



Důvěra v propojeném světě



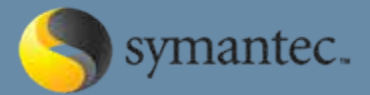
Bezpečnost verze 2.0

Nikol Honova
Government Sales Manager
Symantec ČR a SR



Agenda

- 1 Bezpečnost v2.0
- 2 Základy bezpečnosti
- 3 Bezpečnost informací a interakcí
- 4 Řízení bezpečnosti



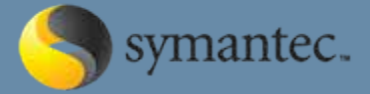
Důvěra v propojeném světě

Bezpečnost v2.0

- Namísto toho, abychom chodili do banky a žádali slečny o transakce, sedíme doma u prohlížeče a navyšujeme si kontokorent, převádíme peníze či počítáme možnosti hypotečního úvěru
- Chceme komunikova z míst, která nás neomezují a nečiní nás závislými
- Vystupujeme z komfortní zóny
- Perimetr mezi námi a bankou už nejsou vchodové dveře ani přepážka.
- Není kudy ho narýsovat. Zcela se rozmazal!



Tak co je (nebo raději kdo) je tím perimetrem?





DŮVĚRA

Srdcem nové bezpečnosti v2.0 je zjištění, že bitevním polem , na kterém ji prosazujeme, už není zařízení – jako tomu bylo v MINULOSTI – vše se posunulo spíše k informacím a interakcím.



Smile Buy Cheap Cvv2s And Get Gifts Hello all carders !

Iam glad to offer my service to serve all you guys. Iam selling US cvv2 with NO LIMIT (UK & Canadian and International cvv2s will be available soon)

*** Cvv2s have the following information:**

- Card Number**
- Card Expiry**
- CVV2**
- First & Last Names**
- Address & City**
- State & Zip/Postal code**
- Country (US)**
- Phone #**

===== Here is the price =====

*** For US cvv2 :**

1 -> 40 cvv2s : \$1.5 per card

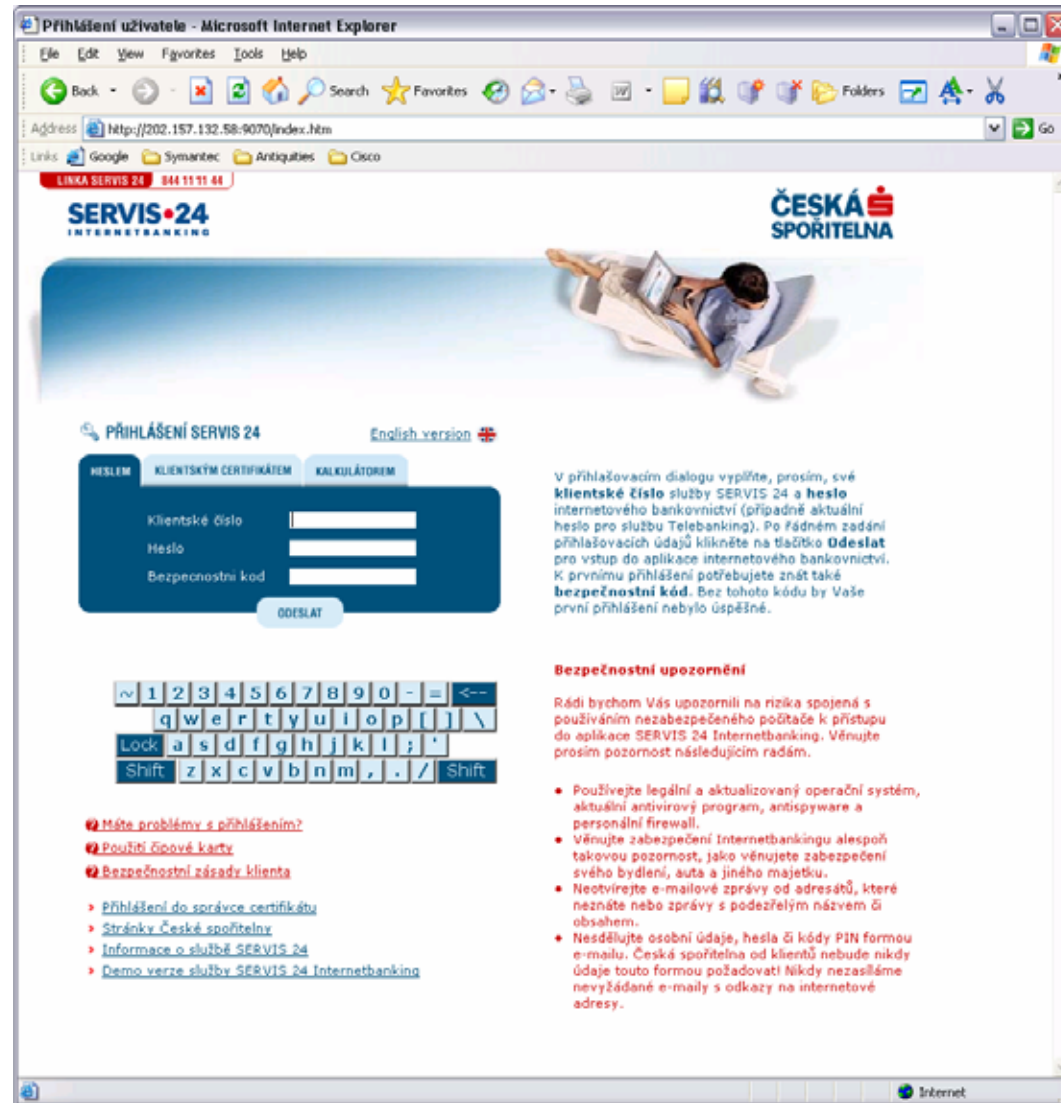
100+ cvv2s : \$1 per card

If your order > 50\$, u will get a calling card with 5\$

If your order > 100\$, u will get a calling card with 10\$

If your order > 200\$, u will get a calling card with 20\$

- Připraveno na celkem profesionální úrovni
- Útok obsahuje jistou porci sociálního inženýrství
 - Chlapík spokojeně relaxující na lehátku
 - Bezpečnostní varování (červený text)
 - Všechny alternativy přístupu (heslo a bezp. kód, certifikát, přístupová kalkulačka)
 - Jak česká, tak i anglická verze
 - URL maškaráda (IP adresa místo odkazu)



