

Základné vlastnosti smernice NIS2

Smernica **NIS 2** (Network and Information Security Directive) je nová európska legislatíva, ktorá nahrádza pôvodnú smernicu NIS a prináša výrazne prísnejšie pravidlá pre kybernetickú bezpečnosť v rámci EÚ. [1]

Medzi jej základné vlastnosti a zmeny patria:

- **Rozšírený rozsah pôsobnosti:** NIS 2 sa vzťahuje na oveľa širšie spektrum odvetví (spolu 18 kritických sektorov) vrátane energetiky, dopravy, zdravotníctva, digitálnej infraštruktúry, verejnej správy či výroby potravín a chemikálií.
- **Prísnejšie bezpečnostné opatrenia:** Organizácie musia implementovať komplexné riadenie rizík, ktoré zahŕňa politiky analýzy rizík, bezpečnosť dodávateľského reťazca, šifrovanie a vzdelávanie zamestnancov v oblasti kyberhygieny.
- **Hlásenie incidentov:** Zavádzajú sa striktné lehoty na oznamovanie významných incidentov. Prvotné varovanie ("včasné oznámenie") musí byť zaslané do **24 hodín** od zistenia incidentu.
- **Zodpovednosť vedenia:** Manažment (štatutárne orgány) nesie priamu osobnú zodpovednosť za dodržiavanie opatrení kybernetickej bezpečnosti. Členovia vedenia musia absolvovať pravidelné školenia v tejto oblasti.
- **Vysoké sankcie:** Za nedodržanie pravidiel hrozia pokuty porovnateľné s GDPR – až do výšky **10 miliónov eur** alebo **2 % z celkového celosvetového ročného obratu**.
- **Bezpečnosť dodávateľského reťazca:** Firmy sú povinné posudzovať a riešiť kybernetické riziká nielen u seba, ale aj u svojich priamych dodávateľov a poskytovateľov služieb. [1, 2, 3, 4, 5]

Kto vydáva potvrdenie o NIS2 a ako prebieha audit

Splnenie požiadaviek smernice NIS2 (na Slovensku transponovanej cez zákon o kybernetickej bezpečnosti) nepotvrdzuje jeden centrálny úrad vydaním certifikátu, ale overuje sa prostredníctvom **povinného auditu kybernetickej bezpečnosti**. [1, 2]

Tu je prehľad toho, kto sa podieľa na príprave, audite a kontrole:

1. Príprava na NIS2 (Konzultanti a firmy)

Prípravu (analýzu rozdielov, nastavenie procesov a implementáciu opatrení) si firma rieši interne alebo s pomocou externých poradenských spoločností, ako sú napríklad [PwC](#), [TÜV SÜD](#) alebo [BizWize](#). Tieto firmy vás pripravujú, ale **nemôžu byť zároveň vašim audítorm** z dôvodu konfliktu záujmov a zachovania nezávislosti. [1, 2, 3, 4]

2. Kto vykonáva audit? (Certifikovaní audítori)

Audit môže vykonať výhradne **certifikovaný audítor kybernetickej bezpečnosti**. Sú to nezávislé subjekty (napr. [Bureau Veritas](#) alebo [CeMS](#)), ktoré majú na túto činnosť autorizáciu. [1, 2, 3, 4]

- **Auditná správa:** Výstupom je oficiálna správa z auditu, ktorá obsahuje zoznam nálezov, klasifikáciu ich kritickosti a posúdenie, či firma spĺňa zákonné normy.
- **Lehota:** Prvý audit musíte absolvovať spravidla **do 2 rokov** od zápisu do registra prevádzkovateľov základných služieb. [1, 2]

3. Kto kontroluje výsledok? (NBÚ)

Záverečnú správu z auditu je prevádzkovateľ povinný doručiť **Národnému bezpečnostnému úradu (NBÚ)** do 30 dní od jej odovzdania audítorom. [1, 2]

- **NBÚ** následne kontroluje, či firma splnila povinnosti. Ak správa poukáže na nedostatky, úrad vyžaduje ich odstránenie v stanovených lehotách.
- **Samohodnotenie:** Menej kritické subjekty ("dôležité subjekty") môžu v určitých prípadoch namiesto externého auditu vykonať samohodnotenie, ale aj to musí podliehať kontrole súladu. [1, 2, 3]

Zhrnutie: Audítor napíše správu o tom, či ste normy splnili, a **NBÚ** je orgán, ktorý na tento proces dohliada a môže udeľovať sankcie v prípade nesúladu. [1, 2]

Povinnosť NIS2, platí len prei **kritické** alebo **dôležité** subjekty podľa počtu zamestnancov a obratu.

