Mestská časť Bratislava-Vajnory

Materiál na rokovanie Miestneho zastupiteľstva **K bodu: 3**
mestskej časti Bratislava-Vajnory
Dňa 18. septembra 2025

Správa o výsledkoch kontrol miestneho kontrolóra

Materiál obsahuje:
1. Návrh uznesenia MZ
2. Správa o výsledkoch kontroly

Predkladateľ:
Ing. Michal Vlček
starosta

Zodpovedný:
Ing. Martin Gramblička
miestny kontrolór

Spracovateľ:
Ing. Martin Gramblička
miestny kontrolór

Bratislava, september 2025

1. NÁVZH UZNESENIA MIESTNEHO ZASTUPITELSTVA

Miestne zastupiteľstvo mestskej časti Bratislava – Vajnory po prerokovaní

b e r i e n a v e d o m i e

správu o výsledkoch kontrol miestneho kontrolóra.

MESTSKÁ ČASŤ BRATISLAVA – VAJNORY
Roľnícka 109, 831 07 Bratislava 36
Miestny kontrolór

Správa z kontroly
stavu kybernetickej bezpečnosti v mestskej časti Bratislava- Vajnory

Oprávnená osoba :	Ing. Martin Gramblička – miestny kontrolór
Povinná osoba :	Miestny úrad mestskej časti Bratislava-Vajnory
Predmet kontroly :	Kontrola stavu kybernetickej bezpečnosti v MČ BA-Vajnory
Cieľ kontroly :	Kontrola stavu kybernetickej bezpečnosti prostredníctvom kontroly zodpovedných zamestnancov či sa vykonali a dodržiavajú požadované zákonné povinnosti
Miesto a čas vykonania kontroly :	MÚ BA-Vajnory, 23.06.2025-11.08.2025
Dátum doručenia správy :	11.08.2025

1. Zákony a predpisy

-Zákon SNR č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov.

-Zákon č. **69/2018** Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

-Zákon č. **95/2019** Z. z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov.

-Vyhláška NBÚ **č. 164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby). *Predpis bol zrušený predpisom 69/2018 Z. z.*

-Vyhláška NBÚ **č. 165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov. *Predpis bol zrušený predpisom 69/2018 Z. z.*

-Vyhláška NBÚ **č. 166/2018** Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov.

-Vyhláška NBÚ **č. 362/2018** Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení .

-Vyhláška NBÚ **č. 436/2019** Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora. *Predpis bol zrušený predpisom 493/2022 Z. z.*

-Vyhláška NBÚ **č. 493/2022** Z. z. o audite kybernetickej bezpečnosti.

Vyhláška NBÚ **č. 264/2023** Z. z. ktorou sa mení a dopĺňa vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

-Vyhláška ÚPVII **č. 179/2020** Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
(Úrad podpredsedu vlády SR pre investície a informatizáciu bol neskôr nahradený Ministerstvom investícií, regionálneho rozvoja a informatizácie SR – MIRRI)

2. Právny stav
2.1.
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v § 1 ustanovil predmet tohto zákona a upravil skutočnosti a to :
a) podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä
1. postavenie a povinnosti prevádzkovateľa základnej služby,
2. bezpečnostné opatrenia,
3. hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
4. riešenie kybernetického bezpečnostného incidentu,
5. opatrenia proti produktom IKT (informačné a komunikačné technológie), službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,
b) správu v oblasti kybernetickej bezpečnosti, najmä
1. organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
2. úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti,
3. národnú stratégiu kybernetickej bezpečnosti,
4. národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy,
5. jednotný informačný systém kybernetickej bezpečnosti,
6. súčinnosť a výmenu informácií,
Pôsobnosť v oblasti kybernetickej bezpečnosti vykonávajú
a) Národný bezpečnostný úrad (ďalej len „úrad“),
b) Ministerstvo dopravy Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Správa štátnych hmotných rezerv Slovenskej republiky (ďalej len „ústredný orgán“),
c) ministerstvá a ostatné ústredné orgány štátnej správy,[10]) ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov

Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti (ďalej len „iný orgán štátnej správy“).
Zákon účinný od 01.04.2018.
Posledná novelizácia zákona účinná od 01.01.2025.

