Doc. dr. sc. Robertina Zdjelar

Kontinuitet poslovanja u kontekstu NIS 2 Direktive

Sažetak

Upravljanje incidentima, incidentima velikih razmjera i krizama podrazumijeva i sprječavanje širenja štete, saniranje štete i vraćanje sustava u jednako ili bolje stanje koje je bilo prije štetnog događaja. 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 utvrdile ključni detalji neophodni za brzo djelovanje u slučaju nastanka štetnog događaja. U ovom člnaku će biti govora o terminološkom određivanju ključnih pojmova vezanih za osiguranje kontinuiteta poslovanja, o upravljanju kontinuitetom poslovanja, o preporukama za oporavak nakon katastrofa, o kategorijama planova koje je potrebno izraditi i primjenjivati ako zatreba. Također biti će riječi i o preporukama temeljenim na međunarodnim standardima o procesu uspostave kontinuiteta poslovanja te na dobrim praksama.

Ključne riječi: CSIRT, kontinuitet poslovanja, NIS 2 Direktiva, plan kontinuiteta poslovanja, plan oporavka od katastrofe, upravljanje kontinuitetom poslovanja

1. Uvod

O rizicima, incidentima i krizama u kontekstu NIS 2 Direktive već je ranije bilo pisano, stoga kao uvod za temu kontinuitet poslovanja valja podsjetiti da je navedenim fenomenima potrebno pristupiti na način da se provedu procjene, da se istima treba upravljati, da je za upravljanje potrebno uspostaviti tim i usvojiti plan, po kojem dalje treba postupati i evaluirati odrađene aktivnosti, ključne pokazatelje praćenja treba mjeriti i evidentirati, a potom provesti analizu i izvući zaključke koji su bitni za poboljšanja. Najzahtjevnije je postupanje u incidentnim i kriznim situacijama, kada nastupe izvanredne okolnosti zbog kojih je sustav onesposobljen isporučiti proizvode ili usluge prema svojim kupcima ili korisnicima na uobičajeni način.

Na samom početku valja reći nešto o ključnim pojmovima vezanim uz temu *kontinuitet poslovanja*. Prema međunarodnom standardu ISO 22301:2019 Sigurnost i otpornost – Sustav upravljanja kontinuitetom poslovanja - Zahtjevi (engl. Security and resilience — Business continuity management systems BCM— Requirements) definirani su pojmovi:

- ***kontinuitet poslovanja*** (engl. Business Continuity BC) koji podrazumijeva „sposobnost organizacije da nastavi isporuku proizvoda i usluga unutar prihvatljivih vremenskih okvira s unaprijed definiranim kapacitetom tijekom poremećaja“ (točka 3.3.),
- ***plan kontinuiteta poslovanja*** (engl. Business Continuity Plan BCP) koji podrazumijeva **„**dokumentirane informacije koje vode organizaciju da odgovori na prekid i nastavi s

radom te obnovi isporuku proizvoda i usluga u skladu s ciljevima kontinuiteta poslovanja“ (točka 3.4.).

„Kontinuitet poslovanja trebao bi postati dio načina poslovanja. Organizacije koje imaju sposobnost kontinuiteta poslovanja, daleko je vjerojatnije da, će preživjeti posljedice velikog incidenta. Upravljanje kontinuitetom poslovanja osigurava da je organizacija sposobna odgovoriti na velike poremećaje koji prijete njezinom opstanku. Kroz ***upravljanje kontinuitetom poslovanja*** *razvija se otpornost cijele organizacije da preživi gubitak dijela ili cijele operativne sposobnosti, pružajući učinkovit odgovor koji štiti interese svojih ključnih dionika i kupaca, reputaciju, marku i aktivnosti stvaranja vrijednosti. Budući da otpornost organizacije ovisi o njenom menadžmentu i operativnom osoblju, kao i o tehnologiji i geografskoj raznolikosti, ova se otpornost mora razvijati u cijeloj organizaciji od višeg menadžmenta na svim mjestima i u opskrbnom lancu.“* (ENISA, 2010, str. 118).

