



Bezpečné chování v síti WEBnet

Ing. Aleš Padrta Ph.D.

Obsah

- ▶ Motivace
- ▶ Základy bezpečnosti
- ▶ Doporučení
 - ▶ Technické prostředky
 - ▶ Bezpečné chování
 - ▶ Zobecněné rady
- ▶ Bezpečnostní incidenty
- ▶ Shrnutí

▶ <http://support.zcu.cz>

▶ Bezpečnost

▶ V okolním světě

- ▶ Běžná (zamykání bytu, auta, ...)
- ▶ Výuka od dětství

▶ V prostředí výpočetní techniky

- ▶ Ne zcela zřejmá
- ▶ Nenápadné pronikání (www → bankovníctví)
- ▶ Syndrom technické magie
- ▶ Výuka od .. mateřské školy? .. střední školy? .. teď?

▶ Podvodníci jsou všude

- ▶ Také v IT → nutné se bránit

▶ <http://support.zcu.cz>

Motivace

- ▶ Proč to dělají
 - ▶ Nejčastěji peníze
- ▶ Cíle útoků
 - ▶ Kontrola nad PC
 - ▶ Výpočetní výkon
 - ▶ Datové úložiště
 - ▶ Nástroj pro další útoky
 - ▶ Zajímavé údaje
 - ▶ Vědeckotechnická špionáž
 - ▶ Osobní informace
 - ▶ Licenční čísla
 - ▶ Krádež elektronické identity
 - ▶ Přesunutí odpovědnosti za své činy

▶ <http://support.zcu.cz>

Základy bezpečnosti

▶ Dosažení cíle

- ▶ Více způsobů → proti **všem** je nutné se bránit
- ▶ Problém nejslabšího článku
 - ▶ Technické prostředky
 - ▶ Chování uživatele

▶ Vícestupňová obrana

- ▶ Několik postupných překážek
- ▶ Chování uživatele
 - ▶ Někdy jediná překážka
 - ▶ Zásadně ovlivňuje bezpečnost

▶ <http://support.zcu.cz>

Doporučené technické prostředky

▶ Aktualizace systému

- ▶ Chyby v programech jsou a budou
- ▶ Naprosto nezbytná
- ▶ Standardní cestou

▶ Antivirový program

- ▶ Blokování známých (!) virů
- ▶ Heuristika (sofistikovaný odhad), ne vždy funguje
- ▶ Univerzitní licence

▶ Firewall

- ▶ Snížení (!) počtu možných útočníků
- ▶ Není zárukou 100% ochrany

▶ <http://support.zcu.cz>

Doporučené technické prostředky

▶ Uživatelské účty

- ▶ Menší práva než administrátor = menší škody

▶ Bezpečná komunikace

- ▶ Citlivé údaje vždy přenášet šifrovaně

- ▶ SSH, HTTPS, IMAP-SSL, POP-SSL

- ▶ Ověření komunikujícího protějšku

- ▶ Komu jsou data zasílána?

- ▶ Certifikáty

- ▶ ZCU ROOT CA, <http://crl.zcu.cz>

▶ <http://support.zcu.cz>

Bezpečné chování – Instalace SW, Hesla

- ▶ Instalace programů
 - ▶ Nejlépe neinstalovat ☺
 - ▶ Pouze oficiální verze
 - ▶ Žádné neověřené patche, cracky apod.
- ▶ Zacházení s heslem
 - ▶ Zvolit vhodné heslo
 - ▶ Dostatečně složitě
 - ▶ Zapamatovatelné
 - ▶ Pečlivě uschovat, nejlépe zapamatovat
 - ▶ Heslo zná pouze uživatel
 - ▶ Nikdo jiný nemá nárok
 - ▶ Opravdu nikdo jiný

▶ <http://support.zcu.cz>

Bezpečné chování – Zacházení s e-mailem

▶ Odesílatel

- ▶ Podvržení identity → Digitální podpis
- ▶ Sociální inženýrství

▶ Časté problémy

- ▶ Nebezpečné přílohy (viry a jiný malware)
- ▶ Odkazy na podvržené stránky (phishing)
- ▶ Šíření poplašných zpráv (Hoax)

▶ Univerzitní e-mail

- ▶ Antispamový filtr (98% je spam)
- ▶ Likvidace zavirovaných příloh
- ▶ Přes 300 tisíc e-mailů denně
 - ▶ Od srpna 2007 nová posila - Fred

