MANAŽÉRSKY CHECKLIST

Connecting your world.

15 BODOV PRE MAJITEĽA FIRMY V REGULÁCII KYBERNETICKEJ BEZPEČNOSTI (NIS2)

LiveTalk by T Business | diel #4 | 21. 10. 2026

Krátky praktický návod pre majiteľov a manažérov stredných firiem, ktoré sa dostali do regulácie kybernetickej bezpečnosti a nevedia, kde začať.

Pripravil ho **Henrich Slezák, IstroSec**, na základe skúseností z praxe a najčastejších otázok, ktoré firmy riešia po vstupe do regulácie.

Zákon č. 69/2018 Z. z., ktorý preberá smernicu NIS2, sa dnes vzťahuje aj na stredné firmy, ktoré sa tým nikdy nezaoberali. Útočník totiž nemusí ísť za veľkou firmou, často stačí jej dodávateľ. Pri útoku NotPetya v roku 2017 sa škodlivý kód dostal do siete dopravcu Maersk cez aktualizáciu ukrajinského účtovného softvéru a škoda sa odhaduje na 250 až 300 miliónov dolárov. Počítače sa podarilo obnoviť len vďaka jedinému doménovému radiču v Ghane, ktorý prežil iba preto, že tam vypadol prúd.

Týka sa nás to? Čo máme urobiť ako prvé? Kto to vo firme zastreší? A vieme to vôbec dokázať? Tento checklist vám pomôže zistiť, čo máte urobiť a v akom poradí. Zodpovednosť podľa zákona nesie vedenie firmy, nie IT oddelenie.

PILIER 1: ZÁKON NIE JE LEN PRE VEĽKÝCH

Cieľ: Vedieť, či sa nás zákon týka. NBÚ firmy neoslovuje, musíme to zistiť sami.

☐ **1. Vieme, v ktorom sektore pôsobíme.**
Zákon má dve prílohy so 16 sektormi. Príloha 1: energetika, doprava, financie, zdravotníctvo, voda, digitálna infraštruktúra, správa IT služieb pre iné firmy, verejná správa, vesmír. Príloha 2: pošta a kuriéri, odpady, chemikálie, potraviny, výroba (zdravotnícke pomôcky, elektronika, stroje, vozidlá), online trhoviská, vyhľadávače a sociálne siete, výskum.
Kontrolná otázka: Vieme napísať, do ktorého sektora patríme?

☐ **2. Vieme, či sme aspoň stredný podnik.**
Zjednodušene: 50 a viac zamestnancov, alebo obrat či bilančná suma nad 10 mil. EUR. Zákon odkazuje na odporúčanie Komisie 2003/361/ES, takže sa počítajú aj prepojené firmy. Sektor a veľkosť musia platiť naraz.
Kontrolná otázka: Vieme, koľko máme zamestnancov a aký obrat vrátane prepojených firiem?

☐ **3. Poznáme výnimky a vieme, čo od nás chcú zákazníci.**
Niektoré činnosti zákon reguluje bez ohľadu na veľkosť, napríklad verejné elektronické komunikácie, dôveryhodné služby, DNS, správu TLD alebo registráciu domén. Ak sme dodávateľ regulovanej firmy, do zákona nepatríme automaticky, ale zákazník s nami musí uzavrieť zmluvu o bezpečnostných opatreniach (§ 19 ods. 2). Ak si nie sme istí, použijeme online dotazník NBÚ (nis2.nbu.gov.sk).
Kontrolná otázka: Žiada už od nás niektorý zákazník bezpečnostné záruky?

SME MALÍ ≠ NIKTO NÁS NEZAUJÍMA
Fínska firma Vastaamo poskytovala psychoterapiu a mala približne 36 000 pacientov. Útočníci ukradli ich záznamy, žiadali od firmy 40 bitcoinov a potom vydierali samotných pacientov. Firma skrachovala vo februári 2021.

