NBÚ/NCKB: NÁRODNÍ AUTORITA KYBERNETICKÉ BEZPEČNOSTI

Daniel Bagge
Národní centrum kybernetické bezpečnosti

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

- Dříve v gesci MV
- 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

VÝZNAMNÉ MILNÍKY (od roku 2011)

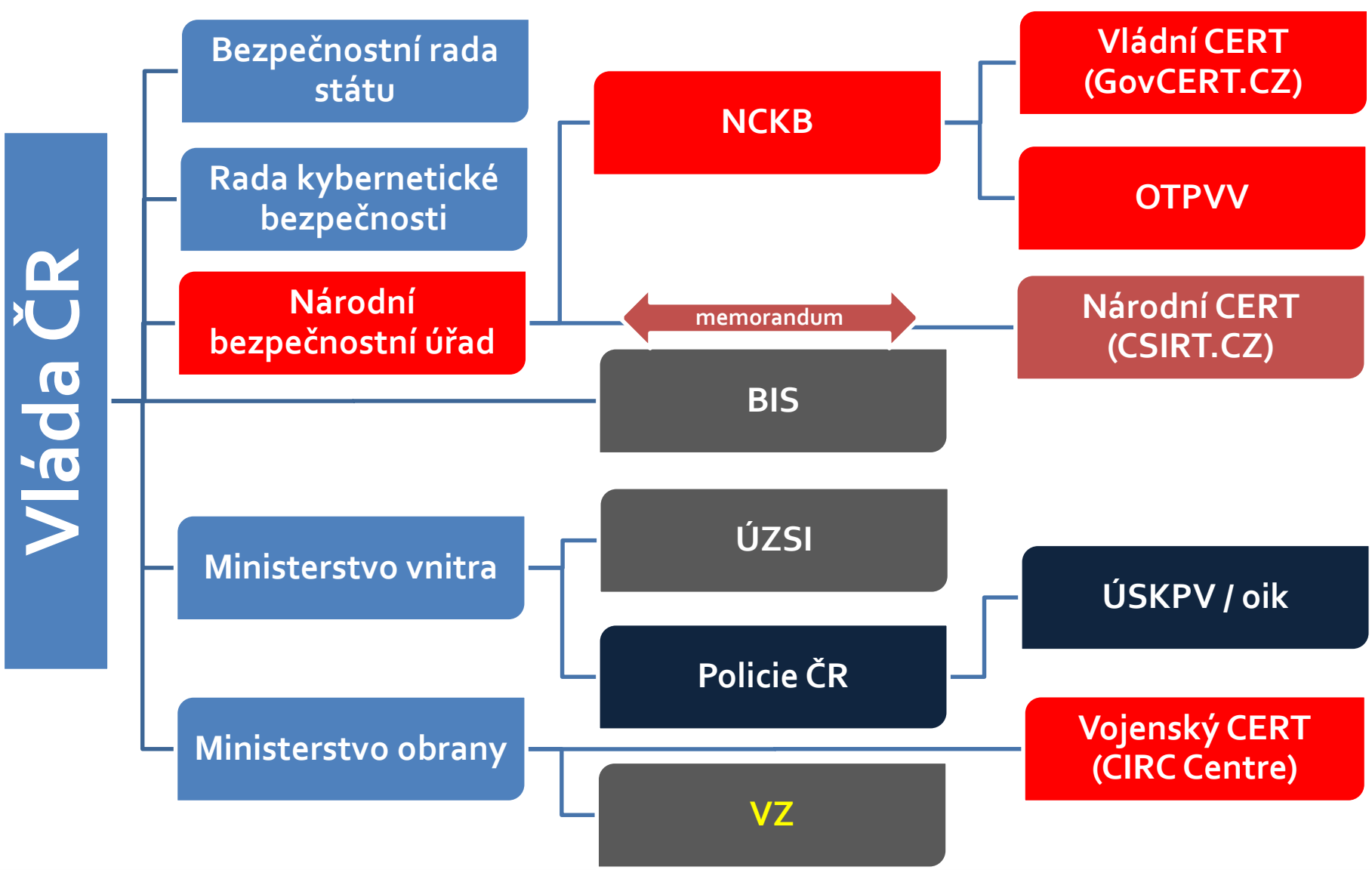
1. Přijetí Zákona o kybernetické bezpečnosti
2. Vybudování Národního centra kybernetické bezpečnosti a GovCERT.CZ (součástí NCKB)
3. NSKB 2012 – 2015 (všechny hlavní cíle realizovány či průběžně plněny)
4. Přijetí nové NSKB 2015 – 2020 a Akčního plánu

