

ROZSAH TRVANIA A ČASOVÝ INTERVAL AUDITU KYBERNETICKEJ BEZPEČNOSTI

A: URČENIE ROZSAHU TRVANIA AUDITU

Audítor zodpovedá za určenie dĺžky trvania auditu na dostatočné posúdenie predmetu auditu. Pri výpočte trvania dĺžky auditu audítor zohľadňuje informácie zo žiadosti o vykonanie auditu kybernetickej bezpečnosti a dodatočne vyžiadaných informácií, predovšetkým z

- počtu používateľov sietí a informačného systému,
- počtu zamestnancov zúčastňujúcich sa na prevádzke sietí a informačného systému,
- kategorizácie sietí a informačných systémov,
- rozsahu účasti tretích strán na prevádzke informačného systému a zabezpečovaní bezpečnostných opatrení,
- množstva, rozsahu a komplexnosti dokumentácie súvisiacej s prevádzkou informačného systému a zabezpečovaním bezpečnostných opatrení vrátane výsledkov predchádzajúcich auditov a vykonaných analýz rizík.

Výpočet dní trvania auditu pre každý informačný systém a lokalitu prevádzkovateľa samostatne.

Počet zamestnancov zúčastňujúcich sa na prevádzke systému a zabezpečovaní bezpečnostných opatrení	Audit v človeko-dňoch
1~10	5
11~20	6
21~30	7
31~50	8
51~70	9
71~90	10
>90	+1 deň za každých ďalších 20 zamestnancov

Za každý ďalší informačný systém sa považuje súbor súvisiacich a navzájom závislých aktív (hardvér, softvér, služby dodávateľov), ktoré podporujú ďalšiu základnú službu, alebo je prevádzka informačných systémov a sietí vykonávaná inými zamestnancami, alebo organizačným útvarom, alebo je na inej lokalite. Pri prítomnosti alebo účasti zamestnancov z iných lokalít (dodávateľ pri externe zabezpečovaných činnostiach) 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 sú zodpovedné tie isté osoby, nezvyšuje sa počet dní auditu, ak budú viaceré informačné systémy auditované súčasne.

Faktory znižujúce rozsah auditu (najviac na 1/3 uvedeného rozsahu pri kombinácii faktorov).

Trvanie auditu sa od výpočtu dní podľa predchádzajúcej tabuľky znižuje

- a) na 1/3, ak má audítor k priamej dispozícii záverečnú správu o výsledkoch auditu z predchádzajúceho auditu kybernetickej bezpečnosti vykonaného v súlade s touto vyhláškou a nevyskytli sa žiadne zmeny v počtoch zamestnancov spravujúcich systémy, v aktívach, použitých technológiách a základných službách podporovaných informačnými systémami v záverečnej správe o výsledkoch auditu. Audítor sa venuje predovšetkým prevereniu skutočnosti, či uvedené zmeny nenastali, a zároveň oblastiam označeným v kontrolnom zázname, ktoré sú povinné pre každý audit,
- b) na 1/2, ak sú všetky informačné systémy zaradené do kategórie citlivosti I,
- c) na 1/2, ak je prevádzkovateľ základnej služby držiteľom certifikátu podľa technickej normy⁶⁾ a certifikovaná oblasť zahŕňa auditované informačné systémy,
- d) na 1/2, ak je auditovaný informačný systém certifikovaný v súlade s požiadavkami na certifikáciu kybernetickej bezpečnosti⁷⁾ informačných technológií,
- e) na iný rozsah podľa rozhodnutia audítora; audítor musí svoje rozhodnutie riadne zdôvodniť.

Faktory zvyšujúce rozsah auditu

Trvanie auditu sa od výpočtu dní podľa predchádzajúcej tabuľky zvyšuje

- a) na dvojnásobok, ak sú informačné systémy zaradené do kategórie citlivosti III,
- b) na dvojnásobok, ak sa vyskytol závažný kybernetický bezpečnostný incident od doby vykonania posledného auditu alebo je uložená pokuta za porušenie povinností podľa zákona,
- c) na iný rozsah podľa rozhodnutia audítora po predošlej konzultácii s prevádzkovateľom základnej služby; audítor musí svoje rozhodnutie riadne 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

⁶⁾ Napríklad STN EN ISO/IEC 27001 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky (ISO/IEC 27001: 2013 vrátane Cor. 1: 2014 a Cor. 2: 2015).

⁷⁾ 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).

- a) každé dva roky 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 alebo nového informačného systému, od ktorých je závislá základná služba, alebo
- e) zavedenie novej technológie, od ktorej je závislá základná služba.