RESPONSIBLE DISCLOSURE - MOŽNOST PRO ČESKOU REPUBLIKU?

Taťána 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**
  - Budapešťská 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

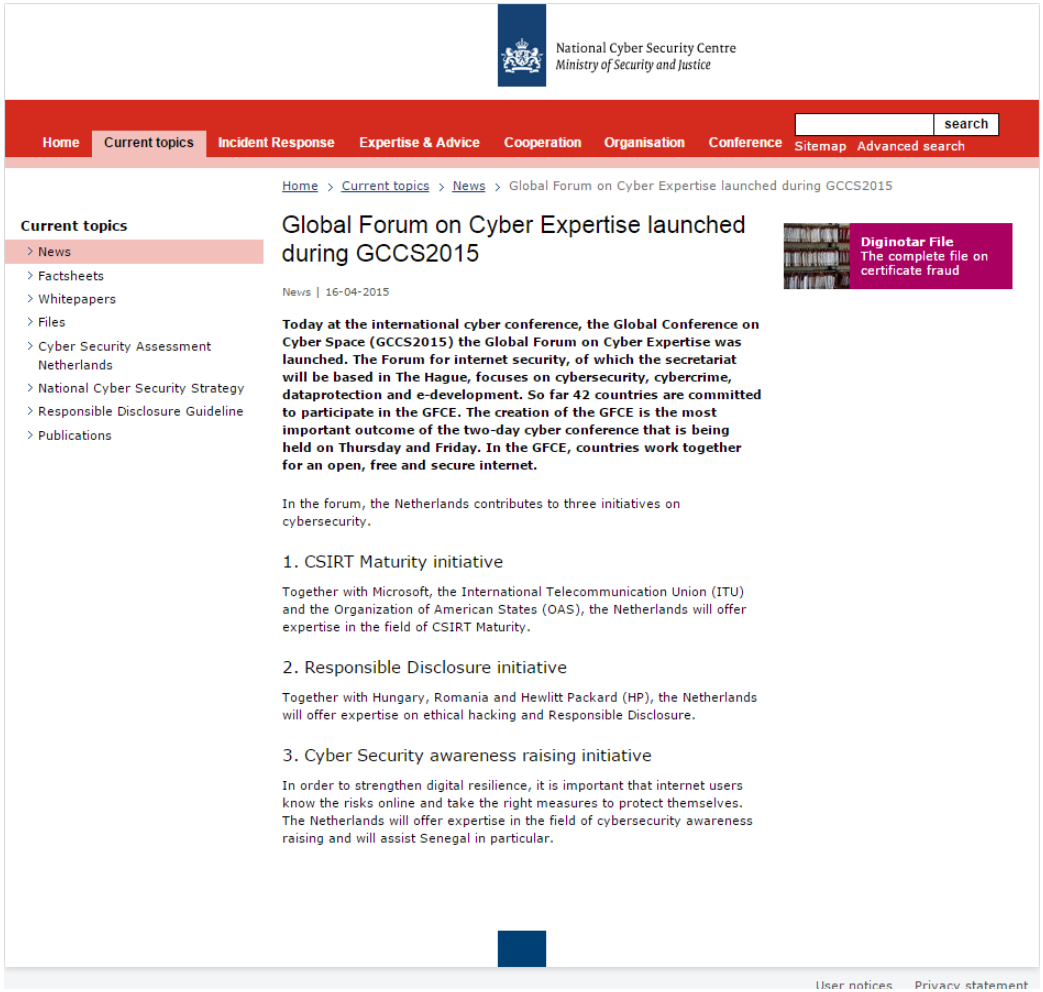
Mnohé organizace jsou proaktivní

- 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



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 hlášeními 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