Sistemi vodenja neprekinjenosti poslovanja in oskrba s pitno vodo

mag. Janez Bauer, MBA

SIQ | 60

Uvod

Pomembnost neprekinjenega poslovanja v kritičnih sektorjih:

- nadaljevanje delovanja v primeru motenj,
- varovanje zdravja ljudi,
- gospodarsko stabilnost in
- ohranjanje zaupanja javnosti.

Uvod

Kritični sektorji, kot so na primer zdravstvo, energetika in oskrba s pitno vodo, se morajo pripraviti na nepredvidene dogodke z:

- uporabo načrtov neprekinjenega poslovanja,
- vzpostavitvijo redundantnih sistemov,
- odpornostjo na kibernetske varnostne izzive,
- rednim testiranjem in usposabljanjem zaposlenih …

Uvod

V EU in RS je to področje urejeno z zakonodajo, kot sta na primer:

- Direktiva o odpornosti kritičnih subjektov (Direktiva EU 2022/2557),
- Zakon o kritični infrastrukturi (ZKI),
- Zakon o informacijski varnosti (ZInfV-1).

Pomembno izhodišče predstavlja standard ISO 22301, ki podaja zahteve za načrtovanje, izvajanje in izboljševanje sistema upravljanja neprekinjenega poslovanja.

Varovanje zdravja in življenj

Pomen neprekinjenega poslovanja za zdravje:

- v sektorjih, kot so zdravstvo, energetika, oskrba s pitno vodo, javna varnost in transport, lahko motnje pomenijo neposredno nevarnost za zdravje in življenja ljudi. Na primer, bolnišnice morajo zagotavljati stalno oskrbo pacientov, elektrarne ne smejo prekinjati dobave električne energije, komunalna podjetja pa zagotavljati neprekinjeno oskrbo z zdravstveno ustrezno pitno vodo.

Gospodarska stabilnost

Vloga pri ohranjanju gospodarske stabilnosti:

- motnje v delovanju finančnih institucij, komunikacijskih omrežij, ponudnikov digitalnih in logističnih storitev lahko povzročijo velike ekonomske posledice, kar lahko vodi v širše gospodarske težave.

Skladnost poslovanja

Zakonske zahteve za kritične sektorje:

- mnogi kritični sektorji so podvrženi strogim regulativnim zahtevam, ki vključujejo zahteve po neprekinjenem poslovanju, na primer NIS-2, DORA, MICA,
- neprekinjenost poslovanja je pogosto zakonsko določena in nadzorovana s strani državnih organov.

Zaupanje deležnikov

Ohranjanje zaupanja javnosti:

- za sektorje, ki so ključni za delovanje družbe, je ohranjanje zaupanja javnosti temeljna vrednota delovanja,
- neprekinjeno poslovanje pripomore k ohranjanju zaupanja strank, uporabnikov in širše javnosti.

Neprekinjeno poslovanje in javno zdravje

Pomen za oskrbo s pitno vodo:

- pitna voda je bistvena za preživetje, higieno in splošno zdravje prebivalstva,
- motnje v oskrbi s pitno vodo lahko povzročijo pomanjkanje čiste vode, kar poveča tveganje za izbruh bolezni, ki se prenašajo z vodo,
- povečanje incidence bolezni, ki so posledica pomanjkljive higiene,
- neprekinjeno poslovanje zagotavlja, da imajo prebivalci dostop do zdravstveno ustrezne vode.

Podpora bistvenim storitvam

Vloga pitne vode v drugih sektorjih:

- pitna voda je nujna za delovanje drugih ključnih storitev, kot so zdravstvene ustanove, šole in živilska industrija, na primer,
- bolnišnice potrebujejo stalno dobavo čiste vode za paciente, pripravo hrane in sterilizacijo opreme,
- neprekinjena oskrba s pitno vodo je tako ključna tudi za podporo teh storitev.

Varovanje okolja

Preprečevanje onesnaženja – varovanje okolja:

- stabilna oskrba z vodo pomaga pri zaščiti vodnih virov pred onesnaženjem in prekomerno izrabo,
- v kriznih razmerah, ko so sistemi za prečiščevanje vode ogroženi ali onemogočeni, lahko pride do izpustov onesnaževal v okoljem,
- neprekinjeno poslovanje pomaga preprečiti take dogodke z vzdrževanjem in nadzorom nad sistemi za črpanje, obdelavo in distribucijo vode.

