MASARYKOVA UNIVERZITA

Kybernetická kriminalita a kybernetická bezpečnost

Václav Stupka

1. Úvod do problematiky

Aspekty rozvoje IT

- Pozitivní
  - Rozvoj vědy a techniky, komunikací
  - Dostupnost informací
- Negativní
  - Tvorba nového prostoru pro páchání kriminality
  - Nové druhy kriminality
  - Pocit beztrestnosti pramenící z „anonymity“
  - Vznik závislostí, aj.

Kybernetický zločin

- Protiprávní jednání spočívající v zneužití ICT jako prostředků ke způsobení závažných škodlivých následků, anebo v kriminálním chování jehož předmětem jsou ICT
- Výskyt v kyberprostoru
- Asymetrická charakteristika kybernetických útoků

Náchylnost ICT

- Globální dostupnost
- Rychlost
- Anonymita
- Dostupnost
- Asymetrie mezi „útočníky“ a „obránci“

Dělení kybernetické kriminality

- Kybernetická kriminalita v užším smyslu
- Trestné činy páchané pomocí počítačových systémů
- Trestné činy páchané za použití počítačů

2. Působnost práva v kyberprostoru

Teritorialita práva

- Jurisdikce a střet kultur
- Mezinárodní spolupráce

Snaha o harmonizaci

Úmluva o kyberkriminalitě

Zákony se vztahem ke kybernetické kriminalitě

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 141/1961 Sb., o trestním řízení soudním – trestní řád
- Zákon č. 200/1990 Sb., o přestupcích
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 40/1964 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 227/2000 Sb., o elektronickém podpisu

Trestní právo

- Procesní
- Hmotné

Trestný čin

- Protiprávní čin, který trestní zákon označuje za trestný čin a který vykazuje znaky uvedené v zákoně
- Formální pojetí trestného činu
- Materiální korektiv
- Ultima ratio
- Při spáchání trestného činu není vyloučena odpovědnost občanskoprávní

3. Kybernetické útoky

Hacking

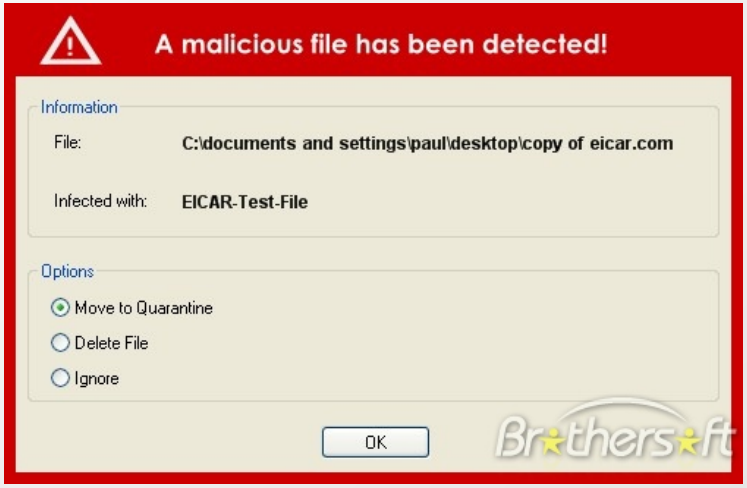
- Nemusí se vždy jednat o trestnou činnost
- Penetrační testování
- § 230 TZ Neoprávněný přístup k počítačovému systému a nosiči informací:
  - Ten kdo překoná bezpečnostní opatření a získá přístup k počítačovému systému,
  - Ten kdo získá přístup k počítačovému systému a:
    - Neoprávněně užije tamní data, osobní informace
    - Vymaže, potlačí, sníží kvalitu, dostupnost dat
    - Padělá, nebo pozmění data
    - Neoprávněně vloží data
    - Učiní jiný škodlivý zásah do technického vybavení

Cracking

- Nejednotná definice a vymezení k hackingu
- Také nemusí být trestný
- § 230 TZ Neoprávněný přístup k počítačovému systému a nosiči informací
- § 270 TZ Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

