Cíl zaměřen:
uživatel

Mgr. Miroslava Jarošová,
Filozofická fakulta Univerzity Karlovy

Bc. Karel Nykles
Západočeská univerzita v Plzni

Obsah

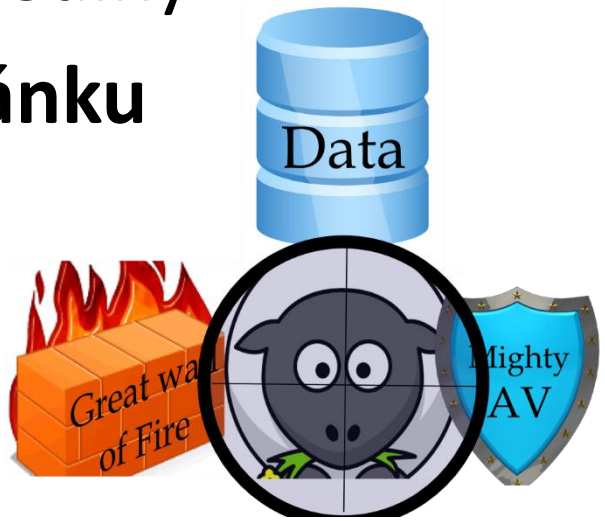
- Kybernetická obrana dneška
- Pohled kompromitovaných uživatelů
- Psychologické vysvětlení
- Jak získané poznatky využít

I. Kybernetická obrana dneška

- Ochrana perimetru
- Analýza provozu sítě
- Analýza provozních logů
- Větší, dražší, rychlejší HW, SW

Asymetrická hrozba

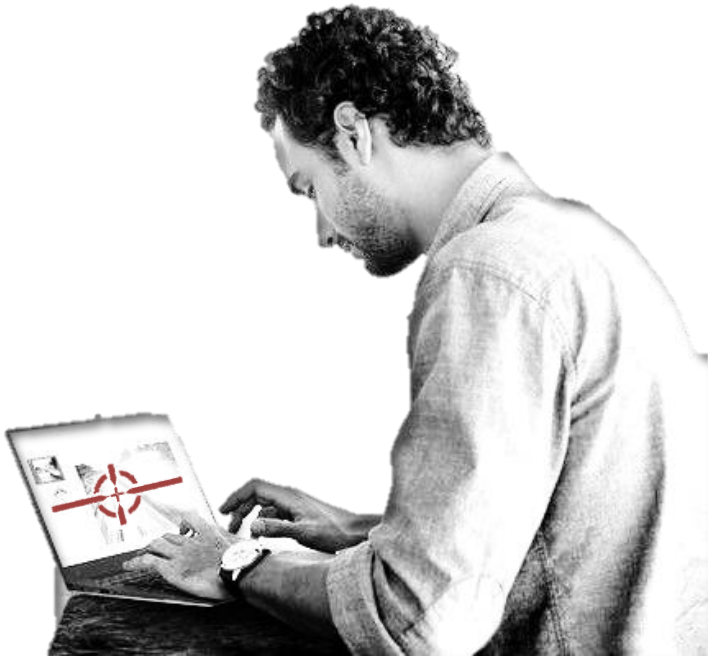
- Obránce musí pokrýt veškeré myslitelné útočné vektory
- Útočníkovi postačí zneužít jediný
- **Identifikace nejslabšího článku**
  - Plán propouštění 2015