STRATEGICKO-PRÁVNÍ RÁMEC

AKTUÁLNÍ STRATEGICKO-PRÁVNÍ RÁMEC

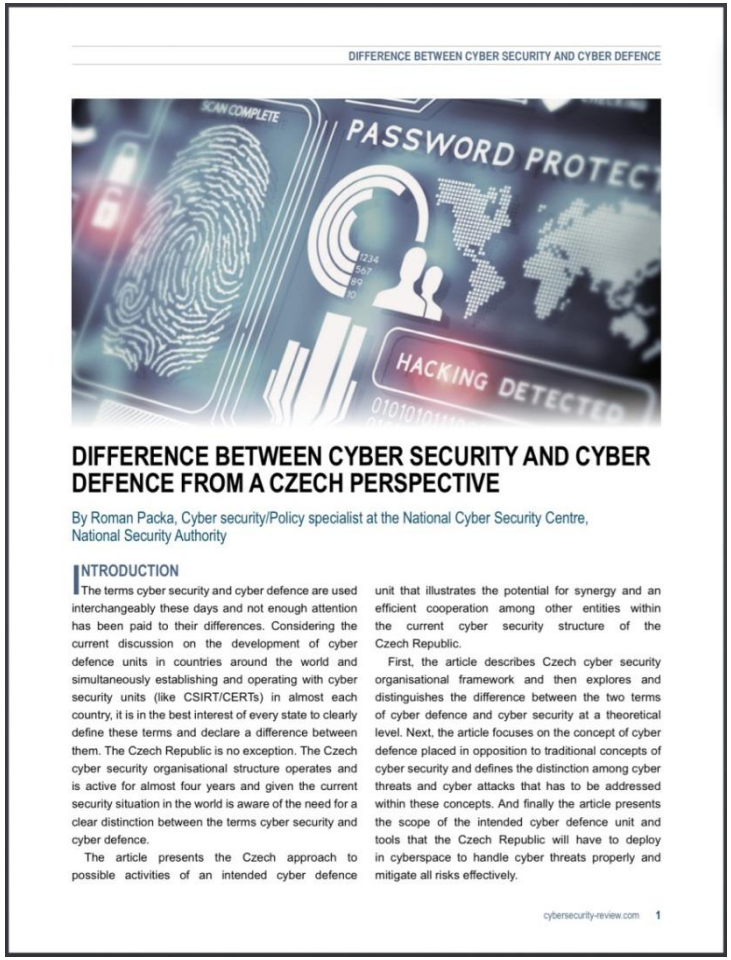
- Bezpečnostní strategie ČR (aktualizace 2015)
- Národní strategie kybernetické bezpečnosti ČR pro období let od 2015 až 2020
  - Akční plán k Národní strategii kybernetické bezpečnosti ČR pro období let od 2015 až 2020
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
  - Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
  - Vyhláška o stanovení významných informačních systémů a jejich určujících kritériích

ORGANIZAČNÍ RÁMEC


Vláda ČR
Bezpečnostní rada státu
Rada kybernetické bezpečnosti
Národní bezpečnostní úřad
NCKB
Vládní CERT (GovCERT.CZ)
OTPVV
memorandum
Národní CERT (CSIRT.CZ)
BIS
Ministerstvo vnitra
ÚZSI
Policie ČR
ÚSKPV / oik
Ministerstvo obrany
Vojenský CERT (CIRC Centre)
VZ

KYBERNETICKÁ BEZPEČNOST/OBRANA/KRIMINALITA – český přístup

- **BEZPEČNOST** – široké spektrum bezpečnostních oblastí, zahrnuje všechny preventivní a reaktivní aktivity státu v oblasti ochrany dat, informací, systémů, služeb a sítí ve smyslu neustálého navyšování integrity, odolnosti a robustnosti státní informační infrastruktury
- **OBRANA** – ochrana státu výhradně proti pokročilým, závažným, nepřátelským kybernetickým útokům. Mezi kybernetickou bezpečností a obranou rozlišujeme v závislosti na:
  1. povaze hrozby
  2. a typu kybernetického útoku a jeho cíli
- **KRIMINALITA** – trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat



DIFFERENCE BETWEEN CYBER SECURITY AND CYBER DEFENCE

DIFFERENCE BETWEEN CYBER SECURITY AND CYBER DEFENCE FROM A CZECH PERSPECTIVE

By Roman Packa, Cyber security/Policy specialist at the National Cyber Security Centre, National Security Authority

INTRODUCTION

The terms cyber security and cyber defence are used interchangeably these days and not enough attention has been paid to their differences. Considering the current discussion on the development of cyber defence units in countries around the world and simultaneously establishing and operating with cyber security units (like CSIRT/CERTs) in almost each country, it is in the best interest of every state to clearly define these terms and declare a difference between them. The Czech Republic is no exception. The Czech cyber security organisational structure operates and is active for almost four years and given the current security situation in the world is aware of the need for a clear distinction between the terms cyber security and cyber defence.

The article presents the Czech approach to possible activities of an intended cyber defence unit that illustrates the potential for synergy and an efficient cooperation among other entities within the current cyber security structure of the Czech Republic.

First, the article describes Czech cyber security organisational framework and then explores and distinguishes the difference between the two terms of cyber defence and cyber security at a theoretical level. Next, the article focuses on the concept of cyber defence placed in opposition to traditional concepts of cyber security and defines the distinction among cyber threats and cyber attacks that has to be addressed within these concepts. And finally the article presents the scope of the intended cyber defence unit and tools that the Czech Republic will have to deploy in cyberspace to handle cyber threats properly and mitigate all risks effectively.

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

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

OBSAH NSKB 2015 - 2020

1. Vize
2. Principy
3. Výzvy
4. Hlavní cíle

1. VIZE

- Dlouhodobé vize a priority ČR v oblasti kybernetické bezpečnosti
  - Aktivně pomáhat svým mezinárodním partnerům, plnit závazky vyplývající z členství v mezinárodních organizacích, kolektivní obrany Severoatlantické aliance
  - Podporovat spolupráci a dialog zemí středoevropského regionu skrze mezinárodní organizace, jejichž je členem
  - Hladce fungující informační společnost
  - Patřit mezi přední státy se silnou expertízou a znalostmi na zabezpečení industriálních systémů
  - …

2. PRINCIPY

- Základní principy, které stát následuje při zajišťování kybernetické bezpečnosti v ČR
  - Ochrana základních lidských práv a svobod a principů demokratického právního státu
  - Komplexní přístup ke kybernetické bezpečnosti založený na principu subsidiarity a spolupráce
  - Budování důvěry a spolupráce mezi veřejným a soukromým sektorem a občanskou společností
  - Rozvoj kapacit k zajišťování kybernetické bezpečnosti

3. VÝZVY

1. Česká republika jako možný testovací objekt
2. Nedostatečná důvěra veřejnosti ve stat
3. Vzrůstající počet uživatelů internetu, informačních a komunikačních technologií a narůstající kritičnost jejich selhání
4. Se vzrůstajícím počtem uživatelů mobilních platforem stoupá i množství mobilního malware
5. Možnosti zneužití zadních vrátek hardware pro exfiltraci informací
6. Koncept „internetu věcí“
7. Bezpečnostní rizika spjatá s přechodem z protokolu IPv4 na IPv6
8. Bezpečnostní rizika spjatá s elektronizací veřejné správy (eGovernment)
9. Nedostatečné zabezpečení malých a středních podniků

3. VÝZVY (pokrač.)

10. Big data, skladování dat v nových prostředích
11. Ochrana průmyslových řídicích systémů a informačních systémů ve zdravotnictví
12. Inteligentní energetické sítě
13. Vzrůstající závislost obranných složek státu na informačních a komunikačních technologiích
14. Malware je stále sofistikovanější
15. Botnety a DDoS/DoS útoky
16. Nárůst informační kriminality
17. Hrozby a rizika spjaté s užíváním sociálních sítí na internetu
18. Nízká digitální gramotnost koncových uživatelů
19. Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství

4. HLAVNÍ CÍLE

I. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti
II. Aktivní mezinárodní spolupráce
III. Ochrana národní KII a VIS
IV. Spolupráce se soukromým sektorem

4. HLAVNÍ CÍLE (pokrač.)

V. Výzkum a vývoj / Spotřebitelská důvěra

VI. Podpora vzdělávání, osvěta a rozvoj informační společnosti

VII. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu

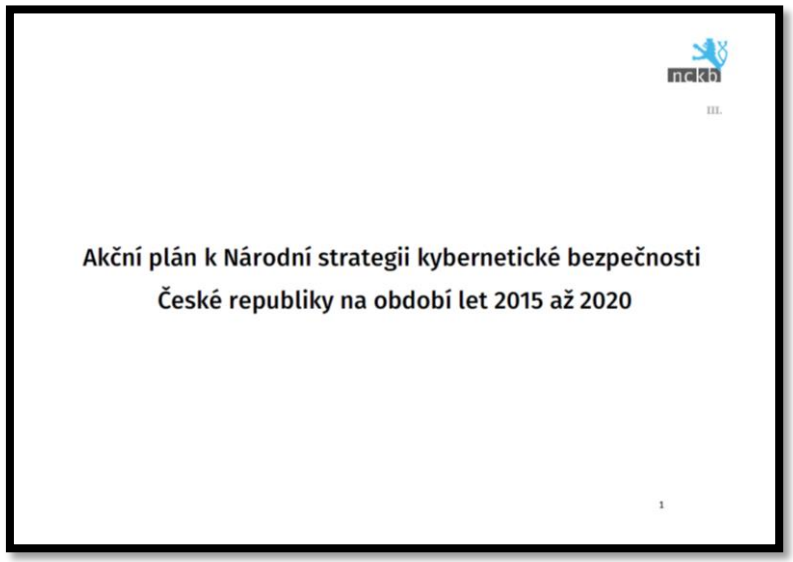
VIII. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce). Účast na tvorbě a implementaci evropských a mezinárodních pravidel

AKČNÍ PLÁN K NSKB 2015 – 2020

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



AKČNÍ PLÁN k NSKB 2015 – 2020: NÁHLED

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti				
Vytvořit efektivní model spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti – pracoviště typu CERT a CSIRT, subjekty KII apod. – a posilovat jejich stávající struktury a procesy.	**A.1.01**	Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO MPO Zpravodajské služby	Q3 2015
	A.1.02	Provést analýzu agend v rámci problematiky kybernetické bezpečnosti a na jejím základě definovat národní zájmy a priority v této oblasti.	NBÚ/NCKB *ve spolupráci s:* MO MZV MPO Zpravodajské služby	Q4 2015
	A.1.03	Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	průběžně

Implementace NSKB a Akčního plánu

- Společná jednání se všemi partnery ohledně implementace Strategie a Akčního plánu, která se konají 2x ročně
- Agenda: sledovat, diskutovat a hodnotit úroveň plnění jednotlivých úkolů Akčního plánu
- Každý rok – informace Vládě ČR ohledně stavu implementace Strategie a Akčního plánu formou přílohy ke Zprávě o stavu kybernetické bezpečnosti ČR

PROCES VYTVÁŘENÍ NSKB 2015 – 2020

NCSS 2015 – 2020 DEVELOPMENT LIFECYCLE

Initiation phase

- Content analysis of NCSSs in the Europe
- Studying guidelines (ENISA, NATO, national level)
- Evaluation of the previous NCSS
- Considering the structure
- Taking a stock of existing policies, legal/strategic documents
- Identyfing stakeholders
- Setting vision, scope and priorities

Drafting phase

- Engaging stakeholders
- Applying guidelines, analysis and other conlusions
- Drafting

NCSS draft

Commenting phase

- Compliance check
- Informal (internal and external) comments

NCSS proposal

- Interministerial (official) commenting procedure + settlement

Approval phase

- National Security Council approval

Government approval

NEW NCSS

NCSS 2015 – 2020 DEVELOPMENT TIMELINE

Initiation phase

- Q4 2013 – Q1 2014

Drafting phase

- Q2 2014: DRAFT

Commenting phase

- Q2 2014: Internal and external (informal) comments
- AUG 14: Interministerial commenting procedure
- SEP 14: Comment settlement

