



Řešení pro vaše technologie, technologie pro vaše řešení

Filip Navrátil
PCS spol. s r.o.
Divize DataGuard
stánek 45 přízemí

Skupina PCS

- Společnosti sjednocené pod názvem PCS se zabývají širokým spektrem činností – od komplexních služeb v oblasti zabezpečovacích a komunikačních systémů, detekci nebezpečných předmětů, přes dodávky analytických přístrojů a měřících ústředen až po řešení bezpečnosti dat. Významnou součástí tvoří vývoj vlastního ekonomického software a nemocničních informačních systémů.
- Skupina PCS působí na českém a slovenském trhu již od roku 1990, zaměstnává přes 100 pracovníků a její roční obrat přesahuje 250 milionů Kč (2007).



Divize DataGuard

- od vzniku v roce 1992 jsme dodavatelem bezpečnostních řešení špičkové kvality
- zastupujeme zejména zahraniční výrobce komplexní antivirové ochrany, kteří kromě tradičního antiviru nabízejí i ochranu proti spamu, spyware a adware, IPS, firewally a další
- nabídku doplňují produkty vzdáleného přístupu, HW/SW auditů firemních sítí a šifrování dat
- jsme distributorem produktů Kaspersky pro Českou a Slovenskou republiku
- u ostatních výrobců jsme držiteli těch nejvyšších úrovní partnerství předpokládajících technické a obchodní certifikace
- od analýzy bezpečnostních rizik, návrhu řešení, testování produktů po realizaci doporučených postupů. Běžnou součástí všech služeb je hot-line a hot-mail, nabízíme i pravidelné kontroly nainstalovaných produktů, stálou technickou pohotovost, školení zaměstnanců nebo úplný outsourcing bezpečnostních prvků
- našimi zákazníky jsou domácí uživatelé stejně jako střední firmy a v neposlední řadě i ty největší korporace v České republice

Státní správa

- mnoho úřadů, institucí i ministerstev využívá služeb PCS, máme tedy přehled o situaci v sektoru státní správy

Aktuální problémy :

- 1. ztráta a zneužití citlivých dat**
- 2. kontrola a regulace přístupu k internetu**

Ztráta a zneužití citlivých dat



Ztráta a zneužití citlivých dat

- Většina společností vnímá jakékoli bezpečnostní hrozby pouze jako hrozby „zvenku“.
- Proti útoku z venku jsou firemní data lépe či hůře chráněna.
- Jsou ale vaše citlivá firemní data chráněna proti zcizení nebo ztrátě zevnitř?
- Ztráta citlivých dat z organizace probíhá většinou standardními kanály jako je email, web, USB zařízení nebo tisk.
- Většina mobilních uživatelů denně opouští společnost s několika důležitými dokumenty.
- Máte nějakou kontrolu nad tím, co se s těmito dokumenty děje?

- Zabezpečte se proti ztrátě dat dříve, než nastane!

Ztráta a zneužití citlivých dat

- Nabízíme řešení prevence ztráty dat (Data Loss Prevention/DLP)
- DLP umožňuje ochranu na více vrstvách, a to jak pro spravované, tak i neznámé zařízení (host –based, gateway)

Data Loss Channels	Gateway			Host		
	Corporate Network	Public Internet	Disconnected	Corporate Network	Public Internet	Disconnected
Email	✓			✓	✓	✓
IM				✓	✓	✓
HTTP	✓			✓	✓	✓
Copy and Paste				✓	✓	✓
Local/Screen capture				✓	✓	✓
External (USB)				✓	✓	✓
Web Mail	✓			✓	✓	✓
Agent-less Devices	✓					
Blackberry	✓					



Ztráta a zneužití citlivých dat

- Kategorie dat a politiky pro jednotlivé skupiny uživatelů jsou definovány na centrálním serveru, na stanicích běží pouze agent, který komunikuje se serverem a prosazuje aktuální politiku (a to i v režimu offline, tj. mimo síť).
- DLP chrání všechny běžné kanály - email, webmail, peer-to-peer applications, IM, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, printers, fax, and removable storage.
- Administrátor má k dispozici následující akce při pokusu o nepovolenou akci:
 - Monitor – povolí přenos dat
 - Prevent – zakáže přenos dat
 - Alert – upozorní administrátora/uživatele
 - Encrypt – zajistí zašifrování dat před odesláním*
 - Quarantine – vyčká na autorizaci*

Ztráta a zneužití citlivých dat

- DLP řešení je spravováno centrální správou, která umožňuje jak instalaci produktu, tak i zpětný reporting.
- Repoty o incidentech zahrnují všechna potřebná data pro analýzu události
 - odesílatel, příjemce, čas incidentu, informace o datech, přílohy emailů, apod.
- Doporučujeme řešení McAfee.



Kontrola a regulace přístupu k internetu



Kontrola a regulace přístupu k internetu

- Přístup k internetu pro pracovní účely je nezbytný!
- Četné studie potvrzují, že více než 60 procent zaměstnanců tráví až třetinu pracovní doby surfováním po stránkách, které nesouvisí s výkonem jejich práce (zábava, sport, cestování, nákupy, pornografie,...)
- Dopady této skutečnosti pro organizace:
 - Únik informací z organizace
 - Snížení produktivity zaměstnanců
 - Zvýšení zátěže linky (filmy, videa, hry...)
 - Bezpečnostní riziko (viry, spyware, adware, ...)
 - Nelegální obsah na svých počítačích
 - Přístup k nevhodnému obsahu

Kontrola a regulace přístupu k internetu

- Monitorování / filtrování přístupu k internetu
 - Monitorováním internetového provozu vám podá přehled o využívání internetu v organizaci a zdokumentuje nevhodnou aktivitu uživatelů.
 - Na základě dat z monitoringu lze přesně rozhodnout, jaké oblasti mají být blokovány.



Kontrola a regulace přístupu k internetu


- Výhody námi nabízeného řešení:
 - Filtrace přístupu k obsahu dle více než 90 kategorií (free mail, games, chat,...)
 - Pravidelně aktualizované databáze URL adres
 - Definice politik dle individuální nebo skupinových potřeb (uživatel, skupina, IP adresa, čas, objem dat ...)
 - Možnost definice vlastních skupin
 - Účelné využití internetové konektivity
 - Akce na jednotlivé skupiny adres (povolit, zakázat, pozdržet, varovat, monitorovat...)
 - Detailní reporting o prováděných akcích

- Doporučujeme řešení Secure Computing





Děkuji za pozornost



Filip Navrátil
PCS spol. s r.o.
Divize DataGuard
stánek 45 přízemí