PILIER 2: REGISTRÁCIA NA NBÚ

Cieľ: Splniť prvý krok načas a bez pokuty.

☐ 4. Oznámime sa NBÚ do 60 dní od začiatku činnosti.

Zákon pýta názov, sídlo, kontakty vrátane e-mailov, verejných IP adries a telefónnych čísel a zoznam členských štátov EÚ, v ktorých pôsobíme. Podanie sa robí elektronicky, potrebujeme aktívnu elektronickú schránku a eID. Aktuálny formulár je na nbu.gov.sk. Za nesplnenie hrozí pokuta od 300 do 500 000 EUR.

Kontrolná otázka: Vieme, kto u nás oznámenie pripraví a podá a kedy to musí byť hotové?

☐ 5. Vieme, odkedy nás povinnosti viažu.

NBÚ nás zapíše do registra a oznámi to cez svoj informačný systém a do elektronickej schránky. Povinnosti vznikajú dňom uvedeným v oznámení, najskôr 30. deň po zápise. Od zápisu sa počíta aj lehota 12 mesiacov na opatrenia.

Kontrolná otázka: Sledujeme elektronickú schránku, kam oznámenie príde?

PILIER 3: MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI

Cieľ: Mať jedného zodpovedného človeka, ktorý je nezávislý od IT.

☐ 6. Vieme, čo musí manažér KB spĺňať.

Je nezávislý od riadenia prevádzky a vývoja IT (náš IT manažér ani správca sietí to zvyčajne byť nemôže), spĺňa znalostné štandardy (vyhláška 492/2022) a má priamy prístup k vedeniu (§ 20 ods. 4, vyhláška 227/2025). Je to skôr dirigent než hráč: nehrá na každý nástroj, ale stará sa, aby hral celý orchester.

Kontrolná otázka: Je kandidát nezávislý od IT a vie to preukázať?

☐ 7. Rozhodli sme sa: zamestnanec, nový človek alebo externista.

Existujúci zamestnanec sa hodí, ak máme človeka mimo IT, ktorý rozumie firme a má čas. Dostane čas, školenie a právomoc. Nového zamestnanca hľadáme, ak potrebujeme plný úväzok, no odborníkov je na trhu málo. Externý poskytovateľ je v praxi bežný, hoci ho zákon výslovne neupravuje. Zodpovednosť však vždy nesie vedenie firmy.

Kontrolná otázka: Vieme pomenovať človeka, ktorý bude manažérom KB?

☐ 8. Ak ho berieme zvonku, vieme sa opýtať správne.

Nie je zároveň správcom nášho IT? Ako preukáže znalosti? Čo je v zmluve: dodržiavanie našich politík, súhlas s kontrolou a auditom, hlásenie incidentov, súčinnosť? Komu a ako často reportuje? Kto ho zastúpi? Kto zdvihne telefón pri incidente? Kto a ako odovzdá dokumentáciu, keď spolupráca skončí?

Kontrolná otázka: Je dohodnutý zástup aj to, ako vzťah skončí?

PILIER 4: OPATRENIA A DODÁVATELIA

Cieľ: Nastaviť bezpečnosť podľa rizík, nie podľa nákupného zoznamu.

☐ 9. Urobíme analýzu rizík a opatrenia do 12 mesiacov od zápisu.

Zistíme, čo je pre firmu kritické a čo jej hrozí, a podľa toho prijmeme opatrenia aspoň v rozsahu § 20: riadenie incidentov, zálohovanie a obnovu, správu prístupov, školenie ľudí a ďalšie. Certifikát ISO 27001 pomáha, ale povinnosti zo zákona nenahradí. Dokumentácia musí zodpovedať reálnemu stavu.

Kontrolná otázka: Vieme, ktoré tri systémy musia fungovať, aby firma prežila?

☐ 10. Máme poriadok v zmluvách s dodávateľmi.

