Kybernetická bezpečnosť na obci

Obsah

ÚVOD

Čoraz častejšie sa stretávame s pojmom kybernetická bezpečnosť. Kybernetická bezpečnosť spočíva v zabezpečení počítačových systémov, vyhľadávaní potenciálnych rizík a ich eliminácii. Jej hlavnou úlohou je zabrániť neoprávneným osobám manipulovať s počítačom a uloženými dátami. Súčasťou kybernetickej bezpečnosti je aj ochrana siete, aplikácií a softvéru.

Prevádzkovateľ musí ochrániť svoje informačné systémy a údaje, ktoré spracúva. Iba na základe nepretržitého fungovania dokáže prevádzkovateľ poskytovať svoje služby. Povinnosť riešiť kybernetickú bezpečnosť navyše ukladá aj zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.

Na koho sa vzťahuje zákon o kybernetickej bezpečnosti?

Samotný zákon sa vzťahuje na tzv. prevádzkovateľov základnej služby. Základnou službou je služba, ktorá je zaradená v zozname základných služieb a závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 k zákonu, alebo je prvkom kritickej infraštruktúry. Zjednodušene povedané, prevádzkovateľ základnej služby je subjekt, ktorý:

- Splnil zákonom definované požiadavky (napr. počet obyvateľov, počet odberateľov, počet lôžok, trhový podiel)
- Jeho výpadok by v značnej miere ohrozil štát, resp. obyvateľov / odberateľov
- Vzťahuje sa na neho zákon o kybernetickej bezpečnosti

Zoznam prevádzkovateľov základných služieb vedie Národný bezpečnostný úrad. Typickými príkladmi sú napríklad banky, letiská, elektrárne, mestá a obce, nemocnice, pošta a podobne.

Každá obec spracúva vo svojich informačných systémoch veľké množstvo údajov o svojich občanoch, cudzincoch žijúcich v obci, ale aj údaje o žiakoch alebo zákonných zástupcoch, ak je obec zriaďovateľom materskej alebo základnej školy. Na základe našich skúseností a poznatkov vieme, že častým problémom v obciach je nesprávne nastavená IT štruktúra a neznalosť danej problematiky. Vďaka našim skúsenostiam dokážeme Vašu obec zabezpečiť a ochrániť pred kybernetickými hrozbami.

Prevádzkovatelia základných služieb, ktorými sú aj mestá a niektoré obce, majú veľa povinností v súvislosti s naplnením požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Nižšie uvádzame základný **prehľad 10 oblastí**, na ktoré sa musia mestá a obce zamerať.

1. Výber vhodného partnera
2. Vlastný audit prostredia
3. Stanovenie rozpočtu
4. Poverenie zodpovedného pracovníka / manažéra kybernetickej bezpečnosti
5. Prijatie technických opatrení
6. Prijatie personálnych opatrení
7. Bezpečnostná dokumentácia
8. Uzatvorenie zmlúv s dodávateľmi služieb
9. Audit certifikovaným audítorom
10. Dodržiavanie opatrení

1. Výber vhodného partnera

Každé mesto alebo obec musí v prvom rade zhodnotiť, či sa do tejto zložitej problematiky pustí samo, alebo sa so žiadosťou o pomoc obráti **na zmluvného partnera**. Veľké, predovšetkým krajské mestá môžu problematiku kybernetickej bezpečnosti zvládnuť samy, nakoľko disponujú dostatočným personálnym aparátom (IT referát), ako aj lepšími finančnými podmienkami.