Elementi neprekinjenega poslovanja

1. **Redundanca, nadomestne zmogljivosti**:

- uvedba rezervnih sistemov, kot so nadomestni podatkovni centri, generatorji električne energije, dodatne komunikacijske povezave in
- zadostno (nadomestno) osebje, ki omogočajo nadaljevanje delovanja v primeru izpada osnovnih sistemov.

Elementi neprekinjenega poslovanja

2. **Načrti za obnovitev po nesrečah**, angl. Disaster Recovery Plans - DRP:

- ti načrti vključujejo podrobne postopke za obnovo kritičnih funkcij po nesrečah, vključno s koraki za povrnitev podatkov, preusmeritev delovanja na nadomestne lokacije in
- postopki za komuniciranje v kriznih razmerah.

Elementi neprekinjenega poslovanja

3. **Kibernetska varnost in zaščita podatkov**:

- v današnji digitalni dobi je varovanje informacijskih sredstev ključna naloga,
- uvedba varnostnih politik in naprednih protokolov, šifriranja podatkov in komunikacij, redno izdelovanje varnostnih kopij in varnostnih preverjanj so nujni za zaščito pred kibernetskimi grožnjami.

Elementi neprekinjenega poslovanja

4. **Vloga usposabljenosti zaposlenih**:

- redno usposabljanje in ozaveščanje osebja, usposabljanja in vaje za krizno upravljanje omogočajo, da je osebje pripravljeno in zna pravilno odreagirati v primeru izrednih dogodkov.

Elementi neprekinjenega poslovanja

5. Redno izvajanje preizkusov in simulacij kriznih situacij:

- omogoča organizacijam, da preverijo učinkovitost svojih načrtov za neprekinjeno poslovanje in
- jih po potrebi izboljšajo.

Zakonodajni okvir

Direktiva o odpornosti kritičnih subjektov (Direktiva EU 2022/2557, CER):

- njen cilj je povečati odpornost kritičnih subjektov na fizične grožnje, vključno s terorizmom, naravnimi nesrečami in drugimi motnjami,
- zajema sektorje kot so energija, promet, zdravstvo, voda, digitalna infrastruktura in finance,
- predpisuje zahteve za ocenjevanje tveganj, načrte za odpornost in poročanje o incidentih.

Zakonodajni okvir

Direktiva o varnosti omrežij in informacijskih sistemov (Direktiva EU 2022/2555, NIS 2):

- namenjena je povečanju varnosti omrežij in informacijskih sistemov po vsej EU,
- od operaterjev ključnih storitev, kot so energetika, transport, bančništvo, zdravstvo in digitalna infrastruktura, zahteva, da sprejmejo ustrezne varnostne ukrepe in
- poročajo o incidentih, ki vplivajo na njihovo delovanje.

Zakonodajni okvir

Direktiva o pitni vodi (Direktiva EU 2020/2184):

- ureja kakovost pitne vode,
- vključuje ukrepe za zaščito javnega zdravja pred škodljivimi učinki onesnaženja vode,
- uvaja zahteve za spremljanje kakovosti vode, obvladovanje tveganj in zagotavljanje varne oskrbe z vodo.

Zakonodajni okvir

- Zakon o kritični infrastrukturi (ZKI)
- Zakon o informacijski varnosti (ZInfV-1)
- Zakon o varstvu pred naravnimi in drugimi nesrečami (ZVNDN)
- Zakon o varstvu osebnih podatkov (ZVOP-2) skupaj s Splošno uredbo o varstvu podatkov (GDPR).
- Energetska zakonodaja vključno z Zakonom o oskrbi z električno energijo in Zakonom o energetiki.

Zakonodajni okvir

Zakon o kritični infrastrukturi (ZKI):

1. **Opredelitev kritične infrastrukture**: zakon določa kritično infrastrukturo kot sisteme, omrežja, objekte, storitve in osnovna sredstva, ki so ključni za delovanje države in katerih motnje ali uničenje bi imelo resne posledice za nacionalno varnost, gospodarstvo, javno zdravje, varnost ali okolje.
2. **Identifikacija kritične infrastrukture**: postopek za določanje, kateri deli infrastrukture so kritični, se izvaja na podlagi nacionalne metodologije, ki upošteva kriterije, kot so obseg in posledice motenj, prepletenost z drugimi sektorji in nujnost za delovanje države.