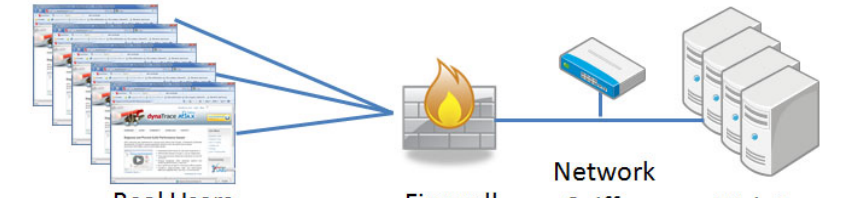
Malware

- Různé formy: viry, troské koně, spyware, adware, keyloggery apod.
- § 231 TZ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému
- § 230 Neoprávněný přístup k počítačovému systému
- § 207 Neoprávněné užívání cizí věci



Sniffing

- Zachytávání datové komunikace, nelegální odposlech, záznam telekomunikačního provozu
- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin uchovávaných v soukromí
- § 231 opatření a přechovávání přístupového zařízení

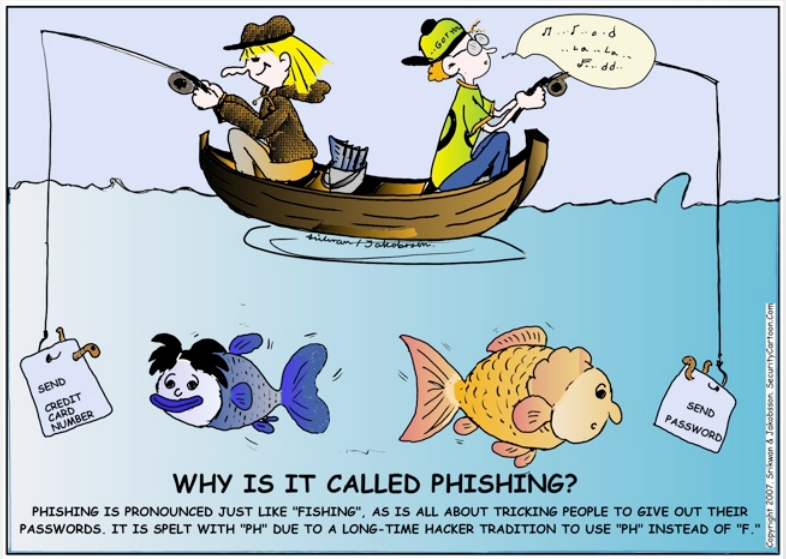


Spam

- Množství spamu kontinuálně roste. Až 99% veškeré emailové komunikace.
- Různé formy: obchodní sdělení, podvody, viry, řeťězové maily, hoax, phishing, aj.
- Boj proti spamu – omezování práva na svobodu projevu ve prospěch ochrany osobní integrity
- Zákon o elektronických komunikacích - § 93
- Zákon o některých službách informační společnosti - § 2 písm. f)

Phishing

- Různé formy podvodného vylákání peněz od uživatele
- Velmi častý druh spamu. Hlavním prostředkem ochrany je osvěta
- § 209 Podvod
- § 234 Neoprávněné opatření padělání a pozměnění platebního prostředku

