Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Audit IT bezpečnosti na doméně a sítích

*Český institut interních auditorů, 30.11.2015*

1

IS VEŘEJ. SPRÁVY

## I. Ukázka požadavků na bezpečnost IT – vyhláška ČNB 163/2014 Sb., příloha 6

2. **Bezpečnostní zásady informačních systémů** obsahují
a) cíle bezpečnosti informačních systémů,
b) hlavní zásady a postupy pro zajištění **důvěrnosti, integrity a dostupnosti** informací,
c) odpovědnosti za ochranu aktiv a plnění bezpečnostních zásad informačních systémů.

5. V oblasti bezpečnosti přístupu k informacím banka nebo družstevní záložna zajistí
a) přidělení **přístupových práv** uživatelům v informačních systémech,
b) jednoznačnou **autentizaci** uživatele, která musí předcházet jeho činnostem v informačních systémech,
c) přístup k informacím v informačních systémech pouze uživateli, který byl pro tento přístup **autorizován**,
d) ochranu důvěrnosti a integrity autentizační informace,
e) **zaznamenávání událostí**, které ohrozily nebo narušily bezpečnost informačních systémů, do bezpečnostních auditních záznamů, ochranu těchto záznamů před neautorizovaným přístupem, zejména úpravou (modifikací) nebo zničením, a jejich archivaci,
f) **vyhodnocování bezpečnostních auditních záznamů** zaměstnancem, který nemá možnost upravovat (modifikovat) v informačních systémech informace související s činností, o které je bezpečnostní auditní záznam pořízen.

6. V oblasti **bezpečnosti komunikačních sítí** banka nebo družstevní záložna zabezpečí
a) připojení sítě, která je pod kontrolou banky nebo družstevní záložny, k vnější komunikační síti, která není pod kontrolou banky nebo družstevní záložny tak, **aby byla minimalizována možnost průniku** do jejích informačních systémů,
b) aby při přenosu důvěrných informací vnější komunikační sítí byla zajištěna
1. přiměřená důvěrnost a integrita informací,
2. spolehlivá autentizace komunikujících stran, včetně ochrany autentizačních informací.

2

VNITŘ – HOSTÉ / UŽIVAT. + VZDÁLENÉ PŘÍSTUPY MOB. TEL.

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Ukázka ČSN ISO/IEC 27001 – audit shody je snadný…

| | | |
|---|---|---|
| A.10.6 Správa sítě<br>Cíl: Zajistit ochranu informací v počítačových sítích a ochranu jejich infrastruktury. | | |
| A.10.6.1 | Síťová opatření | Opatření<br>Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících síť a pro zajištění bezpečnosti informací při přenosu musí být počítačové sítě vhodným způsobem spravovány a kontrolovány. |
| A.10.6.2 | Bezpečnost síťových služeb | Opatření<br>Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu. |
| A.11.4 Řízení přístupu k síti<br>Cíl: Předcházet neautorizovanému přístupu k síťovým službám. | | |
| A.11.4.1 | Politika užívání síťových služeb | Opatření<br>Uživatelé musí mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávnění. |
| A.11.4.2 | Autentizace uživatele externího připojení | Opatření<br>Přístup vzdálených uživatelů musí být autentizován. |
| A.11.4.3 | Identifikace zařízení v sítích | Opatření<br>Pro autentizaci připojení z vybraných lokalit a přenosných zařízení musí být zvýšeno použití automatické identifikace zařízení. |
| A.11.4.4 | Ochrana portů pro vzdálenou diagnostiku a konfiguraci | Opatření<br>Fyzický i logický přístup k diagnostickým a konfiguračním portům musí být bezpečně řízen. |
| A.11.4.5 | Princip oddělení v sítích | Opatření<br>Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích odděleny. |
| A.11.4.6 | Řízení síťových spojení | Opatření<br>U sdílených sítí, zejména těch, které přesahují hranice organizace, musí být omezeny možnosti připojení uživatelů. Omezení musí být v souladu s politikou řízení přístupu a s požadavky aplikací (viz 11.1). |
| A.11.4.7 | Řízení směrování sítě | Opatření<br>Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace musí být zavedeno řízení směrování sítě. |

3

# Využití COBIT

- Sofistikovaný přístup k hodnocení IT a její bezpečnosti
- Stanovují se:
  - Zralostní modely (maturity models), a to vždy podle současného a cílového stavu (scoring 0 – 5 bodů) ▶ **obdoba ANALÝZY RIZIK**
  - Kritické faktory úspěšnosti (CSF) – obsahují opatření, jak dosáhnout cílového stavu ▶ **obdoba POLITIKY a INT. NOREM**
  - Klíčové cílové ukazatele (KGI – vztaženo k cílům IT)
  - Klíčové výkonnostní ukazatele (KPI – vztaženo k bussiness cílům)
- Každá činnost se provádí pro pevně stanovených 34 bussiness procesů, začleněných do oblastí:
  - Plánování a organizace
  - Pořízení a implementace
  - Podpora
  - Monitoring
- (Uvedeno pouze jako příklad, že metodika analýzy rizik a stanovení politik může být založena na různých metodických základech…)

4

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Připravovaný zákon o kybernetické bezpečnosti (asi od 2015)

- Hlavní povinnosti:
  - hlášení bezpečnostních incidentů na NBÚ – viz § 9
  - dodržování protiopatření (reaktivní, ochranné) a reakce na varování vyhlášené NBÚ - viz § 13 - 16
  - poskytnutí kontaktních údajů
- Stanoven národní CERT (CZ.NIC ?) a vládní CERT (=NBÚ) – dohledová pracoviště *(Computer Emergency Response Team)*
- Sankce do 100.000,- Kč – viz § 29
- Týká se providerů, systémů kritické informační infrastruktury *(viz 204/2000 Sb. – Krizový zákon)*, významných systémů –viz §2 -3

5

## Externí odborníci IS/IT (typicky penetrační testy, jednorázová ověření nebo doporučení, ověření aplikací, vztah k roční závěrce aj. )

- **Výhody**
- Odborná fundovanost
- Obvykle dobrá znalost kontrolních / auditních postupů (není vždy)
- Bezkonkurenční orientace v bezpečnostní problematice, sítích, Internetu…
- Obvykle nezávislost na auditované organizaci
- Možnost srovnání s dalšími organizacemi

- **Nevýhody**
- Neznalost organizace
- Nevědí, co je pro organizaci významné a co podružné
- Obvykle ani nedostanou přístupy do vnitřní sítě (pak mohou auditovat jen zvenčí)
- Často snaha závěry formulovat tak, aby získali další kontrakty (podporují určité produkty, bližší rozbory slibují až na další zakázku aj.)

6

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Penetrační test

- Slouží k ověření zabezpečení proti průniku do sítě:
  - z vnějšího prostředí
  - z vnitřního prostředí (průnik na stanice, na servery, škodlivý kód v aplikacích apod.)
- Metodicky se provádí tak, že se napodobí co nejvěrněji dostupné praktiky hackerů
- Je nutně zaměřen hlavně do vstupních částí sítě (připojení k Internetu, hraniční router, firewall...) nebo se provádí bez práv nebo s velmi omezenými právy
- Není tedy sám o sobě zárukou, že celá síť je bezpečná (bývá tak ale často mylně interpretován)
- Důležité: Stanovit omezující podmínky! (jinak se sám penetrační test stává rizikem...)
  - **nedestruktivní**
  - **destruktivní**

7

## Vztah interního auditora k penetračním testům

- Penetrační testy jsou velmi závislé na znalostech nejnovějších a často velmi specializovaných postupů
- Interní auditor obvykle nemá ani potřebné znalosti, ani technické zázemí
- Nejčastěji provádějí specializované firmy
- IA může prověřit: smlouvu s takovou firmou
  - cena, výběr partnera
  - dodržení smlouvy (termíny provedení, dodržení zabezpečovacích prvků)
  - aby termíny testu nenarušily práci běžných uživatelů
  - rozsah dodatečných informací zadaných firmě
  - existenci a dostatečný rozsah omezení ve smlouvě
  - stanovení kontaktní osoby
  - existenci havarijního plánu pro případ zhroucení části sítě
- IA se samozřejmě následně
  musí zajímat o výsledky testu a odstranění nedostatků

8

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# II. Základní pojmy ze sítí

- **Počítačová síť** je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači. Umožňují tedy uživatelům komunikaci podle určitých pravidel, za účelem sdílení využívání společných zdrojů nebo výměny zpráv.
- Typy sítí
  - terminálová
  - serverová
  - peer - to – peer
  - kombinovaná

9

# LAN a WAN

- Z hlediska rozsahu můžeme sítě rozdělit na tři základní skupiny:
- LAN - Local Area Network, lokální sítě. Spojují uzly v rámci jedné budovy nebo několika blízkých budov, vzdálenosti stovky metrů až km (při použití optiky). Nejčastěji je dnes používána technologie Ethernet.
- MAN - Metropolitan Area Network, Metropolitní sítě. Propojují lokální sítě v městské zástavbě, slouží pro přenos dat, hlasu a obrazu. Spojuje vzdálenosti řádově jednotek až desítek km.
- WAN - Wide Area Network - rozsáhlé sítě. Spojují LAN a MAN sítě s působností po celé zemi nebo kontinentu, na libovolné vzdálenosti.

10

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

IPCONFIG /ALL

## Pasivní prvky sítí

- UZLY
  - Počítače, servery, tiskárny – vesměs obsahují síťovou kartu
    - MAC adresa – jedinečné číslo 12 znaků (prvních 6 znaků kód výrobce)
    - dělí se dle typu konektorů (BNC, UTP, combo) a dle rychlosti (10 Mbit/s, 100 Mbit/s až 10Gbit/s)
- KOMUNIKAČNÍ KANÁLY
  - Metalické popř. optické kabely
  - Vzdušné spoje (Wi-Fi, mikrovlné spoje...)

11

## Aktivní prvky sítí

- Umožňují větvení sítí
- HUB – nejjednodušší a nejlevnější (veškerá data, která přijdou na jeden z portů - zásuvek zkopíruje na všechny ostatní porty, bez ohledu na to kterému portu - počítači a IP adrese- data náleží. To má za následek, že všechny počítače v síti „vidí" všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena.)
- REPEATER – obdoba, ale signál zesiluje a jinak upravuje
- SWITCH - analyzuje procházející pakety a podle informací v nich obsažených (adres, identifikátorů apod.) rozhoduje, kam paket předat dál. Na 2. vrstvě (spojové), tj. pracuje podle MAC adres.
- ROUTER – spojuje obvykle aspoň dvě sítě. Pro správnou činnost používá routovací tabulku. Na 3. vrstvě (síťové), tj. pracuje podle IP adres..

12

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Protokoly

- **Protokol** je soubor syntaktických a sémantických pravidel určujících výměnu informace mezi nejméně dvěma entitami spojenými například prostřednictvím počítačové sítě.
- Zahrnuje
  - proceduru navázání spojení
  - adresování
  - přenos dat
  - zpracování chyb
  - řízení toku komunikace
  - přidělování prostředků
- Např. NetBEUI, IPX/SPX, X25, AppleTalk...

13

## Typy protokolů (model ISO / OSI)

- 7. aplikační vrstva – SMTP (simple mail transfer protocol) , FTP, SNMP (simple network management protocol) aj.
- 4. transportní vrstva – TCP (transmission control protocol), SPX, NetBEUI – tvorba paketů
- 3. síťová vrstva – IP (Internet protocol), IPX, NetBEUI – překlad na fyz. adresy, směrování...
- 2. spojová vrstva – starší aktivní prvky – bridge, repeatery...
- 1. fyzická vrstva – kabely, síťové karty

14

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# IP adresy

**IP ADRESA**

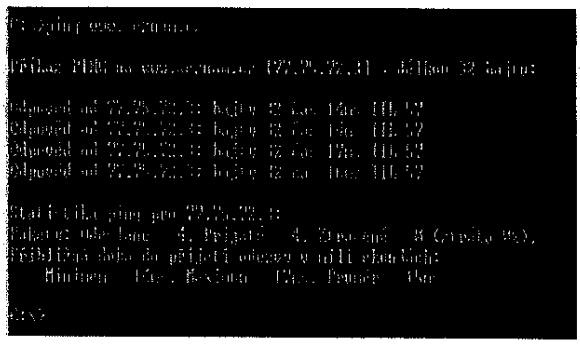
- **Třída A – 0.0.0.0 – 126.255.255.255 (jen 127obrovských sítí – v jedné ale může být až 16 mil. PC)**
- **Třída B – 128.0.0.0 – 191.255.255.255**
- **Třída C – 192.0.0.0 – 223.255.255.255 (první 3 čísla počet sítí – více než 2 mil., v každé ale jen 254 PC)**

- **Rezervované adresy:**
- Třída A 10.0.0.0 – 10.255.255.255
- Třída B 172.16.0.0 – 172.31.0.0
- Třída C 192.168.0.0 – 192.168.255.0
- Loopback adresa 127.0.0.1 – vlastní PC
- Broadcast adresa 255.255.255.255 (popř. 192.255.255.255 – jen do vnitřní sítě C)
- Subnet masky 255.0.0.0 A, 255.255.0.0 B, 255.255.255.0 C

15

# Použití příkazů z příkazové řádky

- PING – ke zjištění, zda nějaký prvek „vidíme“, vrací i základní informace o kvalitě spojení
- možný parametr např. –r 9 (počet zobrazených routerů)

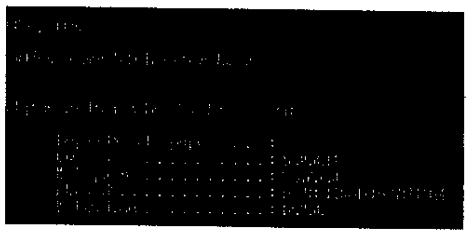


16

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## IPCONFIG

- Příkaz slouží ke zjištění informací o nastavení síťové karty počítače
- Nejčastěji se používá s parametrem IPCONFIG /ALL



17

## TRACERT a ARP

- Příkaz slouží k zobrazení trasy, kudy prochází spojení na cílovou stanici
- Typický tvar TRACERT www.ahoj.cz
- Někdy je blokován na aktivních prvcích

- ARP –a naopak zobrazí počítače, které komunikovaly s mou síťovou adresou („dívaly" se na ní)
- Protokol ARP řeší převod mezi MAC adresou a IP adresou

18

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Příkaz NET

- Rozsáhlá syntaxe

- Nejčastější: NET USER jméno
- NET GROUP jméno
- NET USE, NET SHARE
- NET VIEW (zobrazí připojené počítače)
- (Každá z nich se dá zobrazit nápovědou např. NET USER /?)

19

# III. Přístupová práva v doméně MS WINDOWS

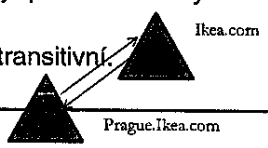
- **Doména**
- **Windows domény** jsou souborem objektů zabezpečení, které sdílejí centrální souborovou databázi. Tato centrální databáze je známá jako **Active Directory** a obsahuje uživatelské účty a informace o zabezpečení zdrojů v této oblasti. Každá osoba, která používá počítače v doméně, získá svůj vlastní účet nebo uživatelské jméno . Tomuto účtu je pak umožněn přístup ke zdrojům v rámci domény.
- V doméně se databáze Active Directory nachází na serverech, které jsou konfigurovány jako **řadič domény**. Řadič domény je server, který spravuje všechny bezpečnostní aspekty mezi uživatelem a doménou, centralizuje zabezpečení a správu.
- Windows domény jsou obecně vhodné pro organizace, kdy se využívá více jak 10 počítačů. Jde o skupinu počítačů, která sdílí společnou adresářovou strukturu.

