DIGITÁLNÍ ČESKO

INSTITUT PRO POLITIKU A SPOLEČNOST

DIGITAL CZECH REPUBLIC

Impact of Digital Revolution on the Czech Republic

16. 1. 2017
Prague

KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE

Jaroslav Šmíd
náměstek ředitele NBÚ

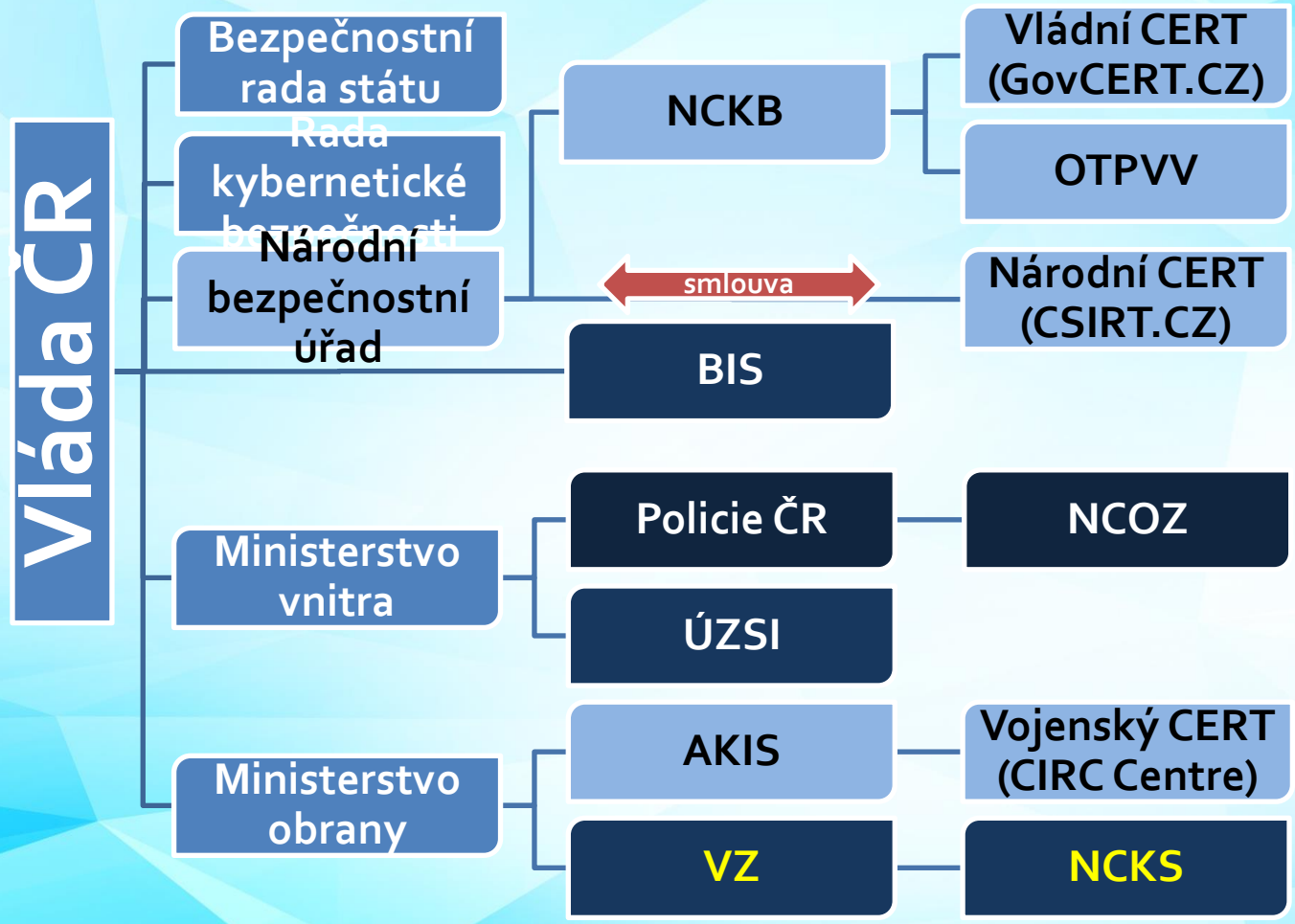
NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

- Byl zřízen 1. srpna 1998 na základě zákona č. 148/1998 Sb., O ochraně utajovaných skutečností
- Rozhoduje o vydání osvědčení fyzické osoby/podnikatele a o vydání dokladu o bezpečnostní způsobilosti fyzické osoby a o zrušení platnosti osvědčení fyzické osoby/podnikatele a dokladu
- Má v kompetenci ochranu utajovaných informací
- Provádí certifikace technických prostředků, informačních systémů, kryptografických zařízení, sítí, apod.
- Je zodpovědný za kryptografickou ochranu utajovaných informací (vyvíjí a schvaluje národních šifrové algoritmy a vytváří národní politiku kryptografické ochrany, atd.)

