# Kybernetický zákon

## Aspekty a konsekvence zákona o kybernetické bezpečnosti

ISSS 2015
jitesar@cisco.com
14. dubna 2015

# Kybernetický zákon a vyhlášky

# Legislativa

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

  Publikováno 29. srpna 2014 ve sbírce zákonů č. 181/2014

  Účinnost od 1. ledna 2015

- **Prováděcí právní předpisy** k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti

  Publikováno v prosinci 2014 ve sbírce zákonů č. 315/2014, č. 316/2014, č. 317/2014

  Nařízení nabývá účinnosti 1. ledna 2015

# Zákon o kybernetické bezpečnosti

## Předpis 181/2014 Sb.
## Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

- Vymezení pojmů
- Definuje Práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

  Subjekty, orgány a osoby, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti
- Systém zajištění kybernetické bezpečnosti

  Organizační a technická bezpečnostní opatření pro zajištění bezpečnosti informací, spolehlivosti a dostupnosti služeb

  Opatření prevence nebo řešení: varování, reaktivní, ochranná

  Hlášení a evidence kybernetické bezpečnostní události a bezpečnostního incidentu, kontaktní údaje

  Národní a vládní CERT – podmínky provozování

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 315/2014 Sb.
## Kritéria pro určení prvku kritické infrastruktury

Prvky kritické infrastruktury:

- Energetika
  - Elektřina, Zemní plyn, Ropa a ropné produkty, Centrální zásobování teplem
- Vodní hospodářství
- Potravinářství a zemědělství
  - Rostlinná výroba, Živočišná výroba, Potravinářská výroba
- Zdravotnictví

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 315/2014 Sb.
## Kritéria pro určení prvku kritické infrastruktury

Prvky kritické infrastruktury:

- Doprava
  - Silniční doprava, Železniční doprava, Letecká doprava
- Komunikační informační systémy
  - Technologické prvky pevné a mobilní sítě el. komunikací, Rozhlasové a televizní vysílání, Satelitní komunikace, Poštovní služby, Technologické prvky informačních systémů (např. provoz domény .cz), Oblast kybernetické bezpečnosti (např. podpůrné systémy jiných prvků KI, informační systém s osobními údaji o více než 300 tis. osobách)

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 315/2014 Sb.
## Kritéria pro určení prvku kritické infrastruktury

Prvky kritické infrastruktury:

- Finanční trh a měna
- Nouzové služby
  - Integrovaný záchranný systém, Radiační monitorování, Předpovědní, varovná a hlásná služba
- Veřejná správa
  - Veřejné finance (např. finanční, celní správa), Sociální ochrana a zaměstnanost (např. sociální zabezpečení, podpora), Zpravodajské služby

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 316/2014 Sb.
## Vyhláška o kybernetické bezpečnosti

Bezpečnostní opatření

- Systém řízení bezpečnosti informací
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Řízení přístupu a bezpečné chování uživatelů
- Akvizice, vývoj a údržba
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Kontrola a audit kritické informační infrastruktury a významných informačních systémů

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 316/2014 Sb.
## Vyhláška o kybernetické bezpečnosti

Technická opatření

- Fyzická bezpečnost
- Nástroj pro ochranu integrity komunikačních sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti
- Bezpečnost průmyslových a řídících systémů

# Prováděcí předpisy k zákonu o kyber. bezp.

Nařízení vlády 316/2014 Sb.
Vyhláška o kybernetické bezpečnosti

Bezpečnostní dokumentace

- Dokumentace
- Prokázání certifikace

Kybernetický bezpečnostní incident

- Typy kybernetických bezpečnostních incidentů (podle příčiny nebo dopadu)
- Kategorie kybernetických bezpečnostních incidentů (III - velmi závažný, II - závažný, I - méně závažný)
- Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

