Seminář pro lokální správce

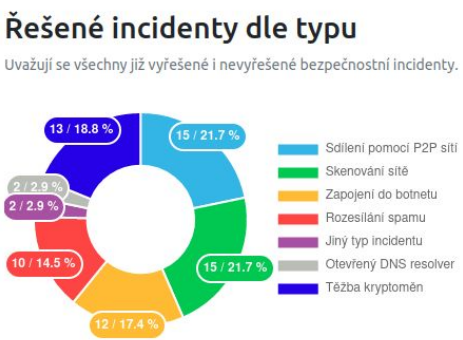
Bezpečnostní okénko

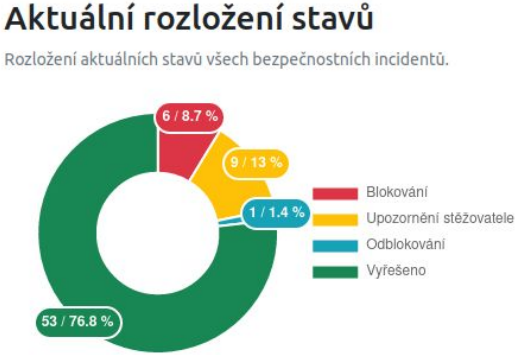
Oddělení Informační bezpečnost

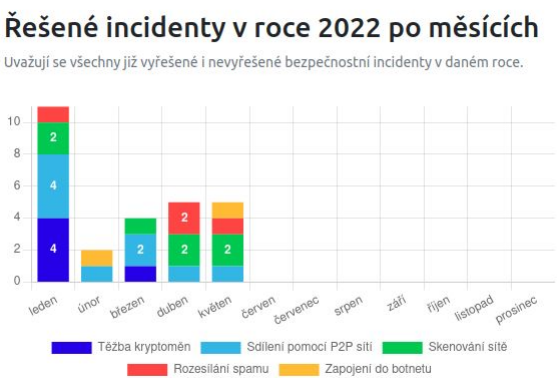
Jiří Čepák, 8. 6. 2022

Nový systém pro správu incidentů

- uživatel sphr2 už není, přichází banan
- standardizovaný text oznámení
- snadné a rychlé řešení incidentů
- přehlednost a statistiky







Karanténní síť

Blockator

Připojení zablokováno

Toto zařízení bylo z důvodu způsobení bezpečnostního incidentu zablokováno bezpečnostním týmem WIRT.

Důvod zablokování

Bylo detekováno nevhodné chování tohoto zařízení, které indikuje jeho napadení virem nebo jiné zneužití. Po odvirování, popř. přeinstalování zařízení můžete použít zde uvedený formulář nebo některou z dalších možností a dát nám vědět, že byl incident vyřešen a jakým způsobem.

Pro více informací, prosím, kontaktujte svého lokálního správce – viz jejich univerzitní, popř. kolejní seznam.

Kontaktujte bezpečnostní tým

Pokud byly splněny kroky uvedené v důvodu zablokování, nebo máte nějaký dotaz, je možné požádat o odblokování nebo kontaktovat bezpečnostní tým některou z následujících možností:

- formulářem níže,
- reakcí e-mailem na lístek, ve kterém se bezpečnostní incident řeší, tj. RT 360519,
- kontaktováním bezpečnostního týmu WIRT.

Váš dotaz, popř. Vámi provedené kroky

Odeslat

PHISHINGATOR.ZČU.CZ

- Testování/cvičení uživatelů na vašich pracovištích
- Role správce testů vs. Naše kooperace
- Návod pro správce testů:

https://support.zcu.cz/index.php/Phishingator_%E2%80%93_N%C3%A1vod_pro_spr%C3%A1vce_test%C5%AF

Antivirové řešení

- Konec stávající smlouvy na McAfee 31. 12. 2022
- Letos soutěžení nového řešení
- Snaha zůstat u McAfee

- Kaspersky
  - nepotvrdila se žádná rizika v souvislosti s válkou na Ukrajině
  - přesto řada společností řešení opustila
- Rozhodnutí z ICT komise
  - konec nákupu nespravovaného antivirového řešení, používat Windows Defender

Penetrační testy 4/2022

- nálezy jsou řešeny s konkrétními správci
- apel na všechny:
  - Zabezpeč(uj)te všechna zařízení v síti
    - různá IoT zařízení
      - RPi s implicitním přihlášením napadené za jednotky hodin
    - síťové tiskárny
      - implicitní admin přístup
      - dostupné z Internetu
  - Vyvarujte se zastaralým a neaktualizovaným OS
    - v síti webnet jsou stále Windows XP (konec 4/2014) a Windows 7 (konec 1/2020)
    - při pentestech nalezena zranitelnost EternalBlue (opravena v r. 2017 i na tehdy nepodporovaných OS)

Důležité

- Vždy změňte implicitní hesla pro vzdálený přístup
- Vždy omezte přístup na firewallu
  - na zařízení
  - s využitím síťového firewallu
- Vždy vypněte služby, které nejsou využívané nebo potřeba
- Vždy pravidelně aktualizujte a je-li to možné, nastavte automatické aktualizace

Bezpečnosti zdar!