AEC DATA SECURITY COMPANY

Uživatel jako zdroj rizik a přístupy k jejich zvládání

Petr Nádeníček

Obsah

- Úvod
- Základní profily uživatelů
- Negativní jevy typické pro organizace
- Vnímání bezpečnostních opatření uživateli
- Jak na uživatele?
- Shrnutí
- Závěr

Pohled na bezpečnost IS/IT

- Různé pohledy na metody zajištění informační bezpečnosti
  - technická/technologická stránka
  - organizační/personální stránka
- Člověk – nejslabší článek „řetězu“ (stará známá pravda).
- Nalezení vhodné rovnováhy mezi oběma hledisky – jeden z předpokladů úspěšného budování bezpečnosti organizace.

Proč se soustředit na uživatele?

- Efekty technických bezpečnostních řešení často degradovány „lidským činitelem“.
- Často nižší přímé náklady organizačních než technických opatření, i když s menší spolehlivostí…
- Aktuální zvýšení některých specifických rizik (globální recese)
  - propouštěný zaměstnanec je horší, než externí hacker - má znalosti a dokáže útok přesně zacílit
  - útoky způsobené propouštěnými zaměstnanci stály celkem za 18 % všech bezpečnostních incidentů v organizacích (zdroj: Verizon, 2008)
  - až 86 % respondentů potvrdilo, že chyby způsobené lidským faktorem jsou hlavní příčinou selhání IS (zdroj: Deloitte, 2009)

Důležité otázky

Moudrost se projevuje především schopností klást otázky.

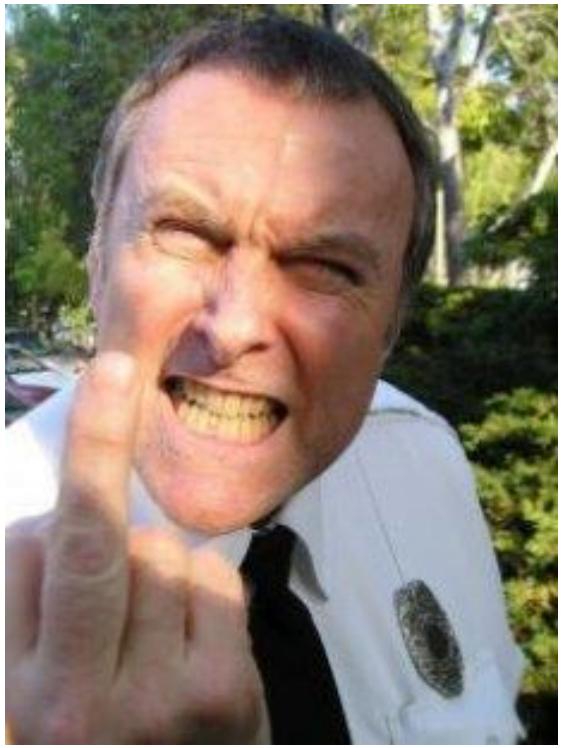
Ferdinando Galiani

- Jací jsou čeští (a moravští) uživatelé?
- Ve kterých oblastech představují uživatelé největší problém?
- Jaké jsou jejich nejčastější prohřešky?
- Jaká opatření a jakým způsobem implementovat, aby byla účinná?
- Jaké „zbraně" na uživatele nasadit?
- Kam až můžeme vůči uživatelům zajít?
- … a spousta dalších otázek.

