O2 CyberNews

Checklist

Jak vyhovět novému kyberzákonu

Od 1. listopadu 2025 je účinný nový **zákon o kybernetické bezpečnosti**. Připravili jsme pro vás jednoduchý checklist, který vám pomůže vyhovět jeho požadavkům.

Konečné znění zákona najdete zde. Aktuální znění vyhlášek týkající se povinností dotčených subjektů v nižším i vyšším režimu si přečtěte zde.

Co si kdy pohlídat

31

1. 11. 2025 – zákon nabývá účinnosti.

30

Do 30 dnů po obdržení rozhodnutí o registraci je potřeba nahlásit kontaktní údaje odpovědných osob.

60

Do 60 dnů (tedy do konce roku 2025) má organizace čas na samoidentifikaci a nahlášení se Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Do 1 roku musí organizace zavést odpovídající bezpečnostní opatření, nastavit evidenci aktiv a rizik, zajistit schopnost detekce a hlášení bezpečnostních incidentů a zavést řízení kybernetické bezpečnosti (ISMS).

Máme splněno?

- [ ] **Zjistili jsme, zda pod regulaci spadáme a do jakého režimu**

  Zákon vyžaduje: samoidentifikaci. Musíte si sami vyhodnotit, zda spadáte mezi regulované subjekty a jestli do vyššího („essential entities“), nebo nižšího („important entities“) režimu. Kritéria najdete v zákoně a dělí se podle sektoru, velikosti organizace či poskytované služby. Zároveň platí, že se regulace může dotýkat jen některých vašich systémů, informačních aktiv nebo dodavatelů a v různých režimech. I to je potřeba identifikovat.

- [ ] **Zaregistrovali jsme se u NÚKIBu**

  Zákon vyžaduje: pokud pod regulaci spadáte, musíte se do konce roku 2025 zaregistrovat na Portálu NÚKIB. Okamžikem registrace vám pak začíná běžet roční lhůta pro zavedení bezpečnostních opatření.

- [ ] **Definovali jsme si role a odpovědnosti**

  Zákon vyžaduje: současně s registrací určit kontaktní osobu pro NÚKIB. A dále zajistit osobní odpovědnost vedení. U vyššího režimu jsou stanoveny i další povinné funkce (manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva a auditor kybernetické bezpečnosti).

- [ ] **Provedli jsme analýzu rizik**

  Zákon vyžaduje: pravidelně vyhodnocovat rizika, vést evidenci aktiv (tedy mít přehled o systémech, datech a službách, které pro vás mají hodnotu) a postupně přijímat přiměřená opatření v rámci systému řízení kybernetické bezpečnosti (ISMS).

  U vyššího režimu bude vyžadován větší rozsah dokumentace (včetně detailní evidence primárních a podpůrných aktiv, metodiky pro jejich hodnocení, ročního přezkumu účinnosti ISMS, prohlášení o aplikovatelnosti, plánu zvládání rizik nebo pravidelných auditů).

- [ ] **Máme procesy pro reakci a hlášení incidentů**

  Zákon vyžaduje: mít procesy pro identifikaci, řešení a hlášení incidentů přes Portál NÚKIB. Hlásit je musíte předběžně do 24 hodin, detailně do 72 hodin, a to v obou režimech.

- [ ] **Zajistili jsme bezpečnost dodavatelského řetězce**

  Zákon vyžaduje: řídit kybernetická rizika v dodavatelském řetězci a smluvních vztazích. U nižšího režimu stačí, aby smlouvy obsahovaly minimální bezpečnostní požadavky, u vyššího je nutné detailnější řízení celého řetězce včetně posouzení rizik dodavatelů.

- [ ] **Nastavili jsme pravidla a školíme zaměstnance**

  Zákon vyžaduje: zavést a udržovat interní politiky kybernetické bezpečnosti a zajistit povědomí zaměstnanců o bezpečnostních zásadách.

- [ ] **Zavedli jsme a ověřujeme technická opatření**

  Zákon vyžaduje: zavést přiměřená technická opatření, jako je segmentace sítí, antivirová ochrana, logování, vícefaktorová autentizace, pravidelné aktualizace a šifrování komunikace. Subjekty ve vyšším režimu mají navíc povinnost systematického monitoringu nebo penetračního testování.

- [ ] **Vedeme dokumentaci a jsme připraveni na kontrolu**

  Zákon vyžaduje: vést dokumentaci o přijatých opatřeních (co je zavedeno, co je v procesu, co se plánuje) a umožnit jejich doložení při kontrole NÚKIBem. Zatímco u nižšího režimu budou kontroly namátkové, u vyššího budou důkladnější a častější. Konkrétně bude NÚKIB u vyššího režimu vyžadovat rozsáhlou dokumentaci k ISMS, roční zprávu o přezkumu, plány zvládání rizik, prohlášení o aplikovatelnosti nebo zprávy z auditů a kontrol.