20

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Strom (tree)

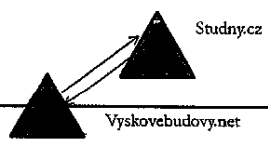
- Doménový strom se vyznačuje tím, že všechny jeho domény sdílejí souvislý obor názvů.
- Znamená to, že název domény v nejvyšší úrovni (tzv. *kořenové domény – např. Ikea.com*) se vyskytuje na konci názvu každé podřízené domény (např. *Prague.Ikea.com*).
- Mezi všemi doménami stromu Active Directory existují takzvané **vztahy důvěryhodnosti**. V praxi to znamená, že například uživatelé, kteří mají své účty v doméně *Ikea.com*, mohou získat prostřednictvím svého doménového účtu přístup ke sdílené složce v doméně *Prague.ikea.com*, samozřejmě za předpokladu, že jim jej správce domény *Prague.ikea.com* udělí.
- Vztahy jsou implicitně obousměrné a transitivní.




21

## Les (Forrest)

- Organizace, která má jednu nebo více domén (jeden strom), může například koupit jinou zavedenou společnost. Například řekněme, že organizace Studny, s.r.o. koupí společnost Výškové budovy, a.s.
- Pokud si obě domény si musí ponechat své názvy (důvodem takového rozhodnutí mohou být například požadavky používaných aplikací nebo zvyklosti uživatelů), již nelze zvažovat jako výslednou strukturu jediný strom Active Directory, ale stromy dva.
- Protože je však nutné tyto domény z pohledu jejich správy spojit, je řešením vytvořit dva stromy, oba v jediném lese Active Directory.
- I mezi dvěma doménami z různých stromů v rámci stejného lesa existují automaticky obousměrné a přenosné vztahy důvěryhodnosti.

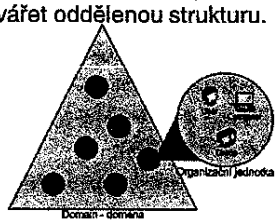



22

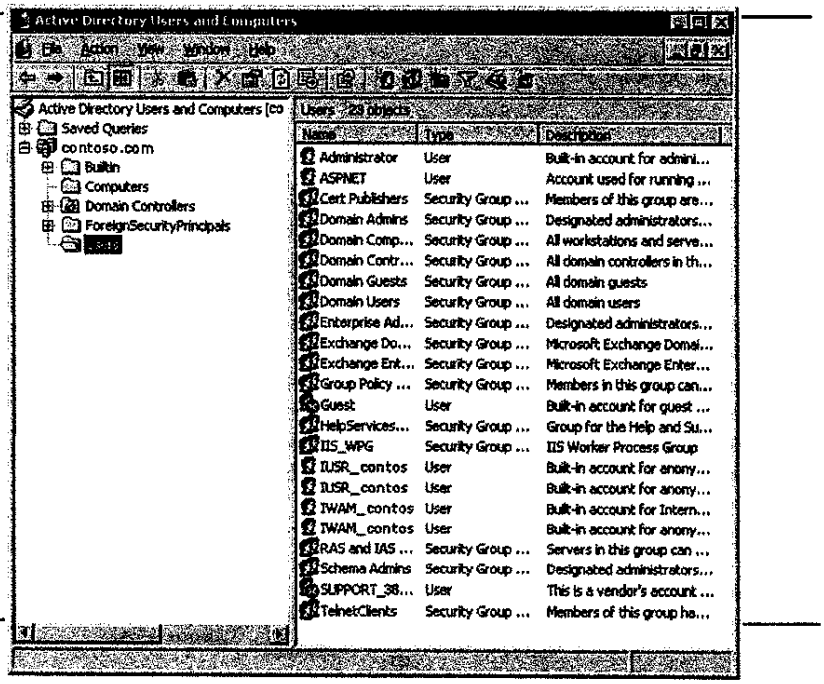
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Organizační jednotka

- ***OU (Organizational Unit)*** je ***kontejner***, který se uvnitř domény používá k seskupování/organizování objektů do logických administračních skupin. **OU** je nejmenší jednotka, na kterou můžeme delegovat *administrační oprávnění*. OU můžeme zanořovat do sebe a vytvářet libovolnou ***hierarchickou strukturu***. Hierarchie OU je lokální uvnitř domény a neovlivňuje jiné domény. OU se většinou vytváří tak, že odráží strukturu organizace (tedy třeba podle divizí a oddělení). Podle potřeby můžeme uživatelské a počítačové účty umísťovat do stejných OU či vytvářet oddělenou strukturu.

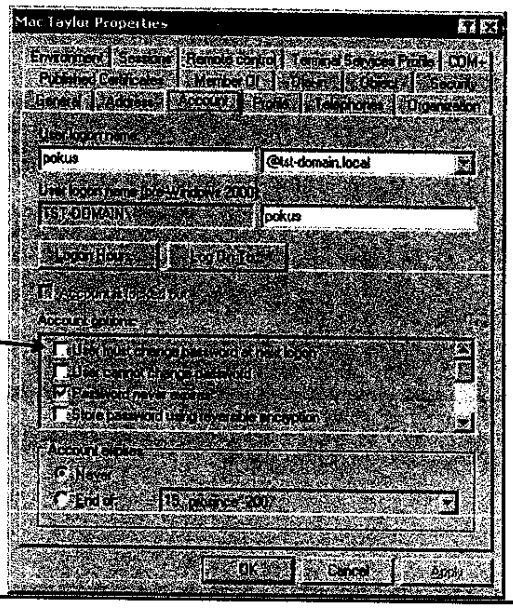



23



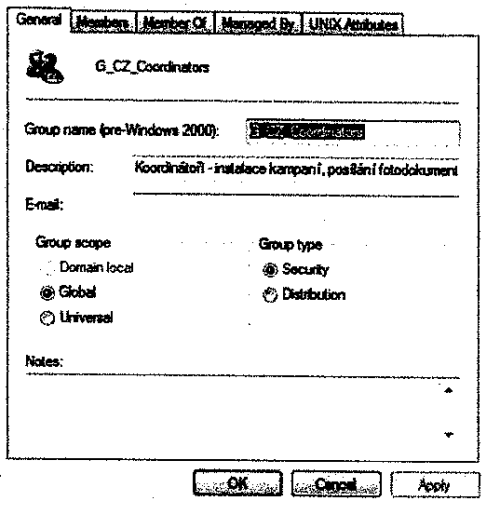
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Nastavení uživatele




Důležité

# Skupiny v Active Directory




26

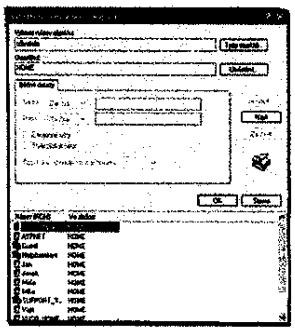
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Skupiny

- **Použití univerzálních skupin:**
- Skupiny mohou mít členy (uživatele nebo skupiny) z jakékoliv domény Windows 2000/2003/2008, doménového stromu nebo doménové struktury a mohou být použity pro přidělování přístupových práv v jakékoliv doménové struktuře. Univerzální skupina je replikována na všechny Global catalogy v úrovni doménového stromu.
- **Použití globálních skupin:** Skupiny s globálním rozsahem mohou mít členy (uživatele nebo skupiny) pouze z domény, v níž je skupina definována, avšak může být použita pro přidělení přístupových práv kdekoliv v rámci doménové struktury. (Globální skupiny jsou viditelné v celém lese.) Globální skupiny je vhodné používat jako kontejnery pro organizaci uživatelů a skupin.
- **Použití doménových lokální skupin:** tyto skupiny lze použít pouze pro přiřazení oprávnění v rámci domény, kde byly vytvořeny.
- Všechny tyto typy skupin mohou obsahovat všechny ostatní typy skupin i uživatelské účty ze všech domén v lese.
- **Lokální uživatelé / skupiny** – definováni na PC (nebo třeba serveru) – mohou se hlásit jen na jediné stanici

27

# Jak auditor získá údaje o právech



1) ACTIVE DIRECTORY

- U správce sítě

Její části lze pozorovat po zadání záložky „Zabezpečení". V tomto tvaru ale není příliš vhodná pro aut. zpracování.

28

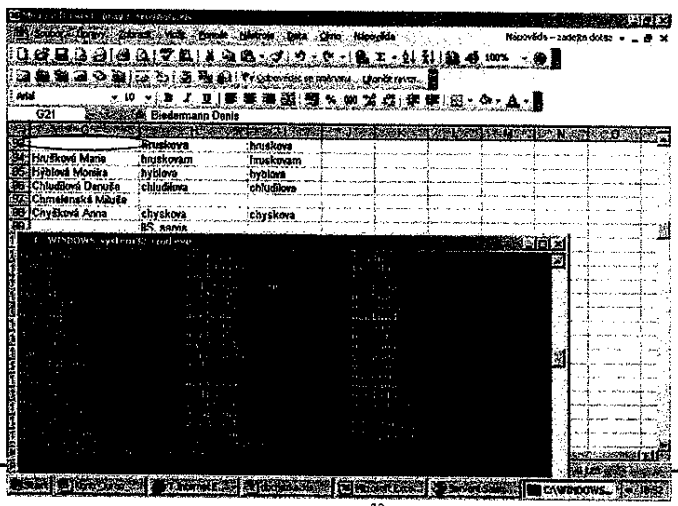
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Získání přehledu o uživatelích

- 2) Použitím příkazu NET z příkazové řádky.
- Postup:
- Spustit přes CMD nebo COMMAND příkaz. řádku (bývalý MS DOS)
- Zadat NET USERS /DOMAIN
- Popřípadě lze přímo zachytit do souboru, např. NET USERS /DOMAIN >c:\prava.txt
- Takový soubor se dá načíst např. do MS EXCELu

29

## Použití pro audit



30

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Přístupová práva k aplikacím

- Hlavní účetní systém
- El. pošta
- Internet
- Office
- atd.

- Ve všech případech stejný princip – získat seznam přístupů a srovnat se seznamem zaměstnanců, **nebo lépe i mezi sebou navzájem.**
- **Často lze přístupy k aplikacím získat z domény – např. příkazem**
  **NET USER xxx /DOMAIN**
  **V řadě případů nemusí být oprávnění na doméně totožné s oprávněním v rámci aplikace!**

31

# Přístupy do databází

Obvyklý problém:

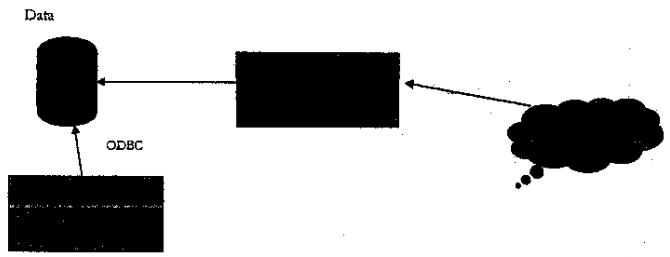
Práva na doméně zabrání ve spuštění aplikace

Práva na aplikaci třeba zabrání v zobrazení něčeho, uložení dat apod.

Ale teprve **práva na databázi** zabrání v prohlížení jinými kanály (typicky přes ODBC do ACCESSu apod.)

**Při auditu je nutno vždy ověřit, že je zabráněno v přístupu, který obchází práva na aplikaci!**

Rovněž různé reporty, tisky apod. často obcházejí uživatelská práva!




32

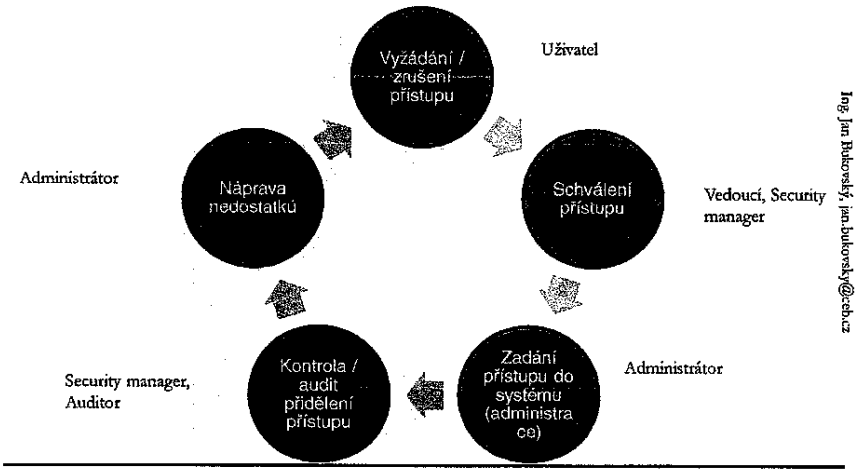
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Kdo smí přidělovat práva – bezpečnostní pravidla v organizaci

- Mělo by být vždy na základě požadavku vedoucího, nikoli podle libovůle informatiků
- Z bezpečnostního pohledu by po vedoucím měl ještě někdo ověřit (bezpečnostní specialista)
- Formální postup pro založení uživatele a změnu práv
- Délka a složitost hesla
- Systém hesel (jedno silné –SINGLE SIGN ON - nebo více)
- Komplexita hesla – nelze zadat „jednoduchá" hesla. Pod tímto pojmem se obvykle rozumí, že heslo musí obsahovat aspoň 1 malé, 1 velké písmeno, jednu číslici a jeden speciální znak (*+ apod.)
- Aplikace přístupné všem / aplikace přístupné na zvláštní povolení
- Doba povoleného přihlášení
- Doba do vypršení hesla
- Velikost schránky e-mailu a adresáře HOME
- Atd.

