Kybernetická bezpečnosť a Vy:
Úvod do legislatívy o kybernetickej bezpečnosti

23. máj 2018

Peter Bíro (CEO)

Obsah seminára

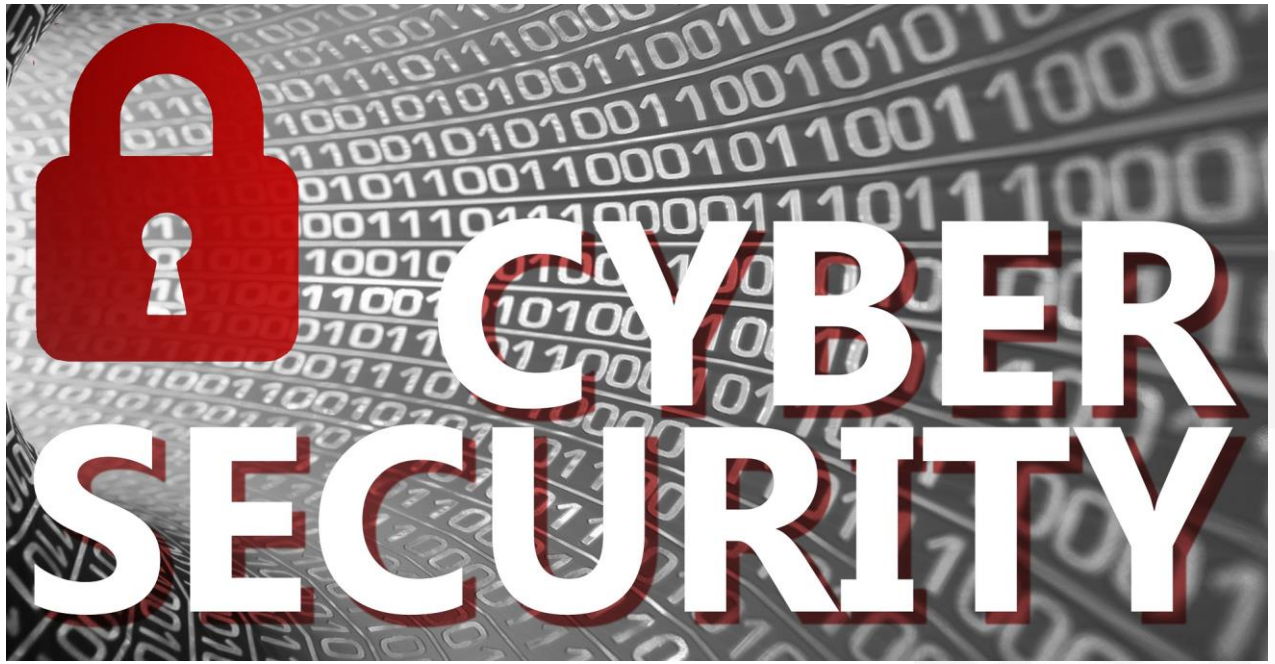
1. Kybernetická bezpečnosť a Vy: Úvod do legislatívy o kybernetickej bezpečnosti

   P. Bíro (SK-NIC, a.s.)

2. Praktické nastavenia pri plnení povinností podľa zákona o kybernetickej bezpečnosti

   R. Janota (NBÚ)

10:00 – 12:30




CYBER
SECURITY

1: Úvod a definície

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

- **1. apríl 2018** = účinnosť
- Transpozícia smernice EÚ o NIS
- Čo by mohlo byť lepšie
- Paralelne ku zákonu o kritickej infraštruktúre aj legislatíve ohľadom GDPR a rôznym iným „bezp. legislatívam“ **(zákon 275/2006 o IS VS, zákon 305/2013 o e-Governmente, zákon 351/2011 o el. komunikáciách)** – požiadavky sa bohužiaľ navzájom neharmonizujú ani nerozoznávajú, ale duplikujú

Definície (§ 3)

- **a)** sieť a informačný systém – elektronická komunikačná sieť, informačný systém (extenzívne = aj listinný), každé zariadenie a komunikačný systém (extenzívne = aj dymový či morzeovka, NIS iba ak automatické spracúvanie digi-údajov) alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov

- **b)** kybernetický priestor – globálny (úrad aj tu) dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky (?) kybernetického priestoru (rekurzia), osoby vykonávajúce aktivity v tomto systéme (osoby nemôžu byť kyber. priestorom) a vzťahy (extenzívne = matka) a interakcie (extenzívne = nákup) medzi nimi

Definície (§ 3)