▶ <http://support.zcu.cz>

Bezpečnostní hování – Zacházení s e-mailem

- ▶ Odesílání e-mailů → Digitální podpis
- ▶ Ověřování adresy → Certifikát

- ▶ Nebezpečné přílohy (virusy a jiný malware)
- ▶ Ověřování podezřelých stránek (phishing)
- ▶ Sdílení falešných zpráv (Hoax)

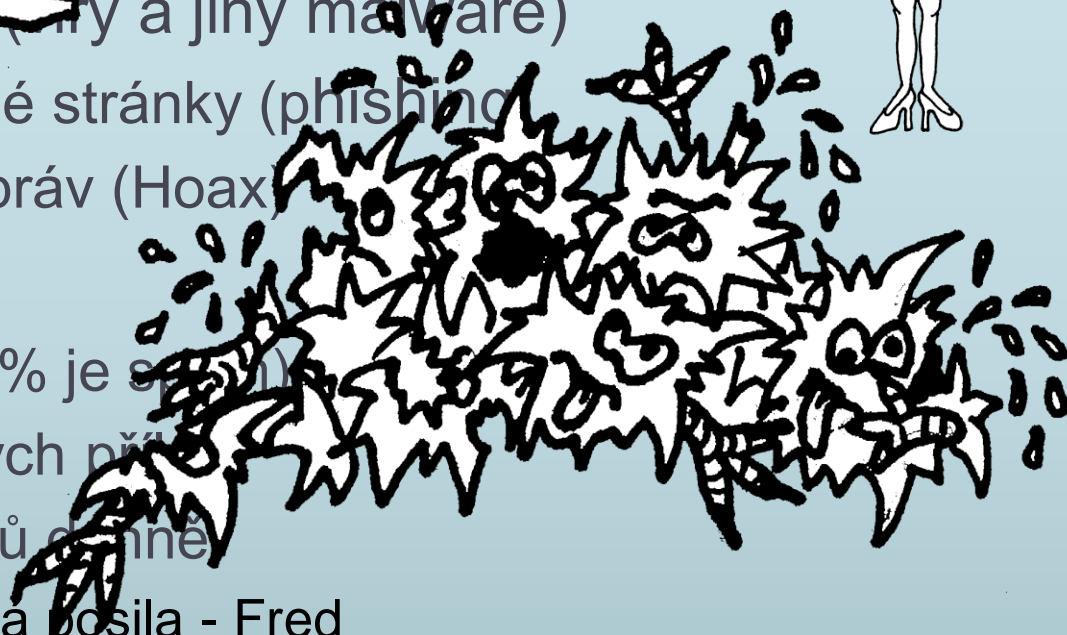
- ▶ Univerzální e-mail

- ▶ Antivirový filtr (98% je efektivní)

- ▶ Lidé často klikají na virovaných přílohách

- ▶ Přibližně 100% z e-mailů obsahuje

srpna 2007 nová posila - Fred



<http://support.zcu.cz>

Zobecněné rady

- ▶ **Bud'te podezřívaví - nejlépe paranoidní 😊**
 - ▶ Divný požadavek?
 - ▶ Jiný postup než obvykle?
 - ▶ Nečekaná odezva?
- ▶ **Ověřujte důležité údaje**
 - ▶ Jiným způsobem (osobně, telefonicky)
- ▶ **Bud'te informovaní**
 - ▶ Více informací = vyšší bezpečnost
 - ▶ Rizika se časem mění
 - ▶ Vhodný kompromis
 - ▶ Aktuality na <http://support.zcu.cz> (novinky)

▶ <http://support.zcu.cz>

Řešení bezpečnostních incidentů

- ▶ Porušení pravidel = bezpečnostní incident
 - ▶ Pravidla používání sítě WEBnet
 - ▶ Zákony ČR (autorský, trestní, ...)
- ▶ Časté problémy
 - ▶ Zneužití počítače (viry, spamy, ...)
 - ▶ Porušování autorského zákona (P2P sítě)
- ▶ Řešení
 - ▶ Odpojení problematického počítače
 - ▶ Technická náprava
 - ▶ Poučení uživatele
 - ▶ Připojení počítače k síti WEBnet

▶ <http://support.zcu.cz>

Shrnutí

- ▶ Výpočetní technika
 - ▶ Zajímavý cíl pro kriminální živly
 - ▶ Potřeba zabezpečení
- ▶ Bezpečnost
 - ▶ Problém nejslabšího článku
 - ▶ Závisí na znalostech
- ▶ Zajištění bezpečnosti
 - ▶ Technické prostředky
 - ▶ Vhodné chování uživatelů (!!)

▶ <http://support.zcu.cz>