Každý prevádzkovateľ základnej služby by sa ale mal vystríhať ponúk od neznámych, respektíve za týmto účelom novo založených spoločností, ktoré garantujú zabezpečenie kybernetickej bezpečnosti za pár eur mesačne. Na trhu pôsobí mnoho nekorektných firiem, ktoré mestám a obciam **ponúkajú takzvaný falošný pocit bezpečia.** Každá dobra služba niečo stojí a v oblasti kybernetickej bezpečnosti to platí dvojnásobne. Na reálne kybernetické hrozby a splnenie požiadaviek zákona o kybernetickej bezpečnosti pripraví mesto alebo obec iba skutočne funkčný a implementovaný proces. **Samotná papierová dokumentácia, ktorú niektoré firmy ponúkajú, nemôže nikdy nahradiť skutočné technické zabezpečenie a zavedené procesy prevádzkovateľa.**

2. Vlastná analýza prostredia

Po tom, čo sa prevádzkovateľ základnej služby rozhodol, či bude v tejto problematike postupovať sám, alebo v súčinnosti s partnerom, nasleduje vlastná IT analýza prostredia. Obec musí poznať všetky svoje **spracovateľské činnosti**. Na to, aby tieto činnosti mohli byť zmapované, musí prevádzkovateľ vykonať audit. Pri audite sa mesto alebo obec musí zamerať na prijaté technické opatrenia na úseku IT zabezpečenia, a to ako po hardwarovej stránke, tak aj po softwarovej stránke. Jednou z možností je aj vykonanie penetračného testovania, teda simulácie útoku na sieť. Ak sa prevádzkovateľ rozhodne vykonať penetračné testovanie, je potrebné vykonať **interný a aj vonkajší penetračný test**. **Pri internom teste** prebieha preverenie formou vnútorného útoku z pohľadu zamestnanca, ktorý má prístup do siete.

Pri vonkajšom teste dochádza k prevereniu bezpečnosti siete v prípade útoku z vonkajšieho prostredia. Rozdiel medzi vnútorným a vonkajším penetračným testom je v tom, že pri vonkajšom penetračnom teste „útočník“ nepozná architektúru siete ani dostupné systémy a aplikácie prevádzkovateľa.

Audit je záležitosťou, ktorú prevádzkovateľ základnej služby nemôže podceniť. Práve na základe výsledkov mesto alebo zistí, kde sú jeho **slabé miesta**. Výsledky auditu následne pomôžu prevádzkovateľovi prijať potrebné opatrenia, aby dosiahol súlad s požiadavkami zákona o kybernetickej bezpečnosti.

3. Stanovenie rozpočtu

Po vykonaní internej analýzy sa prevádzkovateľovi základnej služby odhalili jeho **slabé miesta**. V tejto fáze je potrebné vyhodnotiť, aké opatrenia je potrebné prijať. Následne je dôležité **stanoviť rozpočet**, čo často predstavuje veľký problém pre orgány verejnej moci. Mesto alebo obec musí dopredu schvaľovať svoj rozpočet na celý rok. Ak orgán verejnej moci dopredu nevie, koľko ho budú stáť opatrenia na úseku kybernetickej bezpečnosti, iba ťažko na to vyhradí dostatočnú časť svojich finančných prostriedkov.

Viacero štúdií uvádza, že výdavky na kybernetickú bezpečnosť sa pohybujú v rozmedzí **0,2 až 1,0 percenta z celkových príjmov organizácie.** V prípade mesta alebo obce je potrebné zvážiť aj **počet obyvateľov**, čo určuje rozsah povinnosti podľa zákona. Táto suma môže na prvý pohľad vyzerať vysoko, možno až hrozivo, avšak každý prevádzkovateľ základnej služby si musí uvedomiť, že prípadný nezvládnutý bezpečnostný incident mu môže spôsobiť oveľa väčšie škody. Tak ako niečo stojí fyzické zabezpečenie (okná, dvere, ploty, a pod.) nad nevyhnutnosťou ktorého sa už nikto ani nezamýšľa, rovnako niečo stojí aj dobrá IT bezpečnosť.

4. Poverenie manažéra kybernetickej bezpečnosti

Prevádzkovateľ základnej služby, ktorým je obec, musí určiť manažéra kybernetickej bezpečnosti.

