

Dopad směrnice NIS2 na průmyslové systémy

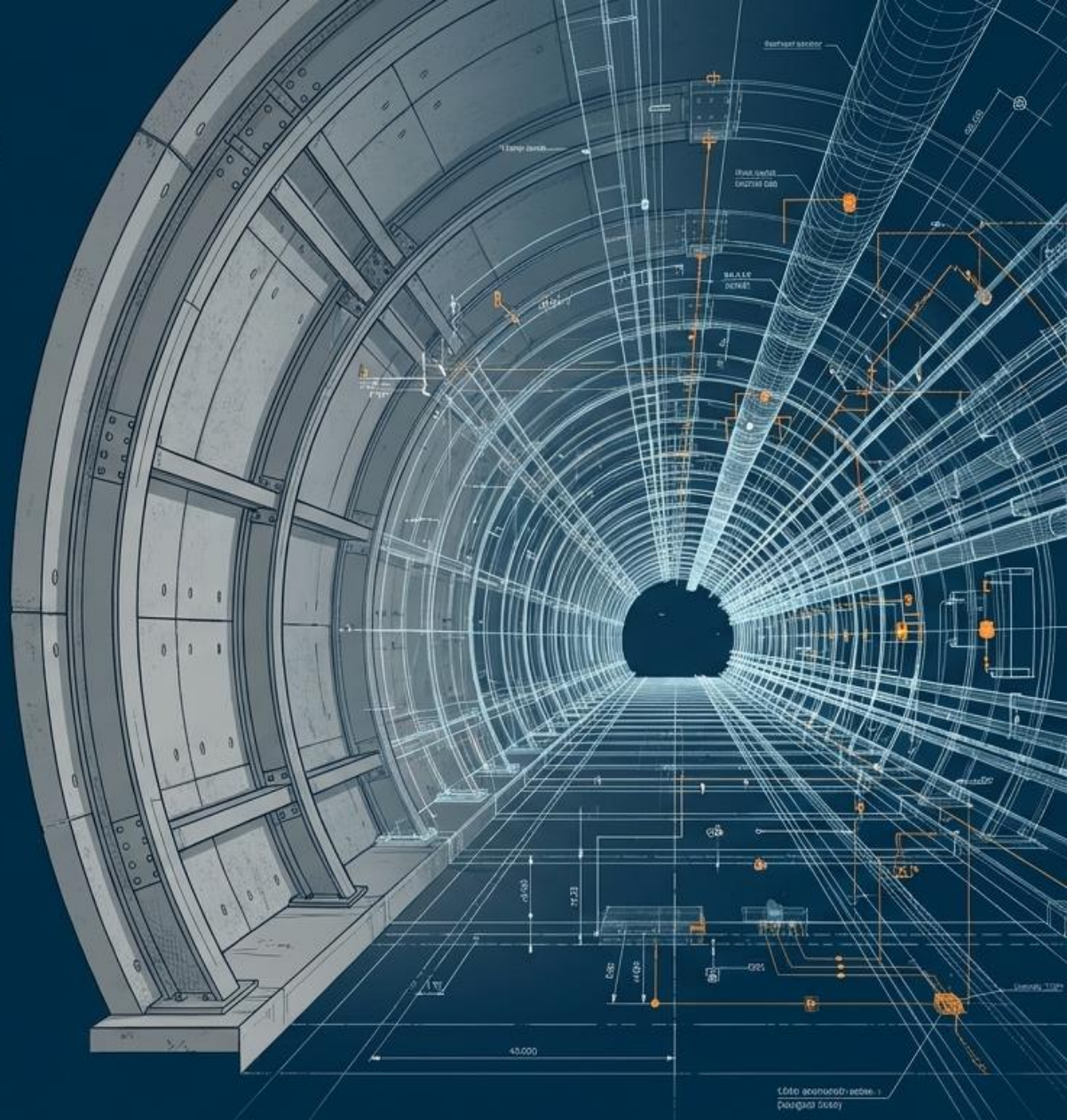
Asociace pro rozvoj infrastruktury

Corpus Solutions, a. s.

