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

symantec™

Důvěra v propojeném světě

symantec.

Bezpečnost v2.0

Dnešní realita.....

- 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?

Otázka důvěry

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.

Černý trh s informacemi

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

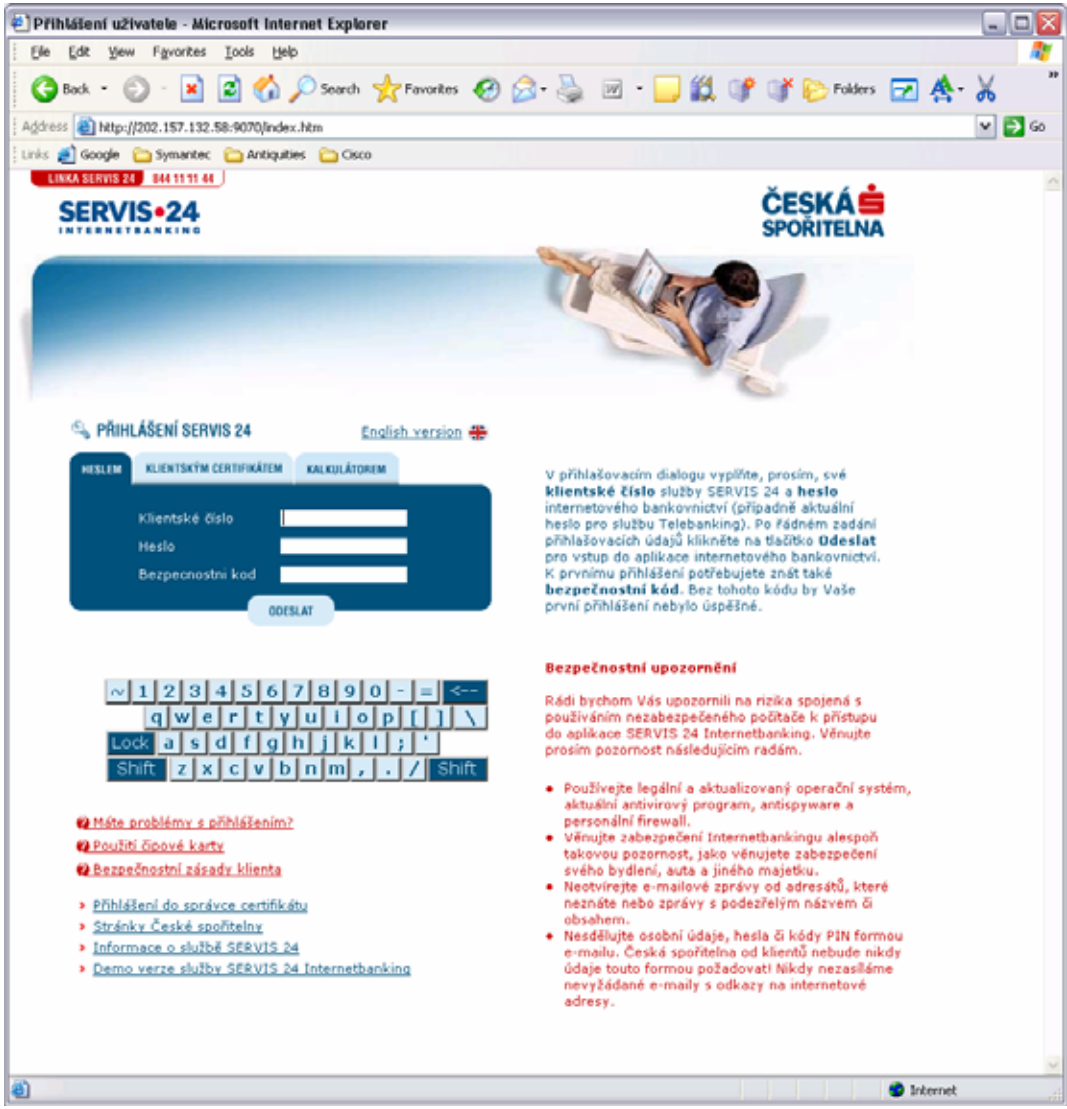
If your order > 50$, u will get a calling card with 5$

