SPOLCHEMIE

KYBERNETICKÁ BEZPEČNOST – NIS2

4.11.2025 – ÚSTÍ NAD LABEM - PAVEL ELKNER

NIS2 – aktuální informace

SVAZ CHEMICKÉHO PRŮMYSLU ČR

- 1.11.2025 vstupuje v platnost Zákon 264/2025 Sb. – Zákon o kybernetické bezpečnosti
- 31.12.2025 nejpozdější termín registrace regulované služby (60 dní) přes portál NÚKIB
- Následně do 30 dnů od doručení rozhodnutí o registraci je povinnost nahlásit kontaktní údaje odpovědných osob

- Směrnice evropského parlamentu a rady (EU) 2022/2555
- Vyhlášky č. 408/2025 Sb. (409 a 410) – Vyhláška o regulovaných službách
- Vyhláška č. 334/2025 Sb. – NÚKIB požadavky na některé úkony

Interní, externí vs hybridní přístup k NIS2

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Předpoklady interního přístupu k NIS2:

- mám znalosti a kapacity v oblastech NIS2,
- chci mít plnou kontrolu nad implementací,
- NIS2 je součástí strategického plánu bezpečnostní politiky společnosti.

Předpoklady externího přístupu k NIS2:

- nemám znalosti a kapacity v oblastech NIS2,
- výhradně chci naplnit pouze požadavky zákonu o NIS2,
- využívám vysokou přidanou hodnotu služeb a zkušeností externích dodavatelů.

Předpoklady hybridního přístupu k NIS2:

- nemám dostatečné znalosti a kapacity v oblastech NIS2,
- NIS2 je součástí strategického plánu bezpečnostní politiky společnosti,
- částečně využívá zkušenosti externích firem.

! Interní přístup ve většině případů neumí řešit penetrační a monitorovací nástroje.
! Externí přístup má nižší počáteční náklad, ale z pohledu dlouhodobých potřeb mohou být náklady výrazně vyšší.

Interní, externí vs hybridní přístup k NIS2

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Kritérium financí	Interní přístup	Externí přístup	Hybridní přístup
Finance krátkodobé	Vysoké	Nízké	Vysoké
Finance dlouhodobé	Nízké	Vysoké	Střední

Kritérium financí:

- Interní přístup má vyšší CAPEX, ale dlouhodobě stabilní náklady,
- Externí přístup má nižší OPEX a větší flexibilitu ve vykazování nákladů.
- Hybridní přístup po finanční stránce nemá jasně definované výhody a nevýhody.

Pro malé firmy je doporučen Externí přístup
Pro střední firmy je doporučen Hybridní přístup
Pro velké firmy je doporučen Interní přístup

Interní, externí vs hybridní přístup k NIS2

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Kritérium odbornosti	Interní přístup	Externí přístup	Hybridní přístup
Odbornost prostředí	Vysoká	Nízká	Střední
Odbornost technická	Nízká	Vysoká	Střední

Kritérium odbornosti:

- Interní přístup má silnou znalost prostředí a procesů, ale omezenou specializaci v oblastech CS,
- Externí přístup má silnou odbornost a zkušenosti z trhu, ale omezené porozumění internímu prostředí.
- Hybridní přístup má silnou odbornost a silnou znalost interního prostředí.

Pro malé firmy je doporučen Externí přístup
Pro střední a velké firmy je doporučen Hybridní přístup

Interní, externí vs hybridní přístup k NIS2

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Kritérium efektivity	Interní přístup	Externí přístup	Hybridní přístup
Efektivita správy	Střední	Vysoká	Střední
Efektivita služeb	Nízká (pro malé a střední firmy)	Vysoká	Střední

Kritérium efektivity a výkonu:

- Interní přístup stabilní výkon, pomalý rozjezd, neefektivní zvládání incidentů
- Externí přístup rychlé nasazení, snadná škálovatelnost, efektivní a rychlé zvládání incidentů.
- Hybridní přístup stabilní výkon, pomalý rozjezd, efektivní a rychlé zvládání incidentů.

Pro malé firmy je doporučen Externí přístup
Pro střední firmy je doporučen Hybridní přístup
Pro velké firmy je doporučen Interní přístup + vybrané externí služby, audity, testy

Interní, externí vs hybridní přístup k NIS2

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Jaký je Váš přístup k implementaci NIS2?
Jaké zkušenosti máte dnes Vy s interním nebo externím přístupem?
Ovlivňuje Vás korporátní oddělení v rámci řešení bezpečnosti a jak?

Režim regulace a zákon o prevenci závažných havárií

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Zákon č. 264/2025 Sb. – Zákon o kybernetické bezpečnosti vs Zákon č. 224/2015 Sb. - Zákon o prevenci závažných havárií

Prevence závažných havárií způsobených vybranými nebezpečnými chemickými látkami nebo chemickými směsi.

