Proces usklađenja s NIS2 i koristi za organizacije koje nisu obveznici NIS2 u Hrvatskoj

Od Regulatornog Tereta do Ključne Konkurentske Prednosti

Sponsored by

embarcadero

Mladen Kuzminski, mag.inf.

- 25+ godina iskustva u projektiranju informacijskih sustava
- Voditelj predstavništva Embarcadero / IDERA / Sencha / Yellowfin / PreEmptive / Kiuwan za Adriatik - Balkan
- IRCA Lead auditor za ISO 27001
- Autor 14 stručnih knjiga i udžbenika
- https://www.linkedin.com/in/mladen/

KONTO d.o.o. Požega, Varaždin

- Osnovano 1993. Razvoj poslovnih aplikacija.
- ISO 9001, ISO 27001, ISO15489, aAa bonitet
- Distributer Embarcadero / IDERA / Sencha / Yellowfin / PreEmptive / Kiuwan / DerScanner za Adriatik - Balkan
- www.konto.hr

NIS2

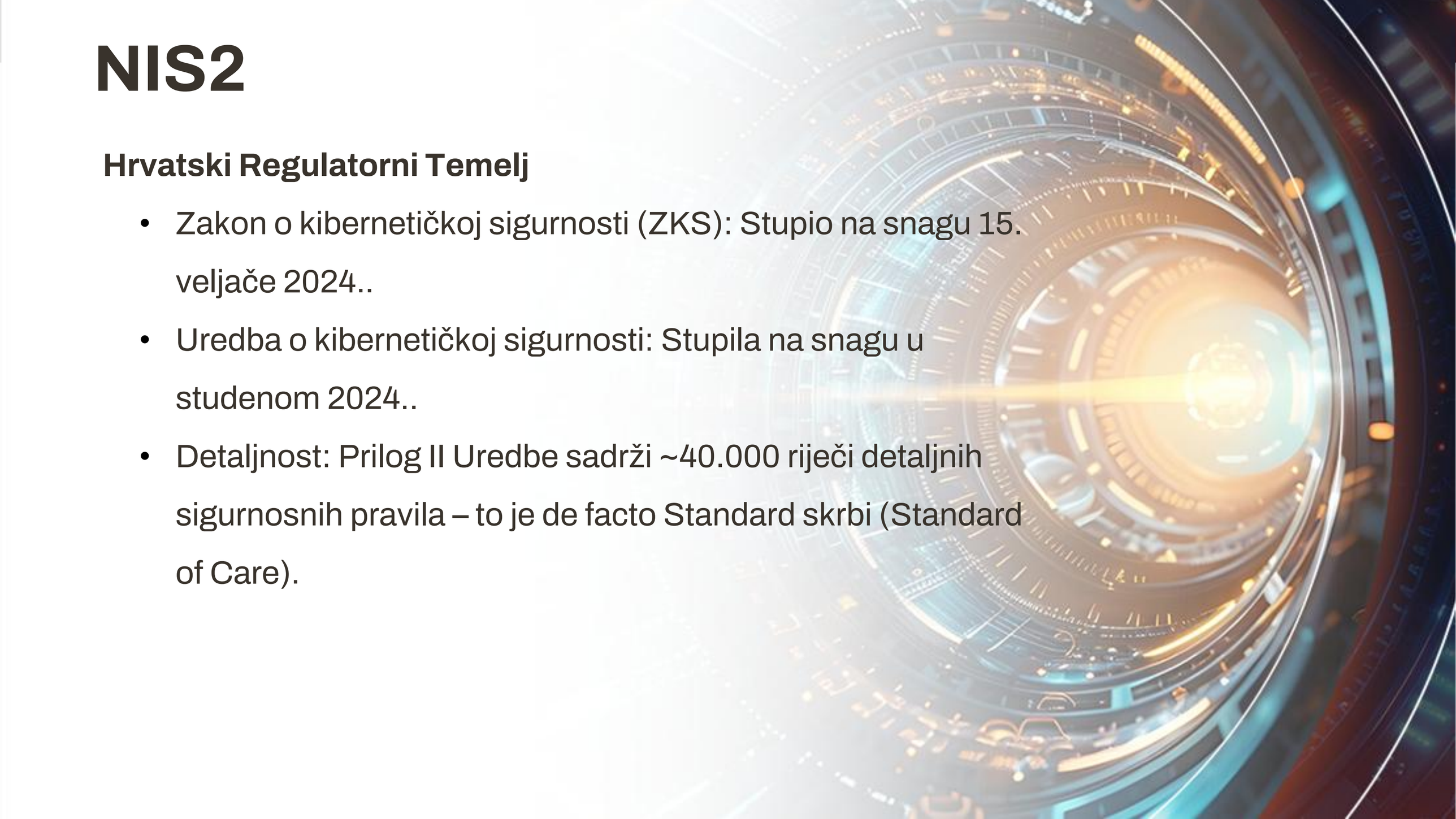
Zašto je NIS2 Prekretnica?

