

Bezpečnostní okénko

Seminář pro lokální správce

Jiří Čepák / 10. 3. 2020

Skupina WIRT

https://support.zcu.cz/index.php/WIRT_-_WEBnet_Incident_Response_Team

Jiří Čepák

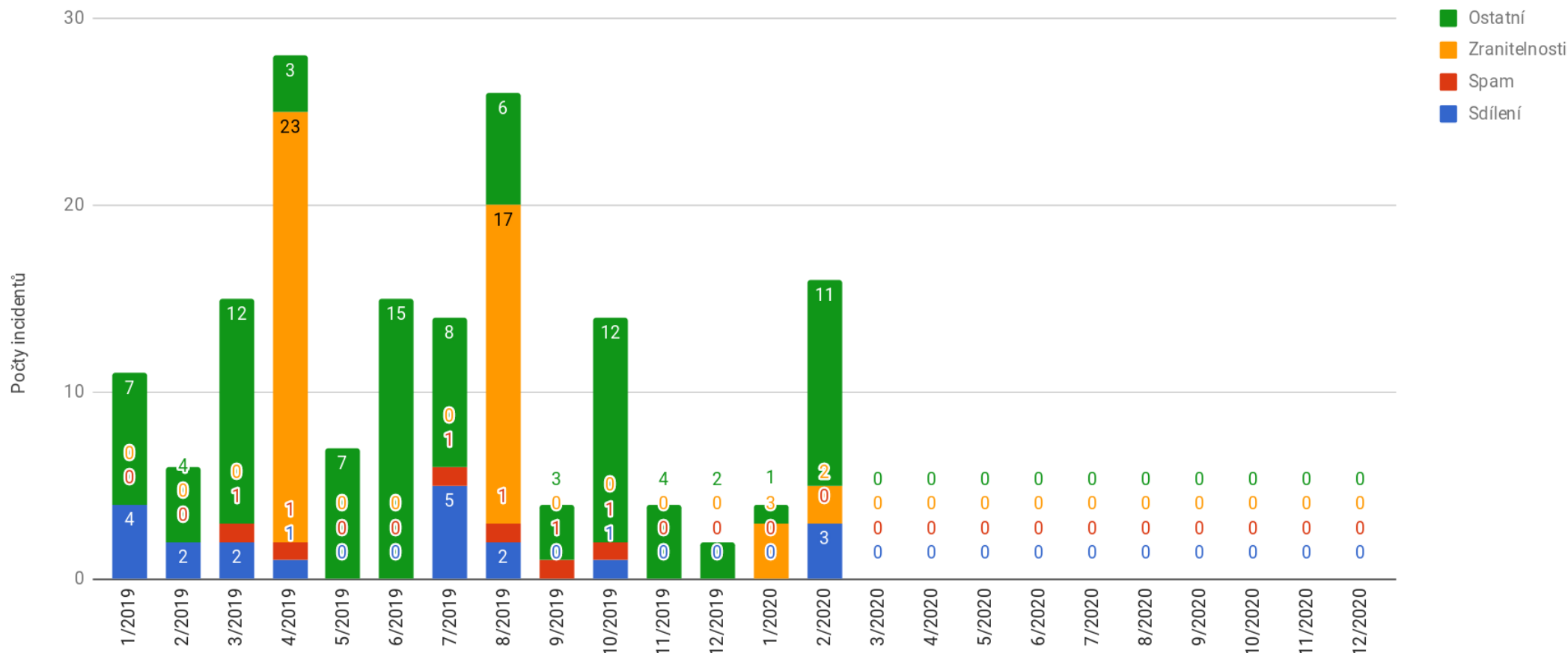
+ Martin Šebela



- Aleš Padrta



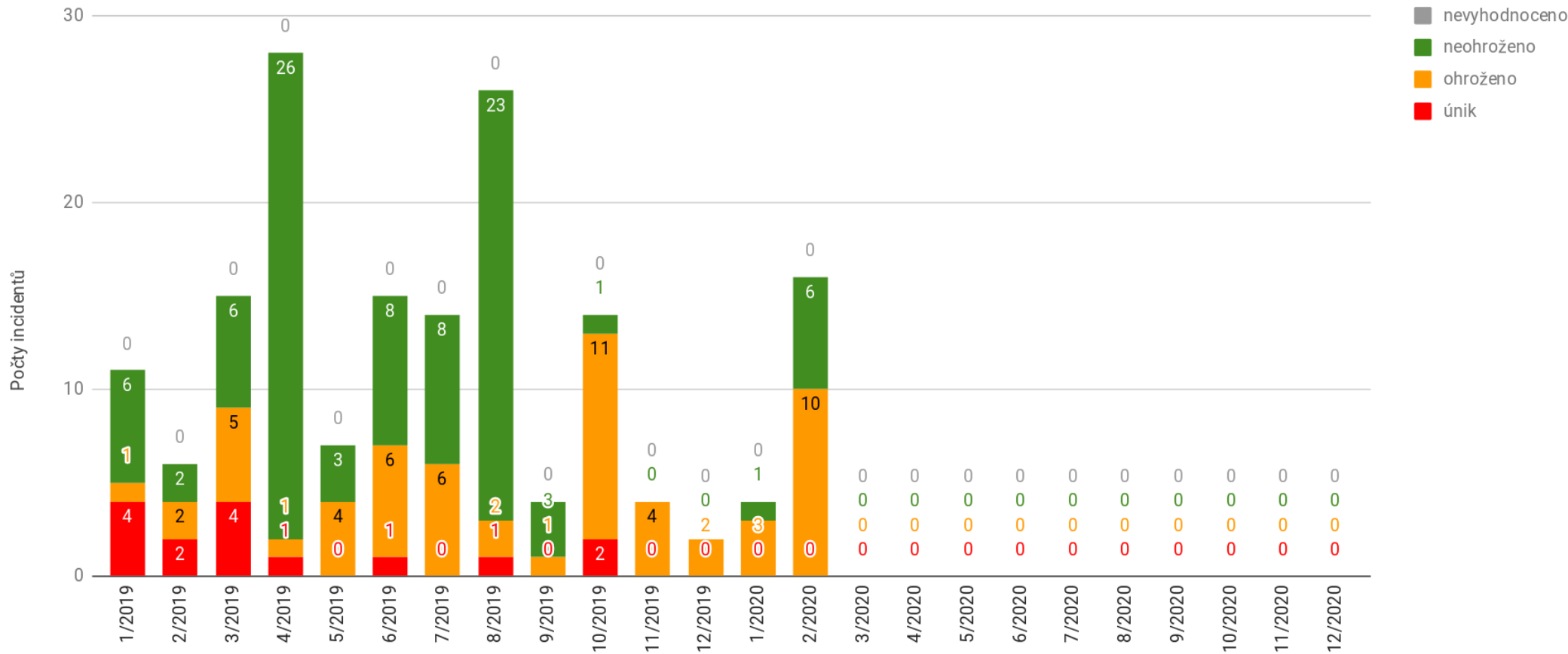
Ohlédnutí za uplynulým rokem – statistika incidentů



4/2019 – UDP 3702 – WS-Discovery – zranitelné vůči DDoS útokům

8/2019 – BlueKeep – chyba v RDP protokolu

Statistika incidentů z pohledu ohrožení osobních údajů



TOP Incident

- cca. 10 dnů zpět
 - Masivní útok na RDP
 - Zašifrované počítače ransomwarem
- Odpojení počítačů od sítě
- Zajištění logů a imagů disků
- Analýza
- Stanovení vektoru útoku
- Obnovení ze záloh
- Opatření
 - Zákaz RDP z veřejného Internetu



Připomenutí zásad bezpečnosti vzdáleného přístupu

- Vzdálený přístup
 - Linux – ssh (secure shell) – typicky TCP/22
 - Windows – rdp (remote desktop protocol) – typicky TCP/3389
- Otevřené do internetu = připojím se odkudkoli
 - Časovaná bomba
 - Zranitelnosti
 - Útok hrubou silou
- Vždy omezit na nezbytné minimum
 - WEBnet – 147.228.0.0/16
 - VPN rozsah – 147.228.232.0/22
 - Vyjmenované adresy – např. veřejná IP doma

Implementace O-metody lovení Phisherů na ZČU

- Vytvoření speciálních identit (tzv. Honeypotích)
- Vyplnění do podvodné phishingové stránky
- On-line hlídání logu přihlášení (webkdc, ...)
- Po použití honeypotí identity notifikace na WIRT
- Hledání dalších přihlášení z této IP adresy – odpovídá kompromitovaným identitám, nebo je Phisher z řad našich uživatelů :-)
- Blokace konta + notifikace uživateli