Zakonodajni okvir

Zakon o kritični infrastrukturi (ZKI):

3. **Upravljanje in koordinacija**: vzpostavljen je sistem upravljanja in koordinacije, ki vključuje pristojna ministrstva, sektorje in upravljavce kritične infrastrukture. Glavni usklajevalni organ je Ministrstvo za obrambo, ki skupaj z drugimi organi koordinira dejavnosti v zvezi s kritično infrastrukturo.

Zakonodajni okvir

Zakon o kritični infrastrukturi (ZKI):

4. **Obveznosti upravljavcev kritične infrastrukture**: upravljavci kritične infrastrukture morajo izvajati ukrepe za zagotavljanje varnosti in neprekinjenega delovanja svoje infrastrukture. Vključuje:
   - prepoznavanje ranljivosti in ocenjevanje tveganj,
   - izdelavo načrtov za zaščito kritične infrastrukture,
   - pripravo in izvajanje načrtov za neprekinjeno poslovanje in obvladovanje kriznih situacij,
   - poročanje o incidentih, ki bi lahko vplivali na delovanje kritične infrastrukture.

Zakonodajni okvir

Zakon o kritični infrastrukturi (ZKI):

5. **Nadzor in sankcije**: nadzor nad izvajanjem zakona in predpisov izvajajo pristojni organi, ki lahko izrečejo kazni za nespoštovanje zahtev. Sankcije vključujejo opozorila, globe in druge ukrepe, odvisno od narave in resnosti kršitve.
6. **Skladnost z EU zakonodajo** …

Zakonodajni okvir

Zakon o informacijski varnosti (ZInfV-1), podlaga NIS 2 EU direktiva:

1. **Širitev obsega subjektov**: NIS 2 Direktiva uvaja razširjen seznam sektorjev in subjektov, ki morajo izpolnjevati zahteve glede informacijske varnosti. Poleg že tradicionalnih sektorjev, kot so energija, transport, bančništvo in zdravstvo, zakon zdaj vključuje tudi nove sektorje, kot so oskrba z živili, javna uprava, in vesoljski sektor.
2. **Zaostrene varnostne zahteve**: novi zakon predvideva strožje varnostne ukrepe, vključno z obveznostjo izvajanja rednih ocen tveganj, varnostnih kontrol in ukrepov za obvladovanje tveganj. Poudarek je tudi na upravljanju dobavne verige, kar vključuje preverjanje varnosti pri ponudnikih storitev in izdelkov.

Zakonodajni okvir

Zakon o informacijski varnosti (ZInfV-1), podlaga NIS 2 EU direktiva:

3. **Izboljšano poročanje o incidentih**: subjekti morajo poročati o pomembnih kibernetskih incidentih in ogrožajočih dogodkih, ki lahko vplivajo na neprekinjeno poslovanje. Poročanje mora biti hitrejše in bolj podrobno, kar bo omogočilo boljši odziv in koordinacijo na nacionalni in evropski ravni, ravno tako pa tudi izboljšalo učenje iz incidentov.
4. **Obvezno imenovanje odgovornih oseb**: za vsak subjekt je predvidena obveznost imenovanja oseb, odgovornih za kibernetsko varnost. Te osebe bodo odgovorne za upravljanje, spremljanje in poročanje o varnostnih ukrepih ter za koordinacijo z nacionalnimi organi.

Zakonodajni okvir

Zakon o informacijski varnosti (ZInfV-1), podlaga NIS 2 EU direktiva:

5. **Usposabljanje in izobraževanje**: poudarek je na krepitvi zavedanja in usposabljanja za kibernetsko varnost, tako znotraj organizacij kot na širši družbeni ravni.
6. **Nacionalni organi in medsektorsko sodelovanje**: novi zakon krepi vlogo nacionalnih organov, kot so SI-CERT (Slovenian Computer Emergency Response Team) in druge agencije, ter uvaja zahteve za medsektorsko sodelovanje. Nacionalni organi bodo imeli okrepljene pristojnosti za nadzor, preiskave in izvrševanje ukrepov v primeru neskladnosti.

Zakonodajni okvir

Zakon o informacijski varnosti (ZInfV-1), podlaga NIS 2 EU direktiva:

7. **Kazni in sankcije**: povečane so kazni za neskladnost z zakonodajo, vključno z denarnimi kaznimi in drugimi sankcijami. To vključuje odgovornost za vodilne kadre v organizacijah, kar poudarja pomen kibernetske varnosti na vseh ravneh upravljanja.
8. **Spodbujanje sodelovanja med državami članicami EU**: zakon spodbuja tesnejše sodelovanje med državami članicami EU pri obravnavi kibernetskih groženj in incidentov. To vključuje izmenjavo informacij, sodelovanje pri preiskavah in usklajevanje odzivov.