Approval phase

- 22 DEC 14: National Security Council approval
- 16 FEB 15: **Government approval**

Execution of the Strategy

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI:

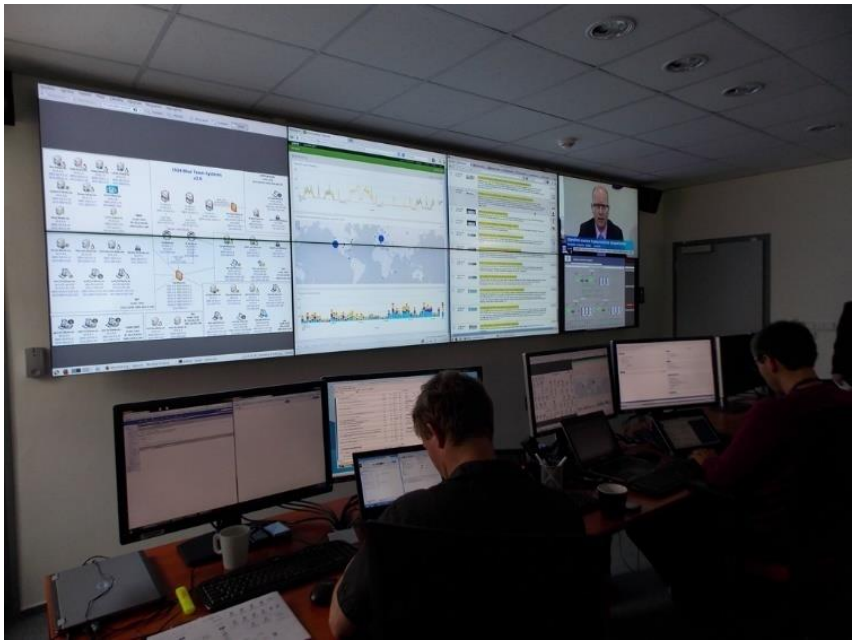
GOVCERT.CZ

ZÁKLADNÍ INFORMACE

- GovCERT.CZ – vládní CERT (Computer Emergency Response Team)
- Chrání kritické prvky národní infrastruktury
- Působnost: Veřejná správa a kritická informační infrastruktura
- Slouží v ČR jako hlavní kontaktní bod v oblasti kybernetické bezpečnosti a ve spolupráci s Národním CERT (CSIRT.CZ, spravován CZ.NIC – nekritická, soukromá sféra) zajišťuje na top úrovni kybernetickou bezpečnost ČR

ZÁKLADNÍ INFORMACE (pokrač.)

- Počet zaměstnanců: 12
- Členění týmu:
  - reaktivní oddělení
  - oddělení vyhledávání
  - analytické oddělení



- Základní služby:
  - proaktivní: koordinační činnost v rámci komunity a informační HUB, schopnosti detekce anomálií
  - reaktivní: reakce na incidenty, zpracování artefaktů

SCHOPNOSTI GovCERT.CZ

- Pomoc s technickým řešením incidentu (incident handling); navázání komunikace s jiným subjektem;
- ICS/SCADA (SCADA laboratoř);
- Open Source Intelligence (OSINT);
- Klientské honeypoty;
- Síťová bezpečnost a analýza síťového provozu;
- Penetrační testování;
- Forenzní analýza;
- Analýza malwaru a reverzní inženýrství;

*** Bližší seznámení s činností GovCERT.CZ: 27.10.2015**

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI: OTPVV

ZÁKLADNÍ INFORMACE

- Počet zaměstnanců: 11
- 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
  - Příprava nového memoranda 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 (ve 3 vlnách) – současný stav:

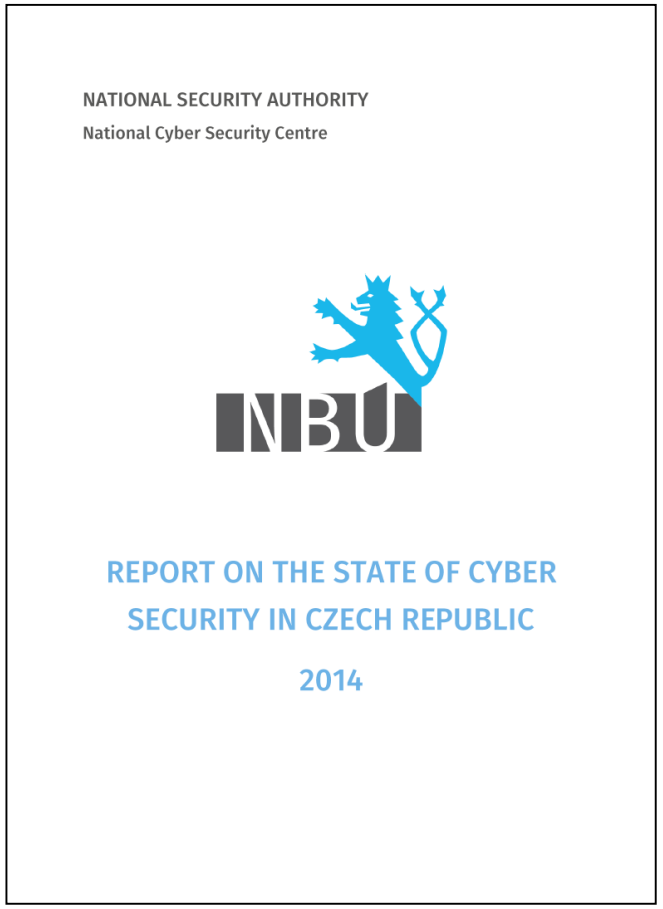
1. vlna – kritické informační/komunikační systémy státní správy – ústřední správní úřady určené jako kritické pro zajištění základních služeb státu – identifikováno 45 informačních/komunikačních systémů splňující kritéria stanovená pro KII, které spravuje 14 subjektů státní správy – DOKONČENO
2. vlna – zbývající část státní správy – PROBÍHÁ
3. vlna – kritická informační infrastruktura v soukromém sektoru – vydána první opatření obecné povahy (OPP) = 17 prvků KII u 10 subjektů (datum nabytí účinnosti zítra, tj. 9.října 2015) a další OOP se připravují

MAPOVÁNÍ A URČOVÁNÍ KII A VIS

- 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
- Současný stav:
  - v příloze vyhlášky 92 VIS provozováno 35 veřejnými subjekty (oficiální počet)
  - Do KII však přeřazeno 22 systémů a 19 nově identifikovaných = NBÚ momentálně eviduje 89 VIS (nejde o konečný počet)
- Předpokládána aktualizace seznamu VIS

VYTVÁŘENÍ A AKTUALIZACE STRATEGICKÝCH A DALŠÍCH ZÁSADNÍCH DOKUMENTŮ

- Národní strategie kybernetické bezpečnosti a Akční plán
- Každoroční zpracovávání Zprávy o stavu kybernetické bezpečnosti ČR
- Zpracovávání analýz / komentářů a podpora ostatním subjektům v otázkách kybernetické bezpečnosti

