigurnosnih mjera za opće dobro.

Mjere za podizanje razine kibernetske sigurnosti koje se nastoje implementirati u sustav trebaju biti organizacijske, logičke i fizičke.

Organizacijske mjere podrazumijevaju propisivanje niza politika, procesa, procedura i radnih uputa koje bi trebale usmjeriti ponašanje svih korisnika sustava u kontekstu kibernetičke sigurnosti. Primjer: politika o elektroničkoj pošti propisuje da se na poslu smiju koristiti samo službene e-mail adrese, a ne privatne. Proces dodijele poslovnih e-mail adresa objašnjavaju način kako svaki zaposlenik treba zatražiti dodjelu službene e-mail adrese. Procedure propisuju način dodjele službene e-mail adrese (oblik e mail adrese, oblik lozinke, veličina dodijeljenog prostora, period mijenjanja lozinke). Radna uputa detaljno objašnjava korisniku kako koristiti e-mail kao i potencijalne ugroze (spamovi, ne otvarati mailove od nepoznatih pošiljatelja, kako ih brisati i tako dalje).

Primjer logičke zaštite su korisnička imena i lozinke koje korisnici imaju za pristup svojim e-mail adresama, broj dana koliko poruke ostaju na serveru, pravila koja se definiraju za prihvat

pojedinih poruka, „pristupne“ liste u kojima se definira da se ne prihvaćaju poruke koje sadrže određene riječi i tako dalje).

Fizičke kontrole znače da su e-mail serveri fizički zaštićeni u posebnim prostorijama, u klimatiziranim uvjetima.

Opisan primjer kontrola vezanih uz elektroničku poštu pokazuje kompleksnost kibersigurnosti. Opisan je jedan mali segment cjelokupnog projekta koji podrazumijeva sudjelovanje svih u organizaciji.

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*** (engl. Cybersecurity testing) i ovisno o rezultatima provedenih provjera poduzimati mjere za daljnji razvoj i unapređenje sustava sigurnosti.

Interni nadzor (engl. Internal audit) također služi za kontinuirano praćenje pravilne i dosljedne primjene definiranih i implementiranih mjera za osiguranje potrebne razine kibernetičke sigurnosti.

Praćenje, mjerenje, analiza i evaluacija služe za objektivno i utemeljeno usmjeravanje aktivnosti za postizanje napretka i poboljšanja u području kibernetičke sigurnosti.

Sve aktivnosti kontrole, testiranja, praćenja i mjerenja 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.

O preporučenim načinima kontrole detaljnije je navedeno u nastavku članka.

2. Koncepti provjere

Rad na poboljšanju kvalitete bilo čega podrazumijeva između ostaloga stalno propitkivanje je li sve što je bitno (a to se isto definira) pod kontrolom, možemo li potvrditi odnosno jesu li dokazi dokumentirani, treba li biti još bolje i može li u datim okvirima biti bolje?

U kontekstu kibernetičke sigurnosti takvo propitkivanje moguće je provoditi na više načina. U uvodu je spomenuto: testiranje kibernetičke sigurnosti, interni auditi te praćenje, mjerenje i izvješćivanje o postignutim rezultatima testova. U nastavku će svaki od načina provjere biti ukratko opisan.

2.1. Testiranje kibernetičke sigurnosti

Područje kibernetičke sigurnosti široko je i kompleksno. Stoga je postupak testiranje potrebno razdijeliti u više faza. Sustavni pristup razvoju podrazumijeva sustavnu analizu, dizajn i implementaciju. Svaka od faza ima predviđeno testiranje „izlaznog rezultata“ konkretne faze u životnom ciklusu programskog proizvoda (eng. Software). Kod sustavne analize potrebno je izraditi specifikaciju sustava na osnovi korisničkih zahtjeva. Oblikovanje sustava temelji se na specifikaciji sustava, a rezultat je programska specifikacija. Implementiranje programske

specifikacije podrazumijeva definirane procedure i podatke. Testiranje se provodi obrnutim redom (eng. Bottom up). Testiranje modula odnosno cjelina u odnosu na definirane potrebe, testiranje integracije više modula u cjelinu, testiranje prihvaćenosti sustava od strane korisnika. Testiranju programskih proizvoda (engl. Software) pridaje se velika pažnja upravo radi toga jer je to neizostavan dio informacijskih sustava/ mrežnih sustava, a nelogičnosti i propusti u toj komponenti uzrok su ranjivosti sustava u cjelini prilikom kibernetičkih napada.