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

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

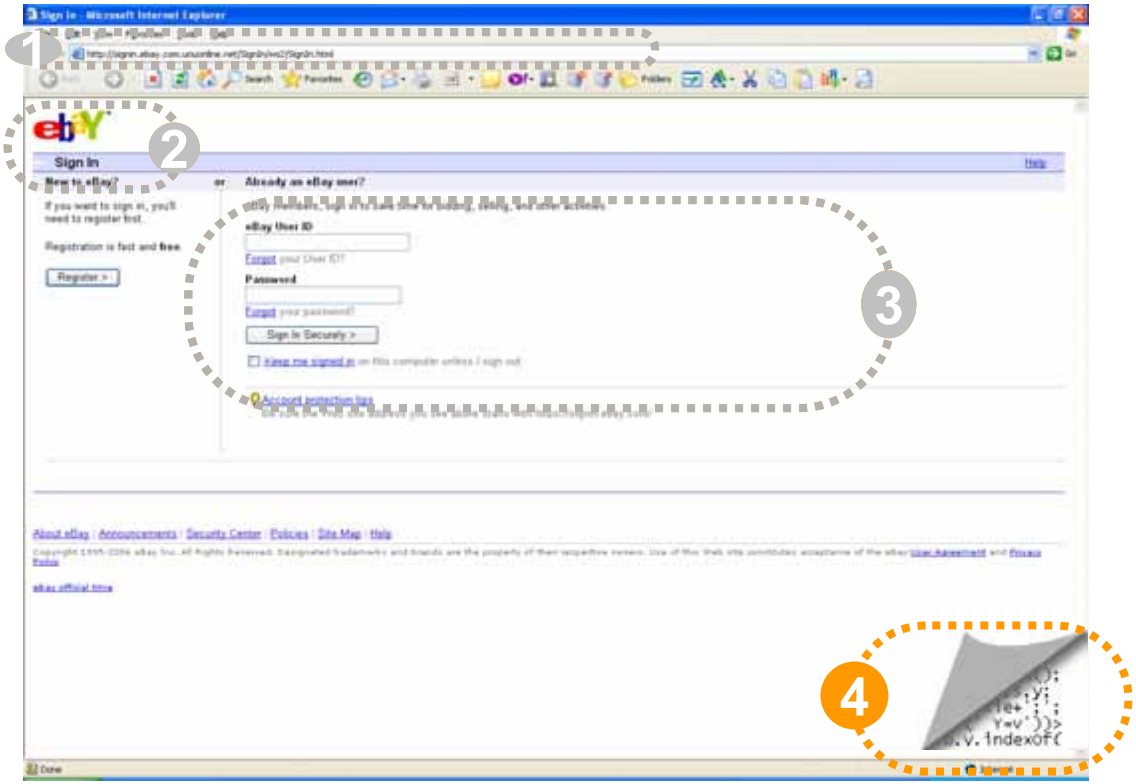
Česká spořitelna

- 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)



Výrazem změny jsou i řešení....