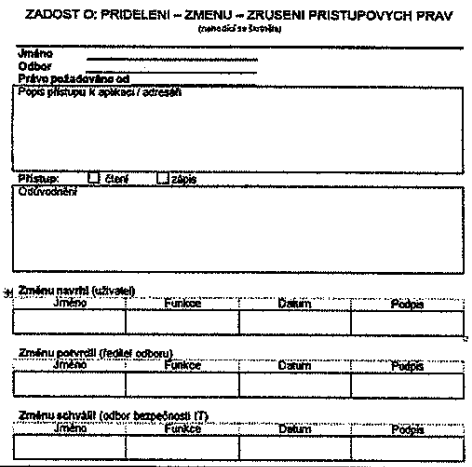
33

## Úkoly v řízení přístupu



Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Formální postup přidělení práv



ZADOST O: PRIDELENI – ZMENU – ZRUSENI PRISTUPOVYCH PRAV

Jméno
Odbor
Právo požadováno od
Popis přístupu k aplikaci / adresáři
Přístup: ☐ čtení ☐ zápis
Ospravedlnění

Změnu navrhl (uživatel)

| Jméno | Funkce | Datum | Podpis |
|---|---|---|---|
| | | | |

Změnu potvrdil (ředitel odboru)

| Jméno | Funkce | Datum | Podpis |
|---|---|---|---|
| | | | |

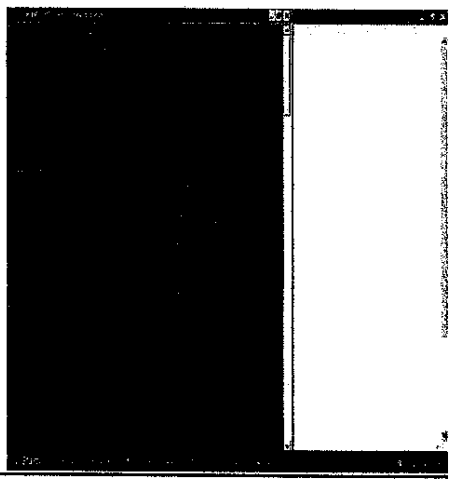
Změnu schválil (odbor bezpečnosti IT)

| Jméno | Funkce | Datum | Podpis |
|---|---|---|---|
| | | | |



# Další přihlašovací údaje

- Velmi dobře patrné z NET USER jm_už / DOMAIN:
  - **Zda je účet aktivní**
  - **Zda nevypršel**
  - **Poslední změna hesla**
  - **Přihlašovací hodiny**
  - **Členství ve skupinách**
  - **Atd.**

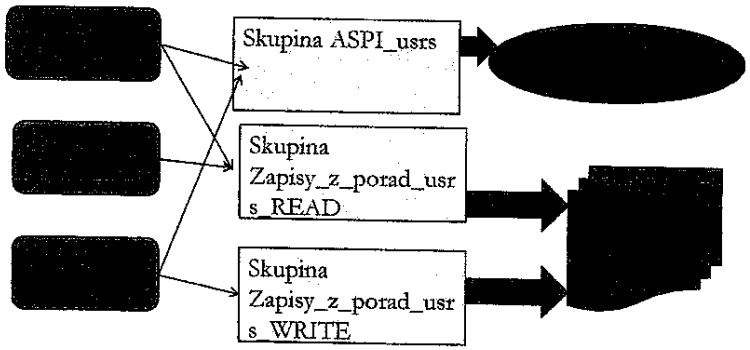


36

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Uživatelé x skupiny

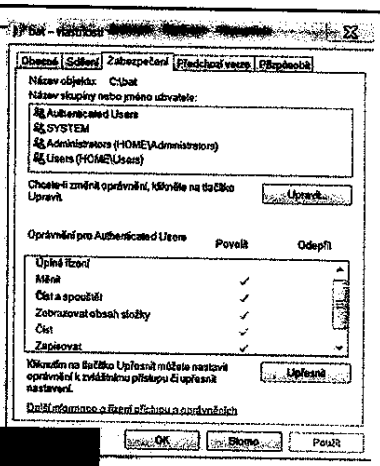
- Správný postup: práva k objektům se přiřazují skupinám, ne přímo jednotlivým uživatelům!

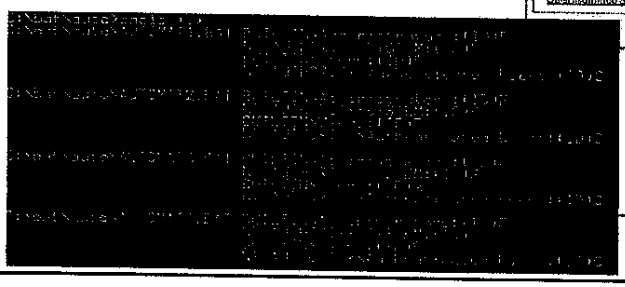



37

## Přístupová práva k souborům a adresářům

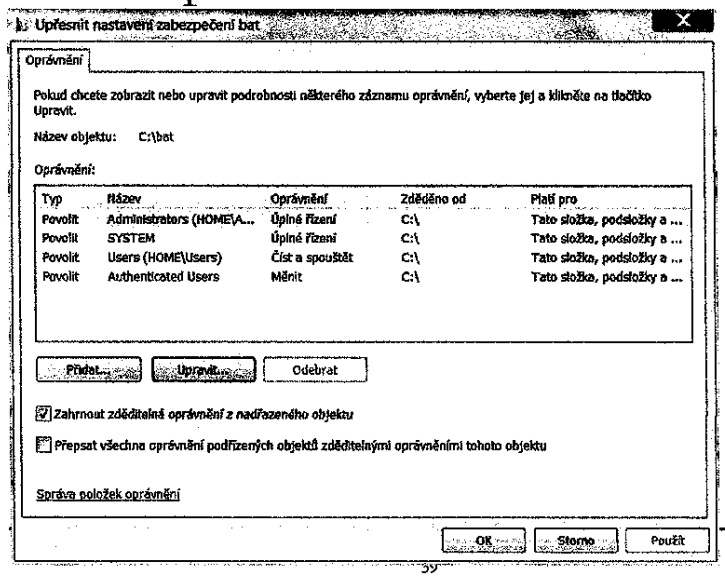
**CACLS C:\BAT*.***
F full, R read, W write
ID zděděno, CI práva budou dědit podřízené adresáře, OI práva budou dědit podřízené soubory



Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Dědění práv




39

# Audit skupin (groups)

- Identifikovat všechny (globální i lokální) skupiny a zdokumentovat příčinu jejich vzniku
- Zhodnotit důvody existence skupin (business reason)
- Prověřit adekvátnost oprávnění přiděleným skupinám
- Prověřit oprávněnost zařazení všech uživatelů ve skupinách (dle důležitosti skupin- Domain admins, Backup Operators ...)
- Prověřit logické chyby – skupiny ve skupinách, neoprávněné dědění, „neviditelné“ složky (chyba List), na které práva jsou

40

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Seznam skupin a jejich předpokládaného naplnění

| Skupina | Popis skupiny | Přístupy přidělené skupině | Předpokládání uživatelé | Skutečnost / Rozdíl |
|---|---|---|---|---|
| US-IK | Mapování Q:\ | Aplikace Skladové hospodářství | Účtárna | 2 pracovníci účtárny a V. Roth na základě sdělení odboru 5000 z 28.4.2011, OK. |
| US-ALIT_R | Komise ALIT | Adresář J:\ALIT čtení | Členové ALIT, audit, dle požadavku předsedy ALIT z 8.3.2010 též dealing | Navíc mají přístup Škoda (už není členem komise) a Javorský. |
| US-ALIT_RW | Komise ALIT | Adresář J:\ALIT zápis | Předseda a tajemník komise | Odpovídá |
| US-Audit | Audit - sledování plnění nápravných opatření | Adresář J:\AUDIT a aplikace IS_AUDIT | Členové PR, NGR, RO | Odpovídá.<br>RO 1100 Ing. Adam práva nemá přidělena (nemůže reagovat na zjištění auditu). |

41

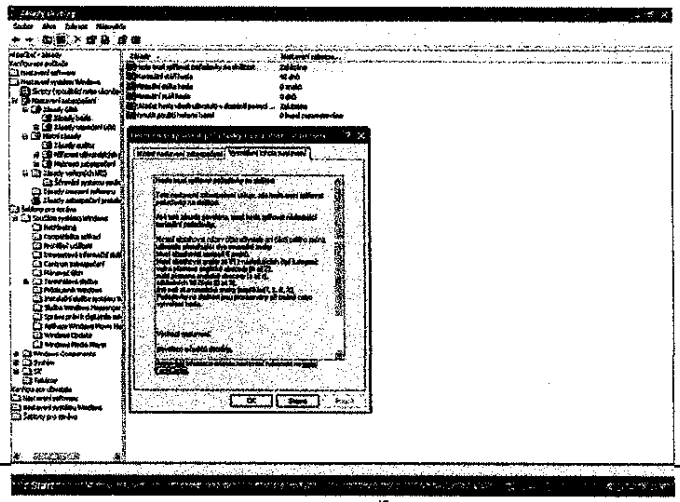
# Politika hesel

- Je politika vyžadována na všech doménách /objektech?
- **Nastavení:**
- - max. stáří: menší než 30 (60) dní
- - min. stáří: různé od 0
  - min. délka: 8
  - unikátnost: 6 (posledních hesel nelze použít)
  - uzamčení: 3 (5) špatných pokusů
    nulování počítadla 1440 min (1 den)
  - odblokování: Admin
  - prac. doba: Ano/Ne ( v závislosti na povaze práce uživatelů)
  - logon-změna: Ano (uživatel musí měnit heslo po prvním přihlášení)
  - komplexita (A-Z, a-z, 0-9 a příp. ještě i speciální znaky +*,$ apod.)
- přednastavitelné účty jsou zablokovány (Guest, Administrator) respektive admin je přejmenován
- ověřit, zda-li každý administrátor má své vlastní heslo a zda-li jsou administrátorská hesla silná

42

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Nastavení komplexity hesla



43

## Politiky vs. Přístupová práva

- Přístupová práva
- Mohou zabránit nalezení, spuštění, změně atd. souborů, a to na síti i na stanici
- R čtení, W zápis, X spouštění, C vytvoření, D smazání, M změna…

- Politika
- Ovlivňuje chování počítače, typicky:
- Vzhled Windows
- Přístup ke konfiguračním aplikacím (CONTROL PANEL, registr, tiskárny…)
- Možnost instalovat programy
- Vlastnosti sítě a připojení
- Přístup k HW (např. mechaniky)

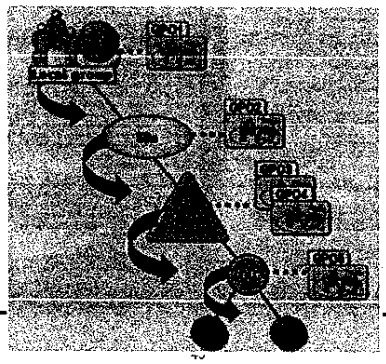
44

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Aplikování skupin zásad

Aplikování politik jde z úrovně 1 na úroveň 5, tedy pokud na úrovni 1 máme nastaveno např. PROXY Enable a na úrovni 4 je PROXY Disable, vyhraje úroveň 4 a proxy v počítači zůstává ve stavu Disable

1. Lokální politiky "Local Group Policy"
2. Politiky na úrovni sítí "Site Level GPOs"
3. Politiky na úrovni domény "Domain level GPOs"
4. Politiky na úrovni organizačních jednotek "Organizational Unit GPOs"
5. Politiky na úrovni podskupin organizačních jednotek "Any child Organizational Unit GPOs"



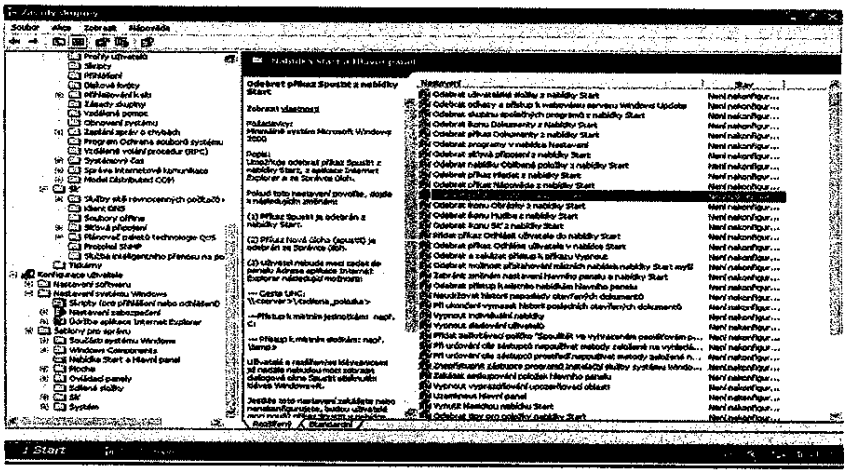
# Rozdělení GPO (na 2 části a každá z nich na 3 další sekce)

| Group Policy area | Description |
|---|---|
| Computer configuration | mění registry v: **HKEY_Local_Machine** |
| User configuration | mění registry v: **HKEY_Current_User** |

| Section | Description |
|---|---|
| Software settings | Instalace, spuštění a nastavení softwaru. Pokud je definován v části konfigurace počítače, bude spuštěn ještě před přihlášením, pokud je definován v části konfigurace uživatele, bude spuštěn až po přihlášení konkrétního uživatele |
| Windows settings | Obsahují skripty (při přihlášení, při odhlášení) a nastavení zabezpečení pro uživatele i počítače a Internet Exploreru |
| Administrative templates | Obsahují stovky nastavení registru pro ovládání různých aspektů uživatele nebo počítačového prostředí |

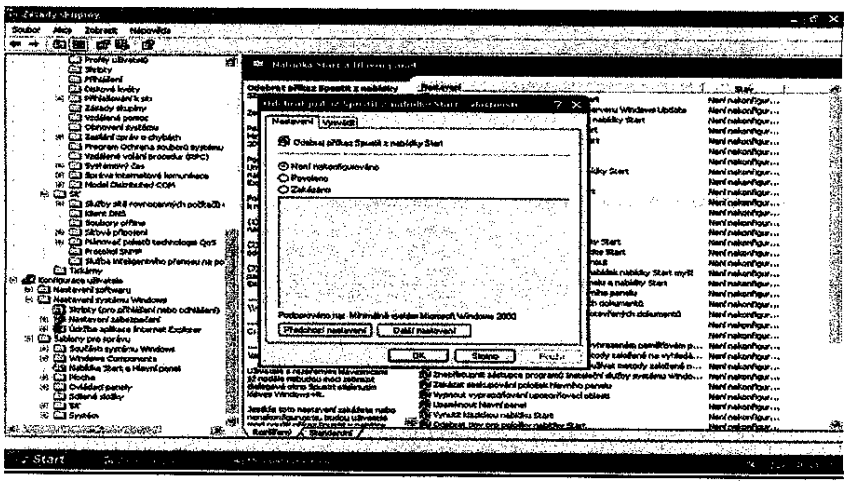
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Politika – přes GPEDIT.MSC



47

# Politika - změna



48

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Čemu by měly politiky bránit - příklady

| Činnost | Group policy | Registr |
|---|---|---|
| Zákaz spouštění jednotlivých částí CONTROL PANELu (Systém, Přidat/upravit programy, Síť...) | Skrýt určené panely v Ovládacích panelech (SYSDM.CPL, NETSETUP.CPL), Odebrat položku Přidat nebo odebrat programy | HKCU/ControlPanel/Don´tLoad/SYSDM.CPL + APPWIZ.CPL + NETSETUP.CPL... |
| Zákaz vypalování CD | Odebrat funkci zápisu na disk CD | HKCU/SW/MS/WIN/CURRENT/POLICIES/EXPLORER/NoCDBurning=1 |
| Zákaz spouštění příkazového řádku MS DOS | Zakázat příkaz k příkazovému řádku | .../POLICIES/WINOLDAPP/DISABLE=1 |
| Zákaz sdílení souborů a složek | Odebrat složku Sdílené dokumenty ze složky Tento počítač | .../POLICIES/NoFileSharing=1 |
| Odstranění nabídky SPUSTIT z Nabídky Start | Odebrat příkaz Spustit z nabídky Start | ../POLICIES/NoRun=1 |

49

## Čemu by měly politiky bránit – příklady II.

| Činnost | Group policy | Registr |
|---|---|---|
| V nabídce Exploreru a Tohoto počítače nebudou vidět žádné disky (popř. jen některé) | Skrýt tyto jednotky v okně Tento počítač | ../POLICIES/NoDrives=3FFFFFF |
| Nezobrazí se nabídka „Okolní počítače" | Zakázat ikonu Celá síť ve složce Místa v síti | ../POLICIES/NoNethood=1 |
| Zákaz spuštění nebezpečných / správcovských aplikací | Zakázat přístup k nástrojům pro úpravu registru, Zakázat příkaz k příkazovému řádku, Path Rules...Disallowed | ../POLICIES/EXPLORER/DisallowRun\Regedt32.exe + Command.com+Compmgmt.msc+Gpedit.msc+CACLS... |
| Brání ve spuštění Hledání | Odebrat příkaz Hledat z nabídky Start | ../POLICIES//NoFind=1 |
| Na plochu ani do Nabídky start se nenahrají žádné změny učiněné uživatelem | Zabránit změnám nastavení hlavního panelu a nabídky Start | ../POLICIES/EXPLORER/NoSaveSettings=1 |

