

[Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti](#) nadobudol účinnosť **1. apríla 2018**.

Zákon upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov.

Podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti sa za základnú službu považuje služba, ktorá je zaradená v [zozname základných služieb](#) a

- ✓ závisí od sietí a informačných systémov a je vykonávaná aspoň v jednom [sektore alebo podsektore](#),
- ✓ je [informačným systémom verejnej správy \(ISVS\)](#), alebo
- ✓ je prvkom [kritickej infraštruktúry](#).

Úrad zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do [registra prevádzkovateľov základných služieb](#)

- I. na základe **oznámenia prevádzkovateľa** služby,
- II. na základe **podnetu ústredného orgánu**, ak došlo k prekročeniu identifikačných kritérií prevádzkovanvej služby,
- III. **z vlastnej iniciatívy**, ak sa dozvedel o prekročení identifikačných kritérií a nedošlo k postupu podľa predchádzajúcich bodov.

Od 1. marca 2020 úrad v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti, na základe podnetu Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, **zaradil do [registra prevádzkovateľov základných služieb](#) ďalších prevádzkovateľov informačných systémov verejnej správy (ISVS)**.

Informačným systémom verejnej správy je podľa [zákona č. 95/2019 Z. z. o informačných technológiách verejnej správy](#) informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.

Podľa zákona o kybernetickej bezpečnosti je informačný systém verejnej správy základnou službou. Komunikácia s občanmi (mailový server, webové sídlo) je kľúčovou službou verejnej správy.

Auditom kybernetickej bezpečnosti sa overuje plnenie povinností podľa zákona č. 69/2018 Z. z. a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby.

Cieľom je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom.

Auditom sa **identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.**

[Audit kybernetickej bezpečnosti vykonáva audítor certifikovaný akreditovaným certifikačným orgánom certifikujúcim osoby príslušným na certifikáciu personálu v oblasti kybernetickej bezpečnosti podľa ISO/IEC 17024.](#)

Prevádzkovateľ základnej služby **je povinný** preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek vykonaním auditu kybernetickej bezpečnosti do 2 rokov odo dňa zaradenia do registra prevádzkovateľov základných služieb. Náklady auditu znáša prevádzkovateľ základnej služby.

Prevádzkovateľ základnej služby je povinný predložiť úradu [záverečnú správu o výsledkoch auditu](#) spolu s opatreniami na nápravu a s lehotami na ich odstránenie **do 30 dní** od ukončenia auditu.

Súčasťou záverečnej správy je aj kontrolný záznam, ktorý [obsahuje súbor požiadaviek podľa zákona a jeho vykonávacích predpisov](#). V kontrolnom zázname audítor uvádza najmä súlad alebo nesúlad s požiadavkami na implementované bezpečnostné opatrenia, zistenia auditu pre jednotlivé požiadavky, získané dôkazy podporujúce uvedené zistenia a referenciu na použitú metódu overenia.

Úrad môže kedykoľvek vykonať audit prevádzkovateľa základnej služby, alebo audítora o vykonanie auditu s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek podľa zákona o kybernetickej bezpečnosti. Náklady takto vykonaného auditu znáša úrad.

Hraničným termínom pre výkon auditu a predloženie záverečnej správy je november 2021 pre prevádzkovateľov zaradených do zoznamu základných služieb ešte v čase polročnej lehoty po vydaní a nadobudnutí účinnosti zákona.

Sankcie

Kontrolu nad dodržiavaním požiadaviek vyplývajúcich so zákona vykonáva Národný bezpečnostný úrad. Národný bezpečnostný úrad je oprávnený kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľov základných služieb. **Národný bezpečnostný úrad môže uložiť pokutu od 300 EUR do 300 000 EUR, pri nedodržaní povinností daných zákonom.**

Zdroj:

<https://www.nbu.gov.sk/kyberneticka-bezpecnost/kontrola-a-audit/index.html>

<https://www.nbu.gov.sk/kyberneticka-bezpecnost/index.html>

<https://www.nbu.gov.sk/kyberneticka-bezpecnost/prevadzkovatelia-zakladnej-sluzby/index.html>