EXKURZ DO KYBERNETICKÉ BEZPEČNOSTI

Témata

- Exkurz do terminologie
- Exkurz do souvislostí
- Exkurz do historie
- Exkurz do současnosti

Dilema

- Intenzivní rozvoj elektronické komunikace a informačních systémů v ČR
(EU: „*Digital Agenda*“, ČR: eGovernment …)

vs.

- (Dosud) malá pozornost ochraně kybernetického prostoru (na osobní, firemní i státní úrovni)
- *The whole topic is hard to be understood by policy makers*

Exkurz do terminologie

- Počítačová bezpečnost (IT Security)
- Počítačová kriminalita (Cyber Crime)
- Informační bezpečnost a ochrana dat (Information Security / Information Assurance) - WikiLeaks
- Kybernetická bezpečnost (Cyber Security) – ochrana národního kybernetického prostoru – ochrana kritických a základních funkcí státu:
  - Kritická infrastruktura (zákon 240/2000 Sb.)
  - Kritická informační infrastruktura

Exkurz do souvislostí

- Neexistují hranice
  - hranice nejsou v kybernetickém prostoru definovány
- Neurčitost útočníka
  - Hactivisté, organizované skupiny (Anonymous)
  - Nestátní/nenárodní útočníci (teroristé)
  - Státem podporované/tolerované aktivity
- Dostupnost prostředků a nástrojů
- Potřeba velmi rychlé reakce
- Obtížná aplikace nyní platných principů a zákonů (např. čl. 4 a 5 NATO)

Exkurz do (právních) souvislostí

Využití/modifikace stávajícího práva.

- **Teritorialita**: Informační infrastruktura na území státu je subjektem státní suverenity;
- **Ochrana dat**: každý je povinen chránit svou informační infrastrukturu;
- **Sebeobrana**: právo na (kybernetickou) sebeobranu v případě aktuálního nebezpečí
- **Včasné varování**: povinnost varovat před možným útokem

Exkurz do (právních) souvislostí

- **Odpovědnost**: Útok byl spuštěn z území státu - odpovědnost státu za tento útok (?);
- **Spolupráce**: Útok veden přes území státu – povinnost státu spolupracovat;
- **Přístup k informacím**: veřejnost má právo na informace o ohrožení jejich života, bezpečnosti a blahobytu x **OUI**
- **Trestní odpovědnost**: každý má odpovědnost včlenit „kybernetické delikty“ do trestního řádu

Exkurz do kybernetických útoků

- Viry, červy, trojské koně, spam (phishing), malware
- DDoS (BotNet), click-jacking, krádeže identit, web defacement
- Zero-day attack, polymorfní malware
- **Uživatel** (sociální inženýrství)

Nejznámější útoky:

- Estonsko 2007
- Gruzie 2008
- Stuxnet 2010 (Írán + SCADA průmyslové systémy)
  (Supervisory Control And Data Acquitision)

NATO Head of States Summit, Prague 2002

Exkurz do NATO

- **2002**: Zasedání NATO Praha (Cyber Defence [CD] Strategic Concept)
- **2004**: NATO CIRC (**C**omputer **I**ncident **R**esponse **C**apability)
- **2008**: NATO CD Formal Policy & Concept (schváleno tichou procedurou)
- **2008**: NATO CD Management Authority / CD Management Board
- **2012**: NATO CD FOC (Full Operational Capability)

Exkurz do NATO - požadavky

- Vytvořit funkční struktury v oblasti **C**yber **D**efence / **C**yber **S**ecurity na národní úrovni
- Definovat národní CD / CS autoritu
- Podpis MoU (sdílení dat a společný postup)
- Vytvoření funkčních
  - kapacit: (CIRC)
  - struktur (CERT/CSIRT)
- Účast na cvičeních (**C**yber **C**oalition / NCDEx)

Exkurz do struktur

Funkčně:

- CERT (**C**omputer **E**mergency **R**esponse **T**eam)
- CSIRT (…. **S**ecurity **I**ncident ...)
- CIRC (**I**ncident **R**esponse **C**apability)
- RRT (**R**apid **R**esponse **T**eam)

Kompetenčně:

- Vojenský CERT
- Vládní CERT (+ zákon 412)
- Národní CERT

Exkurz do světa

- Snaha definovat/tvořit:
  - Strategii pro kybernetickou bezpečnost
  - Zákon o kybernetické bezpečnosti
  - CERT (vládní/národní) + mezinárodní spolupráci
- USA: US International Strategy for CyberSpace (na www.whitehouse.gov)
- NATO Cooperative Cyber Defence Centre of Excellence (www.ccdcoe.org)

Exkurz do historie v ČR

- **2004**: Státní informační politika – eČesko (MI)
- **2005**: Národní strategie informační bezpečnosti ČR
- **2008**: tichá procedura NATO
- **4/2009**: důrazný požadavek NATO – N(CD)A
- **3/2010**: UV_205: MV - Národní autorita
  - Jmenovat Koordinační radu (MV) pro KB (5/2010)
  - Koordinovat KB v rámci ČR i mezinárodně
  - Zpracovat Strategii + věcný záměr zákona / zákon
  - Zahájit provoz CSIRT/CERT

Exkurz do historie v ČR

- **1/2011: Dohoda s CZ.NIC (registr** domén *.cz):
  - provoz Národního CERT
  - dočasně i provoz Vládní CERT (do 6/2012) x prověrky
- **7/2011**: Strategie ČR pro oblast KB + Akční plán (www.govcert.cz)
- **10/2011**: UV_781: NBÚ – Národní autorita
  - Národní centrum kybernetické bezpečnosti (Brno),
  - Součástí: Vládní CERT
  - Budování od 2012, plně funkční od 2016
  - Věcný záměr zákona o KB (3/2012 Vláda)
  - Tabulky + rozpočet

Věcný záměr zákona o KB

- Konstituce práv a povinností orgánu státu, dalších orgánů státu a soukromoprávních subjektů;
- Mechanismus přenosu informací nezbytných pro prevenci před kybernetickými hrozbami;
- Vybudování systému včasného varování, poskytování pomoci při zavádění preventivních opatření a protiopatření;
- Standardizace nastavení bezpečnosti systémů nezbytných pro chod státu v rámci KII státu
- Nastavení pravidel pro koordinaci činností pro a při odvracení hrozícího útoku na prvky KII státu
  - Více na www.nbu.cz

Strategie KB

Východiska:

- ICT významně ovlivňují společnost i ekonomiku
- Zranitelnost ICT → zranitelnost státu
- Individuální odpovědnost
- Přiměřenost opatření

Strategie:

- Legislativní rámec
- Národní centrum KB + vládní CERT
- Ochrana KII + ochrana veřejné správy
- Mezinárodní spolupráce
- Zvyšování povědomí o KB (vzdělávání)

Vojenský pohled

- Kybernetický prostor = páté bojiště (země, moře, vzduch, vesmír, Internet)
- Mít schopnost ochránit své systémy a aktivity
- Mít schopnost plánovat a provádět operace v kybernetickém prostoru (US Cyber Command)
- Kybernetický útok = fyzický útok (+ fyzická reakce)
- „*the cyber domain is in constant conflict*“
- „*the major battle is in unclassified internet*“

Možné otázky

- Jak poznáme, že se jedná o útok a nikoliv o chybu?
- Jaká je identita útočníka (a jak jí dokázat)?
- Kdy je útok vyhlášením války?
- Jak má národní stát reagovat na kybernetický útok?
- „Pravidla války“ – v kybernetickém prostoru?

DĚKUJI ZA POZORNOST