NIS2: koho sa týka a aké povinnosti prináša

Smernica NIS2 sprísňuje pravidlá kybernetickej odolnosti v celej EÚ a zásadne rozširuje okruh organizácií, ktoré musia preukázateľne riadiť kybernetické riziká a incidenty. Zavádza nové povinnosti pre kľúčové (essential) a dôležité (important) subjekty v sektoroch uvedených v prílohách NIS2 a spravidla sa vzťahuje na subjekty aspoň strednej veľkosti podľa odporúčania 2003/361/ES (t. j. nie mikro ani malé podniky).



Cieľom NIS2 je zjednotiť úroveň kybernetickej ochrany v členských štátoch a zvýšiť pripravenosť organizácií na hrozby, ktoré môžu ohroziť ich služby či plynulosť prevádzky. Pre Slovensko to znamená, že do pôsobnosti smernice spadá nielen verejný sektor, ale aj široká skupina súkromných spoločností z kritických odvetví. V tomto článku sa preto pozrieme na to, koho sa NIS2 konkrétne týka a aké povinnosti prináša.

Koho sa NIS2 týka

Smernica NIS2 sa vzťahuje na organizácie, ktoré poskytujú služby nevyhnutné pre chod spoločnosti alebo ekonomiky. Základnú skupinu tvoria subjekty v sektoroch vysokej kritickosti (Príloha I (Annex I)) – klasifikované ako essential entities; ďalšiu skupinu tvoria subjekty v ostatných kritických sektoroch (Príloha II (Annex II)) – important entities.

Ide napríklad o:

- **energetické spoločnosti** zabezpečujúce distribúciu elektriny, plynu alebo ropy,
- **dopravné podniky** v leteckej, železničnej, cestnej či námornej doprave,
- **banky a finančné inštitúcie**,
- **zdravotnícke zariadenia** vrátane nemocníc a poskytovateľov kritickej zdravotnej infraštruktúry,
- **priemyselné podniky** s výrobou závislou od digitálnych procesov,
- **telekomunikačné a IT spoločnosti**, ktoré prevádzkujú kritickú digitálnu infraštruktúru,
- **poštové a logistické služby** alebo **dodávateľov pitnej vody**.



Druhou skupinou sú **poskytovatelia digitálnych služieb**, ktorých činnosť sa opiera o online infraštruktúru s veľkým dosahom. Sem patria:

V digitálnej oblasti NIS2 rozlišuje dve skupiny:

- Digitálni poskytovatelia (Príloha II): online trhoviská, online vyhľadávače, platformy sociálnych sietí.

- Digitálna infraštruktúra (Príloha I): cloudové služby, dátové centrá, poskytovatelia DNS a TLD, CDN a MSP/MSSP.

Práve tieto subjekty sú kľúčové pre digitálnu ekonomiku a ich narušenie môže mať celoeurópsky dopad. Okrem odvetvovej klasifikácie rozhoduje aj **veľkosť podniku**. Povinnosti NIS2 sa spravidla vzťahujú na subjekty aspoň strednej veľkosti (t. j. ≥ 50 zamestnancov a/alebo ≥ 10 mil. € ročný obrat alebo bilančná suma) podľa odporúčania 2003/361/ES.

Do pôsobnosti smernice sa preto dostávajú aj **stredne veľké firmy**, ktoré musia posilniť svoju kybernetickú bezpečnosť a zaviesť nové opatrenia. Pre tieto organizácie už nestačí základné IT zabezpečenie – musia preukázať systematické riadenie rizík, pripravenosť na incidenty a schopnosť obnovy prevádzky. V praxi to znamená potrebu nových procesov, špecializovaných nástrojov a pravidelných kontrol.