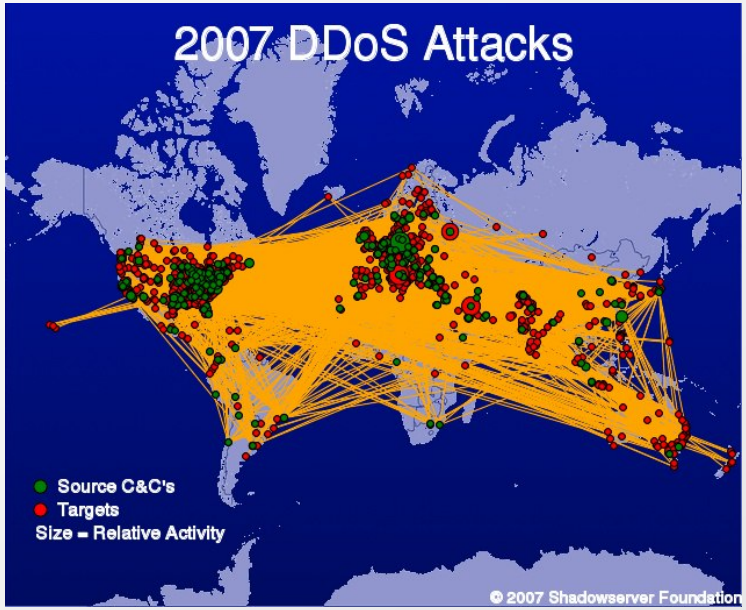


Šíření závadného obsahu

- Různé druhy: zakázané druhy pornografie, nenávistná a extremistická sdělení, pomluvy, stalking
- Různé trestněprávní postihy:
  - § 191 šíření pornografie
  - § 192 výroba a jiné nakládání s dětskou pornografií
  - TČ proti lidskosti, míru
  - TČ proti pořádku ve věcech veřejných
  - § 345 Křivé obvinění
  - § 184 Pomluva
  - § 354 nebezpečné pronásledování

DoS, DDoS

- Zahlcení poškozeného systému nadmírou požadavků
- Složité vyšetřování i stíhání
- § 228 Poškození cizí věci
- § 230



Porušování autorských práv

- Různé formy: P2P, ftp servery, file hosting, streaming, warez fóra, atp.
- Je stahování v pořádku?
  - Volné užití díla – rozmnoženina pro soukromé užití
  - Podmínky: dílo musí být zvěřejněno, není možné obcházet DRM, pouze k osobní potřebě
  - Výjimky: software, databáze, camcording…
- Jinak prostřednictvím licencí

Další specifické útoky

- Cybersquatting
- Racketeering
- Kyberterorismus
- Kybernetická válka
- Kybernetická vražda

4. Kybernetická bezpečnost

Podstata ochrany kyberprostoru

- Bezpečné a spolehlivé fungování ICT je jedním ze základních předpokladů prosperity a trvalého ekonomického růstu
- Rozvoj ICT představuje bezpečnostní výzvu pro celou informační společnost
- Rostoucí závislost společnosti na ICT zvyšuje zranitelnost státu a jeho občanů vůči kybernetickým útokům

Kybernetická kriminalita a kybernetická bezpečnost

Primární oblast zájmu CERTů

Neúmyslné bezpečnostní incidenty
nehody; tecnické poruchy; lidské chyby

Úmyslné útoky proti důvěrnosti, dostupnosti a integritě ICT (Typ "1")
útoky zločinců; teroristů; států; nestátních skupin; útoky proti kritické infrastruktuře; jiné útoky proti ICT

Trestné činy páchané prostřednictvím ICT (Typ "2")
podvody;držení dětské pornografie; šíření závadného obsahu

Primární oblast zájmu OČTŘ

Trestné činy související s ICT (Typ "3")
jakékoliv trestné činy kde hrají roly elektronické důkazní prostředky

