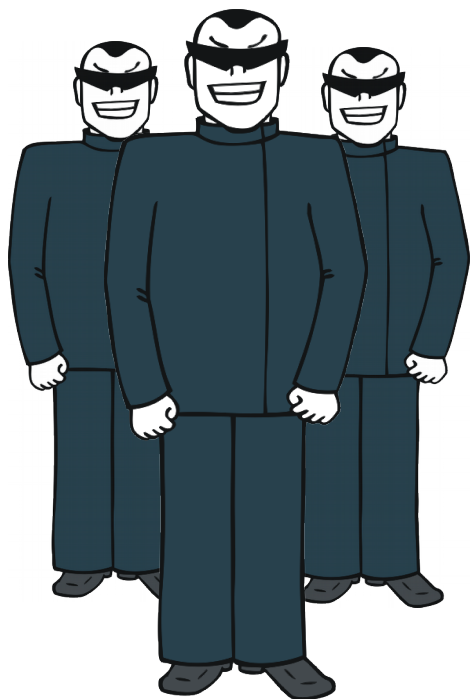


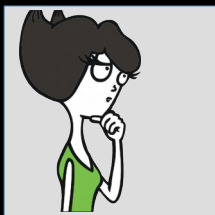
# #SECFEST2018



## Bezpečnost IT na ZČU

Aleš Padrta

[apadrta@civ.zcu.cz](mailto:apadrta@civ.zcu.cz)

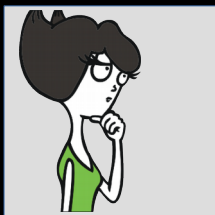


# IT na ZČU

- Sít' (WEBnet)
  - IPv4 147.228.0.0/16
  - IPv6 rozsah 2001:718:1801::/48
- Připojená zařízení
  - Počítače, laptopy
  - Chytré telefony
  - Hloupá zařízení
- Připojení uživatelé
  - Používání Internetu
  - Používání univerzitních služeb

IOT MÁM RÁD. TOLIK  
NEZABEZPEČENÝCH  
ZAŘÍZENÍ SI DÁM LÍBIT.



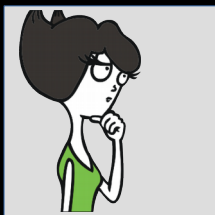


# Co hrozí při výpadku?

- Přístup k Internetu
  - Omezen nebo není
- Používání služeb
  - Dnes je všechno závislé na IT
  - Jídlo – Menza
  - Studium – Portál, Courseware
  - Pohyb po areálu – JIS (dveře, závory)
  - Další agendy – ekonomická, administrativa

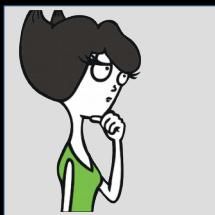
VÝPADKY TAKY  
NEMÁME RÁDI!





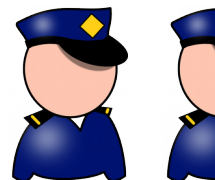
# Život IT systémů

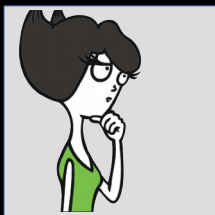
- Návrh ⇒ Vytvoření ⇒ Provoz
- Někdo se je **snaží rozbít**
  - Dostupnost (DDoS, ransomware, ...)
  - Integrita (malware, změna dat, ...)
  - Důvěrnost (neoprávněný přístup)
- Někdo se **snaží bránit rozbíjení**
  - Správci IT systémů
  - Bezpečnostní tým



# Bezpečnostní tým ZČU

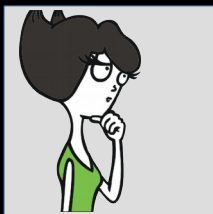
- Typu CERT/CSIRT
- WEBnet Incident Response Team (WIRT)
- Jeden a půl bezpečáka
  - Aleš Padrta, Jiří Čepák
- Kontakt
  - Klasicky přes HelpDesk
- Činnost
  - Reakce na problémy (bezpečnostní incidenty)
  - Prevence výskytu BI





