ZÁPADOČESKÁ
UNIVERZITA
V PLZNI

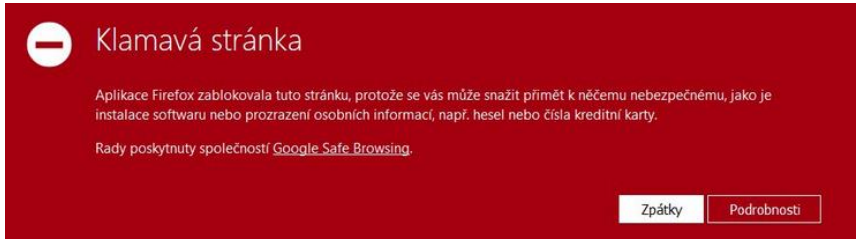
Bezpečnost IT na ZČU

Seminář pro lokální správce

Jiří Čepák, Aleš Padrta / 25. 3. 2019

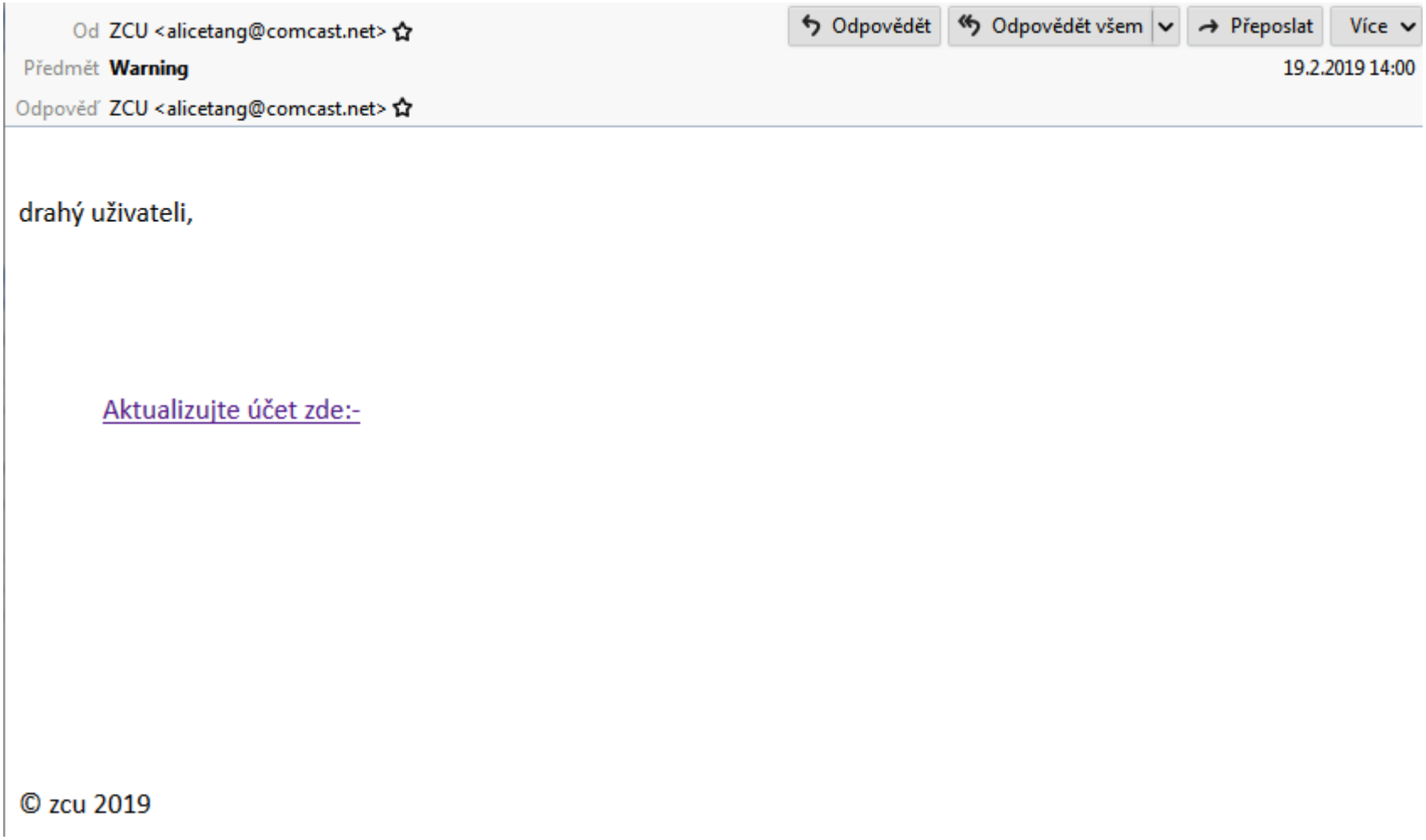
Boj s Phishingem

- Hlašte…(operator@service.zcu.cz)
- Reportování na Phishtank a Google Safe Browsing



- Blokace v McAfee WebControlu
- Upozornění v aktualitách na supportu - https://support.zcu.cz/index.php/Novinky
- Orkáčova metoda
  - Honeypotí identity
    - Vypršelé heslo
    - Možnost změny hesla daleko v budoucnosti
  - Předání identity do falešného přihlašovacího formuláře
  - Hlídání pokusu o přihlášení phishera předanou identitou
  - Hlásil se i jiný náš uživatel ze stejné IP? – kompromitovaná identita

Phishing 2/2019



Od ZCU <alicetang@comcast.net>
Předmět **Warning**
Odpověď ZCU <alicetang@comcast.net>

