MANAŽÉRSKY CHECKLIST

Connecting your world.

15 BODOV PRE DIGITÁLNU STABILITU FIRMY

LiveTalk by T Business
23. 4. 2026

Krátky návod, ako držať kontrolu nad technológiami a regulačnými povinnosťami. Ako ochrániť hodnotu firmy v čase, keď sa zodpovednosť za dáta a kybernetickú bezpečnosť presunula zo serverovej miestnosti do zasadačky vedenia.

PILIER 1: DÁTA A ICH BEZPEČNOSŤ

Cieľ: Vedieť, kde máte „rodinné striebro“ a že oň neprídete.

☐ **1. Máme jasno v tom, kde sú uložené naše kľúčové dáta a kto k nim má prístup.**
Zoznam systémov/aplikácií, vlastníkov dát, používateľov dát, úrovní prístupu. Ak IT nevie odpovedať do 24 hodín, je to červená vlajka.

☐ **2. Preverili sme, že naše zálohy sú fyzicky oddelené od hlavnej siete, aby ich nezašifroval prípadný útok.**
Pravidlo 3–2–1: 3 kópie, 2 rôzne médiá, 1 offline. Len počas roka 2025 ransomware zašifroval zálohy v desiatkach verejne známych prípadov v SR a ČR.

☐ **3. IT tím potvrdil, že sme vykonali test obnovy dát zo zálohy (vieme, ako dlho by to trvalo v ostrom režime).**
Test obnovy dát min. 1× ročne. Ak obnova trvá viac než je pre nás akceptovateľné, treba zaznamenať ako riziko a riadiť ho napr. rozhodnutím o investícii.

☐ **4. Vieme, ktoré dáta podliehajú regulácii (napr. GDPR, Data Act, sektorové regulácie) a máme preukázateľný záznam ich spracúvania.**
GDPR čl. 30 – záznam o činnostiach spracúvania. V audite nestačí slovo, musí to existovať dôkaz alebo záznam.

PILIER 2: KONTINUITA BIZNISU

Cieľ: Zabezpečiť, aby firma fungovala, aj keď technika zlyhá.

☐ **5. Poznáme maximálny čas, počas ktorého môže byť naša firma „offline“ bez toho, aby to ohrozilo náš biznis či existenciu firmy.**
Pre väčšinu stredných firiem je to 24 až 72 hodín. Pre výrobu a zdravotníctvo menej. Toto číslo si musí určiť biznis, nie IT.

☐ **6. Máme určený krízový scenár pre prvých 60 minút po zistení incidentu: kto komu volá, kto rozhoduje, kto komunikuje navonok a hlavne, čo sa komunikuje.**
Krízový telefónny strom a šablóny komunikácie (smerom k zákazníkom, médiám, regulátorovi). Nie v PDF-ku v archíve, ale po ruke v telefónoch.

☐ **7. Máme istotu, že naši dodávatelia (cloud, softvér) garantujú dostupnosť služieb a súvisiace aktualizácie (patchovanie zraniteľností), za ktorú platíme (kontrola SLA zmlúv).**
DORA a NIS2 explicitne vyžadujú riadenie rizík tretích strán. Kontrola SLA nie je len obchodná záležitosť, ale regulačná povinnosť.

☐ **8. Máme identifikovaných svojich kritických dodávateľov tretích strán a vieme, čo sa stane, ak niektorý z nich vypadne.**
NIS2 čl. 21 ods. 2 písm. d). V roku 2025 Deutsche Telekom ako prvý veľký telco bol designovaný ako CTPP podľa DORA (18. 11. 2025). Koncentračné riziko je dnes regulačná téma.

PILIER 3: STRATEGICKÉ RIADENIE A ZODPOVEDNOSŤ

Cieľ: Chrániť firmu ako celok a štatutára ako osobu.

☐ **9. Pravidelne (viackrát ročne) sa venujeme téme riadenia rizík vrátane IT a regulačných rizík na vedení firmy (zápis z tohto stretnutia je vašim argumentom pri audite).**
NIS2 čl. 20 (slovenská transpozícia v § 17a ZoKB): štatutárny orgán schvaľuje opatrenia kybernetickej bezpečnosti. Žiadny zápis = žiadny dôkaz = osobná zodpovednosť.

☐ **10. Máme nastavené základné vzdelávanie zamestnancov v oblasti informačnej a kybernetickej bezpečnosti (pretože 90 % incidentov začína jednoduchým kliknutím na škodlivý e-mail).**
Školenie + periodická simulácia phishingu. Kľúčový nie je certifikát, kľúčové je, koľko ľudí v simulácii klikne. To je tréning.

☐ **11. Otázky na IT tím sú zamerané na biznisové dopady, nie na technické parametre (rozumieme si navzájom).**
Ak odpoveď IT obsahuje iba skratky, otázka bola zle položená. Manažér má právo na odpoveď v biznisovej reči.