V přihlašovacím dialogu vyplňte, prosím, své klientské číslo služby SERVIS 24 a heslo internetového bankovníctví (případně aktuální heslo pro službu Telebanking). Po řádném zadání přihlašovacích údajů klikněte na tlačítko Odeslat pro vstup do aplikace internetového bankovníctví. K prvnímu přihlášení potřebujete znát také bezpečnostní kód. Bez tohoto kódu by Vaše první přihlášení nebylo úspěšné.

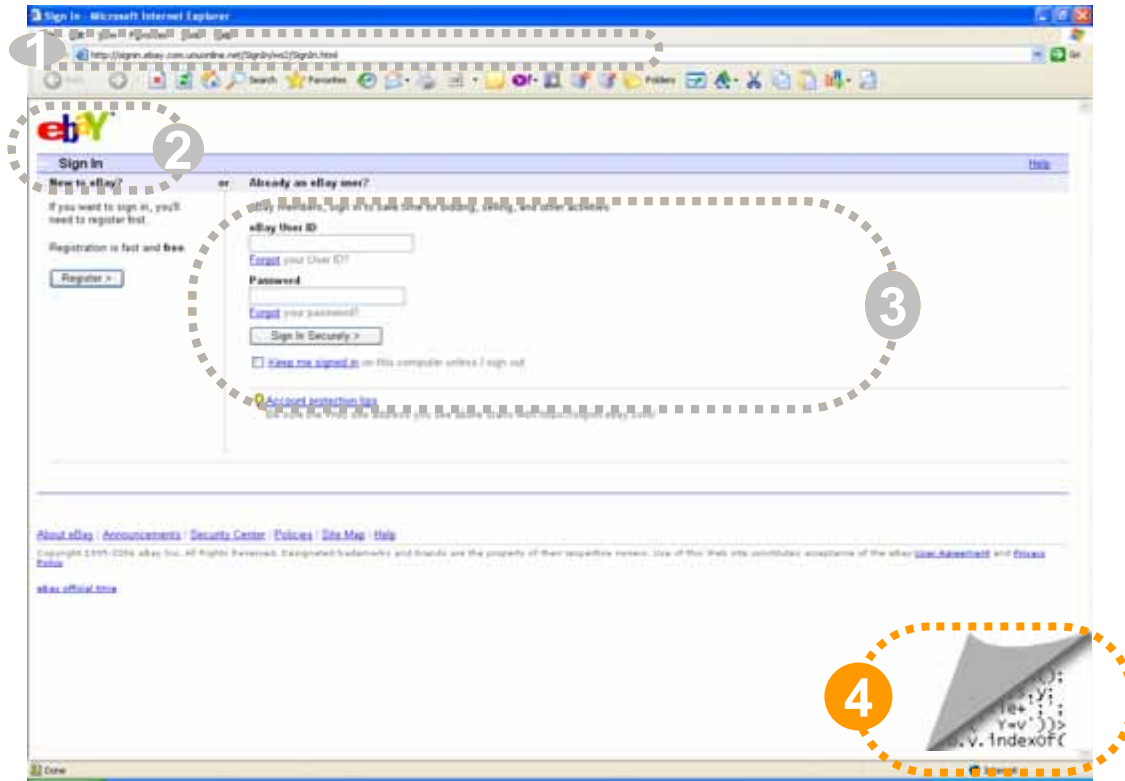
Bezpečnostní upozornění

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpečeného počítače k přístupu do aplikace SERVIS 24 Internetbanking. Věnujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operační systém, aktuální antivirový program, antispyware a personální firewall.
- Věnujte zabezpečení Internetbankingu alespoň takovou pozornost, jako věnujete zabezpečení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od adresátů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- Nesdělujte osobní údaje, hesla či kódy PIN formou e-mailu. Česká spořitelna od klientů nebude nikdy údaje touto formou požadovat! Nikdy nezasíláme nevyžádané e-maily s odkazy na internetové adresy.

Výrazem změny jsou i řešení....