Oba zákony staví na **principu prevence a minimalizace dopadů** a oba řeší **kritická aktiva, zdroje hrozeb, scénáře havárií a opatření pro zmírnění dopadů** – v rámci OT je zde velký průnik technologie opatření ve formách PLC, DCS, ESD a jiných bezpečnostních monitorovacích systémů a rizik vzniklých jejich užíváním.

Režim vyšších a nižších povinností, regulovaná služba a strategická významný služba. Jak s tím naložit? Jak určit svou regulovanou službu?

Nižší režim 50 – 250 zaměstnanců nebo obrat 10 – 50 mil. Euro => Střední podnik

Vyšší režim 250 a více zaměstnanců nebo obrat více jak 50 mil. Euro => Velký podnik

Regulovaná služba dle Vyhlášky č. 408/2025 Sb. (409 a 410) => rozlišuje pro regulované služby Střední podnik a Velký podnik a tím klasifikuje Nižší režim a Vyšší režim

Režim regulace a zákon o prevenci závažných havárií

Zákon č. 264/2025 Sb. – Zákon o kybernetické bezpečnosti vs Zákon č. 224/2015 Sb. - Zákon o prevenci závažných havárií

Poskytovatel regulované služby dle Příloha č. 1 k Zákonu č. 224/2015 Sb. => Vyšší režim

Pokud Váš podnik spadá do Zákona č. 224/2015 Sb., tak víte které regulované služby se Vás týkají.

Poskytovatel strategický významné služby dle SEPaR 2022/2555 => Vyšší režim

Strategicky významná služba je službou takového významu, že její výpadek by měl zásadní dopad na společnost, ekonomiku nebo bezpečnost státu.

Pro následné posouzení aktiv společnosti menších a středních firem, tudíž můžeme uplatnit seznam regulovaných služeb a seznam strategicky významných služeb jako nutných a prioritních pro zajištění kybernetické bezpečnosti z pohledu státu dle Zákona č. 264/2025 Sb..

Režim regulace a zákon o prevenci závažných havárií

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Jak posuzujete vy Vaše regulované služby?
Jste poskytovatelem Strategicky významné služby?
Do jaké míry jste ovlivněni jinými zákony a regulacemi České republiky?

Identifikace a hodnocení aktiv

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Primární aktiva:
- klíčové produkty nebo služby,
- výrobní know-how, postupy, patenty.

Podpůrné aktiva:
- výrobní provozy, sklady, logistika, energetika,
- zaměstnanci a významní dodavatelé,
- informační systémy a software.

Hodnocení aktiv z hlediska financí:
- tržní odhad hmotného majetku (pojistné celky),
- hodnota obnovy hmotného majetku po zničení nebo ztrátě,
- finanční ztráta při výpadku výroby,
- hodnota pojištění,
- výše potenciálních pokut.

Identifikace a hodnocení aktiv

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Hodnocení aktiv z hlediska hmotného majetku:

- technologické posouzení hmotného majetku z hlediska jedinečnosti, (ne)nahraditelnosti a dostupnosti obnovy,
- technologické závislosti nebo návaznost na jiné související technologie,
- zastaralost a zranitelnost technologie,
- řídicí, ERP, ochranné a monitorovací systémy nutné o k provozu dané technologie,
- seznam regulovaných služeb a seznam strategicky významných služeb dle Zákona č. 264/2025 Sb..

Hodnocení aktiv z lidských zdrojů:

- kolik zaměstnanců a s jakou odborností dané aktivum spravuje,
- jaké je riziko ztráty know-how při odchodu zaměstnanců,
- nedbalost a nepozornost zaměstnanců a její vliv na aktivum.

Hodnocení aktiv z know-how a patentů:

- je znalost procesu a technologie know-how společnosti,
- ovlivňuje know-how konkurenceschopnost společnosti,
- vyskytují se zde aktiva ve formě patentů, NDA, autorských práv nebo interních procesů,
- zálohování dokumentace, databází a know-how a stav IT infrastruktury

Identifikace a hodnocení aktiv

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Jak posuzujete vy Vaše aktiva?
Jak vnímáte Vaše aktiva z pohledu jiných regulací státu?
Ceníte si know-how a patenty jako aktivum?

Interní dokumentace a zálohování

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Dokumentace dle NIS2 musí pokrývat:

- Bezpečnostní politiku – základní rámce a odpovědnosti,
- Řízení rizik – procesy, mapy rizik, metodika hodnocení,
- Zálohovací a obnovovací politiku – jakým způsobem a co zálohujeme,
- Plán zvládání incidentů – jak postupujeme při bezpečnostním incidentu, kdo je kontaktován, jaká je komunikace, jak obnovíme systém,
- Kontinuita a obnova činnosti – vazba na dokumentaci záloh, testování, cvičení,
- Dokumentace dodavatelů a třetích stran – smlouvy, požadavky na zálohování, plán obnovy.

