



Vyhláška č. 227/2025 Z. z.

RNDr. Daniel Schikor



Táto vyhláška ustanovuje obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete a informačné systémy a operačné technológie, a obsah a štruktúru bezpečnostnej dokumentácie podľa § 20 zákona.

Bezpečnostné opatrenia sa prijímajú s cieľom:

- identifikovať zraniteľnosti, kybernetické hrozby a riziká,
- chrániť preventívne informačné aktíva pred kybernetickou hrozbou a zabrániť vzniku kybernetického bezpečnostného incidentu,
- detegovať kybernetické bezpečnostné incidenty,
- reagovať na identifikované zraniteľnosti a kybernetické bezpečnostné incidenty a minimalizovať ich vplyv na siete a informačné systémy a
- obnoviť siete a informačné systémy, napraviť negatívne dopady po vzniku kybernetického bezpečnostného incidentu a uviesť poskytované služby do stavu plynulého a nerušeného poskytovania.



Bezpečnostné opatrenia sa prijímajú pre

organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti	správu identít a prístupov
správu zraniteľností a kybernetických hrozieb	bezpečnosť pri prevádzke sietí a informačných systémov
správu aktív a riadenie kybernetických hrozieb a rizík	ochranu proti škodlivému kódu a nežiaducemu obsahu
riadenie udalostí a kybernetických bezpečnostných incidentov	systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť
riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie	monitorovanie, zaznamenávanie a hlásenie udalostí
bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií	fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení
postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti	ochranu záznamov, súkromia a označovanie informácií
kryptografické opatrenia a zásady používania kryptografie	dodávateľský reťazec
bezpečnosť a spôsobilosti ľudských zdrojov	obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT



Bezpečnostné opatrenia musia zahŕňať

určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti

detekciu kybernetických bezpečnostných incidentov

evidenciu kybernetických bezpečnostných incidentov

postupy riešenia a riešenie kybernetických bezpečnostných incidentov

určenie kontaktnej osoby pre prijímanie a evidenciu hlásení

pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálného systému včasného varovania

určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly

určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie

vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti



Rozsah všeobecných bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti je uvedený v prílohe č. 1 vyhlášky a **určuje sa na základe analýzy rizík.**

Bezpečnostné opatrenia sa navrhujú, prijímajú a vykonávajú tak, aby **ošetrili všetky riziká identifikované v rámci vykonanej analýzy rizík**, naplnili požiadavky stratégie kybernetickej bezpečnosti a bezpečnostnej politiky.

Výsledky analýzy rizík a návrhy bezpečnostných opatrení v nadväznosti na identifikované riziká preukázateľným spôsobom schvaľuje osoba ktorá je určená v zmysle zákona.



Termíny kontrolnej činnosti

Každé dva roky

- pravidelne, najmenej raz za dva roky, preskúvané a podpisované dohody o mlčanlivosti, ktoré odrážajú potreby prevádzkovateľa základnej služby pre zachovanie dôvernosti,
- pravidelne, najmenej raz za dva roky monitorované, preskúvané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán, ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby.



Termíny kontrolnej činnosti

Raz ročne

- preskúmavanie identifikovaných rizík najmenej raz ročne, a v závislosti od výsledkov, aj aktualizáciu rizík a revíziu prijatých bezpečnostných opatrení,
- najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností,
- plánovanie a testovanie riešenia kybernetických bezpečnostných incidentov aspoň raz za kalendárny rok a sú definované, prijaté a oznámené procesy, úlohy a zodpovednosti v oblasti riešenia kybernetických bezpečnostných incidentov,
- raz ročne testované pravidlá pre izoláciu kritických komponentov sietí, informačných systémov a operačných technológií počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia.



Termíny kontrolnej činnosti

Raz ročne

- raz ročne testované záložné kópie dát, softvéru a konfigurácie sietí, informačných systémov a operačných technológií; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia,
- raz ročne vykonávaná kontrola a aktualizácia konfigurácie komponentov sietí, informačných systémov a operačných technológií podľa vývoja hrozieb; o kontrole sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia,
- prehodnocovanie odolnosti zavedených kryptografických mechanizmov sa vykonáva najmenej raz ročne a vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia.



