Zákon o kybernetické bezpečnosti základní přehled

Luděk Novák

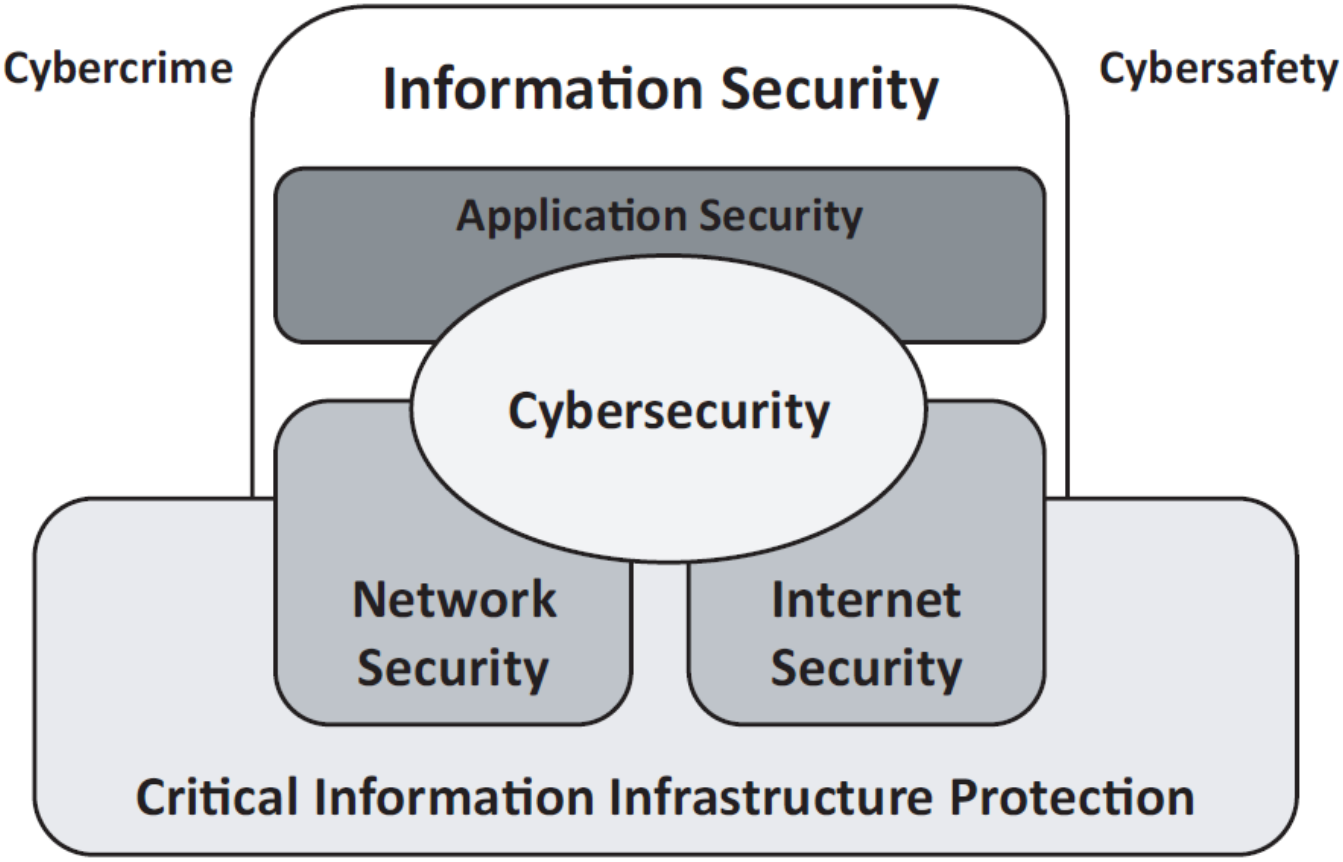
ludekn@email.cz, 603 248 295

Obsah

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- **Vyhláška č. 316/2014 Sb., vyhláška o kybernetické bezpečnosti**
- Nařízení vlády č. 432/2011 Sb., o kritériích pro určení prvku kritické infrastruktury (ve znění nařízení vlády č. 315/2014 Sb.)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Závěr

