REGUVARA · BEZPLATNÝ PRAKTICKÝ PRŮVODCE

NIS2: připravte oznamovací postupy a důkazy

Praktický první krok pro vedení, IT/bezpečnost, právní oddělení a compliance. Základní orientace v působnosti, hlavních oznamovacích lhůtách a pěti úvodních úkolech.

Cíl: rychle zviditelnit správné otázky. Tento průvodce závazně neurčuje, zda konkrétní právnická osoba spadá do působnosti NIS2.

1. Nejprve předběžně posuďte působnost

- Přiřaďte činnost, službu a právnickou osobu k odvětvím v přílohách I a II směrnice NIS2. Samotný název odvětví o působnosti nerozhoduje.
- Prověřte velikost, vazby v rámci skupiny, typ služby, případné určení za kritický subjekt, výjimky a zvláštní pravidla příslušného členského státu. Některé subjekty nebo služby mohou spadat do působnosti bez ohledu na obvyklý velikostní práh.
- U každé potenciálně dotčené právnické osoby zaznamenejte státy, pracoviště, služby, příslušný orgán, registrační a kontaktní povinnosti a odůvodnění.

2. Fáze oznamování významného incidentu na úrovni EU

Fáze	Základ EU podle článku 23	Otázka k přípravě
Včasné varování	Bez zbytečného odkladu, nejpozději do 24 hodin od okamžiku, kdy se subjekt o významném incidentu dozví.	Kdo spustí čas, rozhodne a určí příslušný orgán?
Oznámení incidentu	Bez zbytečného odkladu, nejpozději do 72 hodin od okamžiku, kdy se o něm subjekt dozví; první posouzení závažnosti a dopadu a dostupné ukazatele.	Jak souběžně shromažďovat fakta, časové údaje a neznámé informace?
Průběžná zpráva	Pokud o ni požádá CSIRT nebo příslušný orgán.	Kdo zaznamenává změny a odpovídá na doplňující otázky?
Závěrečná zpráva	Zpravidla do jednoho měsíce od oznámení incidentu. Pokud incident stále probíhá, v tomto termínu se podá zpráva o pokroku a závěrečná zpráva do jednoho měsíce po vyřízení.	Kdo potvrdí vnitrostátní lhůtu a požadovaný obsah?

Lhůty se týkají významných incidentů a okamžiku, kdy se o nich subjekt dozví. Poskytovatelé služeb vytvářejících důvěru podléhají zvláštní 24hodinové lhůtě pro oznámení incidentu. Ověřte vnitrostátní provedení, odvětvová pravidla a další použitelné předpisy EU.

PRACOVNÍ LIST

Od právního textu k prvnímu pracovnímu postupu

NIS2 vyžaduje technická, provozní a organizační opatření přiměřená riziku. Tento přehled pomáhá určit první odpovědné osoby.

3. Oblasti podle článku 21

Opatření chrání sítě a informační systémy používané pro služby včetně jejich fyzického prostředí. Rozsah a nastavení vycházejí z rizika a přiměřenosti.

Oblast	Příklad pracovní otázky
Analýza rizik a bezpečnost systémů	Které služby, systémy, hrozby a závislosti se posuzují? Kdo hodnocení aktualizuje?
Řešení incidentů	Jak jsou organizovány detekce, klasifikace, omezení, eskalace, zajištění důkazů a následné vyhodnocení?
Kontinuita a krizové řízení	Jsou zálohy, obnova, krizové role a cíle obnovení zdokumentovány a vyzkoušeny?
Dodavatelský řetězec	Jsou zaznamenáni přímí dodavatelé, kritické závislosti a bezpečnostní informace?
Bezpečné pořizování a vývoj	Jak se systémy bezpečně vybírají a udržují a jak se řeší nebo zveřejňují zranitelnosti?
Kontrola účinnosti	Jak organizace zjišťuje, zda bezpečnostní opatření fungují?
Kybernetická hygiena a školení	Které základní postupy a školení jsou naplánované a doložitelné?
Kryptografie	Jaká pravidla platí pro kryptografii a případně šifrování?
Lidé, přístupy a aktiva	Jak se kontrolují oprávnění, personální změny, aktiva a přístupy?
Ověřování totožnosti a komunikace	Kde je vhodné MFA nebo průběžné ověřování, zabezpečená komunikace a nouzové kanály?

4. Pět užitečných prvních kroků

- Určete odpovědnou osobu, která bude koordinovat otázky působnosti a otevřené body.
- Sepište služby, právnické osoby, systémy a kritické přímé dodavatele.
- Určete vedení, vedoucího incidentu, IT/bezpečnost, právní/compliance a komunikaci včetně zástupců.
- Ověřte vnitrostátní příslušný orgán, CSIRT, registraci, oznamovací kanál a případné odvětvové povinnosti.
- Proveďte krátké cvičení: odhalte incident, zaznamenejte okamžik zjištění, zahajte eskalaci a shromážděte fakta.

NIS2 se automaticky nevztahuje na každou společnost. Působnost závisí mimo jiné na činnosti, velikosti, právnické osobě, členském státu, zvláštních případech a odvětvových pravidlech.

ZDROJE A PRÁVNÍ STAV

Primární zdroj: směrnice (EU) 2022/2555, zejména články 2-4, 20, 21 a 23 a přílohy I-II. Návrh COM(2026) 13 final není platným právem. Dne 8. října 2026 čekal postup Evropského parlamentu 2026/0012(COD) na rozhodnutí výboru; dne 24. září 2026 byl zveřejněn návrh zprávy výboru. Vnitrostátní provedení a odvětvová pravidla nebyla prověřena pro každou zemi zvlášť.
NIS2 Directive (EUR-Lex) · European Commission FAQ · National transposition · EP procedure 2026/0012(COD) · COM(2026) 13 proposal