50

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Audit z prostředí Internetu

- Značně specializované postupy (v podstatě postup podle hackerů)
- Princip:
- 1) zjistit dostupné informace o síti z databází Internetu
- 2) pokusit se na získané adrese scanovat okolní rozsah adres a použitelné porty
- 3) pokusit se najít nedostatky na nalezených adresách (náchylnost na speciální pakety, zjištění technologie a jejích známých slabin...)
- 4) případně převzít v důsledku těchto slabin kontrolu nad sítí, zjistit hesla, povýšit si práva, měnit obsahy adresářů neboWWW serveru (tato fáze prověrky musí být pouze naznačena a sledována vlatním útvarem IT / bezpečnostním a síťovým odborníkem)

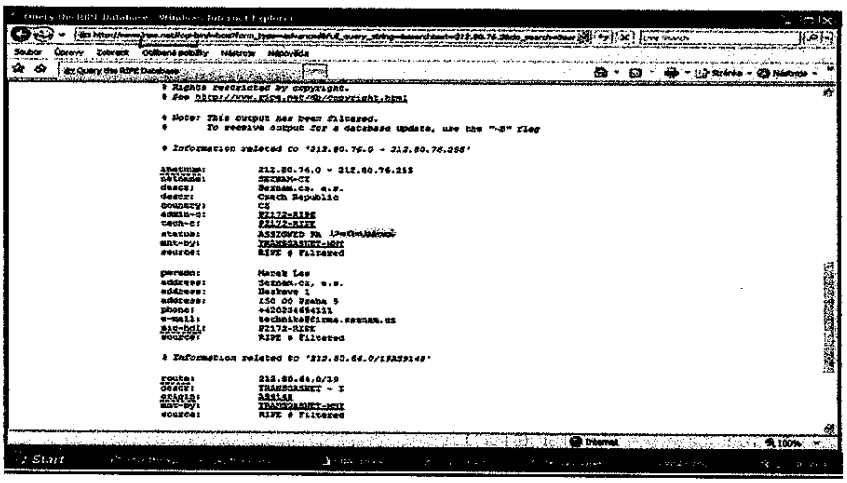
55

# Co je vidět na veřejně dostupných zdrojích na Internetu? Obvykle předem nutný překlad IP adresy – PING, TRACERT...

W: RIPE.NET

TRUSTEDSOURCE.ORG

ARCHIVE.ORG



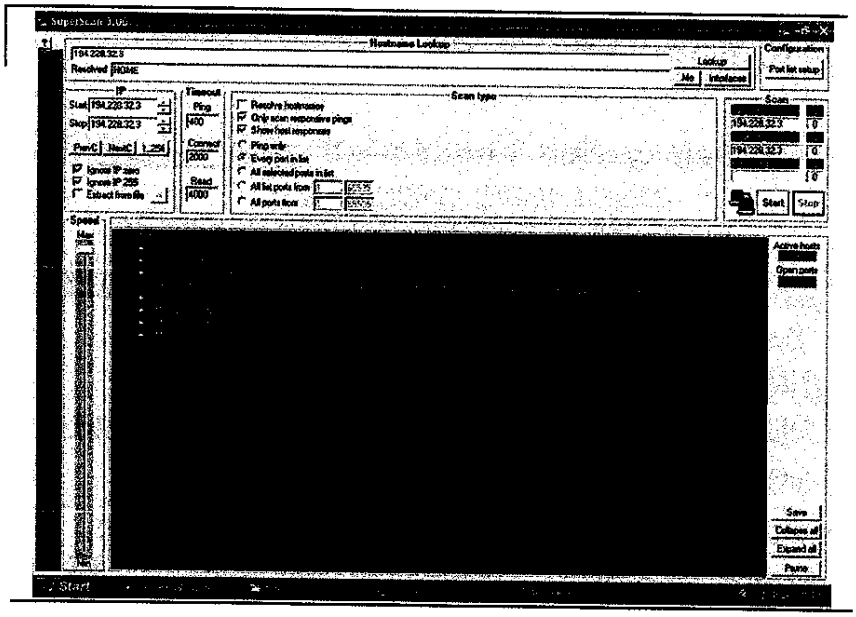
56

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Scanování z prostředí internetu / z vnitřní sítě

- V podstatě totožný princip – zjistit dostupné servery / počítače, otevřené porty, verze HW / SW, běžící procesy ...
- Nejjednodušší – základní myšlenka– provádění příkazů PING na sousední adresy
- Pro porty nutno použít speciální nástroje převzaté z UNIXu (NMAP, NETCAT ...)
  tak třeba Nc –v –z –w2 212.80.76.3 1-140 scanuje porty 1 až 140
- Existuje řada nástrojů i v grafickém rozhraní

57



58

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Porty

- Vstupně-výstupní (LPT, COM..)
- Jiné fyzické porty (třeba USB, na hubech apod.)
- Transportní – náš případ. Nejsou to fyzické porty. TCP/IP protokol je schopen obsluhovat více procesů najednou – všem takovým procesům byly definovány „porty". Každý proces má jediný port. Tak např.:
- Teoreticky použitelných portů je 2*65305

| Proces | port |
|---|---|
| HTTP | 80 |
| FTP | 21 |
| Telnet | 23 |
| SMTP | 25 |
| NetBios | 139 |
| HTTPS(SSL) | 443 |
| Backorifice | 31337 |

59

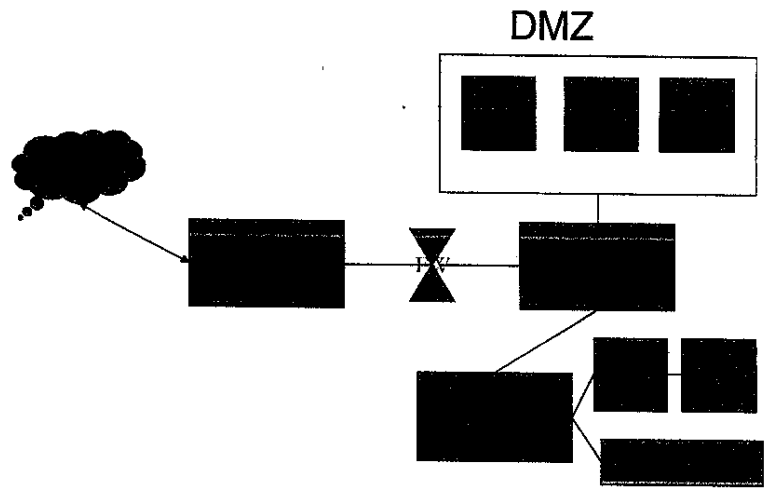
## Topologie sítě

- Popisuje spojení jednotlivých síťových prvků
  - Aktivních (routery, switche apod.)
  - Pasivních (síťové karty ve stanicích a serverech)
- Pro audit je významná otázka, na které prvky je možné „vidět" a odkud (a zda na ně opravdu musí/ má být vidět).
- Obvykle je poprvé potřeba získat informace od síťového specialisty IT.
- Jeho odpovědi pak lze doplnit trasováním (např. příkazem TRACERT 192.168.110.100)

60

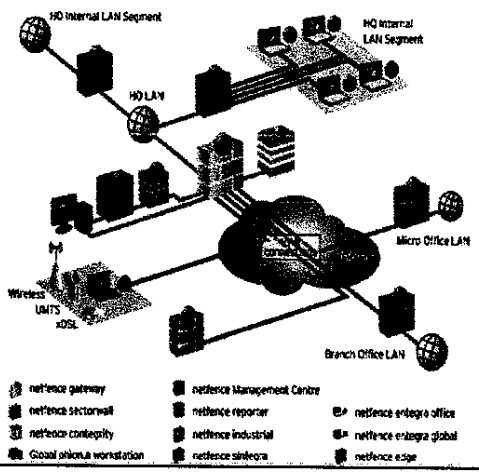
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Topologie - příklad




61

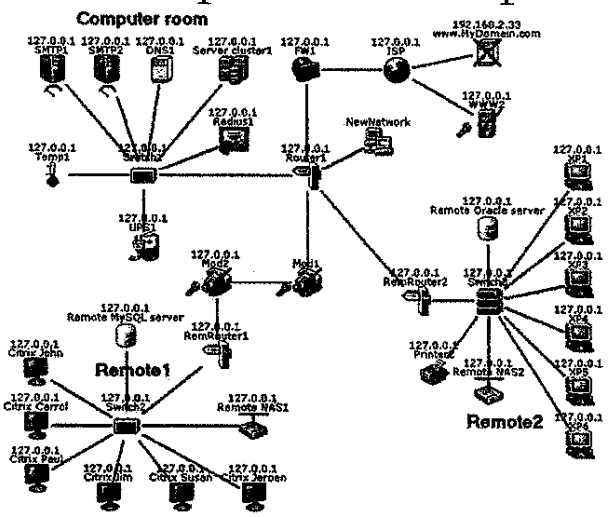
## Obvykle je to ještě o dost složitější...




62

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Úvodní představa o uspořádání sítě




**Použitelné příkazy např.:**
NET VIEW – ukáže seznam dostupných zařízení

NET VIEW SMTP1 – ukáže případné sdílené adresáře na serveru (třeba na file serveru)

NSLOOKUP SMTP1 – ukáže IP adresu serveru nebo akt. prvku

63

# Ukázka ACL – access control listu

- access-list 100 permit tcp any gt 1023 host 192.168.122.100 eq 3389
- access-list 100 permit tcp any gt 1023 host 192.168.102.71 eq 3389
- access-list 100 permit tcp any gt 1023 host 192.168.102.72 eq 3389
- access-list 100 permit icmp host 192.168.102.80 any
- access-list 100 permit icmp any host 192.168.102.80
- access-list 100 permit ip any 192.168.102.0 0.0.0.255
- access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.102.0 0.0.0.255
- access-list 100 permit tcp any gt 1023 host 192.168.122.100 eq 139
- access-list 100 permit tcp any eq 445 host 192.168.122.100 gt 1023 established
- access-list 100 permit tcp any eq 445 host 192.168.102.71 gt 1023 established
- access-list 100 permit ip any host 192.168.122.100 log
- **access-list 100 deny ip any any log**

64

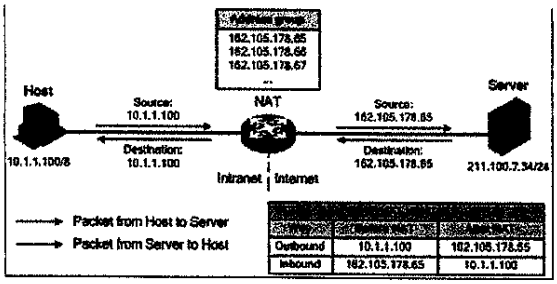
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Demilitarizovaná zóna

- Některé servery v podstatě musí být „vidět" z Internetu (vlastní WWW stránka, mail server...)
- Myšlenka: oddělit je od zbytku sítě tak, aby i při jejich znalosti nemohl hacker získat informace o topologii sítě
- Servery v demilitarizované zóně nemají povolený přístup do lokální sítě. V případě, že dojde k jejich napadení, útočník nebude moci napadnout servery v lokální síti.
- Do DMZ obvykle nelze přistoupit z „běžné" sítě - zkontrolovat! (může ale být povolen přístup pro speciální aplikace nebo jen z vyhrazené adresy nebo sítě pro správu)
- Kontrola v DMZ není obvykle možná bez spolupráce IT specialisty

65

# NAT




- **Native Address Translation** (*nativní překlad adres*) nebo **IP Masquerading** (*IP Maškaráda*) je způsob úpravy síťového provozu přes router přepisem výchozí nebo cílové IP adresy, často i změnu čísla TCP/UDP portu u průchozích IP paketů. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou.

66

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Firewally a proxy

- **Firewall** je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla vždy zahrnují identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port. Modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS.

Firewally se řadí do následujících kategorií:

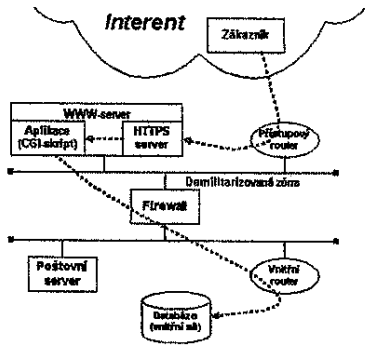
- Paketové filtry
- Aplikační brány (=proxy firewally)
- Stavové paketové filtry (pamatuje si též již povolené pakety a podle toho rozhoduje o nových)
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS

**Proxy server** funguje jako prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Přijatou odpověď následně odesílá zpět na klienta. Proxy server odděluje lokální počítačovou síť (intranet) od Internetu. Dochází k úplnému oddělení sítí.

67

# Použití DMZ např. pro el. bankovnictví

- Problém spočívá v tom, že data jsou umístěna ve vnitřní síti za firewallem. Přitom WWW-server musí být umístěn před firewallem, tj. musí být dostupný z Internetu.
- Aby byl možný z WWW-serveru přístup na data ve vnitřní síti, tak musí být umístěn v demilitarizované zóně, která je chráněna např. filtrací na přístupovém routeru do Internetu. Firewall je nastaven jako filter nebo proxy pro komunikaci mezi WWW-serverem a databází ve vnitřní síti. Pro filtraci je nutné nastavit jen minimální možnost průchodu firewallem tak, aby komunikace ještě byla možná.




