Slezská univerzita v Opavě
Obchodně podnikatelská fakulta v Karviné

BEZPEČNOST A ANONYMITA NA INTERNETU

Ing. Lukáš Macura

27.2.2013

Dohledávání bezpečnostních incidentů na SU

Lukáš Macura, ÚIT
macura@opf.slu.cz

Obsah:

- kdo jsme
- co děláme
- proč to děláme
- proč to neděláme
- naše zásady
- naše zbraně
- pawouk
- nikdo není anonymní
- závěr

Kdo jsme?

- Centrum informačních technologií (CIT)
- správa centrálních systémů univerzity
- tvorba koncepce rozvoje a koordinace nasazení IT v rámci SU
- pokouší se o metodické řízení UIT

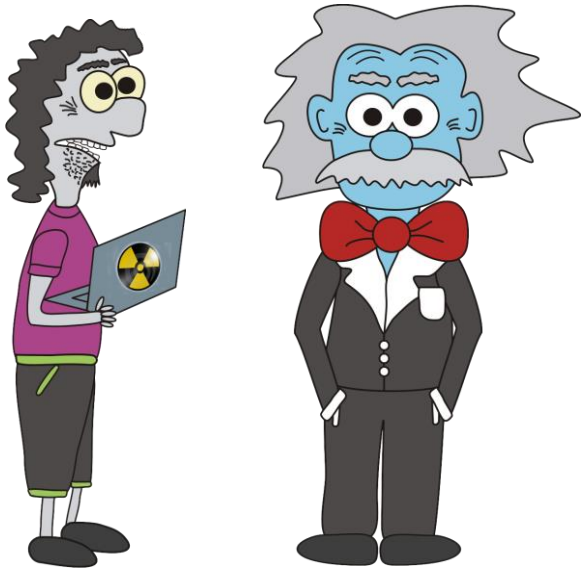
- Ústav informačních technologií (ÚIT)
- působnost v Karviné
- provázanost s CIT (vzájemná
- výpomoc a brainstorming)
- pokouší se o metodické
- řízení CIT

Co děláme?

- správa IS STAG
- správa MAGION
- spisová služba
- správa univerzitní sítě
- správa WWW serverů
- správa LDAP
- koordinace a integrace IT služeb
- koncepce a rozvoj IT

Proč to děláme?

- aby vše fungovalo jak má
- aby uživatelé byli spokojeni a měli všechny potřebné IT služby
- abychom ochránili naše uživatele před útoky zvenku
- a naopak...
- abychom uchránili SU před případnými právními spory
- protože to dělat chceme... ;-)



Proč to neděláme?

- abychom vymýšleli nesmyslná pravidla
- abychom naštvali všechny uživatele
- abychom se cítili jako pánové světa
- abychom šmírovali provoz
- abychom uživatelům dělali práci složitější

Naše zásady

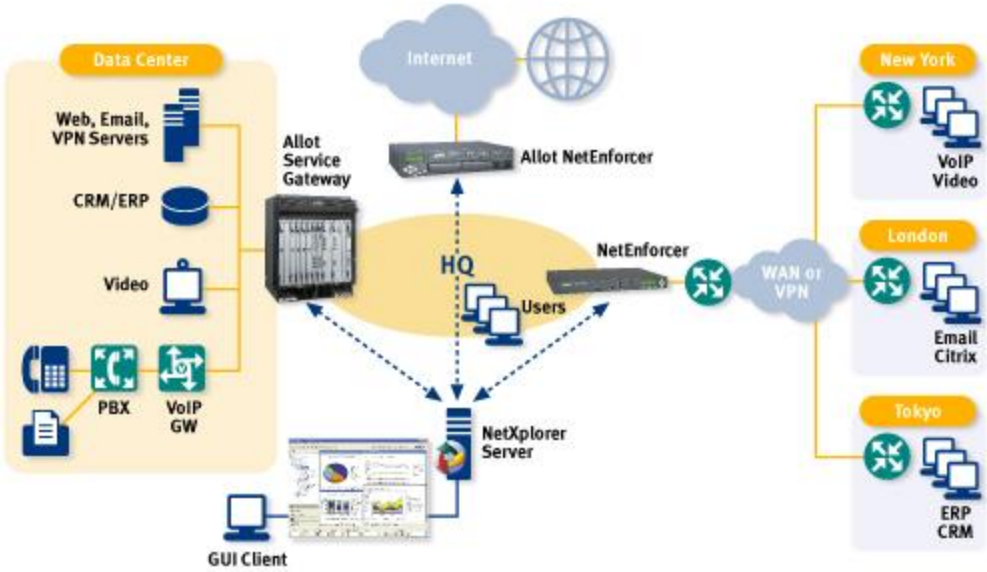
- nešmírujeme
- statistiky sledujeme průběžně
- hloubkovou analýzu síťového provozu děláme až v případě,
- že je to nutné
- ctíme právo uživatele na soukromí, dokud není nezbytně
- nutné jej prolomit
- snažíme se být ”hodní” na ”hodné” uživatele
- a naopak...
- posuďte sami.. (rajčata prosím ne...)

Co očekáváme od uživatelů

- samostatnost
- nemůžeme všem nastavovat všechny služby, to je nereálné
- čtěte manuály
- sledujte http://uit.opf.slu.cz/
- sledujte http://www.slu.cz/help/cz/
- čtěte maily
- v mailech se často objeví důležité informace
- neznalost se neomlouvá

Naše zbraně

- Juniper, ASA
- analýza aktuálního provozu a útoků (firewall)
- logování špatností
- blokování špatností
- ochrana nás před Internetem a naopak...
-
- Allot
- analýza L7 provozu
- detekce P2P sítí a statistika
- provozu
- možnost ”zaříznout” P2P úplně
- statistika ”best off”



Naše zbraně

- Flowmon sonda
- analýza a ukládání dat provozu sítě
- dohledávání incidentů zpětně
- logujeme pouze hlavičky, obsah je nedotknutelný
- korelací nalezneme vše zpětně
- nikdo není anonymní
- ani externí eduroam uživatelé
- Rsyslog
- centrální logovací nástroj
- Zabbix
- centrální monitoring
- FTAS
- pro hlubší porozumnění toků na síti

Pawouk

- IS studentské sítě
- 802.1x a webauth
- radius
- možnost zablokovat studenta
- autorizace PC pro přístup na Internet
- každý tok z a do sítě dohledatelný
- každý je zodpovědný za svoje chování

Nikdo není anonymní!

- za svoje chování na síti je každý plně zodpovědný
- neexistuje anonymní připojení, vše se dá dohledat
- cokoliv děláte, předem přemýšlejte. Srovnejte s reálnou situací.
- Udělali by jste stejnou věc i mimo Internet?
- dávejte si pozor na svoje PC/notebook a chraňte jej před hrozbami
- nezabezpečený počítač je zdrojem problémů

Děkuji za pozornost

Lukáš Macura

Slezská univerzita v Opavě
Obchodně podnikatelská fakulta v Karviné
Ústav informačních technologií

Slezská univerzita v Opavě
Centrum informačních technologií