V zmysle **vyhlášky č. 362/2018 Z. z. Národného bezpečnostného úradu**, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, **manažér kybernetickej bezpečnosti**:

a) má možnosť **predkladať návrhy** a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby,

b) zabezpečuje **aplikáciu bezpečnostných opatrení** v systéme riadenia kybernetickej bezpečnosti,
c) je **nezávislý od riadenia prevádzky** a vývoja služieb informačných technológií,
d) **spĺňa znalostné štandardy** na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu.

Funkciou manažéra kybernetickej bezpečnosti môžu obce a mestá poveriť aj **externý subjekt**. V tomto prípade je ale rovnako dôležité, aby si obce a mestá dobre zhodnotili, komu sa túto funkciu rozhodnú zveriť. Zabezpečenie manažéra kybernetickej bezpečnosti vo vlastnej réžii, teda **prostredníctvom zamestnanca**, by mohlo byť pre menšie obce veľmi nákladné. Z uvedeného dôvodu sa javí poverenie externej spoločnosti ako dobrá alternatíva.

5. Prijatie technických opatrení

Jednou zo základných povinností prevádzkovateľov je prijať **primerané organizačné, technické a personálne opatrenia.** Rovnaká povinnosť sa vzťahuje aj na orgány verejnej moci.

Technické opatrenia musí prevádzkovateľ základnej služby prijať so zreteľom na svoju situáciu a samozrejme aj so zreteľom na svoje finančné možnosti. Mestám a obciam by v tejto problematike mal **pomôcť poverený zodpovedný pracovník za oblasť kybernetickej bezpečnosti, alebo manažéra kybernetickej bezpečnosti**.

Medzi hlavné povinnosti za účelom zabezpečenia technických opatrení patria:

a) hodnotenie zraniteľností a bezpečnostné aktualizácie,
b) riadenie rizík kybernetickej a informačnej bezpečnosti,
c) riadenie prístupov,
d) bezpečnosť pri prevádzke informačných systémov a sietí,
e) ochrana proti škodlivému kódu,
f) sieťová a komunikačná bezpečnosť – Firewall,
g) akvizícia, vývoj a údržba informačných technológií verejnej správy,
h) zaznamenávanie udalostí a monitorovanie,
i) fyzická bezpečnosť a bezpečnosť prostredia,
j) riešenie kybernetických bezpečnostných incidentov,
k) kryptografické opatrenia.

6. Prijatie personálnych opatrení

Akékoľvek prijaté bezpečnostné opatrenia budú vždy vo veľkej miere závislé od ľudského faktora. Zamestnanci obce alebo mesta musia byť v oblasti kybernetickej bezpečnosti adekvátne vzdelaní a rovnako musia vedieť reagovať na prípadné hrozby, alebo vzniknuté incidenty.

V zmysle **vyhláška č. 179/2020 Z. z. Národného bezpečnostného úrad** , ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy, musí obec alebo mesto zabezpečiť svojim zamestnancom vzdelávanie v oblasti kybernetickej bezpečnosti minimálne **jedenkrát za 3 roky**. Mestá s počtom obyvateľom nad 6000 musia zabezpečiť vzdelávanie **každé dva roky**. Krajské mestá musia svojich zamestnancov vzdelávať **minimálne raz ročne**.

7. Bezpečnostná dokumentácia

Po vykonaní auditu, poverení kompetentných osôb a prijatí potrebných opatrení je nutné **celý proces spísať**, respektíve vypracovať kompletnú bezpečnostnú dokumentáciu. **Obsah a štruktúru bezpečnostnej dokumentácie určuje vyhláška, v zmysle ktorej musí dokumentácia obsahovať**:

a) schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,
b) klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
c) zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení; konkrétny obsah môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry,
d) vykonanú analýzu rizík kybernetickej bezpečnosti,
e) záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 zákona.