Kľúčové povinnosti podľa NIS2

Firmy a inštitúcie, ktoré spadajú do pôsobnosti smernice, musia preukázateľne zaviesť opatrenia v oblasti kybernetickej bezpečnosti. Povinnosti možno rozdeliť do troch hlavných oblastí:

1. Analýza rizík a zavádzanie opatrení

Organizácie musia pravidelne identifikovať a hodnotiť kybernetické riziká, ktoré môžu ovplyvniť ich služby alebo infraštruktúru. Na základe analýzy sú povinné prijať primerané technické a organizačné opatrenia – napríklad segmentáciu sietí, zálohovanie kritických dát, viacfaktorovú autentifikáciu alebo školenia zamestnancov. Cieľom je, aby boli schopné predchádzať incidentom a minimalizovať ich dopad.

2. Riadenie a oznamovanie incidentov

Každý významný bezpečnostný incident musí byť riadený podľa vopred nastavených procesov a zároveň nahlásený príslušnému orgánu. NIS2 zavádza trojkrokový mechanizmus: **včasné varovanie do 24 h, oznámenie incidentu do 72 h a finálnu správu do 1 mesiaca** (pri pokračujúcom incidente priebežná správa).

Tento mechanizmus má zabezpečiť rýchlu reakciu a lepšiu koordináciu na celoeurópskej úrovni.

3. Dokumentácia, reportovanie a zodpovednosť

Subjekty musia viesť dokumentáciu o svojich bezpečnostných opatreniach, pravidelne ich vyhodnocovať a byť pripravené doložiť súlad s požiadavkami pri kontrole. Smernica zároveň kladie dôraz na jasne určené **zodpovednosti na úrovni vedenia**. Manažment firiem nesie priamu zodpovednosť za zavedenie opatrení, čo zvyšuje tlak na strategický prístup k riadeniu kybernetickej bezpečnosti.



Legislatívny a odborný rámec

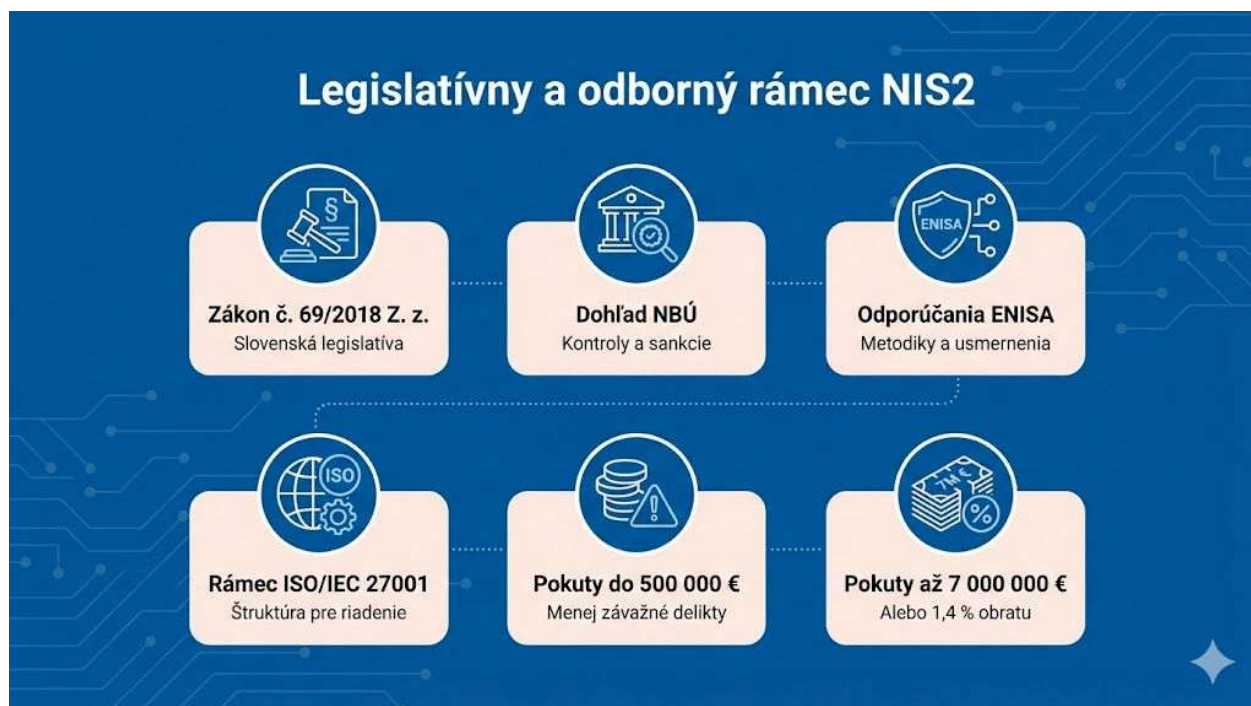
Smernica NIS2 nie je izolovaným dokumentom – nadväzuje na už existujúcu európsku aj slovenskú legislatívu a opiera sa o medzinárodné štandardy v oblasti informačnej bezpečnosti.