23. 4. 2026

Dopad směrnice NIS2 na liniové stavby a průmyslové systémy

Kybernetická bezpečnost už není jen IT doplňkem. Je to základní kámen kritické infrastruktury a osobní odpovědnost vedení.



Cíl prezentace:



Jaké povinnosti vynucuje legislativa vycházející z NIS2, proč to není jen „legislativa“



Představit důvody, proč integrovat **kybernetickou bezpečnost** již v raných fázích návrhu liniové stavby



Naznačit **promítnutí kybernetické bezpečnosti** do jednotlivých fází procesu výstavby



Regulatorní rámce



REGULACE A POVINNOSTI



NIS2 zásadně zpřísňuje povinnosti pro provozovatele liniových staveb včetně řízení rizik, řízení dodavatelů a povinných bezpečnostních opatření.



Regulovaná služba (408/2025):
15. Silniční doprava - řízení provozu na pozemních komunikacích a Provoz inteligentního dopravního systému.



Další regulatorní rámce pro IT i OT systémy

- Zákon č. 264/2025 Sb. o kybernetické bezpečnosti
- Vyhláška č. 408/2025 Sb. o regulovaných službách
- Vyhláška č. 409/2025 Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- ISO 27001 – řízení informační bezpečnosti
- IEC 62443 – bezpečnost průmyslových systémů
- Požadavky investorů

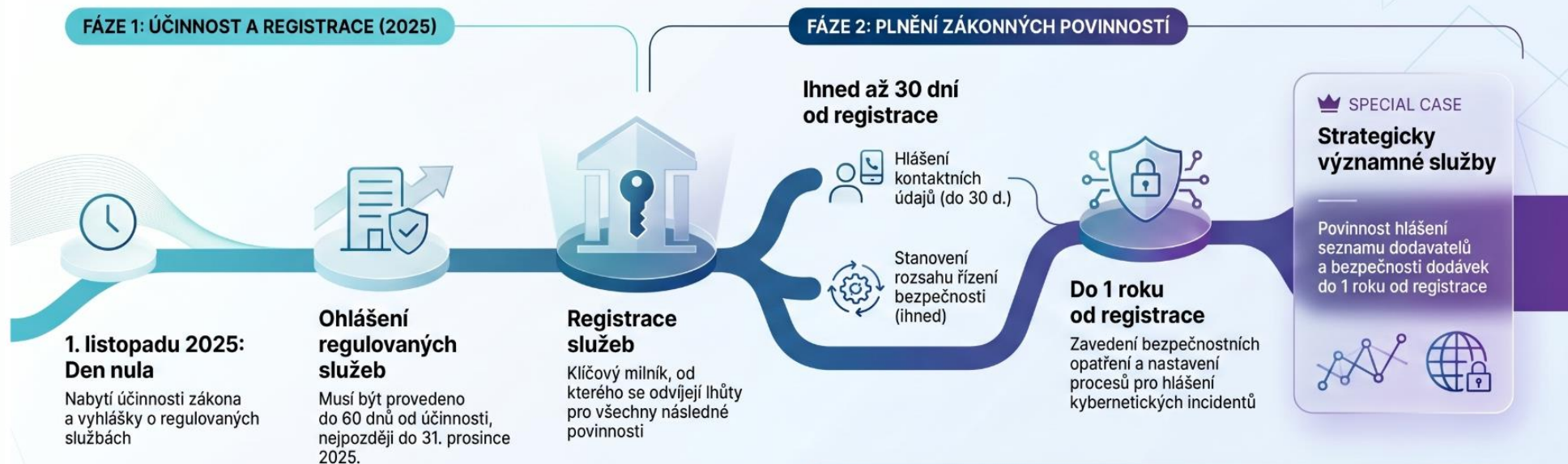


Splnění regulací vyžaduje zapojení bezpečnostních expertů již ve fázi projektové dokumentace.