Bezpečnostná dokumentácia sa vypracúva **na základe posúdenia poskytovanej základnej služby** (v prípade miest a obcí ide o „**Informačný systém verejnej správy**“) a s ňou:

a) súvisiacej infraštruktúry výrobných a produkčných technológií,
b) súvisiacej infraštruktúry informačno-komunikačných technológií,
c) súvisiacej aplikačnej architektúry,

d) súvisiacej bezpečnostnej architektúry a implementovaných bezpečnostných opatrení,
e) súvisiacich organizačných usporiadaní, pracovných rolí, zodpovednosti a delenia právomocí,
f) súvisiacich zaužívaných rámcov riadenia operačných rizík,
g) súvisiacej organizačnej kultúry a spoločenskej zodpovednosti.

Bezpečnostná dokumentácia kybernetickej bezpečnosti **môže zahŕňať aj:**

a) bezpečnostné štandardy, ktoré interpretujú požiadavky platných bezpečnostných politík v konkrétnych situáciách, určujú aktivity, hlavné pravidlá, zodpovednosti a organizáciu riadenia s cieľom podporiť dodržiavanie bezpečnostných politík a
b) bezpečnostné návody, ktoré predstavujú súhrn predpísaných krokov na vykonanie bezpečnostných politík a bezpečnostných štandardov prostredníctvom konkrétnych akcií a ktoré opisujú bezpečnostné konfigurácie a poskytujú konkrétne, platformovo závislé usmernenia na podporu bezpečnostných politík a bezpečnostných štandardov.

8. Uzatvorenie zmlúv s dodávateľmi služieb

V prípadoch, ak **mesto alebo obec nie je reálnym prevádzkovateľom** informačného systému verejnej správy, ale využíva na tento účel externý subjekt, je jeho povinnosťou s týmto subjektom uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností. Požiadavky na zmluvu opäť určuje vyhláška, pričom rozhodujúcim kritériom je opäť počet obyvateľov. Vo všeobecnosti ale platí, **čím väčší je poskytovateľ základnej služby, tým prísnejšia musí byť zmluva s dodávateľmi služieb.**

9. Audit certifikovaným audítorom alebo samohodnotenie

V zmysle zákona o kybernetickej bezpečnosti má mesto alebo obec **povinnosť 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**.

Prijaté opatrenia na meste alebo obci preverí **certifikovaný audítor**. Zoznam certifikovaných audítorov vedie **Kompetenčné a certifikačné centrum kybernetickej bezpečnosti**. Certifikovaní audítori musia spĺňať kvalifikačné požiadavky dané vyhláškou Národného bezpečnostného úradu č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora v súlade s Certifikačnou schémou overovania odbornej spôsobilosti audítora kybernetickej bezpečnosti. Okrem uvedeného musia úspešne absolvovať certifikačný proces.

V zmysle novely zákona o kybernetickej bezpečnosti môže v období od 1.8.2021 do 31.12.2023 prevádzkovateľ I. a II. kategórie nahradiť certifikovaný audit vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených zákonom prostredníctvom manažéra kybernetickej bezpečnosti.

Záver

Každý prevádzkovateľ základnej služby si musí uvedomiť, že po tom, čo prešiel celým procesom a úspešne zvládol audit certifikovaným audítorom, jeho **práca nekončí**. Práve naopak, každé mesto alebo obec musí pokračovať v začatej práci a **dôsledne dodržiavať všetky prijaté a audítorom „odobrené“ opatrenia**. Oblasť kybernetickej bezpečnosti je jedným z najdynamickejšie sa vyvíjajúcim odvetvím a preto to, čo je z hľadiska IT bezpečnosti dostanúce dnes, nemusí byť dostatočné na ďalší rok. Každý prevádzkovateľ základnej služby musí preto sledovať dianie v danej oblasti a za súčinnosti kompetentných osôb **prijímať časom nové a lepšie opatrenia.**