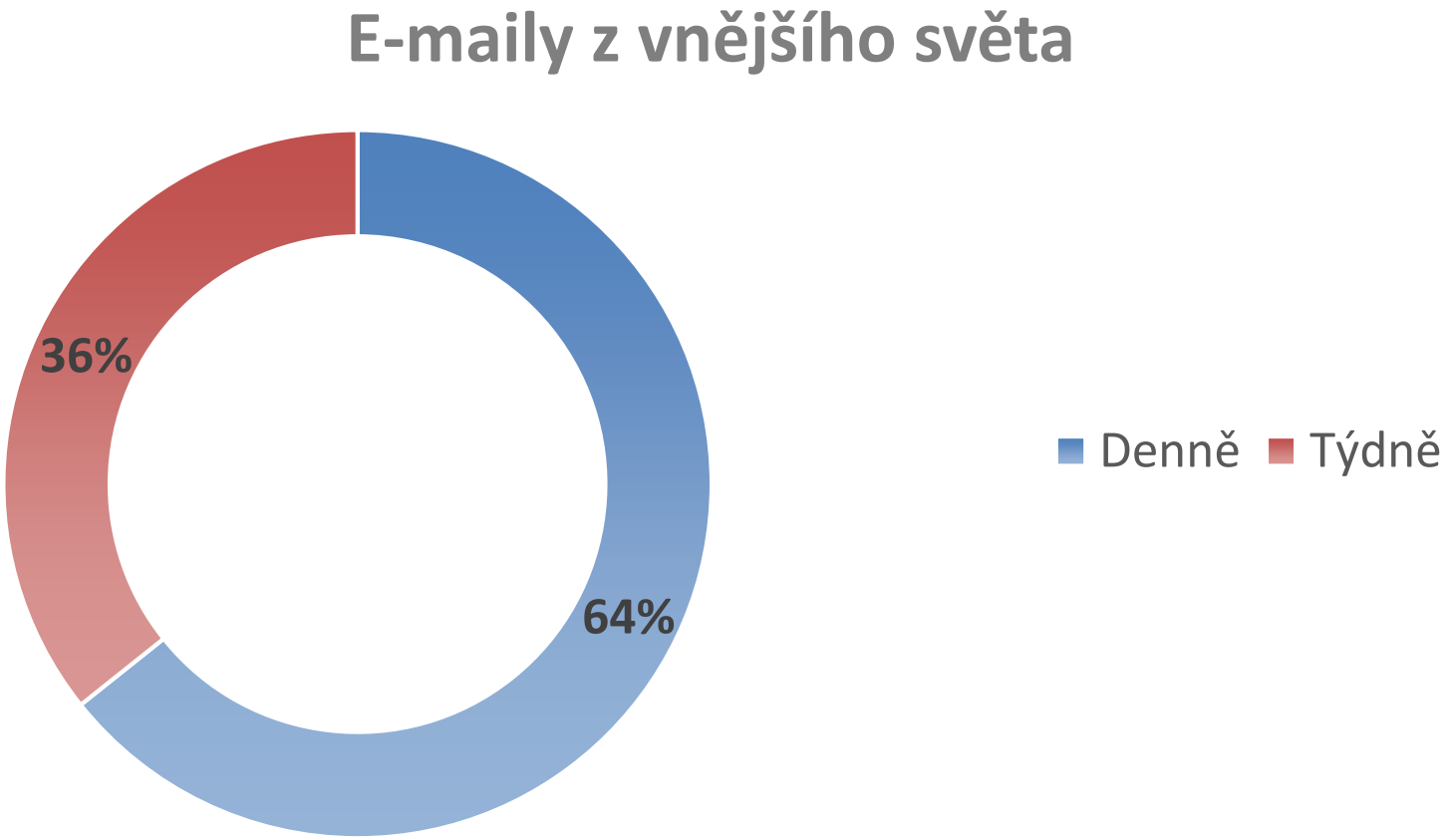
Data z loňského roku

- 112 PC k reinstalaci
- 4 PC a jeden server „Kryptolocknutý“
- Osobně jsem navštívil vyřazený hotel
  - Kryptoloknutá PC, servery, zálohy
- Průnik přes neosobní, převážně strojově přeložený phishing

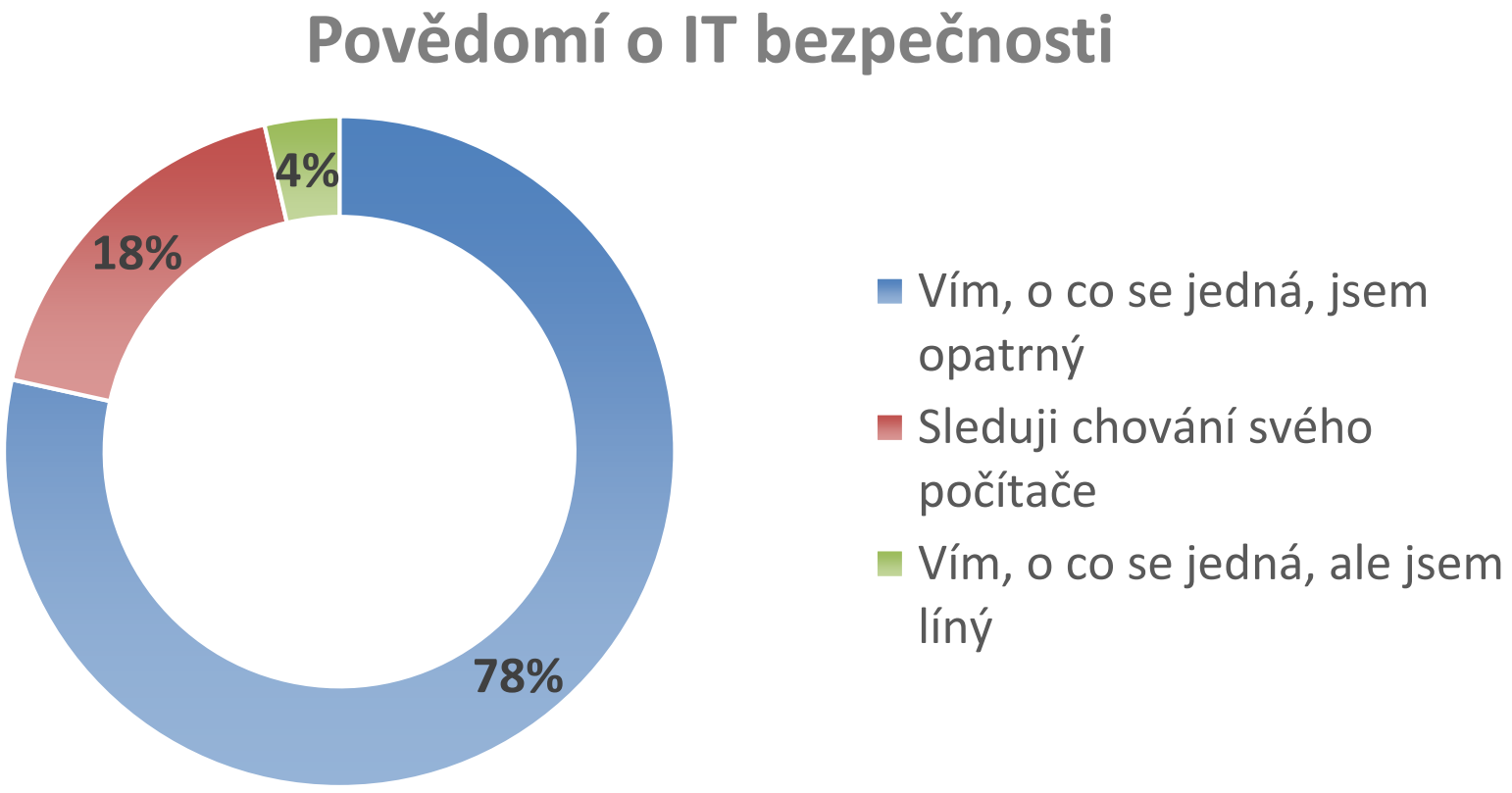
II. Zeptali jsme se kompromitovaných uživatelů