Registrace u NÚKIB = začátek povinností

Časová osa a povinnosti nového zákona o kybernetické bezpečnosti



Přehled lhůt vázaných na okamžik registrace

Povinnost	Lhůta pro splnění
Hlášení kontaktních údajů	do 30 dní od registrace
Stanovení rozsahu řízení bezpečnosti	průběžně ihned od registrace
Zavedení bezpečnostních opatření	do 1 roku od registrace

Od stanovení rozsahu k opatřením

NIS2: Strategický proces implementace a klíčové povinnosti

Příprava a vymezení rozsahu (Kroky 1 a 2)

1. Posoudit dopad a
2. Vymezit rozsah aktiv

Identifikace primárních a podpůrných aktiv, na kterých závisí provoz regulované služby.



Rozsah regulace a režimy povinností

Určení, zda organizace spadá pod nižší nebo vyšší režim povinností v rámci IT/OT.



Kdo podléhá regulaci?

Provozovatelé liniových staveb a celý jejich dodavatelský řetězec včetně subdodavatelů technologií.

Realizace a technická opatření (Kroky 3 až 5)

3. Provést gap analýzu a
4. Nastavit dodavatele a incidenty

Zjištění nedostatků a precizní definování bezpečnostních požadavků do všech výběrových řízení.



Řízení rizik



Přístupy

5. Zavést technická a organizační opatření



Kontinuální audit a zlepšování

Provádění pravidelných bezpečnostních cvičení, auditů a důsledná kontrola dodavatelů.

Bezpečnostní opatření ve vyšším režimu

Kompletní přehled bezpečnostních opatření: Vyhláška č. 409/2025 Sb.

Jasný a strukturovaný seznam všech zákonných požadavků na organizační a technická opatření v oblasti kybernetické bezpečnosti.

ORGANIZAČNÍ OPATŘENÍ (§ 3–16)



§ 3 – Systém řízení bezpečnosti informací

Základní rámec pro systematické řízení bezpečnosti v rámci celé organizace.



§ 4 – Požadavky na vrcholné vedení

Definice odpovědnosti a nezbytné součinnosti nejvyššího managementu.



§ 5 – Stanovení bezpečnostních rolí

Určení konkrétních osob odpovědných za výkon bezpečnostních funkcí.



§ 6 – Řízení bezpečnostní politiky a dokumentace

Pravidla pro tvorbu, schvalování a udržování bezpečnostních předpisů.



§ 7 – Řízení aktiv

Evidence a klasifikace všech informačních a komunikačních aktiv.



§ 8 – Řízení rizik

Metodika identifikace, hodnocení a zvládnutí rizik ohrožujících bezpečnost.



§ 9 – Řízení dodavatelů

Nastavení bezpečnostních pravidel ve vztazích s externími partnery.



§ 10 – Bezpečnost lidských zdrojů

Zajištění důvěryhodnosti a vzdělanosti zaměstnanců v oblasti bezpečnosti.



§ 11 – Řízení změn

Procesy pro bezpečné provádění modifikací v systémech a organizaci.



§ 12 – Akvizice, vývoj a údržba

Zohlednění bezpečnosti při pořizování a vývoji nových systémů.



§ 14 – Zvládnutí kybernetických událostí a incidentů

Postupy pro detekci, hlášení a řešení bezpečnostních narušení.



§ 15 – Řízení kontinuity činnosti

Plány pro obnovu provozu po havárii nebo kybernetickém útoku.



§ 16 – Provádění auditů kybernetické bezpečnosti

Pravidelné nezávislé ověřování účinnosti nastavených opatření.



§ 17 – Fyzická bezpečnost

Ochrana prostor, kde se nacházejí kritická technická aktiva.



§ 18 – Bezpečnost komunikačních sítí

Zabezpečení přenosu dat a síťové infrastruktury pro zneužití.



§ 19 – Správa a ověřování identit

Jednotná identifikace a autentizace uživatelů a zařízení.



§ 20 – Řízení přístupových práv a oprávnění

Technické vynuovení pravidel pro přístup ke jednotlivým zdrojům.



§ 21 – Detekce kybernetických bezpečnostních událostí

Nasazení nástrojů pro včasné rozpoznání podezřelých aktivit.