HISTORIE: KYBERNETICKÁ BEZPEČNOST

- NBÚ / NCKB – civilní, nevojenská agentura
- 19. října 2011 NBÚ ustaven Vládou ČR jako gestor kybernetické bezpečnosti a národní autorita v této oblasti
- Spolu s tím byla přijata Strategie pro kybernetickou oblast ČR 2012 – 2015 a Akční plán
- a také byla ustavena Rada kybernetické bezpečnosti (poradní orgán předsedy vlády ČR)
- 1. ledna 2015 – Zákon o kybernetické bezpečnosti
- Únor 2015 – Národní strategie kybernetické bezpečnosti ČR 2015 - 2020

ORGANIZAČNÍ RÁMEC



ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

ZÁKLADNÍ RYSY

Kdo je povinen dle Zákona?

- **Kritická informační infrastruktura (KII)**

prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti

- **Významné informační systémy (VIS)**

informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon činnosti veřejné správy

- *Definováno v rámci Zákonu o kybernetické bezpečnosti*

ZÁKLADNÍ RYSY (pokrač.)

Povinnosti:

- Hlásit kontaktní údaje
- Hlásit kybernetické bezpečnostní incidenty
- Implementovat kybernetická bezpečnostní opatření (standardizace)
- Přijímat opatření vydávaná NBÚ

Sankce:

Pokud povinný subjekt…

- neimplementuje bezpečnostní opatření
- neuchovává bezpečnostní dokumentaci
- nenahlásí kybernetické bezpečnostní incidenty
- nerealizuje protiopatření vydané NBÚ
- nenahlásí kontaktní informace nebo změny těchto informací

- **NBÚ nyní připravuje novelu ZKB s ohledem na:**
  - **Transpozici směrnice NIS v ČR**
  - **Praktické zkušenosti, které vyplynuly ze zkušeností s implementací ZKB**
  - **Vytvoření Národního centra kybernetické a informační bezpečnost**

NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2015 AŽ 2020

- 16. února 2015 schválena Vládou ČR
- Srovnání s NSKB 2012 – 2015:
kvalitativní posun od budování základních kapacit směrem k hlubšímu a pokročilému zajišťování kybernetické bezpečnosti
- Cílena především na veřejný sektor
a kritickou informační infrastrukturu (KII)

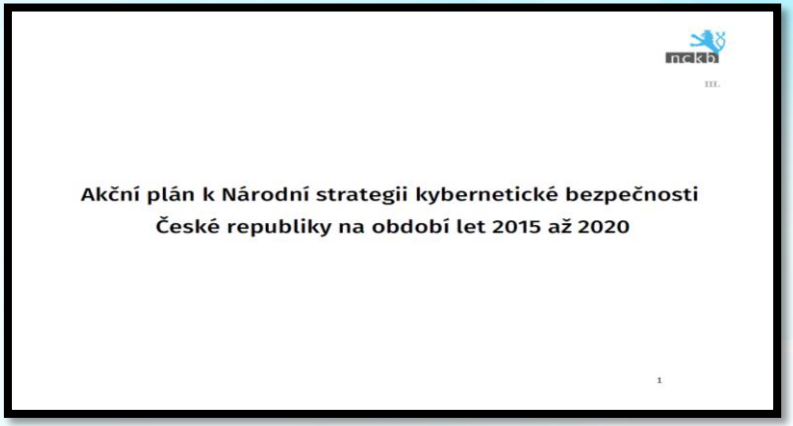
KLÍČOVÉ OBLASTI NSKB 2015 – 2020

- Chránit národní KII a VIS
- Aktivně spolupracovat se zahraničními partnery
- Bojovat efektivněji s informační kriminalitou
- Vybudovat a posilovat národní schopnosti v kybernetické obraně
- Zajistit bezpečný kyberprostor stimulující českou ekonomiku
- Zvyšovat osvětu a digitální gramotnost české společnosti a podporovat vzdělávání