ISO 22301:2019

1. **Politika neprekinjenega poslovanja**: vzpostavitev politike, ki določa zavezanost organizacije k zagotavljanju neprekinjenega poslovanja in opredeljuje obseg BCMS.
2. **Analiza vpliva na poslovanje** (angl. Business Impact Analysis - BIA): identifikacija in ocena potencialnih vplivov motenj na poslovne procese. BIA pomaga določiti ključne funkcije in potrebne vire za ohranjanje teh funkcij.
3. **Ocena tveganj**: analiza in ocena tveganj, ki bi lahko vplivali na poslovanje organizacije. Ta proces vključuje identifikacijo ranljivosti in groženj ter oceno njihove verjetnosti in potencialnega vpliva.

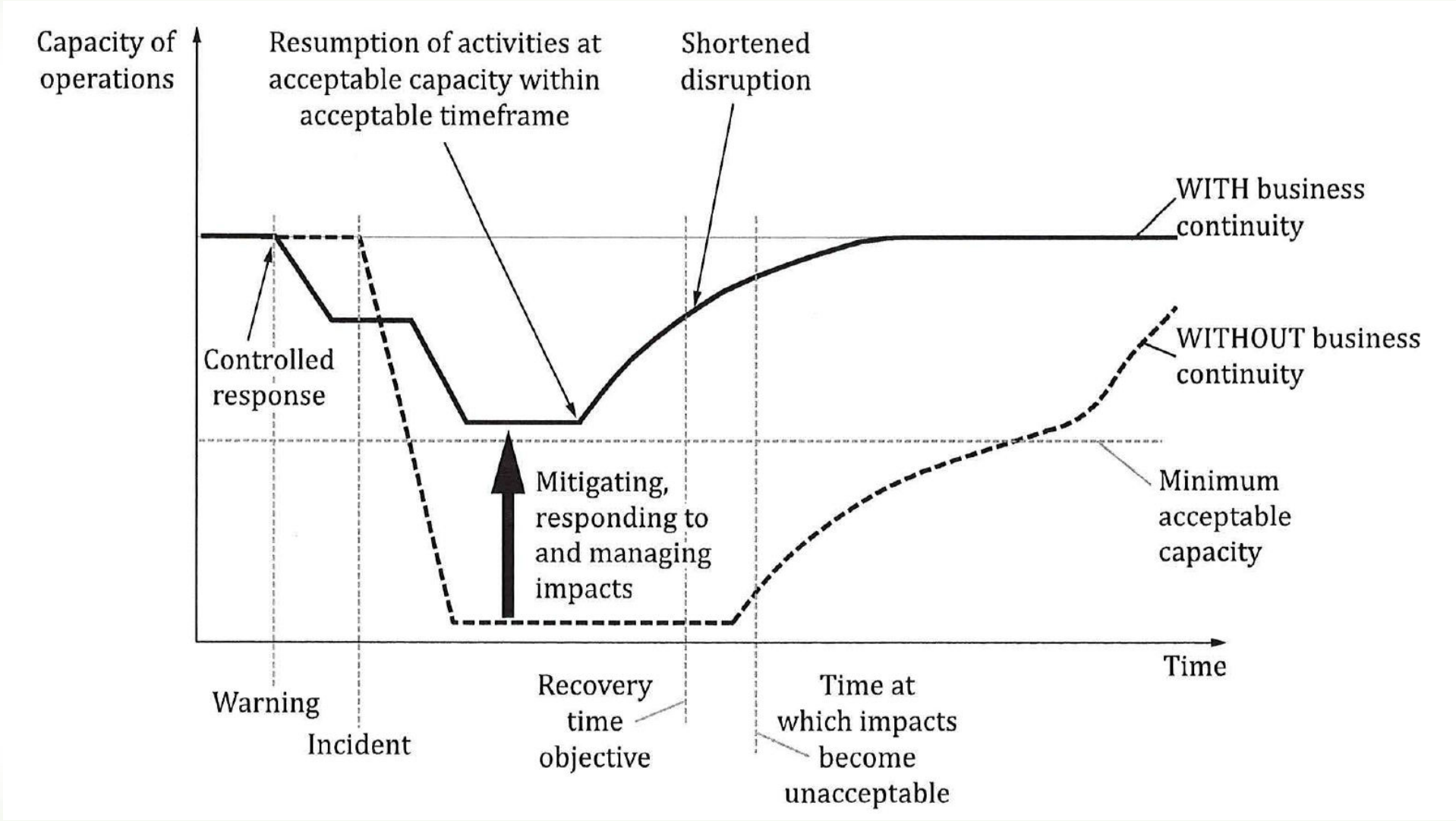
ISO 22301:2019

4. **Strategija neprekinjenega poslovanja**: razvoj strategij in rešitev za obvladovanje identificiranih tveganj in vplivov. To vključuje določanje prioritet za obnovo funkcij in virov, ki so bistveni za delovanje organizacije.
5. **Načrti za neprekinjeno poslovanje**: izdelava načrtov, ki vključujejo postopke in ukrepe za obvladovanje incidentov. Ti načrti zajemajo komunikacijske strategije, naloge in odgovornosti ter postopke za obnovo ključnih funkcij.

ISO 22301:2019

6. **Vaja in testiranje**: redne vaje in testiranja načrtov za neprekinjeno poslovanje omogočajo preverjanje učinkovitosti načrtov in usposabljanje zaposlenih za pravilno ukrepanje med incidenti.
7. **Nenehno izboljševanje**: proces stalnega pregledovanja in izboljševanja BCMS vključuje analizo izvedenih vaj in incidentov, spremljanje skladnosti z zakonodajo in standardi ter prilagajanje načrtov na podlagi novih informacij in izkušenj.
8. **Dokumentacija in nadzor**: ohranjanje ustrezne dokumentacije o vseh elementih BCMS, vključno z načrti, postopki, ocenami tveganj in rezultati testiranj.

ISO 22301:2019



ISO/IEC 27001:2022

Opis zahteve: **kontrola A.5.30** se osredotoča na pripravljenost IKT za neprekinjeno poslovanje, da so IKT sistemi organizacije pripravljeni za neprekinjeno poslovanje, kar vključuje pripravljenost infrastrukture, aplikacij in podatkovnih sistemov. Ključne zahteve:

1. **Analiza vpliva na poslovanje** (angl. Business Impact Analysis - BIA): namen izvajanja analize vplivov na poslovanje je, da se ugotovijo kritični IKT sistemi in storitve, ki so bistveni za delovanje organizacije. To vključuje oceno, kako grožnje in motnje v IKT sistemih vplivajo na poslovne procese.

ISO/IEC 27001:2022

2. **Načrtovanje neprekinjenega poslovanja**: snovanje načrtov in postopkov za zagotavljanje neprekinjenega poslovanja, vključno z obvladovanjem tveganj in strategijami za obnovo v primeru motenj. Ti načrti morajo vključevati varovanje in obnovo IKT sistemov.
3. **Testiranje in preverjanje**: redno testiranje in preverjanje pripravljenosti IKT sistemov za neprekinjeno poslovanje. To vključuje izvajanje vaj in preizkusov, da se zagotovi, da so načrti za neprekinjeno poslovanje učinkoviti in da lahko organizacija v primeru incidentov hitro reagira.

ISO/IEC 27001:2022

4. **Vzdrževanje in nadzor**: kontinuirano spremljanje in vzdrževanje IKT sistemov ter spremljanje njihove pripravljenosti za neprekinjeno poslovanje. To vključuje redne preglede in posodobitve načrtov ter prilagajanje na podlagi novih informacij in sprememb v poslovnem okolju – kontekstu organizacije.
5. **Integracija z drugimi področji**: kontrola A.5.30 mora biti usklajena z drugimi ukrepi in politikami v okviru sistema upravljanja informacijske varnosti, vključno z zaščito pred grožnjami, obvladovanjem ranljivosti in varovanjem informacij.

NIST 800-34

Zahteve NIST glede neprekinjenega poslovanja so del širšega okvirja za obvladovanje tveganj v kibernetski varnosti in upravljanja neprekinjenega poslovanja. Podrobneje so opisana v posebnem dokumentu **NIST Special Publication 800-34**. Ključni elementi:

1. **Ocena tveganj in analize vpliva** (angl. Risk Assessment and Business Impact Analysis - BIA): vključuje identifikacijo potencialnih groženj, oceno verjetnosti njihovega uresničenja ter analiziranje njihovega možnega vpliva na organizacijo. BIA pomaga določiti, kateri poslovni procesi so ključni in kakšen bi bil vpliv motenj na te procese.

