Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Zmeny vo vyhláške o audite kybernetickej bezpečnosti: prehľad a praktické implikácie

Návrh novely vyhlášky č. 493/2022 Z. z. o audite kybernetickej bezpečnosti predstavuje reformu doterajšieho prístupu k auditu kybernetickej bezpečnosti v Slovenskej republike. Reaguje na požiadavky z trhu, opravuje limity pôvodnej právnej úpravy a prináša systematické prepracovanie rámca tak, aby zodpovedal reálnym potrebám praxe, rastúcej komplexnosti prostredia a požiadavkám na efektívne riadenie kybernetických rizík.

Významnou črtou tejto reformy je jej vznik na základe širokej odbornej diskusie. KCCKB spolu so skupinou skúsených audítorov kybernetickej bezpečnosti zohrali aktívnu úlohu pri identifikácii nedostatkov pôvodného znenia a pri formulovaní konkrétnych riešení. Výsledkom je návrh, ktorý predstavuje nielen legislatívnu úpravu, ale aj kvalitatívne nový, prakticky aplikovateľný model auditu.

Novela prináša zásadné sprehľadnenie požiadaviek, výrazné spresnenie metodiky a odstránenie viacerých interpretačných nejasností, ktoré v minulosti komplikovali aplikačnú prax. Zavádzané zmeny posilňujú dôraz na reálny výkon bezpečnostných opatrení, zvyšujú transparentnosť a predvídateľnosť procesov a umožňujú efektívnejšie plánovanie a vykonávanie auditov. Pri príprave novely sa dbalo na lepšie prepojenie Slovenskej a medzinárodnej audítorskej praxe a praxe EU.

V tomto kontexte ide o významné zlepšenie smerom k modernejšiemu, konzistentnejšiemu a funkčnejšiemu systému auditu kybernetickej bezpečnosti.

Predkladaný dokument poskytuje prehľad hlavných materiálnych zmien, ktoré návrh novely zavádza, a poukazuje na ich praktický význam pre regulované subjekty aj audítorskú prax.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Prehľad hlavných materiálnych zmien, ktoré prináša návrh novely vyhlášky č. 493/2022 Z. z. o audite kybernetickej bezpečnosti oproti aktuálne platnému a účinnému zneniu

Návrh novely predmetnej vyhlášky nepredstavuje len technické úpravy súčasného znenia vyhlášky, ale výrazne mení celý režim auditu kybernetickej bezpečnosti: dopĺňa samohodnotenie, rotáciu audítorov, výslovné pokrytie operačných technológií, nové lehoty a následný sledovanie nápravných opatrení pri kritických základných službách, ako aj úplne nové pravidlá pre vstupné údaje a určovanie rozsahu auditu.

1. Zavádza sa samohodnotenie ako nový režim popri audite

Vyhláška už nebude pracovať len s auditom vykonávaným certifikovaným audítorom, ale výslovne aj so samohodnotením, ktoré vykonáva manažér kybernetickej bezpečnosti. Zároveň sa dopĺňa základný rámec zodpovednosti za správnosť a úplnosť výstupu zo samohodnotenia.

2. Zavádza sa rotácia audítora

Ten istý certifikovaný audítor bude môcť vykonať audit u toho istého prevádzkovateľa základnej služby najviac dvakrát po sebe; opätovne sa bude môcť vrátiť až po dvoch auditoch vykonaných inými audítormi.

3. Rozširuje sa záber vyhlášky aj na operačné technológie (OT)

Doterajší dôraz na siete a informačné systémy sa na viacerých miestach rozširuje aj na operačné technológie. Táto zmena sa premieta do predmetu posudzovania, správy o výsledkoch auditu, správy o zistených nedostatkoch aj do kontrolného záznamu.