- Chrání zákazníky před podvodnými weby
- Využívá heuristickou analýzu i blokování phishing webů



1
2
3
4

-  URL analýza
-  Analýza obsahu
-  Analýza vzhledu
-  Analýza zdroje

**Symantec
Confidential
Online**



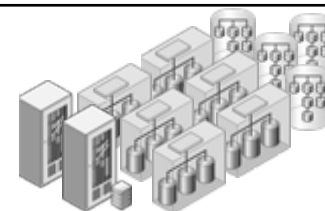
Ochrana interakcí



Ochrana informací



Ochrana infrastruktury





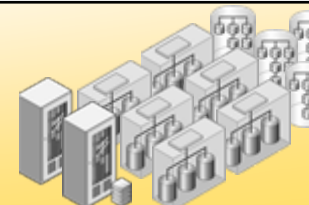
Ochrana interakcí



Ochrana informací



Ochrana infrastruktury





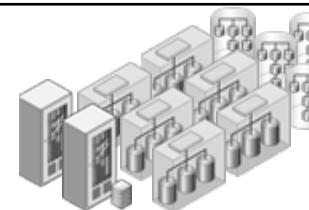
Ochrana interakcí



Ochrana informací



Ochrana infrastruktury





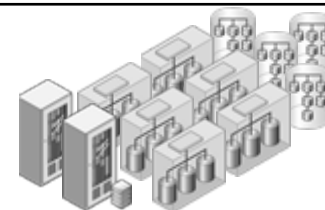
Ochrana interakcí



Ochrana informací



Ochrana infrastruktury





Bezpečnost informací



Základy bezpečnosti



Mobilní telefon



Notebook



Desktop



Soub. server



Aplik. server



Messaging server



DB server

Řízení bezpečnosti



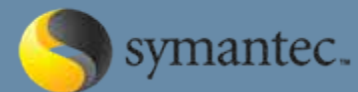
Bezpečnost informací



Základy bezpečnosti



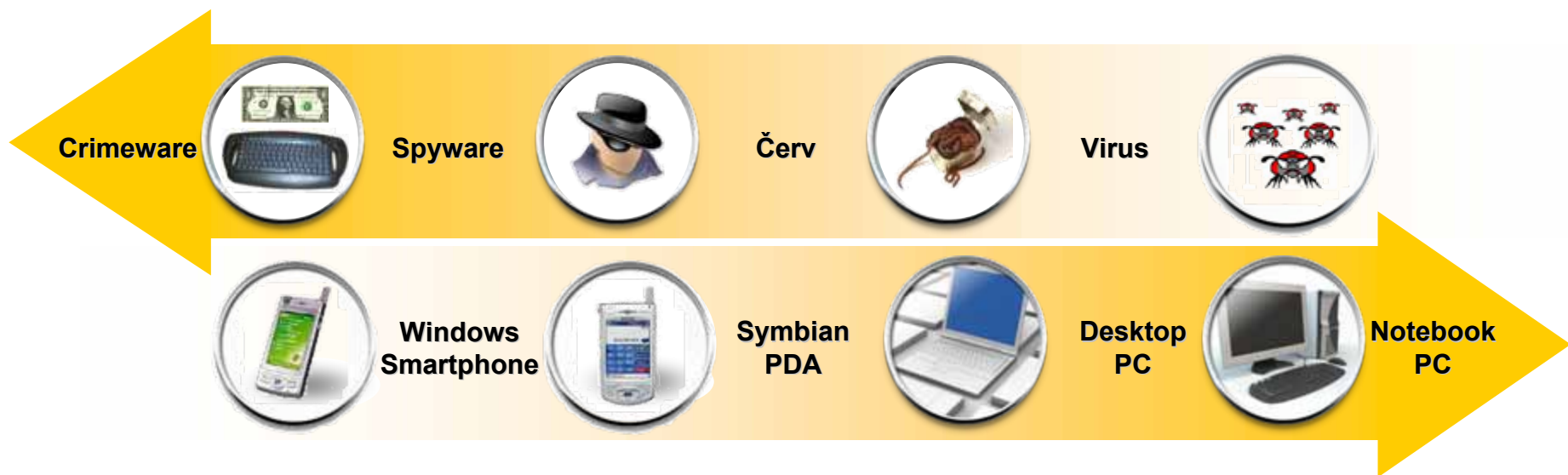
Mobilní telefon Notebook Desktop Soub. server Aplik. server Messaging server DB server



Důvěra v propojeném světě

Ochrana infrastruktury

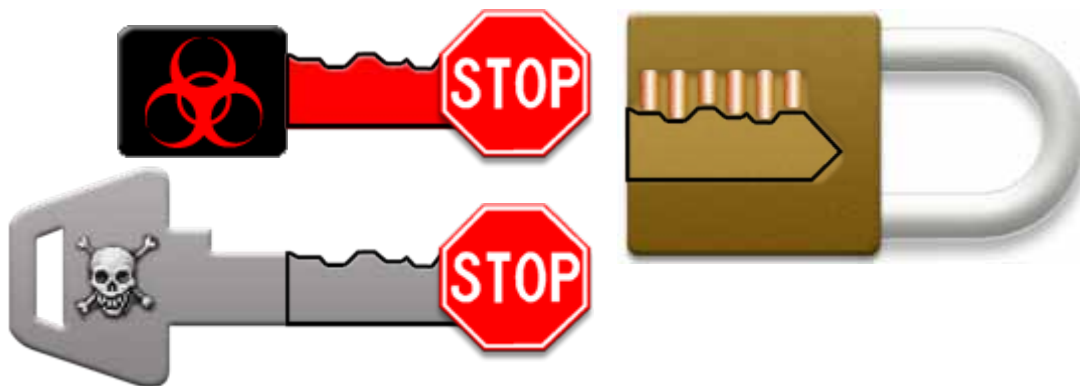
- Ochrana začíná v koncových bodech společnosti
 - Široký rozsah klientských zařízení: notebook, desktop, mobil, PDA
 - Široký rozsah hrozeb: Virus, červ, spyware, ... crimeware





Pouze správně vybroušený zámek může otevřít klíč, a pouze správně „vybroušený“ útok může otevřít a infikovat systém