- Direktiva (EU) 2022/2555: Cilj je postići visoku zajedničku razinu kibernetičke sigurnosti u EU.
- Proširen Opseg: Uključuje ključne sektore (Energetika, Bankarstvo, Zdravstvo, Digitalna infrastruktura).
- Ključni Rok: Obvezan prijenos u nacionalno zakonodavstvo do 17. listopada 2024.
- Naglašava potrebu za upravljanjem rizicima, preventivnim mjerama, kao i prijavljivanjem incidenta.
- Odgovornost Uprave: Upravljačka tijela direktno odgovaraju za neusklađenost (korporativno upravljanje).

NIS2

Hrvatski Regulatorni Temelj

- Zakon o kibernetičkoj sigurnosti (ZKS): Stupio na snagu 15. veljače 2024..
- Uredba o kibernetičkoj sigurnosti: Stupila na snagu u studenom 2024..
- Detaljnost: Prilog II Uredbe sadrži ~40.000 riječi detaljnih sigurnosnih pravila – to je de facto Standard skrbi (Standard of Care).



Ključne promjene

- **Prošireni opseg primjene**: NIS2 Direktiva se odnosi na veći broj sektora, uključujući energetski sektor, financijske institucije, zdravstvo, vodovod, digitalne usluge, javnu upravu, proizvodne tvrtke i mnoge druge.
- **Striktniji sigurnosni zahtjevi**: Tvrtke moraju implementirati strože mjere za upravljanje rizicima i odgovaranje na kibernetičke incidente.
- **Kaznene mjere**: Kazne za nepoštivanje NIS2 Direktive mogu doseći visoke iznose, uključujući i financijske sankcije od nekoliko milijuna eura.

Kategorizacija Poslovnih Subjekata

- **Ključni subjekti:** organizacije koje djeluju u sektorima od vitalnog značaja za društvo: energetika, promet, zdravstvo, bankarstvo, infrastruktura financijskog tržišta, voda, digitalna infrastruktura te javna uprava. Ovi subjekti moraju ispuniti najstrože zahtjeve, uključujući redovite i ciljani nadzor i obavezno izvještavanje o incidentima.
- **Važni subjekti:** organizacije koje pružaju usluge od velikog značaja za funkcioniranje društva. Primjeri subjekti iz sektora poštanskih i kurirskih usluga, upravljanja otpadom, prehrambene industrije te pružatelje digitalnih usluga. Primjena je fleksibilnija, s naglaskom na samoprocjenu i povremene revizije

Rokovi i postupci za usklađivanje

- **Obavještavanje o kategorizaciji:** Nadležna tijela moraju do 15. veljače 2025. dostaviti obavijesti o kategorizaciji poslovnih subjekata. Po primitku te obavijesti, organizacije imaju rok od godinu dana za implementaciju potrebnih mjera.
- **Izvještavanje o incidentima:** Prema Zakonu o kibernetičkoj sigurnosti, nakon dobivanja obavijesti o kategorizaciji, ključni i važni subjekti dužni su u roku od 30 dana početi s redovitim izvještavanjem o sigurnosnim incidentima, što uključuje pravovremeno slanje ranih upozorenja CSIRT-u.
- **Plan provedbe:** Uz obvezu kategorizacije i izvještavanja, predviđeni su i dodatni rokovi za uspostavu planova kontinuiranog poslovanja, provođenje vježbi kibernetičke sigurnosti te usklađivanje tehničkih i organizacijskih mjera.

Ključni zahtjevi NIS2 Direktive

Upravljanje rizicima i sigurnosne mjere

NIS2 Direktiva zahtijeva od subjekata da uvedu adekvatne tehničke, fizičke i organizacijske mjere za smanjenje rizika od cyber napada. Mjere moraju obuhvatiti:

- **Zaštitu mrežnih i informacijskih sustava** od neovlaštenog pristupa, zlonamjernih programa i drugih prijetnji.
- **Upravljanje incidentima**: Subjekti moraju imati planove za odgovor na kibernetičke incidente, uključujući procedure za obavještavanje nadležnih tijela.
- **Oporavak sustava** nakon incidenata, uključujući sigurnosne kopije i mjere za obnovu funkcionalnosti sustava.
- **Kontinuirano praćenje sigurnosti** i provođenje procjena rizika u skladu s promjenama u poslovanju ili tehnologiji.

Upravljanje opskrbnim lancima

Subjekti moraju osigurati sigurnost ne samo vlastitih sustava, već i sustava njihovih dobavljača i partnera. Prema Direktivi, poslovni subjekti moraju:

- Osigurati da dobavljači imaju odgovarajuće sigurnosne mjere.
- Provoditi redovite provjere i revizije sigurnosnih standarda dobavljača.
- Ugovorom osigurati obveze dobavljača u pogledu odgovora na kibernetičke prijetnje

Suradnja i izvještavanje

Povećanje suradnje između privatnog sektora, javnih tijela i nadležnih regulatornih tijela. Obveznici moraju prijavljivati kibernetičke incidente Nacionalnom CERT-u ili odgovarajućem regulatoru u Hrvatskoj, ovisno o vrsti djelatnosti. U ovom kontekstu, od poslovnih subjekata se očekuje:

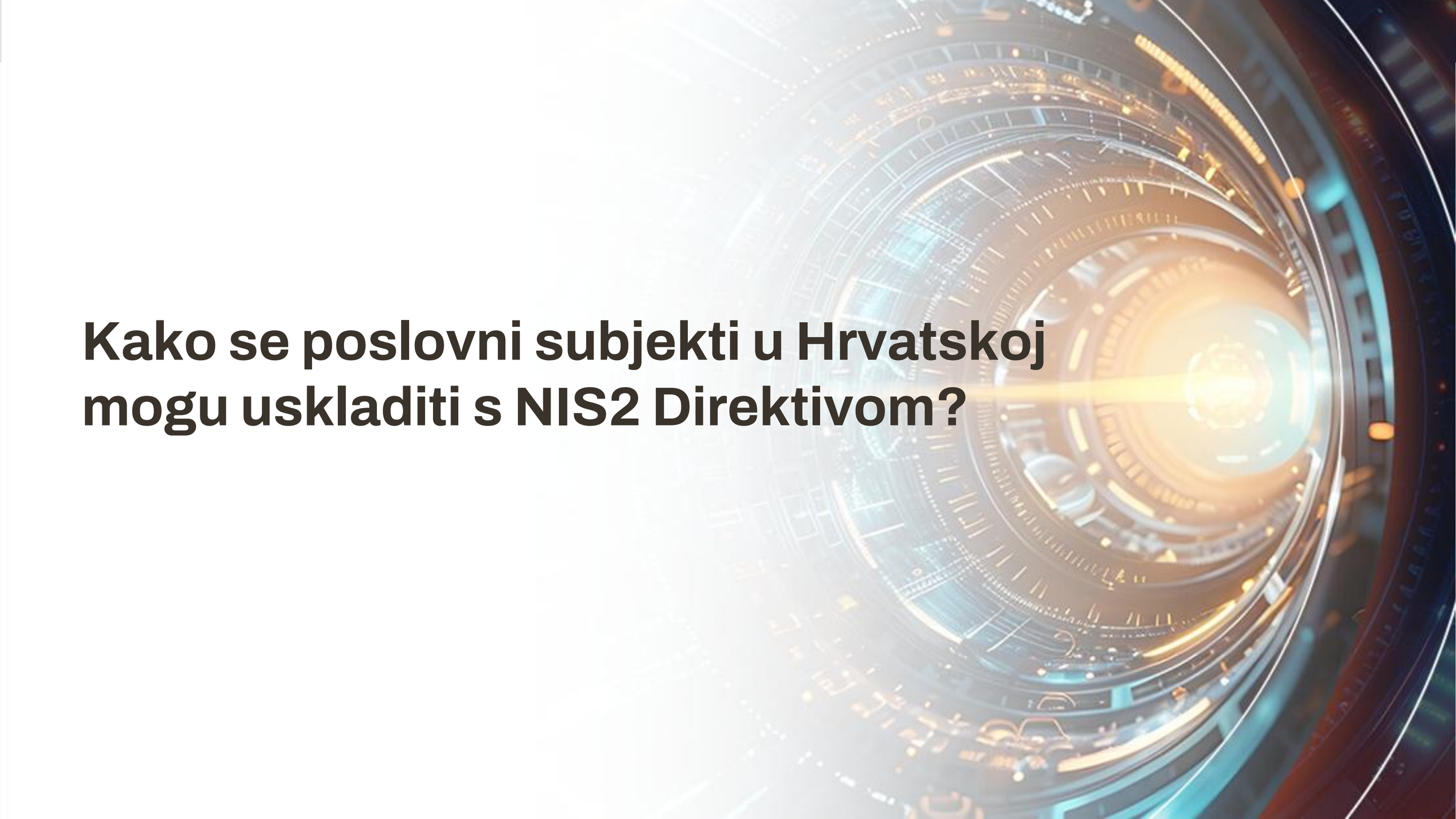
- Pravovremeno prijavljivanje incidenata koji imaju značajan utjecaj na pružanje ključnih usluga.
- Suradnja s Nacionalnim CERT-om u cilju istraživanja incidenata.
- Osiguranje povjerljivosti prilikom razmjene informacija o incidentima.

Financijske i organizacijske mjere

Poslovni subjekti moraju alocirati dovoljno resursa za implementaciju sigurnosnih mjera. Ovo uključuje:

- Osiguranje dovoljnog broja obučenih kadrova za upravljanje sigurnošću mrežnih i informacijskih sustava.
- Ulaganje u edukaciju zaposlenika o prijetnjama i odgovorima na kibernetičke incidente.
- Kontinuirana procjena i poboljšanje sigurnosne politike unutar organizacije.

Kako se poslovni subjekti u Hrvatskoj mogu uskladiti s NIS2 Direktivom?



Procjena trenutne sigurnosne situacije

Prvi korak u procesu usklađivanja je provođenje sveobuhvatne procjene trenutne razine sigurnosti informatičkih sustava i mreža. Tu spada sljedeće:

- Utvrđivanje pripada li organizacija obveznicima
- Mapiranje postojećih sigurnosnih mjera
- Identifikacija jaza između trenutnog stanja i zahtjeva
- Procjena resursa potrebnih za usklađenje
- Definiranje plana i prioriteta implementacije

Uvođenje sigurnosnih standarda

Nakon procjene trenutnog stanja, organizacije trebaju uspostaviti sigurnosne standarde u skladu s najboljim praksama i međunarodnim standardima, kao što su:

- **ISO 27001**: Međunarodni standard za upravljanje informacijskom sigurnošću.
- **NIST Cybersecurity Framework**: Okvir za upravljanje rizicima kibernetičke sigurnosti.
- Ovi standardi pomažu u organizaciji i implementaciji sigurnosnih mjera koje su u skladu s NIS2 zahtjevima.

Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

Ovo je temelj NIS2 usklađenja. Znači stvaranje strukturiranog pristupa kako organizacija identificira, procjenjuje i upravlja kibernetičkim rizicima. Sustav mora biti dokumentiran, redovito ažuriran i integriran u cjelokupno poslovno upravljanje.

Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

1. Identifikacija kritičnih informacijskih sustava

- Određivanje koji IT sustavi su najvažniji za poslovanje (npr. ERP, CRM, email, financijski sustavi)
- Mapiranje svih digitalnih resursa - serveri, mreže, aplikacije, baze podataka
- Procjena što bi se dogodilo ako bi ti sustavi bili nedostupni (financijski gubitak, zastoj poslovanja, regulatorne posljedice, reputacijski gubitak)

Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

2. Procjena prijetnji i ranjivosti

- Prijetnje: Što vas može napasti? (ransomware, phishing, DDoS napadi, unutarnje prijetnje, prirodne katastrofe)
- Ranjivosti: Gdje su vaše slabosti? (zastarjeli software, slabe lozinke, neažurni sustavi, neobučeni zaposlenici)
- Kombinacija prijetnje * ranjivosti = rizik

Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

3. Definiranje mjera za ublažavanje rizika

Nakon što znate rizike, određujete kako ih kontrolirati:

- Izbjeći rizik (npr. ne koristiti određenu tehnologiju)
- Smanjiti rizik (implementirati zaštitne mjere)
- Prenijeti rizik (osiguranje)
- Prihvatiti rizik (svjesno živjeti s njim ako je nizak)

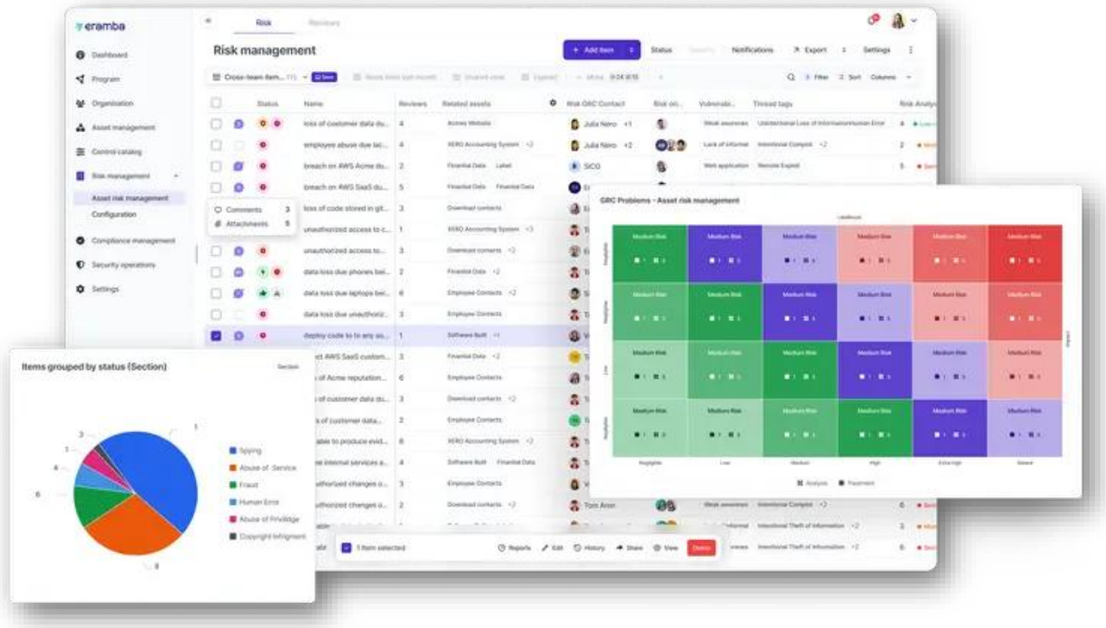
Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

4. Redovito ažuriranje analize rizika

- Prijetnje se mijenjaju - nova vrsta malwarea, nove metode napada
- Vaša infrastruktura se mijenja - novi sustavi, novi zaposlenici
- Analiza rizika mora biti živi dokument, ne jednokratna aktivnost
- Preporuka: revizija minimalno jednom godišnje ili nakon značajnih promjena

Uspostava sustava upravljanja rizicima kibernetičke sigurnosti

Primjer iz prakse – Eramba GRC (Governance, Risk, and Compliance) napredni opensource sustav za upravljanje regulativom.



https://www.eramba.org/

Implementacija tehničkih i organizacijskih mjera

1. Sigurnost mreža i informacijskih sustava

Što to znači:

- Zaštita IT infrastrukture od neovlaštenog pristupa i napada
- Implementacija tehničkih kontrola na svim razinama

Konkretne mjere:

- Firewalli - barijera između vaše mreže i interneta
- Segmentacija mreže - odvajanje kritičnih sustava od manje važnih
- IDS/IPS sustavi - detekcija i prevencija upada
- Antivirusna/anti-malware rješenja - ažurirana i aktivna zaštita
- VPN - sigurna udaljena povezivost zaposlenika
- Patch management - redovito ažuriranje softwarea i zatvaranje sigurnosnih rupa

Implementacija tehničkih i organizacijskih mjera

2. Upravljanje incidentima - detekcija, odgovor, oporavak

Što to znači:

- Sustav za brzo prepoznavanje, reakciju i oporavak od sigurnosnih incidenata.

