

**Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti,
prevádzkovateľ základnej služby a jeho povinnosti**

Vybrané oblasti v zákone a súvisiacej legislatíve

- Zákon o KB a súvisiaca legislatíva
- Prevádzkovateľ základnej služby – určenie a nahlasovacia povinnosť
- Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby - určenie prevádzkovateľa základnej služby (sektorové a dopadové kritériá základnej služby)
- Verejná správa - sektorové a dopadové pravidlá vo Vyhláške 164/2018
- Povinnosti prevádzkovateľa základnej služby
- Vyhláška č. 362/2019 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Dodávateľ, ktorý prevádzkuje podporu základnej služby (zmluva)
- Prevádzkovateľ digitálnej služby v kontexte na prevádzkovateľa základnej služby
- Kybernetický bezpečnostný incident (KBI)
- Vyhláška č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných KBI a podrobnosti hlásenia KBI

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti - súvisiaca legislatíva

- Smernica EP a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a IS v Únii (Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti je transponovaním tejto smernice do legislatívy SR)
- Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby - určenie prevádzkovateľa základnej služby (sektorové a dopadové kritériá základnej služby)
- Vyhláška č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných KBI a podrobnosti hlásenia KBI
- Vyhláška č. 166/2018 Z. z., pre riešenie bezpečnostných incidentov
- Vyhláška č. 362/2019 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Základná služba, prevádzkovateľ, zaradenie do zoznamu PZS - Zákon č. 69/2018 - § 17

- Ohlasovacia povinnosť – ak prevádzkovateľ zistí, že došlo k prekočeniu identifikačných kritérií, je povinný to do 30 dní oznámiť úradu
- Úrad zaradí službu a jej prevádzkovateľa do registra PZS:
 - Na základe oznámenia prevádzkovateľa
 - Na základe podnetu ústredného orgánu (UPVII pre VS)
 - Z vlastnej iniciatívy
- Oznámenie musí obsahovať:
 - Názov, sídlo, kontaktné údaje, zoznam potenciálnych služieb
 - Cezhraničný presah, percentuálny podiel služby na trhu, geografické rozloženie
 - Informáciu o alternatívnych možnostiach zachovania kontinuity v prípade incidentu

Určenie prevádzkovateľa základnej služby - Zákon č. 69/2018 - § 18 a Príloha č. 1

- Identifikačné kritériá prevádzkovej služby sú dopadové kritériá a špecifické sektorové kritériá
- Dopadové kritériá sú učené všeobecne záväzným predpisom a zohľadňujú najmä:
 - Počet používateľov využívajúcich základnú službu (ZS)
 - Závislosť ostatných sektorov podľa prílohy č. 1 od ZS
 - Vplyv, ktorý by KBI z hľadiska rozsahu a trvania mal na hospodárske a spoločenské činnosti a záujmy štátu alebo bezpečnosť štátu
 - Trhový podiel prevádzkovateľa základnej služby
 - Geografické rozloženie z hľadiska oblasti, ktorú by KBI mohol postihnúť
 - Význam PZS z hľadiska zachovania kontinuity poskytovania služby

Určenie prevádzkovateľa základnej služby - Vyhláška č. 164/2018

- Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby:

§ 2: Prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak spĺňa aspoň jedno dopadové kritérium a aspoň jedno sektorové kritérium, ak je uvedené v prílohe č. 1

Záver:

Prevádzkovateľa základnej služby teda určuje podmienka identifikačných kritérií. Ak spadá pod špecifické sektorové kritérium, a v rámci neho aj pod dopadové kritérium, potom je určený ako prevádzkovateľ základnej služby.