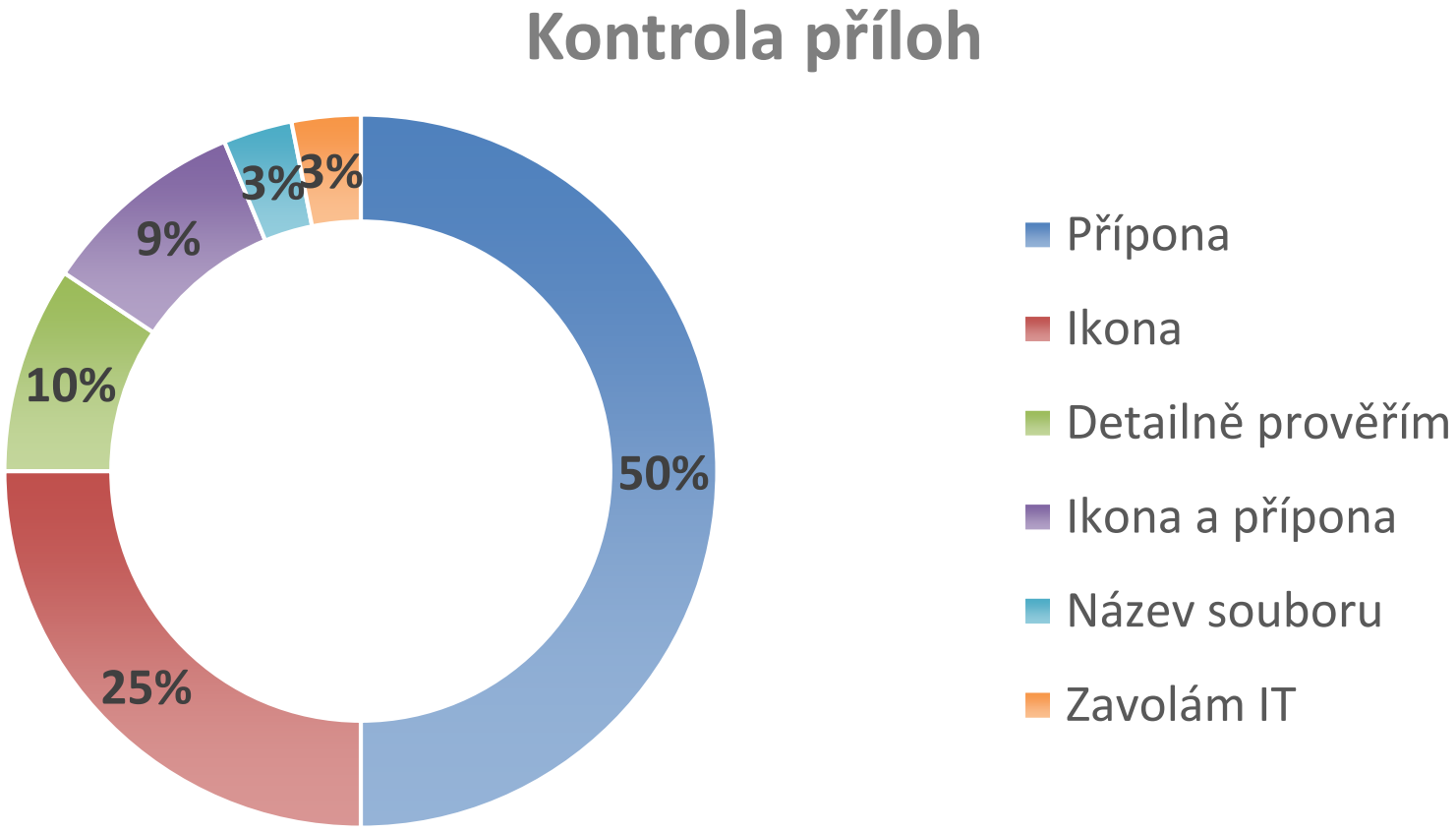
Pohled kompromitovaných uživatelů



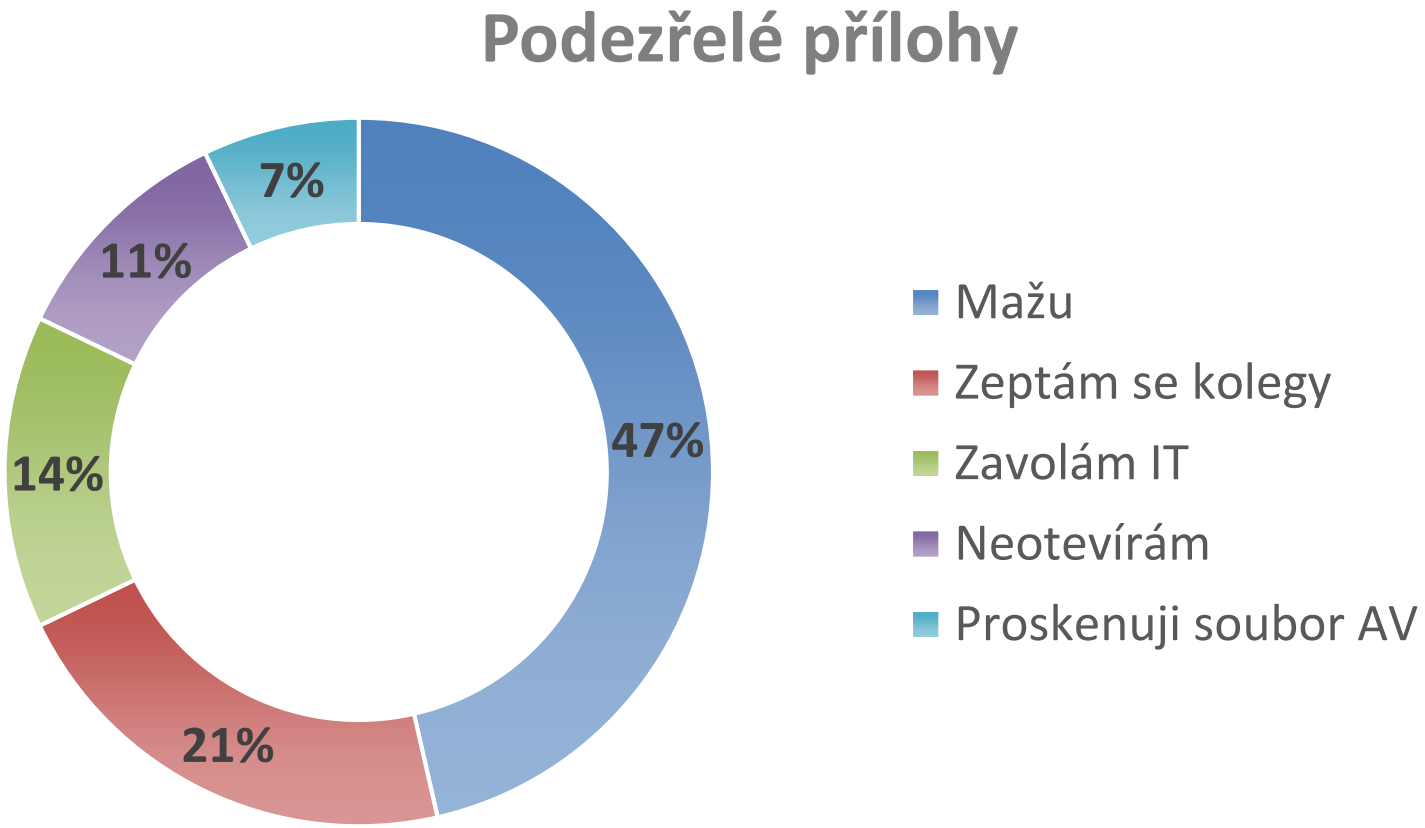
Pohled kompromitovaných uživatelů