© Luděk Novák, ludekn@email.cz

Chápání kybernetické bezpečnosti



Zdroj: ISO/IEC 27032:2012

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

- Základní regulace kybernetického prostředí
- Navazuje na zákon č. 240/2000 Sb., o krizovém řízení
- Úrovně významnosti IS
  - Kritická informační infrastruktura – vládní CERT
  - Významný informační systém – vládní CERT
  - Poskytovatel služby nebo sítě elektronických komunikací – národní CERT
- Určuje pravomoci státu (NBÚ)
  - Určení přiměřená míra bezpečnosti – vyhlášky a kontrolní činnost
  - Opatření NBÚ – varování, reaktivní a ochranná opatření
  - Stav kybernetického nebezpečí
- Povinnosti orgánů a osob
  - Hlášení kontaktních údajů (do 31. ledna 2015)
  - Hlášení bezpečnostních incidentů (nejpozději od 1. 1. 2016)
  - Realizace bezpečnostních opatření (jen KII a VIS do 31. 12. 2015)
- Základ pro vybudování vládního CERT (NCKB) a národního CERT (CZ.NIC?)

http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6688

Vyhláška č. 316/2014 Sb., vyhláška o kybernetické bezpečnosti

- Základem je dobrá praxe spojená s ISO/IEC 27001
- Určuje způsob realizace organizačních a technických opatření
- Rozlišuje primární aktiva (pohled business) a podpůrná aktiva (pohled IT) – 4 úrovně
- Východiskem posouzení přiměřenosti je hodnocení a zvládání rizik – riziko f(dopad, hrozba, zranitelnost)
- Rozdělení incidentů a další podrobnosti (formuláře, formy hlášení apod.)

http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6757

Organizace vyhlášky

- Úvodní ustanovení
- Bezpečnostní opatření
  - Organizační opatření
  - Technická opatření
  - Bezpečnostní dokumentace
- Kybernetický bezpečnostní incident
- Reaktivní opatření a kontaktní údaje
- Účinnost
- Přílohy

