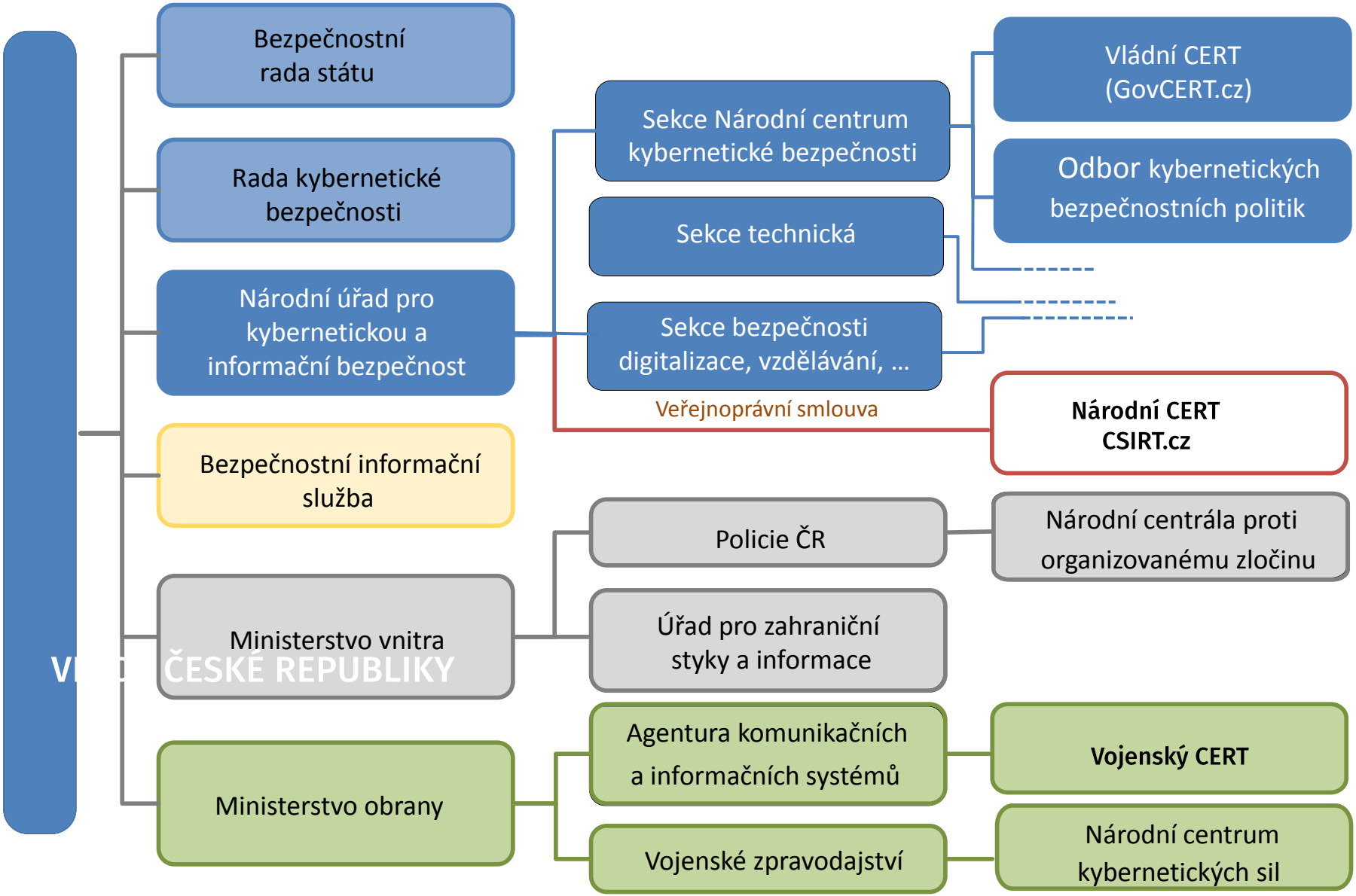
# NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
# a
# jeho role

Jaroslav ŠMÍD

Národní úřad
pro kybernetickou
a informační bezpečnost


Bezpečnostní rada státu
Rada kybernetické bezpečnosti
Národní úřad pro kybernetickou a informační bezpečnost
Bezpečnostní informační služba
Ministerstvo vnitra
Ministerstvo obrany
ČESKÉ REPUBLIKY
Sekce Národní centrum kybernetické bezpečnosti
Sekce technická
Sekce bezpečnosti digitalizace, vzdělávání, …
Veřejnoprávní smlouva
Vládní CERT (GovCERT.cz)
Odbor kybernetických bezpečnostních politik
Národní CERT CSIRT.cz
Policie ČR
Úřad pro zahraniční styky a informace
Národní centrála proti organizovanému zločinu
Agentura komunikačních a informačních systémů
Vojenské zpravodajství
Vojenský CERT
Národní centrum kybernetických sil

*Kybernetická obrana*

Ochrana kritické informační infrastruktury, ...


Kybernetická kriminalita

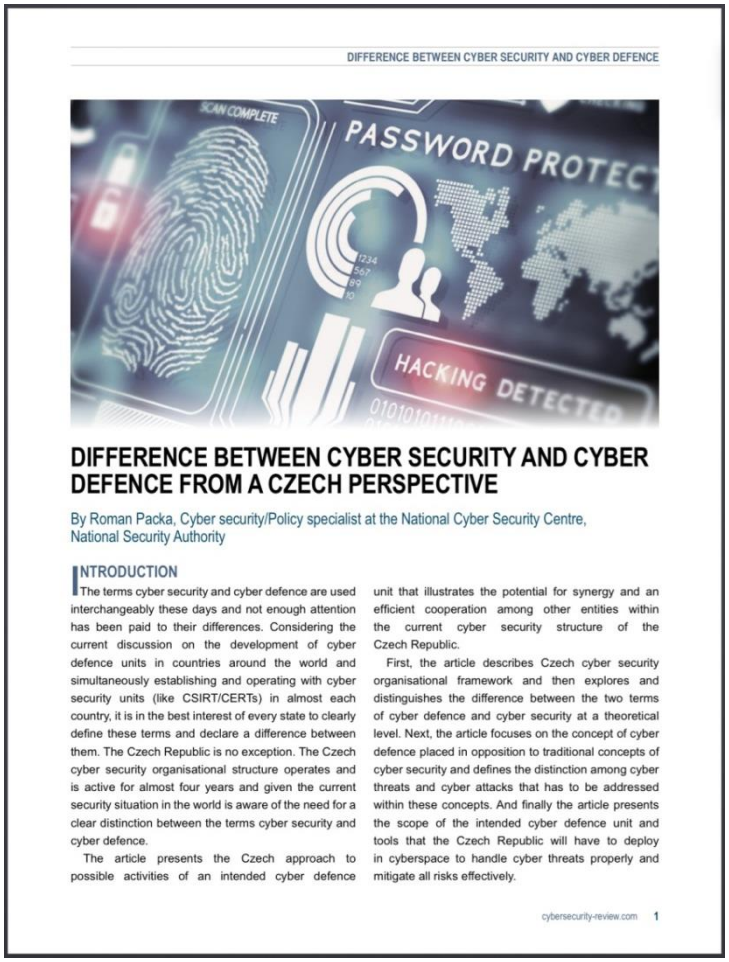

Působení zpravodajských služeb

## KYBERNETICKÁ BEZPEČNOST

- zastřešujícím termínem pro široké spektrum bezpečnostních oblastí, zahrnuje všechny preventivní a reaktivní aktivity státu v oblasti ochrany dat, informací, systémů, služeb a sítí
- smyslem je neustálé navyšování integrity, odolnosti a robustnosti informační a komunikační infrastruktury

## KYBERNETICKÁ OBRANA

- ochrana státu proti pokročilým, závažným, nepřátelským kybernetickým útokům
- smyslem je aktivní působení v kyberprostoru proti útočícím osobám a proti využívané infrastruktuře



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.