Proces testiranja treba biti detaljno razrađen i planiran. Prije svega, važno je odrediti područje testiranja – što će se testirati, koji su ciljevi testiranja, zahtjevi koji se moraju ispuniti, povezanost među komponentama i pouzdanost programskog koda (kada je riječ o programima). Nadalje, važno je odrediti kako će se testirati? Koji su testovi primjereni, kako će se provoditi provjere, koji dokazi govore o tome jesu li rezultati pozitivni ili ne, hoće li se primjenjivati automatizirani testovi i slično. Za testiranje je potrebno razraditi testove pomoću kojih će se određeni predmet kontrole testirati, a također treba biti proveden postupak validacije tih testova. Validacija testova znači da se utvrdi mjere li oni ono što smo planirali mjeriti i jesu li i koliko pouzdani. Pri provedbi testiranja potrebno je voditi zapise o utvrđenom, kako bi se utemeljeno donosilo zaključke, a istovremeno i dokumentiralo ih. Kod razvijenih testova za kontrolu poznati su očekivani rezultati. Upravo te vrijednosti služe kontroloru da utvrdi jesu li rezultati provjere u razini očekivanih.

Od ***tehnika*** koje se koriste u svrhu provjere kibernetičke sigurnosti treba spomenuti ***procjenu ranjivosti*** (engl. Vulnerability assessment), ***testiranje prodora izvana*** (engl. Penetration testing) i ***provjere na zapisima sustava*** (eng. Log files). Provjere kibernetičke sigurnosti usmjerene su na provjeru autentičnosti, autorizaciju, pouzdanost, integritet, dostupnost i otpornost.

Sustav ima implementirane kontrolne mehanizme i sustav zaštite od napada. Međutim, cilj napadača izvana je da iskoristi slabosti implementiranih kontrola te da ulaskom u sustav dođe do podataka, onesposobi sustav za normalan rad, otuđi podatke i iskoristi ih nezakonito i slično. Kako bi se takve situacije spriječile, subjekti sami organiziraju testiranje sustava simuliranjem napada izvana.

Procjenu ranjivosti provodimo identificiranjem sigurnosnih slabosti u računalnom sustavu, mreži, aplikacijama, bazama podataka. Kategorizacijom utvrđenih ranjivosti se omogućava rangiranje, a rangiranjem se dobivaju potrebne informacije na što neodgodivo treba obratiti pažnju i prevenirati iskorištavanje slabosti od napadača. O utvrđenim činjenicama treba izvijestiti odgovorne osobe te otklanjanjem utvrđenih slabosti osigurati poboljšanja u sustavu.

U cijelom procesu testiranja ključno je odabrati pravu tehniku testiranja za određena sigurnosna pitanja. Zato je potrebno odrediti cilj testiranja i napraviti analizu koje su tehnike primjerene. Može se pristupiti i na način da se krene od slabosti, a potom se biraju tehnike za validaciju ili se pak može primijeniti tehnika pregledavanja raspoložive dokumentacije poput zapisa koje sustavi generiraju, tehničkih specifikacija ili zapisa o postavkama sustava.

U svakom slučaju proces osmišljavanja testiranja treba biti usmjeren cilju koji se želi postići, pomno birajući adekvatne testove. Provedba testiranja treba biti koordinirana, odrađena u zadanom opsegu i u skladu sa svrhom.

