VÁŠ PARTNER PRO KYBERNETICKOU BEZPEČNOST

Nová Evropská směrnice kybernetické bezpečnosti NIS2 je tu. Změny zákona a vyhlášky pro zlepšení kybernetické bezpečnosti tak pomalu přicházejí. Týkat se budou mnohem většího rozsahu podniků (NÚKIB odhaduje počet na zhruba 6 000 subjektů). Tyto změny vstoupí v platnost přibližně v polovině roku 2024. Buďte připraveni již nyní!

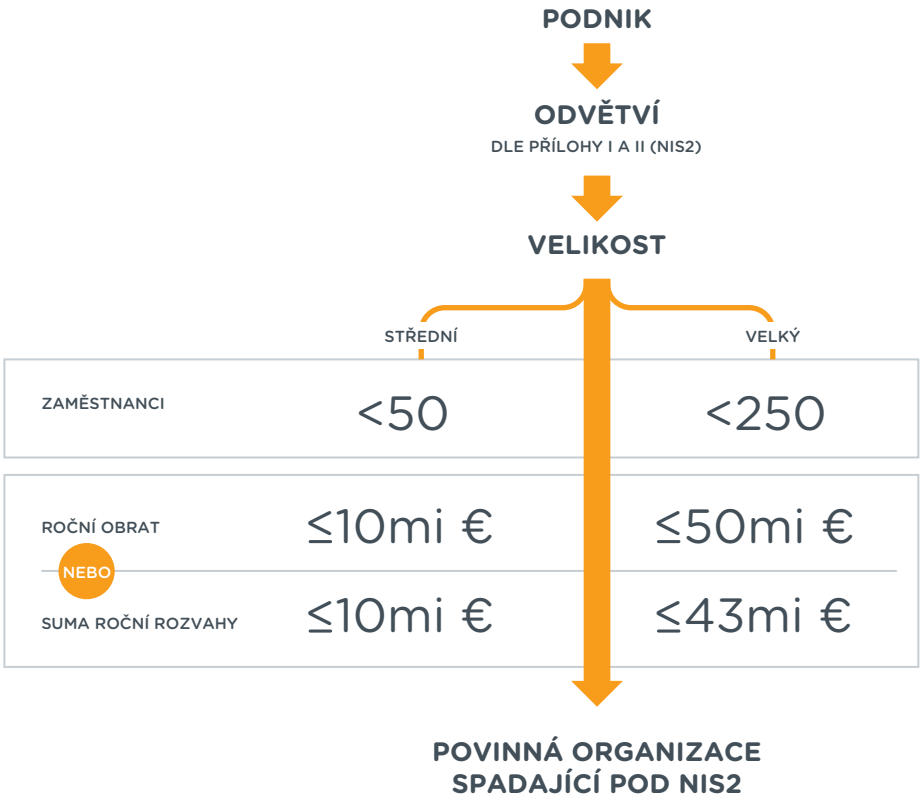
NIS2 – NOVÁ EVROPSKÁ SMĚRNICE KYBERNETICKÉ BEZPEČNOSTI

CO JE NIS2:

NIS2 je nová směrnice o bezpečnosti sítí a informačních systémů (EU 2022/2555), která aktualizuje původní směrnici NIS z roku 2016. Jejím hlavním cílem je zajistit vysokou společnou úroveň kybernetické bezpečnosti v EU, zlepšit ochranu kritických infrastruktur, osobních údajů a podniků všech velikostí před kybernetickými hrozbami.

- Na jejím základě je připravována změna české legislativy, konkrétně zákona č. 181/2014 Sb. – Zákon o kybernetické bezpečnosti (ZoKB) a změna prováděcí vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VoKB).
- Nová česká legislativa bude obsahovat taktéž lhůty pro zahájení plnění nových povinností u těch organizací, které dosud regulaci kybernetické bezpečnosti nepodléhaly.
- Směrnice nově identifikuje 60 služeb roztříděných do 18 odvětví (přílohy I a II Směrnice).
- Nové povinnosti se budou týkat všech subjektů, které poskytují alespoň jednu službu uvedenou v přílohách I a II Směrnice a současně jsou středním nebo velkým podnikem, tedy zaměstnávají více než 50 zaměstnanců, nebo dosahují ročního obratu či bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).
- Pro správné stanovení velikosti podniku je třeba brát v úvahu i skutečnost, zde je daný subjekt nezávislý, tedy zda není partnerem jiného subjektu nebo není s jiným subjektem majetkově propojen.

