PAN
PEK

BIA workshop

Radionica - Analiza utjecaja na poslovanje

dr.sc. Daniel Bara, CISO

Sadržaj

kontekst BIA

kontekst BIA

- ZKS/NIS2 traži dokaz upravljanja kontinuitetom poslovanja
- Organizacija je po ZKS-u *važan subjekt* što znači veći fokus na otpornost
- BIA je poslovni temelj za definiranje prioriteta oporavka
- Rezultat BIA-e ulazi u BCP/DR i mjere sigurnosti

Zašto sada?

- incidenti i prekidi više nisu ***ako***, nego *kada*
- proizvodnja i retail traže visoku dostupnost
- ovisnosti (dobavljači, IT, energenti) su veće nego prije
- BIA nam daje redoslijed: što prvo spašavamo

Što je BIA?

Analiza utjecaja na poslovanje ukoliko proces ili sustav prestane raditi.

fokus

- procesi
- NE tehnologija

rezultat

- prioriteti
- tolerancije prekida

Što BIA nije

- nije audit ni inspekcija
- nije tehnički dizajn rješenja
- nije traženje “krivca”
- nije lov na savršene brojke

ključni pojmovi

- **Kritični proces** -> Aktivnost bez koje tvrtka ne može normalno poslovati (npr. proizvodnja, prodaja, logistika)
- Maksimalni prekid (Maximum Tolerable Period of Disruption - MTPD) Koliko dugo realno možemo dopustiti da proces ne radi prije nego šteta postane ozbiljna.
- Cilj oporavka (Recovery Time Objective - RTO) - U kojem roku moramo vratiti sustav u rad da izbjegnemo veće posljedice.
- Gubitak podataka (Recovery Point Objective - RPO) - Koliko podataka smijemo izgubiti
- Manual fallback - Možemo li privremeno raditi *ručno* i koliko dugo to ima smisla.

primjer 1: proizvodnja +maloprodaja

PAN PEK

Zamislimo da POS sustav padne u 10:00.

MTPD (Maximum Tolerable Period of Disruption)

- Koliko dugo prodavaonica može raditi bez POS-a prije nego šteta postane neprihvatljiva?
  - 30 min → neugodno
  - 2 sata → gubimo promet
  - 1 dan → neprihvatljivo

  MTPD = 4 sata

- To znači: Ako POS ne radi dulje od 4 sata, posljedice su ozbiljne (gubitak prihoda, reputacija, fiskalni problem).

primjer 1: proizvodnja +maloprodaja

PAN PEK

RTO (Recovery Time Objective)

U kojem roku POS mora ponovno raditi?

- Ako je MTPD 4 sata, RTO mora biti kraći.
- RTO = 2 sata

- To znači: IT mora vratiti POS sustav u funkciju unutar 2 sata.

RPO (Recovery Point Objective)

Koliko podataka smijemo izgubiti?

- Ako POS padne u 10:00, zadnji backup je u 9:45.
- Možemo li izgubiti 15 minuta prometa?
  - DA → RPO = 15 minuta
  - NE → RPO mora biti npr. 5 minuta
- RPO = 15 minuta
- To znači: U najgorem slučaju možemo izgubiti najviše 15 minuta podataka.

MTPD govori kada nastaje ozbiljan problem.
RTO govori kada sustav mora ponovno raditi.
RPO govori koliko podataka smijemo izgubiti.

Drugim riječima:

MTPD = granica tolerancije
RTO = cilj oporavka
RPO = prihvatljiv gubitak podataka

Zašto BIA

Zakonska obaveza (ZKS)

Važan subjekt mora znati koje su mu kritične funkcije i koliki je prihvatljiv prekid rada.
👉 BIA je dokaz regulatoru da razumijemo vlastite rizike.

Temelj za kontinuitet (BCP / DR)

Ne možemo planirati oporavak ako ne znamo: što je najvažnije I koliko brzo mora biti vraćeno
👉 BIA određuje što ide prvo, a što može čekati.

Definiranje prioriteta oporavka

Svi sustavi nisu jednako važni.
Proizvodnja = marketing web stranica
POS = interni reporting
👉 BIA daje redoslijed vraćanja sustava.