Mestská časť Bratislava-Vajnory bola dňa 1.3.2020 oznámením Národného bezpečnostného úradu zaradená do registra prevádzkovateľov základnej služby. Udialo sa to na základe § 17 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, podľa ktorého je prevádzkovateľ informačného systému verejnej správy na základe odporúčania Úradu podpredsedu vlády pre investície a informatizáciu automaticky zaradený do jednotného informačného systému kybernetickej bezpečnosti.
https://www.nbu.gov.sk/register-prevadzkovatelov-zakladnej-sluzby-podla-34b-ods-1-a-3-zakona-c-692018-z-z/
Mestská časť Bratislava-Vajnory je povinná dodržiavať ustanovenia tohto zákona, ako aj ďalších súvisiacich právnych predpisov a vyhlášok týkajúcich sa danej oblasti. Nesplnenie týchto povinností môže viesť k udeleniu vysokých pokút, no zabezpečenie IT bezpečnosti by nemalo byť motivované len hrozbou sankcií. Každodenne totiž existujú reálne riziká, ako napríklad únik citlivých údajov, odcudzenie finančných prostriedkov z obecných účtov či vyradenie informačného systému z prevádzky na viac dní. Z tohto dôvodu je nevyhnutné, aby mestská časť vedela v prípade incidentu správne reagovať – teda zdokumentovať udalosť a prijať účinné opatrenia na predchádzanie podobným situáciám v budúcnosti, a to bez ohľadu na prípadné postihy. Kľúčovým predpokladom pre dosiahnutie vysokej úrovne IT bezpečnosti je kvalitne vypracovaná rozdielová analýza, analýza rizík a klasifikácia informačných systémov a údajov. Tieto kroky musia byť realizované v súlade s požiadavkami zákona o kybernetickej bezpečnosti a informačných technológiách vo verejnej správe, ako aj podľa príslušných vyhlášok a noriem.

Povinnosti vyplývajú zo zaradenia do registra prevádzkovateľov základných služieb :
Podľa §19 zákona je prevádzkovateľ základnej služby povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20, na základe ktorého sa bezpečnostné opatrenia prijímajú najmä pre oblasť:
a) organizácie informačnej bezpečnosti,
b) riadenia aktív, hrozieb a rizík,
c) personálnej bezpečnosti,
d) riadenia dodávateľských služieb, akvizícií, vývoja a údržby informačných systémov,
e) technických zraniteľností systémov a zariadení,
f) riadenia bezpečnosti sietí a informačných systémov,
g) riadenia prevádzky,
h) riadenia prístupov,
i) kryptografických opatrení,
j) riešenia kybernetických bezpečnostných incidentov,
k) monitorovania, testovania bezpečnosti a bezpečnostných auditov,
l) fyzickej bezpečnosti a bezpečnosti prostredia,
m) riadenia kontinuity procesov.

Podrobný popis opatrení, ktoré je potrebné prijať je vo vyhláške Národného bezpečnostného úradu číslo 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Audit § 29 zákona