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



1 URL analýza

2 Analýza obsahu

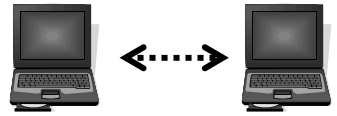
3 Analýza vzhledu

4 Analýza zdroje

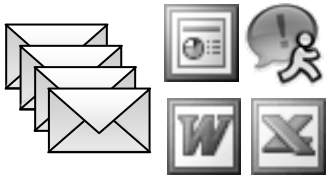
Symantec Confidential Online

Koncepce bezpečnosti v2.0

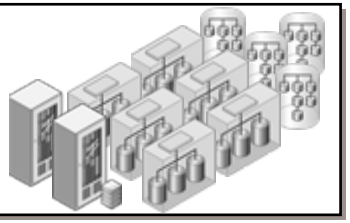
Ochrana interakcí



Ochrana informací

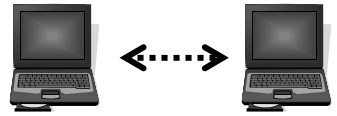


Ochrana infrastruktury



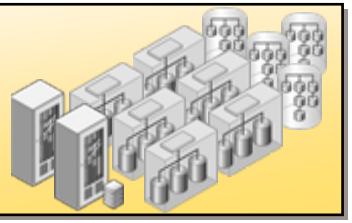
Základem je bezpečnost infrastuktury

Ochrana interakcí



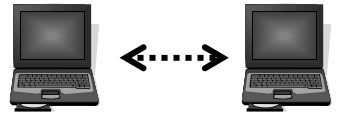
Ochrana informací

Ochrana infrastruktury



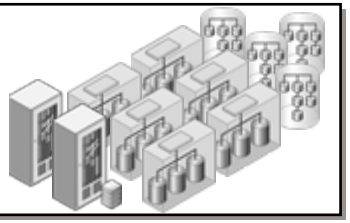
Klíčové je zaměření na ochranu informací

Ochrana interakcí



Ochrana informací

Ochrana infrastruktury

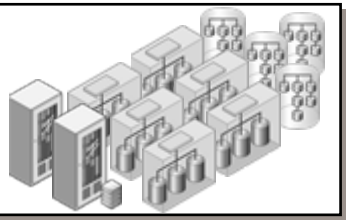


To znamená i bezpečné interakce s nimi

Ochrana interakcí

Ochrana informací

Ochrana infrastruktury



Kompletní řešení je podmínkou...

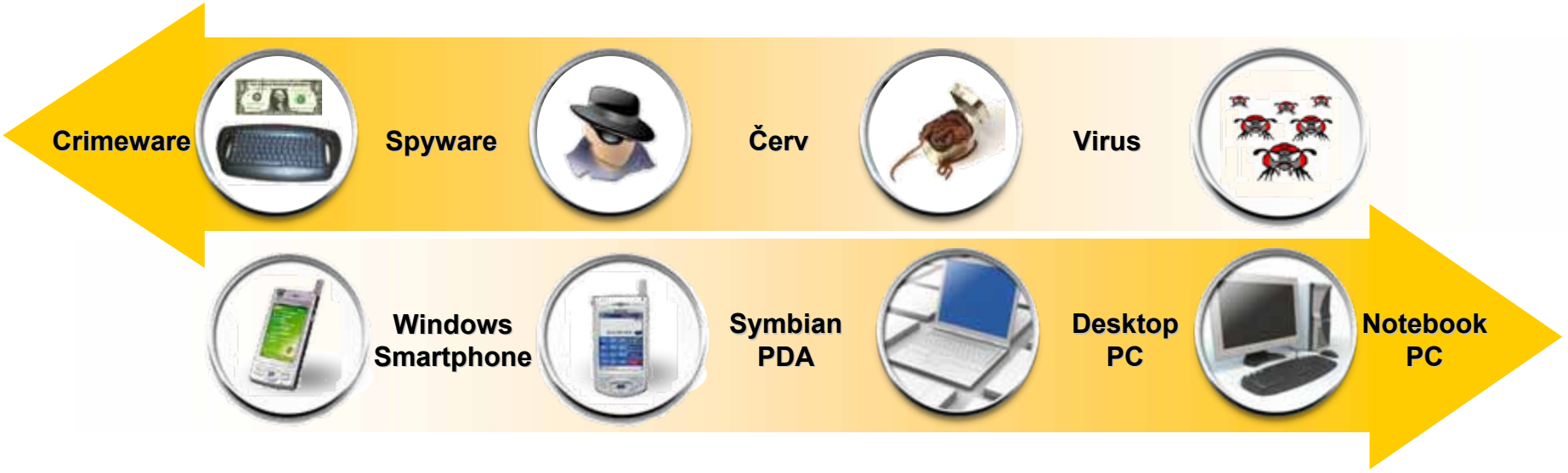
... a jeho součástí je i řízení bezpečnosti