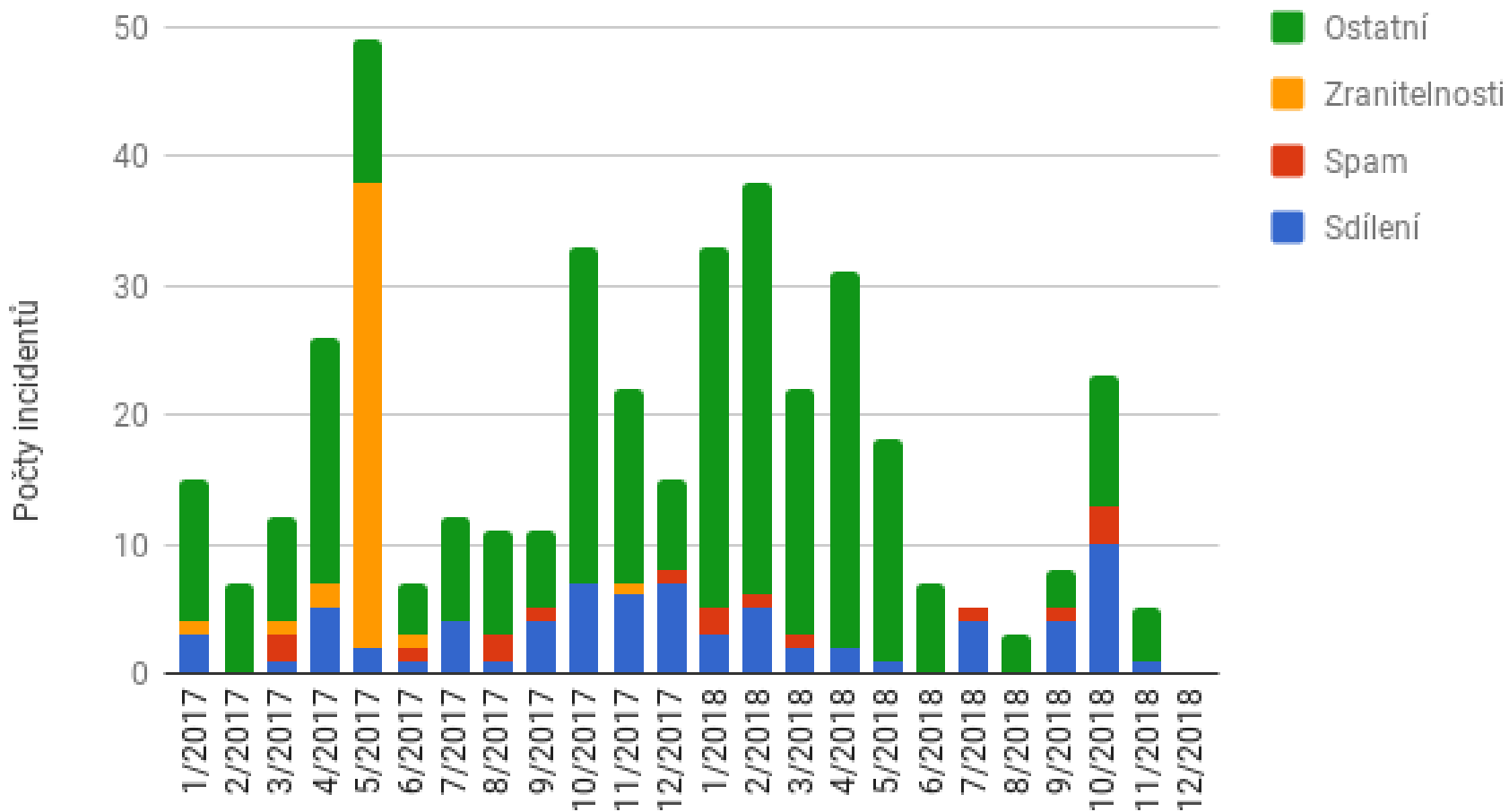
# Bezpečnostní Incident

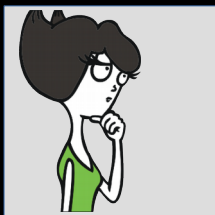
- Oběť nebo viník?
- Zařízení
  - Zavirováno (způsobí další škody)
  - Nepoužitelné (zašifrováno ransomwarem)
  - Licenční potíže
- Uživatel
  - Nelegální činnost (zákony ČR)
  - Zakázaná činnost (vnitřní pravidla ZČU)
  - Krádež konta (využití jeho přístupů někým jiným)



# Trocha statistiky

## Statistika bezpečnostních incidentů





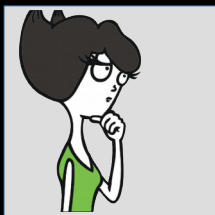
# Postup řešení incidentu

- Zjistit existenci
- Ověřit
- Minimalizovat dopady
  - Zablokovat konto
  - Odpojit zařízení
- Vyřešit technicky
- Vyřešit administrativně
- Návrat k běžnému stavu



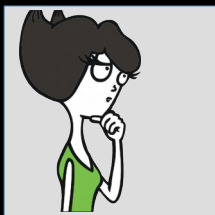
STANDARDNÍ POSTUPY  
JSOU APLIKOVÁNY BEZ  
VÝJIMEK. NA VŠECHNY!