Upravljanje poslovnim rizicima

Prekid rada znači gubitak prihoda, regulatorne posljedice, reputacijski udar
👉 BIA prevodi IT rizik u poslovni utjecaj.

BIA OBUHVAT – LANAC VRIJEDNOSTI

NABAVA
Sirovine • Dobavljači

PROIZVODNJA
Planiranje • Irzada
Sigurnost hrane

LOGISTIKA
Skladište • Dostava

RETAIL
Naplata
• Kupci

VELEPRODAJA
Ugovori • Isporuka

PODRŽAVAJUĆE I REGULATORNE FUNKCIJE

IT
Sustavi & Infrastruktura

FINANCIJE
Plačanja & Obveze

HR
Ljudi & Evidencije

KVALITETA
HACCP & Sljedivost

INVESTICIJE / ENERGIJA
Energenti & Objekti

BIA obuhvača cjelokupan lanac vrijednosti – od sirovine do kupca, uključujući regulatorne i infrastrukturne funkcije.

ključni procesi

PAN PEK

proizvodnja

- Proizvodnja pekarskih proizvoda
- Planiranje proizvodnje
- Kontrola sigurnosti hrane
- Upravljanje proizvodnim resursima

logistika i distribucija

- Planiranje i organizacija isporuka
- Upravljanje skladištem
- Dostava prodavaonicama i kupcima
- Koordinacija s prijevoznicima

retail (maloprodaja)

- Naplata i fiskalizacija
- Upravljanje zalihama u trgovinama
- Interakcija s kupcima
- Upravljanje dnevnim prometom

veleprodaja

- Obrada veleprodajnih narudžbi
- Ugovorno upravljanje kupcima
- Fakturiranje i isporuka
- Upravljanje SLA i rokovima

ključni procesi

financije i računovodstvo

- Obračun i plaćanja
- Upravljanje likvidnošću
- Regulatorna izvješća
- Fiskalne i porezne obveze

hr

- Obračun plaća
- Evidencija radnog vremena
- Upravljanje zaposlenicima
- Podrška u kriznim situacijama

nabava

- Nabava sirovina i ambalaže
- Upravljanje dobavljačima
- Alternativni izvori opskrbe
- Upravljanje lead time-ovima

Investicije / Održavanje / Energenti

- Upravljanje objektima i opremom
- Opskrba energijom (struja, plin, voda)
- Tehničko održavanje pogona
- Fizička otpornost infrastrukture

ključni procesi

PAN PEK

it

- Održavanje poslovnih aplikacija
- Upravljanje infrastrukturom
- Sigurnost i zaštita podataka
- Podrška ključnim sustavima

qa

- Kontrola sigurnosti hrane
- Sljedivost i dokumentacija
- Upravljanje incidentima i recallom
- Regulatorna komunikacija

Što očekujemo od svakog odjela

Identificirati kritične procese

- Procijeniti posljedice prekida

- Identificirati ovisnosti

Definirati toleranciju prekida

tolerancija

BIA po odjelima

1. radionica
Strukturirani razgovor o procesima i rizicima.

2. tablice
Proces → Sustavi → Ovisnosti → Utjecaj.

3. validacija
Provjera s vlasnicima procesa i IT-om.

4. konsolidacija
Objedinjavanje rezultata na razini Društva
i definiranje prioriteta oporavka.