§ 22 – Zaznamenávání událostí

Logování činností systémů u uživatelůch pro účely pozdější analýzy.



§ 23 – Vyhodnocování kybernetických událostí

Procesy pro analýzu sesbíraných dat a identifikaci incidentů.



§ 24 – Aplikační bezpečnost

Zajištění odolnosti softwaru proti útokům.



§ 25 – Kryptografické algoritmy

Použití šifrování k ochraně důvěrnosti a integrity dat.



§ 26 – Zajišťování dostupnosti regulované služby

Opatření proti výpadkům a pro zajištění kapacity systémů.



§ 27 – Zabezpečení specifických technických aktiv

Ochrana průmyslových (OT), řídicích a jiných specializovaných systémů.

Proč je kybernetická bezpečnost zásadní

- **Liniové stavby a související technologie** představují kritickou infrastrukturu, kde útok nebo selhání může mít okamžitý dopad na lidské životy i celostátní dopravu.
- Moderní tunely využívají stovky síťově propojených zařízení (**PLC, SCADA, CCTV, SOS hlášky**) – každé z nich je potenciálním vstupním bodem útoku.
- Globálně narůstá počet útoků na **OT prostředí**. Útočníci cílí na nejzranitelnější komponenty, často přes dodavatele nebo chyby v software.

OT priorita: bezpečný a dostupný provoz



KYBERNETICKÉ HROZBY TUNELOVÝCH STAVEB

Hrozby



Útok na **ventilaci, kamerové systémy** (obtížná reakce na incidenty)



DoS útok na řídicí systémy může zamezit ovládání tunelu a způsobit kolaps provozu.



Manipulace s PLC může vést k nesprávnému řízení dopravního značení či ventilace.

Příklady útoků a incidentů



Německo (2017, 2022)
– útok na Siemens telekomunikační systém (GSM-R) způsobil:
✓ ztrátu komunikace mezi vlakem a řídicím centrem
✓ omezení provozu v tunelových úsecích



Švýcarsko (2020)
– výpadek železničního SCADA v tunelových sekcích:
✓ odpojení senzorů
✓ omezení řízení trakce
✓ snížení rychlostí v tunelech



Austrálie – útok na řízení tunelů v Sydney (2020)
zasazené: CCTV, ventilace, nouzové systémy
✓ tunely přešly do omezeného režimu



Norsko – útok na dopravní agenturu (2021)
✓ výpadky kamer, senzorů a řízení v několika tunelech

Proč je NIS2 důležitá právě pro infrastrukturu



Infrastruktura je dnes **digitální** a **kyberneticky závislá**.



Kybernetický incident může **zastavit provoz** a **ohrožit lidi**.



Nejde jen o data, ale o **bezpečný** a **dostupný chod služby**.



Rizika vznikají i přes **dodavatele** a **vzdálené přístupy**.



Bezpečnost je nutné řešit **už od návrhu stavby**.



Chyby v projektu se v provozu **napravují draze**.



NIS2 přináší povinnost řídit rizika a **nést odpovědnost**.



