ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2022

Vyhlásené: 23. 12. 2022 Časová verzia predpisu účinná od: 1. 1.2023

493

VYHLÁŠKA
Národného bezpečnostného úradu
z 19. decembra 2022
o audite kybernetickej bezpečnosti

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 32 ods. 1 písm. f) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. 287/2021 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

(1) Auditom kybernetickej bezpečnosti (ďalej len „audit“) sa overuje plnenie povinností podľa zákona a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov[1]) prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby, s cieľom 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.

(2) Audit vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa § 29 ods. 3 zákona (ďalej len „audítor“).

(3) Na vykonanie auditu audítor spĺňa podmienky znalostného štandardu overené skúškou doloženou podľa odporúčaní medzinárodne akceptovaných technických noriem[2]) alebo iných, týmto štandardom vecne obdobných a všeobecne uznávaných postupov.

(4) Audítor zodpovedá za správnosť, rozsah a odbornosť pri výkone auditu a spracovaní záverečnej správy o výsledkoch auditu.

(5) Audítor vykonáva audit odborne, objektívne, nestranne, na základe dôkazov podľa odporúčaní technických noriem[2]) alebo iných vecne obdobných a všeobecne uznávaných postupov.

(6) Časový rozsah trvania auditu sa určuje tak, že je dostatočný na posúdenie plnenia povinností podľa zákona a účinnosti prijatých bezpečnostných opatrení. Ak nie je možné v rámci rozsahu trvania auditu hodnotiť každé jednotlivé opatrenie na veľkej populácii prvkov, hodnotí sa ich stav formou vzorkovania, pričom rozsah vzoriek sa určuje s ohľadom na vykonanú klasifikáciu informácií, kategorizáciu sietí a informačných systémov, vykonanú analýzu rizík kybernetickej bezpečnosti a na vypovedaciu schopnosť auditu podľa odseku 1.

(7) Pri výkone auditu sa

a) prijíma žiadosť o vykonanie auditu v rozsahu minimálnych náležitostí uvedených v prílohe č. 1 a posudzuje kompletnosť údajov v žiadosti; môžu vyžadovať ďalšie informácie potrebné na prípravu a výkon auditu,

b) pripravuje harmonogram výkonu auditu, ktorý obsahuje najmä

1. identifikáciu organizačných útvarov, procesov, auditovaných sietí a informačných systémov a fyzických lokalít prevádzkovateľa základnej služby s uvedením času a

2. meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytuje audítorovi počas auditu požadovanú súčinnosť,

c) určuje rozsah auditu spôsobom podľa prílohy č. 2,

d) určujú metódy auditu,

e) pripravujú podklady a pracovné dokumenty potrebné na zaznamenávanie výkonu auditu, ktoré sú prílohou záverečnej správy o výsledkoch auditu, a to najmä

1. zápisy zo stretnutí,

2. evidencia predložených dôkazov,

3. evidencia účastníkov auditu,

4. evidencia navštívených lokalít,

f) preskúmava bezpečnostná dokumentácia a vyhodnocujú bezpečnostné opatrenia a vypracúva kontrolný záznam auditovaných bezpečnostných opatrení (ďalej len „kontrolný záznam“) podľa prílohy č. 3,

g) zbierajú, sústreďujú a vyhodnocujú dôkazy o zisteniach auditu,

h) oboznamuje zodpovedný zamestnanec prevádzkovateľa základnej služby so zistenými nedostatkami a zostavuje súbor odporúčaných opatrení na ich odstránenie,

i) vypracúva záverečná správu o výsledkoch auditu podľa vzoru uvedeného v štandarde na výkon auditu kybernetickej bezpečnosti zverejnenom na webovom sídle úradu.

§ 2

(1) V záverečnej správe o výsledkoch auditu sa hodnotí výsledok auditu a uvedú sa dôkazy, ktoré sa viažu k jednotlivým zisteniam auditu.