# Prováděcí předpisy k zákonu o kyber. bezp.

Nařízení vlády 316/2014 Sb.
Vyhláška o kybernetické bezpečnosti

Příloha č. 1 - Hodnocení a úrovně důležitosti aktiv, stupnice pro:

- Hodnocení důvěrnosti
- Hodnocení integrity
- Hodnocení dostupnosti

Příloha č. 2. Hodnocení rizik (riziko = dopad x hrozba x zranitelnost), stupnice pro:

- Hodnocení dopadů
- Hodnocení hrozeb
- Hodnocení zranitelností

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 316/2014 Sb.
## Vyhláška o kybernetické bezpečnosti

Příloha č. 3 – Minimální požadavky na kryptografické algoritmy

- Symetrické algoritmy
  - Blokové a proudové šifry pro ochranu důvěrnosti a integrity (3DES limity 168b - 10GB, 112b - 10MB, přechod na AES)
  - Módy pro ochranu integrity (HMAC, CMAC,..)
- Asymetrické algoritmy
  - Digitální podpis (DSA/RSA 2048b a více, EC-DSA 224b a více)
  - Výměna klíčů (DH/RSA 2048b a více, Elliptic Curve 224b a více.)
- Algoritmy hash funkcí
  - SHA-2, SHA-3
  - SHA-1 pouze na ověřování již existujících digitálních podpis, nesmí být použito pro generování nových podpisů

# Prováděcí předpisy k zákonu o kyber. bezp.

Nařízení vlády 316/2014 Sb.
Vyhláška o kybernetické bezpečnosti

Příloha č. 4 – Struktura bezpečnostní dokumentace

- Struktura bezpečnostní politiky
- Formát auditní zprávy
- Plán zvládání rizik
- Strategie řízení kontinuity činností
- atd.

Příloha č. 5 – Formulář hlášení kybernetického bezpečnostního incidentu

Příloha č. 6 – Formulář o provedení reaktivního opatření a jeho výsledku

Příloha č. 7 – Formulář pro hlášení kontaktních údajů

# Prováděcí předpisy k zákonu o kyber. bezp.

## Nařízení vlády 317/2014 Sb.
## Vyhláška o významných informačních systémech a jejich určujících kritériích

VIS naplňují kritéria:

- Dopadová - úplná nebo částečná nefunkčnost informačního systému způsobená narušením bezpečnosti informací by mohla mít negativní vliv na:
  - Fungování, poskytování služeb, hospodaření orgánu veřejné moci
  - Ohrožení nebo narušení prvku KI
  - Oběti na životech (10) nebo zranění osob (100)
  - Finanční nebo materiální ztráty, atd. (s mezní hodnotou více než 5 % stanoveného rozpočtu orgánu veřejné moci)
  - Zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50 000 osob

Celkem 92 subjektů (ministerstva, telekomunikační, zeměměřičský, katastrální,. úřad, policie ČR, atd.)

# Prováděcí předpisy k zákonu o kyber. bezp.

Nařízení vlády 317/2014 Sb.
Vyhláška o významných informačních systémech a jejich určujících kritériích

## VIS naplňují kritéria:

- Oblastní (u orgánů veřejné moci)
  - Databáze obsahující osobní údaje
  - Spisová služba
  - Státní dozor
  - Kontrolní a inspekční činnost
  - Tvorba právních předpisů
  - Elektronická pošta
  - Vedení internetových stránek
  - Zadávání veřejných zakázek
  - Státní statistická služba
  - atd.