Kontinuitet poslovanja može biti ugrožen po osnovi različitih uzroka. Prema ENISA (2010, str. 119) uzroci ugroze su podijeljeni na: prirodne katastrofe, probleme sa sustavom / kibernetički napadi ili katastrofe uzrokovane ljudskim djelovanjem.

U ***prirodne katastrofe*** spadaju požar, klimatološke promjene, meteorološki fenomeni, seizmološki fenomeni, poplave, kvarovi na sustavima klima uređaja, elektromagnetsko zračenje, prekidi u napajanju električnom energijom.

U uzroke ***problema sa sustavom i kibernetičke napade*** ubrajaju se kvar odnosno nefunkcioniranje programske podrške (engl. software), kvarovi na opremi, povreda održivosti informacijskog sustava, zasićenost sustava ili uskraćivanje usluge korisnicima.

U uzroke povezane s ***ljudskim djelovanje*** spadaju krađa opreme, podmetanje požara, izazivanje poplave, izazivanje prekida napajanja električnom energijom, prekidanje rada klimatizacijskih uređaja, uništavanje opreme i medija za čuvanje podataka, neovlaštena upotreba opreme.

Upravljanje kontinuitetom poslovanja podrazumijeva prepoznavanje ključnih proizvoda i usluga i ključnih aktivnosti koje osiguravaju isporuku. Učinci nastalog poremećaja na isporuku proizvoda i usluga kao i rizici vezani uz nastali štetan događaj trebaju usmjeriti pažnju na utvrđivanje prioriteta zaštite, vremenski okvir, kapacitete i strategije za nastavljanje isporuke proizvoda i usluga. Sve navedeno treba biti sadržano u planu za osiguranje kontinuiteta poslovanja (engl. Business Continuity Plan BCP).

Upravljanje procesom kontinuiteta (engl. Business Continuity Management BCM) poslovanja u kratkom vremenu čini dostupnima ključne informacije za nastavak redovnog djelovanja, zato je važno da proces bude kontinuirano unapređivan, a da informacije budu aktualne. Poslovna analiza treba osigurati informacije o ključnim ljudskim resursima, procesima i imovini bez kojih nije moguće odrađivati minimalnu zahtijevanu isporuku. Treba imati na umu da je isporuka dobara i usluga vrlo često ugovorna obveza isporučitelja/pružatelja usluge i da za neispunjenje takvih poslovnih ugovora mogu prijetiti i značajne kazne. U tom smislu osiguranjem kontinuiteta poslovanja treba upravljati. Za kontinuitet poslovanja važne su dvije kategorije planova: ***plan kontinuiteta poslovanja*** i ***plan oporavka od katastrofe***, o čemu će biti govora u narednim poglavljima.

2. Pravna regulativa

Članak 11. NIS 2 Direktive (EK, 2022) propisuje da su timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi su definirani člankom 10. NIS 2 Direktive) opremljeni redundantnim sustavima i rezervnim radnim prostorom ***kako bi se osigurao kontinuitet njihovih usluga***. Upravo ta obveza za CSIRTove ukazuje kako treba osmišljavati kontinuitet poslovanja i na ostalim razinama.

Članak 21. NIS 2 Direktive (EK, 2022) govori o **mjerama upravljanja kibersigurnosnim rizicima pri čemu "***države članice Europske unije osiguravaju da ključni i važni subjekti **poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere** za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge.*

Uzimajući u obzir najnovija dostignuća i, ako je to primjenjivo, ***relevantne europske i međunarodne norme te trošak provedbe****, mjerama iz stavka prvog podstavka osigurava se razina sigurnosti mrežnih i informacijskih sustava primjerena postojećem riziku. Pri procjeni proporcionalnosti tih mjera u obzir se uzima stupanj izloženosti subjekta rizicima, veličina subjekta, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni i gospodarski učinak."* Jedna od mjera je osigurati ***„(c) kontinuitet poslovanja, kao što je upravljanje sigurnosnim kopijama i oporavak od katastrofe, te upravljanje krizama***". (EK, 2022)

Spomenute mjere upravljanja kibernetičkim sigurnosnim rizicima propisane su i člankom 30. Zakona o kibernetičkoj sigurnosti („Narodne novine" br. 14/24).