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.
Hlavnými prínosmi auditu sú :
-plnenie povinností prevádzkovateľa základnej služby na vykonanie auditu kybernetickej bezpečnosti,
-audit certifikovaným audítorom overuje plnenie povinnosti podľa zákona o kybernetickej bezpečnosti a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami zákona o kybernetickej bezpečnosti a súvisiacich vyhlášok NBÚ,
-identifikácia nedostatkov pri zabezpečení kybernetickej bezpečnosti s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.
Audit je určený pre prevádzkovateľov základnej služby :
-ktorí si chcú preveriť súlad so zákonom o kybernetickej bezpečnosti nezávislým auditným pohľadom,
-ktorí chcú zabezpečiť kontrolu pri riadení kybernetickej bezpečnosti a pravidelne preskúmavať technické a organizačné opatrenia prijaté v súlade s týmto zákonom,
-ktorí chcú mať odporučenie k tvorbe alebo prepracovaniu bezpečnostnej dokumentácie a zavedeniu bezpečnostných opatrení v súlade s požiadavkami tohto zákona.
Výstupom auditu je auditná správa, ktorá obsahuje stručnú charakteristiku prostredia s ohľadom na prijaté bezpečnostné opatrenia, detailný popis identifikovaných zistení, stanovisko súladu so zákonom o kybernetickej bezpečnosti, zdôvodnenie zistenia a odporučenie nápravných opatrení na odstránenie zistených nedostatkov.

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.
Všeobecným cieľom auditu je proaktívne identifikovať nedostatky v kybernetickej bezpečnosti, najmä neodhalené hrozby a riziká. Spôsob určenia rozsahu auditu je stanovený v prílohe vyhlášky NBÚ č. 493/2022 z. z. o audite kybernetickej bezpečnosti

V § 20 ods. 4 písm. a). zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov je riešená požiadavka na vytvorenie funkcie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti.
Od 01.01.2025 audit kybernetickej bezpečnosti je viazanou živnosťou podľa živnostenského zákona. Služby certifikovaného audítora kybernetickej bezpečnosti možno poskytovať len vtedy, ak FO, alebo PO má živnostenské oprávnenie na výkon viazanej živnosti „Certifikovaný audítor kybernetickej bezpečnosti“.

Poslednou novelizáciou zákona účinnou od 01.01.2025 bola transponovaná smernica NIS2. Smernica NIS2 je celoeurópskou legislatívou v oblasti kybernetickej bezpečnosti. Poskytuje právne opatrenia na zvýšenie celkovej úrovne kybernetickej bezpečnosti v EÚ. Pravidlá EÚ v oblasti kybernetickej bezpečnosti zavedené v roku 2016 boli aktualizované smernicou NIS2, ktorá nadobudla účinnosť v roku 2023. Modernizovala existujúci právny rámec s cieľom udržať krok so zvýšenou digitalizáciou a vyvíjajúcim sa prostredím kybernetických hrozieb. Rozšírením rozsahu pôsobnosti pravidiel kybernetickej bezpečnosti na nové odvetvia a subjekty sa tým ďalej zlepšuje odolnosť a kapacity reakcie na incidenty verejných a súkromných subjektov, príslušných orgánov a EÚ ako celku.

2.2.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov ustanovuje

- organizáciu správy informačných technológií verejnej správy,
- práva a povinnosti orgánu vedenia a orgánu riadenia v oblasti informačných technológií verejnej správy, na ktoré sa vzťahuje tento zákon a
- základné požiadavky kladené na informačné technológie verejnej správy a na ich správu.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „ministerstvo investícií“)

a) zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu,
b) je správcom vládneho elektronického komunikačného systému Govnet

Podľa § 5 ods. 1 správu informačných technológií verejnej správy vykonávajú

- orgán vedenia, ktorým je ministerstvo investícií,
- orgán riadenia vo vzťahu k informačným technológiám verejnej správy v jeho pôsobnosti.