Důvěra v propojeném světě

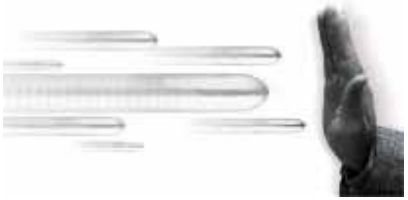
Ochrana infrastruktury

Ochrana před nebezpečnými kódy

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

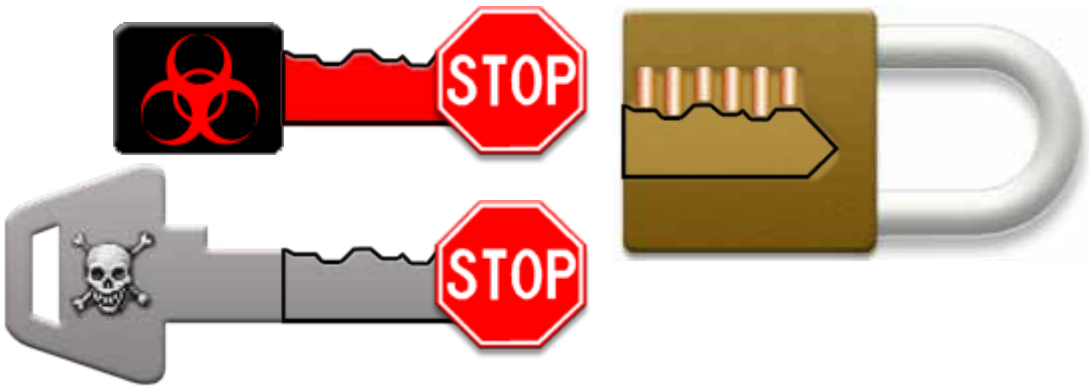


Ochrana v nulových hodinách



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

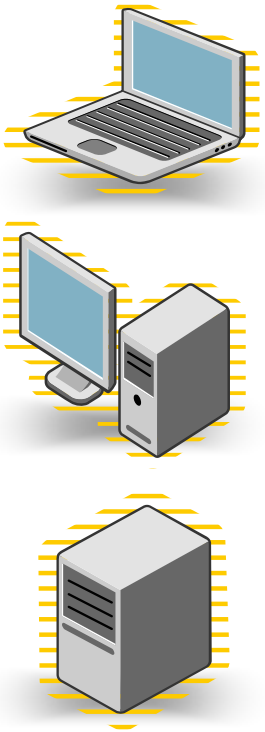
Odchozí komunikace

nové **útoky**

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