AKČNÍ PLÁN k NSKB 2015 - 2020

- Vychází z hlavních cílů Strategie
- Přijat vládou ČR v květnu 2015
- **Obsah:**
  - definuje konkrétní kroky
  - stanovuje termíny plnění
  - určuje odpovědné subjekty
- **141 úkolů pro 17 subjektů:**

  NBÚ/NCKB, MO, MZV, MV,
  MPO, MF, MŠMT, MPSV, MS, VZ,
  BIS, ÚZSI, TAČR, PČR, VP, ÚV ČR a ČTÚ



NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI:

- Odbor vládní CERT GOVCERT.CZ

- Odbor kybernetických bezpečnostních politik

GOVCERT.CZ

- Veřejný sektor a kritická informační infrastruktura
- Členění týmu
  - Reaktivní oddělení
  - Vývoj a bezpečnostní testování
  - Oddělení síťové analýzy
  - Analytické oddělení
- Základní služby
  - Proaktivní: koordinační činnost v rámci komunity a informační HUB
  - Detekční: schopnosti detekce anomálií
  - Reaktivní: reakce na incidenty, zpracování artefaktů
- Zaměření týmu
  - SCADA/ICS systémy
  - Penetrační testování
  - Forenzní činnost
  - Analýza malwaru a reverzní inženýrství
  - …

AKTUÁLNÍ PROJEKTY

- Koordinační centrum pro české bezpečnostní týmy
  - Videokonference se stálými i ad-hoc členy
  - Řešení rozsáhlých bezpečnostních útoků
- Nový webový portál
  - Veřejná a neveřejná část
  - Neveřejné fórum pro bezpečnostní týmy a další organizace
- Příprava technického cvičení Cyber Czech 2016
  - Red/blue tým cvičení s více než 60 účastníky
  - Unikátní cvičení v Evropě
- Forenzní laboratoř a penetrační testování

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI:

Odbor kybernetických bezpečnostních politik

ZÁKLADNÍ INFORMACE

- Připravuje dlouhodobou strategii a poskytuje analýzu, výzkum, expertízu, včetně věcných i právních doporučení k zajištění, aby NCKB, potažmo ČR plnila všechny stanovené cíle v oblasti zajišťování kybernetické bezpečnosti, a to co nejefektivnějším způsobem

- Kontinuálně analyzuje strategické dopady, hrozby a výzvy vycházející z kybernetické bezpečnostního prostředí

- Zajišťuje efektivní koordinaci a harmonizaci kybernetických bezpečnostních politik napříč veřejnou sférou a dalšími soukromoprávními subjekty povinnými dle Zákona.

PLNĚNÍ MEZINÁRODNÍCH ZÁVAZKŮ

- **EU** – kybernetická diplomacie, NIS směrnice, atd.
- **ENISA** – členství v ENISA Management Board, zástupce v expertní skupině na národní strategie kybernetické bezpečnosti
- **OSCE** – opatření pro zvyšování důvěry mezi státy v kyberprostoru

PLNĚNÍ MEZINÁRODNÍCH ZÁVAZKŮ (pokrač.)