IDENTIFIKACE POVINNÉHO SUBJEKTU DLE NIS 2



NIS2 – NOVÁ EVROPSKÁ SMĚRNICE KYBERNETICKÉ BEZPEČNOSTI

ZÁSADNÍ ZMĚNY:

- rozšíření počtu povinných subjektů
  (nejméně 6000 soukromých i státních podniků, firem a organizací);
- rozšíření regulovaných odvětví
  (např. odvětví odpadového hospodářství nebo potravinářství);
- rozšíření stávajících regulovaných odvětví o nové **regulované služby**
  (např. stávající odvětví digitální infrastruktury o **nové regulované služby cloud computingu** nebo **poskytovatele služeb a sítí elektronických komunikací)**;
- změna způsobu **identifikace povinných subjektů**, kdy **primárním kritériem** pro zařazení do regulace je nově velikost organizace;
- **povinné vzdělávání vrcholového vedení organizace** a **větší odpovědnost managementu** za zajišťování kybernetické bezpečnosti v organizaci;
- **dobrovolné hlášení relevantních incidentů**, událostí, hrozeb a zranitelnost;
- podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů;
- větší **důraz na sdílení informací mezi povinnými subjekty**;
- prohloubení spolupráce mezi regulátorem a povinnými subjekty,
- **významné zvýšení pokut** za nedodržení uložených povinností.

KONKRÉTNÍ OPATŘENÍ:

- analýza rizik a politika bezpečnosti informací (ISMS);
- zvládání bezpečnostních incidentů (Incident response);
- kontinuita činností (business continuity), která je rozvedena například o oblasti zálohování, zotavení (disaster recovery) nebo krizové řízení;
- bezpečnost v rámci dodavatelského řetězce;
- bezpečnost v rámci pořízení, vývoje a údržby systémů;
- politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (audit);
- praktiky základní počítačové hygieny a vzdělávání v oblasti kybernetické bezpečnosti;
- politiky a postupy týkající se využívání kryptografie a tam, kde je to vhodné, také šifrování;
- bezpečnost lidských zdrojů, řízení přístupů a aktiv;
- využívání vícefaktorového ověření identity, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci.

NIS2 – NOVÁ EVROPSKÁ SMĚRNICE KYBERNETICKÉ BEZPEČNOSTI

KATEGORIZACE SUBJEKTŮ:

Směrnice NIS2 přináší novou kategorizaci subjektů. Organizace se může nově nacházet v těchto kategoriích:

REŽIM VYŠŠÍCH POVINNOSTÍ

REŽIM NIŽŠÍCH POVINNOSTÍ

Kategorie se liší přísností povinných opatření. Rozdíly jsou dány především mírou rizika, zohledněné při zavádění požadavků k řízení kybernetických bezpečnostních rizik a rozdílným způsobem kontroly dodržování stanovených požadavků.

		PŘÍLOHA NIS2 I	PŘÍLOHA NIS2 II
VELIKOST ORGANIZACE	VELKÁ	REŽIM VYŠŠÍCH POVINNOSTÍ	REŽIM NIŽŠÍCH POVINNOSTÍ
	STŘEDNÍ	REŽIM NIŽŠÍCH POVINNOSTÍ	REŽIM NIŽŠÍCH POVINNOSTÍ

MOŽNÉ SANKCE:

SUBJEKTY V REŽIMU VYŠŠÍCH POVINNOSTÍ

Pro subjekty v **Režimu vyšších povinností** hrozí správní pokuty, jejichž maximální výše bude stanovena na nejméně 10 milionů eur nebo maximálně na alespoň 2 % z celkového celosvětového ročního obratu subjektu v předchozím fiskálním roce, podle toho, co je vyšší.