Ključna je svrha uskladbe poslovanja s NIS 2 Direktivom da se sustavi učine otpornima na učinke koje može imati štetan događaj.

Aktualnost iz nacionalnog zakonodavstva je da je temeljem članka 24. Zakona o kibernetičkoj sigurnosti („Narodne novine" br. 14/24.) Vlada Republike Hrvatske je na sjednici održanoj 21. studenoga 2024. donijela Uredbu o kibernetičkoj sigurnosti („Narodne novine" br. 135/24) koja stupa na snagu osam dana od dana objave u „Narodnim novinama".

Navedenom Uredbom propisane su mjere upravljanja kibernetičkim sigurnosnim rizicima (Prilog II. Uredbe) koje između ostaloga podrazumijevaju *11. Postupanje s incidentima* u okviru kojeg subjekt treba uspostaviti osnovne procedure za postupanje s incidentima, što u operativnom smislu podrazumijeva ***„procjenu utjecaja svakog pojedinog incidenta na kontinuitet poslovanja subjekta i na odgovarajući način uspostaviti sučelje između postupanja s incidentima i upravljanja kontinuitetom poslovanja subjekta".***

Također mjera *12. Kontinuitet poslovanja i upravljanje kibernetičkim krizama* (Prilog II Uredbe) ima za cilj „osigurati postojanje unaprijed pripremljenih planove za minimiziranje prekida u poslovanju i osiguravanje kontinuiteta ključnih poslovnih aktivnosti subjekta za

slučajeve incidenata i kibernetičkih kriza.“ U operativnom smislu subjekt će u okviru provedbe ove mjere:

„12.4. razviti detaljne planove za oporavak od katastrofa (DRP) i kontinuitet poslovanja (BCP).

12.5. provoditi testiranje planova kontinuiteta poslovanja najmanje jednom godišnje. Planovi kontinuiteta poslovanja se moraju testirati kroz vježbe i revidirati periodički, nakon incidenata, promjena u operacijama ili procijenjenim rizicima. Provođenje testiranja planova kontinuiteta poslovanja mora biti dokumentirano kako bi se nedvosmisleno utvrdilo potrebna unaprjeđenja uočena tijekom provedbe testiranja.“ (Prilog II. Uredbe).

U Prilogu II. Uredbe propisano je da „na osnovu rezultata procjene rizika i plana kontinuiteta poslovanja, plan subjekta za pričuvno kopiranje podataka i redundancije treba biti razvijen, održavan i dokumentiran, a mora uzeti u obzir najmanje:

- vrijeme oporavka;
- osiguranje da su pričuvne kopije odnosno redundantni sustavi potpuni i ispravni,
- uključujući konfiguracijske podatke i podatke pohranjene u okruženju usluga računalstva u oblaku;
- pohrana (mrežnih i izvan mrežnih) pričuvnih kopija te redundantnih sustava na sigurnoj lokaciji ili lokacijama, koji nisu na istoj mreži kao i primarni sustav te su na dovoljnoj udaljenosti kako bi izbjegle bilo koju štetu uslijed katastrofe na glavnoj lokaciji;
- primjena odgovarajućih fizičkih kontrola (kao što je ograničenje pristupa) i logičkih kontrola (kao što je enkripcija) za pričuvne kopije, u skladu s razinom kritičnosti podataka na tim kopijama;
- ponovno uspostavljanje podataka iz pričuvnih kopija odnosno aktiviranje prebacivanja na redundantne sustave, uključujući proces odobrenja;
- ovisnost o ključnim komunalnim uslugama;
- hodogram aktivnosti oporavka koji se odnose na vremenski raspored i međuovisnosti pojedinih aktivnosti oporavka.“

