S ktorým právnym predpisom má byť obec v súlade?

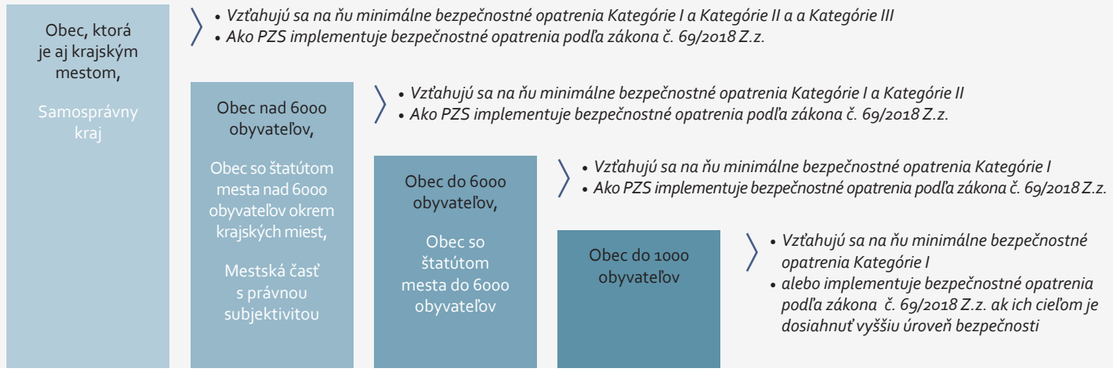
Vyhláška ÚPVII č. 179/2020 Z.z. v porovnaní s vyhláškou NBÚ č. 362/2018 Z.z. okrem požiadaviek na dokumentáciu nevyžaduje žiadne technické opatrenia navyše. V kontexte kybernetického priestoru sa v architektúre ITVS nevyskytujú zásadné špecifiká. Táto právna dvojkoľajnosť, žiaľ spôsobuje najmä v samospráve množstvo zbytočných nedorozumení.

Riešenie tohto problému poskytuje priamo aplikačná prax:

Audítor kybernetickej bezpečnosti posudzuje najprv zhodu prijatých všeobecných bezpečnostných opatrení až následne sektorové bezpečnostné opatrenia (ak sú prijaté). *(29 ods. 2 zákona č. 69/2028 Z.z. o kybernetickej bezpečnosti).*

Naviac - keďže obe spomínané vyhlášky vychádzali z rovnakých technických noriem a štandardov v oblasti kybernetickej bezpečnosti, Vyhláška ÚPVII č. 179/2020 Z.z a **vyhláška NBÚ č. 362/2018 Z.z. nie sú vo vzájomnom rozpore.**

Keďže každý PZS je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia, uprednostniť sa majú tie bezpečnostné opatrenie ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov. Tento princíp sa dá znázorniť nasledujúcim grafom:



Výkon úloh manažéra kybernetickej bezpečnosti

Kým operatívne činnosti v kybernetickej bezpečnosti, ktoré si vyžadujú príslušné odborné spôsobilosti, môžu byť vykonávané aj dodávateľským spôsobom, rozhodnutia o úlohách musí vždy vykonávať štatutárny zástupca, alebo ním poverený zamestnanec organizácie. Hovoríme teda o tzv. **zákonnej zodpovednosti** štatutárneho orgánu, ktorú nie je možné zmluvne preniesť na tretiu stranu, resp. outsourcing štatutárny orgán zodpovednosti nezbaví. Preto zmluva s dodávateľom nepredstavuje nahradenie zákonných zodpovednostných vzťahov.

Zodpovednosť starostu a primátora nie je možné preniesť na manažéra kybernetickej bezpečnosti

Služby kybernetickej bezpečnosti vrátane služby externého manažéra kybernetickej bezpečnosti je možné vykonávať aj dodávateľským spôsobom. Ide však o zmluvnú zodpovednosť, ktorá sa od zákonnej zodpovednosti líši.

V zmysle Obchodného zákonníka je štatutárny orgán spoločnosti povinný konať s odbornou starostlivosťou, v súlade so záujmami spoločnosti, pričom zodpovedá za porušenie týchto povinností. Obdobne to platí aj pre starostov obcí a primátorov miest, ktorým táto zodpovednosť vyplýva z osobitných právnych predpisov (napr. zákon o obecnom zriadení).

Povinnosť štatutárneho orgánu konať s odbornou starostlivosťou vyžaduje, aby si štatutár pri konkrétnom rozhodovaní zaobstaral a vyhodnotil všetky objektívne dostupné informácie, týkajúce sa predmetu konkrétneho rozhodovania. Následne sa má štatutár náležite rozhodnúť v kontexte týchto informácií a vlastnej profesionality ako predpokladu pre výkon funkcie.

