Plán zavedení opatření pro dosažení souladu s normou NIS2

1. Analýza současného stavu

- Identifikace kritických aktiv a systémů.
- Posouzení aktuálních bezpečnostních opatření a zranitelností.
- Vyhodnocení rizik spojených s kybernetickou bezpečností.

2. Stanovení odpovědností a řízení souladu

- Jmenování odpovědné osoby nebo týmu pro kybernetickou bezpečnost.
- Vytvoření strategie řízení rizik a bezpečnostních politik.
- Nastavení interních kontrol a auditních procesů.

3. Technická a organizační opatření

- Zajištění robustního řízení přístupů (vícefaktorová autentizace, princip nejnižších oprávnění).
- Implementace bezpečnostních opatření v oblasti síťové bezpečnosti, ochrany koncových bodů a monitorování provozu.
- Pravidelné zálohování dat a zavedení plánů obnovy po incidentech.
- Šifrování citlivých dat a komunikace.

4. Školení a zvyšování povědomí

- Pravidelná školení zaměstnanců o kybernetických hrozbách a bezpečnostních postupech.
- Simulace phishingových útoků a testování bezpečnostního povědomí.
- Vytvoření bezpečnostních směrnic pro zaměstnance.

5. Incident Management a reakce na bezpečnostní události

- Zavedení plánu reakce na incidenty včetně postupů pro hlášení incidentů.
- Monitorování a detekce kybernetických útoků s využitím SIEM systémů.
- Spolupráce s orgány dohledu a oznamování incidentů dle požadavků NIS2.

6. Právní a regulační compliance

- Pravidelné aktualizace bezpečnostních politik v souladu s legislativou EU.
- Zajištění souladu s GDPR a dalšími relevantními předpisy.
- Dokumentace a archivace všech procesů souvisejících s kybernetickou bezpečností.

7. Nepřetržité zlepšování a auditní činnost

- Pravidelné provádění bezpečnostních auditů a testování odolnosti systémů.
- Implementace zpětné vazby a adaptace na nové hrozby.
- Zavedení cyklu neustálého zlepšování bezpečnostních opatření.

8. Harmonogram zavádění opatření

Fáze	Opatření	Časový rámec
1.	Analýza současného stavu	1-2 měsíce
2.	Jmenování odpovědných osob	1 měsíc
3.	Implementace technických opatření	3-6 měsíců
4.	Školení zaměstnanců	Průběžně
5.	Zavedení procesu řízení incidentů	2-3 měsíce
6.	Audit a nepřetržité zlepšování	Průběžně

Tento plán by měl být pravidelně aktualizován s ohledem na nové hrozby a změny v regulaci NIS2.