68

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Serverová část sítě

- Vedle souborových a aplikačních serverů bývá většinou obsažen:
- PROXY server (Klienti nemusí mít přiřazeny veřejné IP adresy a přesto mohou mít přes proxy server přístup ke službám na internetu.)
- DNS server (překlad jmen Internetových adres)
- DHCP server (přidělování adres stanicím)
- WWW server
- Databázové servery
- Exchange server (elektronická pošta)

69

## Service packy a patche

- Slouží k udržování systému v bezpečném stavu – opravují nedostatky (bezpečnostní nebo funkční) zjištěné v nedávném období
- Nenasazení patchů: obvykle bezpečnostní riziko
- Hrozí DOS útoky, prolomení ochran, viry
- Nasazení patchů: někdy může způsobit chyby ve funkčnosti systému
- Řídí se pomocí tzv. PATCH MANAGEMENTu

70

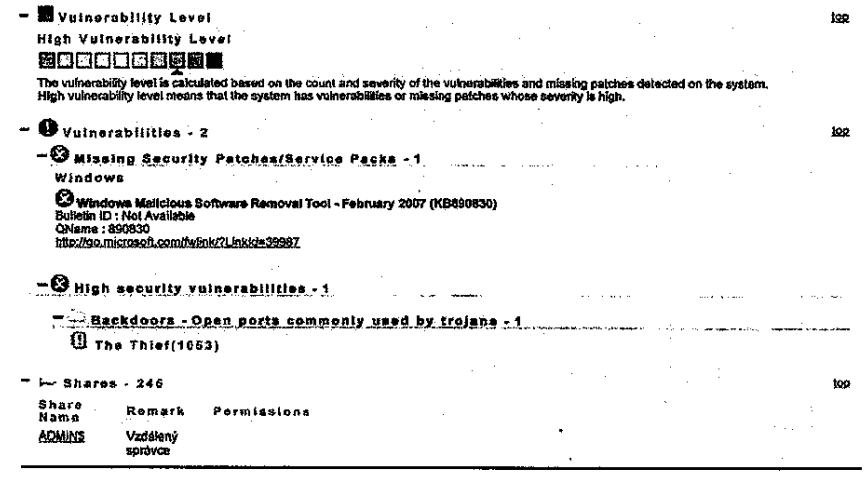
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Security (vulnerability) scannery

- Automatizují dříve popsané postupy
- Obvykle nutné administrátorské oprávnění (někdy stačí lokální – ke stanici a je možné scanovat celou síť)
- Provádí zejména:
  - **Hledání právě aktivních prvků**
  - **Údaje z NetBIOSu (tj. NET VIEW)**
  - **Hledání otevřených portů**
  - **Porovnání nainstalovaných patchů s aktuálním stavem dle výrobce**
  - **Hledání prázdných hesel**
  - **Hledání lokálních uživatelů a běžících procesů**
  - **Atd.**

71

# Vulnerability scaner - ukázka




72

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Internet a mail

- Obecně je vhodné ztěžovat uživatelům přístup na některé stránky (sex, MP3, stahování programů, rádio / televize)
- E-mailový server by měl bránit v přístupu spamu
- **Důvody: hlavně kapacitní** + snaha zaměstnavatele po přiměřeném využití pracovní doby
- Nejsnazší audit: zkouškou takových aktivit
  - zkusit přístup na několik stránek (třeba s pop-up okny, active X...)
  - zkusit poslat zprávu se „spamovým" názvem (Viagra,Cialis...)
  - zkusit poslat extrémně dlouhou zprávu
  - zkusit poslat zprávu obsahující .EXE soubor, přejmenovaný .EXE apod.
- *Závěr: ...bylo ověřeno, že nastavení aktivních prvků nebrání v dostatečné míře přístupu k nevhodným stránkám (z 10 zkoušených přístupů prošlo 8, konkrétně ...)...*
- Další možnost: získat přístup k aplikaci monitorující přístup do Internetu (pokud existuje – může být např. součástí firewallu)
- Jiná možnost: získat nastavení firewallu, proxy serveru, routovací tabulky aj. – poměrně komplikované

73

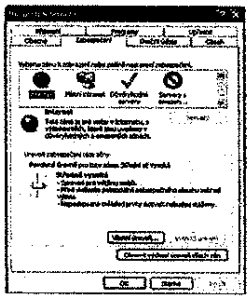
## Napadnutí e-mailů a klienta Internetu

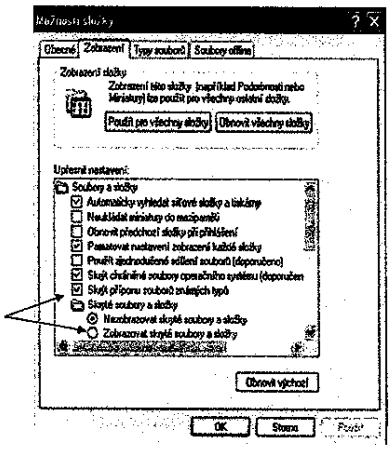
| |
|---|
| Spuštění instalace nebo nepřátelského kódu přes ACTIVE X |
| Spouštění kódu, DIR, sdílení, editace registru aj. přes BACK ORIFICE (v podstatě dálkové ovládání stanice vč. zásahů do registrů, restartů apod.) |
| COOKIES – obsahují i citlivá data |
| Možnost použití skrytých přípon, kterými systém automaticky provádí (spouští) programy<br>(Soubor vypadá jako normální) |
| Pozor na zfalšování emailu pomocí Telnet<br>Helo localhost<br>Mail from: <somebody@domain.net><br>Rcpt to: <lama@domain.net><br>Data<br>Subject: Read this! |

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Napadnutí e-mailů a klienta Internetu - obrana

- Dále se doporučuje zakázat „Skriptovat ovládací prvky ActiveX označené jako bezpečné“





75

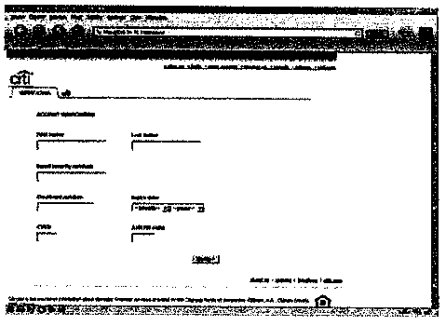
## Nastavení el. pošty a Internetu na serveru - princip

- BLACK LISTY – zakázané stránky, e-mailové adresy, přípony, názvy zpráv (spam)
- WHITE LISTY
- GRAY LISTY (tvoří se třeba automaticky na základě bodování zpráv – pozor na češtinu!)
- Zakázané přílohy - zejména vše spustitelné (.EXE, .COM, .BAT, .CMD, .VBS, .JS...)
  Sporné jsou zazipované přílohy nebo soubory opatřené heslem...
- Problém důvěrnosti pošty vers. zálohování
- U Internetu např. porno, stahování spustitelných souborů, hudby, rasový obsah aj.

76

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Ukázka phishingu

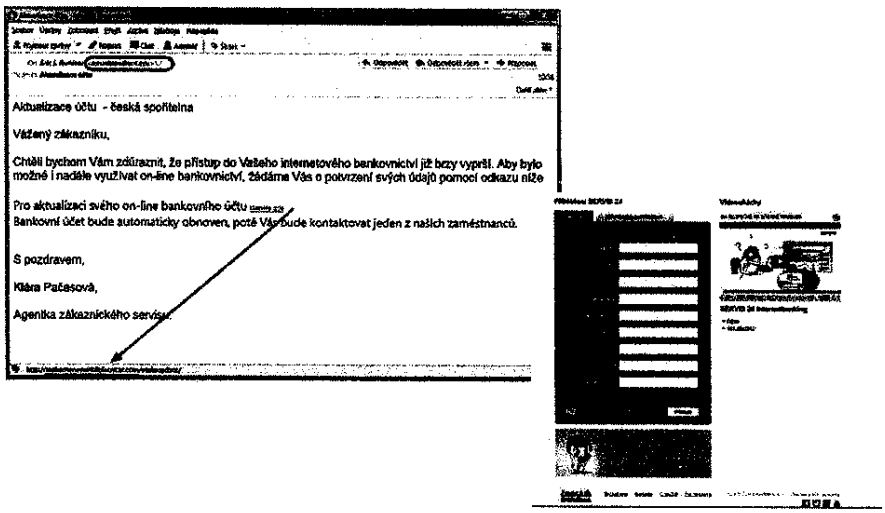


**Skutečná adresa ale byla:**
**http://218.36.71.193/secure/**

- Valued Citibank client
  In our bank we value our clients and money, thats why we have to upgrade our database. The upgrade requires our costumers to update their debit/credit card information to avoid problems in our ATM services.
  The reson to this upgrade is that we want to be well prepared for the smartcard upgrade on VISA creditcards. The smarcards reads a different type of encryption from our databases wich is more secure than the old type.
  Please update your debit/credit card information as soon as possible.
  Click on this link to verify:
  **http://www.securityupdate.citibank.com/secure/**

81

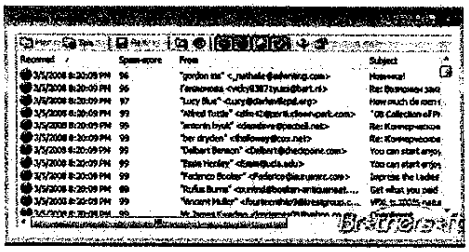
# Ukázka phishingu




82

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Možnost auditu e- mailu: na antispamovém řešení v organizaci



Problém: Má mít interní audit přístup k mailům všech osob v organizaci, i třeba jen dočasný?

83

## Škodlivé kódy

- Viry (např. backdoor, keylogger, bot...)
- Červi (šíří se jako příloha e-mailu)
- Trojské koně (maskovány jako užitečný SW)
- Phishing
- Adware - Spyware – hlavním cílem podsunutí reklamy, získání dat o chování uživatele ... nejde o viry!
- Rootkity (na úrovni kernelu, skrývá se)
- Obvyklý problém: antivirové programy spyware moc nebrání.
- Antiviry musí prohlížet i e-maily (opět: nezvládají spam).
- Antivir musí mít zajištěnu pravidelnou aktualizaci virových definic (ideálně i několikrát denně)

84

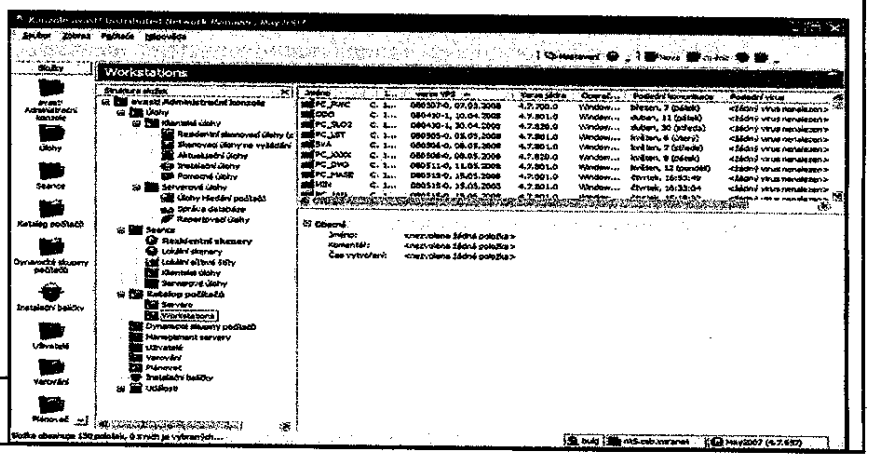
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Aktualizace antiviru

- Měla by být zajištěna automatická aktualizace virových definic hned, jak je zveřejněna na Internetu (nebo poloautomaticky: oznámení změny WWW stránky přes SMS apod.)
- Je nutno zabezpečit rozehrání nových definic na stanice, servery a na EXCHANGE server
- Audit ověřuje aktuálnost antiviru na stanicích (a to nejen virové databáze, ale i verze AV programu)

85

## Aktualizace antiviru - příklad



Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## OWASP Top Ten Most Critical Vulnerabilities

**Vývojář by se měl vyvarovat následujících hlavních chyb:**

- **1** Unvalidated Input
- **2** Broken Access Control
- **3** Broken Authentication and Session Management
- **4** Cross Site Scripting (XSS)
- **5** Buffer Overflows
- **6** Injection Flaws
- **7** Improper Error Handling
- **8** Insecure Storage
- **9** Denial of Service
- **10** Insecure Configuration Management

87

## Omezování bezpečnostních rizik vývojem

- **3 vrstvá architektura (uživatelské rozhraní- aplikační server - databázový server)**
- **provoz mezi uživatelem-aplikačním serverem a app. serverem-databází by měl být chráněn šifrováním**
- **aplikace by měla kontrolovat vstupní hodnoty na délku, speciální znaky a kód**
- **dostatečné auditování a log (včetně login pokusů atd.)**
- **neukládání citlivých údajů (jako heslo) v paměti nebo dokonce v souboru na počítači uživatele (nanejvýš hash formát)**
- **aplikace by měla podporovat silná hesla**
- **vlastní autentizace by měla probíhat jen na aplikačním serveru (ne až na straně uživatele).**
- **DB by měla běžet na „nedefault" portu (třeba MS SQL má default 1433, MySQL 3306 apod.)**
- **DB i aplikační server by měl být nastaven bezpečně (patche, minimalizace služeb atd.)**

88

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Politika hesel

- Je politika vyžadována na všech doménách /objektech?
- **Nastavení:**
- - max. stáří: menší než 30 (60) dní
- - min. stáří: různé od 0
  - min. délka: 8
  - unikátnost: 6 (posledních hesel nelze použít)
  - uzamčení: 3 (5) špatných pokusů
    nulování počítadla 1440 min (1 den)
  - odblokování: Admin
  - prac. doba: Ano/Ne ( v závislosti na povaze práce uživatelů)
  - logon-změna: Ano (uživatel musí měnit heslo po prvním přihlášení)
  - komplexita (A-Z, a-z, 0-9 a příp. ještě i speciální znaky +*,$ apod.)
- přednastavitelné účty jsou zablokovány (Guest, Administrator) respektive admin je přejmenován
- ověřit, zda-li každý administrátor má své vlastní heslo a zda-li jsou administrátorská hesla silná

77

## Politika serveru – autentizační protokol – velmi významná ochrana hesel proti hackerům!

- LAN MANAGER Authentication Level
  - Určuje, který autentizační protokol bude použit při přihlášení v síti
- Do not store LAN manager hash value on next password - DISABLED
  - LM hash (WIN 3.1 – WIN 95)
  - NTLM hash (WinNT, W 2000...)

(LM hash je možno snadno rozluštit – stačí několik hodin – L0PTHRACK, JOHN the RIPPER...)

Zatím nejlepší výsledky má zabezpečení přes KERBEROS.

78

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# V. Hackerské postupy a obrana proti nim

- **Prolamovače hesel**
  - **Brute force**
  - **Slovníkový útok**
  - **Rainbow tables**
- **Keylogger**
- **Backdoor**
- **Rootkit**
- **Sniffer**
- **DoS a DDoS**
- **Trojské koně**
- **Viry a červy**
- **„Otrávení" provozu (Man in the middle)**
- **Webhacking**
  - **Útoky proti uživatelům (CSRF, XSS...)**
  - **Útoky proti databázi (SQL Injection...)**
  - **Útoky proti webové aplikaci (Exploit kity...)**
- **Sociální techniky a phishing**

79

# Elektronické bankovnictví

- Mimořádně nebezpečná oblast využití Internetu
- Dbát na správné přidělení práv (pokud písemný příkaz k úhradě musí podepsat dva jednatelé, nedává smysl, aby elektronicky stejnou operaci prováděla sama fakturantka nebo účetní...)
- Dbát na bezpečné uložení certifikátů (na PC a síť „vidí" informatici – jistější vyjímatelné médium)
- Výši operací vhodně limitovat
- Pokud je možná další autorizace (SMS, verifikace další osobou, další heslo apod.), vždy ji využijte
- Seznámení odpovědných osob s principy phishing, při jakékoli pochybnosti zajistit náhradní způsob plateb a sledovat další vývoj
- **PHISHING** – k získání informací hacker použije vlastní e-mail nebo WWW stránku obdobného vzhledu nebo vlastností jako známá společnost (výzvy k zadání hesel, změně účtů apod.)
- Měla by omezit vhodná personální politika a znalost tohoto nebezpečí ze strany zaměstnanců (osvěta).

