# Nový zákon o kybernetické bezpečnosti krok za krokem

Checklist: 12 důležitých kroků ke splnění nových povinností

Zákon (č. 264/2025 Sb.) nově dopadá na mnohem více organizací a přidává povinnosti v oblasti řízení kybernetických rizik. Tento checklist vám pomůže pochopit hlavní požadavky a stihnout je v termínech. **Zákon je účinný od 1. listopadu 2025**.

## 1. Zjistit, jestli spadáme pod zákon a do jakého režimu

Nový zákon předpokládá, že si sami vyhodnotíte, jestli na vás dopadá. Je potřeba projít kritéria v zákoně a vyhlášce o regulovaných službách a podle nich ověřit, zda poskytujete regulovanou službu ve vyšším nebo nižším režimu povinností.

## 2. Ohlásit regulované služby na Portálu NÚKIB

Pokud na vás zákon dopadá, musíte to včas oznámit. Do 60 dnů od jeho účinnosti je potřeba přes Portál NÚKIB ohlásit regulovanou službu. Připravte si základní informace o organizaci, kontaktních osobách a službách, které poskytujete.

## 3. Doplnit kontaktní údaje na Portálu NÚKIB

Po ohlášení NÚKIB službu zaregistruje a pošle vám potvrzení. Od jeho doručení běží 30denní lhůta, ve které musíte určit kontaktní osobu a doplnit další údaje – pokud jste je nezadali už při prvním ohlášení. Vše se řeší přes Portál NÚKIB. Vyšší režim stanovuje i další povinné role (manažer kybernetické bezpečnosti, architekt a auditor kybernetické bezpečnosti + garanti aktiv).

## 4. Implementovat opatření podle režimu povinností

Od registrace regulované služby máte 12 měsíců na to, abyste zavedli požadovaná bezpečnostní opatření podle vyhlášky a svého režimu. Prakticky to znamená připravit si plán prací, udělat analýzu rizik, nastavit technická opatření, rozběhnout ISMS a dát dohromady tým, který to celé potáhne.

## 5. Připravit analýzu aktiv a provést analýzu rizik

Jaká aktiva používáte a jaká rizika se k nim vážou? Připravte si přehled dat, systémů a služeb, kterých si ceníte, určete klíčová i podpůrná aktiva, udělejte analýzu rizik s popsanou metodikou, navrhněte plán jejich zvládání a nastavte si pravidelné přezkumy (u vyššího režimu každý rok).

Checklist připravila
Cybrela

info@cybrela.com

www.cybrela.com

## 6. Zavést systém řízení kybernetické bezpečnosti (ISMS)

ISMS je základ celého řízení kyberbezpečnosti podle nového zákona. Nastavte procesy tak, aby byly v souladu s vaším režimem povinností, ale zároveň odpovídaly vašemu provozu. U vyššího režimu počítejte s větší podrobností: detailní procesy, rozsáhlá dokumentace, prohlášení o aplikovatelnosti i zprávy z auditů a pravidelné přezkumy.

## 7. Nastavit procesy pro detekci, reakci a hlášení incidentů

Zákon přesně určuje, co a kdy musíte hlásit. Včas nastavte postupy pro detekci a hlášení incidentů. Zajistěte si také přístup do Portálu NÚKIB, přes který se incidenty odesílají. Po registraci běží roční lhůta, po jejímž uplynutí už musíte incidenty hlásit naplno.

## 8. Proškolit zaměstnance a připravit interní pravidla

Aby všechno fungovalo, je potřeba mít jasná pravidla a lidi, kteří jim rozumí a umí s nimi pracovat. Vytvořte interní politiky pro přístupy, dvoufaktorové ověřování nebo práci se zařízeními, a nezapomeňte proškolit zaměstnance. Ideálně pak ověřte, jestli by nenaletěli třeba na phishing.

## 9. Definovat požadavky na bezpečnost do smluv s dodavateli

Spolu s vlastními povinnostmi musíte ohlídat i to, co pro vás dělají dodavatelé. Projděte si smlouvy s IT dodavateli, určete ty nejkritičtější a doplňte do smluv bezpečnostní požadavky odpovídající vašemu režimu. U nižšího režimu stačí základní podmínky, u vyššího už jde o detailnější řízení dodavatelů – od posouzení jejich rizik až po auditní práva, SLA pro řešení incidentů nebo práci s privilegovanými přístupy.

## 10. Implementovat technická opatření

Technická opatření jsou základ toho, aby vaše prostředí něco vydrželo. Patří sem vícefaktorové ověřování, segmentace sítě, ochrana koncových zařízení nebo smysluplné logování. Pokud spadáte do vyššího režimu, přidávají se i náročnější prvky: průběžný monitoring, penetrační testy a detailní řízení přístupů.

## 11. Vytvořit / zaktualizovat bezpečnostní dokumentaci

Bezpečnostní dokumentace je něco, čím se při kontrole začne i skončí, takže je dobré ji mít v pořádku. Udělejte si přehled o tom, co máte hotové, co běží a co je v plánu, veďte evidenci aktiv, rizik, přijatých opatření i incidentů a připravte si i vlastní checklist, podle kterého si budete moci průběžně ověřovat, že vše drží pohromadě.

## 12. Průběžně sledovat hrozby a doporučení

Aby vám systém nezestárl hned po zavedení, je potřeba průběžně sledovat hrozby i doporučení NÚKIB a podle toho upravovat procesy a technická opatření. Stejně důležité je i pravidelné zlepšování a udržování ISMS, aby odpovídal tomu, co se ve vašem provozu i v kyberprostoru mění.

Checklist připravila
Cybrela

info@cybrela.com

www.cybrela.com