Faze:

A) DETEKCIJA:

- SIEM alati (Security Information and Event Management) - prate logove i aktivnosti
- Monitoring 24/7 - kontinuirano praćenje sumnjivog ponašanja
- Alarmiranje - automatsko obavještavanje o anomalijama

Implementacija tehničkih i organizacijskih mjera

2. Upravljanje incidentima - detekcija, odgovor, oporavak

B) ODGOVOR:

- Incident response tim - tko je odgovoran, koje su uloge
- Incident response plan - dokumentirani koraci što raditi
- Izolacija zaraženih sustava - sprečavanje širenja
- Forenzička analiza - kako se incident dogodio
- Komunikacija - obavještavanje uprave, klijenata, nadležnih tijela

Implementacija tehničkih i organizacijskih mjera

2. Upravljanje incidentima - detekcija, odgovor, oporavak

C) OPORAVAK:

- Obnova sustava iz čistih backupa
- Provjera integriteta - jesu li sustavi čisti
- Post-incident review - što smo naučili, kako spriječiti slično u budućnosti

Implementacija tehničkih i organizacijskih mjera

3. Kontinuitet poslovanja i disaster recovery planovi

Što to znači:

- Osigurati da organizacija može nastaviti poslovati čak i nakon ozbiljnog incidenta.

Ključni elementi::

- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)

Implementacija tehničkih i organizacijskih mjera

3. Kontinuitet poslovanja i disaster recovery planovi

Business Continuity Plan (BCP):

- Identifikacija kritičnih poslovnih procesa
- Definiranje maksimalnog prihvatljivog vremena prekida (RTO - Recovery Time Objective)
- Definiranje maksimalnog prihvatljivog gubitka podataka (RPO - Recovery Point Objective)
- Alternativni načini rada tijekom incidenta (npr. rad s papirima ako sustavi ne rade)

Implementacija tehničkih i organizacijskih mjera

3. Kontinuitet poslovanja i disaster recovery planovi

Disaster Recovery Plan (DRP):

- Backup strategija - što, kada i gdje se backupira
- 3-2-1 pravilo: 3 kopije podataka, na 2 različita medija, 1 offsite (izvan lokacije)
- Redundantni sustavi - duplirani serveri, mreže
- Alternativna lokacija - sekundarni data centar ili cloud rješenje
- Redovno testiranje - simulacija katastrofe i provjera funkcionira li plan

Implementacija tehničkih i organizacijskih mjera

4. Sigurnost lanca opskrbe

Što to znači:

- Vaši dobavljači, partneri i podizvođači mogu biti slaba karika u sigurnosti.

Konkretne mjere:

- Due diligence - provjera sigurnosnih praksi dobavljača prije angažmana
- Ugovorne klauzule - sigurnosni zahtjevi u ugovorima
- Redovite provjere - audit dobavljača, certifikati (ISO 27001)
- Pristup po potrebi - dobavljači imaju samo minimalni potrebni pristup
- Monitoring - praćenje aktivnosti trećih strana u vašim sustavima
- Incident response za dobavljače - što ako vaš dobavljač ima incident koji utječe na vas

Implementacija tehničkih i organizacijskih mjera

5. Kontrola pristupa i upravljanje identitetom (IAM - Identity and Access Management)

Što to znači:

- Osigurati da samo ovlaštene osobe mogu pristupiti odgovarajućim sustavima i podacima.

Konkretne mjere:

A) Autentikacija
B) Autorizacija
C) Administracija

Implementacija tehničkih i organizacijskih mjera

5. Kontrola pristupa i upravljanje identitetom (IAM - Identity and Access Management)

A) Autentikacija:

- Jaki password policy - minimalno 12+ znakova, složenost, redovita promjena
- Multi-factor autentikacija (MFA) - obvezna za sve administratorske račune i kritične sustave
- Single Sign-On (SSO) - centralizirano upravljanje prijavama
- Biometrija - otisak prsta, face ID za dodatnu sigurnost

Implementacija tehničkih i organizacijskih mjera

5. Kontrola pristupa i upravljanje identitetom (IAM - Identity and Access Management)

B) Autorizacija:

- Princip najmanje privilegije (Least Privilege) - korisnici imaju samo pristup koji im je nužan za posao
- Segregacija dužnosti - kritične operacije zahtijevaju više osoba
- Role-Based Access Control (RBAC) - pristup temeljem uloge u organizaciji

Implementacija tehničkih i organizacijskih mjera

5. Kontrola pristupa i upravljanje identitetom (IAM - Identity and Access Management)

C) Administracija:

- Redoviti pregled pristupa - tko što može vidjeti i raditi
- Promptno ukidanje pristupa - odmah po odlasku zaposlenika
- Privileged Access Management (PAM) - posebna kontrola administratorskih računa
- Access logs - evidencija tko je i kada pristupao čemu

Implementacija tehničkih i organizacijskih mjera

6. Enkripcija podataka

Što to znači:

- Zaštita podataka šifriranjem kako bi bili nečitljivi neovlaštenim osobama.