Testiranja se uobičavaju provoditi u testnom okruženju koje se posebno priprema, a o čemu se također treba voditi zapis i dokumentirati sve činjenice koje opisuju testnu okolinu. Prilikom

testiranja potrebno je obavezno zapisati ciljeve i razloge, trajanje testiranja, tipove testiranja sudionike u procesu testiranja i raspored aktivnosti ukoliko je test organiziran na način da obuhvaća više dionika. Također ako se testiranje provodi pod zadanim pretpostavkama i s očekivanim rezultatima tada je potrebno sve podatke zapisati kako bi se kasnije moglo djelovati na ono što je bilo pretpostavljeno, a testom je utvrđeno da sustav ne ispunjava.

Završna faza testiranja kibernetičke sigurnosti je ***izvještavanje te davanje tehničkih i drugih preporuka*** za modificiranje procesa, procedura, promjenu sigurnosnih postavki i primjenu tehnoloških rješenja.

2.2. Interni nadzor

Kada se govori o kibernetičkoj sigurnosti Agencija Europske unije za kibersigurnost (engl. European Union Agency for Cybersecurity (ENISA)) je izradila ***Radni okvir za samoprocjenu*** (ENISA, 2023) koji pokriva osnovna područja koja se nadziru i tipove nadzora. Obveza za provođenje samoprocjene o dosegnutoj razini kibernetičke sigurnosti i usklađenosti poslovanja s NIS 2 Direktivom definirano je člankom 14. Direktive NIS 2 (EK, 2022).

Samoprocjena[2] temeljena na ENISA radnom okviru bazira se na 4 grupe parametara za samoprocjenu: organizacijske parametre (engl. Organisation parameters) s 11 uvjeta; ljudski faktor (engl. Human parameters) sa 7 uvjeta; parametre alata (engl. Tool parameters) s 10 uvjeta i parametre procesa (engl. Process parameters) s 17 uvjeta i svaki je moguće ocijeniti s 0 do 4 razinom ispunjenja. Rezultati samoprocjene pomoću ovog testa ukazuju na razinu spremnosti pojedinca za kibernetičke napade, o razumijevanju tehnologije koja je nužna za osiguranje kibernetičke sigurnosti te na razinu zrelosti uspostavljenih procesa i učinke primijenjenih procedura.

Interni nadzor predstavlja internu kontinuiranu aktivnost kojom se provjeravaju rezultati primjene utvrđenih politika i propisanih procedura s ciljem da se utvrdi dosljednost u primjeni, a što potvrđuje činjenicu da se poslovanje odvija dosljedno u skladu s utvrđenim pravilima. Ključno je da iz utvrđenih nesukladnosti i uočenih propusta budu „naučene lekcije“ kako bi se pravovremeno uz nikakvu ili minimalnu štetu uvele nove efikasnije mjere sigurnosti.

Čitatelji koji su upoznati s ISO 9001:2015 međunarodnim standardom za upravljanje kvalitetom (engl. Quality management systems — Requirements) lako mogu povezati proceduru provođenja internog nadzora s preporukama opisanim u nastavku. O internom nadzoru postoje i zahtjevi u okviru ISO/IEC 27001:2022 Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti (engl. Information security, cybersecurity and privacy protection) pod točkom 9.2. interni nadzor (engl. Internal audit).

Interni nadzor potrebno je organizirati vodeći računa o svim bitnim detaljima za osiguranje kvalitete provedenog nadzora. Cilj internog nadzora je osigurati dokaze da je provedena procjena mjera kibernetičke sigurnosti (članak 21. Direktive NIS2 (EK, 2022)) i izvijestiti o tome (članak 23. Direktive NIS 2 (EK, 2022)). Interni nadzor obuhvaća i provjeru politika kibernetičke sigurnosti kod nabave (lanac nabave), suradnju s drugim zainteresiranim

[2] SIM3v1 self-assessment tool — ENISA (europa.eu) dostupno nahttps://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity/csirt-survey, preuzeto: 3. kolovoza 2024.

stranama i koordinaciju aktivnosti vezanih uz kibernetičku sigurnost, edukaciju i treninge, koordinirano razotkrivanje ranjivosti, pripreme za nadzor, spremnost za nenajavljeni nadzor, dokumentaciju vezanu za usklađivanje u područjima gdje postoje odstupanja (u odnosu na zadano stanje, u odnosu na željeno stanje) (eng. Compliance gaps) i upute kako postupati s nesukladnostima.