- **j)** kybernetický bezp. incident – akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť (táto je zadefinovaná celkom dobre) alebo ktorej následkom je
  - strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
  - obmedzenie alebo odmietnutie dostupnosti základnej služby al. digitálnej služby,
  - vysoká pravdepodobnosť (?) kompromitácie činností základnej služby alebo digitálnej služby alebo,
  - ohrozenie bezpečnosti informácií (ATP?).
- **Čl. 4 (7) NIS:** „incident“ je každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov

Definície (§ 3)

- **k)** základná služba – 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
  - je informačným systémom verejnej správy[8)], alebo
  - je prvkom kritickej infraštruktúry[9)],
- **l)** prevádzkovateľ základnej služby – orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k)
- **m)** digitálna služba – služba, ktorej druh je uvedený prílohe č. 2
- **n)** poskytovateľ digitálnej služby – PO al. FO–podnikateľ, kt. poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur

Definície (§ 3)

- **Príloha č. 1:**

- NBÚ: Sektor: 3. digitálna infraštruktúra, podsektor -, prevádzkovateľ služieb:
  - **poskytovateľ služby výmenného uzla internetu** na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené
  - **poskytovateľ služieb systému doménových mien na internete**
  - **subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne**

- ÚPVII: Sektor: 10. verejná správa, podsektor: informačné systémy verejnej správy, prevádzkovateľ služieb: 1. správcovia a prevádzkovatelia sietí a IS VS a 2. správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené (? webhosting ministerstvu!)

Definície (§ 3)

- Vyhláška: (MPK: neuzavreté) – Digitálna infraštruktúra
- **Poskytovateľ služieb systému doménových mien na internete.**
- **Špecifické sektorové kritériá:**
- **a)** Poskytovanie autoritatívnych odpovedí na svojich DNS serveroch pre najmenej 1 000 rôznych domén druhej úrovne
- **b)** Celkový počet DNS dopytov, na ktoré odpovedajú všetky DNS servery organizácie, je najmenej 3 000 000 za 24 hodín. Tento ukazovateľ je počítaný za 7 po sebe nasledujúcich dní a zahŕňa aj rekurzívne dopyty, ale nezahŕňa dopyty na lokálne domény organizácie (DNS).

Definície (§ 3)

- **Poskytovateľ služieb systému doménových mien na internete.**
- **Dopadové kritériá:**
- Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a IS, ktoré postihuje viac ako 25 000 osôb.
- Obmedzenie či narušenie prevádzky inej ZS alebo prvku kritickej infraštruktúry.
- Hospodársku stratu alebo hmotnú škodu najmenej 1 užívateľovi viac ako 250 000 eur.
- Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá by si mohla vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

Definície (§ 3)

- Jednotný IS kyber. bezpečnosti
  - komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov
  - centrálny systém včasného varovania
  - verejná a neverejná časť, prístup bezodplatný
- K neverejnej časti má prístup aj prevádzkovateľ základnej služby a poskytovateľ digitálnej služby
- Oznamovanie skutočnosti bezodkladne (!) (na rozdiel napr. od 78hod podľa GDPR)

2: Základná služba a digitálna služba

Zaradenie do zoznamu ZS (§ 17)

- **Ods. 1) -** Zoznam základných / digitálnych služieb – oznámenie do 30 dní od zistenia prekročenia identifikačných kritérií, ÚOŠS alebo iniciatívne NBÚ – ale podľa **§ 34 (2)** do 6 mesiacov

- **Ods. 5) -** Oznámenie musí obsahovať
  - názov a sídlo + kontaktné údaje
  - Zoznam služieb, ktorých sa prekročenie týka
  - Informáciu o možnom alebo cezhraničnom presahu služby (?)
  - Percentuálny podiel na trhu (neobmedzené na .sk = ??)
  - Geografické rozšírenie služby
  - Informáciu o alternatívnych možnostiach zachovania služby v prípade incidentu (?)

Povinnosti prevádzkovateľa základnej služby (§ 19)

- **Ods. 1) -** Do 6 mesiacov splniť opatrenia podľa par. 20 a sektorové opatrenia, ak existujú / ak zaradený úradom do 9.11.2018 podľa **§ 34**, tak do 2 rokov (**ods. 6**)
- **Ods. 2) -** Pri zmluve s dodávateľom s činnosťami, kt. priamo súvisia so sieťami a IS – povinná zmluva o zabezpečení plnenia bezp. opatrení a notifikačných povinností podľa zákona
- **Ods. 3) -** Dňom zaradenia do registra informovať podnik poskytujúci internet pre základnú službu (elektronické komunikačné služby a siete podľa telco zákona)
- **Ods. 4) -** Povinnosť informovať tretiu stranu (akú ?), ak by bezp. kyber. incident znemožnil plnenie zmluvy podľa ods. 2, tým nedotknutá mlčanlivosť (?)
- **Ods. 5) -** Ak poskytuje službu aj v inom ČŠ, úrad & 2. úrad rozhodnú, podľa kritérií kt. ČŠ bude identifikovaný

