

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 <alictang@comcast.net> ☆

Předmět **Warning**

Odpověď ZCU <alictang@comcast.net> ☆

Odpověď Odpověď všem Přeposlat Více

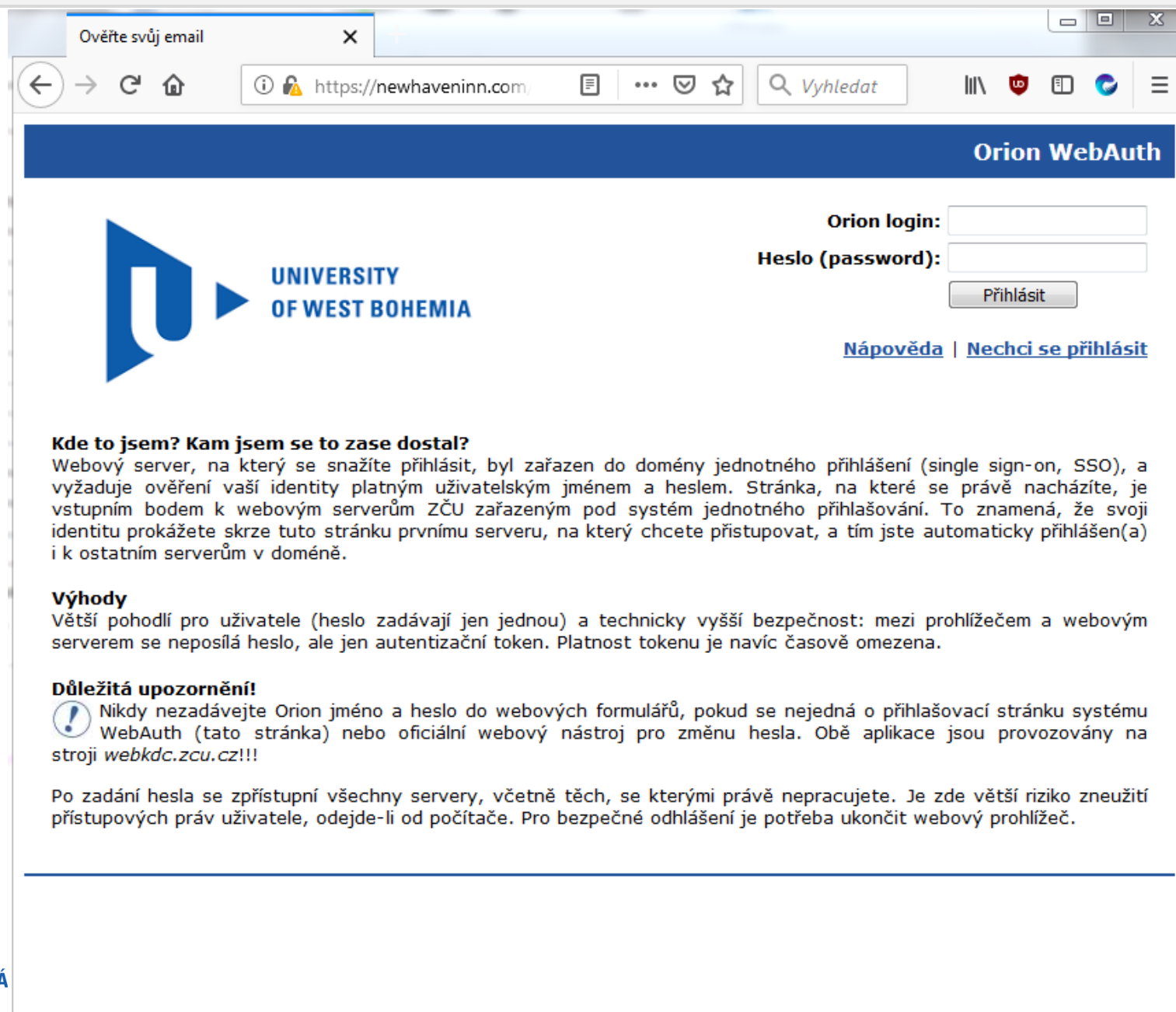
19.2.2019 14:00

drahý uživateli,

[Aktualizujte účet zde:-](#)


© zcu 2019

Phishing 2/2019



The screenshot shows a web browser window with the address bar displaying `https://newhaveninn.com`. The page title is "Ověřte svůj email". The main content area features the Orion WebAuth logo and the University of West Bohemia logo. There is a login form with fields for "Orion login:" and "Heslo (password):", and a "Přihlásit" button. Below the form are links for "Nápověda" and "Nechci se přihlásit".

Orion WebAuth

 **UNIVERSITY OF WEST BOHEMIA**

Orion login:

Heslo (password):

[Nápověda](#) | [Nechci se přihlásit](#)


Kde to jsem? Kam jsem se to zase dostal?

Webový server, na který se snažíte přihlásit, byl zařazen do domény jednotného přihlášení (single sign-on, SSO), a vyžaduje ověření vaší identity platným uživatelským jménem a heslem. Stránka, na které se právě nacházíte, je vstupním bodem k webovým serverům ZČU zařazeným pod systém jednotného přihlašování. To znamená, že svoji identitu prokážete skrze tuto stránku prvnímu serveru, na který chcete přistupovat, a tím jste automaticky přihlášen(a) i k ostatním serverům v doméně.

Výhody

Větší pohodlí pro uživatele (heslo zadávají jen jednou) a technicky vyšší bezpečnost: mezi prohlížečem a webovým serverem se neposílá heslo, ale jen autentizační token. Platnost tokenu je navíc časově omezena.

Důležitá upozornění!

 Nikdy nezadávejte Orion jméno a heslo do webových formulářů, pokud se nejedná o přihlašovací stránku systému WebAuth (tato stránka) nebo oficiální webový nástroj pro změnu hesla. Obě aplikace jsou provozovány na stroji `webkdc.zcu.cz!!!`

Po zadání hesla se zpřístupní všechny servery, včetně těch, se kterými právě nepracujete. Je zde větší riziko zneužití přístupových práv uživatele, odejde-li od počítače. Pro bezpečné odhlášení je potřeba ukončit webový prohlížeč.

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



The screenshot shows a web browser window with the address bar displaying "Západočeská univerzita v Plzni (CZ) | https://portal.zcu.cz/portal/ja/orion/souhlas-se-zmenou.html". The page header includes the ZČU logo and the text "Portál ZČU". A navigation menu contains links for "Já", "Infoservis", "Studium", "Výzkum", and "Řízení". Below this, 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 features a section "Souhlas se změnou Orion hesla na dálku". This section contains a checkbox labeled "Souhlasím s možností změny hesla mého Orion konta na dálku dle pravidel na support.zcu.cz/Orion_heslo" and an "Odeslat" button. A left sidebar menu 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".

Děkuji za pozornost.

TO BYLO KRÁTKÉ, NAPADÁ
VÁS NĚJAKÝ DOTAZ?