Podľa § 5 ods. 2 písm. c) je uvedené, že :
Orgánom riadenia na účely tohto zákona je
c) obec a vyšší územný celok,
V § 6 sú uvedené základné povinnosti v správe informačných technológií verejnej správy.
Podľa § 12 orgán riadenia je povinný zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačných technológií verejnej správy, ktorých je správcom, vrátane organizačného, odborného a technického zabezpečenia a zabezpečenia proti zneužitiu, a to v súlade s týmto zákonom, všeobecne záväznými právnymi predpismi vydanými na jeho vykonanie, štandardmi a národnou koncepciou.
Zákon účinný od 01.05.2019. Posledná novelizácia zákona účinná od 28.06.2025.
Zákon č. 95/2019 Z. z. o informačných technológiách verejnej správy obsahuje jednu špecifickú požiadavku. V zmysle jeho ustanovenia § 23 je správca povinný vypracovať bezpečnostný projekt pre informačný systém verejne správy, ktorý má byť v súlade s osobitným predpisom a to vyhláškou č. 179/2020 Z. z. a stane sa súčasťou bezpečnostnej dokumentácie. Tu môžeme konštatovať že ide o nadbytočnú administratívnu záťaž pre povinné osoby, ktorá efektívne neprináša žiadnu pridanú hodnotu pre informačnú a kybernetickú bezpečnosť v oblasti informačných technológií verejnej správy, nakoľko platí, že audítor kybernetickej bezpečnosti bude posudzovať v prvom rade zhodu s požiadavkami

vyhlášky NBÚ č. 362/2018 Z. z. a nie vyhlášky ÚPVII č. 179/2020 Z. z. Ak je prevádzkovateľ alebo správca informačnej technológie verejnej správy zároveň prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, mal by sa pri návrhu bezpečnostnej dokumentácie riadiť primárne požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a vyhlášky NBÚ č. 362/2018 Z. z.

2.3. Sankcie

Nedodržanie povinností stanovených uvedenými právnymi predpismi môže viesť k spáchaniu správneho deliktu a následnému uloženiu pokuty podľa § 31 zákona o kybernetickej bezpečnosti. Národný bezpečnostný úrad disponuje aj ďalšími oprávneniami, medzi ktoré patrí aj tzv. „blokovanie“.

3. Skutkový stav
3.1.
-Mestská časť Bratislava-Vajnory bola oznámením Národného bezpečnostného úradu zo dňa 27.03.2020 zaradená odo dňa 1.3.2020 do registra prevádzkovateľov základnej služby s výzvou do 30 dní odoslať kontaktné formuláre. Udialo sa to na základe § 17 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, podľa ktorého je prevádzkovateľ informačného systému verejnej správy na základe odporúčania Úradu podpredsedu vlády pre investície a informatizáciu automaticky zaradený do jednotného informačného systému kybernetickej bezpečnosti.
-Dňa 14.04.2025 bol odoslaný kontaktný formulár a formulár ISVS na Národný bezpečnostný úrad.
-Dňa 05.10.2020 odoslaný aktualizovaný formulár a formulár ISVS na Národný bezpečnostný úrad.
-Oznámenie NBÚ o zmene v jednotnom informačnom systéme kybernetickej bezpečnosti zo dňa 12.07.2021.
-Prijatá smernica RKIB 01/2021 Zásady riadenia kybernetickej a informačnej bezpečnosti pre používateľov ICT(informačno-komunikačných technológií) infraštruktúry, účinná od 01.01.2022.
-Prijatá politika kybernetickej a informačnej bezpečnosti, účinná od 01.03.2022.
-Prijatá smernica RKIB 02/2021 Riadenie rizík kybernetickej a informačnej bezpečnosti, účinná od 01.03.2022.
-Prijatá analýza rizík MÚ Bratislava-Vajnory, účinná od 01.03.2022.
-Prijaté smernice, politiky a analýzy rizík oznámené NBÚ dňa 18.03.2022 a zaslaný výsledok samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, ktorý nahrádzal vykonanie auditu.
- Oznámenie NBÚ o povinnosti hlásiť zmeny v údajoch podľa § 19 ods. 7 zákona č. 69/2018 Z. z..