(2) Záverečná správa o výsledkoch auditu obsahuje najmä

a) meno, priezvisko, číslo certifikátu audítora, dátum vyhotovenia správy, certifikačnú značku audítora a jeho vlastnoručný podpis alebo kvalifikovaný elektronický podpis,

b) vymedzenie rozsahu vykonaného auditu,

c) cieľ auditu,

d) metódy auditu,

e) zhrnutie zistení výsledkov auditu a konštatovanie súladu, čiastočného súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,

f) odporúčané nápravné opatrenia pri zistení nedostatkov,

g) dokumenty, najmä

1. kópiu certifikátu audítora,

2. kópiu žiadosti o vykonanie auditu,

3. výpočet rozsahu trvania auditu a zdôvodnenie jeho skrátenia alebo predĺženia,
4. kontrolný záznam,
5. vyjadrenie prevádzkovateľa základnej služby k zisteniam auditu,
6. harmonogram auditu,
7. zoznam evidovaných dôkazov,
8. uvedenie a zdôvodnenie zmien a rozdielov uskutočnenia auditu oproti plánovanému harmonogramu,
9. zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení informačných systémov súvisiacich so základnou službou, vyslovenie súladu, čiastočného súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov a konkrétne uvedenie nedostatkov,

h) informáciu o vykonaných nápravných opatreniach, ak sú na základe predchádzajúceho auditu tieto nápravné opatrenia prijaté.

(3) Prílohou záverečnej správy o výsledkoch auditu je pri zistení nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov aj správa o zistených nedostatkoch, pri ktorých sa uvádza termín vykonania nápravných opatrení na zabezpečenie súladu s požiadavkami na bezpečnosť sietí a informačných systémov. Nápravné opatrenia sa prijímajú tak, že je možné ich zahrnúť do záverečnej správy o výsledkoch auditu.

(4) Ak sú niektoré zistené nedostatky odstránené do termínu vyjadrenia prevádzkovateľa základnej služby k zisteniam auditu pred spracovaním záverečnej správy o výsledkoch auditu, je možné v tejto záverečnej správe o výsledkoch auditu konštatovať pre plnenie daných požiadaviek súlad s požiadavkami na bezpečnosť sietí a informačných systémov.

§ 3

(1) Audit kybernetickej bezpečnosti vykonaný podľa doterajších predpisov sa považuje za audit kybernetickej bezpečnosti podľa tejto vyhlášky.

(2) Audit kybernetickej bezpečnosti začatý a neukončený do 31. decembra 2022 sa dokončí podľa tejto vyhlášky.

§ 4

Zrušuje sa vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

§ 5

Táto vyhláška nadobúda účinnosť 1. januára 2023.

Roman Konečný v. r.

Príloha č. 1
k vyhláške č. 493/2022 Z. z.

MINIMÁLNE NÁLEŽITOSTI ŽIADOSTI O VYKONANIE AUDITU KYBERNETICKEJ BEZPEČNOSTI

1. Identifikácia prevádzkovateľa základnej služby.
2. Identifikácia základných služieb podporených auditovanými informačnými systémami a sieťami.
3. Počet zamestnancov prevádzkovateľa základnej služby.
4. Zoznam informačných systémov a ich klasifikácia s väzbou na základnú službu a pre každý z nich najmenej informácie o informačnom systéme a
   a) identifikácia organizačných útvarov prevádzkovateľa základnej služby a počet zamestnancov prevádzkujúcich informačné systémy a siete, pri externom zabezpečovaní činností správy informačných systémov rozsah využívaných služieb v človekodňoch; pri doložení výsledkov auditu na externe zabezpečované činnosti sa externí pracovníci nezapočítavajú,
   b) väzba siete a informačného systému na prevádzkovanú základnú službu; ktorá základná služba je závislá od informačného systému, aký je vplyv výpadku informačného systému na základnú službu,
   c) počet užívateľov základnej služby, teritoriálne rozloženie a dôsledky pri výpadku základnej služby na jej užívateľov,
   d) systém správy; interné a externé zdroje, identifikácia kľúčových dodávateľov a zmlúv a dohôd o úrovni poskytovaných služieb,
   e) schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia vo vzťahu k externým sieťam,
   f) zoznam aktív a používaných technológií so závislosťami od iných informačných systémov a služieb dodávateľov s uvedením vlastníkov týchto aktív a identifikáciou klasifikačného stupňa podľa osobitného predpisu,[3])
   g) organizačné útvary a počty zamestnancov prevádzkujúcich informačné systémy a siete vrátane počtu dodávateľov; pri prítomnosti zamestnancov dodávateľa na pracovisku prevádzkovateľa počas auditu sa lokality dodávateľov nezapočítavajú,
   h) správa z posledného penetračného testovania informačného systému, použitá metodika a rozsah testovania a doloženie kvalifikácie zamestnancov vykonávajúcich penetračné testy, ak sú penetračné testy vykonané,
   i) záverečná správa z predošlého auditu.
5. Meno, priezvisko a kontaktné údaje zodpovedného zamestnanca prevádzkovateľa základnej služby, ktorý poskytne audítorovi počas výkonu auditu súčinnosť a sprievod.
6. Evidencia záznamov o kybernetických bezpečnostných incidentoch s vplyvom na poskytovanie základných služieb od doby vykonania posledného auditu alebo za posledné dva roky pri prvom audite.
7. Rozhodnutie o uložení pokuty na úseku kybernetickej bezpečnosti, ak je uložená, a ďalšie prípady porušenia povinností podľa zákona, ak sú porušenia zistené.
8. Bezpečnostná dokumentácia podľa § 20 ods. 5 zákona alebo osobitného predpisu.[4])
9. Číslo platného potvrdenia o priemyselnej bezpečnosti, ak je vydané.

