

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Přístupy prosazování bezpečnosti v organizaci

Petr Nádeníček

AEC, spol. s r.o.





Obsah

Vymezení tématu

Faktory působící na prosazování bezpečnosti

Prosazování bezpečnosti z různých úrovní

Prosazování opatření v některých oblastech

Shrnutí, závěr



Vymezení tématu

Co rozumět pod pojmem „prosazování bezpečnosti“?

- Soubor metod jak implementovat bezpečnostní pravidla, procesy a procedury (bezpečnostní opatření) do každodenní praxe organizace.
- Tyto metody se mohou pohybovat v různých rovinách:
 - vysvětlování významu bezpečnosti
 - firemní politiky
 - nátlaku – na různé skupiny
 - zastrahování – příklady důsledků
 - ...



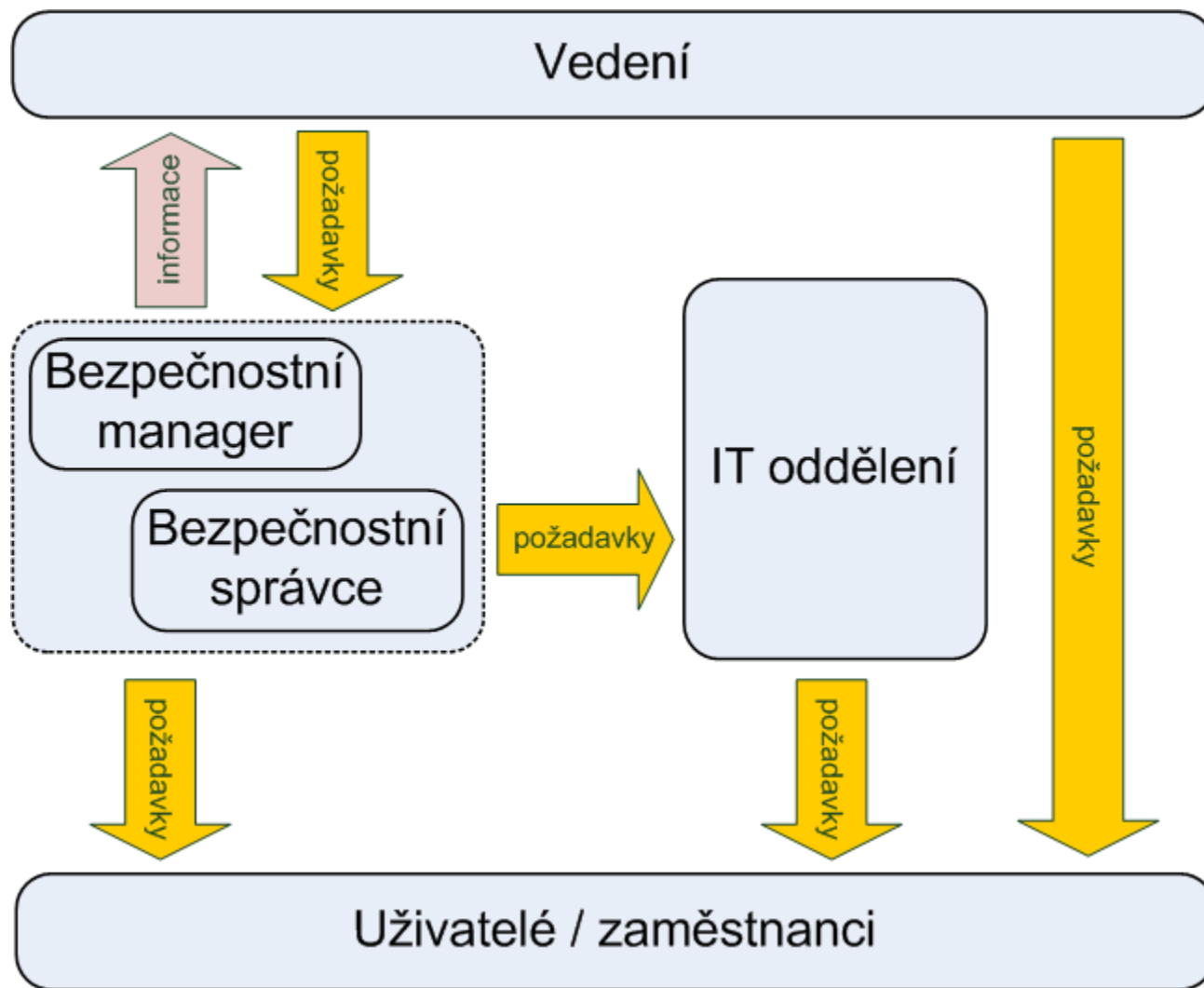
Faktory

Jaké faktory v organizaci působí na to, jakým způsobem je bezpečnost prosazována?

- **Odkud je bezpečnost prosazována**
 - Vedení organizace
 - Bezpečnostní manažer
 - Bezpečnostní správce
 - IT oddělení
- **Další faktory**
 - Velikost a typ organizace
 - Firemní kultura
 - Rozpočty
 - Závislost organizace na „bezpečnosti“



Kým je bezpečnost prosazována?





Prosazování z úrovně vedení

Osvícené vedení – málokdy dosažitelný ideál

- Pouze deklarativní podpora bezpečnosti nestačí
- Negativní i pozitivní vliv vedení na bezpečnost

Ne všude vedení bezpečnost prosazuje

- Důsledky autoritativního (arogantního) vedení
- Nevděčná pozice bezpečnostního manažera/správce
- Potřeba vysvětlení si vzájemných pozic/potřeb (ne vždy možné)

Pohled vedení versus pohled „bezpečnosti“

- Prosazování potřeb „bezpečnosti“
- Prosazování potřeb „businessu“



Prosazování z úrovně bezp. manažera

Úroveň působení bezpečnostního manažera

- Člen vrcholového vedení, středního managementu nebo jiná úroveň...

Prosazení odpovědností a pravomocí do bezpečnostních politik, směrnic a další interní dokumentace organizace

- Nejen formální, ale i v praxi

Důsledné prosazování bezpečnosti v každodenní praxi

- Šetření incidentů, provádění kontrol...nepřivírat oči



Prosazování z úrovně bezp. správce

Pozice bezpečnostního správce v organizaci

- Správce podléhající bezpečnostnímu manažerovi
- Pouze bezpečnostní správce bez nadřízeného bezp. manažera

Často velmi omezené možnosti prosadit bezpečnost z této pozice

- Nemá k dispozici přímé pravomoci – tzn. nutnost prosazovat vše přes nadřízeného

Zaměření správce spíše na operativu – možnost zkresleného pohledu na jiné úrovně řízení bezpečnosti



Prosazování z úrovně IT oddělení

Častá situace v mnoha (zejména malých a středních) organizacích – bezpečnostní správce součástí IT oddělení

Rozporuplné reakce zbytku organizace na snahy IT o zabezpečení IS

- Despekt zbytku organizace vůči IT, nepochopení potřeb
- „Provozní slepota“ IT pracovníků, nepochopení požadavků businessu



Několik tipů k prosazování bezpečnosti v některých konkrétních oblastech

- Přístup k prosazování některých bezpečnostních opatření/oblastí...
- S čím se setkáváme v praxi...
- Co se dá použít...



Bezpečnostní politika

Jen stoh popsaného papíru nebo opravdu používaný soubor pravidel?

Jak přiblížit bezpečnostní politiku celému spektru zaměstnanců organizace?

- Vhodný rozsah, jazyk a struktura samotné politiky
 - Může mít dopad na použitelnost politiky jako takové
- Vytvoření „specializované“ dokumentace, která bezp. politiku zprostředkuje i běžným uživatelům v organizaci
 - Uživatelské příručky – jen to, co se uživatelů přímo týká, s čím se setkávají, co se po nich chce...



Identifikace aktiv

- Často obtížně uchopitelné
 - Do jaké míry podrobnosti zajít?
 - Přístup k fyzickým X informačním aktivům

Stanovení vlastníků aktiv

- U některých aktiv se vlastnictví stanovuje obtížně
- Odpovědnost – ale kde jsou pravomoci?
- To, za co odpovídám, mohu i fakticky ovlivnit?



Personální bezpečnost

Budování bezpečnostního povědomí

Vhodná forma vzdělávání uživatelů

- Prezenční - školení, samostudium - elearning, průběžná – např. bulletiny a novinky
- Přenesení vzdělávání do praxe

Ověření úrovně bezpečnostního povědomí

- Průběžné testy uživatelů (metody sociálního inženýrství) – vhodný způsob popularizace bezpečnosti „virálním“ způsobem
- Průběžné kontroly dodržování pravidel



Zvládání bezpečnostních incidentů

Formální X faktické fungování procesu řízení bezpečnostních incidentů

- **Neochota lidí hlásit incidenty**
 - Neradi na někoho ukazují, psychologie...
- **Neochota vedení vyvozovat důsledky incidentů**
 - Neradi by někomu „uškodili“...
- **Diferenciovaný přístup k různým zaměstnancům**
 - Před bezpečností jsme si všichni rovni, ale někteří jsou si rovnější...

Simulované případy (testy) jsou lepší, než nutnost opravdového trestání.



Prosazování - shrnutí

Co potřebujeme, abychom mohli bezpečnost účinně prosadit? Jak na to?

- **Opravdová podpora vedení**
 - Deklarativní i praktická
- **Vhodná struktura bezpečnostních rolí**
 - Pozice bezpečnostního manažera/správce
- **Návrh „bezpečnosti“ v souladu s businesssem**
 - Respektování a sladění s potřebami businessu
- **Kultura organizace „přátelská“ k bezpečnosti**
 - Reakce na bezpečnostní opatření, ochota přijímat nové věci...



Závěrem

Prosazování bezpečnosti v organizaci je málokdy jednoduché

- Jen málo firem má takové prostředí, které absorbuje zavedení bezpečnosti bez zádrhelů
- Musíme se zamyslet nad tím, jaký způsob prosazování bude pro danou organizaci ten nejvhodnější
- Schopnost „vykouknout ze své jeskyně“ – není jen bezpečnost
- Nutnost vypořádat se s širokým spektrem vlivů

Vyváženost opatření na úrovni organizační bezpečnosti a technické bezpečnosti

- Všechno má svá „pro“ a „proti“

Děkujeme za pozornost.

Petr Nádeníček

AEC, spol. s r.o.

petr.nadenicek@aec.cz