Určenie prevádzkovateľa základnej služby

- Verejná správa: Príloha č. 1 ZoKB

- Verejná správa (sektor), (podsektor nie je určený), orgán verejnej moci (prevádzkovateľ služby)

Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v sektore (podsektore):

- Bezpečnosti
- Informačných systémov verejnej správy
- Obrany
- Spravodajských služieb
- Utajovaných skutočností

Vyhláška č. 164/2018 – sektorové a dopadové kritériá - verejná správa (z prílohy č. 1)

VEREJNÁ SPRÁVA

Prevádzkovateľ služieb (príloha č. 1 k zákonu)	Špecifické sektorové kritériá (jednotlivo)	Dopadové kritériá (jednotlivo)
Orgán verejnej moci.	Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v jednom podsektore a) bezpečnosti, b) informačných systémov verejnej správy, c) obrany, d) spravodajské služby, alebo e) utajovaných skutočností vo vzťahu k fungovaniu príslušného ústredného orgánu podľa zákona.	<p>Dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť:</p> <p>Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 1 000 osôb.</p> <p>Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry.</p> <p>Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať:</p> <p>negatívny vplyv na fungovanie orgánu verejnej moci, vplyv na výkon činnosti orgánu verejnej moci pri zaistovaní prípravy na krízové situácie, vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti orgánu verejnej moci.</p> <p>Viac ako jedna zranená osoba vyžadujúca lekárske ošetrovanie.</p> <p>Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.</p>

Vyhláška č. 164/2018 - súvisiaca legislatíva

- Vyhláška č. 164/2018 - určenie prevádzkovateľa základnej služby (sektorové a dopadové kritériá)
 - Zákon č. 513/2009 Z. z. o dráhach
 - Zákon č. 657/2004 Z. z. o tepelnej energetike
 - Zákon č. 429/2002 Z. z. o burze cenných papierov
 - Zákon č. 324/2011 Z. z. o poštových službách
 - Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach
 - Zákon č. 67/2010 o Z. z. podmienkach uvedenia chemických látok
 - Zákon č. 364/2004 Z. z. o vodách
 - Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti
- Preberaný právne záväzný akt EÚ: Smernica EP a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a IS v Únii

Povinnosti prevádzkovateľa základnej služby - § 19

- Prijat' a dodržiavať všetky bezpečnostné opatrenia najmenej v rozsahu par. 20 a sektorové bezpečnostné opatrenia, ak sú prijaté – do 6 mesiacov odo dňa oznámenia o zaradení do registra PZS (!).
- Pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a IS pre PZS uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohoto zákona počas celej doby platnosti zmluvy.
- Dňom zaradenia do registra PZS o tejto skutočnosti informovať podnik na poskytovanie komunikačných služieb alebo sietí, ku ktorému je sieť alebo IS základnej služby pripojená. Na základe informovania s podnikom uzavrie zmluvu podľa predchádzajúceho odstavca.
- Informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom KBI za predpokladu, že by sa plnenie zmluvy stalo nemožným.
- Ak poskytuje základnú službu aj v inom členskom štáte EÚ, o kritériách rozhodne NBÚ v súčinnosti s orgánom daného členského štátu.

Povinnosti prevádzkovateľa základnej služby - § 19

- PZS je ďalej povinný
 - Riešiť kybernetický bezpečnostný incident,
 - Bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
 - Spolupracovať s NBÚ a ústredným orgánom pri riešení nahláseného KBI (poskytnutie potrebnej súčinnosti),
 - V čase KBI zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
 - Oznámiť orgánu činnému v trestnom konaní trestný čin, ktorého sa KBI týka, ak sa o ňom hodnoverne dozvie,
- Je povinný hlásiť zmeny v údajoch podľa § 17 (povinné informácie o sebe),
- PZS nezodpovedá za škodu, ktorá vznikne inému subjektu obmedzením kontinuity základnej služby pri riešení KBI (zákonným spôsobom a postupom).

Bezpečnostné opatrenia - § 20

- BO sú úlohy, procesy role a technológie v organizačnej, personálnej a technologickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a IS. BO realizované v závislosti od klasifikácie informácií (!) sa prijímajú s cieľom predchádzať KBI a minimalizovať vplyv KBI na na kontinuitu prevádzkovania ZS.
- Klasifikácia informácií a kategorizácia sietí a IS sa vykonáva na základe významnosti, funkcie a účelu informácií a IS s ohľadom na dostupnosť, dôvernosť, integritu, kvalitu služby a kontrolnú činnosť.