Odpovědět | Odpovědět všem | Přeposlat | Více

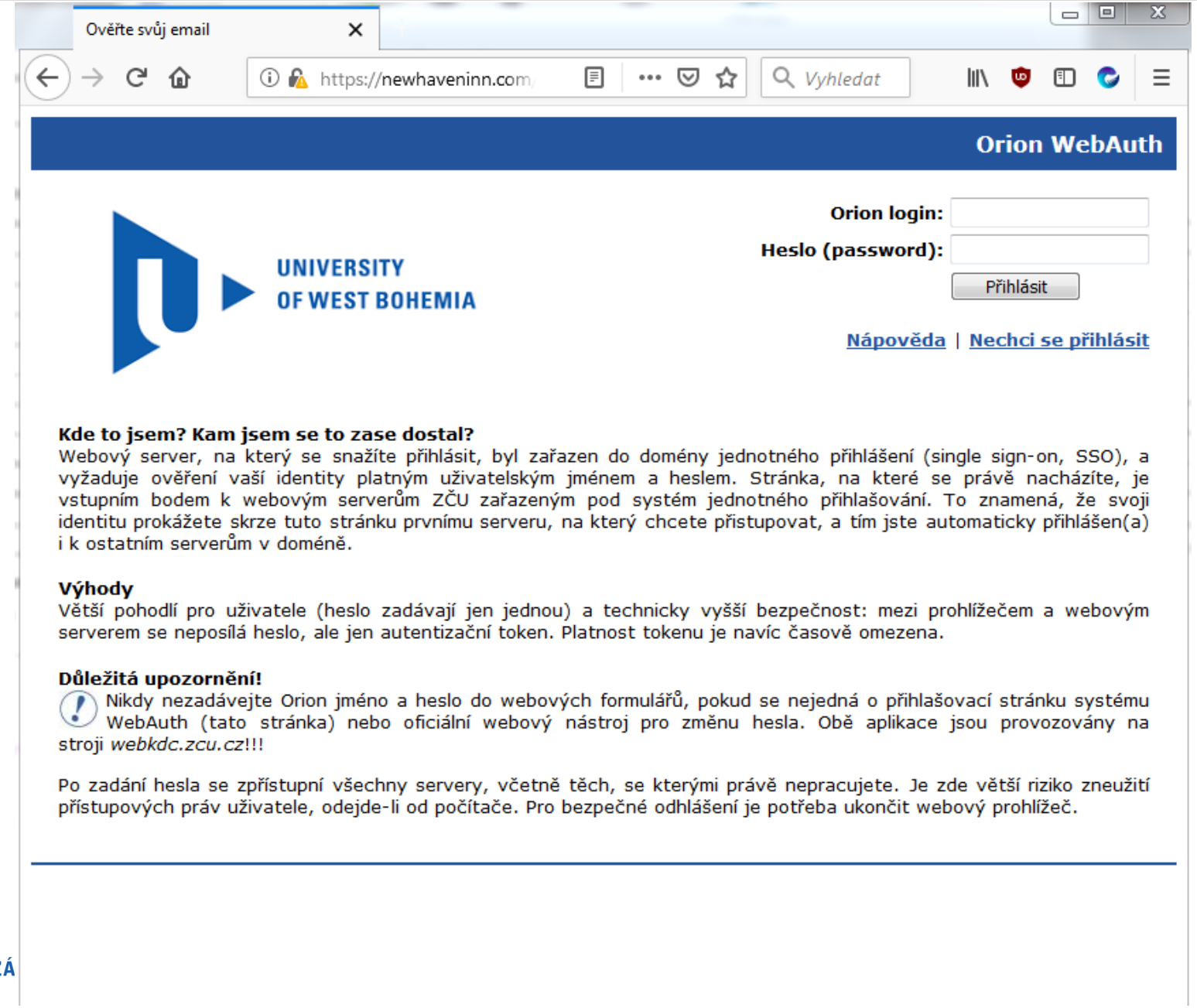
19.2.2019 14:00

drahý uživateli,

Aktualizujte účet zde:-

© zcu 2019

Phishing 2/2019



Phishing 2/2019

- Časová osa:
  - 14:00 – E-maily ve schránkách uživatelů
  - 14:06 – 1. hlášení uživatele na operátory
  - 14:08 – Hlášení od kolegy z CIVu
  - 14:13 – Předání 1. hlášení od operátorů do fronty security
  - 14:30 – Reportování a blokace
  - 14:50 – Počítače s McAfee stránku blokují
  - 16:03 – Stránka hlášena jako klamavá i na ostatních počítačích
- Celkem nahlásilo 20 uživatelů
- Orkáčovou metodou odhaleni 3 uživatelé, kteří podlehli útoku

Phishingátor – cvičení rozpoznávání phishingu

- Bakalářská práce studenta FAV
- Dobrovolné zapojení zaměstnanců i studentů
- Tvorba phishingových kampaní
- Poučení
- Vyhodnocování
- Cílené zvaní na školení
- Více informací již brzy na nějakém dalším semináři

Připomenutí služeb

- McAfee EPO – centrální správa zabezpečení koncových zařízení
- Katedrální FW
  - Zatím jen na Borech, plánované rozšíření do celého WEBnetu
  - Úroveň zabezpečení – Přístupný / Přístupný z daného pracoviště / Přístupný z jiné části WEBnetu / Nepřístupný
  - FW je nastaven vždy na souvislý blok 8 IP adres
  - Zařízení v tomto bloku by měly mít u registrace v kolonce „Info:“ text „Sec:“
- Sauron
  - Správa registrací počítačů

Další spolupráce

- Incidenty – pomoc při řešení, řešení na místě
- Hlášení chyb – např. web ZČU poskytuje interní dokumenty
- Info pro uživatele – povolit změnu hesla po telefonu

Diskuze

Děkuji za pozornost.