Základní profily uživatelů

- Analfabet
  - PC jako psací stroj
  - využívá hlavně otrocky nacvičené postupy
  - každá „nestandardní“ situace jej překvapí a vyvede z míry
  - RIZIKA - pramení z neznalostí, chyb a omylů…
- Brouk Pytlík
  - má určité znalosti a předpoklady pro úspěšné využívání PC a IS
  - šťoural provádějící různé nežádoucí činnosti (SW, internet…)
  - RIZIKA – pramení z „přehnaného sebevědomí“ a víry ve vlastní schopnosti a znalosti (zavlečení virů, porušení licencí…)

Základní profily uživatelů



- Rebel
  - ze zásady nerespektuje opatření a pravidla
  - vždy dokáže najít argument, proč nemusí nebo nemůže něco dodržovat
  - RIZIKA – spojena s nerespektováním pravidel (např. v oblasti nakládání s informacemi)
- Ignorant
  - nadmíru pasivní (v organizaci spíše přežívá)
  - je příliš líný na to, aby dělal cokoliv, co nepatří přímo k výkonu jeho práce nebo nepřináší (z jeho pohledu) žádný výsledek
  - RIZIKA – spojená s pasivitou (bez hrozby postihu neudělá nic)

Základní profily uživatelů

- Rozumný uživatel
  - z pohledu bezpečnostního správce ideální uživatel
  - je vybaven potřebnými dovednostmi pro práci s výpočetní technikou
  - zná bezpečnostní pravidla, respektuje je a aktivně je naplňuje
  - někteří uživatelé se tomuto ideálu přibližují

- Většina uživatelů ve svém profilu kombinuje chování všech uvedených typů.
- Všeobecně čeští uživatelé mají menší respekt před autoritami a ve větší míře ignorují stanovená bezpečnostní pravidla (např. v porovnání s uživateli z anglosaských zemí).

Negativní jevy typické pro české organizace

- Do chování uživatelů se kromě uvedeného promítá také řada dalších aspektů:
  - firemní kultura,
  - přístup managementu,
  - vztahy mezi uživateli a IT personálem,
  - vztahy mezi uživateli navzájem atp.

- Pro české firmy a organizace jsou typické určité negativní jevy, které mají významný vliv na celkovou úroveň zabezpečení.

Negativní jevy typické pro české organizace

- Neformální vazby typu uživatel – management
  - mohou ovlivňovat definici bezpečnostních opatření (vedení pod tlakem)

- Neformální vazby typu uživatel - IT personál
  - mohou např. ovlivňovat řešení bezpečnostních incidentů (administrátor „přehlédne“ bezpečnostní přečin svého známého…)
- Nekompetentnost managementu v otázkách bezpečnosti
  - podpora vedení a jeho povědomí o bezpečnosti
  - vedení často není schopno správně pochopit důležitost a prioritu bezpečnostních opatření v kontextu fungování celé organizace

Negativní jevy typické pro české organizace

- Nedostatečné pravomoci bezpečnostního managementu/IT
  - malá pravomoc bezp. správce/manažera, případně administrátorů
  - vědomí, že IT nemá ve vedení oporu, navádí uživatele k ignorování bezpečnostních pravidel a IT personálu snižuje sebevědomí

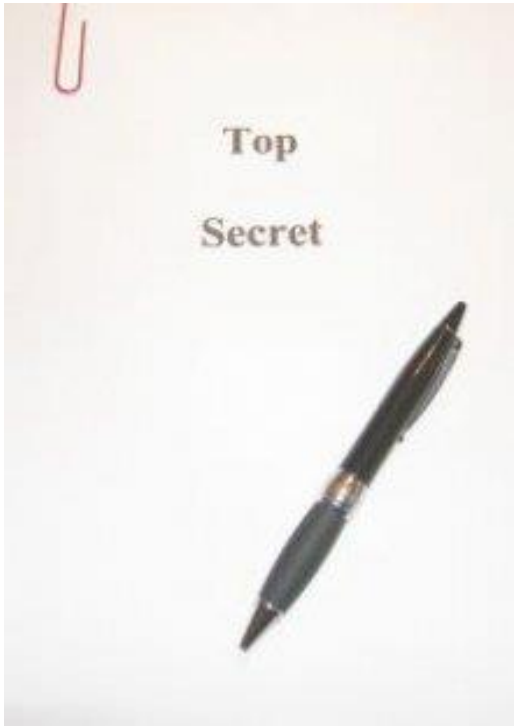
- Rezistence uživatelů
  - odlišné vnímání opatření ze strany uživatelů a bezp. managementu
  - na odpověď typu: „Tak to prostě nejde!“ se reaguje velice těžko

Jak (nyní) běžně spolu-pracujeme s uživateli?

- Standardní způsob zavádění bezpečnosti
  - analýza – bezp. politika – návazná dokumentace – implementace – školení – kontrola – zlepšování
  - „provozní slepota“ bezpečnostního managementu
  - odlišný pohled managementu – uživatelů – IT personálu – bezpečáků
- Uživatelé jsou často postaveni před „hotovou věc“ a podle toho někdy vypadají jejich reakce

Vnímání bezpečnostních opatření uživateli

- tradiční přístupy v duchu normy ISO 27002 (resp. ISO 17799)
  - pohled bezpečnostního managementu: není problém
  - pohled uživatelů: ???
- Zákaz používání soukromých prostředků
  - zákaz zasahování do HW je většinou chápán
  - horší situace je v oblasti např. vlastních USB disků, mobilů apod.
- Povinnost mlčenlivosti
  - informace související s prací nejsou uživateli častěji kompromitovány
  - některé informace ale uživatelé podvědomě za citlivé nepovažují



Vnímání bezpečnostních opatření uživateli

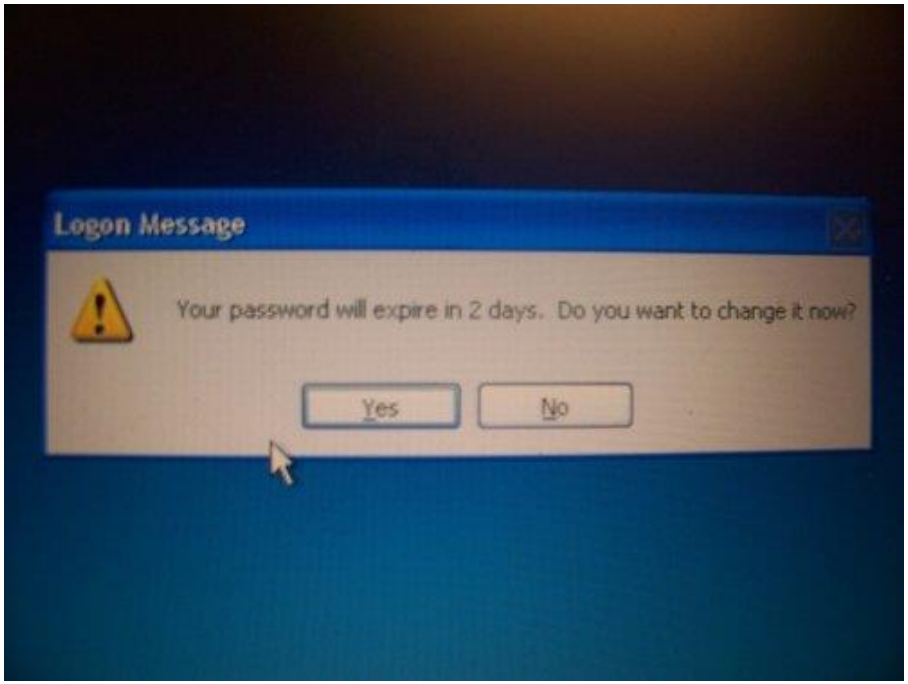
- Odpovědnost vlastníků aktiv
  - stanovení vlastníků aktiv - všeobecný problém
  - uživatelé nechápou, proč by měli zodpovídat za něco, co je z jejich pohledu v IS ("za IS odpovídá IT...")
  - uživatelé se zdráhají přijmout odpovědnost – důvodem bývá jejich pocit, že nemají na aktivum a jeho zabezpečení žádný faktický vliv
- Pravidla pro označování a nakládání s informacemi
  - absence vlastníků informačních aktiv ústí v nepoužívání klasifikace informací ve všech formách
  - těžké/nemožné prosazení těchto pravidel z pozice bezpečáka/IT

Vnímání bezpečnostních opatření uživateli

- Periodická bezpečnostní školení uživatelů
  - nesprávně zvolená úroveň výkladu vůči úrovni uživatelů - pocit podceňování – bagatelizace témat uživateli - nízký efekt školení
  - pokud se toho uživatelům řekne moc najednou, nezapamatují si skoro nic
- Fyzický bezpečnostní perimetr - související pravidla
  - pokud nejsou striktně vyžadována, pak je uživatelé aplikují intuitivně
  - projevy v dílčích porušení (např. ponechání cizích osob bez dozoru „zajděte si tam…“, „východ už najdete…“)

Vnímání bezpečnostních opatření uživateli

- Správa vyměnitelných médií a jejich likvidace
  - některé aplikace ISO 17799 mohou být již zastaralé
  - uživatelé v těchto případech požadavky na označování a likvidaci médií považují za přehnané a nerespektují je
- Pravidla pro používání hesel
  - uživatelé často nechápou, že heslo je vyjádřením jejich identity v IS
  - je to pro ně jen "něco, čím se přihlásí do počítače…„
  - je třeba situaci vysvětlit tak, aby ji na své úrovni pochopili



Vnímání bezpečnostních opatření uživateli

- Pravidla pro opuštění pracoviště, zásada prázdného stolu…
  - dělají mnohdy problémy i bezpečnostním profesionálům ☺
  - pokud nejsou zakotvena ve „firemní kultuře“, je jejich vnímání uživateli značně rozdílné
  - uživatelé bez negativní zkušenosti jsou zpravidla méně obezřetní

- Zabezpečení mobilní výpočetní techniky
  - uživatelé jsou většinou obezřetní u fyzického zabezpečení
  - horší je to u logického zabezpečení – uživatelé si plně neuvědomují všechny hrozby (např. zavlečení infekce do sítě organizace)
  - nutná kontrola ze strany IT

Vnímání bezpečnostních opatření uživateli

- Hlášení a řešení bezpečnostních incidentů
  - lidé se nechtějí cítit jako „práskači“
  - je tedy těžké nutit uživatele hlásit bezpečnostní incidenty
  - vliv osobních vazeb a firemní kultury
  - neoblíbenost registrů, formulářů apod.
  - vliv pohodlnosti uživatelů

Jaká opatření tedy implementovat, abychom se vystříhali negativnímu vlivu uživatelů na bezpečnost IS?

Jak na uživatele?

- Osobnostní charakteristiky jednotlivých uživatelů z pozice bezpečnostního správce nebo administrátora s největší pravděpodobností nezměníme.
- Pokud chceme uživatele pozitivně ovlivňovat s cílem minimalizovat jejich negativní vliv na zabezpečení organizace, musíme začít s tím, nad čím máme kontrolu.
  - návrh bezpečnostních opatření
  - způsob komunikace s uživateli
  - metody kontroly uživatelů
  - jednoduše způsob „práce s uživateli“…

Jak na uživatele?

- „Smysluplnost" bezpečnostních opatření vůči fungování organizace
  - konstruovat opatření tak, aby co nejvíce vyhovovala procesům organizace
  - opatření neomezující běžné činnosti uživatelů, nebudou vnímána uživateli tak negativně
  - pokud je plné přizpůsobení bezp. opatření procesům nemožné, je třeba najít vhodný kompromis a ten dostatečně komunikovat s dotčenými uživateli
  - příklad: postupy pro skartaci médií

Jak na uživatele?

- Poznání samotných uživatelů
  - pokud chceme působit na uživatele efektivně, musíme vědět, s kým máme tu čest
  - lépe se působí na uživatele, o kterém něco víme (u těch problémových to platí dvakrát)
  - spoustu potřebných informací může bezpečnostní správce vyšťourat při prověrkách různých logů i samotných uživatelů přímo na pracovišti…
  - vše musí být v rámci zákona (!)

Jak na uživatele?

- Komunikace směrem k uživatelům
  - neustále vysvětlovat význam a důvody všech bezpečnostních opatření, která nějakým způsobem dotýkají uživatelů
  - možno provádět v rámci periodických školení uživatelů, ale i v každodenním provozu (možnost zapojení firemních komunikačních prostředků: intranet, firemní časopis…)
  - bezpečnostní správce se nesmí uživatelů stranit, ale musí s nimi být v každodenním kontaktu
  - bezpečnostní správce musí být schopen rozeznat hranice „zdravého kontaktu“ s uživateli a chovat se s potřebnou profesionalitou

Jak na uživatele?

- Praktické zkušenosti uživatelů
  - stokrát sdělená informace se uživatelům nezapíše do paměti tak hluboko, jako jednou prožitá
  - je vhodné do každodenní bezpečnostní praxe zahrnout neustálé „zkoušení bdělosti“ uživatelů

  - vhodným nástrojem je testování uživatelů metodami sociálního inženýrství (telefonicky, e-mailem, pohozenými médii: např. před školením – zesílení efektu), lze použít cracking hesel apod.
  - operativní kontroly na pracovištích (správce jako narušitel)
  - pozor na citlivé použití těchto metod v souladu s firemní kulturou

Jak na uživatele?

- Omezení uživatelů technickými prostředky
  - pro prosazení bezpečnostních opatření do praxe přednostně použijte technické prostředky, které již máte k dispozici (např. pro řízení přístupu): síťové prvky, web proxy, DLP…
  - všechno ale není „jen“ otázka dostupných prostředků, ale také toho, kam až je možné v rámci dané organizace zajít
  - přílišné „utažení“ bezpečnosti v rámci IS nemusí být žádoucí
  - ekonomické hledisko řešení bezpečnosti technickými prostředky (u nově pořizovaných bezpečnostních řešení – př. cena DLP řešení versus cena za proškolení uživatelů)

Jak na uživatele?

- Perzekuce
  - když už není zbytí, musíme postupovat v duchu hesla: „na hrubý pytel hrubá záplata“
  - v typických českých firmách a organizacích není příliš zvykem uživatele za chyby přísně trestat

  - exemplární potrestání může mít velký preventivní účinek na všechny uživatele/zaměstnance
  - pozor na „šikanu“ – je třeba přistupovat k trestání velice citlivě tak, aby se zaměstnanec necítil ponížen a neutrpěla jeho důstojnost

Shrnutí

- Uživatel – nezanedbatelný prvek bezpečnosti IT/IS.
- Český uživatel a česká firma/organizace má určitá specifika.
- K řešení bezpečnosti na úrovni uživatelů je třeba přistupovat systematicky, s rozmyslem a s přihlédnutím k místním podmínkám.
- Dostupné nástroje: forma opatření, psychologie, komunikace, praktické zkušenosti, technické prostředky, kontrola, trestání…
- Větší zacílení na uživatele může být jedním ze směrů řešení bezpečnosti IT/IS v aktuální hospodářské recesi.

Závěrem

- Nebylo mým cílem se jen zamýšlet nad negativním vlivem uživatelů, ale především, poskytnout bezpečnostním správcům, manažerům a všemu IT personálu impuls k zamyšlení se nad tím, jak k uživatelům přistupovat tak, aby znamenali co nejmenší riziko.
- Chyby nelze hledat jen u samotných uživatelů, ale je třeba začít u sebe samého (jak s uživateli komunikujeme, jak navrhujeme bezpečnostní opatření, jak řešíme incidenty atd.).

I když jsme „jenom IŤáci“, pracujeme také s lidmi...

Děkuji za pozornost

petr.nadenicek@aec.cz