A) Data at Rest (podaci u mirovanju):

- Šifriranje hard diskova - Full Disk Encryption (BitLocker, FileVault)
- Šifriranje baza podataka - Transparent Data Encryption (TDE)
- Šifriranje backupa - da ukradeni backup bude beskoristan
- Standardi: AES-256 enkripcija

Implementacija tehničkih i organizacijskih mjera

6. Enkripcija podataka

B) Data in Transit (podaci u prijenosu):

- HTTPS/TLS - sva web komunikacija mora biti šifrirana
- VPN tuneli - šifrirana komunikacija između lokacija
- Email enkripcija - S/MIME ili PGP za osjetljive poruke
- SFTP umjesto FTP - šifriran prijenos datoteka

C) Data in Use (podaci u upotrebi):

- Enkripcija u memoriji - najnovija tehnologija za zaštitu podataka dok se obrađuju
- Secure enclaves - izolirano izvođenje kritičnih operacija

Implementacija tehničkih i organizacijskih mjera

6. Enkripcija podataka

Upravljanje ključevima:

- Key Management System (KMS) - sigurno čuvanje enkripcijskih ključeva
- Rotacija ključeva - redovna promjena
- Backup ključeva - u slučaju gubitka (ali ekstremno sigurno čuvan)

Implementacija tehničkih i organizacijskih mjera

KAKO OVO IMPLEMENTIRATI U PRAKSI?

Za male organizacije:

- Počnite s osnovama: antivirusni, firewall, backup, MFA
- Postupno dodajte složenije mjere
- Koristite cloud rješenja koja već imaju ugrađene mnoge zaštite

Za srednje/velike organizacije:

- Angažirajte CISO ili sigurnosnog konzultanta
- Investirajte u SIEM, PAM i naprednije alate
- Uspostavite sigurnosni operativni centar (SOC)

Troškovi:

- Mali: 5,000-20,000 EUR godišnje
- Srednji: 50,000-200,000 EUR godišnje
- Veliki: 500,000+ EUR godišnje

Ali upamtite: **jedan ozbiljan incident može koštati daleko više!**

Upravljanje i odgovornost

1) Imenovanje odgovornih osoba za kibernetičku sigurnost

Što to znači:

- Mora postojati jasna odgovornost - tko je zadužen za kibernetičku sigurnost u organizaciji.

Uprava / Nadzorni odbor
↓
CISO / Sigurnosni menadžer
↓
├── IT sigurnosni tim
├── Incident Response Team
├── DPO
└── Security Champions (u raznim odjelima)

Važno: Ove osobe moraju imati:

- Formalno imenovanje (pisano)
- Odgovarajuće ovlasti i proračun
- Izravan pristup upravi
- Vrijeme i resurse za obavljanje uloge

Upravljanje i odgovornost

2. Aktivno sudjelovanje uprave u nadzoru

Što to znači:

- NIS2 eksplicitno čini upravu (CEO, članovi uprave) osobno odgovornima za kibernetičku sigurnost. Ovo je velika promjena!

Konkretne odgovornosti uprave:

A) Strateška razina:

- Odobravanje sigurnosne strategije - uprava mora razumjeti i podržati sigurnosne ciljeve
- Odobravanje proračuna - izdvajanje dovoljno sredstava za sigurnost
- Postavljanje prioriteta - prepoznavanje sigurnosti kao poslovnog prioriteta
- Integracija u poslovnu strategiju - sigurnost nije odvojena, već dio ukupne strategije

Upravljanje i odgovornost

2. Aktivno sudjelovanje uprave u nadzoru

B) Nadzor:

- Redovita izvješća - minimalno kvartalno o stanju sigurnosti
- Praćenje KPI-jeva - brojevi incidenata, vrijeme odgovora, uspješnost testova
- Sudjelovanje u vježbama - tabletop exercises, simulacije kriza
- Pregled audita - analiza nalaza internih i eksternih revizija

Primjer izvješća upravi:

- Broj incidenata ovaj kvartal: 15 (phishing pokušaja)
- Uspješnost MFA implementacije: 87% zaposlenika
- Budžet potreban za nove sigurnosne alate: 50,000 EUR
- Glavni rizik: zastarjeli server u financijskom odjelu
- Akcija potrebna: odobrenje za zamjenu servera

Upravljanje i odgovornost

2. Aktivno sudjelovanje uprave u nadzoru

C) Rizik i odlučivanje:

- Razumijevanje kibernetičkih rizika - kao što razumiju financijske ili operativne rizike
- Prihvaćanje rezidualne rizika - odluka koliki rizik organizacija može podnijeti
- Krizno odlučivanje - što raditi u slučaju velikog incidenta

D) Osobna odgovornost po NIS2:

- Uprava može biti osobno kažnjena za nepoštivanje
- Mogućnost privremene zabrane obavljanja upravljačkih funkcija
- Kazne: do 10 milijuna EUR ili 2% globalnog godišnjeg prometa (što je veće od toga)

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

Što to znači:

- Ljudi su najslabija karika - 90% sigurnosnih incidenata uključuje ljudsku pogrešku. Obuka je ključna!