## Kybernetická kriminalita

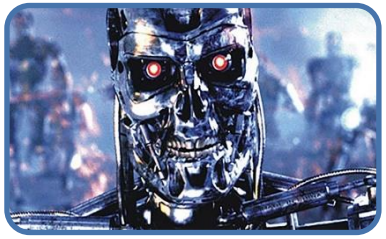
Trestná činnost, pro kterou je určující vztah k software, k datům, respektive uloženým informacím, respektive veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat

## Kybernetický terorismus

Kyberterorismus zahrnuje agresivní a excesivní jednání, které je prováděno se záměrem vyvolat strach ve společnosti, a jehož prostřednictvím je dosahováno politických, náboženských nebo ideologických cílů. Za využití kyberprostoru a informačních a komunikačních technologií ohrožuje chod státu, jeho ústavní zřízení nebo obranyschopnost mimo jiné cílením na kritickou informační infrastrukturu a významné informační systémy.


## Kybernetická špionáž

Užití/zneužití ICT s cílem získat citlivé informace bez souhlasu jeho držitele/majitele. Provádí ji státní i nestátní aktéři za účelem získání strategické, ekonomické, politické, nebo vojenské převahy.



## Kybernetická válka

Národní stát (či skupiny podporované státem) cílí na sítě a systémy jiného státu za účelem jejich zničení či narušení, způsobení škody, extrakce/zničení citlivých informací, narušení bojeschopnosti, apod. Útoky provádí především specializované vojenské/zpravodajské jednotky.

# Milníky

**2011**
- NBÚ ustanoven jako gestor KB
- vznik Národního centra kybernetické bezpečnosti

**2012**
- Národní strategie kybernetické bezpečnosti I.

**2015**
- Zákon o kybernetické bezpečnosti
- Národní strategie kybernetické bezpečnosti II.

**2016**
- Směrnice NIS

**2017**
- Novela zákona o kybernetické bezpečnosti
- Vznik NÚKIB
- Kybernetický balíček EU

NBU

nckb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

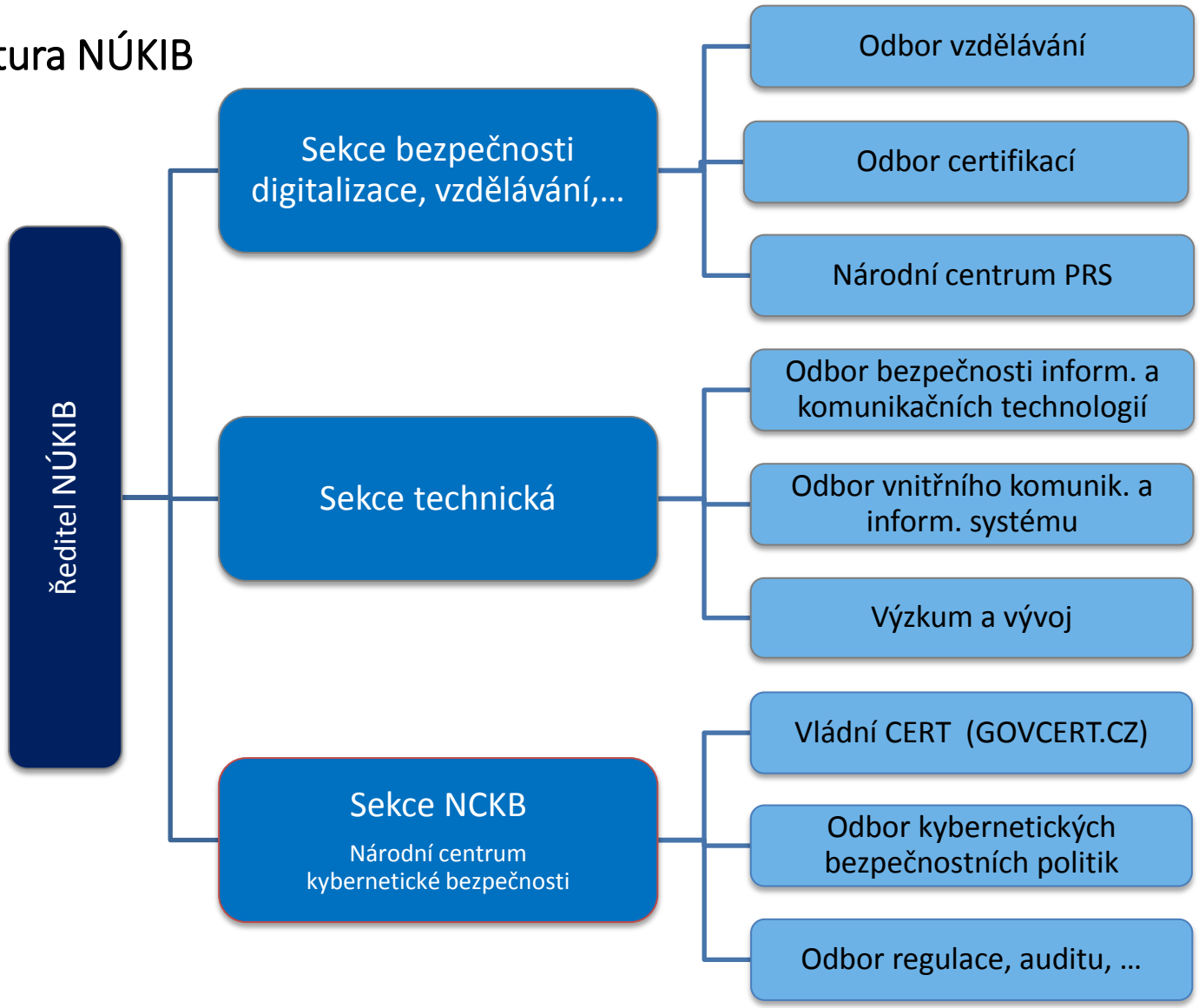
# Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB

- Vznik novelou zákona o kybernetické bezpečnosti k 1. srpnu 2017
- Ústřední správní orgán pro:
  - kybernetickou bezpečnost
  - ochranu utajovaných informací v oblasti informačních a komunikačních systémů
  - kryptografickou ochranu
  - problematiku služby PRS v rámci družicového systému Galileo
- Celkem cca 160 zaměstnanců

