

Smernica EÚ pre sieťovú a informačnú bezpečnosť a jej transpozícia do právneho systému SR

eFOCUS

Rastislav Janota, NBÚ

Koho sa týka KB?

© MAZK ANDERSON

WWW.ANDERZTOONS.COM



PREDTÝM NEŽ NAPIŠEM SVOJE MENO NA TABUĽU, POTREBUJEM
VEDIEŤ ČO PLÁNUJETE UROBIŤ S TÝMI ÚDAJMI

Koho sa týka kybernetická a
informačná bezpečnosť?

NÁS VŠETKÝCH!!!

Ved' každý je zodpovedný za svoje vlastné dáta.

Prečo európska regulácia?

- Jednotný digitálny trh Európskej únie
- Cezhraničná podstata kybernetických incidentov
- Viac a viac údajov dostupných prostredníctvom komunikačných sietí
- Viac a viac služieb dostupných prostredníctvom komunikačných sietí

-
- Snaha EU o zvýšenie schopností kybernetickej bezpečnosti na úrovni členských štátov (ČS)
 - Snaha o zlepšenie kooperácie medzi ČS v oblasti kybernetickej bezpečnosti
 - Snaha o vytvorenie silného hráča z EU v oblasti kybernetickej bezpečnosti

-
- Vytvorenie úvodu do problematiky na úrovni EU pre zachytenie trendov v oblasti kybernetickej bezpečnosti vzhľadom na rýchly rozvoj technológií ako IoT, connected cars a pod.

Aké regulácie existujú?

- **General Data Protection Regulation (GDPR) – 2016/679**
 - Nariadenie (direktíva) platné bez transpozície od 25.5.2018
 - Regulátor – Úrad na ochranu osobných údajov
- **Payment Services Directive (PSD2) – 2015/2366**
 - Implementácia (transpozícia) do 10.5.2018
 - Regulátor – Národná banka Slovenska
- **Regulatory framework for electronic communications (2009)**
 - Posledný update 2009, implementácia (transpozícia) do 25.5.2011
 - Regulátor - Úrad pre reguláciu elektronických komunikácií a poštových služieb -> NBÚ
- **Network and Information Security Directive 2016/1148**
 - Implementácia (transpozícia) do 10.5.2018
 - Regulátor – Národný bezpečnostný úrad (NBÚ)

Koho sa týka KB?

- Užívateľ akéhokoľvek elektronického zariadenia, smart telefónu, tabletu, počítača, IoT zariadenia a pod. doma či v zamestnaní
- Majiteľ akýchkoľvek dát (údajov) v elektronickej podobe
- Užívateľ elektronických služieb – napr. internet bankingu a pod.

-
- Fyzická osoba – živnostník
 - Akákoľvek právnická osoba a pod.

-
- Poskytovateľ digitálnej služby (podľa zákona o kybernetickej bezpečnosti)
 - Prevádzkovateľ základnej služby (podľa zákona o kybernetickej bezpečnosti)

Zákon o kybernetickej bezpečnosti

Obsah zákona

- Organizácia a pôsobnosť orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
- Národné centrum kybernetickej bezpečnosti
- Jednotný informačný systém kybernetickej bezpečnosti,
- Postavenie a povinnosti prevádzkovateľa základných služieb a poskytovateľa digitálnych služieb,
- Jednotky CSIRT pre riešenie kybernetických bezpečnostných incidentov a ich akreditáciu,
- Systém zabezpečenia kybernetickej bezpečnosti, hlásenia a riešenie incidentov
- Kontrolu nad dodržiavaním tohto zákona, priestupky
- Úprava zákona o kritickej infraštruktúre
- Odmeňovanie pracovníkov VS v oblasti kybernetickej bezpečnosti
- Určenie sektorov a VPA pre sektory a podsektory
- Určenie zoznamu všeobecne záväzných právnych predpisov pre oblasť KB

Dotknuté subjekty

- **Prevádzkovateľ základnej služby (PZS)**
 - Smernica v prílohe 2 určuje minimálne 7 sektorov pre PZS
 - Kritéria pre určenie PZS naznačuje smernica a je vhodné ich harmonizovať naprieč ČŠ
 - ČŠ následne musia určiť subjekty v kategórii Prevádzkovateľ základnej služby
 - ČŠ musia vytvoriť zoznam základných služieb a regulovať u PZS len tieto služby
 - ČŠ by mali určiť kritéria na posúdenie závažnosti rušivého vplyvu incidentu
 - ČŠ môžu prijať alebo zachovať ustanovenia, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov
- **Poskytovateľ digitálnych služieb (PDS)**
 - Smernica v prílohe 3 určuje presne 3 druhy digitálnych služieb
 - ČŠ nesmú ukladať PDS žiadne ďalšie bezpečnostné alebo oznamovacie požiadavky nad rámec tých, ktoré určuje smernica