U Prilogu II. Uredbe propisano je „da prilikom testiranja plana kontinuiteta poslovanja potrebno je testirati sljedeće:

- uloge i odgovornosti;
- ključne kontakte tj. kontakte zaposlenika s potrebnim odgovornostima, ovlastima i sposobnostima;
- unutarnje i vanjske komunikacije kanale;
- uvjete aktivacije i deaktivacije plana;
- redoslijed postupanja kod oporavka;
- plan oporavka za specifične operacije;
- potrebni resursi, uključujući pričuvne kopije i redundancije;
- minimalno ponovno uspostavljanje (*Recovery*), a ovisno o planovima i ponovno pokretanje aktivnosti (*Restore*) nakon privremenih mjera;
- povezanost s postupanjem s incidentima;
- mrežne i informacijske sustave, primjerice hardver, softver, servise, podatke itd. (kao što su redundantni mrežni uređaji, poslužitelji koji se nalaze iza sustava za raspodjelu opterećenja, raid polja diskova, servisi za pričuvne kopije, više podatkovnih centara);

- imovina, uključujući objekte, opremu i zalihe;
- korištenje alternativnih i redundantnih izvora napajanje električnom energijom.“

Osim obvezujućih propisima definiranih aktivnosti kao smjernica za dobro postupanje služe i međunarodni standardi i dobre prakse o kojima je u nastavku dat kratak pregled.

3. Međunarodni standardi i dobre prakse

Međunarodni standard ISO 22301:2019 Sigurnost i otpornost – Sustav upravljanja kontinuitetom poslovanja - Zahtjevi (engl. Security and resilience — Business continuity management systems — Requirements) specificira zahtjeve za implementaciju, održavanje i poboljšanje sustava upravljanja za zaštitu od poremećaja, smanjenje vjerojatnosti njihovog pojavljivanja, pripremu za njih, odgovor na njih ***i oporavak od poremećaja kada se pojave***.

Zahtjevi navedeni u ISO 22301:2019 su generički i namijenjeni su za primjenu na sve tipove organizacija, bez obzira na vrstu, veličinu i djelatnost. Primarna svrha primjene ISO 22301:2019 je:

„a) implementirati, održavati i poboljšavati sustav upravljanja kontinuitetom poslovanja;
b) nastojati osigurati sukladnost s navedenom politikom kontinuiteta poslovanja;
c) biti u stanju nastaviti isporučivati proizvode i/ili usluge s prihvatljivim unaprijed definiranim kapacitetom tijekom prekida;
d) nastojati poboljšati svoju otpornost učinkovitom primjenom sustava upravljanja kontinuitetom poslovanja.“

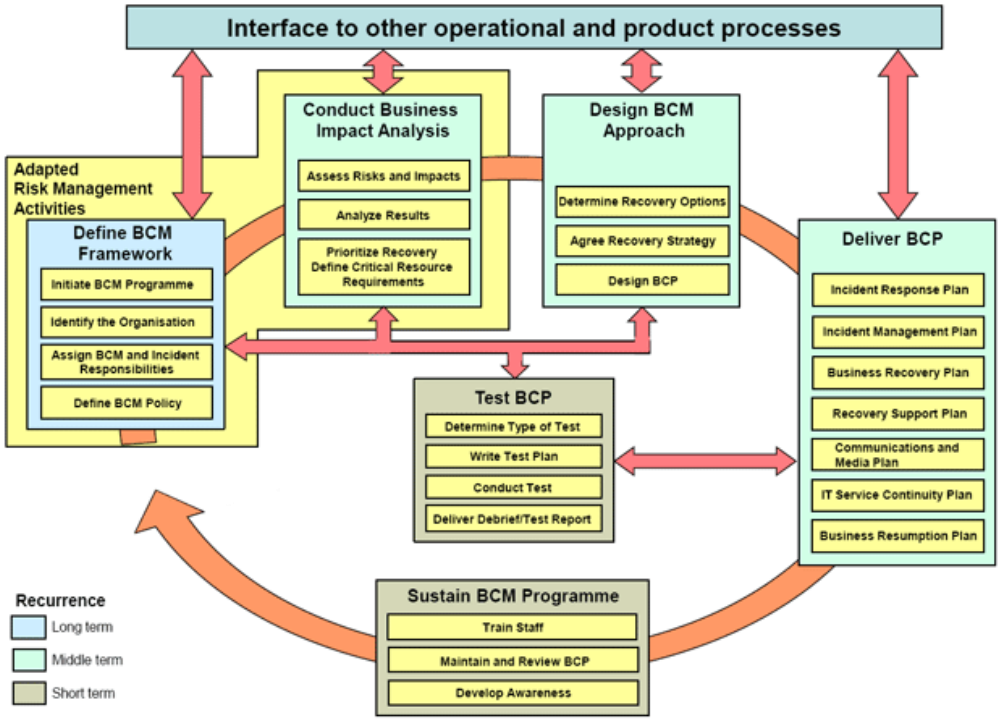
ISO 22301:2019 ima amandman posvećen radnjama vezanim uz klimatske promjene.