Krok 1: Charakteristika „tvaru“ infekčního vektoru



Krok 2: Využití tvaru jako signatury a zablokování všeho, co ji splňuje

Zcela nové útoky dokážeme blokovat, aniž bychom potřebovali znát kódy

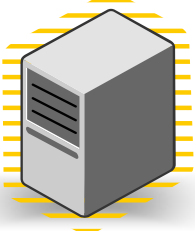
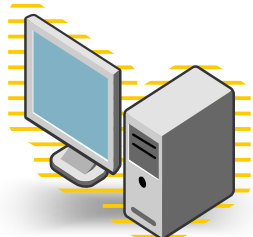
nové
útoky



**Nové útoky vyžadují odchozí komunikaci,
jinak NEPRACUJÍ! To znamená kvalitně
řízený osobní firewall v obousměrném
provozu!**

nová
motivace





Ochrana



Shoda

Politika bezpečnosti konc. bodů

Stav

Anti-Virus Zapnut



Anti-Virus Aktualizován



Osobní Firewall Zapnut



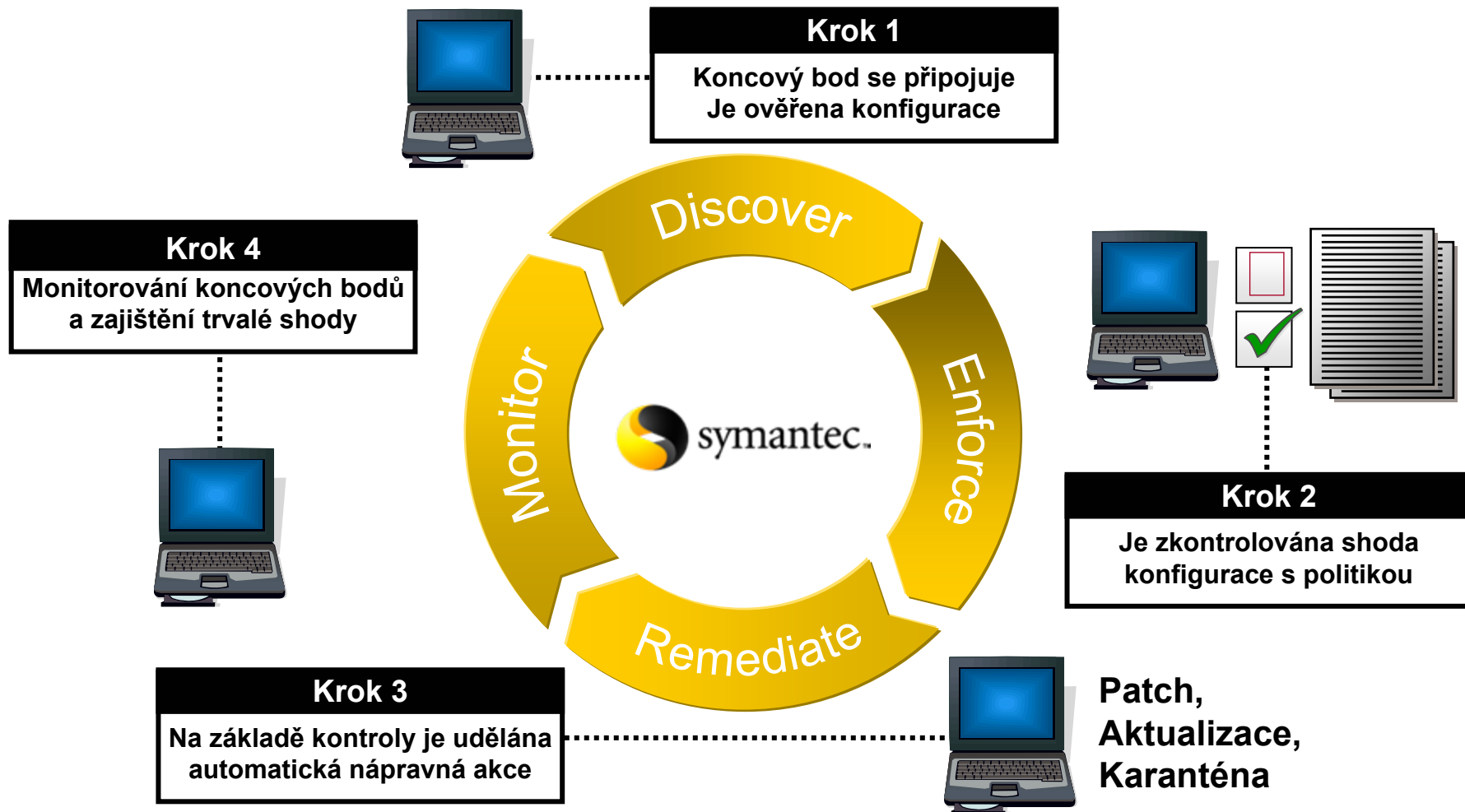
Service Pack Nasazen



Patche Instalován

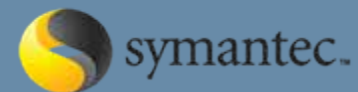


Shoda koncových bodů s politikou



- Datová centra jsou vystavena širokému spektru bezpečnostních hrozeb
 - Co je horší?... Nebezpečný kód ... Nebezpečný uživatel ... Chyba správce ..





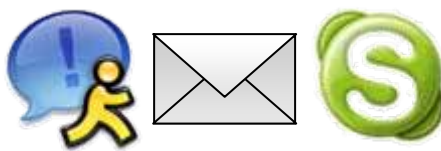
Důvěra v propojeném světě

Ochrana informací a interakcí

- Strukturované informace, které jsou uloženy v databázích
 - Personální záznamy, finanční informace, záznamy o zákaznících
- Nestrukturované informace v poště, na souborových serverech...
 - Zdrojový kód, IT (bezpečnostní) dokumentace, Personální informace
 - Stažené personální záznamy, finanční data, data o obchodech...!



