Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe

JUDr. Jozef Andraško, PhD.

ČPIT 2019
27.9.2019

UNIVERZITA KOMENSKÉHO
V BRATISLAVE
PRÁVNICKÁ FAKULTA

Obsah

- Bezpečnosť ISVS
- Bezpečnostné opatrenia (BO)
- Hlásenie kybernetických bezpečnostných incidentov (KBI)

- APVV-17-0403
- Vplyv vzájomného uznávania prostriedkov elektronickej identifikácie na elektronické služby verejnej správy

Bezpečnosť ISVS

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov **(ZoITVS) + vyhláška**

- Výnos č. 55/2014 Z. z. o štandardoch pre ISVS **(Výnos)**
  - platný a účinný
  - do nadobudnutia účinnosti VZPP podľa § 31
  - najneskôr do 1. mája 2020

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

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) **(GDPR)**

ISVS

- zabezpečiť riadny chod VS
- VS vo funkčnom ponímaní
- formy činnosti VS

ITVS

- **IT** v **pôsobnosti správcu** podporujúca **služby verejnej správy, služby vo verejnom záujme alebo verejné služby**

IT

- prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe
- ...informačné systémy, infraštruktúra, informačná činnosť a elektronické služby

ISVS

- IS v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby

IS

- funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.

ZoITVS (I)

- Bezpečnosť ITVS - § 18 – 23 ZoITVS
- Správca je povinný zabezpečiť riadenie bezpečnosti (§ 14 ods. 1 písm. i)

- **Základné ustanovenia** (§ 18)
- **Bezpečnosť** informačných technológií verejnej správy v oblasti
  - **plánovania a organizácie (§ 19)**
  - **obstarávania a implementácie (§ 20)**
  - **prevádzky, servisu a podpory (§ 21)**
  - **v oblasti monitoringu a hodnotenia (§ 22)**
- **Osobitné opatrenia** na úseku bezpečnosti informačných technológií verejnej správy (§ 23)

Pripravovaná vyhláška

§ 31 písm. a) ZoITVS vyhláška ustanoví:

- jednotlivé **kategórie informačných technológií verejnej správy** a podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu na účely podľa § 11 ods. 4,

§ 31 písm. i) ZoITVS vyhláška ustanoví podrobnosti o:

- **bezpečnosti ITVS** podľa § 18 až 23,
- obsahu **bezpečnostných opatrení**,
- obsahu a štruktúre **bezpečnostného projektu** a
- **rozsah bezpečnostných opatrení** v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov,

Kategórie ITVS (II)

(a) vyhláška ustanoví:

- jednotlivé kategórie informačných technológií verejnej správy a podrobnosti o spôsobe zaraďovania do týchto kategórií **s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov (SIS)**
- **podľa osobitného predpisu** na účely podľa § 11 ods. 4,

- osobitný právny predpis – **ZoKB, § 20 ods. 2**
  - **+** vyhláška č. **362/2018** Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

§ 4 a príloha č. 2 vyhlášky č. 362/2018 Z. z.

- klasifikačné stupne v závislosti od narušenia dôvernosti, integrity a dostupnosti informácií
- kategorizácia SIS je založená na klasifikácii informácií

BO - ZoITVS (I)

- **BO podľa ktorého PP?**
  - **ZoITVS vs. ZoKB**

- **Správca – nie je PZS**
  - BO podľa ZoITVS

- **Správca ako PZS**

a) bezpečnostné opatrenia (BO) podľa ZoKB

V zmysle § 18 ods. 1 zákona o ITVS:
*Povinnosť **správcu**, ktorý je prevádzkovateľom základnej služby, prijať a realizovať bezpečnostné opatrenia vo vzťahu k **informačným systémom verejnej správy v jeho správe** v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje **osobitný predpis*** (§20 ZoKB)

Prevádzkovateľ základnej služby (PZS)

- NBÚ zaradí **základnú službu (A)** do zoznamu ZS a jej prevádzkovateľa do registra PZS:
  - na základe **oznámenia** prevádzkovateľom tejto služby
  - na základe **podnetu ústredného orgánu**
  - z **vlastnej iniciatívy**

preveruje NBÚ podnet?

- NBÚ **v spolupráci s príslušným ústredným orgánom** zaradí **základnú službu (B)** do zoznamu ZS a jej prevádzkovateľa do registra PZS

- NBÚ zaradí **základnú službu (C)** do zoznamu ZS a jej prevádzkovateľa do registra PZS zo zákona

základnou službou **služba**, ktorá je zaradená v **zozname** základných služieb a

(A) závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,
(B) je informačným systémom verejnej správy, alebo
(C) je prvkom kritickej infraštruktúry,

BO - ZoITVS (II)

b) ak BO podľa ZoITVS striktnejšie ako v ZoKB – podľa ZoITVS?