Međunarodni standard ISO 22313:2020 Sigurnost i otpornost – Sustav upravljanja kontinuitetom poslovanja - Smjernice za korištenje ISO 22301 (engl. Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301) daje smjernice za provedbu ISO 22301.

O kontinuitetu poslovanja i oporavku od katastrofa dostupne su preporuke izdane od strane neovisne, neprofitne, globalne Udruge za reviziju i kontrolu informacijskih sustava (ISACA) koja se bavi razvojem, usvajanjem i korištenjem znanja i praksi globalno prihvaćenog informacijskog sustava (IS) (Lyons, R., 2021).

ENISA je u sklopu objave o upravljanju rizicima dala preporuke i oko uspostave kontinuiteta poslovanja što je prikazano sljedećim dijagramom iz čega je vidljivo da se kontinuitetom poslovanja treba baviti na svim razinama, od strateške do operativne.

Dijagram 1. Proces kontinuiteta poslovanja, ENISA



Izvor: ENISA, The Business Continuity Process, preuzeto https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/files/ic_process_transparent.gif

4. Preporučene aktivnosti za osiguranje kontinuiteta poslovanja

Za osiguranje kontinuiteta poslovanja potrebno je predvidjeti i ***oporavak od katastrofe,*** što podrazumijeva politike, procedure, alate koji osiguravaju učinkovit oporavak u zadanom vremenu. Oporavak od katastrofe mora biti opisan za ključne poslovne funkcije i procese bez kojih sustav nikako ne može isporučiti proizvode kupcima ili pružiti usluge korisnicima.

Poslovodstvo treba identificirati mogućnosti i osmisliti strategiju i rješenja koja su primjenjiva u potencijalnim kriznim stanjima, usvojiti i primjenjivati plan kontinuiteta poslovanja i plan oporavka od katastrofe. Strategijama i rješenjima trebaju se postići zaštita prioritetnih aktivnosti, stabilizacija, kontinuitet i oporavak prioritetnih aktivnosti te ublažavanje posljedica.

Postoji nekoliko mogućih pristupa upravljanju kontinuitetom poslovanja. Radi se o planiranom nizu radnji za održavanje kritičnih poslovnih funkcija tijekom prekida. Svaka strategija kontinuiteta poslovanja trebala bi biti usklađena sa životnim ciklusom katastrofe, što u suštini znači da je potrebno znati kako se pripremiti prije nego što poremećaj nastane, kako postupati ako nastane i što je potrebno činiti nakon katastrofe.

Pristupi za razvoj strategije kontinuiteta poslovanja trebaju sagledati opravdanost uvođenja određenih mogućnosti poput osiguranja većeg broja lokacija koje omogućavaju neometan rad u slučaju katastrofe ili ugovaranje uzajamnog čuvanja podataka ili angažman treće strane za uspostavu minimalnih funkcionalnosti za oporavak od katastrofe.