Bezpečnostné opatrenia - § 20

○ BO sa prijímajú pre oblasť

- Organizácie IB
- Riadenia aktív, hrozieb a rizík
- Personálnej bezpečnosti
- Riadenia dodávateľských služieb, akvizície, vývoj a údržby IS
- Technických zraniteľností systémov a zariadení
- Riadenia bezpečnosti sietí a IS
- Riadenia prevádzky
- Riadenia prístupov
- Kryptografických opatrení
- Riešenia KBI
- Monitorovania, testovania bezpečnosti a bezpečnostných auditov
- Fyzickej bezpečnosti a bezpečnosti prostredia
- Riadenia kontinuity procesov

Bezpečnostné opatrenia - § 20

- BO musia zahŕňať najmenej
 - Detekciu kybernetických bezpečnostných incidentov,
 - Evidenciu kybernetických bezpečnostných incidentov,
 - Postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
 - Určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
 - Prepojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálnemu systému včasného varovania,
- BO sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu(!).

Vyhláška č. 362/2019 - obsah a štruktúra bezpečnostnej dokumentácie

Vyhláška 362/2018, § 2:

- **Obsah a štruktúra bezpečnostnej dokumentácie:**
 - **Schválená bezpečnostná stratégia KB a bezpečnostné politiky KB,**
 - **Klasifikácia informácií a kategorizácia sietí a IS,**
 - **Zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,**
 - **Vykonaná analýza rizík KB,**
 - **Záverečná správa o výsledkoch auditu KB (§ 29 ZoKB).**

Vyhláška č. 362/2019 - obsah a štruktúra bezpečnostnej dokumentácie

Vyhláška 362/2018, § 2:

- Bezpečnostná dokumentácia sa vypracúva na základe posúdenia poskytovanej základnej služby (!)
 - Súvisiaca infraštruktúra výrobných a produkčných technológií,
 - Súvisiaca infraštruktúra IKT,
 - Súvisiaca aplikačná architektúra,
 - Súvisiaca bezpečnostná architektúra a implementované bezpečnostné opatrenia,
 - Súvisiace organizačné usporiadanie, pracovné role, zodpovednosti a delenie právomocí,
 - Súvisiace zaužívané rámce riadenia operačných rizík,
 - Súvisiaca organizačná kultúra a spoločenská zodpovednosť.

Zmluva PZS s treťou stranou

- Vyhláška 362/2018, § 8, zmluva s treťou stranou obsahuje najmenej:
 - Obdobie trvania zmluvy,
 - Ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
 - Ustanovenie povinnosti chrániť všetky informácie poskytnuté tretej strane,
 - Ustanovenie povinnosti tretej strany prijímať a dodržiavať bezpečnostné opatrenia,
 - Konkrétnu špecifikáciu a rozsah bezpečnostných opatrení a vyjadrenie súhlasu s nimi,
 - Konkrétny rozsah činností tretej strany,
 - Zoznam pracovných rolí tretej strany, ktoré majú prístup k informáciám a údajom PZS,
 - Ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu PZS v tretej strane.

Zmluva PZS s treťou stranou

○ Vyhláška 362/2018, § 8, zmluva s treťou stranou obsahuje najmenej:

- Vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa (úplne alebo čiastočne) zabezpečujúceho plnenie pre PZS,
- Ustanovenia o povinnosti informovať PZS o KBI a o všetkých skutočnostiach majúcich vplyv na zabezpečenie KB,
- Ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných PZS na plnenie zákonných povinností (ZoKB),
- Ustanovenia o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
- Ustanovenia o sankčných mechanizmoch pri porušení zmluvy,
- Ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
- Záväzok tretej strany vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým mala počas trvania vzťahu tretia strana prístup,
- Záväzok tretej strany udeliť, poskytnúť alebo previesť licencie, práva alebo súhlasy nevyhnutné na zabezpečenie plnenia kontinuity ZS na PZS.

Povinnosti prevádzkovateľa digitálnej služby - § 22

- Prijat' a dodržiavať vhodné a primerané bezpečnostné opatrenia na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riadenia KBI. Povinnosť vyčleniť dostatočné personálne, materiálno-technické a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.
- Prevádzkovateľ digitálnej služby posudzuje najmä:
 - Bezpečnosť sietí a IS,
 - Spôsob zachovania kontinuity digitálnej služby v prípade KBI,
 - Súlad sietí a IS s bezpečnostnými štandardmi v oblasti KB,
 - Hlásiť každý KBI,
 - Riešiť hlásený KBI,
 - Spolupracovať s Úradom (CSIRT NBÚ alebo CSIRT ÚPVII) pri riešení KBI.
- Ak využíva na plnenie služby prevádzkovateľa základnej služby, je povinný s ním uzatvoriť zmluvu o plnení bezpečnostných opatrení a notifikačných povinností.
- O hlásenom KBI informuje tretiu stranu, ak by sa plnenie zmluvy stalo nemožným.