© Luděk Novák, ludekn@email.cz

Přehled organizačních opatření

§ 3 Systém řízení bezpečnosti informací

§ 4 Řízení rizik

§ 5 Bezpečnostní politika

§ 6 Organizační bezpečnost

§ 7 Stanovení bezpečnostních požadavků pro dodavatele

§ 8 Řízení aktiv

§ 9 Bezpečnost lidských zdrojů

§ 10 Řízení provozu a komunikací

§ 11 Řízení přístupu a bezpečné chování uživatelů

§ 12 Akvizice, vývoj a údržba

§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů

§ 14 Řízení kontinuity činností

§ 15 Kontrola a audit KII a VIS

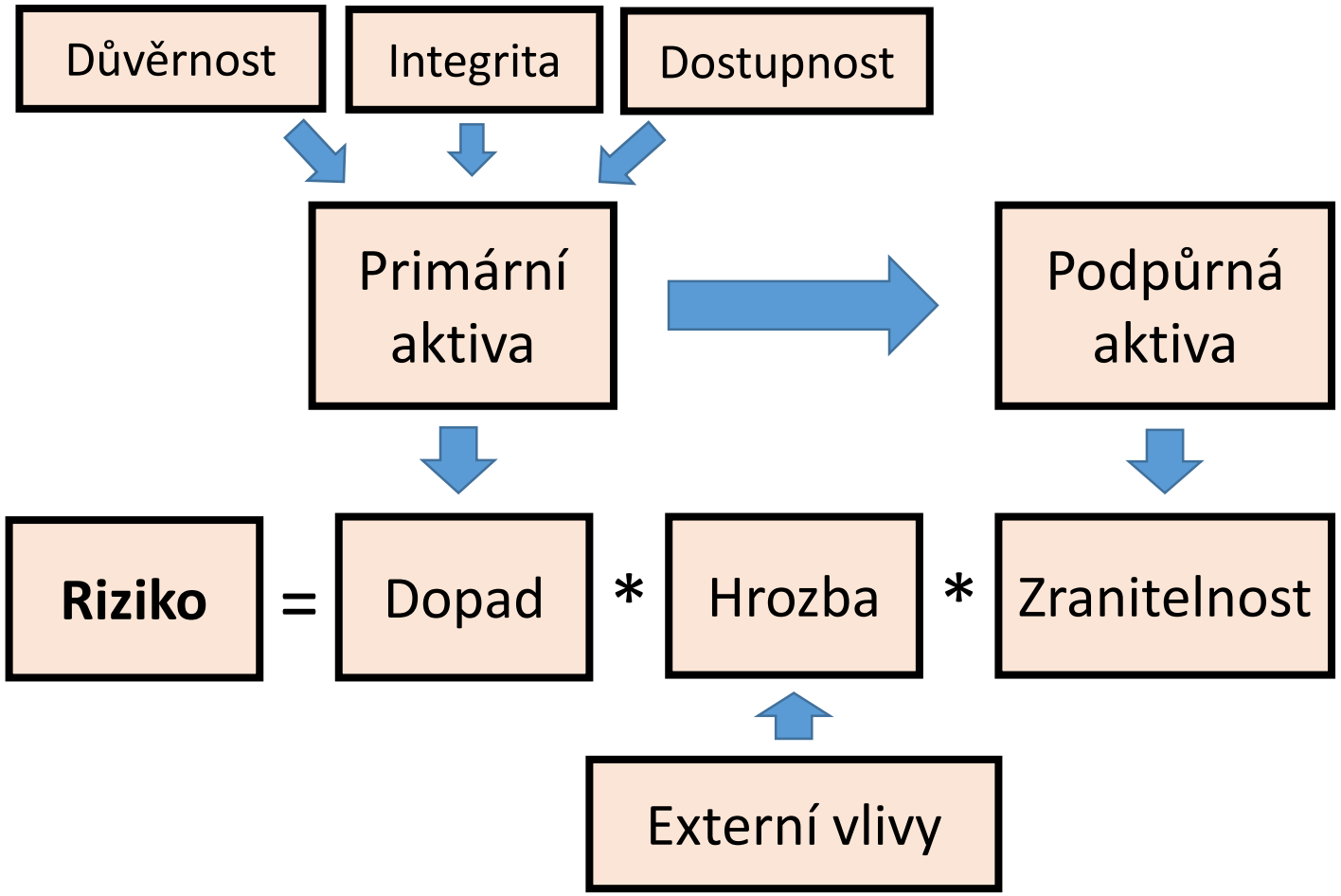
Systém řízení bezpečnosti informací

- Stanovení rozsahu a hranic
- Bezpečnostní politika – cíle, potřeby
- Monitorování účinnosti bezpečnostních opatření
- Vyhodnocuje vhodnost a přiměřenost bezpečnostní politiky
- Provedení auditu kybernetické bezpečnosti
- Vyhodnocení účinnosti ISMS
- Aktualizace ISMS
- Řízení provozu a zdrojů

Řízení rizik

- Metodika identifikace a hodnocení aktiv a rizik
- Identifikace a hodnocení aktiv (viz příloha 1)
- Identifikace a hodnocení rizik (viz příloha 2)
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik – cíle, odpovědná osoba, zdroje, termín
- Reaktivní a ochranná opatření NBÚ
- Výčet hrozeb a zranitelností