Kod odabira strategije kontinuiteta poslovanja treba:

- uzeti u obzir osnovni zahtjev koji se odnosi na prioritetne aktivnosti, vremenski rok u kojem treba uspostaviti minimum funkcionalnosti i kapacitet djelovanja;
- razmotriti intenzitet i tip rizika koji subjekt može/ne može prihvatiti;
- razmotriti opravdanost ulaganja u mjere uvažavajući prethodna dva kriterija.

Mnogo je iskusnih konzultantskih društava koja nude rješenja za kontinuitet poslovanja. Prema Continuity2 Ltd (2023) koji posluju u praksi dvadeset godina, u ovom članku navodi se kao primjer preporuka za pripremu strategije kontinuiteta poslovanja je da se treba:

- procijeniti rizike i učinke za robustan plan kontinuiteta;
- razviti sveobuhvatan plan koji pokriva sve kritične funkcije;
- uključiti ključne dionike u proces planiranja;
- obučite zaposlenike o njihovim ulogama u planu kontinuiteta;
- redovito testirati plan kako bi se utvrdile slabosti;
- povremeno ažurirati plan za trenutne poslovne potrebe;
- priopćiti plan svim zaposlenicima i dionicima;
- osigurati sustave sigurnosnog kopiranja i procese oporavka podataka;
- suradnju s partnerima za usklađene planove kontinuiteta;
- preispitivanje i poboljšanje strategije nakon poremećaja.

Rješenja za osiguranje kontinuiteta poslovanja moraju biti optimizirana u odnosu na troškove koji su nužni da se sustav vrati u funkciju i u odnosu na vrijeme u kojem taj poduhvat treba biti realiziran. Rješenja trebaju zadovoljiti kriterije poput:

- skalabilnosti koja mora biti na visokoj razini, jer se time osigurava širok spektar situacija koje su proanalizirane;
- konzistentnosti za koju je potrebno osigurati ponovljivost i pouzdanost;
- automatizacije koja olakšava prethodno dva kriterija.

Postoje mogućnosti i usvajanja strategije za ublažavanje posljedica katastrofe na način da se putem osiguravajućih društava financijski, putem odštete, kompenzira nastala šteta. Naravno, taj izbor ne uspostavlja redovne uvjete u kojima subjekt funkcionira, ali može ubrzati i pomoći uspostavi istih.

Plan kontinuiteta poslovanja sadrži pristup, aktivnosti i pripremne radnje koje jamče neprekinuto odvijanje temeljnih kritičnih funkcionalnosti i procesa kritičnog i važnog subjekta uslijed katastrofe. Također, plan kontinuiteta poslovanja treba sadržavati informacije o neophodnim resursima za osiguranje kontinuiteta poslovanja, pri čemu se misli na ljudske resurse, opremu, financijske resurse, pravne savjete, zaštitu infrastrukture. Planom kontinuiteta poslovanja između ostaloga definiran je tim za oporavak od katastrofa te su opisane uloge članova tima i način komunikacije te komunikacijski kanali. Specifičnost je i to da treba sadržavati opis koraka za oporavak, utvrđene alternativne lokacije djelovanja ako ih ima. Plan kontinuiteta poslovanja treba biti testiran te ukoliko se utvrdi da postoje odstupanja u odnosu na činjenice utvrđene testiranjem plan treba ažurirati.

Vezano uz kontinuitet poslovanja treba reći da je tema poznata već dugi niz godina, o čemu svjedoče brojni pisani znanstveni i stručni radovi. Postoje razne preporuke opisane na manje ili više detaljan način kako postupati, što predvidjeti, tko sve mora biti uključen u aktivnosti osmišljavanja kontinuiteta poslovanja. Jedan od praktičnih priručnika autorice Snedaker (2007,

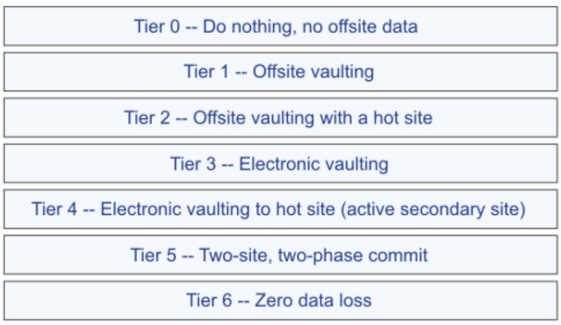
str. 427) daje listu aktivnosti za provjeru je li plan kontinuiteta poslovanja potpun i predviđa li osnovne scenarije za postupanje, što je u nastavku u skraćenom obliku prikazano.