- Kontakt s uživatelem
 - Doporučeno školení o phishingu
 - Doporučeno přihlášení k dobrovolnému odběru cvičných phishingových zpráv

Phishingator – nástroj k rozesílání cvičných phishingových zpráv



Phishingator

<https://phishingator.zcu.cz>

- Bakalářská práce studenta FAV, nyní člena WIRT
- Dobrovolné zapojení zaměstnanců i studentů
- Tvorba phishingových kampaní – i pro lokální správce
- Poučení
- Vyhodnocování
- Cílené zvaní na školení

Další spolupráce

- Incidenty - pomoc při řešení, řešení na místě
- Hlášení chyb
- Phishingové kampaně
- Info pro uživatele - povolit změnu hesla po telefonu
- Necelých 7% uživatelů (909 uživatelů)



The screenshot shows a web browser window with the URL <https://portal.zcu.cz/portal/ja/orion/souhlas-se-zmenou.html>. The page title is "Portál ZČU". The navigation menu includes "Já", "Infoservis", "Studium", "Výzkum", and "Řízení". Below the navigation, there are links for "Můj portál", "Webmail", "Dokumenty", "Orion konto", "JIS karta", "Ekonomika", and "Další aplikace". The main content area is titled "Nastavení parametrů konta" and contains a section "Souhlas se změnou Orion hesla na dálku". This section includes a checkbox for "Souhlasím s možností změny hesla mého Orion konta na dálku dle pravidel na support.zcu.cz/Orion_heslo" and an "Odeslat" button. A sidebar on the left lists various services: "Změna Orion hesla", "Souhlas se změnou hesla na dálku", "Orion skupiny", "WiFi konto pro hosta", "Hostovská konta", "Diskové projekty", and "Diskový prostor".

Diskuze

Děkuji za pozornost.

ZAJÍMÁ VÁS JEŠTĚ NĚCO?

