IT bezpečnost na ZČU včera, dnes a zítra

Seminář CIV by Ing. Petr Žák

Úvodní slovo, aneb o čem to dnes bude?

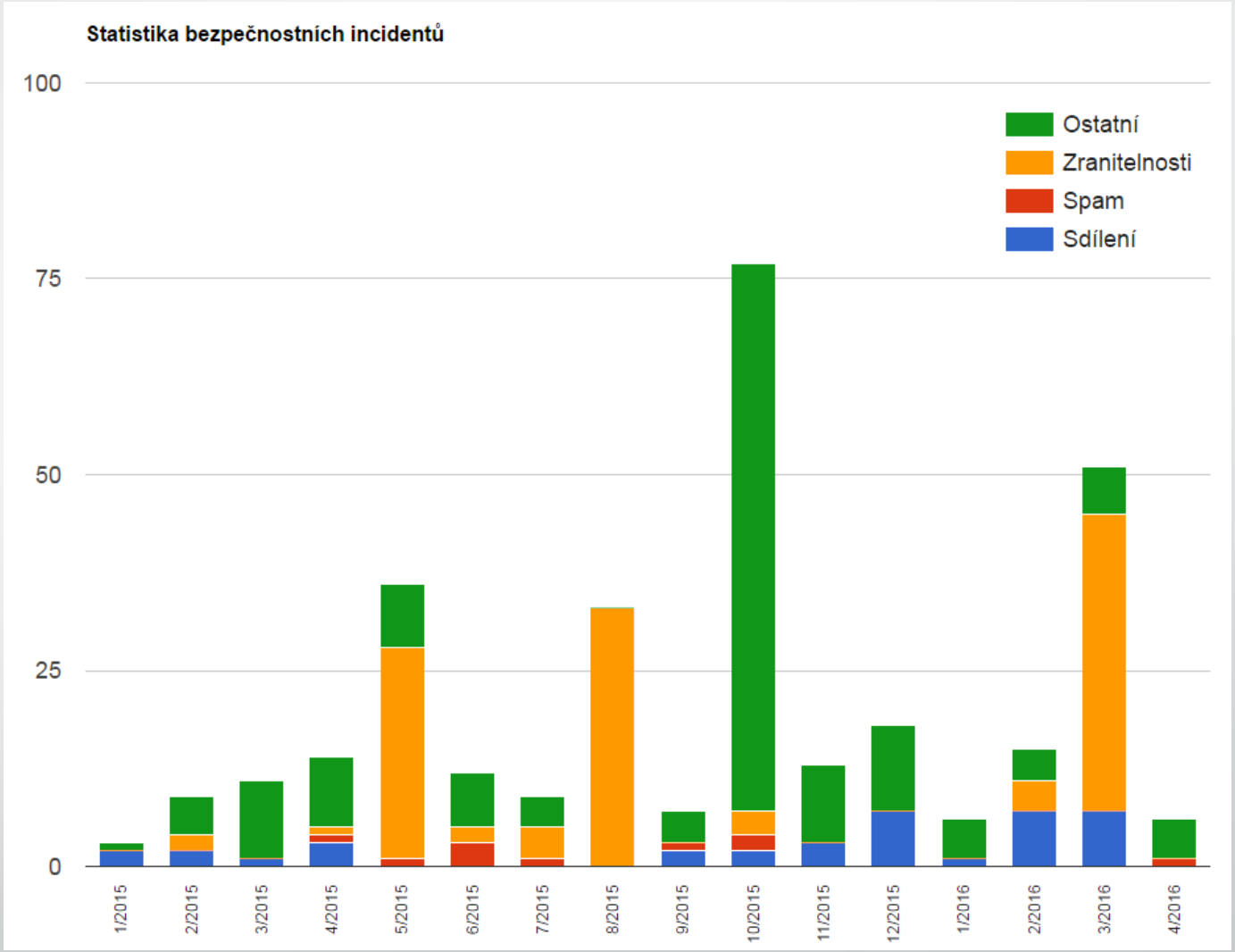
- Shrnutí IT bezpečnostních incidentů na ZČU za poslední cca rok
- Informace o současných hrozbách a problémech
- Plány do budoucna v oblasti IT bezpečnosti na ZČU
- Diskuse

Minulost

...co už je snad za námi

Trochu statistiky

...pro začátek neuškodí



Tiskárny aneb FTP

- Většina síťových tiskáren umožňuje připojení přes FTP a upload souboru
  - Často přístupné odkudkoli bez přihlášení (!), někdy nelze omezit/vypnout
  - Pro nahrání firmwaru, jakýkoli jiný soubor však zpracuje a vytiskne
  - Upload souboru, který tiskárna neumí zpracovat => chybový stav typu „zběsilý tisk“
- Útočníci šíří malware přes otevřená FTP
  - => pokus o upload na tiskárnu
- Řešení: omezit/vypnout, vyžadovat přihlášení, použít firewall
- Zabezpečení administračního rozhraní!