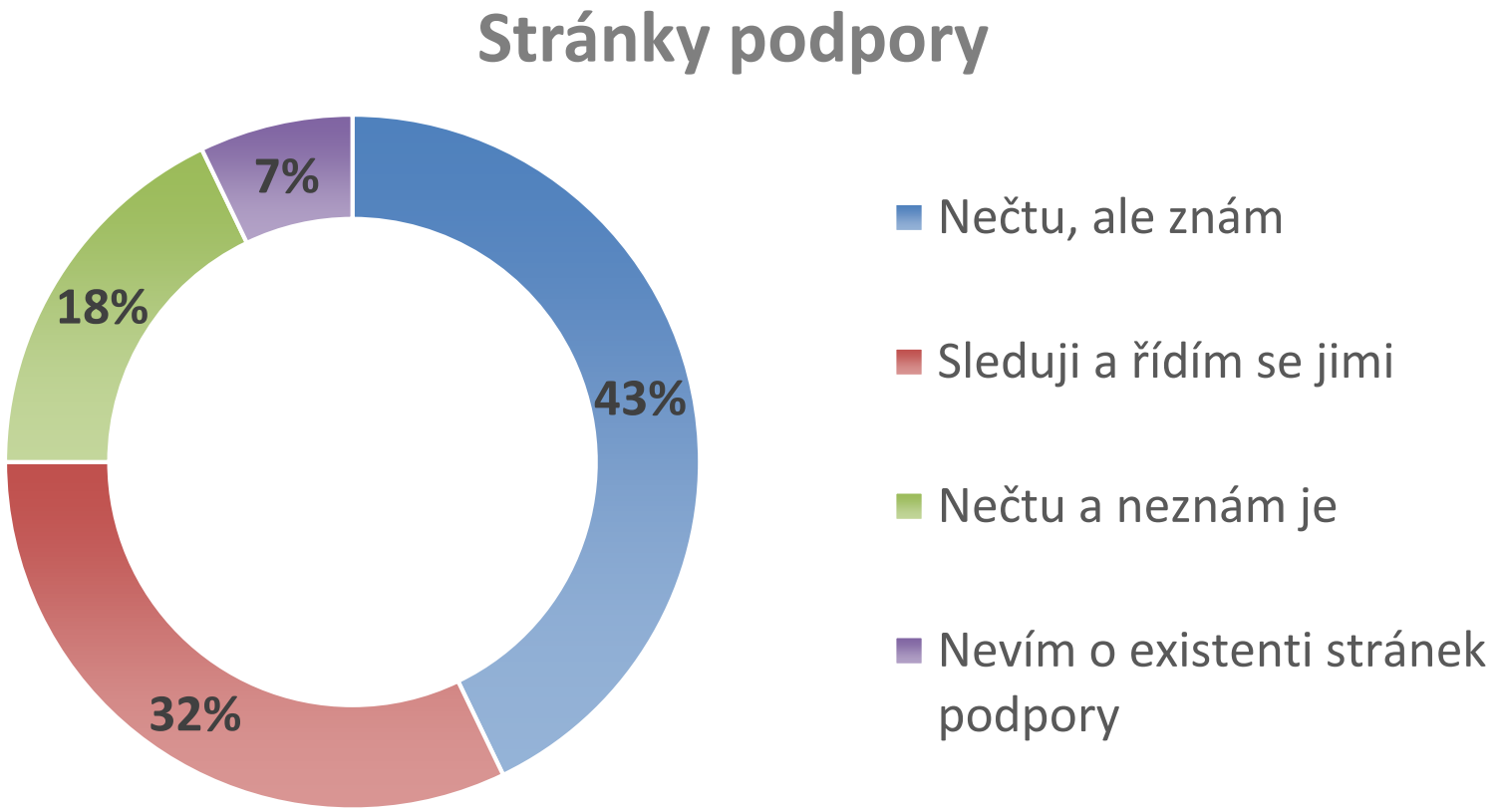
Pohled kompromitovaných uživatelů



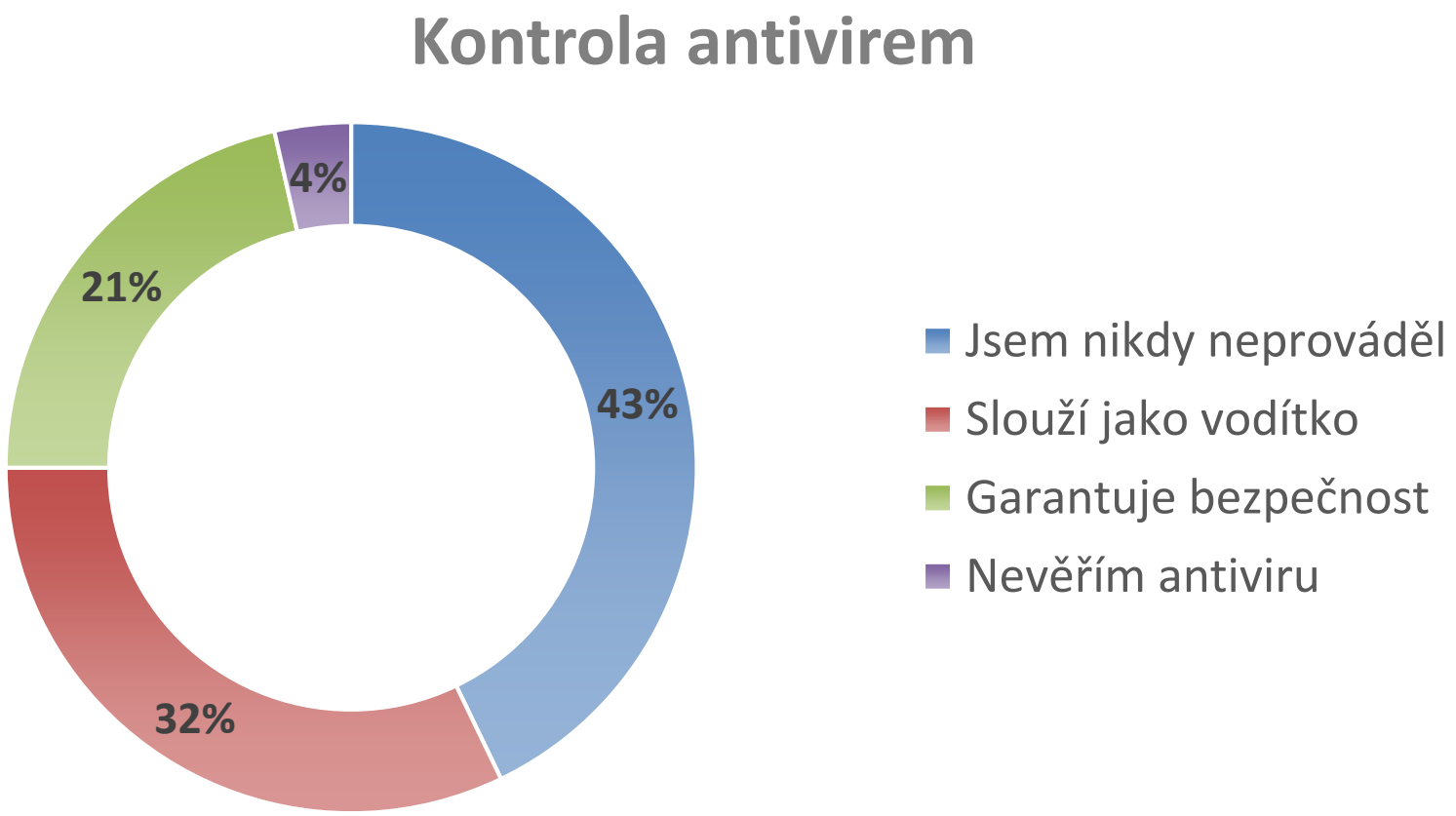
Pohled kompromitovaných uživatelů



Pohled kompromitovaných uživatelů