# Proč a jak vznikají?

- Technická zařízení
  - Vytvářena lidmi
  - Nejsou dokonalá (vznik chyby)
  - Zneužití chyb
- Uživatelé
  - Neznalost
  - Nedbalost
  - Úmysl
- Za vším hledej člověka

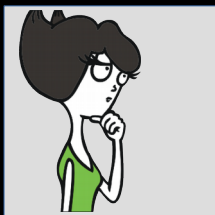


# Prevence – vzdělávání

- Školení o phishingu
  - Zatím jen pro zaměstnance
- Odborné semináře
  - Různá témata
- Secfest
  - Prevence
- FR CESNET
  - Příprava vzdělávacích materiálů

PRO MNE TO BYLO UŽITEČNÉ.  
PHISHING TEĎ POZNÁM I PŘED  
RANNÍ KÁVOU!

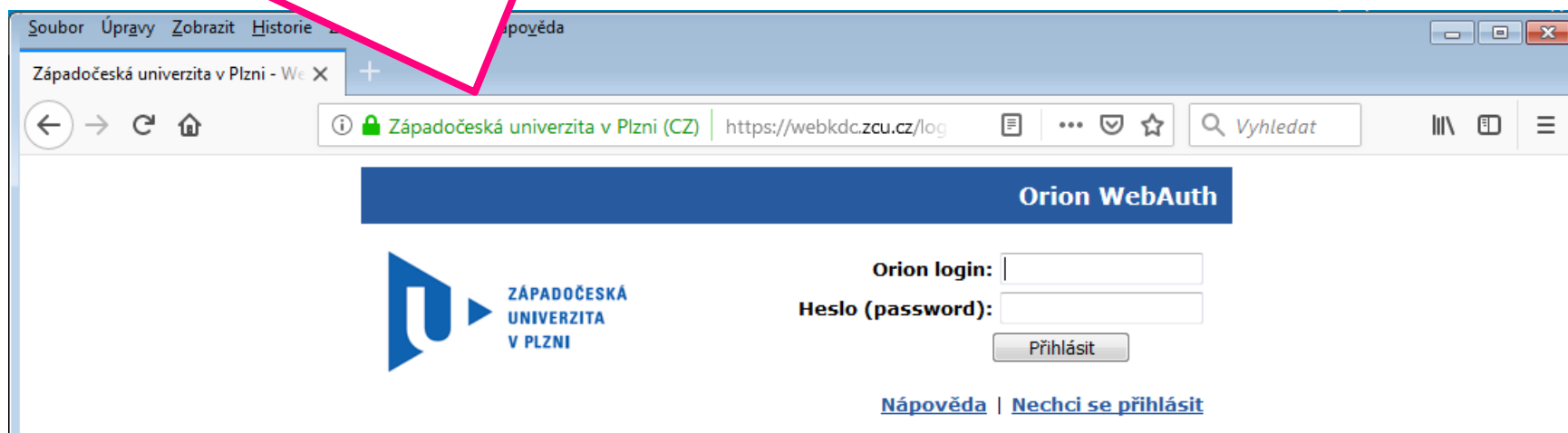


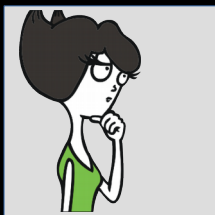


# Prevence – usnadnění

- Přihlašovací stránka – EV certifikát
  - Pomoc při poznávání podvodných webů

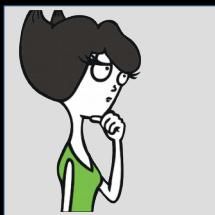
  Západočeská univerzita v Plzni (CZ)





# Největší potíže ZČU

- Správné zacházení s hesly
  - Více informací ⇒ Ondra Caletka
- Rozpoznávání podvodů a fake news
  - Více informací ⇒ Jiří Čepák
- Chápáním svých povinností (a trochu i práv)
  - Více informací ⇒ Jan Kolouch
- Chápání technických principů
  - Neumí odhadnout důsledky
  - Snaha používat vše (s minimem znalostí)



# Dotazy



V PŘÍPADĚ PROBLÉMŮ  
PŘIJĎTE NA HELPDESK.  
PORADÍME VÁM RÁDI A  
S ÚSMĚVEM.