Príloha č. 2
k vyhláške č. 493/2022 Z. z.

ROZSAH TRVANIA A ČASOVÝ INTERVAL AUDITU KYBERNETICKEJ BEZPEČNOSTI

A URČENIE ROZSAHU TRVANIA AUDITU

Pred začiatkom auditu sa určí dĺžka jeho trvania s cieľom dostatočne posúdiť predmet auditu. Pri výpočte trvania dĺžky auditu sa zohľadňujú informácie zo žiadosti o vykonanie auditu kybernetickej bezpečnosti a dodatočne vyžiadané informácie, najmä:

a) počet interných zamestnancov a zamestnancov externých dodávateľov zúčastňujúcich sa na prevádzke sietí a informačných systémov,

b) kategorizácia sietí a informačných systémov,

c) systémová architektúra prostredia (centralizovaný alebo decentralizovaný spôsob prevádzkovania informačných systémov),

d) množstvo, rozsah a komplexnosť dokumentácie súvisiacej s prevádzkou informačného systému a zabezpečovaním bezpečnostných opatrení vrátane výsledkov predchádzajúcich auditov a vykonaných analýz rizík,

e) počet tretích strán zúčastňujúcich sa na prevádzke informačných systémov,

f) počet lokalít v ktorých nachádzajú siete a informačné systémy podporujúce prevádzku základnej služby.

Výpočet dní trvania auditu sa vykonáva celkovo pre prostredie prevádzkovateľa základnej služby v tomto poradí úkonov:

a) výpočet základného počtu dní auditu,

b) zohľadnenie kategórií informačných systémov,

c) uplatnenie ostatných faktorov ovplyvňujúcich dĺžku trvania auditu.

Výpočet základnej dĺžky auditu sa vykonáva na základe počtu interných zamestnancov a externých zamestnancov, zúčastňujúcich sa súhrnne na prevádzke informačných systémov podľa tejto tabuľky:

Celkový počet zamestnancov zúčastňujúcich sa na prevádzke systému a zabezpečovaní bezpečnostných opatrení	**Základný rozsah auditu v človeko-dňoch**
1~10	5
11~20	6
21~30	7
31~40	8
41~50	9
51~60	10
>60	+1 deň za každých ďalších 10 zamestnancov

Pri prítomnosti alebo účasti zamestnancov iných lokalít podieľajúcich sa na prevádzke rovnakého informačného systému formou vzdialeného pripojenia nie je potrebné zvyšovať počet dní auditu.

Ak za niekoľko informačných systémov a zabezpečenie bezpečnostných opatrení pri rozdielnych základných službách sú zodpovedné tie isté osoby, nezvyšuje sa počet dní auditu, ak sú viaceré informačné systémy auditované súčasne.

Faktory vyplývajúce z kategorizácie informačných systémov v prostredí prevádzkovateľa, ak sa v prostredí prevádzkovateľa nachádza

a) najmenej informačný systém kategórie III, môže sa zvýšiť základný rozsah auditu o 50 %,

b) len informačný systém kategórie I, môže sa znížiť základný rozsah auditu o 25 %.

Ostatné faktory upravujúce rozsah auditu

Trvanie auditu sa od výpočtu dní podľa predchádzajúceho bodu znižuje

a) o 10 %, ak je k dispozícii záverečná správa o výsledkoch auditu z predchádzajúceho auditu vykonaného podľa tejto vyhlášky a nevyskytnú sa žiadne zmeny v počtoch zamestnancov spravujúcich systémy, v aktívach, použitých technológiách a základných službách podporovaných informačnými systémami v záverečnej správe o výsledkoch auditu,

b) o 10 %, ak je auditovaný informačný systém certifikovaný v súlade s požiadavkami na certifikáciu kybernetickej bezpečnosti informačných technológií,[5])

c) na iný rozsah podľa rozhodnutia; rozhodnutie sa musí zdôvodniť.