SYSTEMS

SCADA	VENTILACE	OSVĚTLENÍ
KAMERY	HLÁŠENÍ	ŘÍZENÍ DOPRAVY

NÁVRH



BEZPEČNOST
OD ZAČÁTKU

VÝSTAVBA



BEZPEČNÉ
TECHNOLOGIE

PROVOZ



MONITORING
A ŘÍZENÍ RIZIK

REAKCE



PŘÍPRAVENOST
NA INCIDENTY

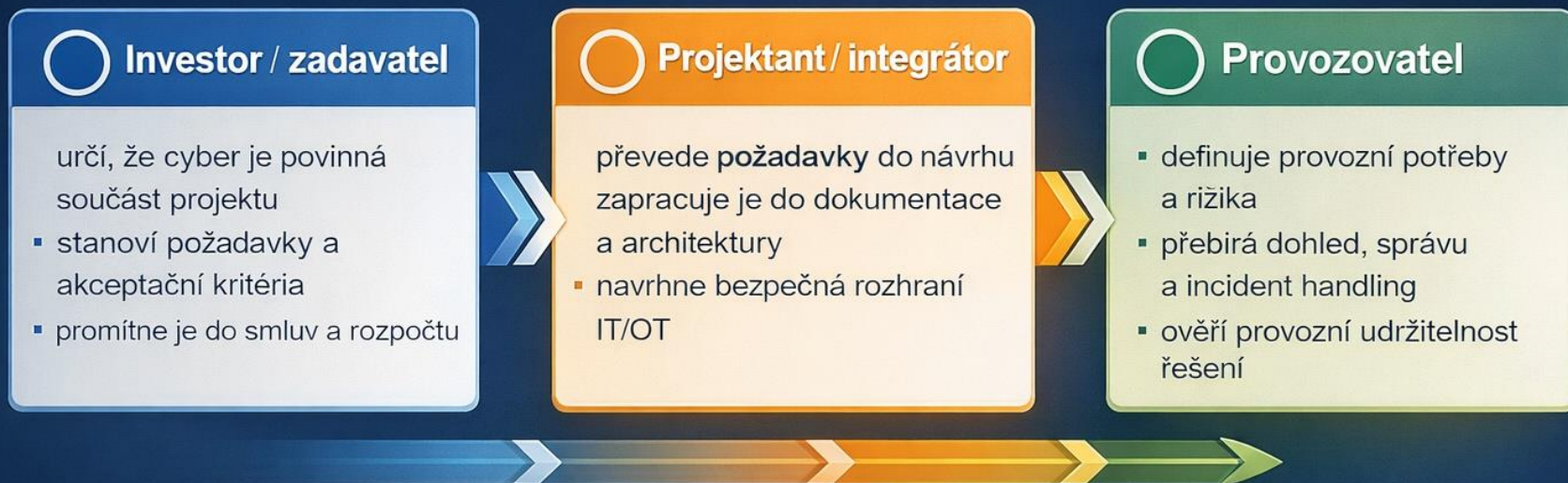
BEA ZODPOVĚDNOST



SHODA
S NIS2

Investor – projektant – provozovatel

Právní odpovědnost bývá na regulovaném subjektu. Praktická odpovědnost se musí rozdělit.



Bez jasného bezpečnostního zadání od investora projektant nic nevynutí – a provozovatel později přebírá riziko čížího návrhu. **Chyba v praxi: cyber** se často objeví až u technologie. Správně má být přítomná už **ve studii, zadání a smlouvách.**

Proces výstavby a zapojení KyBe

Nejde o IT doplněk na konci projektu. NIS2 se má propsat do strategie, rozhodování, nákupu, projektování i přejímky