Sam postupak nadzora treba biti proveden prema unaprijed definiranom opsegu i u okviru planiranog vremena. Prikupljanje podataka u postupku nadzora najčešće se provodi uvidom u dokumentaciju ili da se podaci prikupljaju putem intervjua od zaposlenika. Uočeni propusti prodiskutiraju se s drugom stranom da bi se izbjeglo eventualno krivo shvaćanje situacije. Naposljetku potvrđeni uočeni propusti i nedostaci trebaju biti evidentirani i poslužiti kao temelj za davanje preporuka za poboljšanja. Svaki podatak koji se koristi kao osnova za davanje preporuka ili mišljenja treba biti dokumentiran zajedno s podacima o izvoru.

2.3. Praćenje, mjerenje, analiza i evaluacija

Navedeni procesi kontrole odvijaju se nastavno jedan na drugi. Praćenje (engl. Monitoring) ima za cilj nadgledanje sustava, procesa, proizvoda kako bi se utvrdila razina praćenih svojstava (engl. Performance). Primjer praćenje zapisa koje generira antivirusni program mora biti kontinuirano. Mjerenje (engl. Measurement) je proces utvrđivanja vrijednosti praćenog svojstva. Primjer mjerenja: broj evidentiranih napada na sustav izvana. Analiza je proces ispitivanja sustava, procesa, proizvoda s ciljem boljeg razumijevanja situacije. Primjer: analizom je utvrđeno da je antivirusni program prepoznao x napada izvana, od kojih se u y slučajeva sustav nije se uspio obraniti i napadač je iskoristio ranjivost sustava zbog nedostataka antivirusnog programa (koji npr. nije imao na vrijeme ažuriranu bazu poznatih virusa i zbog toga je napadač uspio prodrijeti u sustav). Evaluacija (engl. Evaluation) je proces procjene učinkovitosti sustava, procesa, proizvoda. Primjer: evaluacijom stupnja sigurnosti sustava pomoću antivirusnog programa zaključeno je da x zabilježenih slučajeva kibernetičkog napada izvana u y situacija sustav zaštite nije dovoljno precizno reagirao kako bi spriječio ulazak napadača u sustav. Temeljem takvog zaključka treba ispitati u čemu je problem neadekvatnosti antivirusne zaštite. Primjer nedovoljno često ažuriranje baze poznatih ugroza što je stvar postavki sustava ili možda pouzdanosti tog antivirusnog alata jer njegov proizvođač nije aktualizirao što je trebalo; možda je pitanje vještina i stručnosti zaposlenika informatičke službe koji nisu dovoljno precizno definirali postavke antivirusnog programa.

U prethodnom odlomku dat je jedan primjer **s ciljem pojašnjenja procesa kontrole koji se opisuje**. **Kontrola se treba provoditi za definirana/zadana** svojstva sustava, proizvoda, programa koji se želi kontrolirati. Kada je poznato što se kontrolira i zašto, tada se kroz proces praćenja, mjerenja, analize i evaluacije dobivaju objektivni dokazi koji služe za davanje preporuka i upravljanje poboljšanjima.

Kada je riječ o mjerenjima i upravljanju, odgovorne osobe trebaju dobiti uvid u aktualno stanje ključnih parametara koji se prate, a temeljem kojih možemo utvrditi je li sve prema očekivanju i ako nije što je to izvan kontrole. Alat koji služi za izvješćivanje naziva se nadzorna ploča (engl. Dashboard).