**Souborový
server**

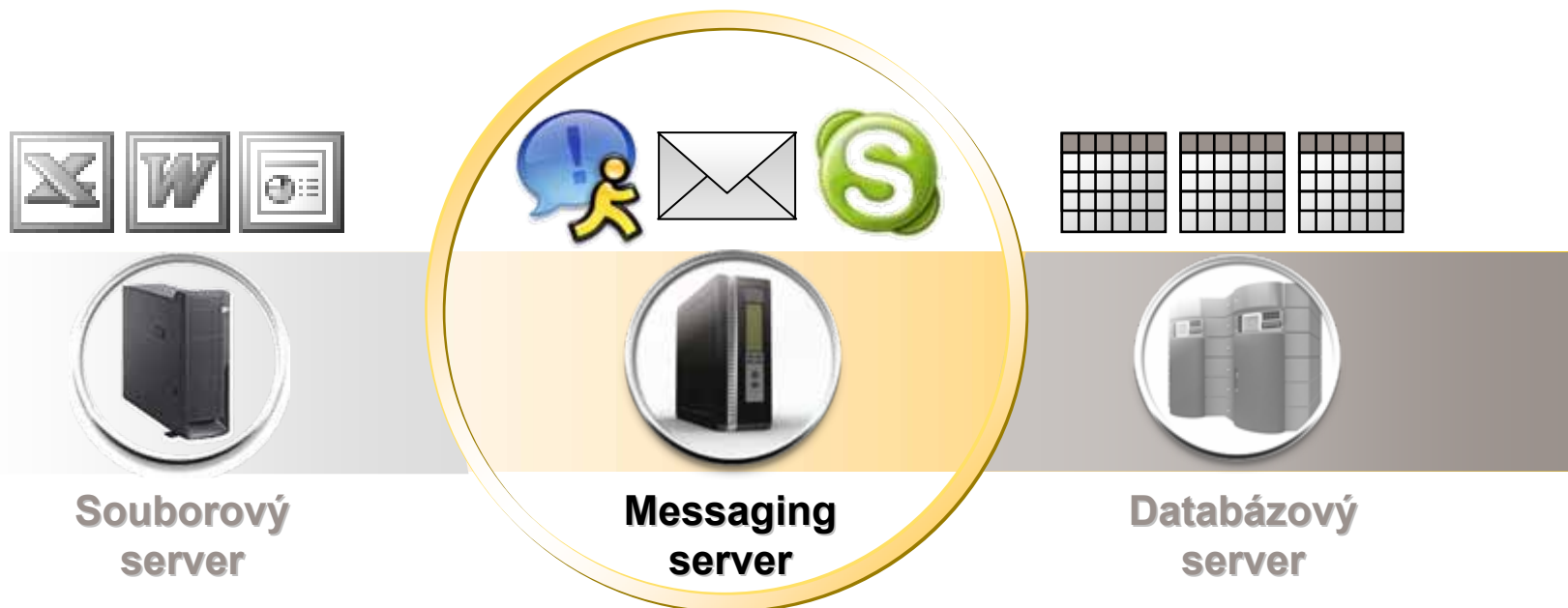


**Messaging
Server**



**Databázový
server**

- Pošta – další aplikace z kategorie „Mission Critical“
 - 75% intelektuálního vlastnictví společností je v poště
 - 80% všech vyšetřování vyžaduje zkoumání obsahu pošty
 - 70% veškeré podnikové pošty je externí nebo interní spam