PAN
PEK

BIA - proizvodnja

proizvodnja

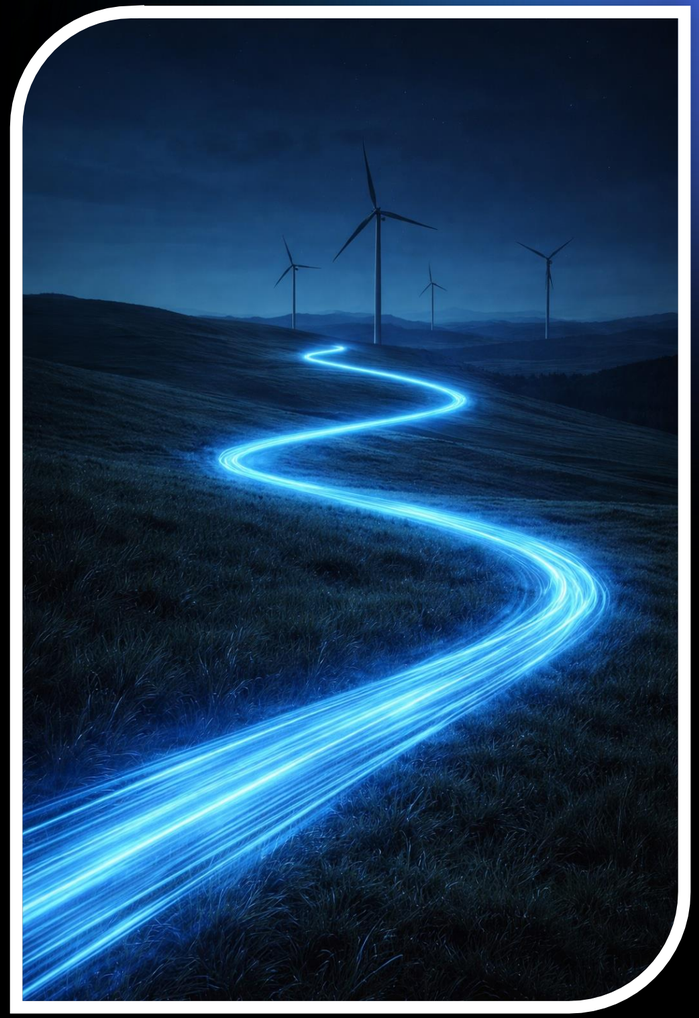
- Koja je osnovna svrha proizvodnje u poslovanju?
- Koji su 3–5 procesa bez kojih proizvodnja ne može funkcionirati?
- Postoje li procesi koji su vremenski osjetljivi?
- Postoje li procesi vezani uz zakonske / IFS / HACCP obveze?

regulatorni i sigurnosni rizici

- Postoji li rizik ugrožavanja zdravstvene ispravnosti hrane?
- Postoji li rizik povlačenja proizvoda (recall)?
- Koji procesi imaju certifikacijske obveze?
- Postoje li zakonske posljedice prekida?

ovisnosti o energentima i infrastrukturi

- Ovisi li proizvodnja o:
  - struji
  - plinu
  - vodi
- Postoji li rezervni izvor?
- Koliko dugo možemo raditi bez pojedinog energenta?
- Što se događa kod potresa / požara / poplave?



posljedice prekida

što se događa ako proizvodnja stane?

- 2 sata?
- 1 dan?
- više dana?

postoje li:

- gubici sirovina?
- kvarenje?
- gubitak ljudi?
- rizik recall-a?

IT i podaci

- Koji IT sustavi su nužni?
- Postoji li manualni rad?
- Ovisi li proizvodnja o vanjskim dobavljačima?
- Koji proces bi bio među prvih 5 za oporavak?

- Koliko dugo može biti prekinut proces? (MTPD)
- U kojem roku mora raditi? (RTO)
- Koliko podataka smijemo izgubiti? (RPO)

sljedeći koraci

Završetak BIA po odjelima

- Održavanje radionica / intervjua
- Popunjavanje BIA Excel tablica
- Validacija odgovora s voditeljima

Konsolidacija i Top 10 kritičnih procesa

Rangiranje procesa prema:

- poslovnom utjecaju
- regulatornom riziku
- vremenskoj osjetljivosti

Definiranje liste najkritičnijih funkcija

Definiranje prioriteta oporavka

- Utvrđivanje MTPD / RTO / RPO
- Određivanje redoslijeda oporavka
- Identifikacija ključnih ovisnosti

- ——

Izrada BCP / DR planova

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Definiranje kriznih procedura
- Plan testiranja i provjere učinkovitosti

PAN
PEK

"

BIA nam omogućuje da u krizi reagiramo prema prioritetima, a ne prema panici.

PAN
PEK

Hvala na pažnji