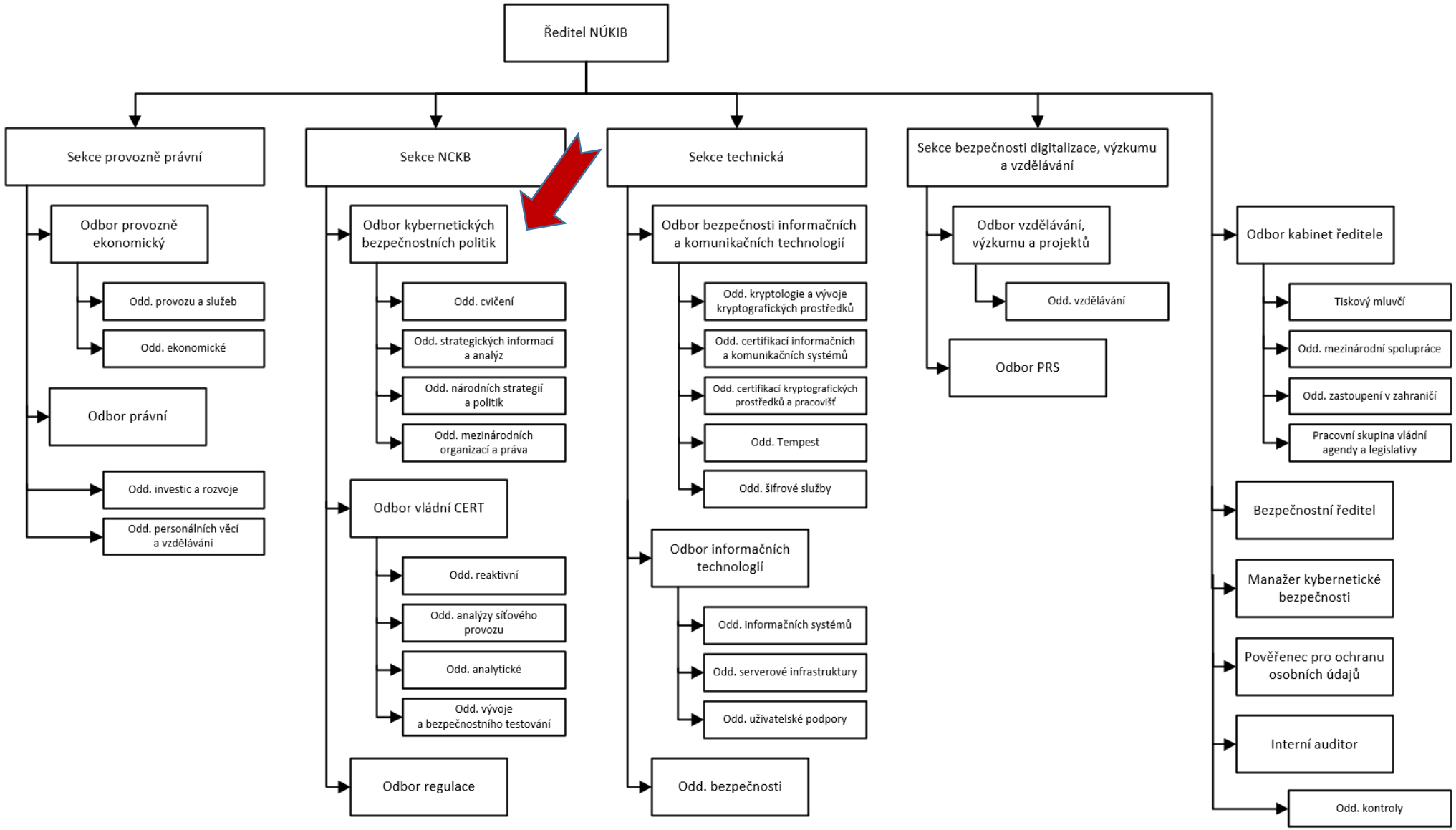
ODDĚLENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH POLITIK