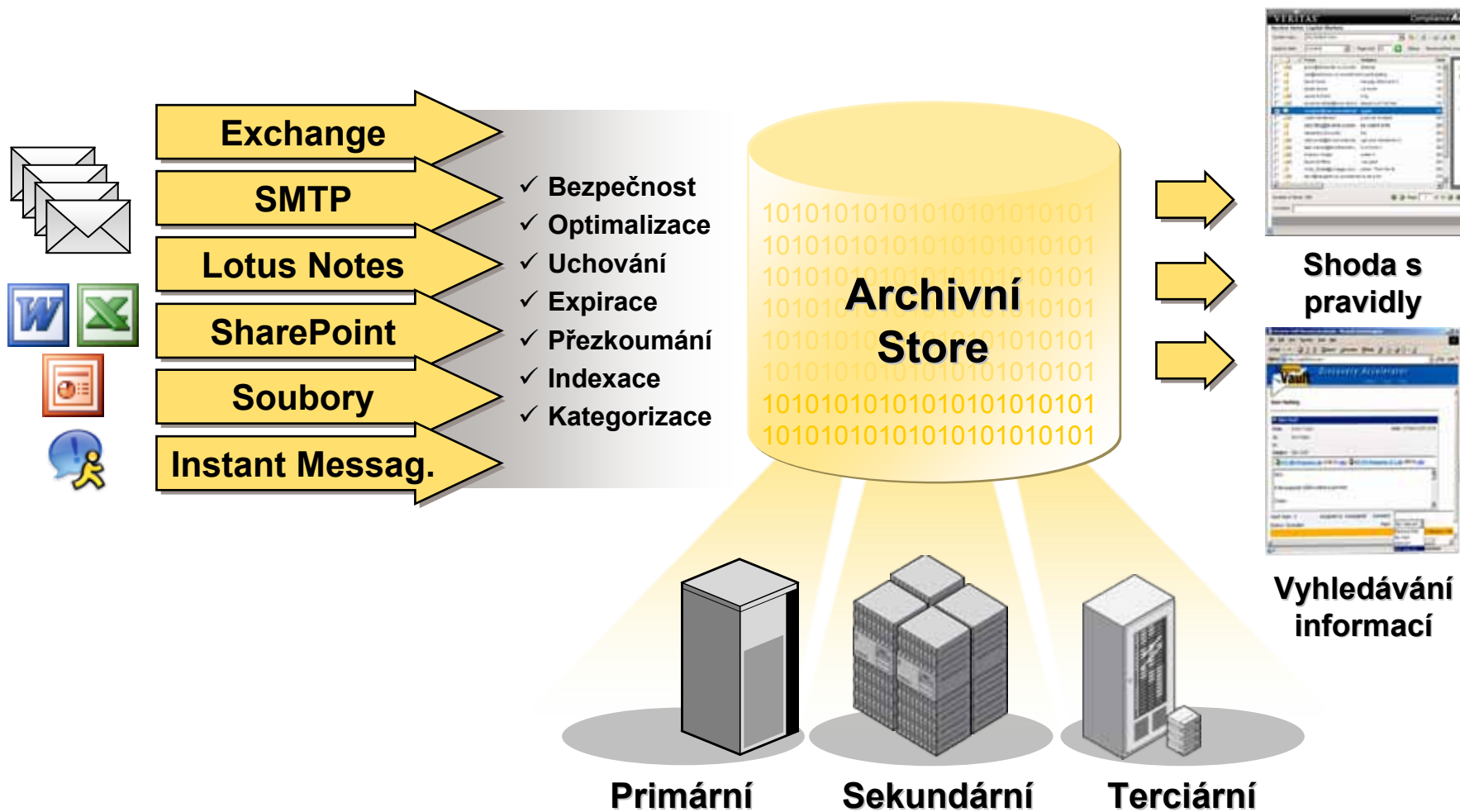


- Dostupná informace je DOBRÁ ale může být **NEBEZPEČNÁ**
- Zabezpečená informace může být **NEDOSTUPNÁ**
- **DOSTUPNÁ A ZABEZPEČENÁ INFORMACE MÁ HODNOTU**



 **Bezpečnost informací**

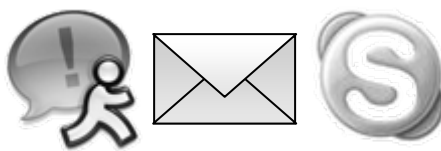
A horizontal bar with a yellow background. It contains four circular icons with a silver border. The first icon contains icons for a person, an envelope, a green 'S', a green 'X', a blue 'W', a red 'E', and two black calendars. The second icon contains icons for a green 'X', a blue 'W', and a red 'E'. The third icon contains icons for an envelope, a blue person, and a green 'S'. The fourth icon contains icons for two black calendars.



- V roce 2005 bylo oficiálně hlášeno 130 velkých průniků do databází
 - 57,000,000 záznamů bylo postiženo (Accenture)
- Hacking, nepoctivost & „nehody“ stojí za 70% těchto problémů
 - 3x se zvýšil jen počet ukradených notebooků...