Povinnosti prevádzkovateľa základnej služby (§ 19)

- **Ods. 7) -** Povinnosť oznamovať zmeny do 30 dní (prostredníctvom jednotného IS)
  - názov a sídlo (zákon o eGov?) + kontaktné údaje
  - zoznam služieb, ktorých sa prekročenie týka
  - informáciu o možnom alebo cezhraničnom presahu služby
  - percentuálny podiel na trhu (zohľadnenie dynamiky vývoja??)
  - geografické rozšírenie služby
  - informáciu o alternatívnych možnostiach zachovania služby v prípade incidentu (zmena BP? Každá zmena spôsobu zálohovania?)

Bezpečnostné opatrenia (§ 20)

- **Ods. 1-2) -** Povinná klasifikácia informácií a kategorizácia sietí a IS - na základe významnosti, funkcie a účelu informácií a IS s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť
- **Ods. 3-4) -** Povinné opatrenia pre oblasti cca podľa STN ISO 27001 (organizácia IB, riadenie rizík, personálna bezp., riadenie prístupov, riešenie bezp. incidentov, kontinuita...) +
  - detekcia, evidencia, postupy riešenia a riešenie bezp. incidentov
  - kontaktná osoba pre prijímanie a evidenciu hlásení (akých?)
  - pripojenie do jednotného systému
- **Ods. 5) -** Povinná aktuálna dokumentácia zodpovedajúca reálnemu stavu

Poskytovateľ digitálnej služby (§ 21)

- Digitálna služba **(príloha 2, podľa NIS) - § 3 n) –** PO alebo živnostník s 50+ zamestnancami a ročným obratom al. celkovou ročnou bilanciou viac ako 10 mil. EUR.

- **Online trhovisko** - digitálna služba (rekurzia), ktorá umožňuje spotrebiteľom alebo podnikateľom uzatvárať online kúpne zmluvy (akýkoľvek e-shop) alebo zmluvy o službách s podnikateľmi buď na webovom sídle online trhoviska, alebo na webovom sídle podnikateľa, ktoré využíva počítačové služby poskytované online trhoviskom (aká externá služba umožňuje priamo uzatvárať zmluvy na webe podnikateľa??)

- **Internetový vyhľadávač** - digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých web. sídlach (také neexistuje a akékoľvek zúženie je ľubovoľne zúžiteľné ďalej) alebo na web. sídlach v konkrétnom jazyku (?) informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom

Poskytovateľ digitálnej služby (§ 21)

- **Služba v oblasti cloud computingu** - digitálna služba (rekurzia), ktorá umožňuje prístup ku škálovateľnému a pružnému (??) súboru počítačových zdrojov (??), ktoré možno zdieľať. (toto spĺňa aj MS Active Directory) – vs **Výnos MF SR č. 55/2014 o štandardoch pre IS VS (§ 2)**

- **x) cloud computingom** model umožňujúci jednoduchý samoobslužný sieťový prístup k službám informačných technológií na vyžiadanie, poskytovaným vo virtuálnom prostredí konfigurovateľných výpočtových zdrojov, ktoré môžu byť pridelené alebo uvoľnené s minimálnym úsilím a časovým obmedzením, a to na základe voliteľného škálovania a navyšovania, nezávisle od lokality zdrojov alebo lokality prístupu k nim a bez osobného kontaktu s poskytovateľom cloudovej služby, pričom využitie týchto služieb je merané a hodnotené podľa ich skutočného využitia **(vychádza z def. NIST)**

- **y) cloudovou službou** ľubovoľný prostriedok alebo zdroj cloud computingu, poskytovaný vzdialeným prístupom na základe podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb

Poskytovateľ digitálnej služby (§ 21)

- **§ 3 n) –** poskytovateľ = PO alebo živnostník s 50+ zamestnancami a ročným obratom alebo celkovou ročnou bilanciou viac ako 10 mil. EUR.