80

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# SQL injection

- **Pod pojmem SQL injection se skrývá podvržení vstupních dat (hodnot proměnných odesílaných serveru) tak, aby byl nějakým způsobem pozměněn výsledek SQL dotazu.**
- Mějme např. SQL dotaz:
- *SELECT * FROM Users Where User_ID= ' ' and Password = ' ';*
- Při správném zadání podmínka dopadne:
- *SELECT * FROM Users Where User_ID= 'ADMIN' and Password = 'superman325';*
- Pokud ale útočník jméno zná a zadá je ve formě **ADMIN ' --**
  , z uvedeného příkladu se pak stane toto:
- *SELECT * FROM Users Where User_ID= 'ADMIN' --and Password = ' ';*
- Výsledkem bude likvidace nutné podmínky na shodu hesla. A pravděpodobně získání přístupu do systému. "--" se totiž postará o odstranění zbytku SQL dotazu – tj. zde jsem i bez hesla získal seznam uživatelů!
- Pomůcka pro ruční test na SQL Injection je např. řetězec ' or 1=1 –
  nebo ' --
- **XSS (Cross Site Scripting)** je obdobou, upravena však bývá přímo odkazovaná adresa,kam útočník podstrčí – opět přes neošetřený vstup- svůj javasriptový kód:
- http://URL/stranka.php?nadpis=cokoliv**<script>alert**('Toto je úspěšný XSS útok.')**;</script>**

89

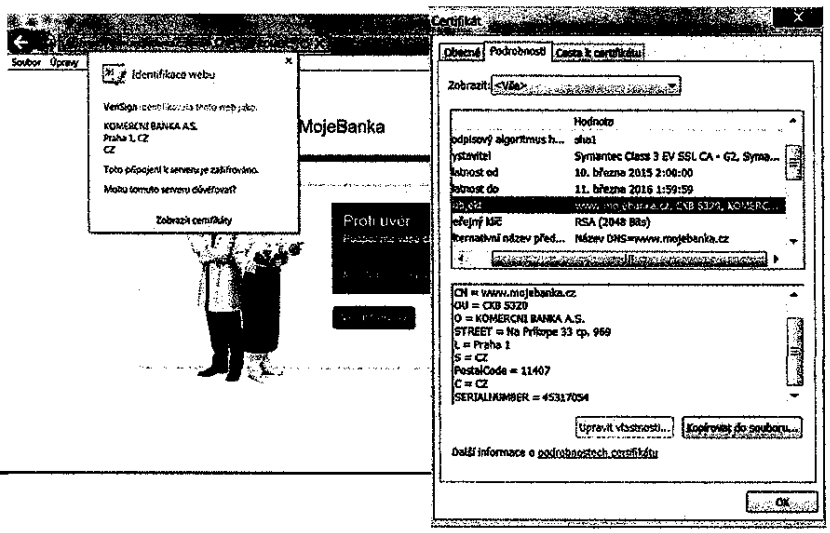
# Zabezpečené protokoly

- **SSH** - je používáno jako bezpečná náhrada starších protokolů a nabízí i nové vlastnosti:
  - Náhrada protokolu Telnet, práce na vzdáleném počítači přes nezabezpečenou síť
  - Náhrada protokolu Rlogin, přihlášení na vzdálený počítač, vzájemná autentizace
  - Náhrada protokolu Rsh, spouštění příkazů na vzdáleném počítači
  - Tunelování spojení
  - Většinou se spojuje s SSH démonem (SSH daemon, sshd) pro navázání spojení. Pro WIN často klient PuTTy.
- **SSL** - Protokol SSL se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP. Po vytvoření SSL spojení (*session*) je komunikace mezi serverem a klientem šifrovaná (asymetricky) a tedy zabezpečená. Nutno ale kontrolovat, kdo certifikát vydal, zda jsme neopustili HTTPS apod.
- **S/MIME** – umožňuje používat šifrování dat a digitálních podpisů v elektronické poště. Šifrování a dešifrování probíhá na straně klienta (který jediný má klíče), protokol tedy nemusí být zvlášť podporován poštovními servery. Nutno dávat pozor na uschování klíčů, sledovat Seznam zneplatněných certifikátů...

90

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# HTTPS - Kdo z Vás toto kontroluje?




# Zabezpečené protokoly II.

- **IPSec** je bezpečnostní rozšíření IP protokolu. Jedná se o zabezpečení již na síťové vrstvě. Toto rozšíření je tak nezávislé na dalších (vyšších) protokolech TCP/UDP. Časté pro VPN.
  - Ověřování - při přijetí paketu může dojít k ověření zda vyslaný paket odpovídá odesílateli či zda vůbec existuje.
  - Šifrování - obě strany se předem dohodnou na formě šifrování paketu. Poté dojde k zašifrování celého paketu krom IP hlavičky, případně celého paketu a bude přidána nová IP hlavička.
  - Základní protokoly šifrování IPSEC:
    - Authentication Header (AH) - zajišťuje autentizace odesílatele a příjemce, integritu dat v hlavičce, ale vlastní data nejsou šifrována.
    - Encapsulation payload security (ESP) - přidává šifrování (celých) paketů. Proto jsou oba protokoly často používány zároveň.
- **Kerberos** je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou autentizaci – klient i server si ověří identitu své protistrany.
  - Kerberos je postavený na symetrické kryptografii (rychlé) a potřebuje proto důvěryhodnou třetí stranu (tou je tzv. „autentizační server", který symetrický klíč generuje na základě znalosti veřejného asymetrického klíče klienta – přidělí mu tzv. Ticket Granting Ticket).

92

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# SYN flooding

- Podstatou SYN floodingu je využití jedné z vlastností TCP protokolu, zvaného **three-way handshake**, neboli třísměrné potřesení rukou, které si klade za cíl ověřit, zda obě strany o spojení opravdu stojí.

  Představme si, že KLIENT iniciuje spojení se SERVEREM. KLIENT tedy pošle první paket s nastaveným SYN bitem.

  SERVER odpoví paketem, který má nastaven SYN a ACK bit a uloží si informaci o nadcházejícím spojení do interní datové struktury. Tomuto stavu se říká polootevřené spojení (half-open connection).

  Klient nyní za normálních okolností dokončí potřesení třetím krokem, kterým je odeslání paketu s nastaveným ACK bitem. V tuto chvíli je úvodní část spojení dokončena a po síti mohou začít proudit data.

- SYN flooding vlastně nedělá nic jiného, než že začne odesílat množství paketů se SYN bitem, jako kdyby chtěl normálně komunikovat, **neprovádí však již třetí fázi handshaku, takže na stroji, který je cílem útoku, dojde postupně k zaplnění bufferů pro polootevřená spojení.** Cíle bylo dosaženo, server není schopen přijímat další pokusy o spojení a tudíž se stává nedostupným. Případnou horší alternativou může být úplné vyčerpání volné paměti, pakliže není omezen maximální počet spojení - to najisto způsobí pád serveru s možným poškozením dat.

  Často spojeno s funkcí zvanou IP spoofing, neboli falšování IP adres (hacker nahradí svou adresu falešnou, takže se nedá zjistit, odkud k SYN floodingu vlastně došlo).

93

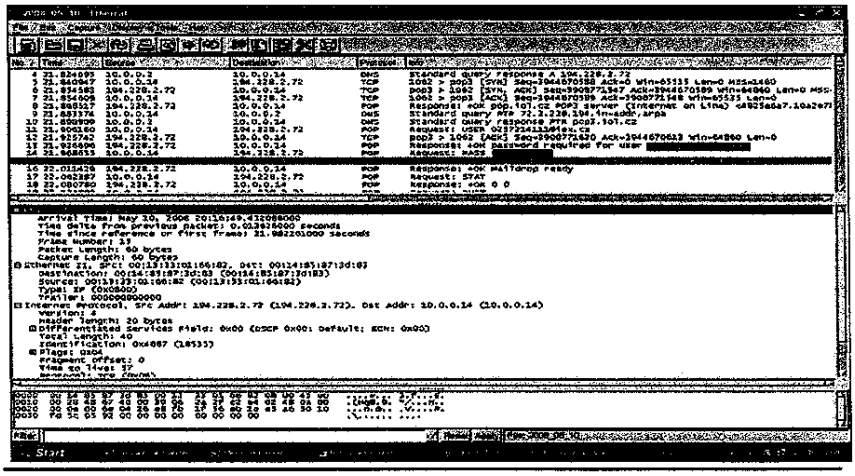
# Sniffery

- (TCPDUMP, ETHEREAL, CAIN...)
- Sledování a zachytávání paketů procházejících sítí může být zneužito pro získání hesel či jiných citlivých informací
- Může však sloužit i síťovým administrátorům při analýze síťového provozu, monitorování zátěže či stopování útoků.

94

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Ukázka – činnost snifferu proti POP3



95

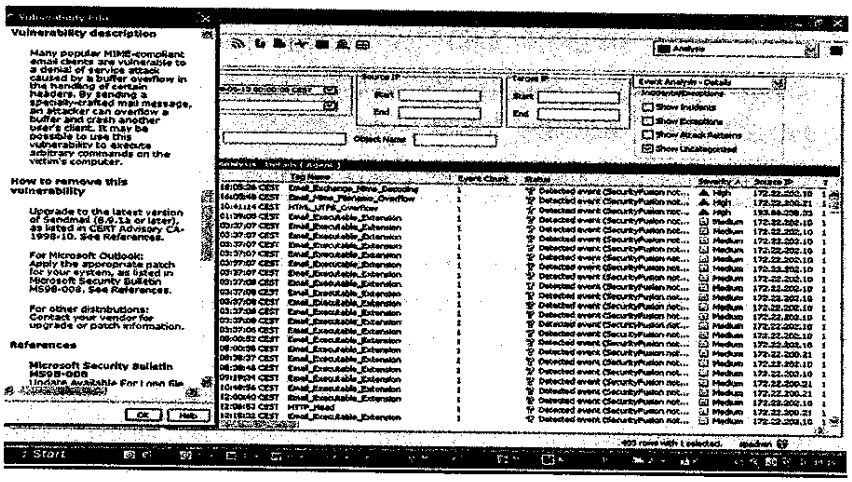
# IDS / IPS

- Obrana proti snifferům (jistější by ovšem bylo veškerý provoz šifrovat)
- Systémy IDS sledují a vyhodnocují provoz v síti. Pakety porovnávají s databází známých útoků. Výsledky se logují.
- Ke sledování provozu využívají „sondy" umísťované do různých segmentů sítě.
- Systémy IPS na útoky reagují aktivně, tj. zasílají např. zprávy, blokují porty, zahazují podezřelé pakety, blokují segmenty sítě apod.

96

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Činnost IDS - ukázka

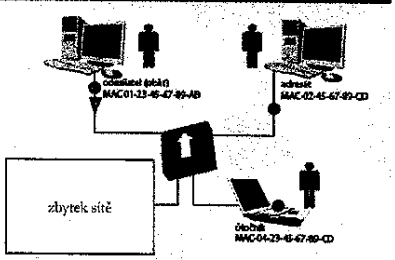



97

# ARP poissoning, DHCP spoofing aj.

- Jde o techniky, kdy útočník donutí síťové prvky k tomu, aby mu posílaly pakety určené původně pro jinou stanici
- K tomu potřebuje útočník být uvnitř sítě a nainstalovat speciální SW.

**Ukázka útoku ve vzdáleném Ethernetu**




Útočník přesvědčí odesílatele o tom, že adresa adresáta je MAC-04-23-45-67-89-CD.
Útočník přesvědčí adresáta o tom, že adresa odesílatele je MAC-04-23-45-67-89-CD.
Pak si útočník provoz odchytí a po prohlédnutí ho přepošle na správnou adresu podle IP adresy (ta totiž zůstává celou dobu správná)

98

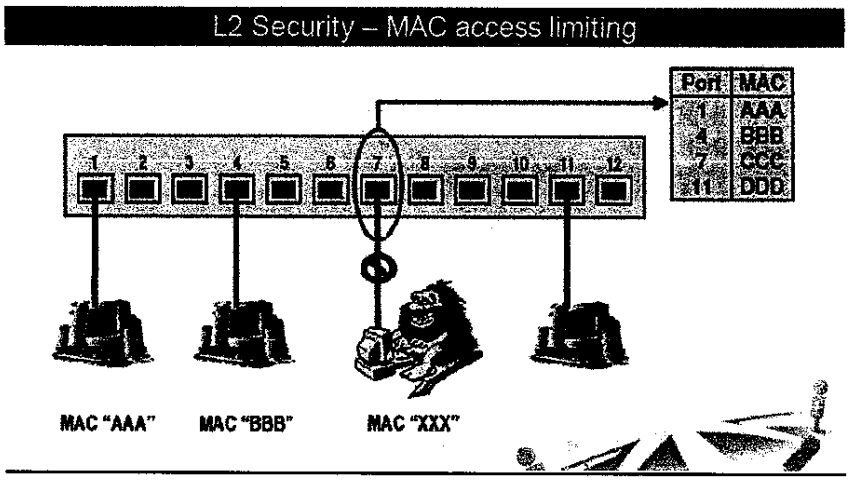
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Obrana proti přesměrování ARP

- Zavedením trvalých ARP záznamů:
  ARP –s stanice 00-00-C5-74-EB-C0 (již nemůže použít MAC adresu, která byla staticky přidělena)
- Hlášení změn MAC adres (např. utilita ARP WATCH)
- Switch umožňující inspekci ARP paketů (stanici s podezřelým ARP provozem switch odpojí – tzv. DHCP Snooping + Dynamic ARP Inspection)
- L2 security (port security – odpojení uživatele s cizí MAC adresou)

99

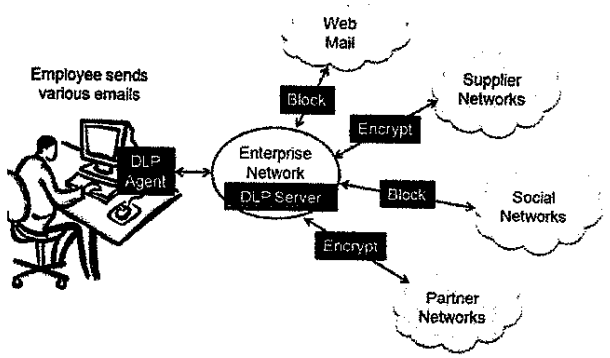
## Bezpečnost L2 – ochrana před připojením cizí stanice




100

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# DLP – Data Loss Prevention




Slouží k obraně proti zneužití citlivých dat. Předem definovaná citlivá data může:

- Blokovat
- Šifrovat
- Zaznamenávat pokusy o jejich zneužití
- Varovat uživatele (=edukace zaměstnanců)

101

# Ukázka logu z DLP zařízení

ID: 164176

| | | | |
|---|---|---|---|
| Severity: | Medium | Status: | New |
| Action: | Permitted | Event time : | 13 Nov. 2015, 10:32:45 AM |
| Channel: | Endpoint email | Incident time: | 13 Nov. 2015, 10:32:47 AM |
| Assigned to: | Unassigned | Total matches: | 3 |
| Incident tag: | N/A | | |
| Detected by: | Endpoint Agent | | |
| Destinations: | | | |
| Email Direction: | Outbound | | |
| Email address: | jan.bukovsky@ceb.cz | | |
| Action Taken: | Permitted | | |
| Transaction Size: | 15.5 KB | | |
| Details: | FW: TEST DLP IČO | | |
| Violation triggers: | | | |
| Policy: | test reg | | |
| Rule: | modulo 11 | | |
| > Classifier: | Account Number 6-13 digits (Regular Expression) | | |
| 3 match(es): | 89123456, 23564552, 8989898 | | |

Zpracovává :
Maily
Tisky
Použití schránky
Nahrání na USB flash
Kopírování nebo přejmenování souborů
Atd.