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

A) Osnovna obuka za sve zaposlenike (godišnje):

- Prepoznavanje phishinga - lažni emailovi, sumnjivi linkovi
- Sigurno korištenje lozinki - jaki passwordi, ne dijeljenje, password manageri
- Social engineering - kako nas manipulatori mogu prevariti
- Sigurno korištenje uređaja - zaključavanje ekrana, šifriranje laptopa
- Mobilna sigurnost - aplikacije, javni WiFi, izgubljeni telefoni
- Fizička sigurnost - ne ostavljanje dokumenata, pristupne kartice
- Clean desk policy - čišćenje stola na kraju dana
- Što raditi ako sumnjate na incident - koga kontaktirati

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

B) Napredna obuka za IT osoblje:

- Sigurno programiranje (secure coding)
- Konfiguracija sigurnosnih alata
- Incident response procedure
- Forenzička analiza

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

C) Specijalizirana obuka za upravu:

- Kibernetički rizici i poslovni utjecaj
- Regulatorne obveze (NIS2, GDPR)
- Odgovornost uprave
- Krizno upravljanje

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

D) Phishing simulacije:

- Redovito slanje lažnih phishing emailova zaposlenicima (mjesečno/kvartalno)
- Praćenje tko klikne na link
- Dodatna obuka za one koji "padnu“
- Cilj: Ne kažnjavanje, već učenje!

Upravljanje i odgovornost

3. Obuka zaposlenika i podizanje svijesti

E) Kontinuirana svijest:

- Newsletteri - mjesečni savjeti o sigurnosti
- Posteri - podsjetnici u uredima
- Screensaveri - poruke o sigurnosti
- Lunch & Learn - neformalne prezentacije uz ručak
- Gamifikacija - nagrade za sigurnosno ponašanje

Upravljanje i odgovornost

4. Uspostava politika i procedura

Što to znači:

- Pisana pravila kako se stvari rade u kontekstu sigurnosti. Dokumenti koji definiraju "pravila igre".

Ključne politike:

- Informacijska sigurnosna politika (Information Security Policy
- Politika prihvatljive uporabe (Acceptable Use Policy - AUP)
- Politika upravljanja pristupom (Access Control Policy)
- Politika upravljanja lozinkama (Password Policy)
- Politika backup-a i obnove
- Politika udaljenoga rada (Remote Work Policy)
- Politika upravljanja incidentima
- Politika dobavljača (Vendor Management Policy)
- Politika uništavanja podataka (Data Disposal Policy)

Upravljanje i odgovornost

4. Uspostava politika i procedura

Politike (strategija, što)
↓
Standardi (specifikacije, kako točno)
↓
Procedure (koraci, detaljno kako)
↓
Radne upute (vodič za krajnjeg korisnika)

Upravljanje i odgovornost

5. Dokumentiranje svih procesa i mjera

Što to znači:

- Sve što radite oko sigurnosti mora biti dokumentirano. "Što nije zapisano, nije se ni dogodilo.“

Što se dokumentira:

- Sigurnosni sustav (arhitektura sustava)
- Procesi
- Rizici i kontrole
- Incidenti
- Obuke
- Pregledi i testovi
- Promjene
- Usklađenost

Upravljanje i odgovornost

6. Redovite revizije i testiranje sustava

Što to znači:

- Nisu dovoljne samo postavljene mjere - morate provjeravati da rade i da su učinkovite!

Vrste revizija:

- Interne revizije (Internal Audits)
- Eksterne revizije (External Audits)
- Vulnerability Assessment
- Penetration Testing (Pen Test)
- Disaster Recovery testiranje
- Business Continuity Plan testiranje
- Configuration reviews
- Log reviews
- Management reviews

Dojava i izvještavanje

NIS2 direktiva zahtijeva da organizacije brzo obavijeste nadležna tijela o značajnim sigurnosnim incidentima.

Razlozi:

1. Nacionalna sigurnost - ozbiljni incidenti mogu utjecati na cijelu državu
2. Zaštita drugih - informacije o napadu mogu pomoći drugim organizacijama da se zaštite
3. Koordinirani odgovor - nadležna tijela mogu pružiti pomoć i resurse
4. Trend analysis - prikupljanje podataka o prijetnjama na nacionalnoj razini
5. Regulatory compliance - zakonska obveza

Važno: Nepoštivanje obveze dojave može dovesti do značajnih kazni - do 10 milijuna EUR ili 2% globalnog godišnjeg prometa!

Dojava i izvještavanje

1) Uspostava procedura za dojavu incidenata

- Interna procedura za dojavu: Detekcija, Inicijalna prijava, Trijaža i klasifikacija, Eskalacija, Odluka o eksternoj dojavi
- Definirati što se I kako prijavljuje
- Definirani komunikacijski kanali

Dojava i izvještavanje

2. Rana obavijest - 24 sata od saznanja

Što to znači:

- Najbrža, najkraća obavijest da se incident dogodio. Svrha je da nadležno tijelo zna što se događa **odmah**.