SUBJEKTY V REŽIMU NIŽŠÍCH POVINNOSTÍ

Pro subjekty v **Režimu nižších povinností** hrozí správní pokuty, jejichž maximální výše bude stanovena na nejméně 7 milionů eur nebo maximálně na alespoň 1,4 % z celkového celosvětového ročního obratu subjektu v předchozím fiskálním roce, podle toho, co je vyšší.

PODLE NOVÉ SMĚRNICE NIS2 BUDE NUTNÉ PROVÁDĚT:

1. Identifikaci mezer ve vztahu k požadavkům nové Směrnice.
2. Identifikaci opatření potřebných ke splnění stanovených povinností.
3. Navržení rámců organizačních a technických opatření.
4. Implementaci organizačních a technických opatření.
5. Navržení a zavedení monitorovacích mechanismů pro průběžné ověřování účinnosti opatření.

ODVĚTVÍ

Příloha I a II (NIS2)

1. ENERGETIKA

Příloha I

- Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.
- Subjekty poskytující službu dálkového vytápění nebo chlazení.
- Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.
- Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.
- Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

2. DOPRAVA

- Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.
- Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.
- Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.
- Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

3. BANKOVNICTVÍ

- Sektor infrastruktura finančních trhů je regulován nařízením DORA.

4. INFRASTRUKTURA FINANČNÍCH TRHŮ

- Sektor infrastruktura finančních trhů je regulován nařízením DORA.

5. ZDRAVOTNICTVÍ

- Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

6. PITNÁ VODA

- Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

7. ODPADNÍ VODA

- Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

8. DIGITÁLNÍ INFRASTRUKTURA

- Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů.

9. POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

- Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

10. VEŘEJNÁ SPRÁVA

- Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

11. VESMÍR

- V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

12. POŠTOVNÍ SLUŽBY

Příloha II

- Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

13. ODPADNÍ HOSPODÁŘSTVÍ

- Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

14. CHEMICKÝ PRŮMYSL

- Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

15. POTRAVINÁŘSTVÍ

- Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

16. VÝROBA

- Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

17. POSKYTOVATELÉ DIGI SLUŽEB

- Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

18. VÝZKUM

- Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely

VÍCE INFORMACÍ NA NAŠEM WEBU NEBO U NAŠICH SPECIALISTŮ

KYBERNETICKÁ BEZPEČNOST Z POHLEDU CRA:

- Kybernetická bezpečnost není jednorázová akce ale kontinuální činnost.
- Bezpečnostní dokumentace nejsou jen prázdné texty.
- Součástí kybernetické bezpečnosti nejsou jen firewally, antiviry a další nástroje či technologie.
- Součástí kybernetické bezpečnosti je i vaše know-how, zaměstnanci, podpůrné systémy a technologie, procesy, obchodní partneři i dodavatelé.
- Toto všechno ovlivňuje vaše podnikání a může být cílem nebo zdrojem bezpečnostních incidentů.
- Součástí kybernetické bezpečnosti je ve finále i vaše reputace!

NABÍDKA CRA:

- Základní analýza stavu kybernetické bezpečnosti.
- Interní audit dle požadavků ISMS a ZoKB.
- Tvorba povinné dokumentace a řídící dokumentace dle ISMS.
- GAP analýza včetně návrhů nápravných opatření.
- Analýza rizik.
- Skenování známých zranitelností.
- Penetrační testování (perimetr, wifi, aplikace/web).
- Kampaně (phishing, smishing, vishing).
- Průběžná validace kybernetické bezpečnosti pomocí AI.
- Pokročilá analýza provozu se zaměřením na malware a APT útoky.
- Individuální projekty na míru, např. služby sdíleného Chief Information Security Officera (CISO), který zajistí trvalou kontinuitu kybernetické bezpečnosti ve vaší společnosti.

PROČ CRA:

- **Jsme provozovatelem kritické informační infrastruktury na území ČR.**
- **Jsme držiteli všech důležitých certifikací, zejména ISO/IEC27001:2013.**
- **Máme dlouholeté zkušenosti a znalosti v oblasti datových služeb a kybernetické bezpečnosti.**
- **Víme co potřebujete a dokážeme vám pomoci.**

ČESKÉ RADIOKOMUNIKACE a.s. | prodej@cra.cz