Gap analiza – Pan-pek (NIS2/ZKS)

Ovaj dokument prikazuje gap analizu usklađenosti Pan-peka s NIS2 direktivom i Zakonom o kibernetičkoj sigurnosti (ZKS). Analiza je napravljena na temelju trenutno dostupnih informacija o organizaciji, IT sustavima, sigurnosnim kontrolama i postojećoj dokumentaciji.

Kontrola / Zahtjev (NIS2)	**Stanje u Pan-peku**	**Dokaz**	**Status**	**Preporuka**
Politike i procedure kibernetičke sigurnosti	Osnovna dokumentacija postoji, pravilnici djelomično pokrivaju IS, GDPR dokumentacija kompletna	Politike IS, GDPR registar	Djelomično	Razviti pun ISMS okvir ili minimalno formalne politike IS u skladu s NIS2
Incident management	Proces nije dokumentiran, postoji CISO ali bez formalnog IR plana	Interna praksa	Nije implementirano	Izraditi Incident Response Plan, definirati procedure izvještavanja prema CERT-u
BCP i DR (kontinuitet poslovanja)	Ne postoji formalna dokumentacija ni testiranje	-	Nije implementirano	Razviti BCP i DR plan, uključiti testiranje oporavka
IAM (Identity & Access Management)	Nema sustava, pristupi se dijelom kontroliraju ručno, MFA djelomično uveden	O365 postavke	Djelomično	Implementirati IAM rješenje + proširiti MFA na sve korisnike
Antivirus / EDR	Antivirus postoji, Wazuh instaliran ali nije u pogonu	Antivirus licence, Wazuh agenti	Djelomično	Pustiti Wazuh u produkciju, razmotriti EDR/XDR
Backup i oporavak	Backup postoji, ali bez testiranja oporavka	Backup logovi	Djelomično	Uvesti redovite DR testove i procedure
VPN i udaljeni pristupi	VPN postoji, MFA nije za sve	VPN konfiguracija	Djelomično	MFA obvezan za sve udaljene

				pristupe
Fizička sigurnost	Biometrija na ulazu, kontrola ulaza, video nadzor, server soba osigurana	Kontrola pristupa	Implementirano	Redovito testirati sustave i ažurirati procedure
Obuka zaposlenika	Provedena osnovna GDPR obuka, nema kontinuiranog IS awareness programa	Evidencija obuka	Djelomično	Uvesti redovite edukacije i phishing simulacije
Onboarding/offboarding	Nije dokumentirano	-	Nije implementirano	Dokumentirati i automatizirati onboarding i offboarding procese
Suradnja s CERT-om i prijava incidenata	Pan-pek važan entitet, formalni proces prijave nije postavljen	-	Nije implementirano	Uspostaviti formalni proces prijave i komunikacije s CERT-om
Upravljanje trećim stranama	ERP SPIN, O365 cloud, dio vanjskih vendora, ali bez formalnih sigurnosnih zahtjeva	Ugovori s dobavljačima	Djelomično	Uvesti sigurnosne zahtjeve i SLA kontrole za dobavljače
Rizici i procjena prijetnji	Nema sustavne procjene rizika	-	Nije implementirano	Uvesti formalni proces procjene rizika (ISO 27005 ili slično)

Glavni identificirani gapovi

1. Nema BCP/DR dokumentacije ni testiranja.
2. Nema formalnog Incident Response Plana ni procesa prijave prema CERT-u.
3. IAM i MFA nisu u potpunosti implementirani.
4. Wazuh nije u pogonu, nema aktivnog SIEM/EDR-a.
5. Obuke zaposlenika nisu redovite niti strukturirane.
6. Onboarding/offboarding procesa nema.
7. Procjena rizika i upravljanje dobavljačima nisu sustavno provedeni.
8.

Zagreb, 14.6.2025