Regulované sektory podľa zákona

- **PZS**

- | | |
|-------------------------------------|--|
| • Bankovníctvo | • Chemický priemysel |
| • Dodávka a distribúcia pitnej vody | • Finančný sektor / financie |
| • Doprava | • Verejná správa |
| • Digitálna infraštruktúra | • Telekomunikačný sektor / Telekomunikácie |
| • Energetika | • Zdravotníctvo |

- **Rozsah**

- Predpoklad je zhruba 140 subjektov poskytujúcich základné služby naprieč sektormi

Regulované DS podľa zákona

- **PDS**

-
- On line trhovisko
-
- Internetový vyhľadávač
-
- Služby cloudcomputingu
-

- **Rozsah**

- Predpoklad je do 10 subjektov poskytujúcich digitálne služby

Vecne príslušná autorita

- Jednotlivé sektory resp. podsektory (Príloha 1 zákona) sú v pôsobnosti určenej VPA (Vecne príslušná autorita)
- Vecne príslušná autorita vo svojej pôsobnosti (okrem iných povinností)
 - zodpovedá za zabezpečenie kybernetickej bezpečnosti vo svojom sektore (podsektore),
 - plní úlohy jednotky CSIRT resp. prevádzkuje jednotku CSIRT v rozsahu svojej pôsobnosti
 - poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité pre zabezpečenie kybernetickej bezpečnosti,
 - spolupracuje s ostatnými vecne príslušnými autoritami a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,
 - zabezpečuje zvyšovanie úrovne bezpečnostného povedomia, koordinuje spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje politiku správania sa v kybernetickom priestore.

Jednotky CSIRT

- **Smernica**

- ČŠ určí jednu alebo viac jednotiek spĺňajúcich požiadavky Prílohy 1 Smernice NIS, pokrývajúce aspoň odvetvia z Prílohy 2 Smernice NIS (akreditácia CSIRT)
- Jednotky CSIRT podľa Smernice možno zriadiť v rámci príslušného orgánu
- S cieľom prispieť k rozvoju dôvery medzi členskými štátmi a podporiť rýchlu a účinnú operačnú spoluprácu sa zriaďuje sieť vnútroštátnych jednotiek CSIRT

- **Zákon**

- Možnosť dobrovoľnej akreditácie CSIRTu ľubovoľnou právnickou osobou
- CSIRT musí plniť rovnaké požiadavky ako CSIRT VPA
- Získava možnosť prístupu do IS Kybernetickej bezpečnosti s právom využiť dostupné služby pre seba a svojich klientov

Oznamovanie incidentov

- Centrálné miesto – Jednotný informačný systém kybernetickej bezpečnosti
- Prístup do neho pre všetky subjekty povinné zo smernice
- Všetky akreditované CSIRTy majú prístup k incidentom svojich klientov s možnosťou využitia vlastností JIS KB
- Úrad má potrebné informácie pre asistenciu pri riešení incidentov, pre možnú eskaláciu a pre štatistické potreby
- Pripravený na ako jednotné ohlasovacie miesto na všetky incidenty podobného druhu aj pre účely iných ohlasovacích povinností s prístupom príslušných regulátorov
- Ochrana osobných údajov (GDPR) – Úrad na ochranu osobných údajov (prostredníctvom NBÚ)
- Payment Services Directive 2 – Národná Banka Slovenska (zatiaľ nedošlo k dohode)
- Zákon č. 351/2011 Z.z. o elektronických komunikáciách – Národný bezpečnostný úrad
- Smernica NIS (Zákon o kybernetickej bezpečnosti) – Národný bezpečnostný úrad

Všeobecné záväzné predpisy

- Podrobnosti o technickom, technologickom a personálnom vybavení,
- Prahové hodnoty pre identifikáciu základnej služby,
- Obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie, rozsah bezpečnostných opatrení,
- Kategórie a prahové hodnoty kybernetických bezpečnostných incidentov hlásených prevádzkovateľom základnej služby a poskytovateľom digitálnej služby,
- Podrobnosti o požiadavkách na audit a rozsahu auditu,
- Bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti,
- Klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
- Podrobnosti o vymieňaní informácií a osobných údajov s orgánmi členských štátov Európskej únie.

Ako zákon vznikal?

- Transpozícia smernice po jej schválení v júli 2016
- Niekoľko iterácii
- V polovici októbra medzinárodný workshop o transpozícii NIS ako súčasť aktivít predsedníctva v Bratislave
- V decembri 2016 prvý krát predstavená členom Výboru pre kybernetickú bezpečnosť Bezpečnostnej rady Slovenskej republiky
- Zapracovaná prvá časť pripomienok
- Na konci januára zákon predložený na verejné pripomienkovanie odbornej verejnosti (výbor, komisia riaditeľa a pod.)
- Zapracovaná druhá časť pripomienok
- 16.2. verejný workshop k zákonu po druhej sade pripomienok
- Marec/apríl zapracovávanie pripomienok a dolad'ovanie legislatívnej techniky

Ďakujeme za pozornost