Souborový server

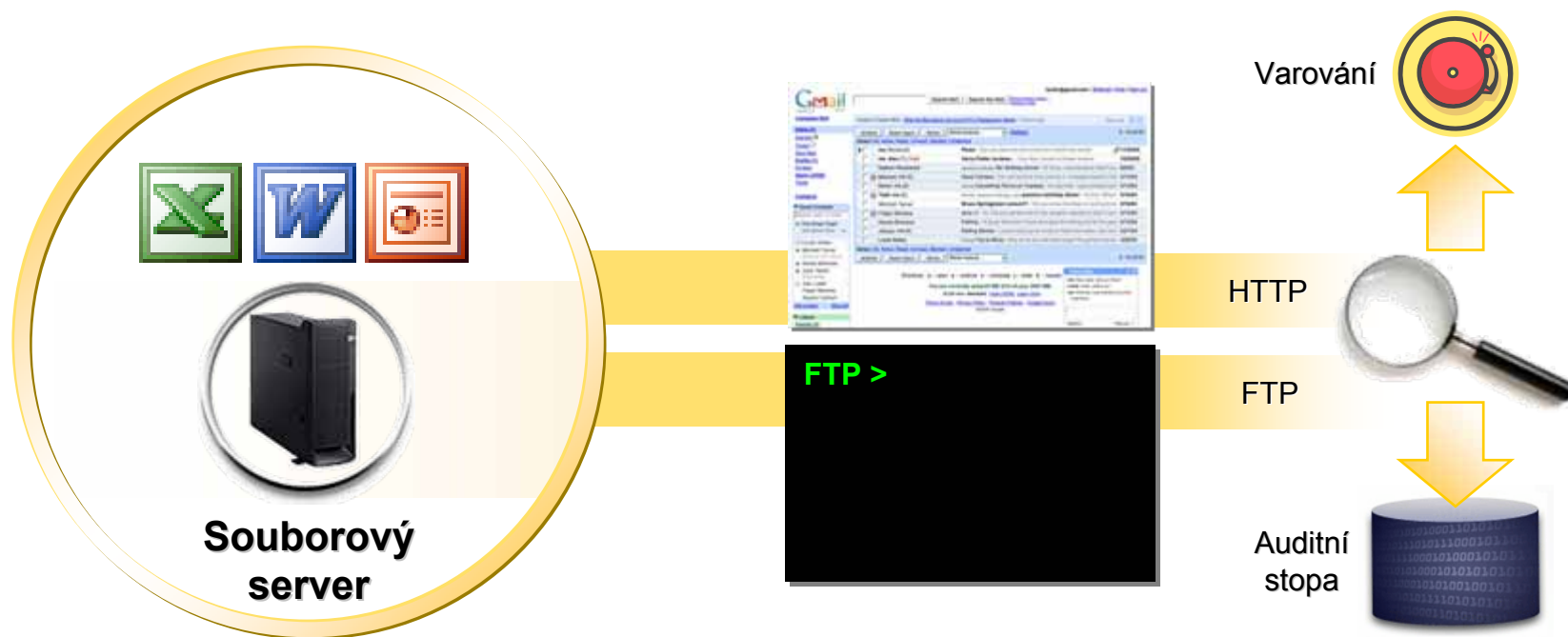


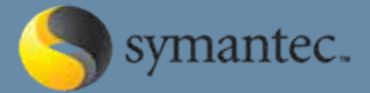
Messaging server



Databázový server

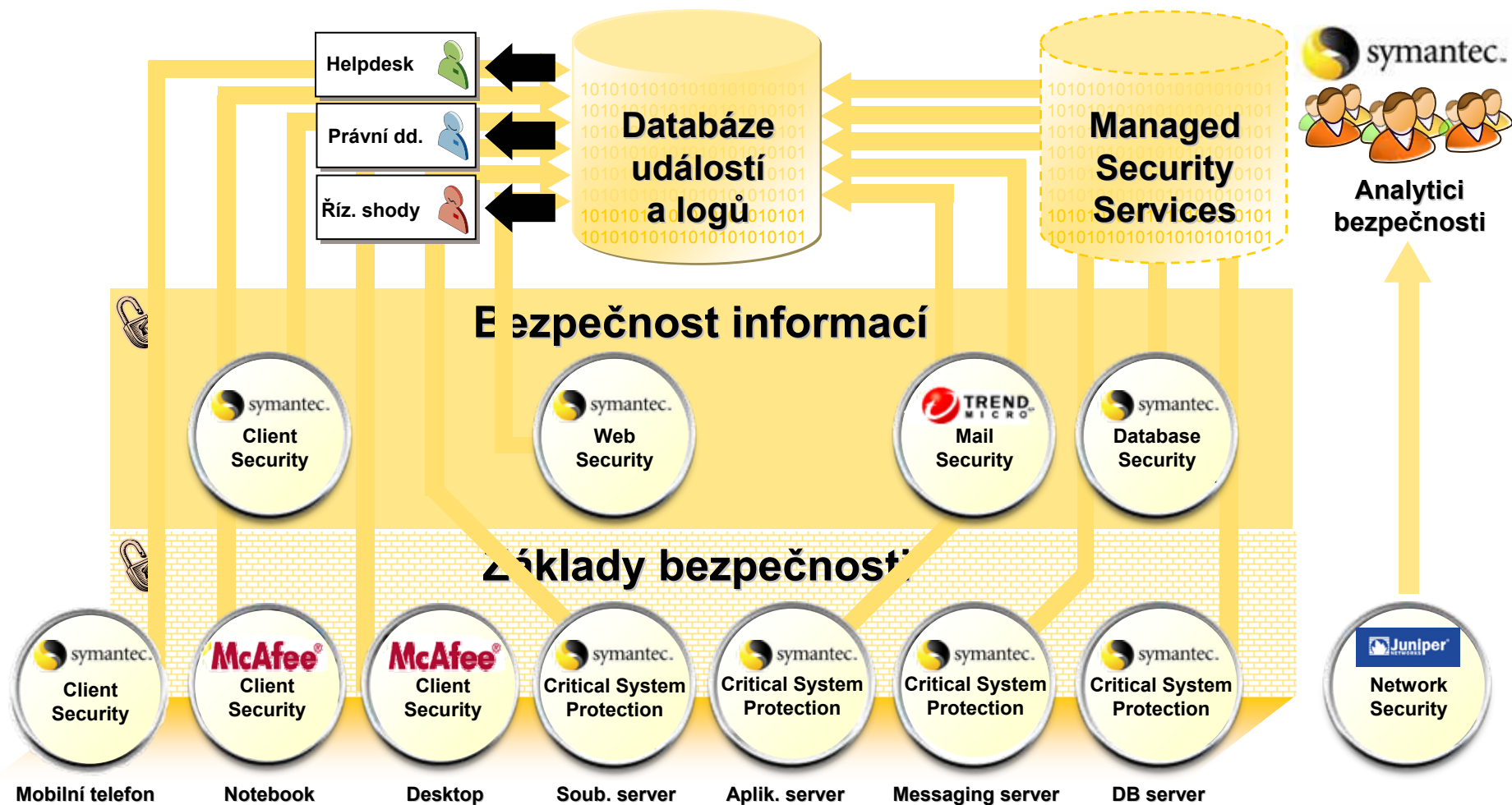
- 1 z každých 50 souborů obsahuje citlivé informace
 - Downloady z ERP systémů, citlivé dokumenty, archivace pošty do PST
- 1 z každých 400 zpráv obsahuje citlivé informace
 - Webmail, FTP ... jakož i standardní podnikové poštovní účty