Zaradenie do registra prevádzkovateľov základnej služby podľa zákona o kybernetickej bezpečnosti prináša prevádzkovateľovi viacero povinností. Medzi kľúčové patria:

implementácia všeobecných bezpečnostných opatrení, vykonanie auditu kybernetickej bezpečnosti, predloženie záverečnej správy z auditu a zavedenie nápravných opatrení, ako aj znášanie nákladov spojených s auditom.
-Implementácia bezpečnostných opatrení - prevádzkovateľ je povinný do šiestich mesiacov od oznámenia o zaradení do registra prijať a dodržiavať bezpečnostné opatrenia aspoň v rozsahu uvedenom v zákone.
-Audit kybernetickej bezpečnosti - do dvoch rokov od zaradenia do registra musí prevádzkovateľ podstúpiť audit kybernetickej bezpečnosti, ktorý overí účinnosť prijatých opatrení.
-Záverečná správa z auditu - po ukončení auditu je prevádzkovateľ povinný do 30 dní predložiť Úradu záverečnú správu z auditu a navrhované nápravné opatrenia s termínmi ich realizácie.
-Nápravné opatrenia - prevádzkovateľ je povinný prijať a realizovať opatrenia na nápravu zistených nedostatkov v kybernetickej bezpečnosti.
-Náklady na audit - náklady spojené s auditom kybernetickej bezpečnosti znáša prevádzkovateľ.
-Spolupráca s audítorom - prevádzkovateľ je povinný poskytnúť audítorovi všetky potrebné dokumenty a informácie na vykonanie auditu.

Dôležité je, že tieto povinnosti sú stanovené zákonom a ich nedodržiavanie môže viesť k sankciám.

Tiež je potrebné zabezpečiť si dohľad nad kybernetickou bezpečnosťou formou manažéra kybernetickej bezpečnosti.
Manažér kybernetickej bezpečnosti je zodpovedný za vytváranie a realizáciu bezpečnostnej stratégie, riadenie kybernetických rizík, riešenie bezpečnostných incidentov, vzdelávanie zamestnancov v oblasti bezpečnosti, nepretržité monitorovanie IT systémov a zabezpečenie súladu s platnou legislatívou. Jeho kľúčovou úlohou je ochrana digitálnej infraštruktúry a citlivých údajov organizácie pred kybernetickými útokmi. Týmto spôsobom prispieva k zabezpečeniu plynulého chodu organizácie, ochrane jej finančných prostriedkov a dobrej povesti. Medzi hlavné činnosti manažéra kybernetickej bezpečnosti patria :
x Riadenie rizík - identifikácia, hodnotenie a implementácia opatrení na minimalizáciu bezpečnostných rizík v digitálnom prostredí.
x Implementácia bezpečnostných opatrení - výber a nasadenie technológií a procesov na zabezpečenie sietí, systémov a dát proti neoprávnenému prístupu a útokom.
x Reakcia na incidenty - vytvorenie a riadenie krízových plánov pre prípad kybernetických incidentov, vrátane koordinácie tímu na zastavenie útokov, minimalizáciu škôd a obnovenie systémov.
x Vzdelávanie zamestnancov - zabezpečovanie neustáleho vzdelávania zamestnancov v oblasti kybernetickej bezpečnosti s cieľom zvýšiť celkovú odolnosť organizácie.
x Monitoring a audit - nepretržité sledovanie bezpečnostných udalostí a pravidelné audity systémov na odhaľovanie slabín a zabezpečenie súladu s bezpečnostnými politikami.
x Dodržiavanie legislatívy - zabezpečenie, aby organizácia spĺňala všetky relevantné zákony a nariadenia týkajúce sa ochrany dát a kybernetickej bezpečnosti.
x Zabezpečenie kontinuity prevádzky - príprava a realizácia plánov na obnovu činností v prípade vážnych kybernetických incidentov.

Podľa § 9 ods. 2 vyhlášky č. 362/2018 Z. z. zmluva s treťou stranou musí obsahovať minimálne :

- obdobie trvania zmluvy,
- ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
- ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
- ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou,
- konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
- konkrétny rozsah činnosti tretej strany,
- zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona,
- ustanovenie o rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby v tretej strane,
- vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
- ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
- ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,
- ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
- ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
- ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
- záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup prevádzkovateľovi základnej služby,
- záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

Význam kontroly kybernetickej bezpečnosti :

• Ochrana dôverných informácií - zabezpečenie, že citlivé údaje sú chránené pred neoprávneným prístupom, únikom alebo zneužitím.