# VIS a KII = různé úrovně zabezpečení

VIS - Významný Informační Systém

KII – Kritická Informační Infrastruktura

KS – Komunikační Systém (KS-VIS)

IS – Informační Systém (IS-VIS, IS-KII)

- V základní rovině jsou požadavky na KII i VIS identické.
- V některých konkrétních bodech jsou u KII (KS i IS) zvýšené požadavky na bezpečnost oproti VIS (IS)

# Technická bezpečnostní opatření dle zákona o kybernetické bezpečnosti

# § 16 Fyzická bezpečnost

- VIS i KII – zamezení neoprávněnému vstupu, zamezení poškození a zásahům, kompromitace aktiv

- KII – ochrana objektů, ochrana vymezených prostor s technickými aktivy, ochrana jednotlivých technických aktiv

- Prostředky fyzické bezpečnosti – mechanické zábranné, EZS, systémy pro kontrolu vstupu, kamerové systémy, ochrana před výpadkem el. en., systémy pro zajištění optimálních provoz. podmínek

# Matice technologického souladu

- Řešení fyzické bezpečnosti
  - kamerové systémy
  - EZS
  - čipové ověřování
  - biometrické ověřování
  - …

# § 17 Nástroj pro ochranu integrity komunikačních sítí

- VIS i KII – ochrana integrity rozhraní vnější a vnitřní sítě
  - řízení bezpečného přístupu mezi vnější a vnitřní sítí
  - segmentace pomocí DMZ => dojde ke zvýšení bezpečnosti aplikací v DMZ a k zamezení přímé komunikace mezi vnější a vnitřní sítí
  - šifrování vzdáleného přístupu a u přístupu  pomocí bezdrátových technologií
  - odstranění nebo blokování informací, které neodpovídají požadavkům na ochranu integrity KS

- KII - ochrana integrity vnitřní sítě její segmentací (DMZ ...)

# Matice technologického souladu

- Ochrana integrity komunikačních sítí
  - Firewally (Cisco, SourceFire, …)
  - IPS (Cisco, SourceFire, …)
  - síťové aktivní prvky (Cisco, …)
  - design od certifikovaných systémových engineerů
  - …






# § 18 Nástroj pro ověřování identity uživatelů

- VIS+KII – nástroje pro ověření identity musí zajistit
  - Ověření identity všech uživatelů a administrátorů
  - Minimální délka hesla je 8 znaků
  - Minimální složitost hesla vyžaduje alespoň jedno velké písmeno, jedno malé písmeno, jednu číslici a jeden speciální znak
  - Maximální doba platnosti hesla je 100 dní

# Matice technologického souladu

- Ověřování identity uživatelů
  - Cisco ISE
  - Cisco ACS
  - RSA tokens
  - MS Active Directory
  - LDAP
  - ...

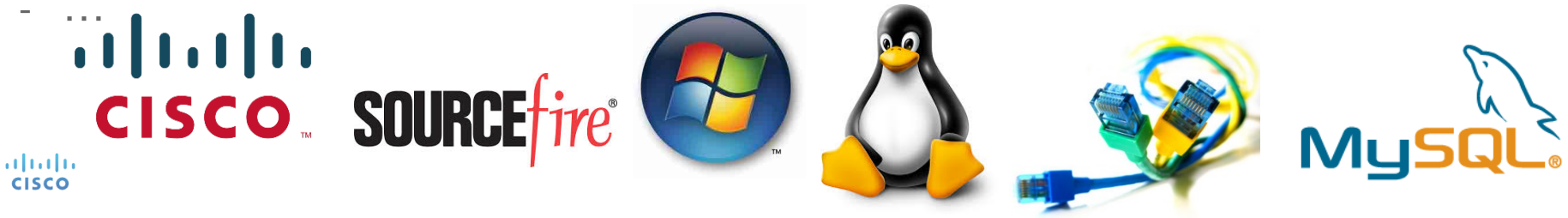

# § 19 Nástroj pro řízení přístupových oprávnění

- VIS i KII – musí se použít nástroje pro řízení přístupových oprávnění, které musí zajistit
  - Řízení oprávnění uživatelů pro přístup k aplikacím a datovým souborům
  - Řízení oprávnění pro čtení, zápis dat a pro změna oprávnění