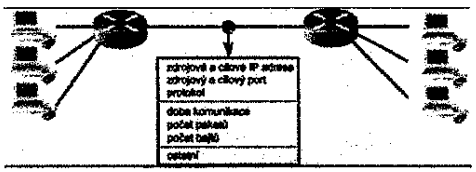
DLP:

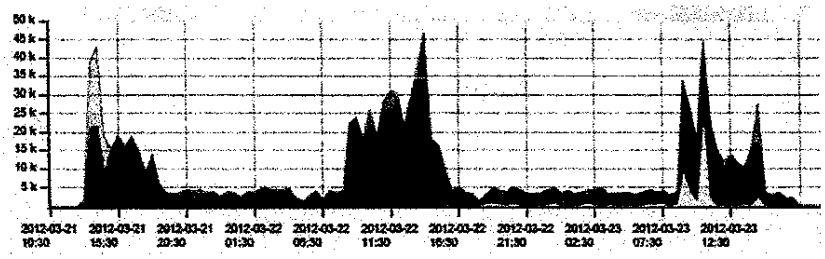
- Koncových stanic
- Síťové

102

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

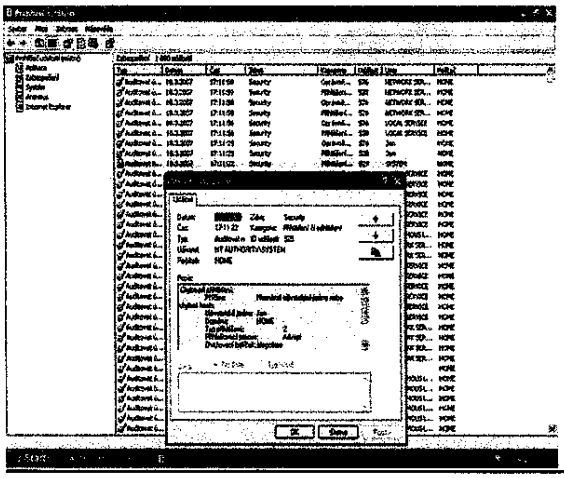
# NetFlow




103

# Logování Windovs – Event Viewer



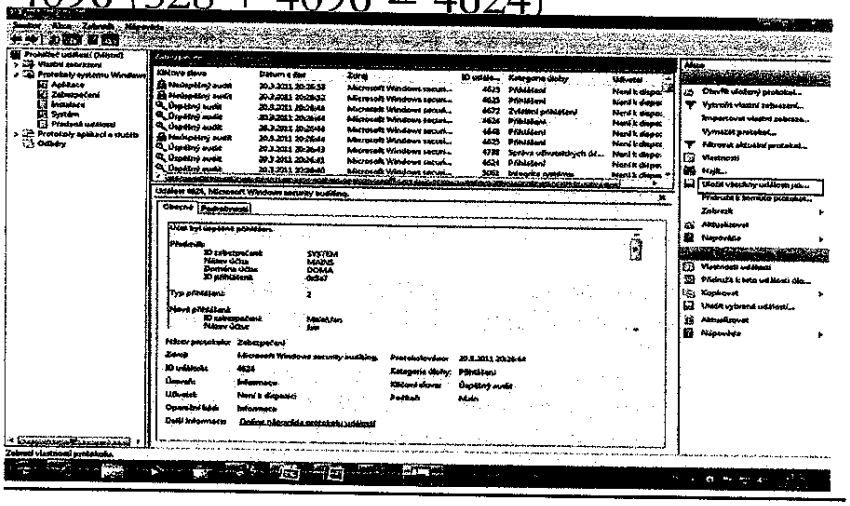
- 529 – neznámé jméno/heslo
- 530 – přihlášení mimo hodiny
- 531 – zakázaný účet
- 533 – nelze se hlásit z tohoto PC
- 535 – platnost hela vypršela
- 517 – auditní log byl smazán
- 520 – změna syst. času…

Logy se ukládají do C:\WINDOWS\SYSTEM32\CONFIG jako soubory *.EVT

**Logy se dají exportovat a importovat (přes nabídku AKCE) což lze využít při auditu!**

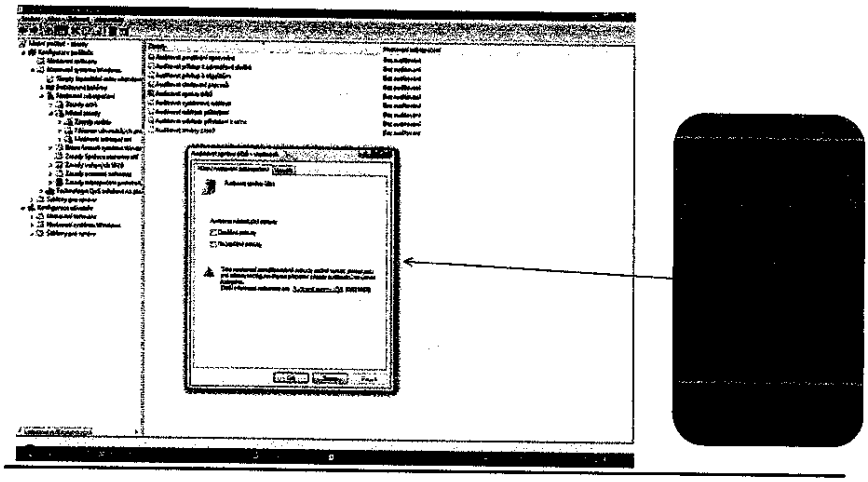
104

## Od WIN VISTA nová čísla událostí + 4096 (528 + 4096 = 4624)





## Aby bylo možno logování rozumně využívat musí být zapnuto ! (Přes GPEDIT.MSC)



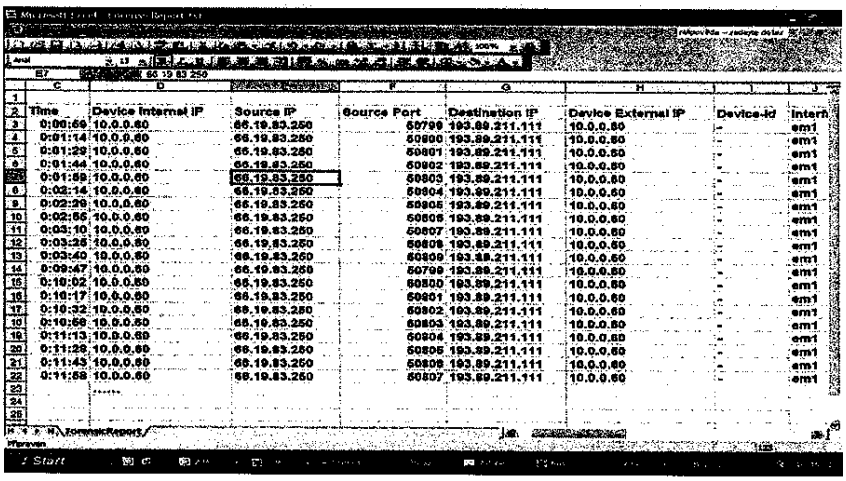
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Některé možné zásady pro sledování logů

- Změny vlastního logu (ID 516, 517, změna času ID 520)
- Jakékoli změny group policy (ID 608 – 609)
- Jakékoli změny v založení a zrušení účtů (ID 624, 630, ale i 625 a dále sada ID k odemknutí účtů 621,626,628..)
- Jakékoli změny ve skupinách (ID 631, 634 a dále změny ve složení skupin ID 632 – 633)
- Více než 50 chybných přihlášení během deseti minut (ID 529 – 534, 537)
- Počty a časy úspěšných přihlášení (ID 528, 538)
- Četnost chybných přihlášení (ID 529 – 532, a zejména 644 – uzamčení účtu)
- Kritické chyby (klasifikace EMERGENCY, ALERT, CRIT, ERR popř. i WARNING, nebo např. restart domény – ID 512)
- Seznam ID viz např. WWW.EVENTID.NET

107

## Ukázka zpracovaného logu – scanování portů



| Time | Device Internal IP | Source IP | Source Port | Destination IP | Device External IP | Device-Id | Intern |
|---|---|---|---|---|---|---|---|
| 0:00:59 | 10.0.0.60 | 66.19.83.250 | 50798 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:01:14 | 10.0.0.60 | 66.19.83.250 | 50800 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:01:29 | 10.0.0.60 | 66.19.83.250 | 50801 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:01:44 | 10.0.0.60 | 66.19.83.250 | 50802 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:01:59 | 10.0.0.60 | 66.19.83.250 | 50803 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:02:14 | 10.0.0.60 | 66.19.83.250 | 50804 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:02:29 | 10.0.0.60 | 66.19.83.250 | 50805 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:02:56 | 10.0.0.60 | 66.19.83.250 | 50806 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:03:10 | 10.0.0.60 | 66.19.83.250 | 50807 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:03:25 | 10.0.0.60 | 66.19.83.250 | 50808 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:03:40 | 10.0.0.60 | 66.19.83.250 | 50809 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:09:47 | 10.0.0.60 | 66.19.83.250 | 50799 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:10:02 | 10.0.0.60 | 66.19.83.250 | 50800 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:10:17 | 10.0.0.60 | 66.19.83.250 | 50801 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:10:32 | 10.0.0.60 | 66.19.83.250 | 50802 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:10:59 | 10.0.0.60 | 66.19.83.250 | 50803 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:11:13 | 10.0.0.60 | 66.19.83.250 | 50804 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:11:28 | 10.0.0.60 | 66.19.83.250 | 50805 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:11:43 | 10.0.0.60 | 66.19.83.250 | 50806 | 193.89.211.111 | 10.0.0.60 | - | em1 |
| 0:11:58 | 10.0.0.60 | 66.19.83.250 | 50807 | 193.89.211.111 | 10.0.0.60 | - | em1 |

108

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Práce s logy v organizaci

- Logy musí být někým sledovány a vyhodnocovány
- Z podezřelých událostí musí být vyvozovány závěry a nápravná opatření
- Příznaky nedostatků:
  - Neexistuje žádná politika / metodika sledování logů
  - Pracovník pověřený vyhodnocováním není na výzvu schopen předvést, kde logy sleduje („porucha", opravdu neví kde jsou...)
  - Není schopen doložit, jak provádí nějaké výběry (třeba přístup na významný objekt, změny skupin...)
  - Logy jsou někým mazány (517 / 1102) a nikomu to nevadí
  - Sestavy posílané mailem nejsou otevřeny
  - Logy jsou přístupné jen z několika posledních dní
  - V organizaci nejsou zaznamenány žádné bezpečnostní incidenty
  - Výsledky monitorování nikdo nikomu nepředkládá



# SIEM

SIEM = Security Information + Event Management

**Schopnosti SIEM**:

**Agregace dat** - seskupení vybraných dat - např. data z přepínačů, firewallů, serverů, počítačových stanic, databází, IDS/IPS, aplikací atd.

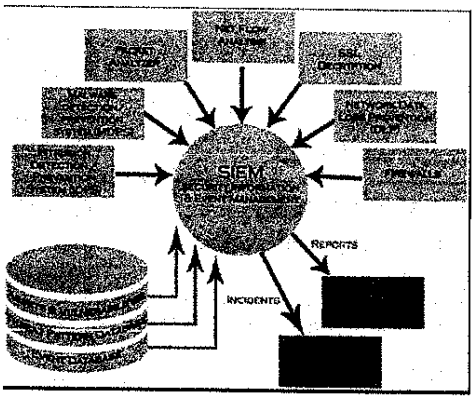
**Korelace** - nalézání vzájemných vztahů událostí, např. monitorování činnosti konkrétního uživatele, pohled na určité události v nějakém časovém intervalu atp.

**Varování** (alerting)

Informační panely, přehledové sestavy (**dashboards**)

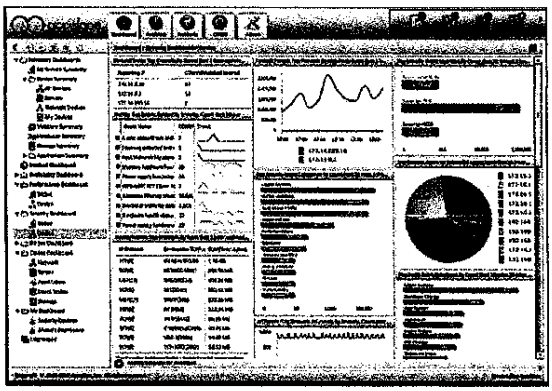
**Reportování shod** (compliance)

Zachování, **ukládání historických dat (logů)**



Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Porovnání a vyhodnocení logů z více zdrojů – typická vlastnost SIEM



111

## Způsob napadnutí a obrana proti němu

| | |
|---|---|
| Hromadný ping, scanování portů | Detekce (IDS, SNORT aj.), správné nastavení hraničních prvků |
| Detekce operačního nebo dalších systémů | Patche, správné nastavení hraničních prvků |
| Odposlech hesel, monitorování síťového provozu | Nastražení honey potů, šifrování provozu SSH, SSL, Kerberos, fyz. ochrana |
| Odcizení hesel a následný útok brutální silou | Fyzická ochrana, silná hesla |

112

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Způsob napadnutí a obrana proti němu

| | |
|---|---|
| Inventarizace kont, sdílených souborů, aplikací... | Nasazení vnitřních routerů, zákaz NetBIOSu (port 139), zákaz sdílení |
| Přeplnění bufferu, SynFlood (DOS, DDOS) | Patche hraničních routerů a firewallů, nasazení IDS |
| Použití známých chyb operačního systému, aplikací, akt. prvků | Patche, sledovat nově nalezené chyby |
| Instalace zadních vrátek | Antiviry, anti-spyware, anti-rootkity, sledování událostí |

113

## Způsob napadnutí a obrana proti němu

| | |
|---|---|
| Zneužití vzdáleného přístupu nebo tel. připojení | CALL BACK, silná hesla, šifrování dat, zabezpečený tunel |
| Zneužití e-mailu k zavirování nebo podsunutí nesprávných informací | Nepovolovat OPEN RELAY, antivir na poštovním serveru i klientovi, likvidace spamu |
| Zneužití nadbytečných služeb, portů, příliš rozsáhlých práv... | Zavřít porty, snížit práva, neinstalovat zbytečné služby |

114

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Předpokládané typy chyb - Internet

- Ve veřejně dostupných zdrojích je vidět víc, než je nezbytné (jména, funkce, telefony) – lepší nechávat tam zastaralé údaje
- Směrem do Internetu jsou otevřeny zbytečné porty (co je nad port 80 a 25, je v tomto případě krajně podezřelé)
- Nastavení firewallů a routerů nebrání přístupu na podezřelé stránky, poštu lze zahltit spamem

115

## Předpokládané typy chyb II.

- Nejsou nasazeny důležité bezpečnostní patche (nebo dokonce service packy)
- V síti jsou počítače a prvky s beznadějně zastaralou verzí SW (typicky WIN 95/98, dnes už i WIN XP)
- Řada přístupných portů umožňujících běh nezabezpečených protokolů (typicky FTP, TELNET...)
- „Vidíme" i tam, kam bychom nemuseli (DMZ, vzdálené segmenty apod.)

116

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Předpokládané typy chyb III.

- Neblokované spustitelné programy v mailu, nezobrazují se přípony souborů
- V prohlížeči není zablokovaná JAVA, ACTIVE X atd.
- ACL neobsahuje řádek access-list 100 deny ip any any log
- Antivir na některých stanicích se neaktualizuje
- Antivir je aktualizován jen nahodile nebo jen 1x za dlouhou dobu (týdně apod.)

