**1. Je tento zoznam ISVS niekde zverejnený? Aby sme vedeli určiť, ktoré IS máme vyplniť do zoznamu pre NBU. Treba tam zahrnúť napr. systém REGOB, CISMA?**

Zoznam informačných systémov verejnej správy nie je nikde zverejnený, každá obec/mesto si musí vytvoriť vlastný zoznam a to na základe vykonanej klasifikácie informácií a kategorizácii sietí a informačných systémov.

Systém REGOB a CISMA, či podobné „národné informačné systémy“ podľa nášho názoru (vychádzajúc z verejne dostupných informácií) nepovažujeme za informačné systémy, ktorých prevádzkovateľom sú obce. Osobitný zákon č. 95/2019 Z.z. o informačných systémoch verejnej správy definuje pojem informačný systém verejnej správy a ustanovuje, kto je správcom informačného systému a ďalej ustanovuje, že správca informačného systému je tiež jeho prevádzkovateľom.

Z osobitných zákonov upravujúcich REGOB či CISMA vyplýva, že ich správcom a teda i prevádzkovateľom je Ministerstvo vnútra SR.

**2. Je ten zoznam informačných systémov niekde zverejnený?**

Zoznam informačných systémov verejnej správy nie je zverejnený, každá obec/mesto si musí vytvoriť vlastný zoznam a to na základe vykonanej klasifikácie informácií a kategorizácii sietí a informačných systémov.

**3. Sú mestá a obce aj prevádzkovateľom národných IS, ktoré používajú? Ide napríklad o IS DCOM, Centrálna ohlasovňa, Centrálny informačný systém matrík, Register adries a ďalšie.**

Podľa nášho názoru nie sú obce prevádzkovateľom týchto informačných systémov. Osobitný zákon č. 95/2019 Z.z. o informačných systémoch verejnej správy definuje pojem informačný systém verejnej správy a ustanovuje, kto je správcom takéhoto systému a ďalej ustanovuje, že správca informačného systému je tiež jeho prevádzkovateľom.

Osobitné zákony (napr. zák. č. 253/1998 Z.z. o hlásení pobytu občanov SR a registri obyvateľov SR, zák. č. 125/2015 Z.z. o registri adries, zák. č. 154/1994 Z.z. o matrikách) ustanovujú, kto je správcom týchto informačných systémov. Pokiaľ ide o matriky, register adries a centrálnu ohlasovňu, je to Ministerstvo vnútra SR, ktoré je tak i prevádzkovateľom týchto informačných systémov.

IS DCOM je v zmysle zák. č. 305/2013 Z.z. o e-Governmente považovaný za nadrezortný informačný systém, ktorého správcom je záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska (známe aj pod skratkou DEUS). V zmysle vyššie uvedeného výkladu je tak DEUS i prevádzkovateľom IS DCOM.

**4. V rámci nášho mikroregiónu Obec Trávnica a Podhájska má viac sko 1000 obyvateľov. Podhájska bola vyzvaná na zaslanie dokumentov na NBÚ, ale Trávnica nie?**

Obec Trávnica môže byť Národným bezpečnostným úradom zaradená do registra prevádzkovateľov základnej služby neskôr, skutočnosť, že ide o geograficky blízke obce nemá vplyv na okamih zápisu do registra.

Obec Trávnica sa taktiež môže samoidentifikovať ako prevádzkovateľ základnej služby dobrovoľne, v súlade s ust. § 18 zák. č. 69/2018 Z.z. a s vyhláškou NBÚ č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby), pokiaľ dosiahne hraničnú hodnotu pre to ktoré dopadové alebo špecifické sektorové kritérium. V takom prípade oznámi Národnému bezpečnostnému úradu svoju identifikáciu prostredníctvom formuláru dostupného na <https://www.nbu.gov.sk/kyberneticka-bezpecnost/prevadzkovatelia-zakladnej-sluzby/>.

**5. Ako je to s počtom obyvateľov v mestskej časti?**

Mestská časť je rovnako tak prevádzkovateľom základnej služby ako iné samosprávy, pokiaľ prevádzkuje taký informačný systém, kde prípadný kybernetický bezpečnostný incident môže postihnúť viac ako 1000 osôb (alebo iné dopadové či sektorové kritérium) v zmysle prílohy č. 1 k zák. č. 69/2018 Z.z. o kybernetickej bezpečnosti.