Kybernetický bezpečnostný incident (KBI)

- Zákon o KB

§ 24 Zákona

- PZS je povinný hlásiť každý závažný KBI ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie (odsek 2)
- Kategórie (I, II, III) v závislosti od:
 - počtu používateľov základnej služby zasiahnutých KBI,
 - dĺžky trvania KBI ,
 - geografického rozšírenia KBI,
 - stupňa narušenia fungovania základnej (alebo digitálnej) služby,
 - rozsahu vplyvu na hospodárske alebo spoločenské činnosti štátu.
- Ak PZS využíva služby prevádzkovateľa digitálnej služby (PDS), hlásenie podáva PDS.
- Hlásenie sa vykonáva prostredníctvom jednotného IS KB (JISKB).
- Ak účinky KBI do okamihu jeho hlásenia nepominuli, PZS je povinný odoslať neúplné hlásenie.

Kybernetický bezpečnostný incident (KBI)

- Vyhláška č. 165/2018

- Vyhláška č. 165/2018 - ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.
- 3 stupne závažných KBI (I, II, III – príloha č. 1 tejto vyhlášky) delenie podľa dopadu:
 - Podľa počtu používateľov základnej služby zasiahnutých KBI,
 - Podľa dĺžky trvania a geografického rozšírenia,
 - Podľa stupňa narušenia fungovania základnej služby.
- Hlásenie KBI obsahuje:
 - Kto KBI hlási (Identifikačné údaje a kontaktné údaje),
 - O závažnom KBI (časové údaje, detailný opis priebehu, rozsah škôd),
 - O zasiahnutej službe (popis zasiahnutých aktív, vplyv na službu),
 - O riešení (stav riešenia, vykonané opatrenia, popis následkov KBI).

Audit - § 29

- Podľa § 29 ods. 1 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.
- Podľa § 29 ods. 3 zákona č. 69/2018 Z. z. audit kybernetickej bezpečnosti vykonáva orgán posudzovania zhody podľa osobitného predpisu, ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti.
- Podľa § 32 písm. f) zákona č. 69/2018 Z. z. úrad ustanoví všeobecne záväzným právnym predpisom pravidlá a rozsah auditu kybernetickej bezpečnosti a podrobnosti o akreditácii orgánov posudzovania zhody a o obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 ods. 1 až 4.

Audit – Vyjadrenie NBÚ

- 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. Audit sa vykoná v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale. Audit vykonáva orgán posudzovania zhody, ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti.
- Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.
- Úrad môže kedykoľvek vykonať audit prevádzkovateľa základnej služby, alebo požiadať orgán posudzovania zhody o vykonanie auditu s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek podľa zákona o kybernetickej bezpečnosti. Náklady takto vykonaného auditu znáša úrad.

Audit – orgán posudzovania zhody

- Čl. 2 bod 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13. 8. 2008):

Orgánom posudzovania zhody je subjekt vykonávajúci činnosti posudzovania zhody vrátane kalibrácie, skúšania, osvedčovania a inšpekcie.

- Ďalšie podmienky určuje Vyhláška NBÚ, ktorou sa ustanovujú pravidlá a rozsah auditu kybernetickej bezpečnosti a podrobnosti o akreditácii orgánov posudzovania zhody.

Modlitba podľa Kyberzákona

NBÚ a UPPVII náš, ktorý si v kyberpriestore,
autentifikuj sa meno tvoje, príd' legislatíva tvoja,
bud' kyberbezpečnosť tvoja,
ako v cloude tak i na našich desktopoch.

Základnú službu kybernetickú definuj nám dnes,
a odpusť nám naše bezpečnostné incidenty,
ako i my odpúšťame našim audítorom,
a neuved' nás do sektorového kritéria ale zbav nás aj toho dopadového.

Enter.

Ďakujem za pozornosť.