117

## Předpokládané typy chyb IV.

- Není nasazen systém IDS / IPS, nebo nasazen je, ale nemá sondy v rozhodujících segmentech sítě
- Nic nenasvědčuje dennímu sledování logů z IDS, konfiguraci IDS není nikdo schopen vysvětlit
- Podaří se připojit stanici zvenčí do vnitřní sítě
- Podaří se nasadit sniffer
- Není nasazena žádná ochrana proti ARP poissoningu

118

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Odstranění hrozeb

| Hrozba | Řešení | Funkce | Technologie |
|---|---|---|---|
| Zachycení dat, nežádoucí čtení, modifikace | Zašifrování | Brání falšování a čtení zakódováním dat | Symetrické / asymetrické šifrování |
| Nesprávná identifikace uživatelů - podvod | Autentizace | Ověřuje a identifikuje odesílatele a příjemce | Autentizace certifikátem nebo biometrickými parametry, Digitální podpis |
| Neautorizovaný uživatel získá přístup zvenčí do sítě | Firewall | Filtruje a zabraňuje provozu nebo vstupu do sítě | Firewally, VPN |

119

# VI. Bezpečnost mobilních zařízení
## Hlavní Problémy Notebooků

| Riziko | Vyvolá | Ochrana |
|---|---|---|
| ODCIZENÍ NOTEBOOKU | Ztrátu firemních dat, případně včetně přihlašovacích údajů do Vaší domény | Šifrování CELÉHO disku Okamžité hlášení odcizení |
| Připojení do cizích sítí | Možnost odposlechu nebo jiného napadení | Zabránit buď tomuto připojení, nebo naopak připojení do naší sítě |
| *Zařízení není* tak dobře updatováno jako běžné stanice | Zavirování, napadnutí. V případě připojení do naší sítě se viry dále šíří. | Vynucení patchů a spouštění antiviru. Do sítě se připojí jen „compliant" zařízení. |
| Soubory offline | Při odcizení notebooku budou k dispozici dokonce i Vaše soubory uložené jinak na doméně | Nepovolovat offline soubory |

120

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

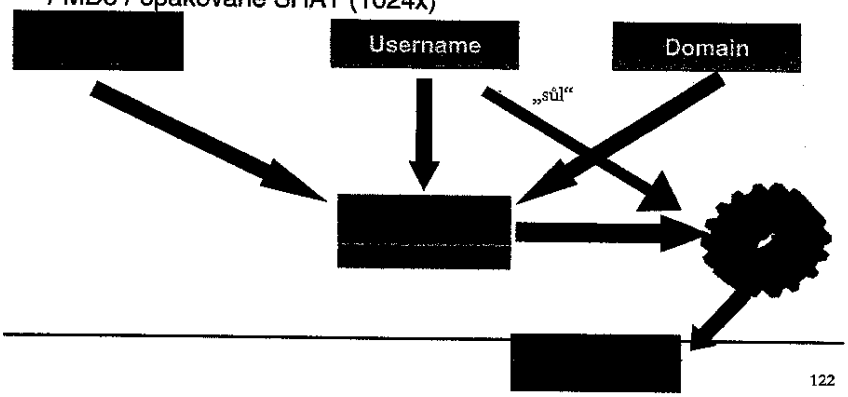
## Cached Credentials

- Když se na počítači přihlašujete na doménový účet, musí se vaše heslo ověřit **online** (**online logon**) na nějakém blízkém **domain controlleru**.
- Jenže pokud byste si později notebook od sítě odpojili a odnesli domů, už byste se na svůj doménový účet nepřihlásili. Proto si počítač uloží do registrového klíče **HKLM\Security\Cache** nějaké informace o vašem účtu. Když se pak přihlašujete **offline** (**offline logon**), stačí přihlašovací informaci zkontrolovat v lokálních registrech a systém vás může pustit na počítač.
- Zvláště ve starších systémech (XP, W2003) je relativně snadno zneužitelný.

121

## Obsah Cached Credentials

- Mimo tzv. **password verifier** , se tam ukládá seznam **SIDů** doménových skupin a uživatelská práva.
- Password verifier je klasický NT hash, znovu hashnutý pomocí MD4 / MD5 / opakovaně SHA1 (1024x)




122

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Hlavní Problémy mobilů a tabletů

| Riziko | Vyvolá | Ochrana |
|---|---|---|
| ODCIZENÍ MOBILU | Ztrátu firemních dat | Šifrování CELÉHO mobilu, silné heslo. Zamykání. Okamžité hlášení odcizení a blokování zařízení (není ale spolehlivé – stačí se nepřipojit) |
| Možnost odposlechu | Ztrátu důvěrných údajů | Nelze – pouze školit uživatele |
| Zařízení není tak dobře updatováno jako běžné stanice | Zavirování, napadnutí. V případě připojení do naší sítě se viry dále šíří. | Vynucení patchů a spouštění antiviru (pokud je pro konkrétní zařízení k dispozici). Do sítě se připojí jen „compliant" zařízení. |
| Nebezpečné aktivity uživatele | Spolu s hrou nebo programem se nainstaluje škodlivý kód | Nepovolovat jailbreak, nepovolovat některé rizikové aplikace |

123

# Vzdálená správa mobilních zařízení

| | |
|---|---|
| **Ochrana dat** | Kontrola a ochrana aplikací<br>Bezpečné úložiště - Secure Container<br>Blokování aplikací - Application Blacklisting<br>Šifrování |
| **Ochrana aplikací** | Data Protection (Lokalizace, Lock, Wipe, Delete)<br>Detekce Jailbroken a Rooted zařízení a jejich blokace |

124

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Doporučené nastavení mobilního zařízení - příklad

Vypnout Jednoduchý kód, nastavit kódový zámek, který bude mít **nejméně 8 znaků.**
V případě deseti neúspěšných pokusů o zadání kódu budou **veškerá data z mobilu automaticky smazána.**
Je zakázáno aktivovat tzv. **Jailbreak,** nebo jiný postup zpřístupňující data v mobilním zařízení způsobem obcházejícím aplikační rozhraní výrobce.

| | |
|---|---|
| | Vypnuto |
| | Zapnuto |
| | 5 min |
| | Po 15 min |
| | Vypnuto |
| | Zapnuto |
| | Poslední zprávy: 50 |
| | Vypnuto |
| | Zapnuto |

125

# Nastavení kódového zámku u iPhonu


126

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

## Srovnání mobilních operačních systémů

| | Apple iOS | Android |
|---|---|---|
| Úložiště | App Store je relativně bezpečné, Apple všechny aplikace kontroluje | Poněkud méně bezpečné (výrobců je mnoho, jasná autorita pro vyřazení aplikací není) |
| Viry a antivir | Virů relativně málo / Antivir neexistuje | Nejvíce virů / Antiviry k dispozici |
| Šifrování zařízení | AES 256 | AES 128 |
| Množství vynutitelných politik | Standardně vysoké | Vysoké, t.č. už vyšší než u iOS (např. oddělený sandbox) |
| Připojení USB flash disku nebo jiných zařízení | Snadno nelze | Připojitelné |
| Kód operačního systému | Nativní (známý jen firmě Apple) | Otevřený |

127

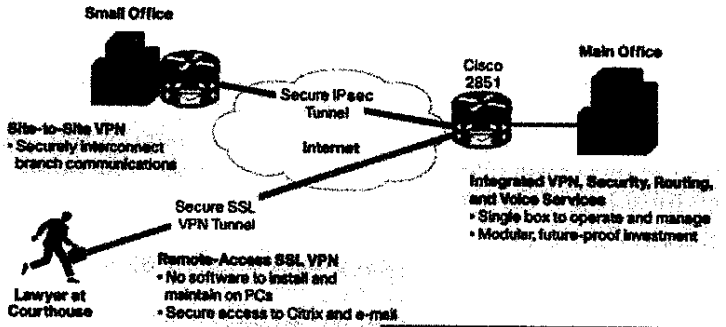
## Bezpečná vzdálená správa

- Vždy šifrujte komunikaci
- Zabezpečte primárně místo, odkud spravujete – vlastní pracovní stanici
- Pro přístup z vnějšku používejte vždy VPN, pokud možno 2FA (klientský cert, autentizační kalkulačka, aplikace na mobilu + přístup do domény)
- Notebooky – šifrované partition, nepoužívat „sleep mode".
- Nehlaste se na lokální stanice s domain adminem.

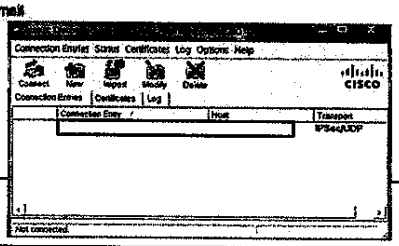
128

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# VPN – IPSEC, SSL

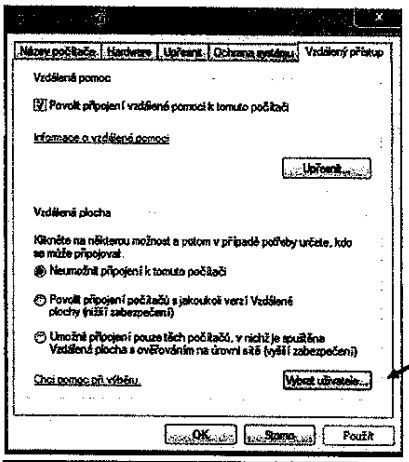



**Virtuální privátní síť** je propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.



129

# Vzdálená plocha




*Terminal server – nyní již není nezbytný, vzdálenou plochu lze aktivovat na každém serveru. Terminal server se používá k vzdálenému hlášení z jednoho místa (je vhodně konfigurován – mapování disků, instalované aplikace apod.)*
*Ochrana např.: nedefaultní porty (ne 3389), oddělený segment sítě, předchozí 2FA autentizace, silné logování…*

Zde povolení uživatelé se stanou členy skupiny **Remote Desktop Users.** Tu je nutno vždy auditovat!

130

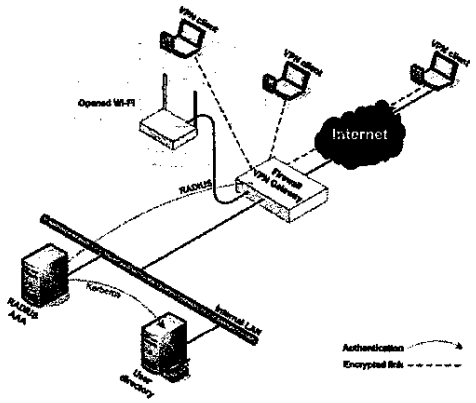
Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# VPN

- VPN – Virtual Private Network
- VPN je privátní síť, vybudovaná v rámci veřejné síťové infrastruktury, jakou je např. globální Internet.
- Důvody pro její použití jsou převážně ekonomické (není nutno pořizovat speciální linky pro přenos mezi lokalitami). Kromě toho řešení vyniká větší mobilitou proti leased line.
- Typické použití:
  - připojení notebooků zaměstnanců v době, kdy jsou mimo pracoviště
  - spojení mezi centrálou a (malými) pobočkami
- Zásadní význam má zabezpečení přenosového kanálu (mělo by být shodné, jako by šlo o skutečně privátní přenos – tj. pronajatou linku)

131

# VPN – obecné řešení




*Tj. uživatel používá tunelované spojení až na vstupní prvek – koncentrátor, VPN Gateway apod. Přihlášení do sítě zajišťuje samostatný RADIUS server.*

132

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

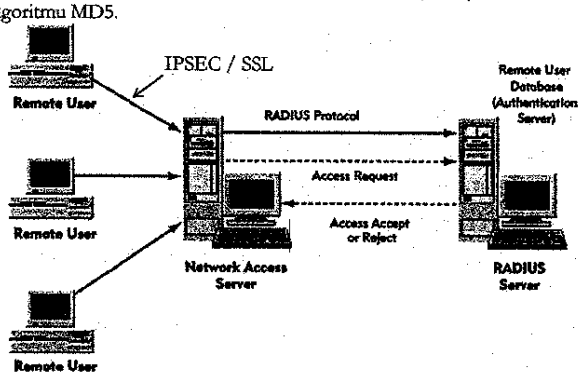
# Nejčastější způsoby realizace VPN

- V současné době jsou nejčastější VPN na bázi:
  - IPSEC (velmi bezpečné, ale nasazení je náročné)
  - SSL (nelze použít pro všechny aplikace – typicky pro klient-server aplikace – pošta, sdílení souborů apod.)
  - SSH
- Stále se ovšem vyskytují dříve vyvinutá řešení VPN na 2. vrstvě (L2VPN) - nejčastěji protokol PPP – Point to Point Protocol
- Nejčastější aplikace ve VPN:
  - Elektronická pošta (např. MS OWA)
  - Přístup ke vzdálené ploše terminálového serveru (odtud se spustí další aplikace)
  - Přímý přístup k souborovému systému (např. protokolem SSH – PUTTY apod.)

133

# RADIUS

**RADIUS** (*Remote Authentication Dial In User Service*) je AAA protokol(*authentication, authorization and accounting*) používaný pro přístup k síti nebo pro IP mobilitu.
Je považován za síťově bezpečný, neboť transakce mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Všechny uživatelská jména jsou přes síť zasílána šifrovaně. Uživatelské heslo je ukryto metodou založenou na algoritmu MD5.




134

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Audit VPN

- Mnoho technických řešení
- Osvědčený je audit logu přihlášení přes VPN za několik dní a jeho porovnání s evidencí přístupů do VPN

Alert: NAP User Account Denied Access
Source: SRV02.domain.cz
Path: SRV02.domain.cz
Last modified by: System
Last modified time: 2/25/2014 4:06:02 PM
Alert description: Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
Security ID: NULL SID
Account Name: XBAO35ccf151
Account Domain: DOMAIN
Fully Qualified Account Name: DOMAIN\XBAO

RADIUS Client:
Client Friendly Name: VPN
Client IP Address: 192.168.11.22

135

# Předpokládané typy chyb

- Notebooky obsahují citlivá data, která by měla být uložena na síti
- Nezašifrovaná data na noteboocích
- Lokální administrátorská práva na noteboocích
- Notebooky nejsou aktualizovány, není prováděna profylaxe
- Na mobilech není PIN nebo je slabý
- Mobilní zařízení jsou „jailbreaknuta"
- Na VPN není dvoufaktorová autentizace
- Přístup na VPN možný i z cizích zařízení, SSL certifikát hlásí běžně chybu
- Na notebooku není antivir, nebo je jeho verze / verze virové databáze zastaralá

136

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# I interní audit může udělat při prověrce IT chyby...

- Zaměření na formuláře a jejich náležitosti (podpisy, data) místo na to, jak se měla skutečně nastavit práva
- Auditor je při formulaci příliš pasivní a bojí se reakce odborníků, vůči nimž se cítí zranitelný
- Auditor trvá na neudržitelných zjištěních (třeba chybějící patche na aplikace na příslušném serveru neexistující)
- Auditor se pouští do teoretické oblasti (nemá oporu v best practices, v předpisech, ve faktech...)
- Zjištění nebyla dostatečně ověřena
- Zjištění jsou formulována příliš tvrdě („tím byla hrubě ohrožena akceschopnost útvaru IT"...)
- Auditor si nechal vnutit komentáře, které s věcí ve skutečnosti nesouvisí

137

# Častý jev v IT: možnost zablokovat uživatele více způsoby

- Správné je uživateli bránit v přístupu na všech úrovních, ale i zablokování na jediné z nich ve skutečnosti k zabránění přístupu stačí.
- Auditor nemusí hned sám do zprávy psát, ale pokud si to útvar IT vyžádá, je jeho připomínka korektní!

I když zde práva zůstanou, uživatel se stejně k údajům v databázi nedostane!

Toto „sériové" uspořádání je v IT velmi časté (dva firewally, antivir na více prvcích, uživatel ve skupině pro čtení i pro čtení a zápis aj.)

Ing. Jan Bukovský, jan.bukovsky@ceb.cz 138

Ing. Jan Bukovský,
jan.bukovsky@czka.cz

# Dotazy?

- Děkuji Vám za pozornost !

139