Trvanie auditu sa od výpočtu dní podľa predchádzajúceho bodu zvyšuje,

a) ak sú informačné systémy zaradené do kategórie III,

b) o 10 %, ak sa vyskytne závažný kybernetický bezpečnostný incident od vykonania posledného auditu alebo je uložená pokuta za porušenie povinností podľa zákona,

c) na iný rozsah podľa rozhodnutia po predošlej konzultácii s prevádzkovateľom základnej služby; rozhodnutie sa musí zdôvodniť.

Do časového rozsahu trvania auditu sa započítava čas audítora pri posúdení žiadosti o vykonanie auditu kybernetickej bezpečnosti, doručenie vyžiadaných dodatočných podkladov, predbežná analýza plnenia povinností, posúdenie povinnej dokumentácie a spracovanie záverečnej správy o výsledkoch auditu, a to spolu najviac v rozsahu 1/3 celkového potrebného časového rozsahu trvania auditu.

B URČENIE ČASOVÉHO INTERVALU AUDITU

Audit sa vykonáva

a) každé dva roky, audit sa musí začať do dvoch rokov od vydania záverečnej správy o výsledkoch auditu a

b) pri každej významnej zmene, najneskôr do dvoch mesiacov, odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia.

Významným vplyvom sa rozumie najmä

a) vplyv na prijatú klasifikáciu informácií a kategorizáciu sietí a informačných systémov,

b) zmena dopadových kritérií základnej služby,

c) zmena alebo výmena informačného systému a prevádzkových parametrov základnej služby,

d) zavedenie novej siete, nového informačného systému, od ktorých je závislá základná služba,

e) zavedenie novej technológie, od ktorej je závislá základná služba, alebo

f) zmena systémovej architektúry alebo sieťovej topológie.

Príloha č. 3
k vyhláške č. 493/2022 Z. z.

KONTROLNÝ ZÁZNAM AUDITOVANÝCH BEZPEČNOSTNÝCH OPATRENÍ

Kontrolný záznam obsahuje súbor požiadaviek na bezpečnosť sietí a informačných systémov podľa zákona a jeho vykonávacích predpisov a osobitných predpisov. Pri spoločných požiadavkách na prevádzkovateľa základnej služby sa vyplní spoločný kontrolný záznam za všetky informačné systémy relevantné pre audit. Bezpečnostné opatrenia, ktoré sú odlišné pre jednotlivé auditované informačné systémy, sa vyplnia samostatne pre každý informačný systém alebo sieť.

V kontrolnom zázname sa uvedie

a) súlad, čiastočný súlad alebo nesúlad s požiadavkami na bezpečnosť sietí a informačných systémov na prijaté bezpečnostné opatrenia,

b) zistenia auditu pre jednotlivé požiadavky na bezpečnosť sietí a informačných systémov,

c) získané dôkazy podporujúce uvedené zistenia a

d) referencia na použitú metódu auditu, napríklad

1. pozorovanie činností a stavu bezpečnostných opatrení,
2. analýza predložených záznamov,
3. analýza predložených postupov, predpisov a dokumentov,
4. rozhovory a dotazníky.

Súčasťou kontrolného záznamu je aj overenie úplnosti požadovanej bezpečnostnej dokumentácie a overenie klasifikácie informácií a kategorizácie sietí a informačných systémov.

Ak sú auditované informačné systémy, pre ktoré platia dodatočné požiadavky nad rámec bezpečnostných opatrení uvedených v zákone alebo v osobitnom predpise,[4]) uvedie sa v kontrolnom zázname spôsob plnenia podľa požiadaviek, ktoré sa aplikujú na prevádzkovateľa základnej služby.

So zistenými nedostatkami je priebežne oboznámený zodpovedný pracovník prevádzkovateľa základnej služby počas auditu a zároveň dokumentuje odporúčané opatrenia na odstránenie nedostatkov.

Kontrolný záznam sa uchováva s odbornou starostlivosťou a s ohľadom na citlivosť informácií dva roky od skončenia auditu.

1) Napríklad § 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, § 14 zákona č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov, zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 2 ods. 9 zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. 132/2013 Z. z., zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

2) Napríklad STN EN ISO/IEC 17024 Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb (ISO/IEC 17024: 2012).

3) Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

4) Napríklad zákon č. 95/2019 Z. z., vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

5) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7. 6. 2019).

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Úrad vlády Slovenskej republiky, Námestie slobody 1, 813 70 Bratislava,
tel.: 02 888 91 131, e-mail: helpdesk@slov-lex.sk.