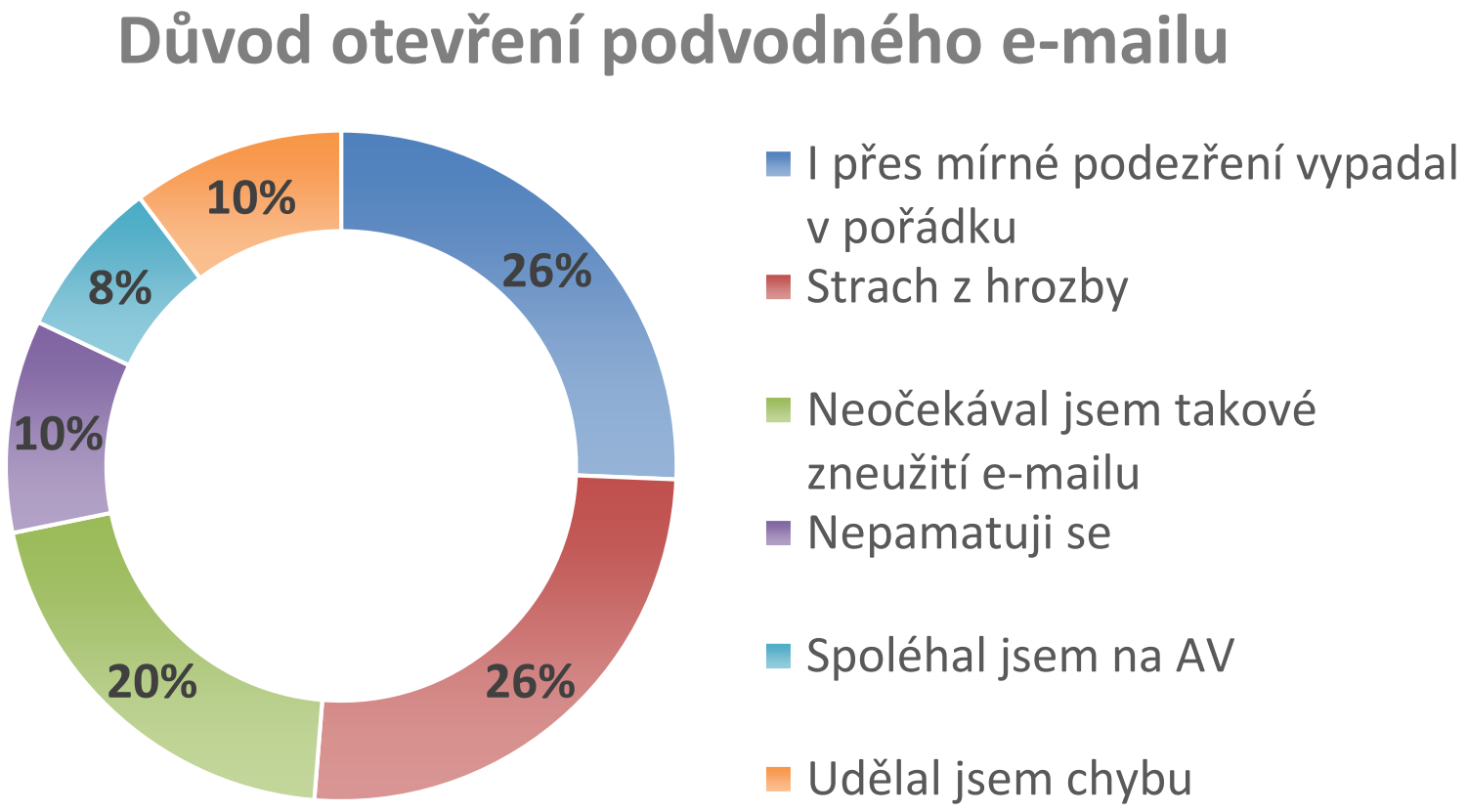


Pohled kompromitovaných uživatelů

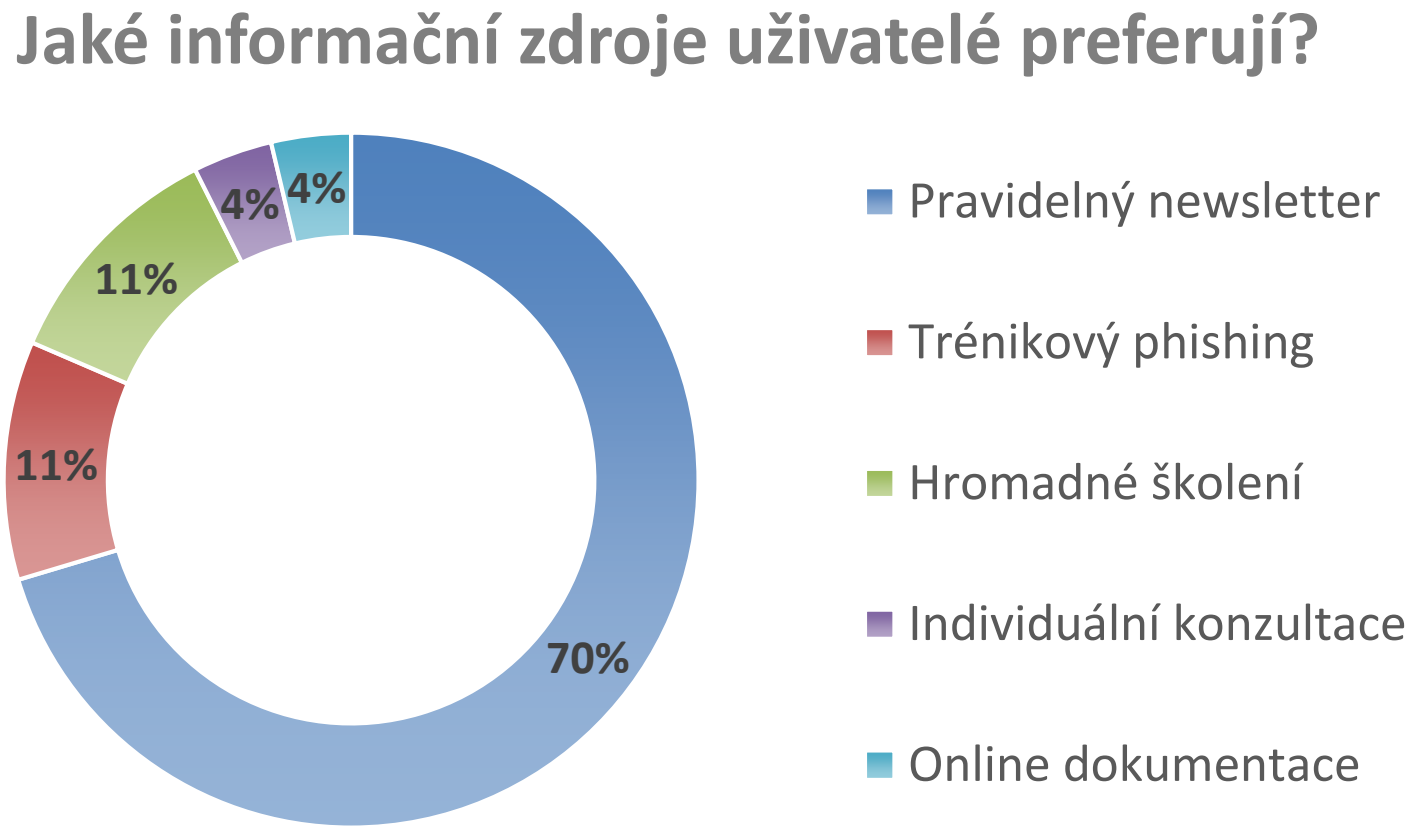


Proč tedy uživatelé podlehnou?

Pohled kompromitovaných uživatelů