Termíny kontrolnej činnosti

Raz ročne

- v pravidelných intervaloch, najmenej raz ročne je vykonávaná kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom vykonávania oprávnení vrátane detekcie a následného zneplatnenia nepoužívaných prístupových účtov; vyhotovuje sa o tom záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia,
- súlad so stratégiou kybernetickej bezpečnosti, bezpečnostnými politikami, bezpečnostnými štandardmi a normami je prehodnocovaný najmenej raz za kalendárny rok v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií.



Termíny kontrolnej činnosti

Pravidelné činnosti bez presne stanoveného intervalu (ale musia byť vykonávané)

- riadenie kybernetickej bezpečnosti je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií,
- prijaté a aplikované postupy na pravidelné prehodnocovanie odolnosti zavedených kryptografických mechanizmov.



Uchovávanie záznamov

Záznamy o testovaní izolácie, záloh, konfigurácií, kryptografie, prístupov – uchovávať od posledného auditu do nasledujúceho auditu alebo samohodnotenia.

Najmenej 12 mesiacov sú uchovávané relevantné prevádzkové a bezpečnostné logy, ktoré zachytávajú činnosti, výnimky, poruchy a iné relevantné prevádzkové a bezpečnostné udalosti, pričom bude zabránené zmene ich integrity a neoprávneným prístupom k nim.



Bezpečnostné incidenty

Povinnosť hlásiť každý závažný kybernetický bezpečnostný incident. Za závažný kybernetický bezpečnostný incident sa považuje rozsiahly kybernetický bezpečnostný incident a kybernetický bezpečnostný incident, ktorý spôsobil:

- úplný výpadok alebo nedostupnosť činnosti na viac ako 60 minút (KPZS 30 minút),
- narušenie alebo obmedzenie činnosti na viac ako 180 minút (KPZS 60 minút),
- ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb,
- hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur,
- zamedzenie vykonania záchranných prác alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni alebo spôsobenie viac ako 100 zranených osôb vyžadujúcich lekárske ošetrovanie alebo úmrtie aspoň jednej osoby.



Bezpečnostné incidenty

Hlásenie závažného kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti (jiskb.nbu.gov.sk) pričom je potrebné dodržať zákonom stanovenú časovú následnosť:

- **do 24 hodín** od jeho zistenia sa hlási včasné varovanie, v ktorom sa uvádza najmä, či závažný kybernetický bezpečnostný incident mohol byť spôsobený protiprávnym konaním, alebo či môže mať cezhraničný vplyv,
- **do 72 hodín** od jeho zistenia sa hlási oznámenie o závažnom kybernetickom bezpečnostnom incidente, v ktorom sa aktualizujú a dopĺňajú informácie z včasného varovania, najmä sa uvádza prvotné posúdenie kybernetického bezpečnostného incidentu, jeho závažnosti a následkov,
- **1 mesiac** po nahlásení oznámenia sa hlási záverečná správa, ktorá obsahuje najmä podrobný opis závažného kybernetického bezpečnostného incidentu vrátane jeho závažnosti a následkov, druh kybernetickej hrozby alebo hlavnú príčinu, ktorá pravdepodobne kybernetický bezpečnostný incident spôsobila, zavedené a prebiehajúce opatrenia a cezhraničný vplyv, ak existuje. Ak v čase predkladania záverečnej správy závažný kybernetický bezpečnostný incident ešte prebieha, hlásia sa ďalšie aktualizované alebo iné vyžiadané informácie a aktualizovaná záverečná správa do 30 dní odo dňa, keď sa závažný kybernetický bezpečnostný incident vyriešil.



Ďakujem za pozornosť

V prípade záujmu navštívte našu stránku www.somi.sk alebo FB <https://www.facebook.com/somi.sk>
E-mailový kontakt: daniel.schikor@somisk.sk