nová **motivace**

Kontrola přístupu k síti



Ochrana

Viry

Trojany

Neznámé útoky

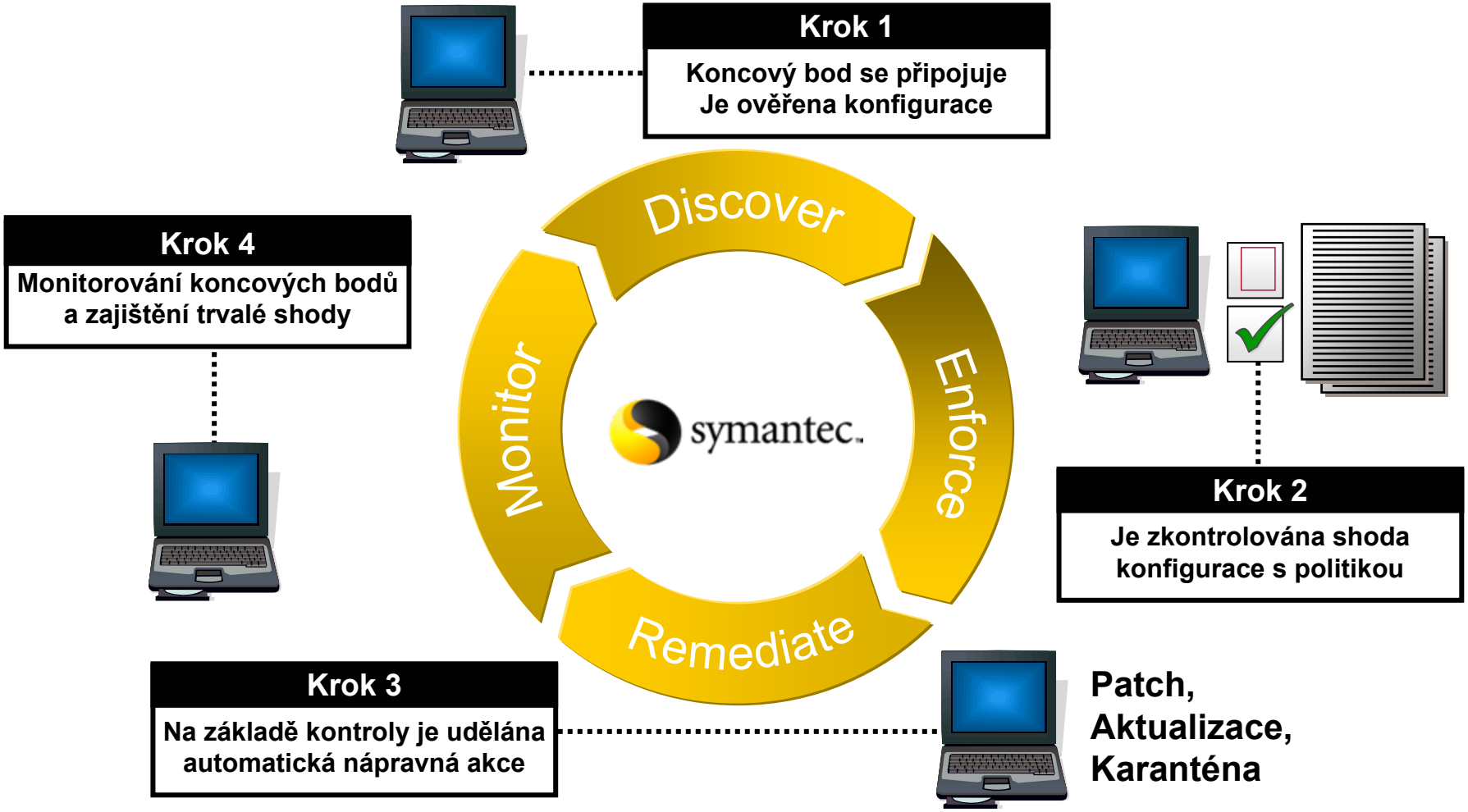
Červy

Spyware

Shoda

Politika bezpečnosti konc. bodů	Stavs
Anti-Virus Zaplnut	✓
Anti-Virus Aktualizován	✓
Osobní Firewall Zapnut	✓
Service Pack Nasazen	✓
Patche Instalován	✓

Shoda koncových bodů s politikou



I servery jsou koncovými body

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

symantec.