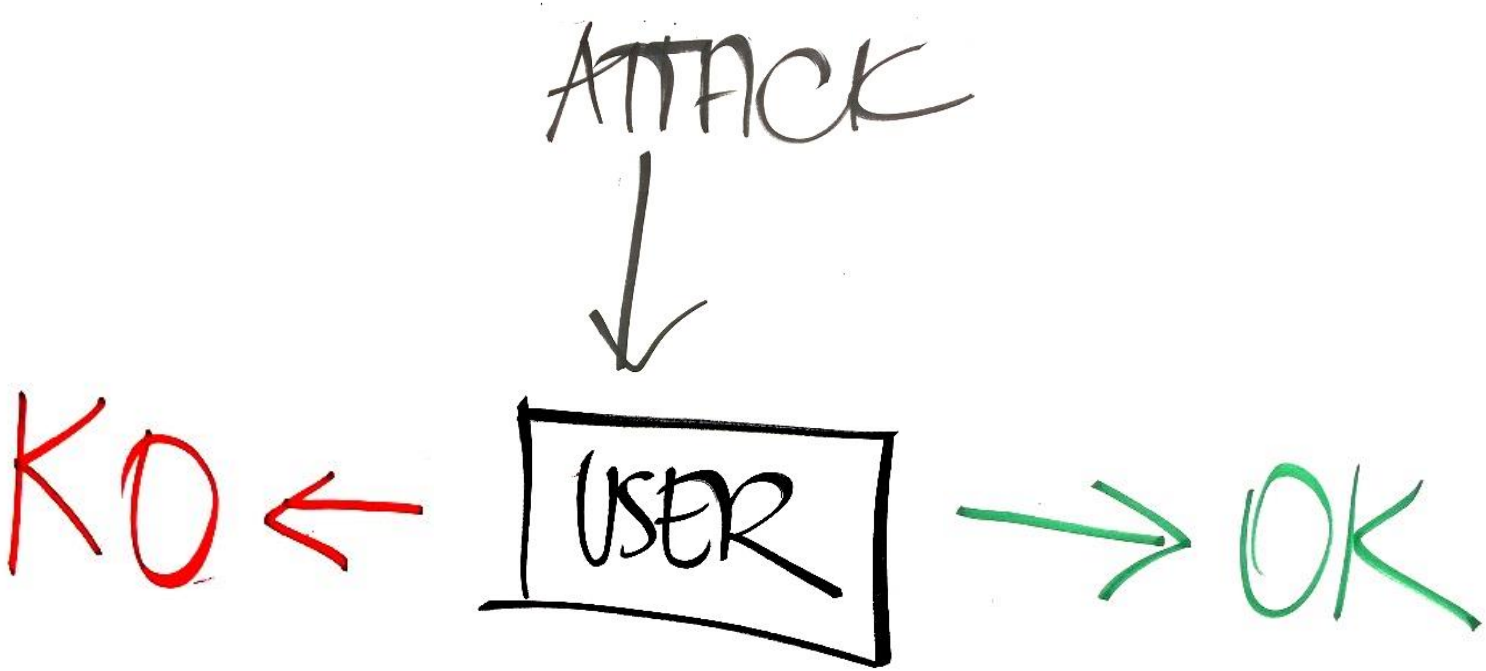


Pohled kompromitovaných uživatelů



Pohled správců IT

III. Psychologické vysvětlení



Jak se uživatelé rozhodují?