Ředitel NÚKIB
Sekce provozně právní
Odbor provozně ekonomický
Odd. provozu a služeb
Odd. ekonomické
Odbor právní
Odd. investic a rozvoje
Odd. personálních věcí a vzdělávání
Sekce NCKB
Odbor kybernetických bezpečnostních politik
Odd. cvičení
Odd. strategických informací a analýz
Odd. národních strategií a politik
Odd. mezinárodních organizací a práva
Odbor vládní CERT
Odd. reaktivní
Odd. analýzy síťového provozu
Odd. analytické
Odd. vývoje a bezpečnostního testování
Odbor regulace
Sekce technická
Odbor bezpečnosti informačních a komunikačních technologií
Odd. kryptologie a vývoje kryptografických prostředků
Odd. certifikací informačních a komunikačních systémů
Odd. certifikací kryptografických prostředků a pracovišť
Odd. Tempest
Odd. šifrové služby
Odbor informačních technologií
Odd. informačních systémů
Odd. serverové infrastruktury
Odd. uživatelské podpory
Odd. bezpečnosti
Sekce bezpečnosti digitalizace, výzkumu a vzdělávání
Odbor vzdělávání, výzkumu a projektů
Odd. vzdělávání
Odbor PRS
Odbor kabinet ředitele
Tiskový mluvčí
Odd. mezinárodní spolupráce
Odd. zastoupení v zahraničí
Pracovní skupina vládní agendy a legislativy
Bezpečnostní ředitel
Manažer kybernetické bezpečnosti
Pověřenec pro ochranu osobních údajů
Interní auditor
Odd. kontroly

NASTAPO:

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

Zajišťuje efektivní koordinaci a harmonizaci kybernetických bezpečnostních politik napříč veřejnou sférou a dalšími subjekty

Usiluje o budování koherentní národní komunity kybernetické bezpečnosti v ČR

NASTAPO/Právní podpora (LEGAD)

- **Právní poradenství a podpora v aktivitách a činnosti GovCERT.CZ**
- **Jedná se zejména o:**
- Právní poradenství při řešení incidentů
- Přípravu vybraných výběrových řízení (např. SANS kurzy)
- Spolupráci v rámci CSIRT Network
- Přípravu na další ročníky cvičení Cyber Czech
- Právní pomoc při budování forenzní laboratoře
- A další…

Cyber Con Brno 2019

2019 – 5. ročník

Univerzitní kino Scala

Konference a workshopy pro odbornou i širokou veřejnost

Cíl: sdílení znalostí/zkušeností, osvěta společnosti

ODDĚLENÍ CVIČENÍ:

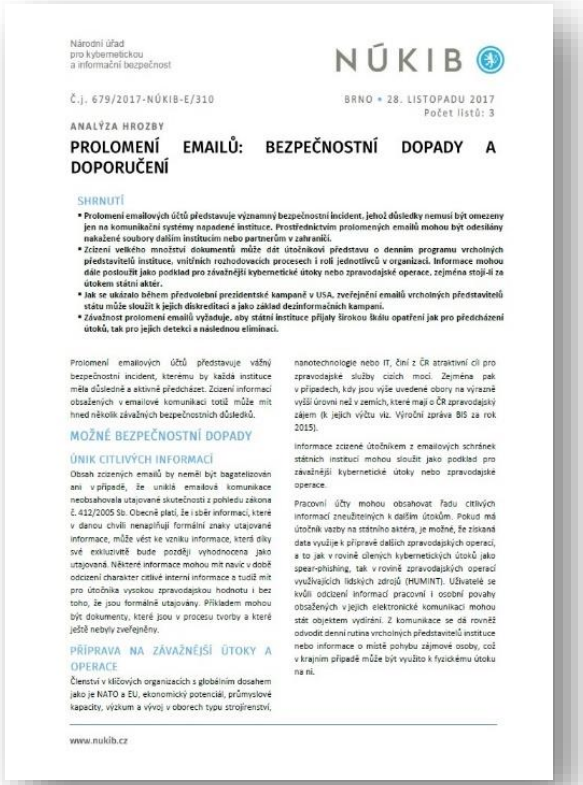
- Technická cvičení
- Strategická table-top cvičení
- Komunikační cvičení
- Mobilní table-top cvičení