Zaradenie do zoznamu digitálnych služieb (§ 21)

- **Ods. 1) -** Zoznam základných / digitálnych služieb – oznámenie do 30 dní od začatia poskytovania digitálnej služby (kontra § 34 prechodné *„osoba existujúca ku dňu účinnosti zákona oznámiť informácie podľa ods. 1 do 6 mesiacov“* – aká osoba??) (platia súčasne) alebo iniciatívne NBÚ

- Oznámenie musí obsahovať
  - názov a sídlo + kontaktné údaje **(a) a b))**
  - poskytovanú službu (pravdepodobne digitálnu) **(c)**
  - názov, sídlo a kontaktné údaje zástupcu podľa § 23 **(d)** (v princípe na účely ak nie je v EÚ, ale načo uvádzať, ak je v SR)

Povinnosti poskytovateľa digitálnej služby (§ 22)

- **Ods. 1)** - Do 6 mesiacov splniť opatrenia podľa osobitného predpisu **(Vykonávacie nariadenie Komisie (EÚ) 2018/151 k smernici o NIS)** + *„na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby“* (kedy nastáva splniteľnosť tohto?)

- **Ods. 2) -** Pri posudzovaní splnenia posudzuje najmä
  - Bezpečnosť sietí a IS (ktorých?) a schopnosť predchádzať a riešiť kyb. bezp. incident
  - Spôsob zachovania kontinuity pri kyb. bezp. incidente
  - Súlad sietí a IS s bezp. štandardmi v oblasti kyb. bezp. (to sú ktoré? Napr. 27001 je IB)

Povinnosti poskytovateľa digitálnej služby (§ 22)

- **Ods. 3) -** je povinný
  - hlásiť každý kyb. bezp. incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kyb. bezp. incident podstatný vplyv podľa osobitného predpisu **(Vykonávacie nariadenie Komisie (EÚ) 2018/151 k smernici o NIS)**, a to bezodkladne po jeho zistení
  - riešiť kyb. bezp. incident a spolupracovať pri tom s NBÚ
- **Ods. 4) -** Ak na poskytovanie digi-služby využíva služby prevádzkovateľa ZS, povinná vzájomná zmluva o zabezpečení plnenia bezp. opatrení a notifikácií (= každý web s digi-službou (!))
- **Ods. 5) -** Povinnosť informovať tretiu stranu (akú ?), ak by kyb. bezp. incident znemožnil plnenie zmluvy (ktorej?), tým nedotknutá mlčanlivosť (?)

3: Hlásenie incidentov, kontrola a sankcie

Hlásenie a riešenie bezp. incidentov (§ 24-26)

- **§ 24-26 -** Hlásenie kyb. bezp. incidentov – podľa vykonávacieho predpisu – 3 stupne – geografický SR = 3!
- **§ 24 ods. 3) -** Ak prevádzkovateľ zákl. služby využíva na to digi-službu, hlási aj závažný kyb. bezp. incident prevádzkovateľa digi-služby (duplicita, v princípe iba cloud, ale pozor napr. na integrované Google)
- Hlásenie prostredníctvom jednotného IS (ale úrad sprístupní do 18 mesiacov) (**§ 34)**
- **§ 27 ods. 1)** - NBÚ môže uložiť povinnosť vykonať v prípade závažného kyb. bezp. incidentu reaktívne opatrenie (primeranosť?) a požadovať návrh opatrení a ich vykonanie na zabránenie opakovania incidentu

Kontrola a audit (§ 28-29)

- **§ 28** - Kontrola – ako kontrola v štátnej správe
- **§ 29** - Audit (iba pre prevádzkovaľa ZS) – podľa vykonávacieho predpisu, povinne do 2 rokov od zaradenia, po každej významnej zmene (!!) a po každej určenej perióde (!)
- Vykonať môže iba akreditovaný orgán posudzovania zhody **(3)**
- Povinne do 30 dní od ukončenia správu NBÚ aj s opatreniami na nápravu a lehotami **(4)**
- Aj NBÚ môže nariadiť audit **(5)**
- Náklady na audit 2 rokov znáša prevádzkovateľ ZS, nariadený NBÚ znáša NBÚ, ostatné nevedno, takže prevádzkovateľ... **(6)**

Sankcie (§ 30-31)

- **§ 30 - <u>Priestupok</u>** – FO (100-5000 EUR):
  - porušenie mlčanlivosti – naveky – zbavuje riaditeľ NBÚ
  - nepravdivé údaje pri oznámení prevádzkovateľa (??!)
  - poruší povinnosti prevádzkovateľa ZS (??!)
  - neprijme bezp. dokumentáciu prevádzkovateľa ZS (??!)
  - nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby (???! extenzívne protiústavné – NBÚ nereguluje personálne ani pracovné právo)

- **§ 31 - <u>Správne delikty</u>** – 300 EUR - 1 % celkového ročného obratu za predchádzajúci účtovný rok (do 300.000 EUR) – napr. aj neohlásenie incidentu či nevykonanie opatrenia na nápravu v lehote podľa záverečnej správy o výsledkoch auditu

OTÁZKY ?

Peter Bíro (CEO)