Uživatel jako naivní vědec

Rozhodování o pravosti aneb intuitivní analýza variance

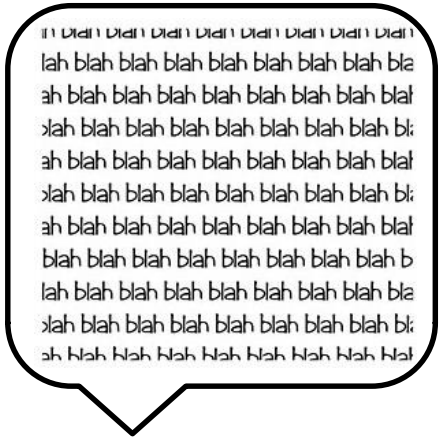
Konzistence ✓ Vypadá to jako ostatní maily od odesílatele?

Konsenzus ✓ Reaguje odesílatel v dané situaci vždy takto?

Typičnost ✓ Postupují v dané situaci podobně i ostatní odesílatelé?

Jenže…

VERSUS



Dvojí mysl

Vědomá	**Nevědomá**
Pomalá	Rychlá (milisekundy)
Záměrná	Automatická
Precizní (výpočty)	Přibližná (heuristiky)
Složité myšlenkové operace	Jednoduché myšlenkové operace
Sekvenční	Paralelní
Vyžaduje úsilí	Zadarmo
Racionální	Intuitivní
PŘESNÁ ROZHODNUTÍ	**RYCHLÉ ODHADY**

Uživatel jako kognitivní lakomec

Rozhodování o pravosti aneb odhady a heuristisky

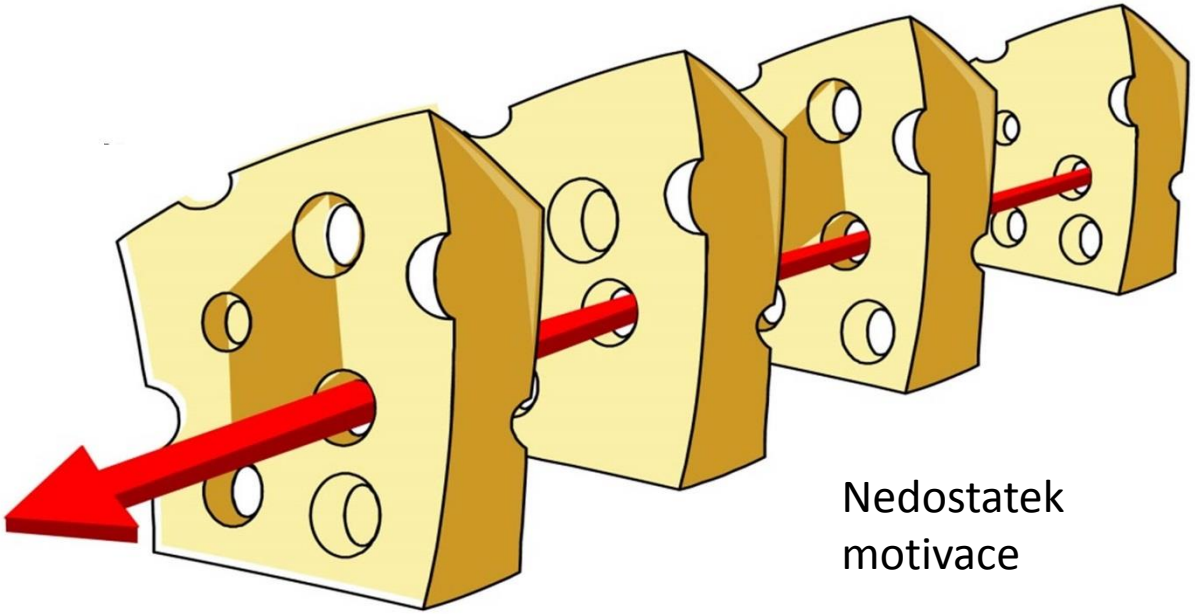
Reprezentativnost	Dostatečná shoda?
Dostupnost	Vybavím si podobné?
Představitelnost	Může to tak probíhat?
Prvotní instinkt	Co na to intuice?
Efekt falešné shody	Chovají se tak i ostatní?

Jak je přimět jednat bez rozmyslu

Vědomé Automatické

- Informační přetížení
- Časový tlak
- Hrozba
- Anonymita (nedostatek odpovědnosti)
- Nedostatečná motivace

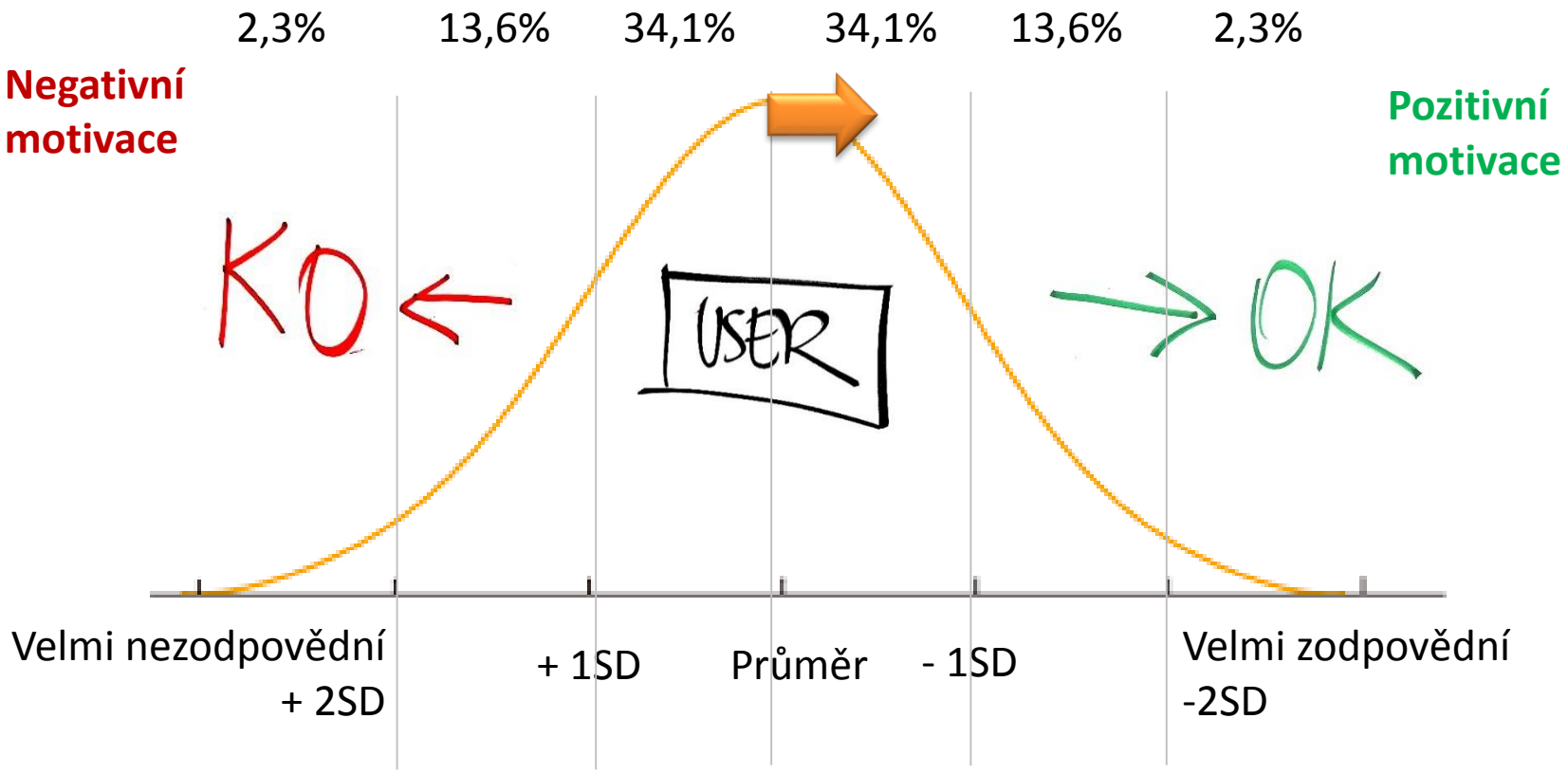
Řekněte sýr


Informační
přetížení
Anonymita
Nedostatek
motivace
Hrozba

Jak je přimět jednat s rozmyslem

Vědomé Automatické

- Snadná porozumitelnost
- Příběhy
- Jasná rozhodovací pravidla
- Odpovědnost
- Principy gamifikace
- Publicita


2,3%
13,6%
34,1%
34,1%
13,6%
2,3%
Negativní motivace
Pozitivní motivace
KO
USER
OK
Velmi nezodpovědní
+ 2SD
+ 1SD
Průměr
- 1SD
Velmi zodpovědní
-2SD

IV. Jak získané poznatky využít

- Klasifikace uživatelů
- Zlepšení bezpečnosti s pomocí uživatelů
- Návrh IT domobrany
- Shrnutí

Klasifikace uživatelů

Ostřílený mazák

Uživatel

Uživatel

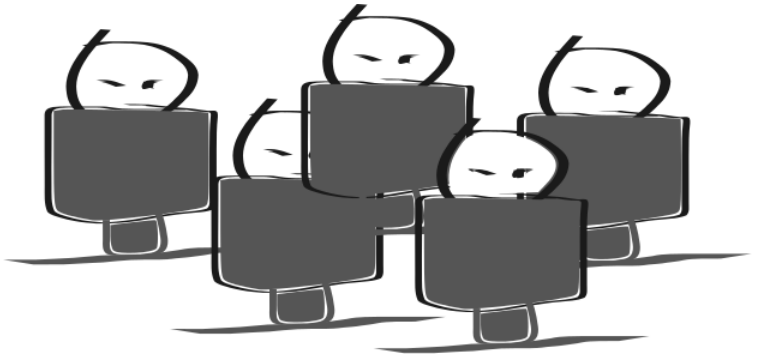
Průšvihář

Uživatel - průšvihář

- Notorická oběť bezpečnostních incidentů
- Nereaguje na pokusy o vzdělávání
- Nemá zájem cokoli měnit
- **Ideální honeypot**
- Podrobně sledovat jeho systém

Uživatel – běžný

- Bezpečnost není jejich pracovní náplň
- **Učí se** každým dnem
- Různá míra podlehnutí sociálnímu inženýrství
- Lze je **motivovat**
- Časem se zlepšují



Uživatel – ostřílený mazák

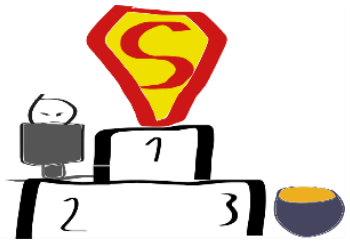
- Rozpoznává podvodné jednání
- Odolává sociálnímu inženýrství
- Má autoritu mezi ostatními (min. v IT)

- Vaše tajná, **nultá linie podpory**!
- Obvykle dotázán dříve než podpora

Zlepšení bezpečnosti s pomocí uživatelů

Návrh IT domobrany - soutěž

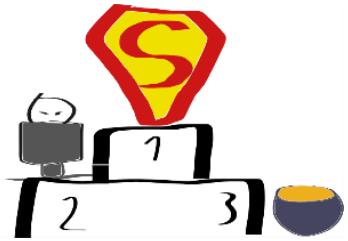
- Uživatelé reportují podezřelé aktivity
- Hodnocení na základě úspěšnosti
- Interní tabulka „průšvihářů“ (pro IT)
- Veřejná tabulka ostřílených mazáků
- Zvýhodnění pro aktivní uživatele



Návrh IT domobrany - příběh

- Proběhlé incidenty interně medializovat
- Krátký příběh o průběhu BI
- Popis hrozeb a jak s nimi bylo naloženo
- Odkaz na stránky podpory
- Zaslat všem uživatelům (newsletter)

Shrnutí



- Včasné varování od průšvihářů
- Znalostní báze mezi uživateli
- Vzdělání uživatelů - příběhy, soutěž
- Bezpečnost jako výzva
- Bezpečnost jako soutěž
- Bezpečnost jako součást pracovní náplně

Závěrečná vize – uživatelé budoucnosti

- Informovaní
- Motivovaní
- Pomáhající si
- Odolnější SI

Díky za pozornost

Miroslava Jarošová, FF UK, j.mirka@hotmail.com
Karel Nykles, ZČU CIV, knykles@civ.zcu.cz