• Prevencia kybernetických hrozieb - znižovanie rizika úspešného útoku a ochrana pred jeho negatívnymi dôsledkami, ako sú výpadky služieb či poškodenie reputácie.
• Zabezpečenie nepretržitej prevádzky - udržiavanie dostupnosti systémov a sietí aj v prípade kybernetického incidentu, čím sa minimalizuje narušenie činnosti organizácie.
• Zmiernenie finančných strát a reputácii - efektívna bezpečnostná kontrola pomáha predchádzať vysokým nákladom spojeným s riešením incidentov a obnovou dôvery verejnosti.
• Dodržiavanie legislatívnych požiadaviek - zabezpečenie súladu s platnými zákonmi a normami, ako je napríklad zákon o kybernetickej bezpečnosti, čím sa predchádza právnym postihom.
Kontrolu by mali vykonávať špecializované firmy, konzultanti. O kontrole kybernetickej bezpečnosti: môžeme hovoriť ako o kľúčovom nástroji ochrany digitálneho prostredia. Kontrola kybernetickej bezpečnosti predstavuje systematický proces hodnotenia a posilňovania ochrany informačných systémov, sietí a dát pred digitálnymi hrozbami. Jej cieľom je identifikovať zraniteľné miesta, vyhodnotiť riziká a navrhnúť efektívne opatrenia na zvýšenie bezpečnosti. Výsledkom je komplexný návrh na zlepšenie stavu kybernetickej ochrany a zabezpečenie súladu s platnou legislatívou a technickými normami.

Kontrola kybernetickej bezpečnosti zahŕňa :
-Analýza rizík - Identifikácia možných hrozieb a zraniteľností v rámci technickej infraštruktúry a procesov.
-Hodnotenie aktuálneho stavu bezpečnosti - Posúdenie účinnosti existujúcich bezpečnostných opatrení a politiky ochrany.
-Overenie súladu s predpismi - Kontrola dodržiavania zákonných požiadaviek a noriem v oblasti kybernetickej bezpečnosti (napr. zákon o kybernetickej bezpečnosti, NIS2, ISO/IEC 27001).
-Identifikácia slabých miest - Odhalenie kritických oblastí, ktoré sú najviac ohrozené kybernetickými útokmi.
-Návrh zlepšujúcich opatrení - Odporúčania na posilnenie bezpečnostnej architektúry a zníženie identifikovaných rizík.
-Školenia a osveta - Vzdelávanie zamestnancov a zvyšovanie povedomia o kybernetických hrozbách, bezpečnom správaní a prevencii incidentov.

Pri posudzovaní kybernetickej bezpečnosti je dôležité spomenúť aj kybernetickú odolnosť.

Kybernetická odolnosť ako základ stabilnej prevádzky IT služieb.

Prevádzka informačných a komunikačných technológií (IKT) pri poskytovaní IT služieb nevyhnutne prináša určité riziká. Súčasťou tejto prevádzky je aj nasadenie bezpečnostných technológií, ktorých úlohou je podporiť ochranu systémov a dát. Spoločným cieľom oboch oblastí je zabezpečiť stabilnú, spoľahlivú a dlhodobo udržateľnú dodávku IT služieb, pričom sa kladie dôraz na minimalizáciu známych zraniteľností a kybernetických hrozieb. Tento cieľ sa v odbornej literatúre označuje ako kybernetická odolnosť.
Kybernetická odolnosť predstavuje rozšírený koncept nad rámec tradičnej kybernetickej bezpečnosti. Zohľadňuje realitu, že bezpečnostné incidenty nie sú len hypotetickou možnosťou, ale prakticky nevyhnutnou súčasťou digitálneho prostredia. Organizácia, ktorá je