Primjer:
10:00 - Zaposlenik primijeti da su datoteke šifrirane
10:15 - Prijavljuje IT-u
10:30 - IT potvrđuje ransomware napad
10:30 = START TOČKA za 24-satni rok
Do 10:30 sljedećeg dana - mora biti poslana rana obavijest

Dojava i izvještavanje

2. Rana obavijest - 24 sata od saznanja

Što se uključuje u ranu obavijest:

- Identifikacija organizacije
- Osnove incidenta
- Početna procjena utjecaja
- Status odgovora
- Indikatori kompromitacije (ako su poznati)

Dojava i izvještavanje

3. Obavijest o incidentu - 72 sata

Detaljnija obavijest s više informacija nakon što ste imali vremena analizirati situaciju

Što sve uključuje:

- Ažurirane informacije o incidentu
- Detaljan utjecaj
- Prekogranični učinci
- Primijenjene mjere
- Indikatori kompromitacije (IOC)
- Potencijalni kaskadni učinci
- Prijetnje i ranjivosti

Dojava i izvještavanje

4. Konačno izvješće - najkasnije mjesec dana

Završno, sveobuhvatno izvješće s kompletnom analizom incidenta i naučenim lekcijama.

Što sve uključuje:

- Izvršni sažetak
- Detaljan timeline
- Root cause analiza
- Tehnička analiza
- Konačni utjecaj
- Poduzete korektivne mjere
- Preventivne mjere za budućnost
- Preporuke
- Troškovi
- Status usklađenosti

Dojava i izvještavanje

5. Određivanje nadležnog tijela za dojavu

Morate znati kome prijavljujete incident - koje tijelo je nadležno u Hrvatskoj.

NCERT (National CERT) - Nacionalni CERT
https://www.cert.hr

GDPR - Agencija za zaštitu osobnih podataka (AZOP)
https://azop.hr

Dojava i izvještavanje

6. Priprema predložaka i komunikacijskih kanala

Ne čekajte incident da biste razmišljali kako prijaviti - **pripremite sve unaprijed!**

Zašto se uskladiti ako niste obveznik?

Ključne koristi dobrovoljnog usklađenja

Poboljšana sigurnost

- Sveobuhvatan pristup zaštiti organizacije
- Smanjenje vjerojatnosti sigurnosnih incidenata
- Minimiziranje potencijalnih financijskih gubitaka
- Zaštita reputacije i povjerenja klijenata
- Strukturirani pristup upravljanju kibernetičkim prijetnjama
- Bolja pripremljenost za odgovor na napade

Konkurentska prednost

- Diferencijacija na tržištu kroz visoku razinu sigurnosti
- Povećano povjerenje klijenata i partnera
- Olakšana suradnja s velikim organizacijama
- Ispunjavanje sigurnosnih zahtjeva u nabavi
- Mogućnost certificiranja i eksternih verifikacija
- Pristup novim tržištima s visokim sigurnosnim standardima

Priprema za budućnost

- Očekuje se daljnje širenje opsega direktive
- Proaktivno građenje kapaciteta
- Izbjegavanje hitnih i skupih prilagodbi kasnije
- Usklađenost s trendovima u regulaciji
- Smanjenje rizika od budućih kazni
- Lakša adaptacija na nove zahtjeve

Sigurnost lanca opskrbe

- Obveznici moraju osigurati sigurnost svojih dobavljača
- Neusklađeni partneri postaju rizik
- Mogućnost gubitka poslovnih prilika
- Usklađenje otvara vrata suradnji s velikim organizacijama
- Due diligence procesi sve češće uključuju NIS2
- Postajete preferiran poslovni partner

Organizacijska kultura

- Razvoj kulture sigurnosti u organizaciji
- Podizanje svijesti zaposlenika
- Smanjenje rizika od ljudskih pogrešaka
- Jasne procedure i odgovornosti
- Kontinuirano poboljšanje procesa
- Zaposlenici postaju ljudski firewall

Usklađenost s drugim standardima

- NIS2 kompatibilan s ISO 27001, NIST frameworks
- Temelj za druge certifikacije i standard
- Smanjenje troškova višestrukih usklađivanja
- Iskoristivost već provedenih mjera
- Holističko upravljanje sigurnošću
- Međunarodno priznati okvir

Kako započeti s usklađenjem?

- Provedite inicijalnu procjenu trenutnog stanja
- Definirajte sigurnosne ciljeve organizacije
- Započnite s osnovnim mjerama (backup, prava pristup, enkripcija)
- Educirajte zaposlenike i upravu
- Angažirajte eksterne stručnjake po potrebi
- Planirajte postupnu implementaciju

Zaključak

- NIS2 podiže letvicu kibernetičke sigurnosti u EU
- Usklađenje obveznika je zakonska obveza
- Za neobveznike - strateška investicija u budućnost
- Koristi nadilaze troškove implementacije
- Kibernetička sigurnost više nije opcija, već nužnost
- Proaktivan pristup štiti organizaciju i njenu budućnost

Pitanja?

<https://idera.konto.hr/>

<mailto:mladen@konto.hr>

Hvala!