**6. Mohli by ste vydať zoznam systémov, ktorých by sa to mohlo týkať? Prečo sa máme každý trápiť s tým istým problémom, keď každý rieši to isté? Prípadne dať k dispozícii vzorovo vyplnené tlačivá, aby sme nevymýšľali vymyslené.**

Zostavenie zoznamu informačných systémov, resp. príprava metodiky ako postupovať v otázkach kybernetickej bezpečnosti pre obce je v súčasnosti predmetom diskusie v rámci Clustra kybernetickej bezpečnosti. V prípade, ak takýto zoznam alebo metodiku vydáme, budeme Vás včas informovať.

**7. Keď ste vy v sklze, prečo sa nemôžu posunúť termíny aj pre poskytovateľov základnej služby?**

Termíny na splnenie povinností v oblasti kybernetickej bezpečnosti sú stanovené spoločne a jednotne pre celú EU. Neskorým zavedením potrebnej legislatívy na národnej úrovni ako aj odkladaním zápisu samospráv medzi prevádzkovateľov základnej služby sa SR sama vystavila (a aj svojich prevádzkovateľov základnej služby) do časového tlaku, avšak to nie dôvod na predĺženie termínov na splnenie povinností.

**8. Väčšina obcí nie je priamo prevádzkovateľom IS VS, rovnako tak ani webstránok alebo e-mailu. Po technickej stránke sú web stránky a e-mail prevádzkované napr. poskytovateľmi webhostingu, skrátka jedná sa o externe zaisťovanú službu. To isté platí o samotnom IS - niektorí ho používajú ako službu v cloude, iní, aj keď majú server ""u seba"", tak na jeho prevádzku, resp. zabezpečenie nemajú dosah, pretože vždy (väčšinou) sa o to stará dodávateľ. Z uvedeného vyplýva, že obce nemajú možnosť nijak ovplyvniť požiadavky, ktoré sú kladené napr. na kryptovanie, prístupy, technické zraniteľnosti.. atď. Otázka znie: v týchto prípadoch logicky vychádza, že je pre obce potrebné dať do súladu predovšetkým §20, ods.3, písmeno d) - riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov. A tým pádom sa vlastne aj ostatné požiadavky vzťahujú na toho, kto túto službu obciam poskytuje, v zmysle zmluvného záväzku, je tak?**

Áno, pri kategorizácii informačných systémov možno zistiť vlastníka toho – ktorého informačného systému a vplyvu konkrétneho informačného systému na prevádzkovanie základnej služby. Následne analýza určí, aké opatrenia po právnej, organizačnej a technickej stránke sa musia pre takéto informačné systémy vykonať tak aby sa samospráva dostala do súladu so zákonom a aby aj prípadní dodávatelia plnili rovnaké bezpečnostné opatrenia ako zákon ukladá samosprávam.

**9. Do akej výšky môžme očakávať sankcie zo strany NBÚ?**

Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti v závislosti od závažnosti konania rozlišuje priestupky (platia fyzické osoby – štatutári a zodpovední zamestnanci) a správne delikty (platia samosprávy). Za priestupok môže byť uložená pokuta vo výške najviac 5.000,- EUR a za správny delikt najviac 300.000,- EUR.

**10. Môže byť manažérom kybernetickej bezpečnosti externý subjekt, resp. právnická osoba?**

Áno, ale bude musieť spĺňať odborné požiadavky (bezpečnostné a znalostné štandardy), ktoré Národný bezpečnostný úrad ustanoví na výkon funkcie manažéra kybernetickej bezpečnosti samostatnou vyhláškou, ktorá je zatiaľ iba v prípravnej fáze.

**11. Vyhl. 362/2019, §5, písm. a), ods.4 vraví o požiadavkach na znalostné štandardy bezpečnostného manažéra, citujem: ""spĺňa znalostné štandardy na funkciu manažéra kybernetickej bezpečnosti podľa osobitného predpisu"" - bude tento predpis vo forme vyhlášky, alebo...?**

Áno, NBÚ ustanoví bezpečnostné a znalostné štandardy na výkon funkcie manažéra kybernetickej bezpečnosti samostatnou vyhláškou, ktorá je zatiaľ iba v prípravnej fáze. V súčasnosti nevieme povedať, kedy presne bude táto vyhláška zverejnená na portáli Slov-lex.