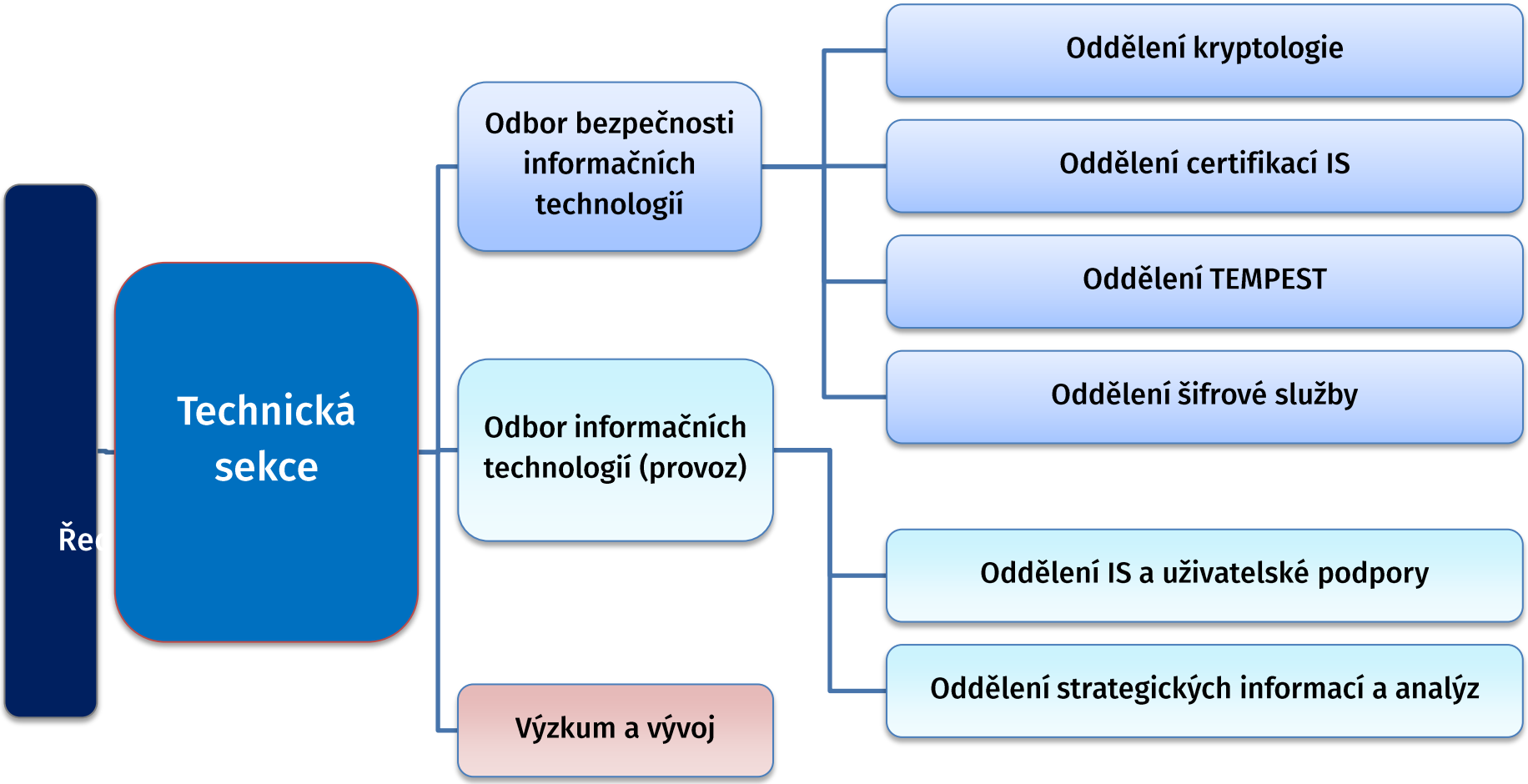
# Služby NÚKIB v oblasti kybernetické bezpečnosti

- Vládní CERT České republiky (GovCERT.CZ)
- Spolupráce s ostatními CERT a CSIRT bezpečnostními týmy v ČR i v zahraničí
- Příprava bezpečnostních standardů
- Kybernetická cvičení, osvěta a podpora vzdělávání
- Výzkum a vývoj
- Ochrana utajovaných informací v oblasti IS/KS
- Kryptografická ochrana
- Kontaktní místo GALILEO
- Ukládá správní tresty za nedodržení zákonných povinností v oblasti KB