kybernetický odolná, disponuje schopnosťou incidentom predchádzať, efektívne ich zvládať a zároveň udržiavať kontinuitu činností aj počas ich priebehu.
Ide o komplexný prístup, ktorý presahuje rámec ochrany pred následkami incidentov. Zatiaľ čo kybernetická bezpečnosť sa sústreďuje najmä na prevenciu a ochranu, kybernetická odolnosť zahŕňa komplexnú metodiku zameranú na zachovanie funkčnosti systémov počas incidentu a obnovu po jeho ukončení.
Kybernetická odolnosť prepája kľúčové oblasti: štandardnú prevádzku IKT, bezpečnostné opatrenia, riadenie kontinuity činností a strategické ciele organizácie. Predstavuje schopnosť organizácie pokračovať v plnení svojich úloh aj napriek nepriaznivým udalostiam, ako sú kybernetické útoky, technické poruchy, ľudské zlyhania či prírodné katastrofy.
Rovnako ako kybernetická bezpečnosť, aj kybernetická odolnosť zasahuje do viacerých úrovní riadenia a procesov organizácie, pričom prevádzka IT systémov tvorí jej neoddeliteľnú súčasť.

4. Kontrolné zistenia

4.1. Register prevádzkovateľa základnej služby

Od 01.03.20202 bola mestská časť zaradená do registra prevádzkovateľov základnej služby a to oznámením Národného bezpečnostného úradu, Odboru regulácie a dohľadu zo dňa 24.03.2020. Názov základnej služby je : informačný systém verejnej správy, identifikácia základnej služby je podľa § 3 písm. k) druhý bod zákona o kybernetickej bezpečnosti a zaradené podľa § 17 ods. 3 tohto zákona. Súčasťou tohto oznámenia bolo aj informácia pre prevádzkovateľa základnej služby so žiadosťou o vyplnenie priložených formulárov a to v lehote do 30 dní odo dňa doručenia oznámenia. Záverom bola mestská časť upozornená, že v prípade porušenia povinností vyplývajúcich podľa § 31 ods. 1 a 2 zákona č. 69/2018 Z. z., ako prevádzkovateľovi základnej služby hrozí pokuta za správny delikt až do výšky 300.000 €.

4.2. Audit

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti, v dôsledku čoho ukladá povinnosti prevádzkovateľom základných služieb. Účinnosť zákona nastala od 01.04.2018.
Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb. Národný bezpečnostný úrad pripravil zjednodušený spôsob overenia miery implementácie požiadaviek zákona o kybernetickej bezpečnosti. Tento krok prišiel v reakcii na jeho novelu účinnú od 1. augusta 2021. Prvý audit mal prevádzkovateľ základnej služby povinnosť vykonať do dvoch rokov od zapísania do registra prevádzkovateľov základnej služby. Mieru implementácie požiadaviek tohto zákona bolo možné vykonať samohodnotením prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, ktorú vykonala mestská časť v roku 2022. Ďalšia povinnosť vykonať audit bola do dvoch rokov od samohodnotenia. Po posledných novelizáciách a úpravách je tento termín pre mestskú časť je do 30.9.2025. Audit kybernetickej bezpečnosti môže vykonať len certifikovaný audítor kybernetickej bezpečnosti. Táto certifikácia je

vydávaná akreditovaným certifikačným orgánom a potvrdzuje, že daná osoba spĺňa prísne odborné požiadavky a má dostatočné znalosti a skúsenosti v oblasti kybernetickej bezpečnosti.