Důvěra v propojeném světě

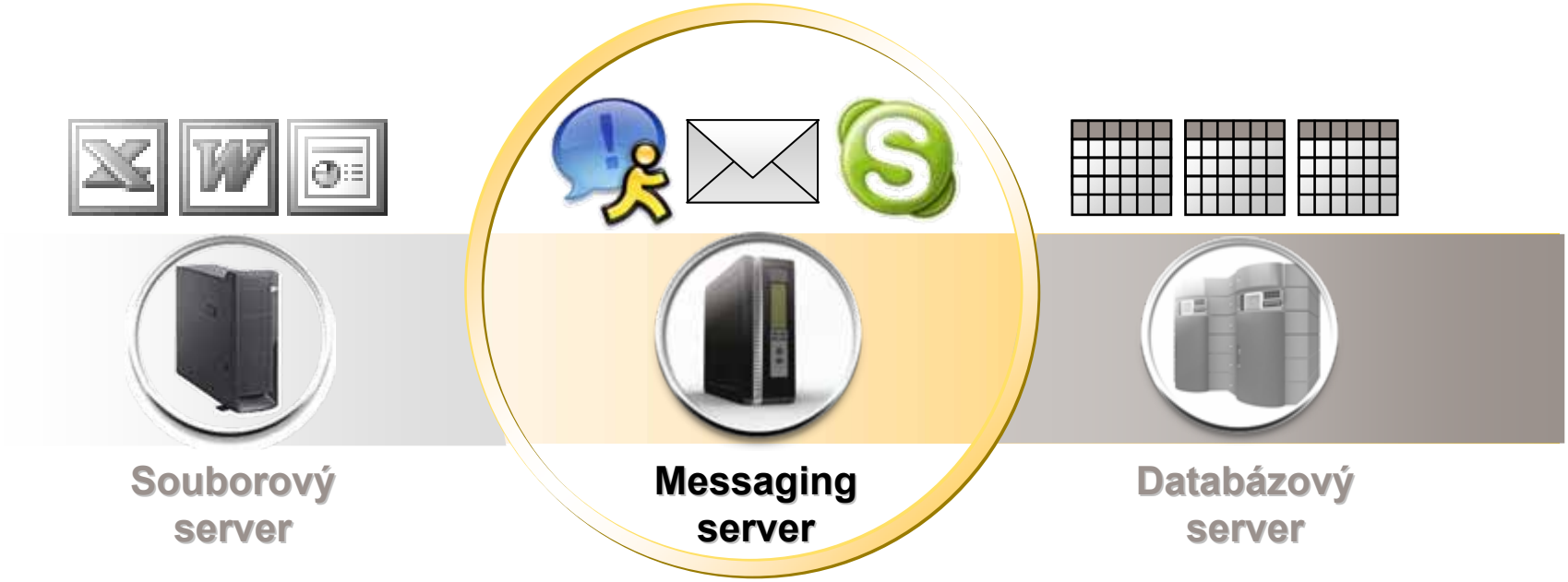
Ochrana informací a interakcí

Dostupné a bezpečné informace

- 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...!