Důvěra v propojeném světě

Řízení bezpečnosti





Základy bezpečnosti



Mobilní telefon



Notebook



Desktop



Soub. server



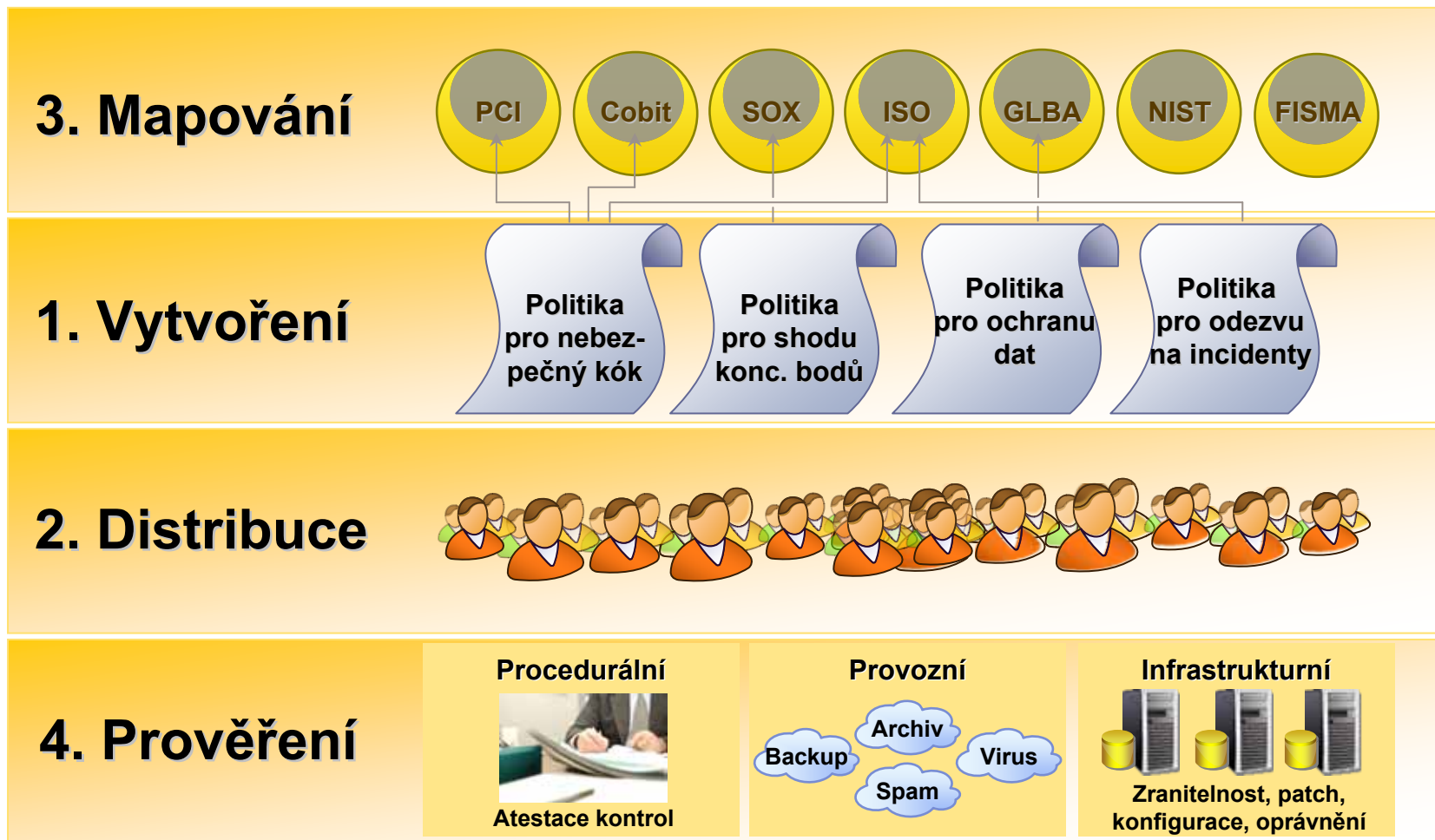
Aplik. server



Messaging server



DB server



Volba
standardu

Reporting

Detekce
odchylek

Náprava

Browse Standards

Name

Built-in (5)

Sec 0 % Compliant Evaluated on Wednesday, August 17, 2005 at 6:08

Sec

Sec

Object Name

AD-DOMAIN\HPOV-FW

AD-DOMAIN\W3K320C

CIS CC-AS Look For: Filter by Find Now Clear

CC-EU

CC-US

CC-US HKU\DEFAULT\Software\Microsoft\SystemCertificates\Root\Protected

CC-US Registry Key Secured?

CC-US HTTP SSL Service Disabled?

CC-US HTTP SSL Service Permissions Restricted?

ICMP Redirects Ignored?

Idle Session Timeout 15 Minutes or Less?

IIS Admin Service Disabled?

IIS Admin Service Permissions Restricted?

Vše

Compliance Center

Standards

Compliance

Statistics

Description

Version

Remediation

0 % Compliant Evaluated on Wednesday, August 17, 2005 at 6:08

Client Name: AD-DOMAIN\HPOV-FW

Control Name: AD-DOMAIN\W3K320C

Compliance | Statistics | Description | Version | Remediation

To set permissions for `%SystemRoot%\regedit.exe`:

1. Select **Start>Run** to open the **Run** dialog.
2. Enter **mmc** in the **Open** text box.
3. Click **OK** to open the **Microsoft Management Console**.
4. Select **File>Add/Remove Snap-in** to open the **Add/Remove Snap-in** dialog.
5. Click **Add** on the **Standalone** tab to open the **Add Standalone Snap-in** dialog.
6. Select **Security Templates** from the **Available Standalone Snap-ins** list.

Express Value: Automatic for IISADMIN

The following accounts are missing required permissions:
System, INTERACTIVE. **FAIL**



Řízení bezpečnosti



Bezpečnost informací



Základy bezpečnosti



Mobilní telefon



Notebook



Desktop



Soub. server



Aplik. server



Messaging server



DB server



Důvěra v propojeném světě



DĚKUJI za pozornost ...