- KII – povinnost zaznamenávat použití přístupových oprávnění

# Matice technologického souladu

- Nástroj pro řízení přístupových oprávnění
  - Policy Server (ISE)
  - IPS (Cisco, SourceFire, …)
  - Firewally (Cisco, SourceFire, …)
  - 802.1x, BYOD
  - Definice práv na úrovni aplikací a operačních systémů
  - …



# § 20 Nástroj pro ochranu před škodlivým kódem

- VIS i KII – povinnost použití nástrojů pro antivirovou ochranu
  - Ověření a kontrola komunikace mezi vnější a vnitřní sítí
  - Ověření a kontrola serverů a sdílených datových uložišť
  - Ověření a kontrola pracovních stanic
  - Požadavek na pravidelnou aktualizaci definic a signatur

# Matice technologického souladu

- Ochrana před škodlivým kódem
  - Email a Web Security řešení (Cisco ESA a WSA)
  - Anvirus a antimalware řešení pro koncové stanice
  - Specializovaná síťová antimalware řešení (SourceFire, AMP, ThreatGrid)
  - …




# § 21 Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů

VIS i KII – má povinnost použit nástroje pro zaznamenávání činností, které zajistí

- sběr informací o provozních a bezpečnostních událostech

- Zaznamenání zejména událostí
  - typ činnosti
  - přesný čas události
  - identifikace technického aktiva, který činnost zaznamenal
  - identifikace původce a místa činnosti
  - úspěšnost či neúspěšnost činnosti

- Ochranu informací před neoprávněným čtením a změnou

# § 21 Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů

- VIS i KII zaznamenání
  - přihlášení a odhlášení uživatelů a administrátorů
  - činnosti provedené administrátory
  - činnosti vedoucí k navýšení oprávnění
  - neúspěšné činnosti
  - spuštění a ukončení práce systému
  - varovná  nebo chybová hlášení
  - přístupy logům
  - pokus o manipulaci s logy
  - použití mechanismů autentizace, včetně změn údajů k přihlášení
  - neprovedené činnosti v důsledku nedostatku oprávnění

# Matice technologického souladu

- Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů

- AAA (ISE, ACS), Sec. Management (Prime, CSM)
- Firewally (Cisco, SourceFire, …)
- IPS (Cisco, SourceFire, …)
- 802.1x, BYOD
- Definice práv na úrovni aplikací a operačních systémů



# § 22 Nástroj pro detekci kybernetických bezpečnostních událostí (KBU)

- VIS i KII
  - povinnost použití nástroje pro detekci KBU
  - zajistění ověření, kontroly a případné blokování komunikace mezi vnitřní a vnější sítí
- KII
  - ověření, kontrola a případné blokování komunikace v rámci vnitřní komunikační sítě
  - ověření, kontrola a případné blokování komunikace v rámci určených serverů

# Matice technologického souladu

- Detekce bezpečnostních událostí

- Cisco a SourceFire bezpečnostní prvky (FW, Content GW, IPS/IDS)
- AMP, ThreatGrid, CTA
- LanCope StealthWatch
- INVEA FlowMon
- Arbor Networks DDoS
- ...






# § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (KBU)

- KII
  - povinné použití nástroje pro sběr a vyhodnocení KBU
  - poskytnutí informací o KBU bezpečnostním rolím
  - nepřetržité vyhodnocování KBU
  - stanovení bezp. politiky pro použití a údržbu nástroje
  - pravidelná aktualizace nastavených pravidel pro zpřesnění chodu nástroje pro vyhodnocování KBU
  - zajištění využívání získaných informací o KBU k optimalizaci bezpečnostních vlastností ICT

# Matice technologického souladu

- Sběr a vyhodnocení bezpečnostních událostí
  - SourceFire FireSight Management Center
  - SIEM systémy: RSA Envision, AccelOps, LogRhytm, Splunk
  - ...