Model řízení rizik



© Luděk Novák, ludekn@email.cz

Bezpečnostní politika

- Systém řízení bezpečnosti informací
- Organizační bezpečnost
- Řízení vztahů s dodavateli
- Klasifikace aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Bezpečné chování uživatelů
- Zálohování a obnova
- Bezpečná výměna informací
- Řízení technických zranitelností
- Bezpečnost mobilních zařízení
- Licence software
- Dlouhodobé ukládání a archivace
- Ochrana osobních údajů
- Fyzická bezpečnost
- Bezpečnost komunikační sítě
- Ochrana před malware
- Nasazení a použití IDS/IPS
- Využití a údržba SIEM
- Používání kryptografické ochrany

Organizační bezpečnost

- Vymezení základních rolí
  - Výbor kybernetické bezpečnosti
  - Manažer kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Auditor kybernetické bezpečnosti
  - Garant aktiva
- Odborné školení

Bezpečnostní požadavky pro dodavatele

- Pravidla pro zapojení dodavatelů
- Smlouva jako doklad rozsahu zapojení
  - Hodnocení rizik před uzavřením smlouvy
  - Dohoda u úrovni bezpečnosti služeb
  - Pravidelné hodnocení rizik a kontrola opatření

Řízení aktiv

- Identifikace a evidence primárních aktiv
- Určení garantů primárních aktiv
- Určení důležitosti z hlediska důvěrnosti, integrity, dostupnosti
- Identifikace a evidence podpůrných aktiv
- Určení garantů podpůrných aktiv
- Určení vazeb mezi primárními a podpůrnými aktivy
- Pravidla ochrany pro jednotlivé úrovně a jejich zavedení

Bezpečnost lidských zdrojů

- Plán rozvoje bezpečnostního povědomí
- Poučení uživatelů, administrátorů atd.
- Kontrola dodržování pravidel
- Vrácení svěřených aktiv
- Evidence školení – předmět + účastníci
- Pravidla pro určení osob
- Hodnocení účinnosti plánu rozvoje povědomí
- Řešení případů poručení pravidel
- Změna oprávnění při změně pozice

Řízení provozu a komunikací

- Vyhodnocení provozních informací
- Provozní pravidla a postupy
- Pravidelné zálohování + prověření použitelnosti
- Oddělení provozního prostředí od testovacího a vývojového
- Řešení reaktivních opatření
- Integrita komunikačních sítí
- Pravidla ochrany pro sítě
- Smlouva pro předávání informací

Řízení přístupu a bezpečné chování uživatelů

- Řízení přístupů na základě potřeb
- Ochrana údajů určených pro přihlašování
- Samostatný identifikátor pro přihlášení
- Omezení administrátorských oprávnění
- Přidělování práv podle politiky
- Nástroje pro ověřování identity

© Luděk Novák, ludekn@email.cz

Akvizice, vývoj a údržba

- Bezpečnostní požadavky na změny systémů
- Identifikace , hodnocení a řízení rizik spojených s akvizicí, vývojem a údržbou
- Bezpečnost vývojového prostředí
- Provádí testování bezpečnosti

Zvládání kybernetických událostí a incidentů

- Opatření pro oznámení incidentů na vládní CERT
- Prostředí pro vyhodnocení událostí a incidentů
- Klasifikace hlášení a přijímání opatření pro minimalizaci dopadů
- Určení příčin bezpečnostních incidentů a stanovení nutných opatření
- Dokumentace

Řízení kontinuity činností

- Práva a povinnosti garantů, administrátorů a bezp. rolí
- Cíle řízení kontinuity
  - Minimální úroveň služeb
  - Doba obnovení chodu (RTO)
  - Doba obnovení dat (RPO)
- Strategie kontinuity
- Vyhodnocení dopadů a rizik kontinuity
- Stanovení a testování plánů kontinuity
- Opatření pro zvýšení odolnosti vůči výpadkům
- Stanovení a aktualizace postupů pro opatření NBÚ

Kontrola a audit

- Posouzení souladu
- Provedení a dokumentace kontrol

- Kontrola zranitelnosti technických prostředků

© Luděk Novák, ludekn@email.cz

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 KII a VIS, jejich uživatelů a administrátorů

