Odborný seminář IKSP
Vybrané aspekty kybernetické kriminality

---

# Kybernetická kriminalita v prostředí cloudu

Ing. Jindřich Kodl, CSc.

13. 10.2016

# Služby cloudu

- Zavádění a využívání cloudu
  - Žádné známky zpomalování
  - Rozšiřování služeb velkou rychlostí napříč všemi sektory
- **Cloud – dobrý sluha, zlý pán**
- Sdílení zdrojů k dosažení úspor při zpracovávání dat
  - Výhodné pro podniky
  - Atraktivní pro zločince

# Atraktivnost pro kriminalitu

- Cloudové služby soustřeďují velké objemy dat na jednom logickém místě
- Větší investice do času i zdrojů vyžadovaných k útoku se hackerům vyplatí

*Zúžení problematiky v přednášce*

- Problematika veřejných cloudů
- Charakter útoků na privátní cloudy se může pohybovat ve standardní rovině

# Výhoda cloudu

- U jednotlivých podniků je počítačová kriminalita často důsledkem špatných bezpečnostních protokolů a nevhodného zabezpečení IT podpory.
- Cloudy jsou farmy šifrovaných serverů nakonfigurovaných k šíření informací přes širokou oblast
  - ⇒ Zaměření útoky při šíření informací v kyberprostoru při plánování masivnějších útoků,
  - ⇒ Cílem je identifikovat slabá místa v zabezpečení komunikace

# (Ne)výhody cloudu

Takže, může cloud computing předcházet a snížit kybernetickou kriminalitu?

- V případě uložených dat - omezení možností jejich získání => poukázání na skutečnost, že narušení bezpečnosti dat cloudu může být významně eliminováno.
- Mnohé úspěšné útoky ale stále vedou k pochybnostem, že úložiště v rámci třetí strany je krok správným směrem.

# (Ne)výhody cloudu

- Hlavní výhody v cloudovém prostředí je zabezpečení backendu cloudu => zabezpečení uložených dat.
  - *Zde mohou snadněji páchat trestnou činnost zaměstnanci než externí narušitelé*
- Potvrzení:

  Zpráva zveřejněná před časem McAfee a Guardian Analytics uvedla, že *hackeři nyní sami používají cloudové infrastruktury , aby využili výhod poskytovaných služeb při přípravách svých kampaní*.

# (Ne)výhody cloudu

- Hlavní nevýhoda v cloudovém prostředí spočívá ve frontendu cloudu

- Správa dat uživatelů (podniků, organizací jednotlivců) přechází z prostoru uzavřeného perimetrem do volného kyberprostoru.

# Cloud - případy narušení

- Firemní cloud computing – využití cloudu ve formě sjednané služby
  - nastavené parametry bezpečnosti – nutné útoky „zvenčí“
- Cloudová řešení u běžných uživatelů
  - Citlivé informace předávány do nechráněných cloudů
  - Zabezpečená data v cloudech – data může číst nebo indexovat sám poskytovatel

# Typy útoků

**Jaké typy útoků jsou nejčastější proti službám cloudu**

- Objemové útoky – zahlcení propustnosti přenosového kanálu
- Záplava pakety SYN = SYN-flood útok označovaný jako Denial of Service.
- Využití botnetů – zahlcení DNS serverů (domain name server)
- sofistikovaná dlouhodobá napadení přístupových cest dat a vlastního obsahu dat během jejich cesty do cloudu

# Typy útoků

**Typy útoků vůči elektronickým účtům**

- Útoky postavené na využití malware zavedeného do pracovní stanice klienta či zaměstnance
- Osvědčené malwarové nástroje typu SpyEye  k získání přístupu k elektronickému bankovnictví obětí
- Automatizované napadení
- Stále nové typy malware

# Typy útoků

Napadení autentizačních a autorizačních nastavení jednotlivých uživatelů.

- Stálé využívání jednofaktorové autentizace (nezřídka uživatelské jméno a heslo)
- Narušení oprávnění umožňuje přístup k datům i v cloudových aplikacích.
- Získané pověření uživatele může v rámci platného přihlašovacího procesu obejít i bezpečnostní prvky poskytovatele cloudu i v případě šifrované komunikace

# Případy útoků

Obecně řečeno:

Kybernetická kriminalita v případě služeb cloudu - teroristické činnosti úspěšné zejména skrze služby, které podporuje a sdílí daná informační či komunikační síť.

Využívá zejména „nebezpečného“ chování uživatelů, nejen při komunikaci v rámci veřejných sítí (Internetu), ale i v prostředí poskytovaných služeb, ve vztahu k ochraně svých dat.

Zatím se jedná o rovinu krádeží nikoli však loupeží