# § 24 Aplikační bezpečnost

- VIS i KII – provádí se bezpečnostní testy aplikací, které jsou přístupné z vnější sítě před uvedením do provozu a po každé zásadní změně bezpečnostních mechanizmů
- KII – zajišťuje ochranu aplikací a informací dostupných z vnějších sítí
  - neoprávněnou činnosti
  - popřením provedených činností
  - kompromitací nebo neautorizovanou změnou
  - transakcí před nedokončením, nesprávným směrováním, neautorizovanou změnou, kompromitací, neautorizovaným duplikováním, opakováním

# Matice technologického souladu

- Aplikační bezpečnost
  - Aplikační inspekce FW (Cisco, SourceFire …)
  - Dynamická analýza (AMP, ThreatGrid)
  - IPS (Cisco, SourceFire)
  - Specializované aplikační FW (F5)
  - Auditovací a penetrační nástroje
  - …

# § 25 Kryptografické prostředky

- VIS i KII – stanovení politiky pro používání kryptografické ochrany
  - Typ a síla kryptografického algoritmu
  - Ochrana citlivých dat při přenosu po komunikačních sítích, při uložení na mobilní zařízení nebo na vyměnitelná média

  - Povinnost kryptografickými prostředky zajistit
    - Ochranu důvěryhodnosti a integrity předávaných nebo ukládaných dat
    - Prokázání odpovědnosti za provedené činnosti

# § 25 Kryptografické prostředky

- KII – stanovení požadavků na správu a minimálních požadavků na sílu šífrovacích klíčů
  - Symetrické algoritmy
    - AES (128,192,256), RC4 (min. 128), SNOW 2.0 (128,256) …
    - Omezené použití pro 3DES (168) ... => migrace na AES
  - Šifrovací módy pro integritu dat
    - HMAC, CBC-MAC-EMAC,CMAC
    - Omezené použití pro CBC-MAC-X9.19
  - Asymetrické algoritmy
    - DSA (min. 2048,224), EC-DSA (min. 224), RSA PSS (min. 2048)
    - SHA1 nepoužívat k novým podpisům, pouze ke kontrole starých
    - Diffie-Hellman (min.2048,224)
    - ECDH (min.224), ECIES-KEM (min.256), PSEC-KEM (min.256), (ACE-KEM (min.256), RSA-OAEP (min. 2048), RSA-KEM (min.2048)
  - Algoritmy hash funkcí
    - SHA2 (SHA-224, SHA-256, SHA-384, SHA-512/224, SHA-512/256)
    - RIPEMD-160
    - Whirpool

# Matice technologického souladu

- Definice vysokých standardů kryptografických prostředků

- Prvky s podporou požadovaných standardů (Cisco VPN klient, směrovače, FW, AAA server - ISE)
- MDM pro mobilní zařízení (MobileIron, Air-Watch)
- …

# § 26 Nástroje pro zajištění vysoké úrovně dostupnosti

- KII – použití nástrojů pro vysokou úroveň dostupnosti a odolnosti, které zajistí
  - Potřebnou úroveň kontinuity činností
  - Odolnosti vůči útokům (KBU) na snížení dostupnosti
  - Redundanci důležitých prvků KII
    - Využitím redundance v návrhu
    - Vytvořením skladu náhradních technických aktiv
    - Pomocí servisní smlouvy zajišťující výměnu vadných technických aktiv v definovaném čase

# Matice technologického souladu

- Zajištění vysoké úrovně dostupnosti
  - Redundancí kritických komponent
  - Rozsáhlý servisní sklad u dodavatele
  - Rychlý servis prvků v režimu 24/7/365

# § 27 Bezpečnost průmyslových a řídicích systémů

- KII
  - Omezení fyzického přístupu k průmyslovým a řídícím systémům
  - Omezení propojení a vzdáleného přístupu k průmyslovým a řídícím systémům
  - Ochrana jednotlivých technických aktiv před známými zranitelnostmi
  - Obnovení chodu po kybernetickém bezpečnostním incidentu

# Materiály a odkazy

# Dokumenty ke stažení

- Zákon č. 181 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)


CISCO
TOMORROW starts here.