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 nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-25-0
Verzia V.1

www.cybercompetence.sk

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

KYBERNETICKÁ BEZPEČNOSŤ V SAMOSPRÁVE MIEST A OBCÍ

Je obec prevádzkovateľom základných služieb?

V zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti je prevádzkovateľom základnej služby (PZS) orgán verejnej moci (OVM), alebo osoba, ktorá prevádzkuje aspoň jednu základnú službu, ktorá je zaradená v zozname základných služieb, ktoré závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 zákona.

Obce patria do sektoru verejná správa, podsektor informačné systémy verejnej správy, ako **správcovia alebo prevádzkovatelia informačných technológií verejnej správy** (definícia ITVS je v § 2 ods. 3 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe).

Prevádzkovateľom základnej služby je tiež subjekt, ktorý je súčasťou kritickej infraštruktúry. (Definícia prvku kritickej infraštruktúry je v § 2 písm. a) zákona č. 45/2011 Z.z. o kritickej infraštruktúre).

Sú splnené všetky kritériá §3 písm. I) Zákona 69/2018:		
1.	Služba je zaradená v zozname základných služieb	✓
2.	Služba závisí od sietí a informačných systémov	✓
3.	Je činnosťou aspoň v jednom sektore alebo podsektore	✓
4.	Môže byť prvkom kritickej infraštruktúry	~

Kritériá základnej služby

Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z. stanovuje, že prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak:

- spĺňa aspoň jedno dopadové kritérium a
- aspoň jedno špecifické sektorové kritérium.

Špecifické sektorové kritérium pre obce

Špecifickým sektorovým kritériom pre obce je prevádzka služby, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako **podstatná služba v podsektore informačné systémy verejnej správy.** Túto podmienku spĺňajú všetky samosprávne orgány Slovenskej republiky.

Dopadové kritériá pre obce

Podľa rovnakej vyhlášky musí zároveň platiť aspoň jedno dopadové kritérium. Dopadovými kritériami podľa vyhlášky sú:

- 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,**
- Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry,
- Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať:
  - *negatívny vplyv na fungovanie orgánu verejnej moci,*
  - *vplyv na výkon činnosti orgánu verejnej moci pri zaisťovaní prípravy na krízové situácie,*
  - *vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti organu verejnej moci,*
- Viac ako jedna zranená osoba vyžadujúca lekárske ošetrenie,
- 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.

Je obec prevádzkovateľom základnej služby? Každá, v ktorej žije viac ako 1 000 obyvateľov, jednoznačne áno. Vysvetlime si prečo.

Pokiaľ ide o dopadové kritériá, mnohé obce spĺňajú aj viaceré dopadové kritériá naraz. Avšak jedno dopadové kritérium majú spoločné všetky obce nad 1000 obyvateľov: ak ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov **postihuje viac ako 1 000 osôb.** Pretože v prípade kybernetického bezpečnostného incidentu sa tento dotýka všetkých obyvateľov bez rozdielu.

Na Slovensku je 1018 obcí, ktoré sú prevádzkovateľmi základných služieb na základe počtu obyvateľov od 1 000 do 20 000. Samozrejme, okrem toho sú prevádzkovateľmi základných služieb aj všetky mestá s vyšším počtom obyvateľov než 20 000.

Aké povinnosti sa vzťahujú na prevádzkovateľov základných služieb?

Podľa § 19 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti sú to nasledujúce povinnosti:	
(1)	prijať a dodržiavať: • všeobecné bezpečnostné opatrenia najmenej v rozsahu podľa § 20 a • sektorové bezpečnostné opatrenia, ak sú prijaté
(2)	ak sú činností vykonávané dodávateľským spôsobom, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona počas celej doby platnosti zmluvy
(3)	informovať podnik na poskytovanie elektronických komunikačných služieb ku ktorému základná služba pripojená
(4)	informovať v nevyhnutnom rozsahu tretie strany o hlásenom kybernetickom bezpečnostnom incidente
(6a)	riešiť kybernetický bezpečnostný incident,
(6b)	bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
(6c)	spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť
(6d)	v čase kybernetického bezpečnostného incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
(6e)	oznámiť orgánu činnému v trestnom konaní skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka
(7)	hlásiť zmeny v údajoch podľa § 17 ods. 5 prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

Bezpečnostné opatrenia

Opatrenia podľa § 20 (1) Zákona sú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Cieľom opatrení je predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na poskytované služby.