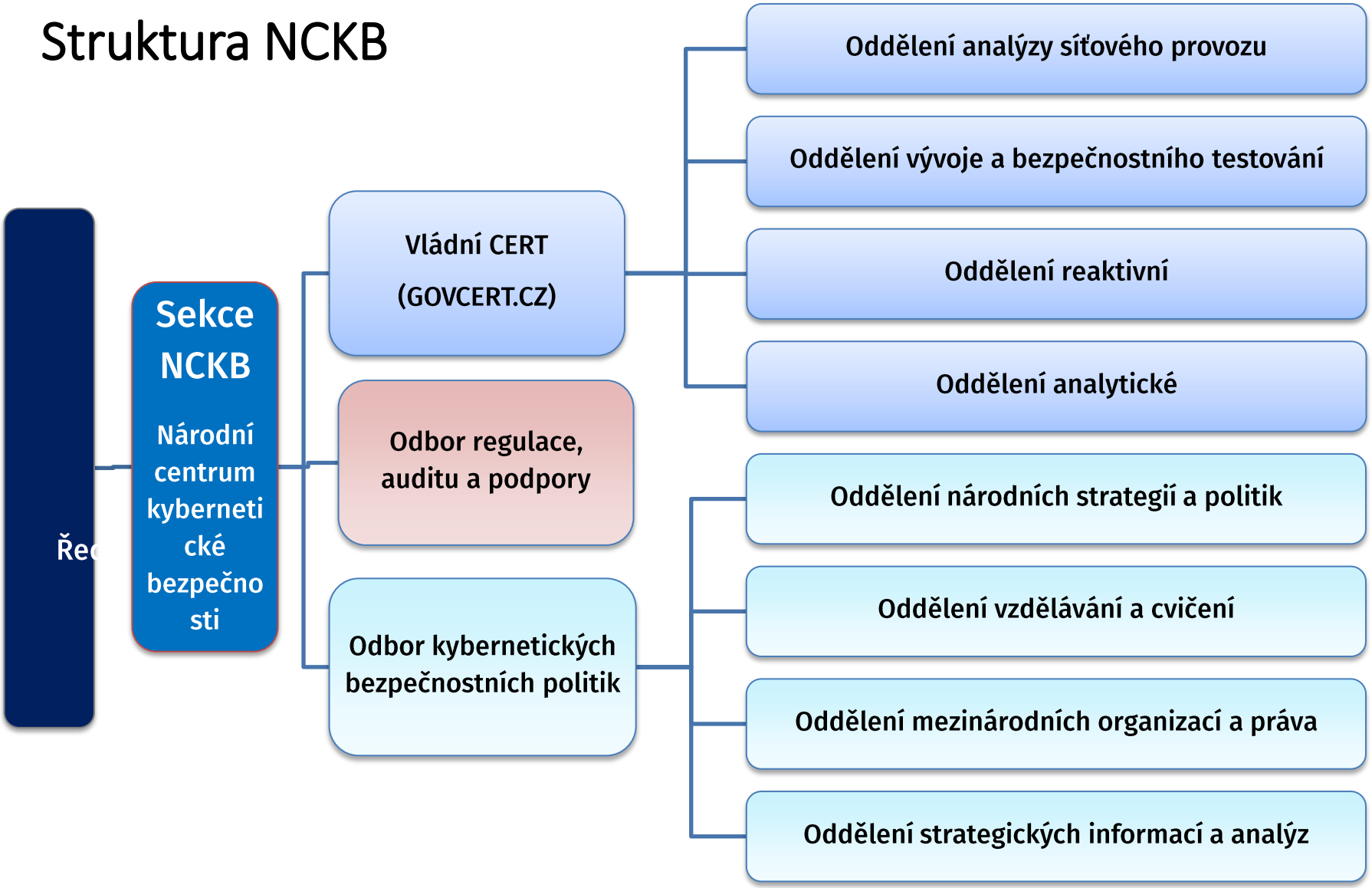
# Struktura NÚKIB



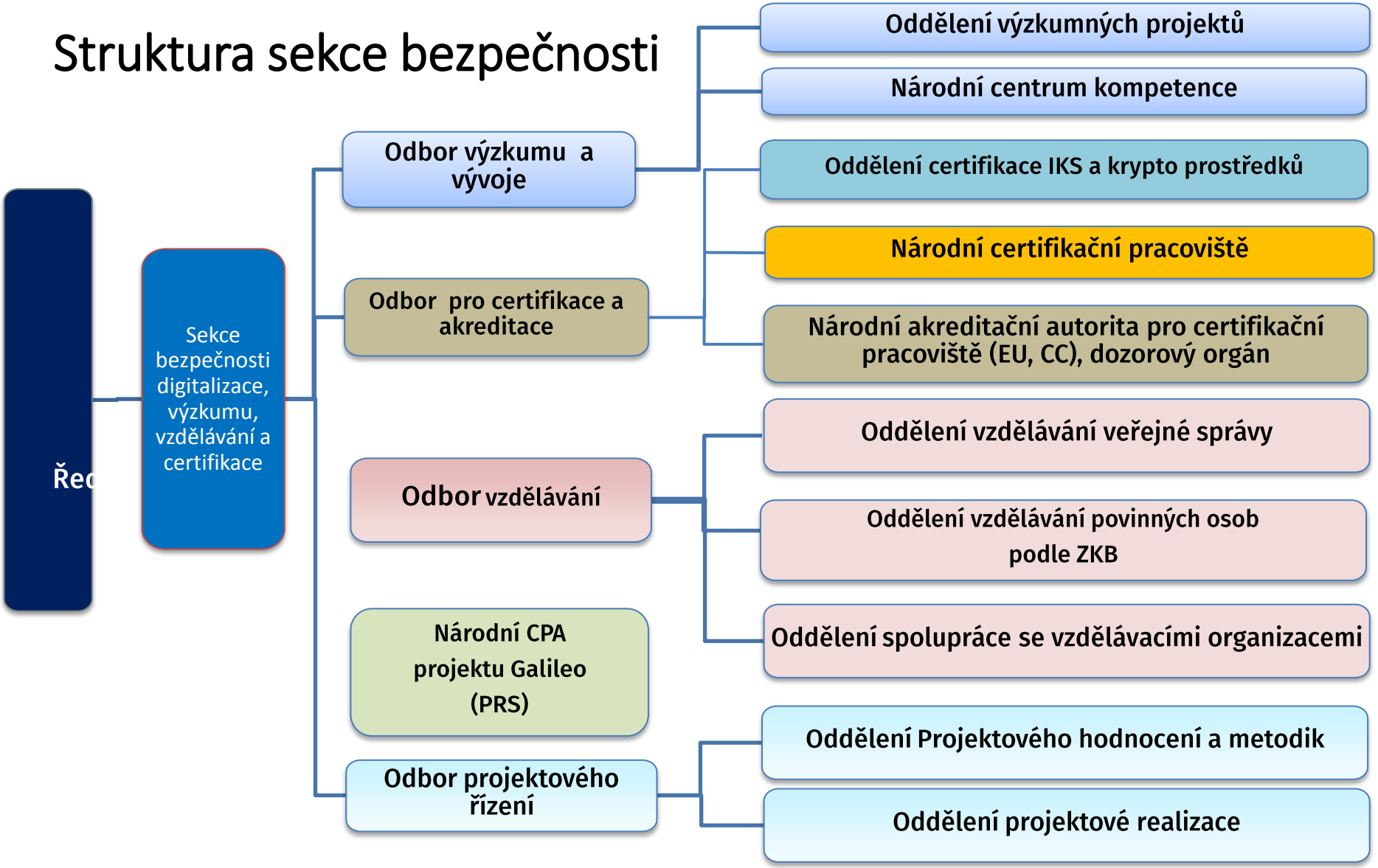
# Struktura technické sekce



# Struktura NCKB



# Struktura sekce bezpečnosti



# Kybernetická bezpečnost, aktivity EU

- Směrnice NIS
  - Směrnice stanovuje opatření pro bezpečnost sítí a informačních systémů v rámci Unie s cílem zlepšit fungování vnitřního trhu
  - Státy musí přijmout národní strategii pro bezpečnost sítí a IS
  - Státy musí určit vnitrostátní příslušné orgány pro oblast regulace, jednotná kontaktní místa a týmy CSIRT
  - Státy musí určit provozovatele základních služeb (PZS) - do 9. 11 2018
  - Směrnice přímo definuje poskytovatele digitálních služeb (PDS)
  - PZS a PDS povinnost zavést bezpečnostní opatření a hlásit incidenty
- Kybernetický balíček (viz dále)

# Směrnice NIS - provozovatelé základních služeb (PZS)

- Základní služba
  - Služba závislá na informačních či komunikačních systémech
  - Narušení služby by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:
    1. energetika
    2. doprava
    3. bankovnictví
    4. infrastruktura finančních trhů
    5. zdravotnictví
    6. vodní hospodářství
    7. digitální infrastruktura
    8. chemický průmysl

- Informační systém základní služby
  - systém, na jehož fungování je závislé poskytování základní služby

# Směrnice NIS - provozovatelé základních služeb (PZS)

- PZS budou určováni podle kritérií stanovených novou vyhláškou č. 437/2017 Sb.
  - Vyhláška účinná od 1. února 2018
  - Na nastavování kritérií se podílela pracovní skupina z řad soukromé i státní sféry (14 podskupin dle odvětví a pododvětví, cca 100 členů)
- Pro určení bude nutné naplnit jak dopadová tak odvětvová kritéria
  - Odvětví kopírují NIS (+ chemický průmysl)
  - Dopadová kritéria respektují požadavky směrnice a zohledňují národní podmínky
- Kritéria a definice nastavena tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb (ne např. fakturační, marketingové systémy ani např. bankomaty)
- PZS budou určováni rozhodnutím ve správním řízení

# Směrnice NIS – Poskytovatelé digitální služeb (PDS)

- Poskytovatel digitální služby poskytuje službu:
  - **On-line tržiště** - umožňuje on-line uzavírat kupní smlouvu nebo smlouvu o poskytnutí služeb prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, která využívá službu on-line tržiště
  - **Internetového vyhledávače**
  - **Cloud computingu** - umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, jež je možno sdílet
- Regulace se netýká malých a mikro podniků
  - <50 zaměstnanců a roční bilanční suma nebo obrat <10 mil. €
- Funguje zde princip samourčení – naplnění definice = povinná osoba

# Kybernetický balíček

- Soubor koncepčních a legislativní dokumentů vydaných 13. 9. 2017 Evropskou Komisí
- Jedná se o 4 zásadní dokumenty:
  - Sdělení Komise Parlamentu a Radě o kybernetické bezpečnosti
    - Strategický dokument navazující na Strategii EU pro KB
  - Nařízení o agentuře ENISA a bezpečnostní certifikaci – dva cíle
    - Zavést permanentní mandát pro Agenturu ENISA s dalšími novými úkoly
    - Stanovit právní základ pro společnou bezpečnostní certifikaci ICT produktů a služeb uznatelnou napříč celou EU
  - Koncept společného zvládání kybernetických incidentů (tzv. Blueprint)
    - Soubor procesních postupů, jak reagovat na rozsáhlé přeshraniční incidenty v oblasti kybernetické bezpečnosti
  - Dokument o harmonizaci směrnice NIS
    - Shrnuje základní cíle směrnice NIS

# Kybernetický balíček

- Rozšíření a upřesnění Strategie KB EU z r. 2013
  - ENISA – vytváření certifikačních schémat ICT produktů
  - Budování **hodnotitelských pracovišť** – laboratoří, akreditačního orgánu, dozorového orgánu
  - Nastavit strukturovanou spolupráci i při incidentech s nižšími dopady
  - Vytváření výzkumných **center kompetenc**e a jejich koordinace
  - Kontaktní místa pro koordinaci vzdělávacích pracovišť
  - …

# Cvičení

- **Technická cvičení** - Cyber Coalition, Locked Shields, Cyber Europe, CyberCzech, CyberCzech, CECSP

- Netechnická / table-top cvičení - Locked Shields,Cybereurope, Crisis management exercise, Strategic TTX, CyberCzech,

- **Další rozvoj:**
  - Cvičení na klíč dle odvětví
  - Spojení kybernetických cvičení s konvenčními
  - Podpora mezinárodních partnerů
  - Propojení technických a netechnických v reálném čase

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

About Us | Cyber Defence Library | Tallinn Manual | Events | Resources | Cyb

## Czech Team Wins Cyber Defence Exercise Locked Shields 2017

**The team from Czech Republic wins the largest live-fire cyber defence exercise Locked Shields team from NATO take secon nd third place r**

The defensive team from Cz lic also take scenario inject. NCIRC tea best in German team came out Kingdom achieved the challenges.