Na Slovensku je základom **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** a **zákon č. 95/2019 Z. z.**, ktoré upravujú povinnosti prevádzkovateľov základných a digitálnych služieb. Výklad a detailné požiadavky ďalej rozpracúva **Národný bezpečnostný úrad (NBÚ)** prostredníctvom vyhlášok a metodických usmernení. NBÚ je zároveň orgánom dohľadu, ktorý vykonáva kontroly a ukladá sankcie.

Na európskej úrovni NIS2 dopĺňajú odporúčania **ENISA (Európskej agentúry pre kybernetickú bezpečnosť)**, ktorá vydáva metodiky k riadeniu rizík, hláseniu incidentov či implementácii bezpečnostných opatrení. ENISA zdôrazňuje, že NIS2 rozširuje rozsah pôsobnosti, posilňuje bezpečnostné opatrenia a zavádza nové požiadavky oproti pôvodnej NIS1.

Ako referenčný rámec pre implementáciu opatrení sa najčastejšie využíva **ISO/IEC 27001**, medzinárodná norma pre systémy riadenia informačnej bezpečnosti. Firmám poskytuje štruktúru na zavádzanie kontrol, auditov a kontinuálne zlepšovanie bezpečnostného prostredia.

Nedodržanie povinností pritom nie je len formálnym rizikom. Sankcie môžu dosiahnuť až **500 000 € pri menej závažných deliktoch** a v prípade vážnych porušení až **7 miliónov € alebo 1,4 % celosvetového obratu** organizácie.



Ako sa pripraviť v praxi

Pre mnohé organizácie predstavuje NIS2 úplne novú úroveň povinností, ktoré si vyžadujú systematický prístup. Základom je začať s **komplexnou analýzou rizík**, ktorá odhalí slabé miesta v infraštruktúre a procesoch. Na jej základe možno nastaviť opatrenia – od technických (napr. viacfaktorová autentifikácia, zálohovanie dát, segmentácia sietí) až po organizačné (školenia zamestnancov, nastavenie interných politík a plánov reakcie na incidenty).

Dôležitým krokom je aj **pripravenosť na incidenty**. Firmy by mali mať vypracované scenáre postupu pri kybernetickom útoku a zabezpečiť, aby zodpovedné tímy vedeli reagovať v krátkom čase. V prípade

závažných incidentov platí trojkrokový režim: včasné varovanie do 24 hodín, oznámenie incidentu do 72 hodín a finálna správa do 1 mesiaca (pri pokračujúcom incidente priebežná správa).

Rovnako podstatná je **kontinuálna dokumentácia a pravidelný audit**. Organizácie musia byť schopné kedykoľvek preukázať, že ich opatrenia sú primerané a že sa pravidelne vyhodnocujú. Tento proces sa v praxi najľahšie riadi prostredníctvom špecializovaných nástrojov na evidenciu a reportovanie.

Z pohľadu manažmentu je dôležité uvedomiť si, že NIS2 presúva časť zodpovednosti priamo na vedenie firmy. Manažéri preto musia venovať kybernetickej bezpečnosti rovnakú váhu ako finančným či právnym otázkam – ide o tému, ktorá je priamo spojená s reputáciou a dôveryhodnosťou spoločnosti.



Záver

Smernica NIS2 zásadne mení prístup ku kybernetickej bezpečnosti – rozširuje okruh povinných subjektov a vyžaduje, aby organizácie preukázali systematické riadenie rizík, pripravenosť na incidenty a jasne určené zodpovednosti. Pre mnohé firmy to znamená nutnosť zaviesť nové procesy, technické opatrenia a pravidelnú kontrolu zo strany vedenia.

Zdroje: AI a <https://www.riskminder.tech/post/nis2-koho-sa-tyka-a-ake-povinnosti-prinasa>

Vypracoval: Peter Medo máj 2026