Dodávateľov s priamym vplyvom na dostupnosť a bezpečnosť našich systémov prejdeme a doplníme zmluvy o bezpečnostných opatreniach a hlásení incidentov (§ 19 ods. 2). Výnimkou sú dodávatelia s nízkym rizikom.

Kontrolná otázka: Vieme, ktorí dodávatelia sú pre nás kritickí?

☐ 11. Vieme, kedy je audit alebo samohodnotenie.

Prvý audit je do 2 rokov od zápisu (§ 29 ods. 1 zákona). Robí ho certifikovaný audítor a je ukončený odovzdaním záverečnej správy, trvať môže najviac 12 mesiacov. Pri nekritickej službe ho môže nahradiť samohodnotenie, ktoré robí manažér KB v systéme NBÚ každé 2 roky, no audit je potom povinný do 5 rokov od zápisu. Ďalšie audity sa robia najneskôr do konca 3. kalendárneho roka nasledujúceho po roku, v ktorom skončil posledný audit, pri samohodnotení do konca 5. roka (vyhláška 493/2022 v znení 212/2026). Pri významnej zmene opatrení je audit do 6 mesiacov. Správu z auditu odovzdávame NBÚ do 30 dní.

Kontrolná otázka: Máme termíny zapísané v kalendári?

STAČÍ JEDNO CHÝBAJÚCE NASTAVENIE

Pri útoku na Change Healthcare vo februári 2024 sa útočníci dostali cez portál bez viacfaktorového overenia. Platforma bola odstavená na viac než mesiac. Dokument by to nezastavil, nastavenie áno.

PILIER 5: INCIDENTY A UDRŽIAVANIE

Cieľ: Vedieť, čo robiť v prvých hodinách, a držať poriadok každý rok.

☐ 12. Vieme včas nahlásiť závažný incident.

Hlási sa cez systém NBÚ: včasné varovanie do 24 hodín od zistenia, oznámenie do 72 hodín a záverečná správa najneskôr do mesiaca po oznámení. Zabezpečíme dôkazy a ak vznikla trestná činnosť, oznámime ju polícii.

Kontrolná otázka: Vie každý u nás, komu nahlásiť podozrenie a kto rozhodne, že ide o závažný incident?

☐ 13. Vieme, kto rozhodne o výkupnom, a odporúčame ho neplatiť.

Rozhodnutie je podnikateľské aj právne, nie technické, preto musí mať vedenie pri stole hotové podklady: stav záloh a riziko pri platbe aj bez nej. Odporúčanie polície a bezpečnostných orgánov je výkupné neplatiť. Platba nezaručí, že dáta dostaneme späť, financuje ďalšie útoky a môže z nás spraviť opakovaný cieľ. Najlepšou odpoveďou je otestovaná záloha. Incident aj vydieranie nahlásime polícii.

Kontrolná otázka: Máme otestované zálohy a vieme, ako dlho trvá obnova?

☐ 14. Hlásime aj to, čo sa ešte nestalo, a zmeny údajov.

Okrem závažných incidentov hlásime cez systém NBÚ aj významnú kybernetickú hrozbu, o ktorej sa dozvieme, a udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný incident. Hlásime aj zraniteľnosť našich verejne dostupných sietí a systémov, ak sa dá zneužiť na závažný incident a nestihli sme ju v primeranom čase odstrániť alebo zmierniť (§ 24 ods. 5). Zmeny údajov zapísaných v registri, ktoré nie sú referenčné, oznamujeme cez systém NBÚ. Zákon uvádza dve lehoty, 14 dní (§ 17 ods. 6) a 30 dní (§ 19 ods. 7), preto sa riadime kratšou. Oznamujeme aj zmenu štatutárneho orgánu (§ 19 ods. 6 písm. i).

Kontrolná otázka: Vieme, kto u nás sleduje hrozby a zmeny údajov?