V zmysle § 18 ods. 2 zákona o ITVS:
Obsah *bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a* ***spôsob a rozsah ich prijímania a realizácie*** *v súlade s osobitným predpisom[22] (§ 2 ods. 2 písm. e) ZoKB) ustanovuje tento zákon.*

§ 2 ods. 2 písm. e) ZoKB hovorí, že:
ZoKB sa nevzťahuje na: *požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,[6]) ak ich* ***cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona.***

Odkaz 6) *Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*
Zákon č. 275/2006 Z. z*. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*

Bezpečnostné opatrenia – ZoKB (vyhláška č. 362/2018 Z. z.)

Bezpečnostné opatrenie pre	Kategória I	Kategória II	Kategória III
Oblasť podľa *§ 20 ods. 3 písm. a)* zákona **organizácia informačnej bezpečnosti**	Odporúčané	Odporúčané	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. b)* zákona **riadenia aktív, hrozieb a rizík**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. c)* zákona **Personálna bezpečnosť**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. d)* zákona **riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. e)* zákona **technické zraniteľnosti systémov a zariadení**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. f)* zákona **riadenie bezpečnosti sietí a informačných systémov**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. g)* zákona **riadenie prevádzky**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. h)* zákona **riadenie prístupov**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. i)* zákona **kryptografické opatrenia**	Odporúčané	Odporúčané	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. j)* zákona **riešenie kybernetických bezpečnostných incidentov**	**Povinné**	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. k)* zákona **monitorovanie, testovanie bezpečnosti a bezpečnostných auditov**	Odporúčané	**Povinné**	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. l)* zákona **fyzická bezpečnosť a bezpečnosť prostredia**	Odporúčané	Odporúčané	**Povinné**
Oblasť podľa *§ 20 ods. 3 písm. m)* zákona **riadenie kontinuity procesov**	Odporúčané	**Povinné**	**Povinné**

Hlásenie bezpečnostných incidentov (ZoITVS) I

Orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti sú **povinní** vo vzťahu k ITVS

- ak sú zaradení do registra PZS podľa osobitného predpisu (ISVS ako ZS), **nahlasovať** spôsobom podľa osobitného predpisu (**JISKB**) **aj kybernetický bezpečnostný incident (KBI)**, **na ktorý sa nevzťahuje povinnosť nahlasovania** podľa osobitného predpisu (ZoKB-**ZKBI**);

OR-PZS
I
JISKB
I
KBI

- ak nie sú do tohto registra zaradení, nahlasujú takýto kybernetický bezpečnostný incident **orgánu vedenia ním určeným spôsobom**,

OR
I
KB
I
KBI

- určiť jeden **kontaktný bod** na nahlasovanie kybernetických bezpečnostných incidentov

Hlásenie bezpečnostných incidentov (ZoITVS) II

- **JISKB – 18.10.2019**

Prechodné ustanovenia (§ 33 ods. 5 ZoITVS)

- **Do uplynutia 30 dní** odo dňa zriadenia a uvedenia do prevádzky JISKB **nahlasuje orgán riadenia** podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, **ktorí sú zaradení do registra PZS** podľa osobitného predpisu, **kybernetický bezpečnostný incident** podľa § 23 ods. 3 písm. a) **orgánu vedenia ním určeným spôsobom.**

Hlásenie BI – GDPR

- **„porušenie ochrany osobných údajov“** je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim;

- prevádzkovateľ, sprostredkovateľ
  - **výnimky** - nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb...

Povinnosť	Lehota
Prevádzkovateľ oznamuje dozornému orgánu (čl. 33 ods. 1)	**Bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín** po tom, čo sa o porušení ochrany osobných údajov dozvedel
Sprostredkovateľ oznamuje prevádzkovateľovi (čl. 33 ods. 2)	**Bez zbytočného odkladu** po tom, čo sa o porušení ochrany osobných údajov dozvedel
Prevádzkovateľ oznamuje dotknutej osobe (čl. 34 ods. 1)	**Bez zbytočného odkladu**

- **ÚOOÚ**
- **Prístup do NČ JISKB**
- **Hlásenia/oznámenie náležitosti v zmysle GDPR**

	ZoITVS I	ZoITVS II	ZoKB	GDPR
Subjekt	Orgán riadenia (PZS)	Orgán riadenia (nie je PZS)	Správca - PZS	prevádzkovateľ/ sprostredkovateľ
Druh BI	KBI	KBI	ZKBI	POOÚ
Komu oznamuje BI	NBÚ (JISKB) 30 dní od JISKB – KB orgánu vedenia	Orgánu vedenie (KB)	NBÚ (JISKB)	ÚOOÚ
Lehota	-	-	bezodkladne	bez zbytočného odkladu/72 hodín

Otázky?

jozef.andrasko@flaw.uniba.sk