Informační rizika v messaging systémech

- 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

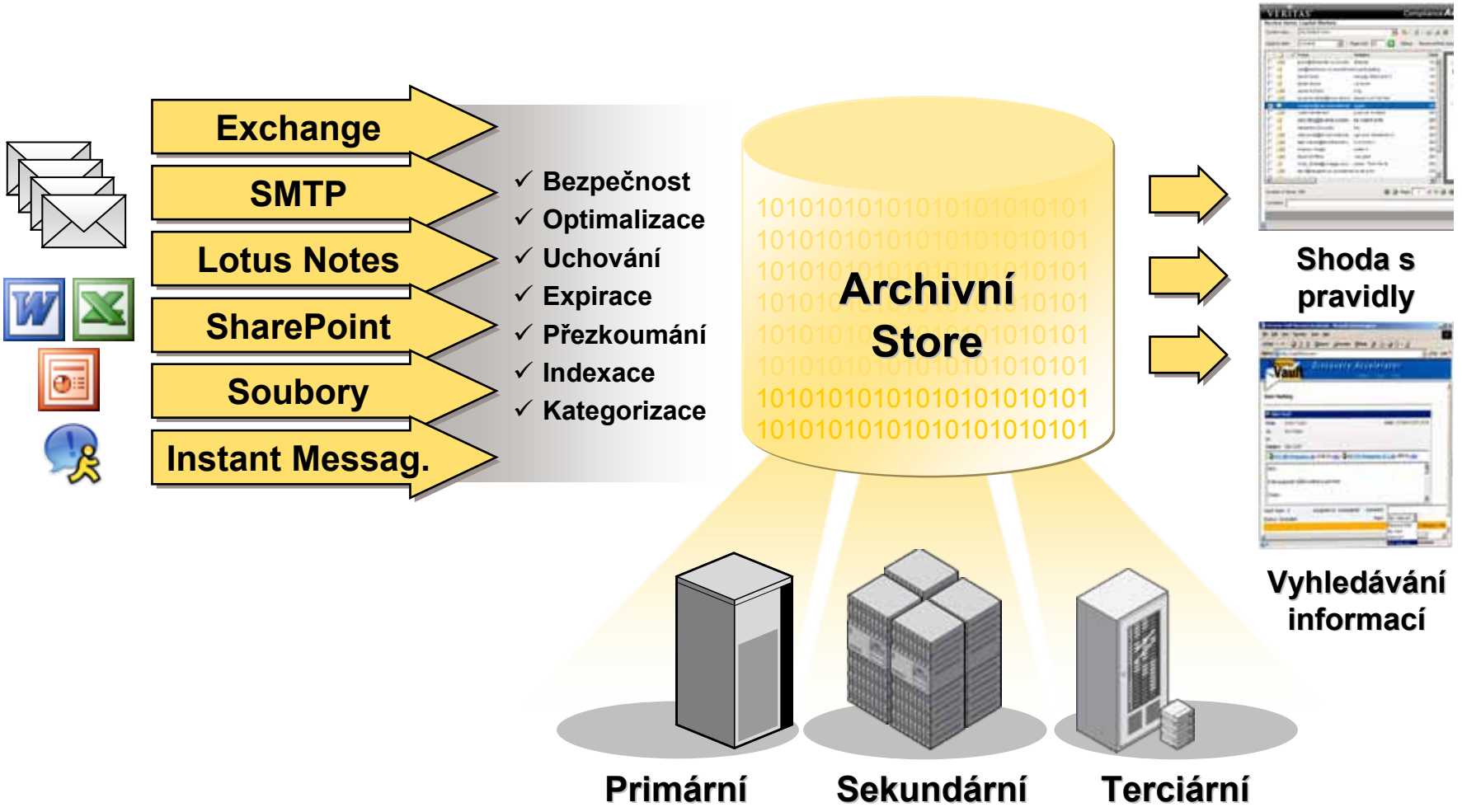


Symantec Mail Security – Nežádoucí venku

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

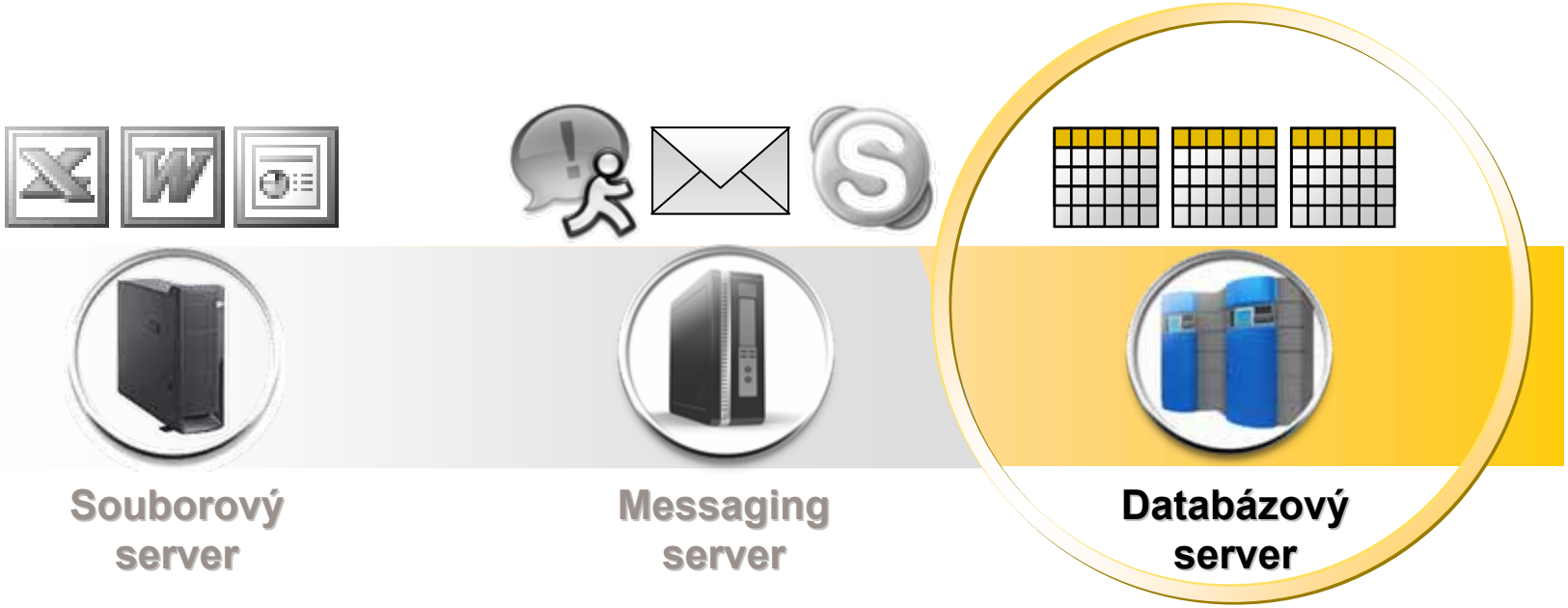