4. Mení sa periodicita a režim vykonávania auditu a samohodnotenia

Aktuálne sa audit vykonáva každé dva roky a pri významnej zmene najneskôr do dvoch mesiacov od jej vplyvu. Po novom sa audit bude vykonávať najneskôr do konca tretieho kalendárneho roka po poslednom audite, resp. do konca piateho kalendárneho roka, ak nejde o prevádzkovateľa kritickej základnej služby. Pri významnej zmene sa lehota predlžuje na šesť mesiacov. Zároveň sa zavádza samohodnotenie každé dva roky s tým, že v čase vykonania auditu sa samohodnotenie nevykonáva.

5. Zavádza sa povinný výstup zo samohodnotenia a pravidlá jeho predkladania

Správa o vykonaní samohodnotenia má mať minimálny obsah a má sa predkladať cez jednotný informačný systém kybernetickej bezpečnosti, najneskôr do konca kalendárneho roka, v ktorom sa samohodnotenie vykonáva.

6. Zavádza sa maximálna dĺžka výkonu auditu

Po novom sa výslovne ustanovuje, že audit je ukončený odovzdaním záverečnej správy a maximálna doba výkonu auditu je 12 po sebe nasledujúcich mesiacov.

7. Sprísňuje sa následné sledovanie nápravných opatrení pri kritických základných službách

Ak zistené nedostatky nebudú odstránené ešte pred finalizáciou záverečnej správy, pri prevádzkovateľovi kritickej základnej služby sa zavádza povinnosť zaslať úradu informáciu o plnení nápravných opatrení. Táto povinnosť má byť naviazaná na kontrolu stavu plnenia po 16 mesiacoch a informácia sa má zaslať najneskôr do 18 mesiacov od predloženia záverečnej správy. Táto konkrétna zmena má podľa návrhu nadobudnúť účinnosť až 1. januára 2031.

8. Mení sa režim pri čiastočnom súlade a čiastočne aj obsah záverečnej správy

Správa o zistených nedostatkoch už nebude viazaná len na nesúlad, ale aj na prípady čiastočného súladu, čo môže v praxi znamenať viac prípadov formálneho spracovania nedostatkov a termínov nápravy.

9. Úplne sa prepracúva príloha č. 1 – minimálne náležitosti žiadosti o vykonanie auditu

Rozsah vstupných údajov sa výrazne rozširuje, najmä o údaje o kritickosti subjektu, osobe, ktorej sa odovzdáva záverečná správa, zamestnancoch a ďalších osobách zapojených do bezpečnostných opatrení, tretích stranách, identických činnostiach, lokalitách, IKT a OT systémoch, analýze rizík, úrovni vykonávania opatrení, počte zákazníkov – kritických subjektov, certifikácii a počte používateľov. V praxi to znamená podstatne širší a detailnejší vstup pre plánovanie auditu.

10. Úplne sa prepracúva príloha č. 2 – metodika určovania rozsahu trvania auditu a časového intervalu

Metodika sa výrazne spresňuje a komplikuje. Zavádza sa detailnejšie určovanie rozsahu auditu podľa efektívneho počtu osôb, rozlíšenie auditu na mieste a na diaľku, pojem audítorského tímu, pravidlá pre identické činnosti a výber vzorky lokalít, ako aj nové faktory viazané na kritickosť subjektu, komplexnosť IKT/OT prostredia a závislosť od tretích strán. Ide o zásadné prepracovanie spôsobu, ako sa bude určovať rozsah auditu.
Certifikačný orgán audítorov pripraví vysvetlenie, preškolí audítorov a vyrobí spoločnú kalkulačku pre svojich audítorov.

11. Zavádzajú sa nové prechodné pravidlá a účinnosť

Audity začaté a neukončené do 31. mája 2026 sa dokončia podľa doterajšieho znenia. Audity začaté od 1. júna 2026 do 31. decembra 2026 sa už môžu vykonať podľa nového znenia. Novela má byť účinná od 1. júna 2026, s výnimkou jednej povinnosti odloženej na 1. január 2031.