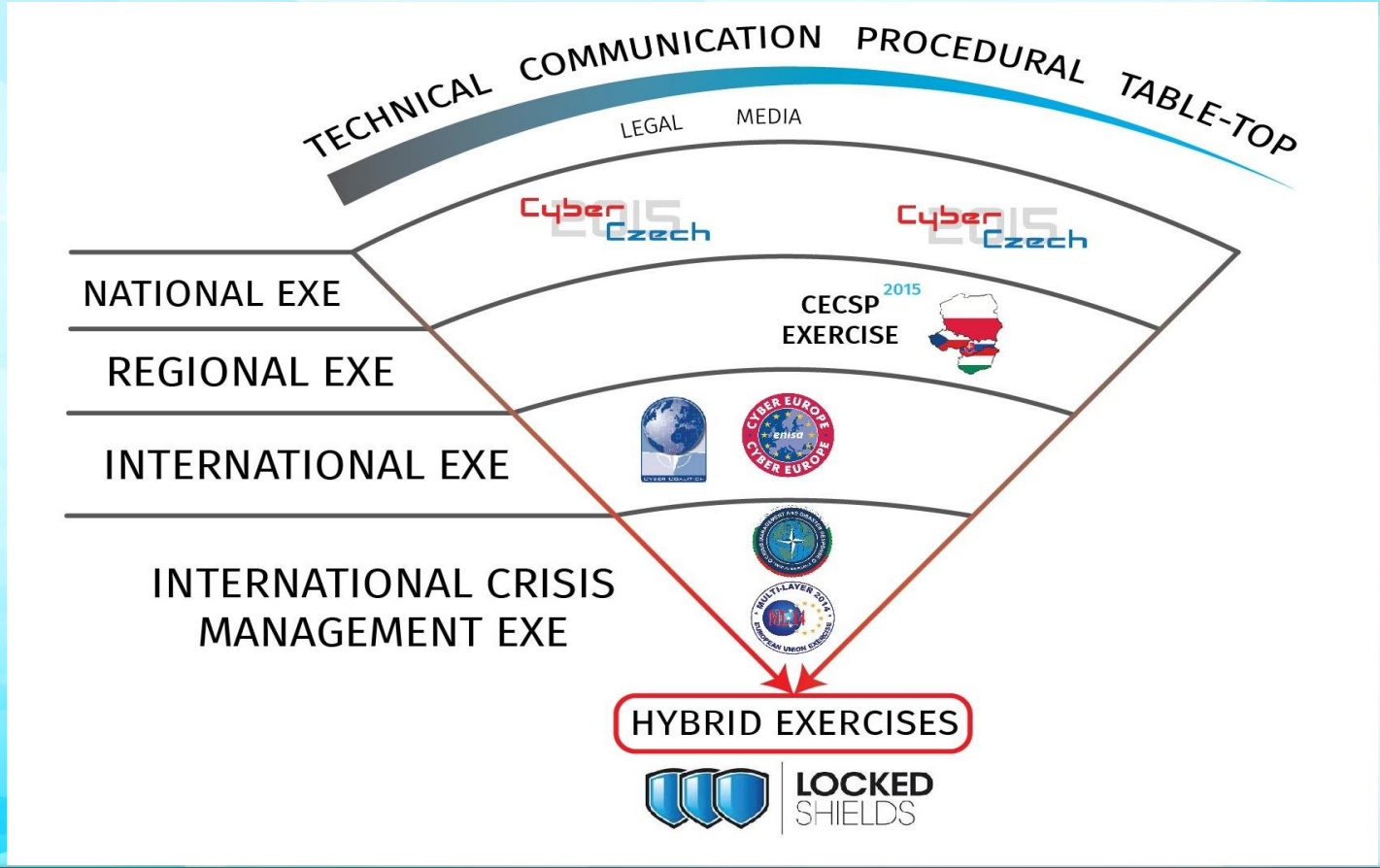
- CECSP – Středoevropské platformy pro kybernetickou bezpečnost, založilo NBÚ
- NATO – kontaktní bod pro kybernetickou obranu
  - Memorandum ohledně spolupráce v kybernetické obraně
  - Zastupování ČR v Cyber Defence Committee
- CCDCOE – 1 stálý zástupce v Tallinnu, Estonsko

MAPOVÁNÍ A URČOVÁNÍ KII A VIS

- Určování KII:
  - KII ve veřejném sektoru – NBÚ navrhne Ministerstvu vnitra zařadit IS nebo KS do seznamu, který bude následně předložen vládě ČR. Vláda ČR rozhodne usnesením a navrhovaný IS nebo KS určí.
  - KII v soukromém sektoru – vydávána opatření obecné povahy (OPP)
- Určování VIS:
  - Jedná se pouze o systémy orgánů veřejné moci
  - Naplnění kritérií posuzuje sám správce informačního systémů – Kritéria pro významné informační systémy jsou stanovena vyhláškou o významných informačních systémech, která zároveň uvádí jejich výčet

NCKB:

KYBERNETICKÁ BEZPEČNOSTNÍ CVIČENÍ


TECHNICAL
COMMUNICATION
PROCEDURAL
TABLE-TOP
LEGAL
MEDIA
Cyber Czech
Cyber Czech
NATIONAL EXE
REGIONAL EXE
INTERNATIONAL EXE
INTERNATIONAL CRISIS MANAGEMENT EXE
CECSP 2015 EXERCISE
HYBRID EXERCISES
LOCKED SHIELDS

Děkuji za pozornost!

Jaroslav Šmíd

náměstek ředitele NBÚ

www.nbu.cz

www.govcert.cz

j.smid@nbu.cz