Ilegální software

- Nové metody obrany proti pirátskému softwaru (automatické hlášení) => výrazně vyšší pravděpodobnost odhalení
- Rozsáhlý případ na ZČU
  - Desítky ilegálních instalací na studentských i univerzitních (!!!) strojích
  - Stížnost ze strany vlastníka => závažný problém legální i provozní
    - Nutno řešit, odstraňovat, vysvětlovat => ztráta času
    - Odmítnutí prodeje dalších licencí do vyřešení => provozní problém
    - Možnost legálních následků a z nich plynoucích finančních nákladů
    - Poškození dobrého jména a image ZČU
- Řešení: nepoužívat!

Houdini

- „Blast from the past“
- Virus – „jednoduchý“ skript, šíření přes USB disky, uživatelské spuštění
- Nedetekován antivirovými systémy
- Veliká fluktuace USB disků, půjčování, veřejné stroje => masivní nákaza, obtížné zastavení
- Nakonec rozebrán FLAB CESNET a nákaza zlikvidována
- Pomoc i externím subjektům
- Zvláštní seminář 8.6.2016

Současnost

…co nás trápilo, trápí a trápit ještě bude

Ransomware

- Pravděpodobně největší hrozba současnosti
- Zašifrování dat či celého disku, požadavek na výkupné, často není jiná možnost obnovy než zaplatit
- …a bude hůř!
  - „Easy money“ pro útočníka => veliká „oblíbenost“
  - Snadné provedení útoku; zdrojové kódy dostupné, „Malware as a Service“
  - Různé vektory útoku: e-mail, web, skripty, MS Office makra…
  - Nové verze každý den (!) => antiviry často nedetekují
- Řešení: zálohovat, zálohovat, zálohovat!
  - Trvale připojený externí disk nebo namapovaný AFS projekt/cloudové úložiště není dobrá záloha!

Služby „otevřené do světa“

- Remote Desktop (RDP), SSH…
- Nebezpečí uhádnutí hesla, nebezpečí zneužití zranitelnosti
- Scany a pokusy jsou na denním pořádku!
- Řešení:
  - Službu nepotřebuji => službu vypnu
  - Omezit přístup pouze na určitý IP rozsah, použít VPN
  - Silná hesla (!), fail2ban…

Zranitelnosti

- Šifrovací protokol SSL (HTTPS, SMTPS…)
  - Řada objevených zranitelností (Heartbleed, POODLE, FREAK, LOGJAM…)
  - Zastaralé šifrovací algoritmy
  - Řešení: Správná konfigurace serverů (https://www.ssllabs.com/ssltest/), použití TLS
- Content management systémy pro web
  - Wordpress, Drupal, Joomla… + pluginy
  - Řešení: Aktualizovat, nepoužívat nebezpečné pluginy

…a spousta dalšího

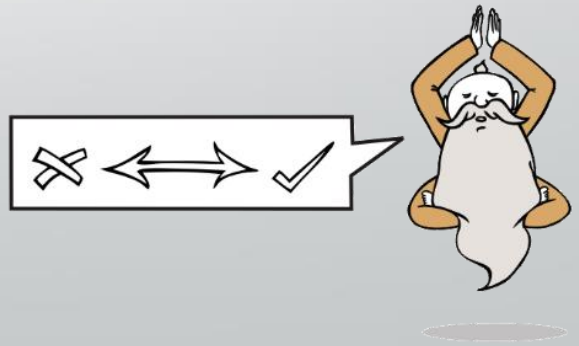
- IT bezpečnost je nekonečný proces; incidenty, problémy a výzvy každý den
- Ze strany WIRT/CIV:
  - Reakce: manuální i automatická detekce incidentů, odpojování problematických strojů a uživatelů, odstraňování malwaru, pomoc správcům, poučení uživatelů…
  - Prevence: vyhledávání a odstraňování zranitelností, pořádání seminářů a školení…

Zpátky do budoucnosti!

...velkolepé plány

Firewall nové generace

- Služba „Zabezpečení zařízení v katedrální síti“ (support.zcu.cz)
- Možnost umístit část segmentu za firewall a omezit přístup pouze na definované IP rozsahy
- Primárně pro „hloupá“ zařízení bez vlastního FW (tiskárny, kamery, průmyslová zařízení, IoT prvky…)
- Zatím pouze v kampusu Bory ☹



McAfee Endpoint Security

- Náhrada VSE a HIPS + nově kontrola webových stránek
- Antivirus + Firewall + Web Control
- Moderní uživatelské rozhraní, lepší ovládání, nová funkčnost, podpora do budoucna…větší, lepší, hezčí!
- Postupný upgrade, v současné fázi na IS strojích, lokálně spravované v létě, úplný konec starých modulů cca září/říjen
- 15.6.2016 seminář pro lokální správce

Semináře

- Seminář o IT bezpečnosti pro vedoucí pracovníky
  - Základní informace, největší hrozby, rady a doporučení, zodpovědnosti, materiály
  - Cílem zvýšit/vytvořit povědomí o existenci problematiky
- - // - pro zahraniční pracovníky
  - Modifikace na žádost UJP
- Budeme opakovat, možno i na vyžádání

Konec

Děkuji za pozornost, je čas na diskusi…