V zmysle § 19 (1) Prevádzkovateľ základnej služby je povinný prijať a dodržiavať:

- Všeobecné bezpečnostné opatrenia najmenej v rozsahu podľa §20
- Sektorové bezpečnostné opatrenia, ak sú prijaté

Všeobecné rozdelenie bezpečnostných opatrení

- ***Technické opatrenia*** - opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy,
- ***Organizačné opatrenia*** - opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie,
- ***Personálne opatrenia*** - podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov.

Efektívnu bezpečnosť je možné dosiahnuť zásadne len pomocou kombinácie technických a organizačných opatrení.

Akokoľvek rozsiahla bude vaša bezpečnostná dokumentácia, sama o sebe neposkytne ochranu pred kybernetickými hrozbami. Ani dokonale automatizované technické riešenie, ktoré vám odporučil dodávateľ, vám bez schémy počítačovej siete, bez nákresu aplikačnej architektúry, bez opisu konfigurácií systémov a bez platných bezpečnostných politík nezaručí pokrytie bezpečnostných cieľov vašej organizácie. Bezpečnosť je holistický proces.

Aké bezpečnostné opatrenia má obec implementovať?

Podľa prílohy č. 3 k vyhláške Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení sú prevádzkovatelia základných služieb povinní implementovať bezpečnostné opatrenia podľa kategórie prevádzkovaných systémov.

Kategórie systémov vs. kategórie opatrení

Podľa prílohy č. 2 vyhlášky č. 179/2020 Z.z. ÚPVII ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy sú skupiny minimálnych bezpečnostných opatrení rozdelené do troch kategórií.

Vyhláška NBÚ č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení však neurčuje kategórie opatrení, ale kategórie systémov. A kategória systémov je odvodená od klasifikácie spracúvaných údajov.

V závislosti od kategórie systému sú potom určené minimálne požiadavky na bezpečnostné opatrenia, v prílohe č. 3 vyhlášky.

Bezpečnostné opatrenie	Kategória I	Kategória II	Kategória III
organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
personálna bezpečnosť	Odporúčané	Povinné	Povinné
riadenie prístupov	Odporúčané	Povinné	Povinné
riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	Povinné	Povinné	Povinné
bezpečnosť pri prevádzke informačných systémov a sietí	Odporúčané	Povinné	Povinné
hodnotenie zraniteľností a bezpečnostné aktualizácie	Odporúčané	Povinné	Povinné
ochrana proti škodlivému kódu	Odporúčané	Povinné	Povinné
sieťová a komunikačná bezpečnosť	Odporúčané	Odporúčané	Povinné
akvizícia, vývoj a údržba informačných sietí a informačných systémov	Odporúčané	Odporúčané	Povinné
zaznamenávanie udalostí a monitorovanie	Povinné	Povinné	Povinné
fyzická bezpečnosť a bezpečnosť prostredia	Odporúčané	Odporúčané	Povinné
riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
kontinuita prevádzky	Odporúčané	Odporúčané	Povinné
audit, riadenie súladu a kontrolné činnosti	Odporúčané	Povinné	Povinné
určenie manažéra kybernetickej bezpečnosti	Povinné	Povinné	Povinné

Nedajte sa pomýliť. Cieľom zákona o kybernetickej bezpečnosti a jeho vykonávacích predpisov nie je vynútiť **vlastníctvo** konkrétnych nástrojov, ale zaručiť určité **spôsobilosti** subjektov. Spôsob, akým PZS vykonáva opatrenia, je výhradne jeho rozhodnutím. Audítor posudzuje vyspelosť procesu, nie existenciu technológie.

Audit kybernetickej bezpečnosti

Každý prevádzkovateľ základnej služby je okrem implementácie bezpečnostných opatrení povinný aj preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale **(2 roky od posledného auditu).**

Kategorizácia sietí a informačných systémov, okrem stanovenia opatrení zároveň predurčuje aj spôsob, akým má PZS vykonať audit kybernetickej bezpečnosti.

Audit kybernetickej bezpečnosti je posudzovanie zhody, ktoré môže vykonávať len certifikovaný audítor kybernetickej bezpečnosti

Do 31. decembra 2023 je **pre I. a II. kategóriu prevádzkovaných systémov** možné namiesto auditu vykonať **preverenie účinnosti prijatých bezpečnostných opatrení samohodnotením.**

Samohodnotenie môže byť vykonané prostredníctvom manažéra kybernetickej bezpečnosti, postupom uvedeným na stránke nbu.gov.sk.