4.3. Manažér kybernetickej bezpečnosti

Požiadavka na vytvorenie roly manažéra kybernetickej bezpečnosti je riešená v § 20 ods. 4 písm. a). zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Na túto funkciu sú kladené vysoké požiadavky ako odborná spôsobilosť, certifikát o odbornej spôsobilosti, certifikáciu a iné. Má zodpovednosť a úlohy ako napr. zavádzanie a dohľad nad bezpečnostnými opatreniami podľa zákona, riadenie kybernetických rizík a incidentov, koordinácia so štátnymi orgánmi atď. Táto pozícia by mala byť zabezpečená prostredníctvom externého dodávateľa, najlepšie spoločnosťou, ktorá bude vykonávať externý audit kybernetickej bezpečnosti. V súčasnosti funkciu manažéra kybernetickej bezpečnosti zabezpečuje pre mestskú časť Ing. Tomáš Kulka - vedúci ekonomického oddelenia.

5. Odporúčania

-Na základe budúceho vykonaného auditu kybernetickej bezpečnosti a jeho odporúčaní, realizovať bezpečnostné opatrenia.
-Oficiálne určiť externého manažéra kybernetickej bezpečnosti menovacím dekrétom.
-Vyčleniť v rozpočte mestskej časti potrebné finančné prostriedky na plnenie povinností stanovených príslušnými predpismi.
-Zabezpečiť pravidelné a systematické školenia zamestnancov s cieľom zvyšovať ich odborné znalosti a IT zručnosti prostredníctvom kombinácie technických a organizačných opatrení, nakoľko 95 % kybernetických útokov je spôsobených ľudskou chybou.

6. Záver

Na základe budúcej schválenej a aktuálnej bezpečnostnej dokumentácie, ktorá musí odrážať aktuálny stav, pokračovať v plánovaní a realizácii nevyhnutných bezpečnostných a súvisiacich opatrení.

V Bratislave 18.08.2025

.....

Ing. Martin Gramblička
miestny kontrolór

Stav a vývoj dlhu obce
(mestská časť BA – Vajnory)

informácia pre miestne zastupiteľstvo, stav k 31.08.2025

Celkový dlh obce k 31.08.2025 :

Podľa § 17 ods. 15 zákona č. 583/2004 o rozpočtových pravidlách územnej samosprávy a o zmene a doplnení niektorých zákonov *hlavný kontrolór obce sleduje počas rozpočtového roka stav a vývoj dlhu obce,* pričom dosiahnutie hranice celkovej sumy dlhu podľa odsekov 10 až 12 je povinný bezodkladne oznámiť ministerstvu financií (od 50% do 58 %, od 58% do 60%, od 60%).

Dlh - Celková suma dlhu obce **k 31.08.2025** je **18,35 %**
Dlhová služba - Suma ročných splátok úveru **k 31.08.2025** je **4,39 %**

Výška bežných príjmov za rok 2024 bola **5.630.781,99 €**
Výška bežných príjmov za rok 2024 znížená o tuzemské transfery a granty je **3.549.029,64 €**
Mesačná splátka úveru je **10.416,– €**
Zostatok istiny k 31.08.2025 je **1.033.352,- €**
Suma mesačných splátok k 31.08.2025 je **130.015,33 €**
Suma mesačných úrokových splátok k 31.08.2025 je **25.775,90 €**

Na základe preverenia splnenia uvedených podmienok zákona č. 583/2004 Z. z. o rozpočtových pravidlách územnej samosprávy v znení neskorších predpisov konštatujem, že:

- Podmienka neprekročenia celkovej sumy dlhu obce v hodnote **60 %** skutočných bežných príjmov predchádzajúceho rozpočtového roka **je splnená.**
- Podmienka neprekročenia sumy ročných splátok úveru v hodnote **25 %** skutočných bežných príjmov predchádzajúceho rozpočtového roka **je splnená.**

tab. : prepočet dodržania podmienok v maximálnych hodnotách.

skutočné bežné príjmy k 31.12.2024	Zákon č.583/2004 Z. z.	Zákon č.583/2004 Z. z.
	60%	25%
5.630.781,99 € 3.549.029,64 €	3.378 469,19 €	887 257,41 €

V Bratislave 04.09.2025

Ing. Martin Gramblička
miestny kontrolór