SVĚTOVÝ
MEZINÁRODNÍ
REGIONÁLNÍ
BILATERÁLNÍ
NÁRODNÍ
PCSS
CROSSED SWORDS
LOCKED SHIELDS
AFRICA ENDEAVOR
MULTI-LAYER 2014
EUROPEAN UNION EXERCISE
CYBER COALITION
PARTNERS
CYBER EUROPE
enisa
Prague Security Studies Institute
2017
NATO SUMMER SCHOOL TTX
CECSP EXERCISE
2015
CECSP
BALKANS
STRATEGIC TTX
Electro Czech
ČESKÝ STATISTICKÝ ÚŘAD
COMM CZECH
Table-top cvičení
Procedurální cvičení
Komunikační cvičení
Červené vs. modré týmy
Hybridní / komplexní cvičení
STRATEGICKÁ CVIČENÍ
CVIČENÍ KRIZOVÉHO ŘÍZENÍ
KONTROLA SPOJENÍ
TECHNICKÁ CVIČENÍ
TECHNICKO - STRATEGICKÁ CVIČENÍ
TYPY CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI

ODDĚLENÍ MEZINÁRODNÍCH ORGANIZACÍ A PRÁVA

- Zastoupení ČR v mezinárodních organizacích řešících problematiku KB – primárně NATO, EU, OSN, OBSE
  - příprava instrukcí, podkladů, účast na pracovních jednáních
  - EU – Horizontální pracovní skupina pro otázky kybernetické bezpečnosti, Skupina pro spolupráci ke směrnici NIS; příprava CZ PRES 2022
  - NATO – Cyber Defence Committee (působení spojenců v kyberprostoru)
  - OSN – Open-Ended Working Group (globální pravidla působení států v kyberprostoru)
  - OBSE – Informal Working Group (opatření pro budování důvěry mezi státy Západu a Východu)
  - GFCE – platforma pro rozvojovou spolupráci v kyber
  - CECSP – V4 + AT. Dnes víceméně nefunkční
  - výhled: OECD – nová pracovní skupina: Security in the Digital Economy (bezpečné technologie jako předpoklad ekonomického rozvoje)

OSINA: TVORBA A SDÍLENÍ STRATEGICKÝCH INFORMACÍ A ANALÝZ



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 odesílány nakažené soubory dalším institucím nebo partnerům v zahraničí.**
- **Získení velkého množství dokumentů může dát útočníkovi představu 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 důsledně a aktivně předcházet. Získení informací obsažených v emailové komunikaci totiž může mít hned několik závažných bezpečnostních důsledků.

MOŽNÉ BEZPEČNOSTNÍ DOPADY

ÚNIK CITLIVÝCH INFORMACÍ

Obsah získaných 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 danou chvíli nenaplňují 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 klíčových 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 strategickou 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 získané 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.