Příprava a požadavky

Fáze 1-3

Projekt a smluvní zajištění

Fáze 4-5

Realizace a ověření

Fáze 6-7

Předání a ostrý provoz

Fáze 8-9

	1. Záměr / strategie	2. Koncepce / studie	3. Zadání / požadavky	4. Projekt / povolení	5. Smlouvy / výběr dodavatelů	6. Realizace / instalace	7. Testy / zkušební provoz	8. Předání / uvedení do provozu	9. Provoz / údržba / změny
	Definice rámce a rozsahu KyBe	Mapování aktiv a rizik	Technické bezpečnostní parametry	Návrh architektury a řešení	Přenos povinností na dodavatele	Implementace a hardening	Verifikace bezpečnosti	Dokumentace a převzetí odpovědnosti	Kontinuální monitoring a údržba
	Hlavním subjektem je Investor; určují se cíle z pohledu KyBe (C/I/A), rozsah povinností a režim služby/odpovědnosti.	Spolupráce Investora a Provozovatele na identifikaci primárních a podpůrných aktiv, definici OT/IT zán a vazeb na dispečink.	Definice požadavků pro technologie (IT/OT, SCADA, PLC, CCTV) včetně segmentace sítě, MFA, logování a vzdáleného přístupu.	Projektant a architekt KyBe navrhnou konkrétní řešení (IAM, zálohování, síťová architektura) v souladu s požadavky.	Investor do smluv promítá bezpečnostní požadavky, testy a podmínky předání konfigurací.	Dodavatel provádí konfiguraci, nastavení FW pravidel, certifikátů a změnu výchozích účtů; probíhá napojení na SOC.	Investor a Provozovatel provádějí penetrační testy, sudity a ověřují funkčnost detekce incidentů a eskalací.	Provozovatel přebírá "as-built" dokumentaci, administrátorské účty a provozní příručky (playbooky).	Společná role Provozovatele a SOC; zahrnuje patchování, zvládnání incidentů, reporting a řízení zranitelnosti.
SOC / Dohled	Požadavek na dohled	Scope monitoringu	Požadavky na logy a SIEM	Návrh use casů a integrace	Povinnosti dodavatelů	Napojení technologií do SOC	Ověření detekce a eskalací	Předání dashboardů	24/7 monitoring, triage
Primární subjekt	Investor	Investor + Provozovatel	Investor + kyber role	Projektant + architekt KyBe	Investor	Dodavatel	Investor + Provozovatel	Provozovatel	Provozovatel + SOC
Klíčové role	Vlastník služby, CISO, architekt	Vlastník služby, CISO, architekt, PM	Vlastník služby, CISO, architekt, PM	Projektant, CISO, architekt, PM	PM investora, Nákup, Právo	Integrátor/zhotovitel, PM investora	Integrátor, PM, CISO, Vlastník služby	Vlastník služby, Integrátor, PM, CISO	Vlastník služby, CISO, Architekt, SOC

Odpovědnost subjektů

Kdo nese odpovědnost?

Právní odpovědnost je u poskytovatele regulované služby — **ne u projektanta.**



**Investor /
provozovatel
regulované služby**

**Nese
odpovědnost**

Určí, zda projekt patří do rozsahu regulované služby a že KyBe bude součástí zadání, projekt a dodavatelé musí požadavky převést do návrhu, smluv a přejímky



Vrcholné vedení

**Schvaluje
a dohlíží**

Vlastní governance, rozhoduje o prioritách, rozpočtu a bezpečostních milnících



**CISO / security
architekt
+ vlastník služby**

**Definují
požadavky**

Překládají NIS2 do rozsahu, rizik, technických standardů a akceptačních kritérií.

Projektant, integrátor a zhotovitel plní požadavky — ale odpovědnost nezmizí u investora.

Praktický dopad pro firmy: management musí kyberbezpečnost udělat součástí řízení organizace — včetně investic, řízení a provozu.

Osobní a trestní odpovědnost managementu

Vedení už nemůže kyberbezpečnost pouze „delegovat na IT“

PILÍŘE ROLE MANAGEMENTU A PÉČE



Péče řádného hospodáře

Povinnost jednat preventivně k předcházení incidentům a uchovávat důkazy o všech rozhodnutích.

Strategický dohled a zdroje

Management musí schvalovat bezpečnostní opatření, přidělovat rozpočty a zajišťovat školení kompetencí.



Přímá osobní odpovědnost

Vedení je přímo odpovědné za veškerá selhání v oblasti zabezpečení organizace.



HROZÍCÍ SANKCE A DOPADY



Pokuta až 250 000 000 Kč

Sankce může dosáhnout výše 250 milionů korun nebo 2 % z celosvětového obratu.

Zákaz výkonu funkce

Osobní dopad zahrnuje zákaz činnosti člena statutárního orgánu a zápis do veřejných registrů.



Provozní a reputační škody

Výpadky kritické infrastruktury vedou k pokutám a definitivní ztrátě důvěry klientů.



Závěrem

- NIS2 mění řízení infrastruktury, ne jen compliance.
- Kyberbezpečnost musí být součástí projektu od začátku.
- Nejdřív rozsah a aktiva, potom rizika a opatření.
- Odpovědnost nese regulovaný subjekt a vedení.
- Rozhodují návrh, smlouvy, testy a provoz, ne až finální audit.
- Vytvořte plán činností a projektů na podporu požadavků legislativy a nejlepší praxe

Děkujeme vám za pozornost

Jan.kriz@corpus.cz

corpus.cz