Plan oporavka od katastrofe (engl. Disaster recovery plan) treba biti usmjeren na radnje koje se poduzimaju u času kada katastrofa nastane i svrha mu je:

- definirati na koji način zaustaviti djelovanje štetnog događaja i kako se može smanjiti šteta u času kada je katastrofa već nastala;
- pripremiti subjekt na način da se osigura razumijevanje o utjecaju katastrofe na zaposlene i poslovne kapacitete;
- uputiti na neodgodive aktivnosti za obuzdavanje katastrofe;
- provesti oporavak subjekta od katastrofe.

Kada je riječ o vrijednoj imovini subjekta, što poslovni podaci svakako jesu, i čiji gubitak doista znači katastrofu, potrebno je osigurati upravljanje sigurnosnim kopijama. Danas dostupna tehnološka rješenja osiguravaju automatizaciju procesa izrade sigurnosne kopije, smještanje i čuvanje sigurnosnih kopija na više lokacija, provjeru čitljivosti sigurnosne kopije. Pri osmišljavanju strategije za čuvanje i zaštitu poslovnih podataka treba se osvrnuti i na preporuke IBMa (2021) za odabir strategije oporavka od katastrofa. IBMov (2021) radni okvir za procjenu strategije oporavka u 7 razina.

Slika 1. IBM radni okvir za procjenu strategije oporavka u 7 razina



Izvor: IBM (2021), Slika 1. Razine oporavnka od katastrofe
(engl. *Figure 1. Tiers of disaster recovery)*

Prema slici 1. sigurnost i zaštita podataka može biti organizirana na način da se:

- podaci čuvaju na lokaciji izvan lokacije na kojoj je subjekt (razina 1.);
- podaci čuvaju na lokaciji izvan lokacije na kojoj je subjekt i da postoji lokacija za oporavak za dohvaćanje podataka nakon katastrofe (razina 2.);
- kritični podaci elektronički se prenose od mjesta gdje nastaju do mjesta oporavka, a postoji i trezor za nekritične podatak izvan lokacije (razina 3.);
- podacima se aktivno upravlja programski na dvije fizički odvojene lokacije. Poslužitelji na svakoj lokaciji postavljeni su u ravnopravnom direktnom (peer-to-peer) odnosu. Kritični podaci repliciraju se asinkrono. Kopije podataka dostupne su na obje lokacije, a svaki poslužitelj može oporaviti poslužitelj na alternativnoj lokaciji. Kao dio ove strategije, mediji za pohranu sigurnosnih kopija pohranjuju se izvan lokacije i prate pomoću upravitelja oporavka od katastrofe (razina 4);
- uz ispunjene uvjete razina 4 podaci, uključujući sigurnosne kopije baze podataka i spremišta za kopiranje, repliciraju se sinkrono. Odabrani podaci održavaju se u statusu slike

tako da se ažuriranja primjenjuju i na lokalnu i na udaljenu kopiju baze podataka. Sinkroniziraju se podaci, metapodaci i podaci o inventaru za bazu podataka. Podaci na obje lokacije moraju se ažurirati. Fizički mediji nisu pohranjeni izvan lokacije (razina 5);

- lokalne i udaljene kopije svih podataka ažuriraju se sinkrono, a koristi se dvostruka internetska pohrana s potpunom mogućnošću prebacivanja mreže. Sustavi su povezani s automatiziranim mogućnostima prebacivanja u slučaju pogreške i povratka u slučaju pogreške kada je to potrebno (razina 6). IBM (2021).