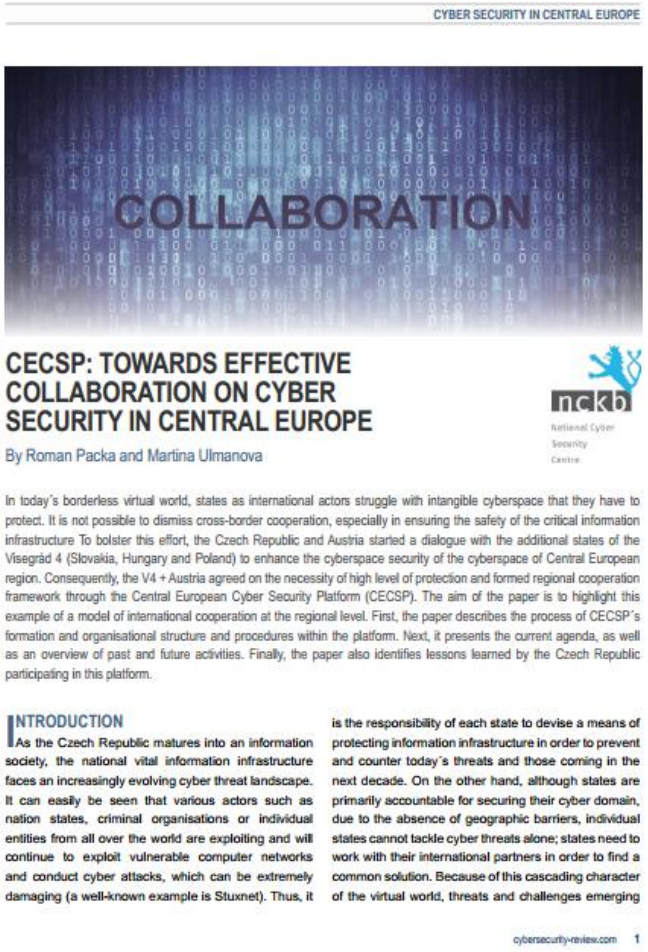


DALŠÍ AKTIVITY

- Prezentování aktivit NCKB na národní i mezinárodní úrovni (konference, semináře, videokonference)

DALŠÍ AKTIVITY

- Publikační činnost:
  - PAČKA, R. (2015): The Real Dawn of the Age of Cyber Warfare. In Diplomatic Courier.
  - PAČKA, R. (2015): Difference Between Cyber Security and Cyber Defence from a Czech Perspective. In Cyber Security Review.
  - BAGGE, D. (2014): Regional cyber security: The case of the Czech Republic. In Journal of European Security and Defense Studies.
  - PAČKA, R. – ULMANOVÁ, M. (2014): CECSP: Towards Effective Collaboration on Cyber Security in Central Europe. In Cyber Security Review.
  - BAGGE, D. (2014): Global nature of cyber security threat: Czech perspective, cooperation with industry, academia and international stakeholders. In Cyber Security Review.
  - Etc.
- Poskytování pracovních stáží vysokoškolským studentům
- Podpora aktivit GovCERT.CZ (právní a věcná podpora GovCERT.CZ při incident/event handlingu)



CYBER SECURITY IN CENTRAL EUROPE

COLLABORATION

CECSP: TOWARDS EFFECTIVE COLLABORATION ON CYBER SECURITY IN CENTRAL EUROPE

By Roman Packa and Martina Ulmanova

In today's borderless virtual world, states as international actors struggle with intangible cyberspace that they have to protect. It is not possible to dismiss cross-border cooperation, especially in ensuring the safety of the critical information infrastructure To bolster this effort, the Czech Republic and Austria started a dialogue with the additional states of the Visegrád 4 (Slovakia, Hungary and Poland) to enhance the cyberspace security of the cyberspace of Central European region. Consequently, the V4 + Austria agreed on the necessity of high level of protection and formed regional cooperation framework through the Central European Cyber Security Platform (CECSP). The aim of the paper is to highlight this example of a model of international cooperation at the regional level. First, the paper describes the process of CECSP´s formation and organisational structure and procedures within the platform. Next, it presents the current agenda, as well as an overview of past and future activities. Finally, the paper also identifies lessons learned by the Czech Republic participating in this platform.

INTRODUCTION

As the Czech Republic matures into an information society, the national vital information infrastructure faces an increasingly evolving cyber threat landscape. It can easily be seen that various actors such as nation states, criminal organisations or individual entities from all over the world are exploiting and will continue to exploit vulnerable computer networks and conduct cyber attacks, which can be extremely damaging (a well-known example is Stuxnet). Thus, it is the responsibility of each state to devise a means of protecting information infrastructure in order to prevent and counter today´s threats and those coming in the next decade. On the other hand, although states are primarily accountable for securing their cyber domain, due to the absence of geographic barriers, individual states cannot tackle cyber threats alone; states need to work with their international partners in order to find a common solution. Because of this cascading character of the virtual world, threats and challenges emerging

cybersecurity-review.com 1

BUDOUCÍ AGENDA

- **Implementace Národní strategie kybernetické bezpečnosti a Akčního plánu**
  → prohloubení a rozšíření stávající agendy
  - Hlubší kooperace s KII a VIS subjekty
  - Osvětová činnost / vzdělávací programy
  - Výzkum a vývoj
  - Hlubší spolupráce s Policií ČR v oblasti informační kriminality
  - Úzká spolupráce se zpravodajskými službami a Armádou ČR / spolupráce v rámci kybernetické obrany ČR
  - Atd.

Děkuji za pozornost!

Daniel Bagge

d.bagge@nbu.cz

www.nbu.cz

www.govcert.cz