Kontrolom u smislu praćenja kibernetičkih napada bave se analitičari, a njihova domena je praćenje zbivanja na računalnoj mreži i na korisničkim uređajima (prijenosna računala, stolna

računala, tableti, mobiteli ako su umreženi i sl). Tehnike i alati koji se pri tome koriste su antivirusni programi, sustavi vatrozida (eng. Firewall), alati za prepoznavanje neovlaštenih upada u sustav. Naravno, izvori ugroze mogu biti korisnici svega spomenutog, koji svojim postupcima dovedu sustav u stanje ugroze. Primjer: mogu svi alati za sigurnost koji su spomenuti besprijekorno funkcionirati, no npr. jedan korisnik priključi u računalo USB memorijski stik, koji prethodno nije testiran antivirusnim programom i cijeli sustav može biti izložen napadu koji nije izvršen izravno izvana, već je na prilično jednostavan način nepažnja korisnika iskorištena i svi sustavi zaštite budu izvan funkcije.

Za ovu vrstu kontrole potrebno je definirati ciljeve praćenja, što se će mjeriti, kakav je postojeći očekivani raspon vrijednosti toga što će se mjeriti da se može utvrditi je li nešto izmaklo kontroli, treba utvrditi metode kako će se mjerenje provoditi i koliko često, a na kraju je potrebno izvijestiti o rezultatima mjerenja, ali i temeljem toga poduzimati adekvatne mjere za poboljšanje.

3. Zaključak

Direktiva NIS 2 (EK, 2022) ne propisuje kako i koliko često treba provjeravati spremnost sustava na kibernetičke napade i otpornost na iste. Takvu odluku svaki poslovni subjekt, obveznik primjene Direktive NIS 2 donosi prema okolnostima u kojima sustav funkcionira.

U članku je prikazano nekoliko preporuka na koje se može provesti procjena i kontrola postignute razine kibernetičke sigurnosti. Opisane kontrole konceptualno su poznate i iz drugih sustava upravljanja i nisu nove niti posebno osmišljene za upravljanje kibernetičkom sigurnosti, ali su provjereno učinkovite ako se provode na propisani način pa ih valja primjenjivati i u ovom području. Možda je korisno za primijetiti da je u svemu bitno utvrđivanje jasnog, ostvarivog, mjerljivog cilja, a iz toga proizlazi i potreba praćenja ostvarenja tih ciljeva kao i načini kako će se to praćenje ostvariti i dokumentirati, što se može naučiti iz grešaka, definirati preporuke i dati ih ponovo provođenje.

Uspješnost u provođenju kontrola i djelovanju na osnovi rezultata tih kontrola ovisi o tome jesmo li prepoznali o čemu ovisi naš cilj, bez čega cilj nije ostvariv. Ako je to pravilno i jasno definirano važno je da svaki član tima snage usmjeri upravo na ključne pokazatelje.

Reference

1. ENISA (2023) “Focus on National Cybersecurity Capabilities: New Self-Assessment Framework to Empower EU Member States.” Accessed August 9, 2023. preuzeto https://www.enisa.europa.eu/news/enisa-news/nationalcybersecurity-capabilities-framework ENISA. “Diagnose Your SME’s Cybersecurity, pristupljeno 1. srpnja, 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 highcommonlevelofcybersecurityacrossthe Union, amendingRegulation (EU) No 910/2014 andDirective (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.

3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, preuzeto https://www.iso.org/standard/27001, pristupljeno 4. kolovoza 2024.
4. ISO 9001:2015 Quality management systems — Requirements, preuzeto s https://www.iso.org/standard/62085.html, pristupljeno 4. kolovoza 2024.
5. Kaplan, S. R., Norton, D. P., (1996), Translating strategy into action – The Balanced Scorecard, Harvard Business School, Boston
6. „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 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 Directive Lead Implementer, ISO 27001 interni auditor, ISO 9001 Lead auditor***, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata.