

Bezpečnost v praxi
prostředí Internetu; případová studie

PV080

Vašek Matyáš

Internet a bezpečnost

- Důvěrnost a integrita emailu
 - S/MIME (Netscape, Outlook) – stejný certifikát jako pro SSL – viz přednášku k podpisu
 - PGP (ale i další – disk, ICQ atd.)
- Důvěrnost a integrita WWW komunikace
- Anonymita – viz dřívější přednášky
- Firewally
- Odmítnutí služby
- Eternity server

Pretty Good Privacy

- Umožňuje šifrování a digitální podpis (+ jiné)
- Kombinace sym. a asym. kryptografie
 - Šifrování – veřejným klíčem příjemce se šifruje vždy nově generovaný klíč pro sym. šifru
 - Podpis – soukromým klíčem se podpíše haš zprávy
- Autor Phil Zimmermann, přes 20 let od v1!
- Integrace – elm, mutt, Eudora, Outlook...
- Nyní výraznější vývoj přes Gnu Privacy Guard (GPG / GnuPG)
- Více na www.gpg.cz (dříve www.pgp.cz)

PGP klíč

- RSA (2.6.x) a Diffie-Hellman/DSS
- Délka klíče
- *UserID* – obvykle jméno a email
- Otisk (fingerprint)
- Úroveň důvěry – zachovávat opatrnost!!!
- A další: KeyID, datum vytvoření, platnost (novější verze PGP)...

Klíče PGP

- Klíčenka (keyring)
- Revokování – problém ztráty hesla nebo narušení integrity
- Tranzitivita důvěry
 - Věřím těm, kterým věří ti, kterým věří Alice
- Servery klíčů
 - Také přes www.gpg.cz

Podepisování klíče

- Podepsat vlastní klíč!!!
 - Integrita
- Cizí klíče jen při důvěryhodném předání!!!
 - Zaslání emailem nebo web link NEJSOU DŮVĚRYHODNÉ!
 - Osobní předání na disketě
 - Ověření otisku před podpisem (telefon, papír ap.)
 - Důvěryhodný zprostředkovatel (!)

Další vylepšení PGP

- Šifrování disku
 - Dokonalejší mazání dat (wipe/shred)
 - Práce s certifikáty X.509 a PKI vůbec
 - Rozdělení klíče (prahová kryptografie)
 - Problém s odvoláním klíče – designated revoker
 - ICQ plugin
 - Fotografie k *UserID*
- ...atd

Ukázka práce s PGP/GPG

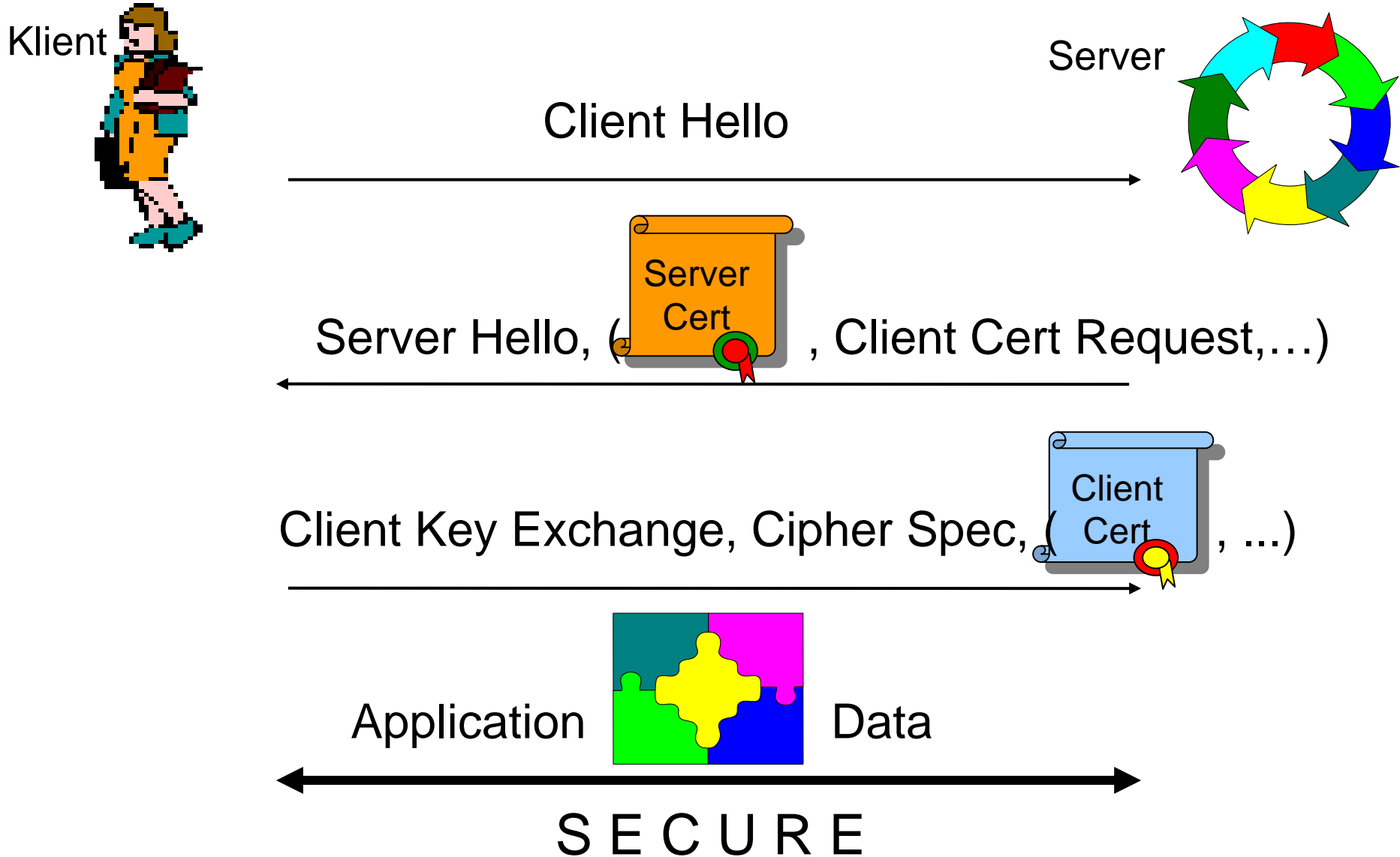
TLS (Transport Layer Security), dříve jako SSL (Secure Sockets Layer)

- Protokol pro
 - Autentizaci entit (klient, server)
 - Kontrolu integrity
 - Důvěrnost komunikace
- Vyvinut firmou Netscape, široce podporován
- Běží na protokolech jako TCP a je transparentní pro vyšší HTTP, FTP...
- Certifikáty X.509, WWW prohlížeče

O TLS/SSL

- TLS/SSL Record Protocol
 - Základní vrstva
- TLS/SSL Handshake Protocol
 - Pro úvodní autentizaci a nastavení parametrů spojení
 - Autentizace serveru default (lze zrušit), klienta na vyžádání
 - Autentizace digitálními certifikáty (klíči)

TLS/SSL Handshake Protocol



Protokoly, o kterých můžete slyšet

- IPSec – zajištění bezp. pro IPv4
- IPv6
 - Šifrování i ochrana integrity přímo v možnostech IP
- SET (Secure Electronic Transactions)
 - Dnes zajímavý příklad: bezpečnost vs. přidaná hodnota
 - Bezpečnost velmi vysoká
 - Použitelnost z hlediska zákazníka a obchodníka komplikovaná
 - Náročnost vedla k zániku (původní verze)

Autentizace pro internetbanking

- TLS/SSL kanál – ochrana hesla
- Klientský certifikát (Trojský kůň!)
- Jednorázová hesla
 - Fyzický generátor (lze i závislost na čase ap.)
 - Předem vygenerovaná posloupnost na papíru
- Homebanking, speciální aplikace/plugin

Firewally

- Název odpovídá koncepci – jedná se o umělou překážku mezi chráněnou zónou a potenciálně nebezpečným okolím
- Chrání proti útokům zvenčí (proti těm, které přes něj vedou! 😊) na data/slужby uvnitř
- Možnosti řešení:
 1. *Povol*
 2. *Zakaž*
 3. *Přelož (proxy – aplikační brána), příp. jiné*
- Citlivá otázka útoků odmítnutím služby

Systemy detekce průniku (narušení)

- Intrusion Detection Systems
- Principy jako u antivirů
 - Detekce atypického chování
 - Detekce vzoru (průniku)
- Umístění (v systému)
 - Počítačové (host-based)
 - Síťové (network-based)
- Také neochrání proti tzv. sociálnímu inženýrství 😊

Odmítnutí služby (Denial of service)

- Provozovatel serveru
 - Ochrana vlastního systému
 - Závislost na páteřních sítích, DNS, příp. službách CA
- Uživatel – primárně ochrana vlastního počítače, ale dále
 - Může k provozu potřebovat fungující lokální síť
 - Spoléhá na ISP
 - Spoléhá na provozovatele serveru
- Distribuovaná verze útoku, farmy připravených strojů aj.

Zajímavost – Eternity server

- Ross Anderson '96 (Pragocrypt)
 - <http://www.cl.cam.ac.uk/~rja14/#Peer-to-Peer>
- „Věčné“ uložení informací
- Lze jen uložit, nalézt a vyzvednout
 - lze dále kombinovat, např. se šifrováním
- Mazat nemůže ani původce (násilné donucení!)
- Velké množství spolupracujících serverů
- Různé geografické a právní umístění

Steganografické souborové systémy

- Běžné použití kryptosystému k utajení dat:
 - $E_K(M) = M'$ (jednoznačně)
 - $D_K(M') = M$ (jednoznačně)
- Osobě, která nezná K , je M nečitelné.
- Majitel M nepopře existenci utajené informace ...
- ... a může být k odhalení K donucen (soud, ...).
- Když K prozradí, dojde jednoznačně k odhalení M .
- Když místo pravého K oznámí nějaký jiný, náhodný klíč, bude evidentní, že lže.

Steganografické souborové systémy II.

- Jak zajistit, aby majitel M mohl popřít existenci M , a to věrohodně, tj. tak, že mu nebude možné dokázat, že M existuje?
- = věrohodná popiratelnost (plausible deniability, PD)
- Triviálně např. one-time-pad zajišťuje PD:
 - M = „zabijupapouska“
 - K = „jkhgxyzileqwpov“
 - M' = „ikiogtxlteqhyv“
 - a při vymáhání klíče je možné věrohodně tvrdit:
 - K = „wcxuxzileqwpov“
 - M = „milujupapouska“

Steganografické souborové systémy III.

- Zajímavější situace z praxe: souborové systémy (FS).
- Klasický kryptografický FS:
 - šifruje obsah souborů i veškeré režijní struktury FS
 - měněné bloky automaticky „v pozadí“ (de)šifrovány
 - FreeOTFE, TrueCrypt, linuxový cryptoloop, eCryptfs, ...
- Platí: dobře zašifrovaná data \approx proud náhodných bitů.
- I když je na disku krypt. FS dobře ukryt (vedlejší diskový oddíl), existuje a vzbudí pozornost právě svým kvalitně náhodným vzhledem.
- Běžné soubory na disku zpravidla nevykazují takovou úroveň náhodnosti.

Steganografické souborové systémy IV.

- Kryptografický FS poskytující PD (spadá již pod steganografii):
 - šifruje obsah všech souborů (dobrý důvod: důvěrnost dat)
 - šifruje režijní struktury (dobrý důvod: důvěrnost metadat)
 - „volného místo“ zaplňuje náhodnými bity a v tomto stavu jej neustále udržuje (dobrý důvod: zničení obsahu souborů při mazání + maskování množství a pozice volného místa)
- Celá plocha FS je nerozpoznatelná od náhodných dat.
- Necht' FS obsahuje soubory, jejichž obsah vypadá důvěrně, ale jejichž odhalení nezpůsobí potíže.
- Skutečně důvěrná data jsou (zašifrovaná) přítomna ve „volném místě“ – často v separátním, vnořeném FS.

Steganografické souborové systémy V.

- Majitel pod nátlakem odhalí klíč k dešifrování vnějšího kryptografického FS – pointa: něco odhalil.
- Že je něco ve „volném místě,“ nelze dokázat – vypadá náhodně a pro to existuje dobrý důvod.
- Kontroverze kolem FS s ukrytým obsahem.
 - Zatajování vnořeného FS je sice v čisté teorii možné, nicméně není to o nic méně lživé – např. před soudem by nakonec stejně leckdo vypověděl pravdu.
 - Data ve vnořeném FS jsou utajená pouze za idealizovaných okolností – v praxi může být existence vnořeného FS odhalena např. skrze OS a aplikace (dočasné ulož. aplikací MS Office, indexovací SW typu Google Desktop, odkazy na nedávno otevřené dokumenty v MS Windows ap.).

***„Případová studie“ –
Co je to vlastně bezpečnost?***

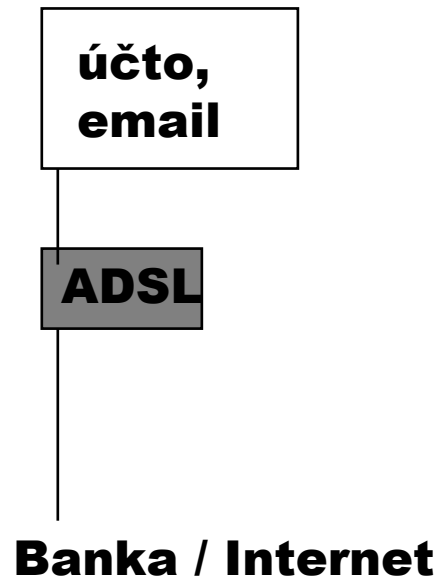
Spolupráce – Roman Pavlík (www.tns.cz)

DoTheThing!, s.r.o.

- Pracovní síly na „záskok“ v oblastech manuálních prací, pohostinství ap.
- Začínáme jako „studentská“ firma se dvěma spolujemajiteli.
- Využití studentů – výrazný podíl komunikace po Internetu.

IT SECURITY

DoTheThing!, s.r.o., založena!



Potřeby

- Účetní software.
- MS Office, Outlook.
- ADSL připojení do Internetu.
- Homebanking.

IT Security – rozhodují spolumajitelé

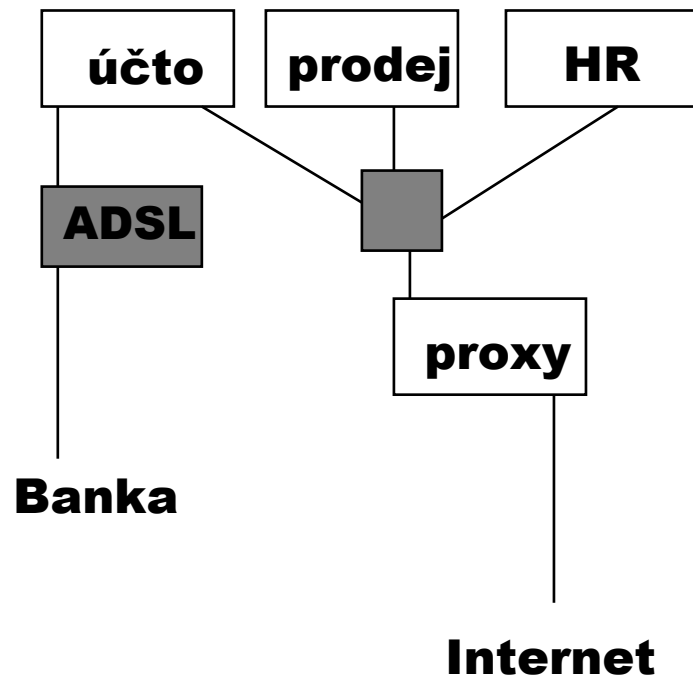
- Všichni (oba) mohou všechno.
- Antivirový software.

Antiviry

- Není jen prvotní nainstalování „krabice“.
- Dostupnost nových virových vzorků!
- „Otevřenost“ architektury – doplnění vlastních vzorků.
- Administrace systému.
- Podpora kontroly komprimovaných dat.
- Heuristické funkce.

...

DoTheThing!, s.r.o. roste...



Potřeby

- Interní síť s připojením na Internet.
- Stroj účto pouze pro účetní - autentizace heslem.
- Správce interní sítě – na částečný úvazek.

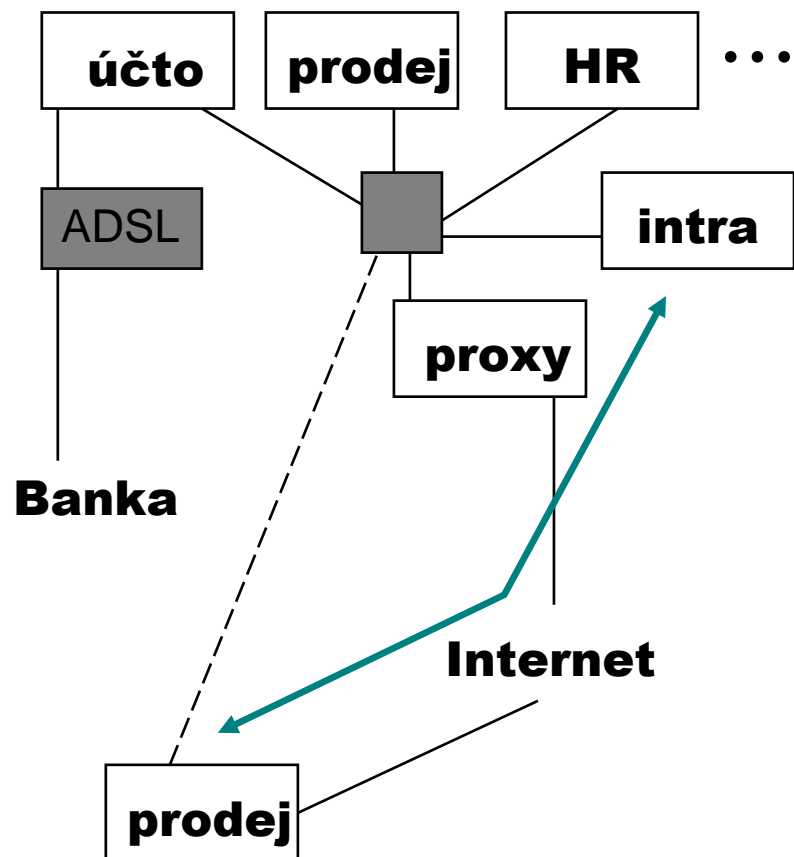
IT Security – rozhoduje správce

- Firewall pro bezpečné připojení do Internetu.
- Antivirový software pro další počítače.

Firewall

- Podpora protokolů HTTP, FTP, stahování a distribuce pošty z účtu u providera.
- Co není povoleno, je zakázáno!
- Administrace systému.
- Cache pro protokol HTTP.
- NAT funkce – možnost použití interních adres.

... a roste



Potřeby

- Interní databáze klientů.
- Možnost práce ve vnitřní síti vzdáleně (střídající se obchodní cestující).
- Zálohování dat.

IT Security – správce (a vývojář) na plný úvazek

- Autentizace pro vnitřní síť.
- VPN modul pro firewall.
- Autentizace na firewallu.

Autentizace na „vnitřních“ stanicích

- Spolehlivý autentizační systém.
- Autorizace na úrovni aplikace ve vnitřní síti.
- Heslo – paměť uživatelů – kdo bude administrovat?
- Čipové karty – zapomětlivost uživatelů a cena!
- Biometrický systém!

Řešení:

- Ověření otisku prstu.



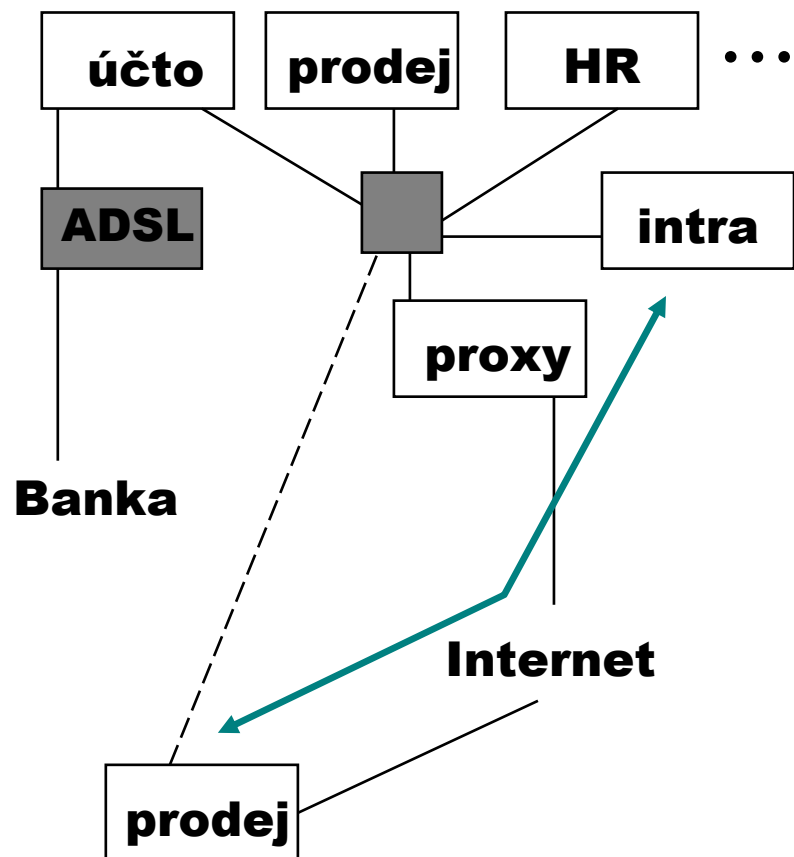
VPN modul pro firewall

- Při výběrovém řízení pro firewall jsme VPN modul nezvažovali.
- Výrobce nabízí „upgrade“ funkčnosti – cca 20 % nákladů navíc.
- Nutnost přečíslovat interní síť – možnost růstu na dalších pobočkách v rámci VPN.
- Autentizace bude na úrovni **sdíleného tajemství** – heslo pro přístup do interní sítě.

Možnost spojení s GetItThere, a.s.

- Spediční firma pro internetové obchody – synergie!
- Pro diskuzi podmínek možného spojení použijeme jednoduchou klientskou aplikaci:
 - Šifrování a digitální podpis
 - Výměna klíčů, dostatečná bezpečnost...
- Různé IT prostředky (O/S, IS, DB, FW, VPN...).
- Nezvážíme po spojení outsourcingování některých IT činností?

...databáze poškozena!!



Co víme?

- V době (odhad!) poškození databáze bylo na stroji intra přihlášeno 5 lidí.

Závěr:

- Černý Petr je někdo z nich!

Co teď?

- Poslední **použitelná** záloha databáze je stará 22 dnů!?
- Kdo měl přístup do interní sítě přes počítač „obchodního cestujícího“?
- Je to virus? Nebo Trojský kůň? Nebo útok?
- Je to první pokus o útok? Je to vůbec útok? Kdo sleduje logy firewallu? Proč se neloguje na počítači intra?
- Není Černý Petr administrátor?
- Není možné se přihlásit na účto přes modem?
- Co budeme dělat?

Zásadní chyby

- V systému zůstal princip „všichni směřjí všechno“ a „někdo se o to určitě stará“.
- Updaty & záplaty jednotlivých komponent nebyly vždy instalovány.
- Ačkoliv každá komponenta zvlášť byla pečlivě vybrána, systém jako celek neposkytuje očekávané zabezpečení.

Chyby technické

- Firewall neuměl VPN – nutno investovat více prostředků.
- Spolupráce antivirového SW s firewallem nevyřešena.
- Autentizace se provádí na každé komponentě zvlášť, nespolupracuje navzájem.
 - Heslo pro účto
 - Heslo pro interní síť – je společné? Je to „veřejné tajemství“
 - Biometrika jen na vnitřních stanicích

Nevěděli jsme co chceme – výsledný systém byl nekoncepční a obtížně rozšiřitelný.

Zásadní otázky

- Kdo zodpovídá za zálohování (a kontrolu médií)?
- Kdy jsme měli oddělit správu IT a bezpečnost?
- Není to útok s cílem snížit hodnotu firmy?
- Co řekneme GetItThere, a.s.?
- Co dříve – dokončit spojení nebo obnovit chod firmy?

Bezpečnost

1. Prevence.

2. Detekce.

3. Reakce.

Zásadní kroky

1. Analýza/odhad rizik.
2. Specifikace bezpečnostní politiky a architektury.
3. Popis bezpečnostních mechanismů.

Bezpečnostní politika

Celková bezpečnostní politika

- Cíle bezpečnostní politiky
- Bezpečnostní infrastruktura
- Identifikace kritických aktiv
- Identifikace hrozeb
- Výsledek analýzy rizik
- Postup dosažení bezpečnostních cílů
- Havarijní plán
- Časový rozvrh implementace

Systemová bezpečnostní politika

- Popis hrozeb
- Personální bezpečnost
- Bezpečnost prostředí – fyzická bezpečnost
- Bezpečnost komunikací a řízení provozu
- Systém řízení přístupu
- Vývoj a údržba systémů
- Havarijní plán
- Soulad s legislativou

IT rizika jsou rizika jako každá jiná

- Řešení IT rizik není jen o technologiích!
- Princip jednoznačné zodpovědnosti.
- Systematické uvažování.
- Obecná firemní kultura.
- Povědomí uživatelů.