Zákon o kybernetické bezpečnosti

září 2014

Zákon o kybernetické bezpečnosti ZKB

- Platnost od 1.1.2015
- Bude s vztahovat na:
  - kritickou informační infrastrukturu - KII
  - významné informační systémy - VIS
- Bude se týkat:
  - státního sektoru- datové schránky, db soc. dávek, katastry, …
  - soukromé sféry - peněžnictví, energetika, zdravotnictví, doprava

Definice vol.I

- Kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.
- Kritickou informační infrastrukturou (KII) se rozumí prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.
- Významným informačním systémem (VIS) se rozumí informační systém spravovaný orgánem veřejné správy, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon činnosti veřejné správy.

Původ ZKB

- NBÚ
  - dostalo zadání
  - na půdorysu ISO 27 000 připravilo návrh
  - vláda v lednu 2014 schválila návrh zákona
  - pracuje se na vyhláškách
- V EU má něco podobného Francie ovšem s většími „právy státu“
- V únor 2013 EU vydala záměr směrnice, který bude EU mustrem. Ovšem s mnohem větším rozsahem (soc. sítě, ...).

Důsledky ZKB

- 2 zásady ctěné od vzniku ZKB:
  1. minimalizace zásahů do práv soukromých subjektů
  2. individuální zodpovědnost za bezpečnost vlastní sítě
- Vzniklo NCKB - govcert.cz
  - přes národní CERT bude monitorovat a vydávat bezpečnostní doporučení
- Běžný uživatel bude mít vyšší zabezpečení
- Stát neupadne do chaosu

Hlavní pilíře ZKB

1. Standardizace bezpečnostních opatření
   - definují vyhlášky
2. Hlášení kybernetických bezpečnostních incidentů
   - vyžadované / požadované
3. Hlášení protiopatření
   - zdroj pro ostatní + statistické určení „flákače“

Definice vol.II

- Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
- Kybernetickým bezpečnostním incidentem je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
- ZKB stanovuje povinnost detekce a hlášení kybernetických bezpečnostních incidentů.

Přehled technických opatření

- §16 Fyzická bezpečnost
- §17 Nástroj pro ochranu integrity komunikačních sítí
- §18 Nástroj pro ověřování identity uživatelů
- §19 Nástroj pro řízení přístupových oprávnění
- §20 Nástroj pro ochranu před škodlivým kódem
- §21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů,
- §22 Nástroj pro detekci kybernetických bezpečnostních událostí
- §23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- §24 Aplikační bezpečnost
- §25 Kryptografické prostředky
- §26 Nástroje pro zajištění vysoké úrovně dostupnosti
- §27 Bezpečnost průmyslových a řídicích systémů

Kybernetický bezpečnostní incident

- Typy kybernetických bezpečnostních incidentů KBI podle
  - příčiny
    - Způsobené útokem nebo jiným průnikem
    - Způsobené škodlivým kódem
  - dopadu
    - Způsobující narušení důvěrnosti
    - Způsobující narušení integrity
    - Způsobující narušení dostupnosti