"The winning tea categories can l performed a highlights

"Th

**NATO CCD COE**
@ccdcoe

Sledovat

Czech Team #LockedShields 2017 winner! Estonian team 2nd @e_riik , NCIRC 3rd @NCIAgency! Congrats to all!

LOCKED SHIELDS

# Vzdělávání

- **E-learning pro zaměstnance veřejné správy**
- Dva moduly:
  A. **Základy kybernetické bezpečnosti**: určeny všem, všeobecné základy
  B. **Kurz kybernetické bezpečnosti dle ZKB**: určen pro pracovníky vykonávající role dle ZKB
- Volena **srozumitelná forma** s jasnými doporučeními, příklady a návody, které mohou účastníci využít při práci.
- **Modul A spuštěn** ve třetím čtvrtletí 2017, **modul B** na začátku roku 2018.
- Základní kurz potenciálně **vhodný pro široké spektrum státních zaměstnanců** bez ohledu na zařazení.

# Spolupráce s vysokými školami

- Cílem **pomoci školám při tvorbě nových studijních programů**, které budou přímo vzdělávat experty na kyber bezpečnost.
- **Pravidelné mapování** programů, oborů a předmětů prvním krokem.
- Aktivní spoluúčast při výuce předmětů zaměřených na KB. Zejména předmět **Kybernetická bezpečnost** na MU, UPOL a UNOB.
- **Nabídka stáží** na NCKB. Cílem rozšířit znalosti a povědomí studentů o KB. Rovněž prezentace NCKB v rámci studentské komunity.

# Spolupráce se středními školami

- **Mapování výuky kybernetické bezpečnosti**, informatiky a ICT i na středních školách.
- **Podpora při tvorbě zcela nového oboru KB/tematického celku KB v rámci oboru ICT** na: SŠIPF v Brně, SŠTE v Brně, SŠIS ve Dvoře Králové; úzká komunikace se SPŠ Smíchov.
- Podpora Středoškolské kybernetické soutěže ČR – AFCEA - ENISA.
  - Prvního kola soutěže se zúčastnilo téměř 1100 studentů z různých středních škol, druhého kola se zúčastnilo již vice než 3000 studentů

CYBER SECURITY COMPETITION CZECH

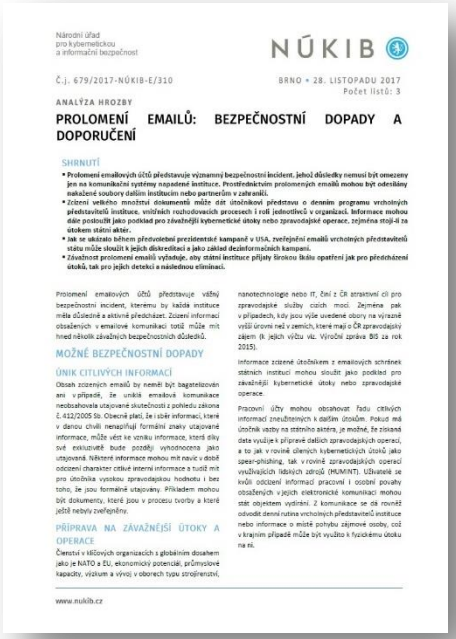
Finále se zúčastní 40 nejlepších studentů a studentek z 26 středních škol z celé České republiky. Soutěžící se do finále probojovali úspěšným absolvováním dvou vyřazovacích online kol. Nejúspěšnější studenti dostanou v průběhu letních soustředění příležitost ke kvalifikaci do evropského finále, které se uskuteční v říjnu 2018 v Londýně za účasti 20 týmů z evropských zemí.

# Spolupráce se základními školami

- Projekt interaktivního modulu „**Digitální stopa**“. Cílí na problematiku rizikového chování v prostředí internetu a sociálních sítí.
- **Přednášková a osvětová činnost**. Na základě žádosti škol připravena přednáška o kyberkriminalitě, závadovém jednání a sociálně patologických jevech, se kterými se lze setkat v prostředí internetu.
- Školní diář
- Přednášková činnost pro učitelé a rodiče.

# Strategické informace a analýzy

## Příklady výstupů



Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Č.j. 679/2017-NÚKIB-E/310 BRNO • 28. LISTOPADU 2017

Počet listů: 3

ANALÝZA HROZBY

**PROLOMENÍ EMAILŮ: BEZPEČNOSTNÍ DOPADY A DOPORUČENÍ**

SHRNUTÍ

- Prolomení emailových účtů představuje významný bezpečnostní incident, jehož důsledky nemusí být omezeny jen na komunikační systémy napadené instituce. Prostřednictvím prolomených emailů mohou být odeslány nakažené soubory dalším institucím nebo partnerům v zahraničí.
- Zcízení velkého množství dokumentů může být útočníkovi představou o denním programu vrcholných představitelů instituce, vnitřních rozhodovacích procesech i roli jednotlivců v organizaci. Informace mohou dále posloužit jako podklad pro závažnější kybernetické útoky nebo zpravodajské operace, zejména stojí-li za útokem státní aktér.
- Jak se ukázalo během předvolební prezidentské kampaně v USA, zveřejnění emailů vrcholných představitelů státu může sloužit k jejich diskreditaci a jako základ dezinformačních kampaní.
- Závažnost prolomení emailů vyžaduje, aby státní instituce přijaly širokou škálu opatření jak pro předcházení útoků, tak pro jejich detekci a následnou eliminaci.

Prolomení emailových účtů představuje vážný bezpečnostní incident, kterému by každá instituce měla účelně a aktivně předcházet. Zcízení informací obsažených v emailové komunikaci totiž může mít hned několik závažných bezpečnostních důsledků.

MOŽNÉ BEZPEČNOSTNÍ DOPADY

ÚNIK CITLIVÝCH INFORMACÍ

Obsah zcízených emailů by neměl být bagatelizován ani v případě, že uniklá emailová komunikace neobsahovala utajované skutečnosti z pohledu zákona č. 412/2005 Sb. Obecně platí, že i sběr informací, které v daném cíli nenapňují formální znaky utajované informace, může vést ke vzniku informace, která díky své exkluzivitě bude později vyhodnocena jako utajovaná. Některé informace mohou mít navíc v době odcizení charakter citlivé interní informace a tudíž mít pro útočníka vysokou zpravodajskou hodnotu i bez toho, že jsou formálně utajovány. Příkladem mohou být dokumenty, které jsou v procesu tvorby a které ještě nebyly zveřejněny.

PŘÍPRAVA NA ZÁVAŽNĚJŠÍ ÚTOKY A OPERACE

Členství v věcných organizacích s globálním dosahem jako je NATO a EU, ekonomický potenciál, průmyslové kapacity, výzkum a vývoj v oborech typu strojírenství, nanotechnologie nebo IT, činí z ČR atraktivní cíl pro zpravodajské služby cizích mocí. Zejména pak v případech, kdy jsou výše uvedené obory na výrazně vyšší úrovni než v zemích, které mají o ČR zpravodajský zájem (k jejich výčtu viz. Výroční zpráva BIS za rok 2015).