Što je razina razine sigurnosti podataka odnosno informacijskih sustava viša to se jamči kraće vrijeme oporavka, ali su troškovi uspostave uvjeta i održavanja istih značajno viši u odnosu na niže razine. Odabrati strategiju oporavka podrazumijeva da je potrebno procijeniti potrebe i provesti izračun opravdanosti investicije za ispunjenje uvjeta koje zahtijeva svaka viša razina sigurnosti. Kombiniranje raznih opcija koje u konačnici moraju osigurati kontinuitet poslovanja i omogućiti brzi oporavak od katastrofe treba pažljivo proanalizirati jer naknadne promjene u pristupu mogu biti skupe.

5. Zaključak

Planiranje i uspostava uvjeta za kontinuitet poslovanja zahtjevan su zadatak jer spoznaja o mogućim prekidima poslovanja i svijest o šteti stvaraju pravovremeno kod svih dionika – poslovodstva, zaposlenika, ali i dionika u opskrbnom lancu. Osim tehničkih preduvjeta, svijest i spremnost doprinose otpornosti na moguću štetu nastalu uslijed incidenta.

Uspostava kontinuiteta poslovanja koncept je poznat već više od dvadeset godina. Stavljanjem u fokus digitalne transformacije kao prioriteta razvoja ne samo s tehnološkim učincima nego i s učincima vezanim uz održivost poslovanja i zaštitu okoliša neophodno je usvojiti nove poslovne modele i implementirati ih u praksi te integrirati u njih kontinuitet poslovanja.

Kao preporuku za sveobuhvatnu metodologiju za razvoj kontinuiteta poslovanja svakako treba istaknuti ENISA pristup kontinuitetu poslovanja za mala i srednja poduzeća – „Upravljanje kontinuitetom poslovanja IT-a“ (ENISA, 2010).

Reference

1. Continuity2 Ltd (2023). 10 Best Practices for Effective Business Continuity Strategy, objavljeno 30. studenoga 2023., preuzeto https://continuity2.com/blog/10-best-practices-for-effective-business-continuity-strategy, pristupljeno 23. studenoga 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. European Network and Information Security Agency ENISA, (2010). IT Business Continuity Management - ENISA approach to Business Continuity for SMEs, preuzeto https://www.enisa.europa.eu/topics/risk-management/approaches-for-smes/risk-management-for-smes-and-micro-enterprises, 10. rujna 2024.

4. European Network and Information Security Agency ENISA, The Business Continuity Process, preuzeto https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/files/ic_process_transparent.gif, pristupljeno 10. rujna 2024.
5. IBM, (2021). Integrating disaster recovery manager and node replication into your disaster recovery strategy, IBM Tivoli Storage Manager, Version 7.1, preuzeto https://www.ibm.com/docs/en/tsmhfw/7.1.0?topic=SSATMW_7.1.0/com.ibm.itsm.srv.doc/c_7tiers.html, pristupljeno 10. kolovoz 2024.
6. ISO 22301:2019 Sigurnost i otpornost – Sustav upravljanja kontinuitetom poslovanja - Zahtjevi (engl. Security and resilience — Business continuity management systems — Requirements), preuzeto https://www.iso.org/standard/75106.html, pristupljeno 11. studenoga 2024.
7. ISO 22313:2020 Sigurnost i otpornost – Sustav upravljanja kontinuitetom poslovanja - Smjernice za korištenje ISO 22301 (engl. Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301), preuzeto https://www.iso.org/standard/75107.html, pristupljeno 11. studenoga 2024.
8. Lyons, R. (2021). Key Considerations for Business Continuity and Disaster Recovery, ISACA, zadnja objava 23. travnja 2021, preuzeto https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/key-considerations-for-business-continuity-and-disaster-recovery, pristupljeno 11. studenoga 2024.
9. Snedaker, S. (2007). Business Continuity & Disaster Recovery for IT Professionals, Syngress Publishing, Inc. ISBN: 978-1-59749-172-3
10. Uredba o kibernetičkoj sigurnosti („Narodne novine“ br. 135/24)
11. 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.