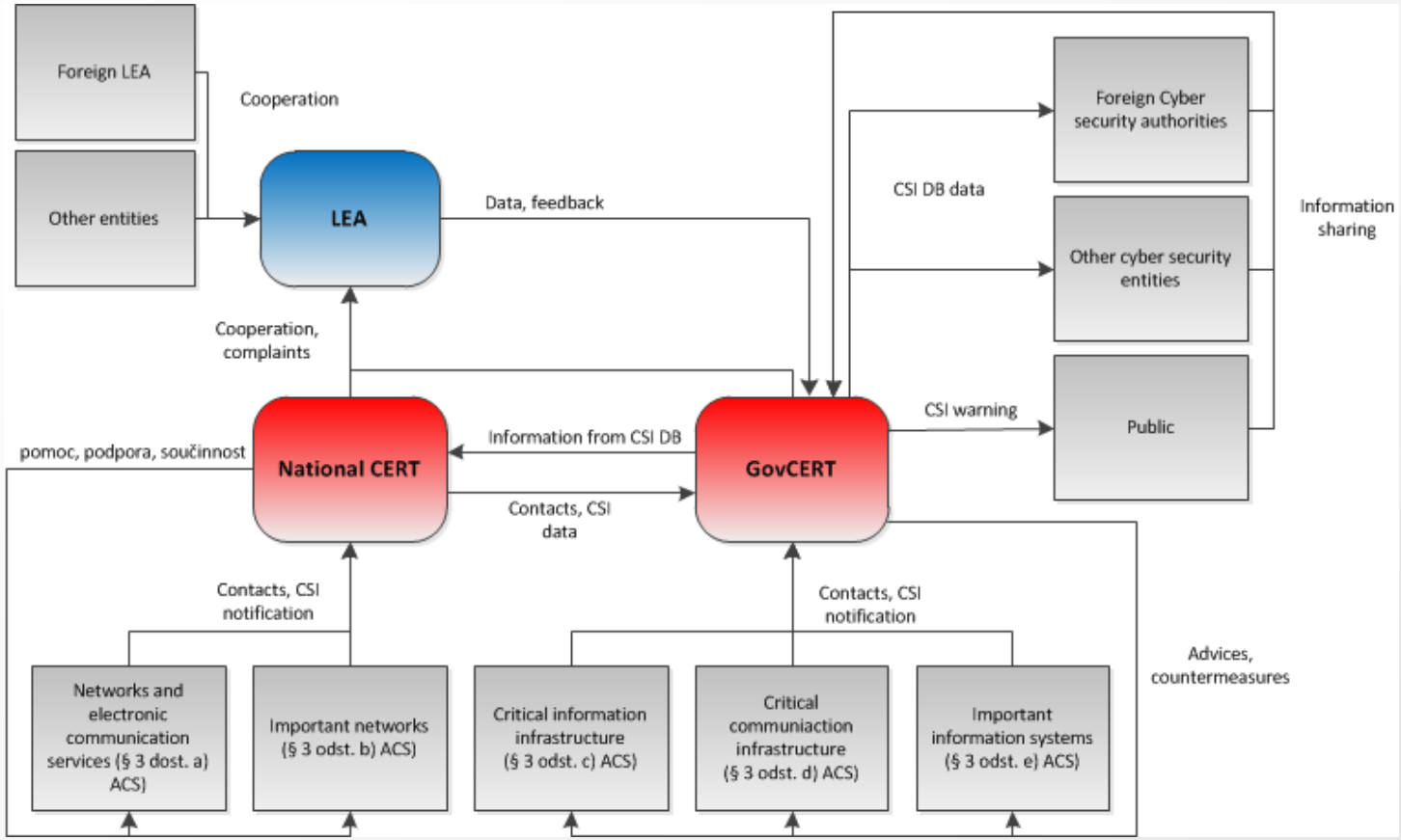
Ve světě

- Nedostatečná pozornost, organizovanost
- V poslední době patrná globální snaha o zjištění kybernetické bezpečnosti jednotlivých států
- Nutnost vnitrostátní i mezinárodní kooperace
- Sdílení best practises a informací o hrozbách
- Důležitá informovanost uživatelů
- Vznik mezinárodních organizací sdružujících CERT/CSIRT týmy

V ČR

- Přechod gesce pod NBÚ
- Zatím spíše soukromá sféra
- Zákon o kybernetické bezpečnosti
- Cíl – vytvořit vládní CERT, dohled nad kritickou infrastrukturou
- Definování standardů, osvěta, dohled, reakce, prevence
- Kooperace s ostatními CERTY (i mezinárodní)

Systém KB v ČR



Věcná působnost zákona o KB

- Kritická a ostatní část kyberprostoru
- Kritická: Kritická informační infrastruktura vs. Kritická komunikační infrastruktura
- Ostatní: komunikační infrastruktura, ISVS

- Kybernetická bezpečnostní událost

Osobní působnost zákona o KB

- ISP
- Správci kritické komunikační infrastruktury
- Správci IS kritické informační infrastruktury
- Správci ISVS

KBU a KBI

- Kybernetická bezpečnostní událost
  - Může způsobit narušení bezpečnosti služeb, informací, nebo integrity sítí
- Kybernetický bezpečnostní incident
  - Vlastní narušení

Bezpečnostní opatření

- Preventivní (organizační, tehcnická)
- Varování
- Reaktivní
- Ochranná

Stav kybernetického nebezpečí

- Pro případ rozsáhlé bezpečnostní události, která by mohla ohrozit fungování služeb informační společnosti v ČR, nebo v mezinárodním měřítku.
- Vyhlašuje ředitel NBÚ
- Nejvýše 7 dnů
- Krizový štáb
- Nouzový stav
- Povinnost ISP k protiopatření

Každý svého štěstí strůjcem.

Děkuji za pozornost!

vaclav.stupka@law.muni.cz