Informace zcízené útočníkem z emailových schránek státních institucí mohou sloužit jako podklad pro závažnější kybernetické útoky nebo zpravodajské operace.

Pracovní účty mohou obsahovat řadu citlivých informací zneužitelných k dalším útokům. Pokud má útočník vazby na státního aktéra, je možné, že získaná data využije k přípravě dalších zpravodajských operací, a to jak v rovině cílených kybernetických útoků jako spear-phishing, tak v rovině zpravodajských operací využívajících lidských zdrojů (HUMINT). Uživatelé se kvůli odcizení informací pracovní i osobní povahy obsažených v jejich elektronické komunikaci mohou stát objektem vydírání. Z komunikace se dá rovněž odvodit denní rutina vrcholných představitelů instituce nebo informace o místě pohybu zájmové osoby, což v krajním případě může být využito k fyzickému útoku na ni.

www.nukib.cz

National Cyber and Information Security Agency

NÚKIB

REF.NR. 794/2017-NÚKIB-E/310 • BRNO • 10 NOVEMBER 2017

STRATEGIC ANALYSIS

**NORTH KOREA IN CYBERSPACE: ALL-PURPOSE CYBER THREAT ACTOR**

SUMMARY

- DPRK's approach in cyberspace is characteristic for broader-than-usual scope of activities that includes cyberespionage, information campaigns, patriotic hacking and profit-oriented cybercrime operations. Notable cybercrime activity of DPRK actors in recent years is likely a result of tightening international sanctions, which affected financial revenue from otherwise legal operations. DPRK is a state actor with a characteristic of a cybercrime syndicate.
- Exploitation of cyberspace for espionage and cybercrime purposes will become more prominent part of Pyongyang's asymmetric posture irrespective of a particular development in physical domain. The possibility of a breakdown in relations with China or Russia is a factor that would only increase prominence of cyberspace for Pyongyang.
- Czech Republic is a credible target for DPRK cyberespionage efforts by its association to the US, the EU and NATO, and related compliance with UNSC/U.S.-led sanctions. While there is no imminent threat from the DPRK for the Czech Republic and its CII from Pyongyang, DPRK's resort to for-profit operations including spreading of ransomware and attacks on banks could mean that institutions in the Czech Republic could become victims of DPRK activity as collateral damage if not by design.

KEY FACTS

| | |
|---|---|
| Target | Critical information infrastructure, government networks, news organizations and banks/financial institutions, indiscriminate targeting via ransomware campaigns |
| Attacker | Reconnaissance General Bureau (RGB) of the Korean People's Army is the major DPRK organization responsible for operations in cyberspace. Threat actors known as Lazarus Group and Guardians of Peace are likely subordinate units either under the RGB, Korean People's Army, or Korean Workers Party. |
| Methods | DDoS, ransomware, spear-phishing, watering hole, zero day exploits |
| Damage | Denial of service, hardware damage, data loss, bank theft |

The most striking aspect that sets DPRK apart from the rest of the state cyberthreat actors is its large-scale engagement in activities typical for cybercrime groups. DPRK's involvement in outright crime has, however, a clear precedent in North Korea's past behavior in the physical domain.

The continuing and ever-tightening grip of international sanctions imposed by the UN Security Council (UNSC), the US and its allies, and even China, means that Pyongyang will continue to employ non-conventional options in cyberspace with increasing intensity.

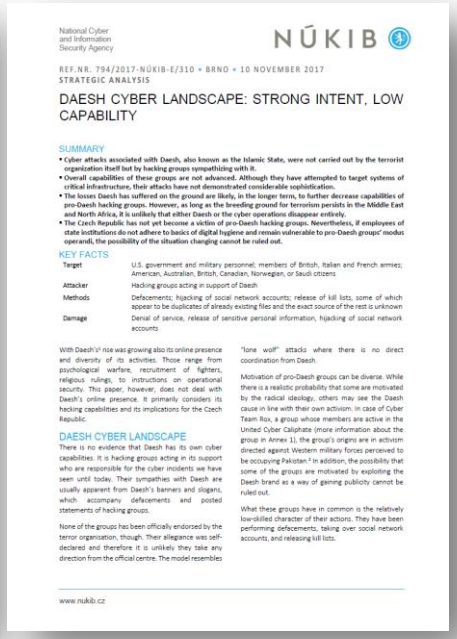
Behind the opaque nature of the North Korean regime is a threat actor, possessing robust capabilities, which utilizes cyberspace in areas that other state actors heretofore avoided. Furthermore, cyber groups associated with the DPRK are demonstrating improved

*Figure 1: Kim Jong-un inspects Sol-Tech Complex 28 technological centre in Pyongyang*



Source: KCNA

www.nukib.cz



National Cyber and Information Security Agency

NÚKIB

REF.NR. 794/2017-NÚKIB-E/310 • BRNO • 10 NOVEMBER 2017

STRATEGIC ANALYSIS

**DAESH CYBER LANDSCAPE: STRONG INTENT, LOW CAPABILITY**

SUMMARY

- Cyber attacks associated with Daesh, also known as the Islamic State, were not carried out by the terrorist organization itself but by hacking groups sympathizing with it.
- Overall capabilities of these groups are not advanced. Although they have attempted to target systems of critical infrastructure, their attacks have not demonstrated considerable sophistication.
- The losses Daesh has suffered on the ground are likely, in the longer term, to further decrease capabilities of pro-Daesh hacking groups. However, as long as the breeding ground for terrorism persists in the Middle East and North Africa, it is unlikely that either Daesh or the cyber operations disappear entirely.
- The Czech Republic has not yet become a victim of pro-Daesh hacking groups. Nevertheless, if employees of state institutions do not adhere to basics of digital hygiene and remain vulnerable to pro-Daesh groups' modus operandi, the possibility of the situation changing cannot be ruled out.

KEY FACTS

| | |
|---|---|
| Target | U.S. government and military personnel; members of British, Italian and French armies; American, Australian, British, Canadian, Norwegian, or Saudi citizens |
| Attacker | Hacking groups acting in support of Daesh |
| Methods | Defacements; hijacking of social network accounts; release of kill lists, some of which appear to be duplicates of already existing files and the exact source of the rest is unknown |
| Damage | Denial of service, release of sensitive personal information, hijacking of social network accounts |

With Daesh's[1] rise was growing also its online presence and diversity of its activities. Those range from psychological warfare, recruitment of fighters, religious rulings, to instructions on operational security. This paper, however, does not deal with Daesh's online presence. It primarily considers its hacking capabilities and its implications for the Czech Republic.

DAESH CYBER LANDSCAPE

There is no evidence that Daesh has its own cyber capabilities. It is hacking groups acting in its support who are responsible for the cyber incidents we have seen until today. Their sympathies with Daesh are usually apparent from Daesh's banners and slogans, which accompany defacements and posted statements of hacking groups.

None of the groups has been officially endorsed by the terror organisation, though. Their allegiance was self-declared and therefore it is unlikely they take any direction from the official centre. The model resembles "lone wolf" attacks where there is no direct coordination from Daesh.

Motivation of pro-Daesh groups can be diverse. While there is a realistic probability that some are motivated by the radical ideology, others may see the Daesh cause in line with their own activism. In case of Cyber Team Rox, a group whose members are active in the United Cyber Caliphate (more information about the group in Annex 1), the group's origins are in activism directed against Western military forces perceived to be occupying Pakistan.[2] In addition, the possibility that some of the groups are motivated by exploiting the Daesh brand as a way of gaining publicity cannot be ruled out.