§ 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 úrovně dostupnosti

§ 27 Bezpečnost průmyslových a řídicích systémů

© Luděk Novák, ludekn@email.cz

Technická opatření a technologie

Fyzická bezpečnost
- CCTV, integrace bezpečnosti do datových sítí

Nástroj pro ochranu integrity komunikačních sítí
- Firewall, router, VPN, VLAN, …

Nástroj pro ověřování identity uživatelů
- Čipové karty, biometrika, AD/LDAP, TACACS, RADIUS

Nástroj pro řízení přístupových oprávnění
- AAA, DLP, ARM, …

Nástroj pro ochranu před škodlivým kódem
- Antiviry, řízení technických zranitelností, …

Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů
- Syslog servery, podpora vyhodnocení, …

Technická opatření a technologie

Nástroj pro detekci kybernetických bezpečnostních událostí
- IDS/IPS

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- SIEM

Aplikační bezpečnost
- Aplikační firewall, bezpečnostní testy

Kryptografické prostředky
- TSL/SSL, SSH, VPN, …

Nástroje pro zajištění úrovně dostupnosti
- HA, clustery, robustnost (odolnost vůči DDoS)

Bezpečnost průmyslových a řídicích systémů
- SCADA, …

Kybernetický bezpečnostní incident

§ 30 Typy kybernetických bezpečnostních incidentů

- Podle příčiny - fyzická poškození, škodlivý SW, útoky, porušením opatření, kompromitací informací …
- Podle dopadu na důvěrnost, integritu a dostupnost

§ 31 Kategorie kybernetických bezpečnostních incidentů

- Kategorie III – velmi závažný kybernetický incident
- Kategorie II – závažný kybernetický incident
- Kategorie I – méně závažný kybernetický incident

§ 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

Přílohy

Příloha 1: Hodnocení a úrovně důležitosti aktiv

Příloha 2: Hodnocení rizik

Příloha 3: Minimální požadavky na kryptografické algoritmy

Příloha 4: Struktura bezpečnostní dokumentace

Příloha 5: Formulář pro hlášení kybernetického bezpečnostního incidentu

Příloha 6: Formulář oznámení o provedení reaktivního opatření a jeho výsledku

Příloha 7: Formulář pro hlášení kontaktních údajů

Nařízení vlády č. 432/2011 Sb., o kritériích pro určení prvku KI
(ve znění nařízení vlády č. 315/2014 Sb.)

- Stanoví průřezová a odvětvová kritéria pro určení kritické infrastruktury
- Průřezová kritéria
  - > 250 mrtvých nebo > 2.500 raněných s hospitalizací 24h
  - ztráta státu > 0,5% DHP (cca 20 miliard CZK)
  - neposkytnutí nezbytných služeb pro > 125 000 osob
- Odvětvová kritéria
  - Řeší různé odvětví včetně kritické informační infrastruktury
  - Systémy veřejné moci s osobními údaji >300.000 osob

http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6757

© Luděk Novák, ludekn@email.cz

Vyhláška č. 317/2014 Sb., o VIS a jejich určujících kritériích

- Vymezuje významné informační systémy
- Dopadová určující kritéria
  - omezení výkonu veřejné moci >3 pracovní dny
  - >10 mrtvých nebo >100 raněných
  - ztráta >5% rozpočtu orgánu veřejné moci
  - zásah do osobního života > 50.000 osob
- Oblastní určující kritéria
  - 92 vyjmenovaných VIS

http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6757

© Luděk Novák, ludekn@email.cz

Závěr

- Zákon o kybernetické bezpečnosti byl schválen a platí – na diskusi a kritiku je pozdě
- Požadavky zákona a vyhlášek jsou věcné a lze je racionálně obhájit
  - Může pomoci v rozvoji bezpečnosti
  - Stanovená opatření jsou realistická
- Velkou pozitivní roli sehrává NBÚ – cíl zlepšení stavu bezpečnosti