



RESPONSIBLE DISCLOSURE - MOŽNOST PRO ČESKOU REPUBLIKU?

Tat'ána Jančárková
NBÚ/NCKB



Národní centrum
kybernetické
bezpečnosti



NIKDO NENÍ DOKONALÝ

- **Zranitelnosti** jsou inherentní vlastností informačních systémů a ICT produktů
- **Aktivní vyhledávání** zranitelností přispívá ke **zvyšování bezpečnosti**
- **Riziko zneužití** odhalených zranitelností
- Obavy ze **ztráty důvěry** trhu v případě zveřejnění
- Trestněprávní a civilní odpovědnost – **kybernetické trestné činy** nebo **náhrada škody**



TRESTNĚPRÁVNÍ ROZMĚR

- **Mezinárodní závazky**
 - Budapeštská úmluva
 - Rámcové rozhodnutí Rady EU, o útocích proti informačním systémům, č.2005/222/SVV ze dne 24.2.2005
- **„Kybernetické trestné činy“ v trestním zákoníku**
 - § 182 Porušení tajemství dopravovaných zpráv
 - § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
 - § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
 - § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
 - § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi



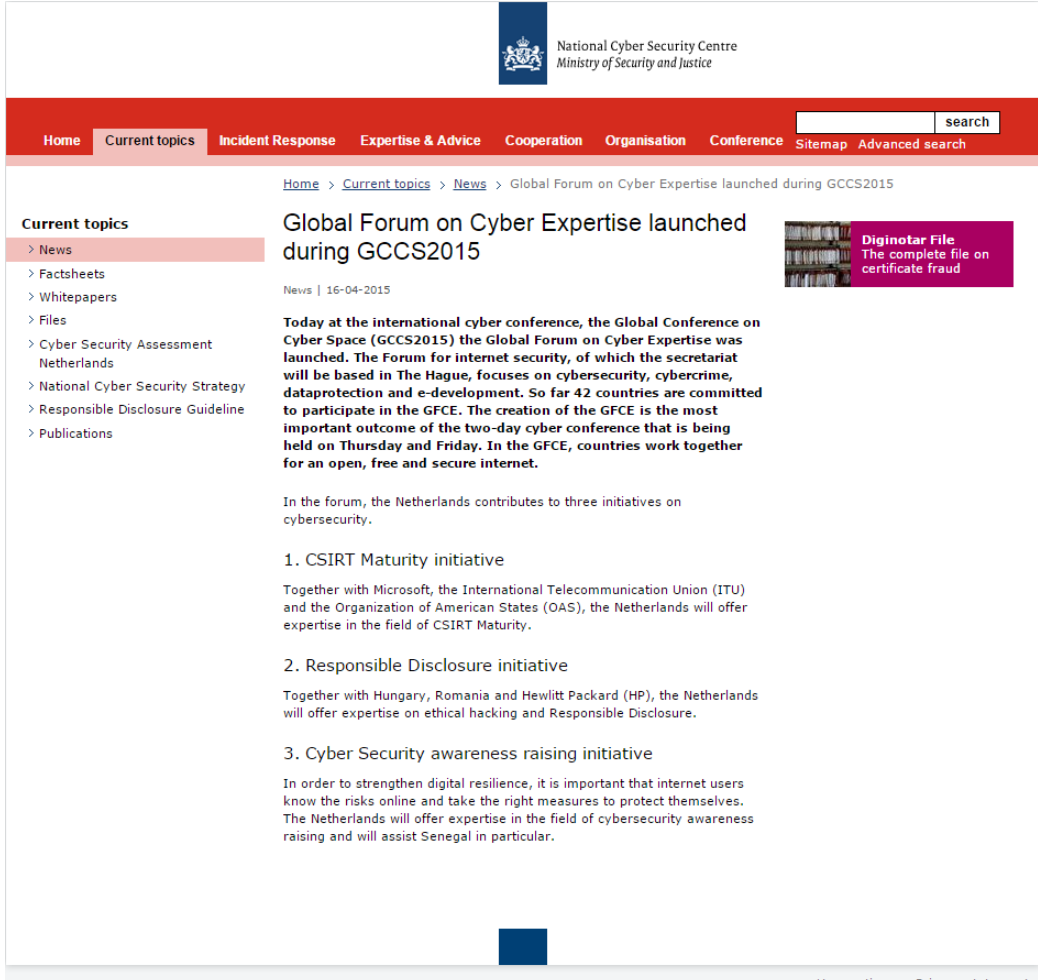
MNOHÉ ORGANIZACE JSOU PROAKTIVNÍ

- <https://bugcrowd.com/list-of-bug-bounty-programs>
- <https://hackerone.com/disclosure-guidelines>
- <https://www.t-mobile.cz/bug-bounty>
- <http://help.soundcloud.com/customer/portal/articles/439715-responsible-disclosure>
- <https://www.airbnb.cz/security>

(...)