NIST 800-34

2. **Razvoj in implementacija strategij neprekinjenega poslovanja**: na podlagi rezultatov ocene tveganj in BIA organizacije razvijejo strategije za zagotavljanje neprekinjenega poslovanja. To vključuje določanje prioritet za obnovo funkcij, določanje alternativnih lokacij za poslovanje, načrte za obnovo podatkov in infrastrukture ter zagotavljanje potrebnih virov.

NIST 800-34

3. **Načrti za odzivanje na incidente, upravljanje kriz in obnovo** (angl. Incident Response, Crisis Management, and Recovery Plans): priporoča pripravo in dokumentiranje načrtov za odzivanje na incidente, ki vključujejo postopke za hitro obvladovanje in zmanjšanje vpliva incidentov. Ti morajo nasloviti tako organizacijske, tehnične, informacijske kot človeške vidike zagotavljanja razpoložljivosti. Krizni načrti zajemajo strategije za komuniciranje in upravljanje med kriznimi situacijami. Načrti za obnovo pa določajo korake za obnovitev normalnega delovanja organizacije po incidentu.

NIST 800-34

4. **Testiranje in redne vaje** (angl. Testing and Exercises): so ključni za preverjanje učinkovitosti načrtov za neprekinjeno poslovanje. To vključuje simulacije različnih scenarijev motenj, s čimer se preveri pripravljenost in usposobljenost osebja ter učinkovitost tehničnih in organizacijskih ukrepov.
5. **Nenehno izboljševanje**: poudarja pomembnost nenehnega izboljševanja procesov za neprekinjeno poslovanje. To vključuje redne preglede in posodobitve načrtov ter prilagoditve na podlagi povratnih informacij iz vaj, incidentov in spreminjajočih se groženj.

NIST 800-34

6. **Dokumentacija in vodenje zapisov**: vse ključne informacije, povezane z neprekinjenim poslovanjem, morajo biti ustrezno dokumentirane. To vključuje načrte, postopke, rezultate testiranj, poročila o incidentih in druge relevantne informacije. Poudarja pomen vzdrževanja ažurnih in natančnih zapisov za podporo odločanju in skladnost z regulativnimi zahtevami.
7. **Integracija z drugimi področji upravljanja tveganj**: procesi za neprekinjeno poslovanje morajo biti usklajeni z drugimi procesi za obvladovanje tveganj, kot so informacijska varnost, fizična varnost in krizno upravljanje. S tem zagotovimo celovit pristop k zaščiti organizacije pred različnimi vrstami groženj in ranljivosti.

Koraki za uvedbo sistema neprekinjenega poslovanja

Izdelava politike neprekinjenega poslovanja	Izvedba analize ocene učinka - BIA	Prepoznavanje preventivnih ukrepov	Snovanje strategij neprekinjenega poslovanja	Izdelava načrtov neprekinjenega poslovanja	Planiranje testiranj, usposabljanj, vaj	Planiranje vzdrževanja in izboljševanje
• Prepoznavanje statutarnih in regulativnih zahtev • Snovanje politike - izjave • Objava politike	• Opredelitev procesov in njihove kritičnosti za neprekinjeno poslovanje - okrevanje • Prepoznavanje in ocenjevanje učinkov na neprekinjenost delovanja in ocena časov izpada • Opredeljevanje potrebnih virov • Opredeljevanje prioritet za okrevanje sistema	• Opredeljevanje kontrol • Uvedba kontrol • Vzdrževanje kontrol	• Varnostno kopiranje in obnova • Opredeljevanje vlog in odgovornosti • Določevanje rezervnih lokacij • Opredeljevanje opreme in drugih virov ter stroškov • Integracije v arhitekturo organizacije	• Dokumentiranje strategij(e) okrevanja	• Planiranje testiranja • Usposabljanje osebja • Planiranje vaj • Izvajanje planov	• Pregledovanje in posodabljanje načrtov • Koordinacija z notranjimi in zunanjimi udeleženci • Razdeljevanje posodobljenih načrtov

Sklepne misli in ključne točke

1. Pomen neprekinjenega poslovanja.
2. Zakonodajni okvir.
3. Standardi in dobre prakse.
4. Redundanca in varnost informacij.
5. Pripravljenost zaposlenih.
6. Pomen analize tveganj – BIA.
7. Vključevanje deležnikov.

Hvala.

SIQ | 60