



Zákon o kybernetické bezpečnosti

Petr Nižnanský

Zákon o kybernetické bezpečnosti

- Předkladatel zákona - NBÚ
- Účinnost od 1.1.2015
- Být v souladu se zákonem do 1.1.2016

Co to vlastně je?

Kritická infrastruktura

- *“Narušení funkce systémů určených jako kritická informační infrastruktura by mělo závažný dopad např. na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.”*
- Průřezová kritéria
 - 250 mrtvých nebo 2500 zraněných
 - Hospodářská ztráta větší než 0,5 HDP (19,4 mld. Kč - 2013)
 - Závažný zásah do života více než 125 000 lidí

Významný informační systém

- *“Zásadní význam pro fungování veřejné správy (dle stávajícího návrhu vyhlášky např. informační systém základních registrů ISZR, samotné základní registry ROB, ROS, RÚIAN a RPP, informační systém datových schránek ISDS, editační agendové IS atd.).”*
- **Neplatí pro obce, městské části a soukromý sektor!**
- Dopadová kritéria
 - 10 mrtvých nebo 100 zraněných
 - Ztráta větší než 5% rozpočtu
 - Závažný zásah do života více než 50 000 lidí

Nové povinnosti

- Hlásit kontaktní údaje
- Detekovat kybernetické bezpečnostní události
- Hlásit kybernetické bezpečnostní incidenty
- * **Bezpečnostní dokumentace**
- Poslouchat NBÚ (nařízení, vyhlášky...)

CERT

- CERT/CSIRT -
“Bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích.”
- Vládní CERT (NCKB) - veřejný sektor
- Národní CERT (CZ.NIC) - privátní sektor



Požadavek na role

- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Auditor kybernetické bezpečnosti
- Garant aktiva

Kybernetické nebezpečí

- *“Stav kdy je ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.”*
- Max 7 dní s prodloužením na 30.
- Informace se musí zveřejňovat v rozhlasovém a televizním vysílání.



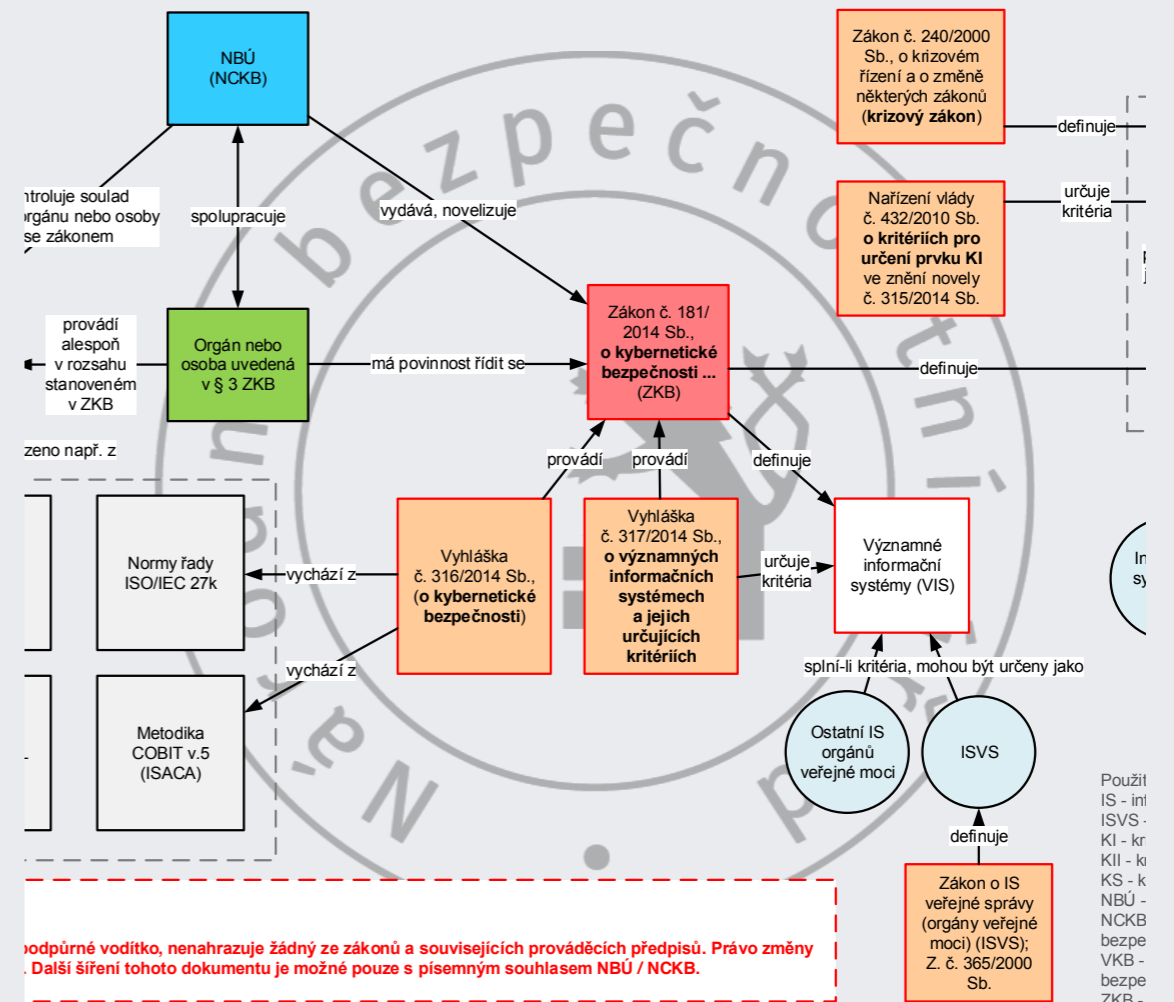
Kryptografie

- Asymetrická krypto: 2048 bitů, ECC 256 bitů.
- Symetrická krypto:
 - přecházet na AES
 - AES, 3DES, Blowfish, Twofish, Kasumi, Serpent, Camelia, SNOW 2.0, SNOW 3G
- Nepoužívat SHA-1!

Chci vědět víc!

- Zákon a vyhlášky
- NCKB - govcert.cz
- Dále: kybernetickyzakon.cz, zakonyprolidi.cz

KYBERNETICKÉ BEZPEČNOSTI Schéma k zákonu a jeho prováděcím předpisům



Názory?
Dotazy?