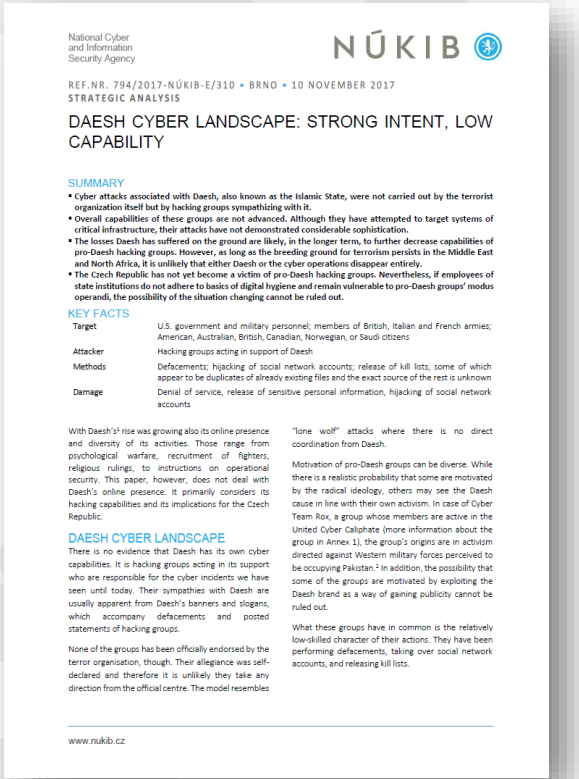
The continuing and ever-tightening grip of international sanctions imposed by the UN Security Council (UNSC), the US and its allies, and even China, means that Pyongyang will continue to employ non-conventional options in cyberspace with increasing intensity.

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

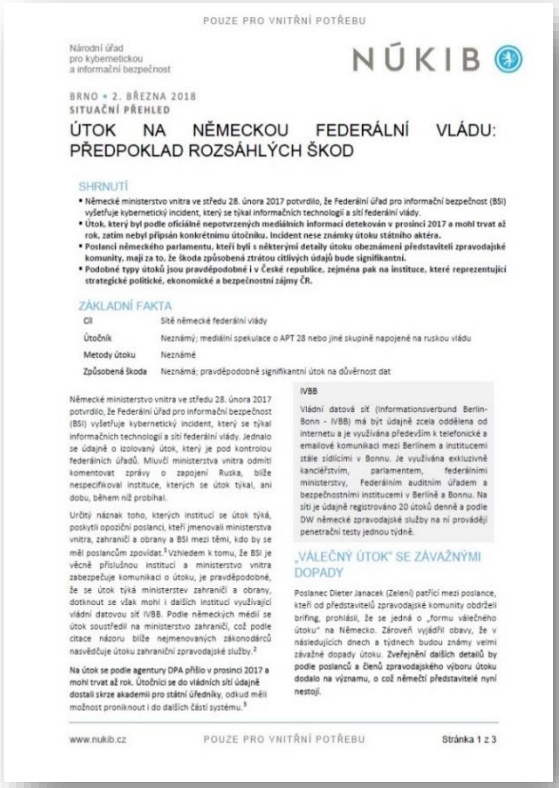
There is no evidence that Daesh has its own cyber capabilities. It is hacking groups acting in its support who are responsible for the cyber incidents we have seen until today. Their sympathies with Daesh are usually apparent from Daesh's banners and slogans, which accompany defacements and posted statements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



POUZE PRO VNITŘNÍ POTŘEBU

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

BRNO • 2. BŘEZNA 2018
SITUAČNÍ PŘEHLED

ÚTOK NA NĚMECKOU FEDERÁLNÍ VLÁDU: PŘEDPOKLAD ROZSÁHLÝCH ŠKOD

SHRNUTÍ

- **Německé ministerstvo vnitra ve středu 28. února 2017 potvrdilo, že Federální úřad pro informační bezpečnost (BSI) vyšetřuje kybernetický incident, který se týkal informačních technologií a sítí federální vlády.**
- **Útok, který byl podle oficiálně nepotvrzených mediálních informací detekován v prosinci 2017 a mohl trvat až rok, zatím nebyl připsán konkrétnímu útočníku. Incident nese známky útoku státního aktéra.**
- **Poslanci německého parlamentu, kteří byli s některými detaily útoku obeznámeni představiteli zpravodajské komunity, mají za to, že škoda způsobená ztrátou citlivých údajů bude signifikantní.**
- **Podobné typy útoků jsou pravděpodobné i v České republice, zejména pak na instituce, které reprezentující strategické politické, ekonomické a bezpečnostní zájmy ČR.**