Záloha a obnova – postup:

- Inventarizace dat a systémů – zálohování kritických dat a softwaru,
- Zvolení zálohovacího nástroje – způsob zálohování, frekvence zálohování, retenční doba, lokalita záloh,
- Ověření obnovy – testování validity záloh, dokumentování výsledků,
- Dokumentace zálohovacího plánu a výsledků – kdo zálohy spravuje, odpovědnosti, výsledky testů, incidenty spojené se zálohami,
- Propojení s incidentním plánem – pokud dojde k incidentu musí být nastaven proces, který říká jak aktivujeme zálohu, provádíme obnovu.

Externí poskytovatelé služeb NIS2 pro segment OT

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Externí a hybridní režim – klade důraz na dodavatelský řetězec firem poskytujících služby v oblastech IT a OT

Typické služby – monitoring a detekce hrozeb, penetrační testy, bezpečnostní audity, poradenství, řízení incidentů, dokumentace zvládání incidentů, poradenství ve specifických architekturách OT systémů a systému patchování nebo updatování u nepřetržitých provozů 24/365.

Typická řešení – segmentace sítí, firewally mezi OT a IT sítěmi, Couplery mezi jednotlivými OT sítěmi, bezpečnostní monitoring sítí, fyzické oddělení hardwaru od personálů, více faktorová autentizace, standardizace postupů a plánu obnov, zálohování, ověřování dodavatelského řetězce

Životní cykly OT techniky 20 a více let, OT technika navržena jako neoddělitelná funkční součást technologie.

Požadavky na externího dodavatele:

- provádění bezpečnostních testů v minimálním dopadu na provoz technologie,
- znalost OT protokolů a komunikačních sítí různých výrobců a typů OT techniky,
- zajištění plánu obnovy, zajištění plánu zálohování a zajištění plánu provádění změn,
- znalost bezpečnostní politiky upgradování a patchování OT produktů,
- znalost segmentace sítí a návrhu minimalizace propojení s IT sítěmi.

Externí poskytovatelé služeb NIS2 pro segment OT

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Předpokládané certifikace a kompetence:

- ISO 27001 (norma pro systémy řízení bezpečnosti informací),
- IEC 62443 (kybernetická bezpečnost průmyslových řídicích systémů),
- Active a Passive Asset Discovery (limitovaný monitoring sítí při odstávce a plán obnovy),
- znalost IEC 61 508 a IEC 61 511 (funkční bezpečnost),
- znalost Purdue model (standardizovaný funkční model síťové architektury průmyslového prostředí).

Výběr externího dodavatele:

- ověření referencí v OT bezpečnosti v průmyslu, certifikací a kompetencí,
- sjednání oboustranně vyhovující rolí a činností v OT bezpečnosti,
- sjednání požadavků na bezpečnost, audity, hlášení incidentů, přístupu do sítí a změnového managementu,
- on-board a integrace do organizace rizik a aktiv a hodnocení hrozeb a zranitelností,
- provádění pravidelných testů, monitoringu, auditů a reportingu bezpečnosti,
- postupy zvládání incidentů, způsob komunikace a odpovědnosti (simulace incidentů),

Nevhodný nebo nezkušený dodavatel bezpečnosti je rizikem pro provoz stejně jako jakýkoliv bezpečnostní incident.

Externí poskytovatelé služeb NIS2 pro segment OT

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Rizika

- Dodavatel nemá dostatečné zkušenosti s OT – provedení penetračního testu při odstaveném provozu.
- Riziko „poslední míle“ – dodavatel musí být integrován do interního řízení bezpečnosti.
- Riziko změn OT prostředí nebo dodavatele – nutné nové/obnovené analýzy rizik.
- Riziko nesplnění požadavků NIS2 – změna dodavatele.
- Riziko výpadku provozu při testování – úzká spolupráce s dodavatelem, včetně dobrého plánování prováděných testů.

Rozdíly v přístupy mezi IT a OT bezpečností

IT bezpečnost	OT bezpečnost
Důvěrnost –> Integrita -> Dostupnost	Dostupnost/Bezpečnost –> Integrita -> Důvěrnost
Kancelářské sítě, cloud, SaaS	Purdue model, oddělení IT/OT, zóny
ISO 27001	IEC 62443
Patching, Endpoint Detection and Response	Omezené okno údržby, pasivní monitoring
Agresivnější scany	Bezpečnostní testy s minimálním dopadem

Externí poskytovatelé služeb NIS2 pro segment OT

SVAZ CHEMICKÉHO PRŮMYSLU ČR

Jaké máte zkušenosti s dodavateli OT bezpečnosti?
Jaká je dostupnost těchto externích firem?

SPOLCHEMIE

JE TO CHEMIE / JSME TO MY