What these groups have in common is the relatively low-skilled character of their actions. They have been performing defacements, taking over social network accounts, and releasing kill lists.

www.nukib.cz

UNCLASSIFIED

STRATEGIC ANALYSIS • 8 DECEMBER 2016 • REF.NR. N/A

**CHINESE CYBER CAMPAIGN IN SOUTH CHINA SEA: ASSERTING BEIJING'S "CORE INTERESTS" IN CYBERSPACE**

SUMMARY

- China's cyber activities observed in the South China Sea theatre demonstrate particular employment of China's vast cyber warfare and information warfare apparatus for collection of strategic intelligence in a pursuit of its core national interests. These capabilities could be deployed in support of Chinese interests vis-a-vis the Czech Republic, the CEE region, or the NATO and European Union.
- DDoS attacks are another method of choice for Chinese cyber groups that are likely tasked (or at the very least tolerated) by the government to executive punitive attacks in response to undesirable actions of other states. DDoS attacks are generally less harmful than the espionage-driven activity of APT actors but they are also more visible to the general population, creating perception of insecurity, which in turn generates pressure on the receiving governments.
- Chinese cyber campaign is likely to continue along with Beijing's strengthening foothold on the ground. Relative weakness of regional actors in the area of cyber security and defence further increases Beijing's incentive for exploitation as the risk of timely attribution is low.

KEY FACTS

| | |
|---|---|
| Target: | Mainly governments and international organizations. |
| Threat Actors: | Chinese government or government-affiliated actors. Significant links between Naikon APT and Unit 78020 belonging to the Chinese military. |
| Methods: | Spear-phishing attacks carrying malware enabling the attacker remote access to infected networks; DDoS campaigns, website defacement. |
| Damage: | Compromised networks, stolen sensitive intelligence, denial of service. |

Since 2009, China has engaged with increasing intensity in a multi-pronged campaign aimed at asserting territorial and maritime claims in the South China Sea (SCS). The cyber element of Beijing's campaign in the region has mostly focused on intelligence collection and punitive attacks by patriotic hackers promoting the position of the Chinese government.

China's cyber activities observed in the South China Sea theatre are not in any sense particular for countries that are currently in dispute with Beijing. They merely demonstrate specific employment of China's vast cyber warfare and information warfare apparatus in a pursuit of its core national interests'. It is prudent to assume that the Czech Republic and other EU/NATO members are subject to cyber operations similar in method to those observed in the South China Sea region, considering the diverging trajectory of Chinese and Western interests on a number of issues. Escalation of disagreement would likely result in defacement and DDoS attacks conducted by less sophisticated elements of Chinese

Figure 1: South China Sea dispute



Source: Wikimedia Commons

www.nckb.cz

UNCLASSIFIED

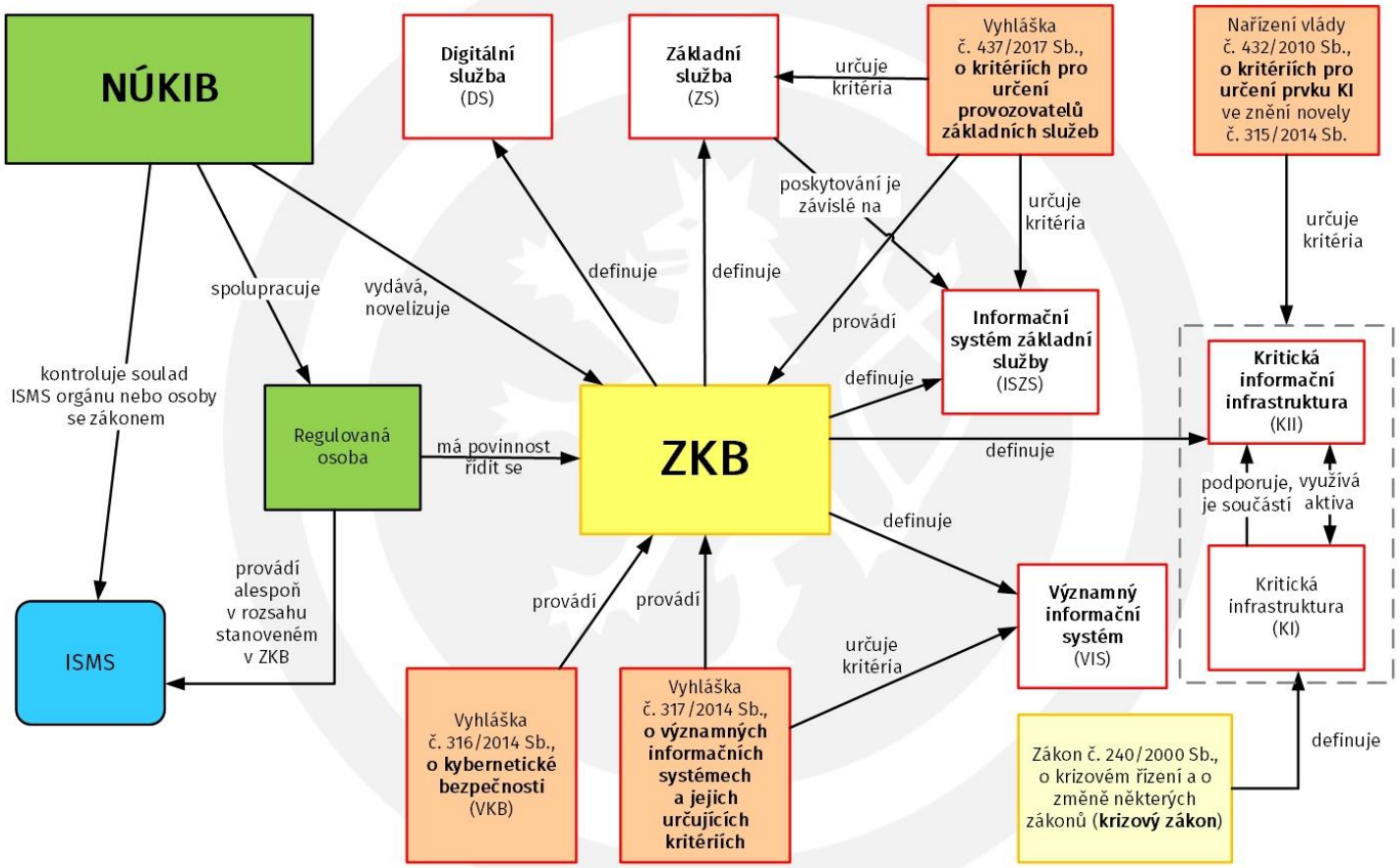


25

# Regulace, audit, podpora

- **Regulace**
  - stanovení, které subjekty a ICT dle kritérií ZKB spadají pod regulaci a které nikoliv
    - Regulované subjekty v naší kompetenci: KII, VIS a nově PZS
  - příprava legislativy (aktuálně transpozice Směrnice NIS a vyhlášek k ZKB)
- **Audit (kontrola ZKB)**
  - ke kontrole dodržování ZKB přistupujeme podobně jako k auditu systému řízení bezpečnosti informací podle ISO 27 001, což přináší přidanou hodnotu i pro regulované subjekty
- **Podpora**
  - výklad ZKB, výklad vyhlášek
  - metodická podpora při implementaci ZKB (implementaci organizačních a technických opatření) – „konzultační a poradenská činnost“ v oblasti kybernetické bezpečnosti pro regulované subjekty