☐ 15. Raz ročne všetko prejdeme znova.

Aktualizujeme analýzu rizík a dokumentáciu, precvičíme incident a obnovu zo záloh, preškolíme ľudí a skontrolujeme, či sa nezmenili systémy, dodávatelia alebo ľudia. Zákon nechce papier raz, ale bezpečnú firmu stále.

Kontrolná otázka: Kedy sme naposledy aktualizovali analýzu rizík?

POKUTY NIE SÚ SYMBOLICKÉ
Za chýbajúce oznámenie je to od 300 do 500 000 EUR. Za nesplnenie bezpečnostných opatrení alebo nehlásenie incidentu až 7 mil. EUR alebo 1,4 % ročného obratu, pri kritickej základnej službe až 10 mil. EUR alebo 2 % obratu. Ide o horné hranice, ale ukazujú, ako vážne to zákon myslí.

30-DŇOVÝ ZÁKLADNÝ PLÁN, AK ZAČÍNATE OD NULY

Ak máte viac ako polovicu bodov nesplnených, nezačínajte veľkým projektom. Začnite praktikami.

Týždeň	Čo urobiť
1	Zistiť sektor a veľkosť firmy a vyplniť dotazník NBÚ (body 1 až 3).
2	Aktivovať elektronickú schránku a určiť manažéra KB (body 4, 6 až 8).
3	Odoslať oznámenie na NBÚ. Spraviť zoznam dôležitých systémov a dodávateľov (body 4, 9, 10).
4	Urobiť prvú analýzu rizík, naplánovať opatrenia na 12 mesiacov a schváliť ich s vedením (body 9, 11).

RÝCHLY TEST PRIPRAVENOSTI

Po prečítaní checklistu si úprimne označte, čo má firma zvládnuté a kde ešte zostáva priestor na zlepšenie.

1. VIEME, ČI SA NÁS ZÁKON TÝKA?	☐ Áno	☐ Čiastočne	☐ Nie
2. JE OZNÁMENIE NA NBÚ ODOSLANÉ (ALEBO MÁME ISTÝ DÔVOD, PREČO NIE)?	☐ Áno	☐ Čiastočne	☐ Nie
3. MÁME MENOVANÉHO MANAŽÉRA KB, KTORÝ JE NEZÁVISLÝ OD IT, A URČENÝ ZÁSTUP?	☐ Áno	☐ Čiastočne	☐ Nie
4. MÁME ZOZNAM DÔLEŽITÝCH SYSTÉMOV A DODÁVATEĽOV A VIEME, S KTORÝMI TREBA DOPLNIŤ ZMLUVU?	☐ Áno	☐ Čiastočne	☐ Nie
5. UROBILI SME ANALÝZU RIZÍK A VIEME, ČO JE NAJVÄČŠIE RIZIKO?	☐ Áno	☐ Čiastočne	☐ Nie
6. VIEME, KOHO ZAVOLAŤ PRI INCIDENTE, A VIEME HO NAHLÁSIŤ DO 24 HODÍN?	☐ Áno	☐ Čiastočne	☐ Nie
7. VEDENIE FIRMY O PLÁNE VIE A SCHVÁLILO HO?	☐ Áno	☐ Čiastočne	☐ Nie

Každé „NIE“ alebo „ČIASTOČNE“ ukazuje konkrétnu oblasť, ktorú je lepšie vyriešiť pred kontrolou či incidentom než po ňom.

Zaujala vás táto téma alebo máte otázky k vašej konkrétnej situácii?
Radi sa na to s vami pozrieme. Stačí nás kontaktovať cez online formulár.

Praktické odporúčania pre vedenie podniku. Nenahrádzajú právne poradenstvo. Vychádzajú zo znenia zákona č. 69/2018 Z. z. účinného od 30. 4. 2026, stav k 23. 10. 2026. Presné povinnosti a formuláre si overte na nbu.gov.sk.