Analýza SSL provozu

Václav Stupka

SSL provoz

- Secure socket layer
- Vrstva mezi transportní a aplikační
- Založená na asymetrickém a symetrickém šifrování
- Nejčastěji využíváno pro HTTPS
  - Eshopy
  - Platební terminály
  - Různé služby

Proč dekrypce?

- Nebezpečnost bezpečnostního nástroje
- Bezpečnostní analýza přenášených dat
- Zneužití:
  - Přenos dat k útočníkovi
  - Průmyslová špionáž
  - Etc.
- Roste míra zneužití
- Zabezpečenou komunikaci nelze analyzovat

Jak to funguje?

- Asymetrická vs symetrická kryptografie
- Handshake a předávání klíčů
- Přenos v rámci zabezpečené session
- Man in the middle

Kdo?

- ISP
- Provozovatel sítě
- Zaměstnavatel
- Pentester
- Já?
- ZoKB?

Trestněprávní kvalifikace

- § 230 – neoprávněný přístup k počítačovému systému a nosiči informací
  - Počítačový systém?
  - Nosič informací?
- § 182 – porušení tajemství dopravovaných zpráv
  - Co je tajemstvím dopravovaných zpráv?
- § 231 – opatření a přechovávání přístupového zařízení a hesla
  - Úmysl spáchat TČ (§§ 230 a 182)

Jak tedy?

- §12/2 Společenská škodlivost a ultima ratio
- Výkon práv povinností?
- § 30 svolení poškozeného
- § 31 přípustné riziko
- §§ 28 a 29 krajní nouze a nutná obrana

Další možné typy odpovědnosti

- Soukromoprávní –
  - nemajetková újma a škoda
- Správněprávní –
  - osobní údaje,
  - ZEK,
  - ZoKB

Závěr a diskuse

- Analýza je v podstatě nutná
- Potřeba ochrany soukromí
- Jak se vyrovnat se vznikem odpovědnosti?

Díky za pozornost

vaclav.stupka@law.muni.cz