ZÁKLADNÍ FAKTA

Cíl	Sítě německé federální vlády
Útočník	Neznámý; mediální spekulace o APT 28 nebo jiné skupině napojené na ruskou vládu
Metody útoku	Neznámé
Způsobená škoda	Neznámá; pravděpodobně signifikantní útok na důvěrnost dat

Německé ministerstvo vnitra ve středu 28. února 2017 potvrdilo, že Federální úřad pro informační bezpečnost (BSI) vyšetřuje kybernetický incident, který se týkal informačních technologií a sítí federální vlády. Jednalo se údajně o izolovaný útok, který je pod kontrolou federálních úřadů. Mluvčí ministerstva vnitra odmítl komentovat zprávy o zapojení Ruska, blíže nespecifikoval institute, kterých se útok týkal, ani dobu, během níž probíhal.

Určitý náznak toho, kterých institucí se útok týká, poskytli opoziční poslanci, kteří jmenovali ministerstva vnitra, zahraničí a obrany a BSI mezi těmi, kdo by se měli poslancům zpovídat.[1] Vzhledem k tomu, že BSI je věcně příslušnou institucí a ministerstvo vnitra zabezpečuje komunikaci o útoku, je pravděpodobné, že se útok týká ministerstev zahraničí a obrany, dotknout se však mohl i dalších institucí využívající vládní datovou síť IVBB. Podle německých médií se útok soustředil na ministerstvo zahraničí, což podle citace názoru blíže nejmenovaných zákonodárců nasvědčuje útoku zahraniční zpravodajské služby.[2]

Na útok se podle agentury DPA přišlo v prosinci 2017 a mohl trvat až rok. Útočníci se do vládních sítí údajně dostali skrze akademii pro státní úředníky, odkud měli možnost proniknout i do dalších částí systému.[3]

IVBB

Vládní datová síť (Informationsverbund Berlin-Bonn - IVBB) má být údajně zcela oddělena od internetu a je využívána především k telefonické a emailové komunikaci mezi Berlínem a institucemi stále sídlícími v Bonnu. Je využívána exkluzivně kancléřstvím, parlamentem, federálními ministerstvy, Federálním auditním úřadem a bezpečnostními institucemi v Berlíně a Bonnu. Na síti je údajně registrováno 20 útoků denně a podle DW německé zpravodajské služby na ni provádějí penetrační testy jednou týdně.

„VÁLEČNÝ ÚTOK" SE ZÁVAŽNÝMI DOPADY

Poslanec Dieter Janacek (Zelení) patřící mezi poslance, kteří od představitelů zpravodajské komunity obdrželi briefing, prohlásil, že se jedná o „formu válečného útoku" na Německo. Zároveň vyjádřil obavy, že v následujících dnech a týdnech budou známy velmi závažné dopady útoku. **Zveřejnění dalších detailů by podle poslanců a členů zpravodajského výboru útoku dodalo na významu, o což němečtí představitelé nyní nestojí.**

www.nukib.cz POUZE PRO VNITŘNÍ POTŘEBU Stránka 1 z 3

NÚKIB

TVORBA A SDÍLENÍ STRATEGICKÝCH INFORMACÍ A ANALÝZ

• Hlavní aktivitou je tvorba (netechnických) analytických materiálů a strategických brífingů k hrozbám a trendům v oblasti KB

• Informační podpora decision-makerů založená na otevřených zdrojích a přidané hodnotě v podobě expertízy pracovníků NÚKIB snaha přispívat k informovanému rozhodování

• Zajímá nás strategický kontext (politický, bezpečnostní, ekonomický a sociální) hrozeb a trendů v KB

• Aktivity oddělení rozvíjíme od února 2016

Pro koho to děláme?

Vedení NÚKIB
Předseda vlády a ministři
Bezpečnostní komunita: zpravodajské služby a policie
Mezinárodní organizace: NATO, EU
Bilaterální partneři: UK, USA, KOR aj.