TÉMA REZONUJÍCÍ NA MEZINÁRODNÍCH FÓRECH

- EU
- UN GGE
- GCCS2015



The screenshot shows the website of the National Cyber Security Centre (NCSC), part of the Ministry of Security and Justice. The page features a red navigation bar with links for Home, Current topics, Incident Response, Expertise & Advice, Cooperation, Organisation, and Conference. A search bar is located on the right. The main content area displays a news article titled "Global Forum on Cyber Expertise launched during GCCS2015" dated 16-04-2015. The article text states: "Today at the international cyber conference, the Global Conference on Cyber Space (GCCS2015) the Global Forum on Cyber Expertise was launched. The Forum for internet security, of which the secretariat will be based in The Hague, focuses on cybersecurity, cybercrime, dataprotection and e-development. So far 42 countries are committed to participate in the GFCE. The creation of the GFCE is the most important outcome of the two-day cyber conference that is being held on Thursday and Friday. In the GFCE, countries work together for an open, free and secure internet." Below the text, three initiatives are listed: 1. CSIRT Maturity initiative, 2. Responsible Disclosure initiative, and 3. Cyber Security awareness raising initiative. A sidebar on the left contains a "Current topics" menu with options like News, Factsheets, Whitepapers, Files, Cyber Security Assessment Netherlands, National Cyber Security Strategy, Responsible Disclosure Guideline, and Publications. A small purple box on the right contains the text "Digitotar File The complete file on certificate fraud".

TÉMA REZONUJÍCÍ NA MEZINÁRODNÍCH FÓRECH (2)

- *States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICT and ICT-dependent infrastructure*

UN GGE Report on Developments in the field of ICT in the context of international security (22 July 2015, A/70/174)



TÉMA PRO ČESKOU REPUBLIKU?

- Zájem organizací? (soukromý i veřejný sektor)
- Jaké místo pro NCKB/GovCERT?
- Další aktéři?

VÝHODY

- vyšší bezpečnost informačních systémů a ICT systémů
- lepší reputace organizace – předcházení zveřejnění citlivých údajů koncových uživatelů
- předcházení ekonomickým ztrátám
- dobré PR – odpovědný přístup k poskytované službě
- nižší náklady na detekci
- vědomí sdílené odpovědnosti mezi organizacemi a testery



RIZIKA A NEVÝHODY

- vstupní náklady časové, organizační, materiální
- zahlcení hlášenými o nízkorizikových zranitelnostech
- „pozvánka“ k nezákonným zásahům do systémů
- špatné PR v případě nezvládnutého zveřejnění



VLASTNÍK SYSTÉMU/VÝROBCE PRODUKTU (ORGANIZACE)

- **Primární odpovědnost** za bezpečnost systému/produktu
- **Vlastní rozhodnutí**, zda přijme RD politiku
- Požadavky v případě kladného rozhodnutí:
 - Zveřejnění RD politiky
 - Standardizovaný a přístupný komunikační kanál
 - Kapacita na odpovídající reakci
 - Průběžná komunikace a koordinace s ohlašovatelem
 - Systém motivace ohlašovatelů
 - Jasný postoj k právním implikacím



OHLAŠOVATEL (DISCLOSER)

- Nezbavuje se automaticky **právní odpovědnosti**
- **Rychlost** oznámení
- **Důvěrnost** komunikace
- **Přiměřenost** jednání
- Dodržení **pravidel**



NCKB/GovCERT

- Neukládá povinnosti – bez rozhodnutí vlastníka systému/výrobce produktu přijmout RD politiku žádná neexistuje
- Nezasahuje do právního řádu
- Vedlejší role
 - propagace RD
 - informování komunity o zranitelnostech
 - zprostředkování kontaktu
 - koordinace zveřejnění



KYBERKRIMINALITA?

- Zásada **legality** x zásada **oportunity**
 - zahájení trestního stíhání může být nutné
 - RD nezbavuje trestní odpovědnosti
- Institut **zastavení trestního stíhání** podle § 172 TŘ
 - Výkladové stanovisko NSZ?



REAKCE? ZKUŠENOSTI? NÁVRHY?

- Vhodná odvětví?
- Ekonomická výhodnost?
- Motivace testerů?
- Zkušenosti z bug bounty programů?



REAKCE? ZKUŠENOSTI? NÁVRHY?

t.jancarkova@nbu.cz

nckb@nbu.cz