**12. Pri všetkej úcte, neviem kto tu zaspal dobu, ale povinností pribúda a peniaze do samospráv sa nenavyšujú, dokonca tento rok to vyzerá veľmi zle.**

Zákon o kybernetickej bezpečnosti je účinný od 01.04.2018, pričom od začiatku účinnosti bol ponechaný čas na splnenie zákonných požiadaviek. Ovplyvnenie skutočnosti, že samosprávy nemajú dostatok financií na riešenie kybernetickej bezpečnosti nie je v kompetencii Clustra kybernetickej bezpečnosti, odporúčame preto túto otázku smerovať na kompetentnejšie orgány – najlepšie na Váš sektorový orgán, ktorým je UPVII a ktorý zároveň riadi operačné programy zo štrukturálnych fondov, ktoré Vám môžu pomôcť financovať bezpečnostné opatrenia.

**13. Kto vie vykonať klasifikáciu IS?**

Klasifikáciu informačných systémov môže vykonať ktorýkoľvek odborný pracovník pôsobiaci v oblasti IT s dostatočnými znalosťami v oblasti kybernetickej bezpečnosti. Pri hľadaní externého dodávateľa takejto služby odporúčame, aby aby preukázal, že disponuje vo svojom tíme osobou ktorá je certifikovaný Lead audítor na ISO 27 000 a že vie preukázať aspoň 1 pozitívnu referenciu na už ním doteraz vykonanú klasifikaciu informácií a kategorizáciu sietí a IS. Vhnete sa tak dodaniu nekvalitnej služby a následne tak aj problémom s povinným auditom.

**14. Mám ešte jednu otázku ohľadom menovaných systémov. My sme napríklad, rovnako ako cca 2000 obcí a miest na Slovensku, v rámci projektu DCOM dostali prakticky kompletné IT vybavenie, ktoré máme ale len vo výpožičke od štátu. Nemáme do toho vybavenia žiadny administrátorský prístup, preto nevieme takmer nič nastaviť, zmeniť či nainštalovať nejaký nový softvér.Čo s tým máme robiť?**

IS DCOM je v zmysle zák. č. 305/2013 Z.z. o e-Governmente považovaný za nadrezortný informačný systém, ktorého správcom je záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska (známe aj pod skratkou DEUS). V zmysle vyššie uvedeného výkladu je DEUS i prevádzkovateľom IS DCOM.

Predpokladáme, že DEUS v otázke kybernetickej bezpečnosti prijal potrebné opatrenia, avšak odporúčame sa obrátiť na DEUS s otázkou, akým spôsobom je zo strany DEUS vyriešená otázka kybernetickej bezpečnosti a splnenie zákonných požiadaviek a aké kroky požaduje DEUS od Vašej obce v tejto otázke vykonať.

**15. Prosím Vás, kamerový systém obce patrí medzi základnú službu?**

Podľa nášho názoru možno i kamerový systém obce zaradiť medzi základnú službu, vzhľadom na to, že poskytuje obrazové informácie, ktoré súvisia so zabezpečením verejného poriadku a bezpečnosti. V prípade, ak by prišlo k jeho výpadku, alebo obmedzeniu činnosti, môže prísť k narušeniu verejného poriadku a bezpečnosti. Záver o tom, či vo Vašom prípade ide o základnú službu, alebo nie, ukáže až analýza kybernetickej bezpečnosti.

**16. Kto bude robiť tieto audity?**

Auditor kybernetickej bezpečnosti certifikovaný certifikačným orgánom. Certifikáty pre audítorov kybernetickej bezpečnosti udeľuje výlučne Kompetenčné a certifikačné centrum kybernetickej bezpečnosti – príspevková organizácia, ktorej zriaďovateľom je Národný bezpečnostný úrad.

**17. Viete ale urobiť aspoň zoznam štátnych (národných), národných systémov, ktoré nepatria (ak nepatria) do základnej služby?**

Tvorba tohto zoznamu nie je v kompetencii Clustra kybernetickej bezpečnosti. Otázku odporúčame smerovať na Národný bezpečnostný úrad.