☐ **12. Vieme, aké legislatívne povinnosti (NIS2, DORA, AI Act, GDPR) sa nás týkajú, a máme plán na ich postupné plnenie.**
Nie všetko platí pre všetkých. Ale každý manažér musí vedieť, čo zo zoznamu sa týka jeho firmy. Neznalosť neospravedlňuje

☐ **13. Štatutár osobne rozumie, aké rozhodnutia o kybernetickej bezpečnosti schvaľuje, a že ich schvaľovanie je regulačnou povinnosťou.**
Bod 10. Prílohy 1 vyhlášky 227/2025 Z. z.:„štatutárny orgán sa preukázateľne zaväzuje dodržiavať povinnosti v oblasti kybernetickej bezpečnosti v súlade so stratégiou kybernetickej bezpečnosti a určenými bezpečnostnými politikami a postupmi.“ Od NIS2 nie je možné delegovať zodpovednosť 100 % na IT riaditeľa. Sankcie smerujú na štatutárny orgán.

PILIER 4: AI A NOVÉ TECHNOLÓGIE

Cieľ: Vedieť, čo vo firme robí AI a kto za ňu zodpovedá.

☐ **14. Vieme, kto vo firme používa AI nástroje a aké dáta do nich môžu vkladať (AI Act čl. 4 AI literacy).**
Od 2. 2. 2025. Nejde o zákaz AI. Ide o to, aby zamestnanci mali základné vedomosti o tom, čo AI je a čo doň môžu / nesmú vkladať. Predpoklad: máte prehľad o používaných AI nástrojoch vo firme.

☐ **15. Máme prípravu na Annex III AI Actu (vysokorizikové systémy, 2. 8. 2026), ak nás sa týka (HR, úverovanie, vzdelávanie, kritická infraštruktúra).**
Posúdenie, či váš AI prípad spadá pod Annex III, musí byť zdokumentované. Ak áno, čakajú vás významné povinnosti vrátane risk management systému.

30-DŇOVÁ BASELINE, AK ZAČÍNATE OD NULY

Ak máte viac ako polovicu bodov vyššie nesplnených, nestrácajte čas s rozsiahlymi auditmi. Začnite napríklad takto:

Týždeň	Akcia
1	Mapa kľúčových dát: kto má prístup, kde sú uložené. Test obnovy dát zo zálohy (1 systém stačí).
2	Krízový telefónny strom + šablóna komunikácie smerom von (kto, čo a komu komunikuje). Identifikácia troch najkritickejších dodávateľov vrátane kontaktov a ich SLA.
3	Phishing simulácia (stačí jednoduchá, interná) a školenie zamestnancov. Vyčleniť rozpočet 1–2 % obratu na kybernetickú bezpečnosť na ďalší rok.
4	Bod „kybernetická odolnosť“ na porade vedenia. Zrealizovať stručný zápis zo stretnutia vedenia – aktuálny stav, úlohy, riešitelia, termíny. Plán postupného súladu s NIS2 (alebo doklad, že sa vás netýka).

ČO REGULÁCIA VYŽADUJE OD ŠTATUTÁRA

Regulácia	Koho sa týka	Čo musí štatutár
NIS2 / zákon 69/2018 Z. z.	Prevádzkovatelia základných služieb + dôležitých služieb (stredné/veľké firmy v mnohých sektoroch)	Schvaľovať a kontrolovať opatrenia kybernetickej bezpečnosti. Zápis z porady vedenia. Osobná zodpovednosť.
DORA	Finančný sektor a ich IKT* dodávatelia	Management body je „fully responsible“ za riadenie IKT rizík. Riadenie rizík tretích strán.
AI Act	Každý, kto používa alebo poskytuje AI systémy	čl. 4 – AI literacy v organizácii. čl. 5 – vedieť, čo je zakázané. Annex III – posúdenie od 2. 8. 2026.
GDPR	Každý, kto spracúva osobné údaje	Záznamy o činnostiach spracúvania. Hlásenie incidentov do 72 hodín.
Vyhláška NBÚ 227/2025 Z. z.	Prevádzkovatelia základných služieb	Konkretizuje bezpečnostné opatrenia (organizačné, personálne, technické).
Vyhláška NBÚ 226/2025 Z. z.	Prevádzkovatelia základných služieb	Stanovuje lehoty a obsah hlásenia zraniteľností a hlásenia incidentov (24h/72h/finálna správa).

*IKT = informačné a komunikačné technológie

ČO TENTO CHECKLIST NENAHRÁDZA

- Nenahrádza právne stanovisko (či sa vás NIS2 alebo iná regulácia týka, na to potrebujete vykonať posúdenie).
- Nenahrádza bezpečnostný audit ani audit kybernetickej bezpečnosti (tento checklist je o rýchlej manažérskej kontrole, nie o technickej zrelosti).
- Nenahrádza zdravý rozum (ak máte pocit, že niečo nesedí, povedzte to nahlas vo vedení).

NAŠLI STE V CHECKLISTE BODY, KTORÉ NEMÁTE SPLNENÉ?

Nemusíte na to byť sami. Digitálna odolnosť nie je jednorazová úloha, ale proces. Radi s vami prejdeme vaše konkrétne otázky a navrhneme kroky, ktoré posilnia bezpečnosť, regulačný súlad a odolnosť vašej firmy.

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