# Regulace

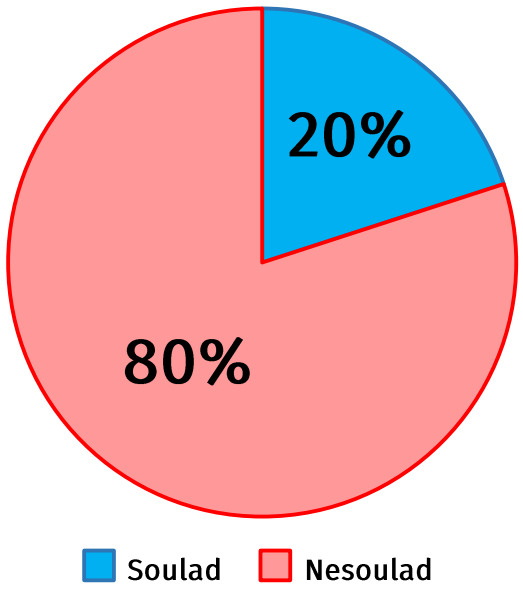

NÚKIB
Digitální služba (DS)
Základní služba (ZS)
určuje kritéria
Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI ve znění novely č. 315/2014 Sb.
poskytování je závislé na
určuje kritéria
určuje kritéria
spolupracuje
vydává, novelizuje
definuje
definuje
provádí
Informační systém základní služby (ISZS)
definuje
kontroluje soulad ISMS orgánu nebo osoby se zákonem
Regulovaná osoba
má povinnost řídit se
ZKB
definuje
Kritická informační infrastruktura (KII)
podporuje, je součástí
využívá aktiva
Kritická infrastruktura (KI)
definuje
provádí alespoň v rozsahu stanoveném v ZKB
ISMS
provádí
provádí
Významný informační systém (VIS)
určuje kritéria
Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti (VKB)
Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
definuje

# Stav implementace směrnice NIS v ČR

| NIS Directive 2017 | ZKB 2015 – 2017 | Novela ZKB 1. 8. 2017 -> |
|---|---|---|
| Národní strategie kybernetické bezpečnosti | ✓ | ✓ |
| Stanovení bezpečnostních požadavků na IS/KS | ✓ | ✓ |
| Zřídit Cyber Incident Response Teams (CSIRT) | ✓ | ✓ |
| Ustavit národní autoritu v oblasti KB | ✓ | ✓ |
| Stanovit jednotné kontaktní místi pro oblast KB | ✓ | ✓ |
| Určit PZS | ⚠ * | ✓ *** |
| Určit PDS | ✗ ** | ✓ *** |

* Částečně zavedeno – kritická informační infrastruktura
** Nezavedeno
*** Probíhá implementace

*Naše kontrolní činnost v oblasti kybernetické bezpečnosti dokazuje, že 80% regulovaných subjektů, nezvládá systém řízení kybernetické a informační bezpečnosti.*



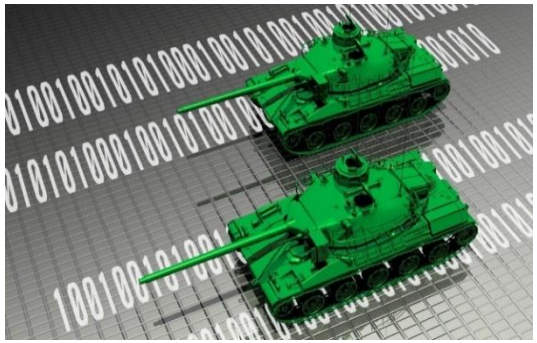

**Problematické oblasti:**

- Detekce a zvládání kybernetických bezpečnostních incidentů
- Řízení aktiv a rizik
- Organizační bezpečnost
- Bezpečnost aplikací
- Bezpečnost komunikační infrastruktury
- Řízení dodavatelů
- Řízení identit a oprávnění
- Fyzická bezpečnost
- Řízení kontinuity činností
- …

*… naše poslání je regulovaným subjektům s kybernetickou bezpečností pomoci.*

# Práce a aktivity na národní úrovni

- Odborná pracovní skupina BRS pro hybridní hrozby:
  - Ad hoc setkávání k problematice HH
  - Pracovní skupina pro Smart Cities pod Radou vlády pro udržitelný rozvoj
- Plnění AP Auditu Národní Bezpečnosti (ANB)



# Výzkum a Vývoj (VaV)

- Aktivity 2017:
  - ✓ **Založení PS k VaV** v oblasti kybernetické bezpečnosti (MV, MO, TAČR a zpravodajské služby)
  - ✓ **Jednání s ÚV a TAČR**
    - ✓ Vytvořit **databázi výzkumných projektů** v rámci kybernetické bezpečnosti a podávat z ní informace dalším subjektům (součinnost s ÚV a TAČR)
    - ✓ Ve spolupráci s ostatními organizačními složkami státu vypracovat **národní koncepci VaV** v oblasti kybernetické bezpečnosti
  - ✓ Připravit podmínky pro zřízení **centra kompetence**

# Vládní CERT

- Veřejný sektor a kritická informační infrastruktura
- Struktura týmu:
  - Zpracování incidentů
  - Vývoj a bezpečnostní testování
  - Síťová bezpečnost
  - Analytická skupina
- Základní služby:
  - Reaktivní: zpracování a řešení incidentů, zpracování artefaktů a analýza dat
  - Detekční: detekce anomálií, zpracování indikátorů kompromitace
  - Proaktivní: koordinace v rámci české bezpečnostní komunity a sdílení informací, penetrační testování, kybernetická cvičení a další

# Oblasti zaměření

- **SCADA/ICS systémy**
- **Penetrační testování**
- **Forenzní úkoly**
- **Analýza malware a reverzní inženýrství**
- Virtuální prostředí a cloudová řešení
- Bezpečný vývoj a databázové systémy
- UNIXové systémy
- Windows systémy
- Síťová bezpečnost a analýza síťového provozu
- Honeypoty

# Aktuální situace

- Rozsáhlé phishingové kampaně
- Velké množství škodlivého kódu, převážně ransomware
- Špionážní malware
- Těžba krypto měn

Rozložení typů incidentů zůstává přibližně stejné

# Detekce incidentů

- Nasazení síťových sond
- Nasazení honeypotů
- Analýza indikátorů kompromitace a dalších veřejně dostupných dat
- Systém včasného varování

# Aktuální projekty

- Forenzní laboratoř
- Laboratoř škodlivého kódu
- Skenování zranitelností (OWASP)
- Penetrační testování
- ICS / SCADA laboratoř
- Budování scrubbing centra
- Koordinační centrum pro české bezpečnostní týmy
- Organizace a účast na národních i mezinárodních cvičeních kybernetické bezpečnosti

# Nabízené služby

- Pomoc s technickou částí zpracování incidentu
- Ustavení komunikace s další stranou
- Zpracování artefaktů, technická analýza (forenzní, sítě, malware, …)
- Konzultace technických řešení
- Detekční služby – IoC, Sondy, honeypoty, ...
- Open Source Intelligence (OSINT)
- Penetrační testování (externí)

# Analýzy ministerstev

- Usnesení Vlády ČR ze dne 8. 2. 2016 č. 104
- Subjekty: všechna ministerstva, Poslanecká sněmovna, Senát a Kancelář prezidenta republiky
- Zjištění aktuální situace v oblasti kybernetické bezpečnosti
- Kontrola indikátorů kompromitace z incidentu na Ministerstvu zahraničních věcí

# Analýzy ministerstev

- Nedostatek lidských zdrojů
- Nedostatečná podpora ze strany vedení
- Nevhodný rozsah systému řízení bezpečnosti
- Neexistující bezpečnostní monitoring
- Neexistující sběr logů (centrální, často ani lokální)
- Nedostatečná aktualizace systémů
- Nedostatečné řízení zranitelností
  - Nízké bezpečnostní povědomí uživatelů
  - Výjimky pro uživatele (nejčastěji management)
  - Závislost na dodavatelích a outsourcing
  - Neexistence centralizované správy

# Děkuji za pozornost