Archivace a bezpečnost

Archiv : Uložení, uchování & vyhledávání



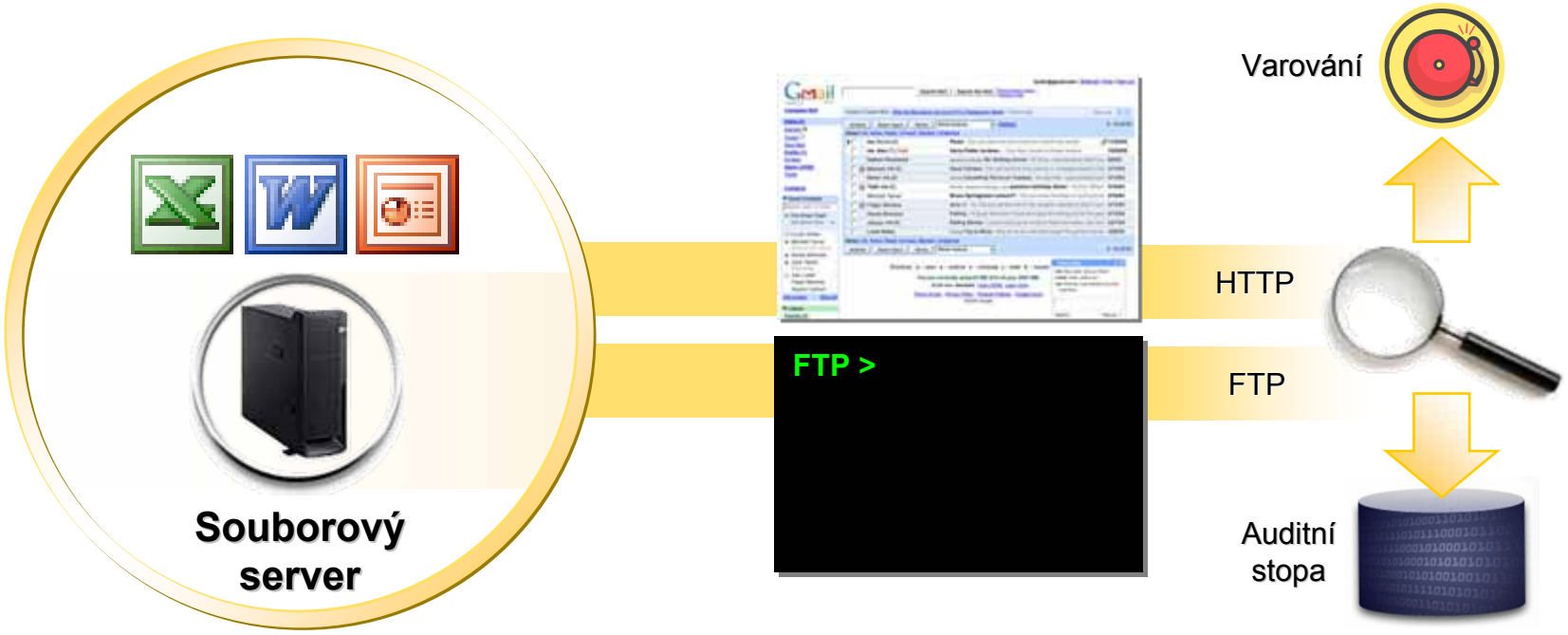
Ochrana databázových systémů

- 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...



Informační rizika v uživatelských souborech

- 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

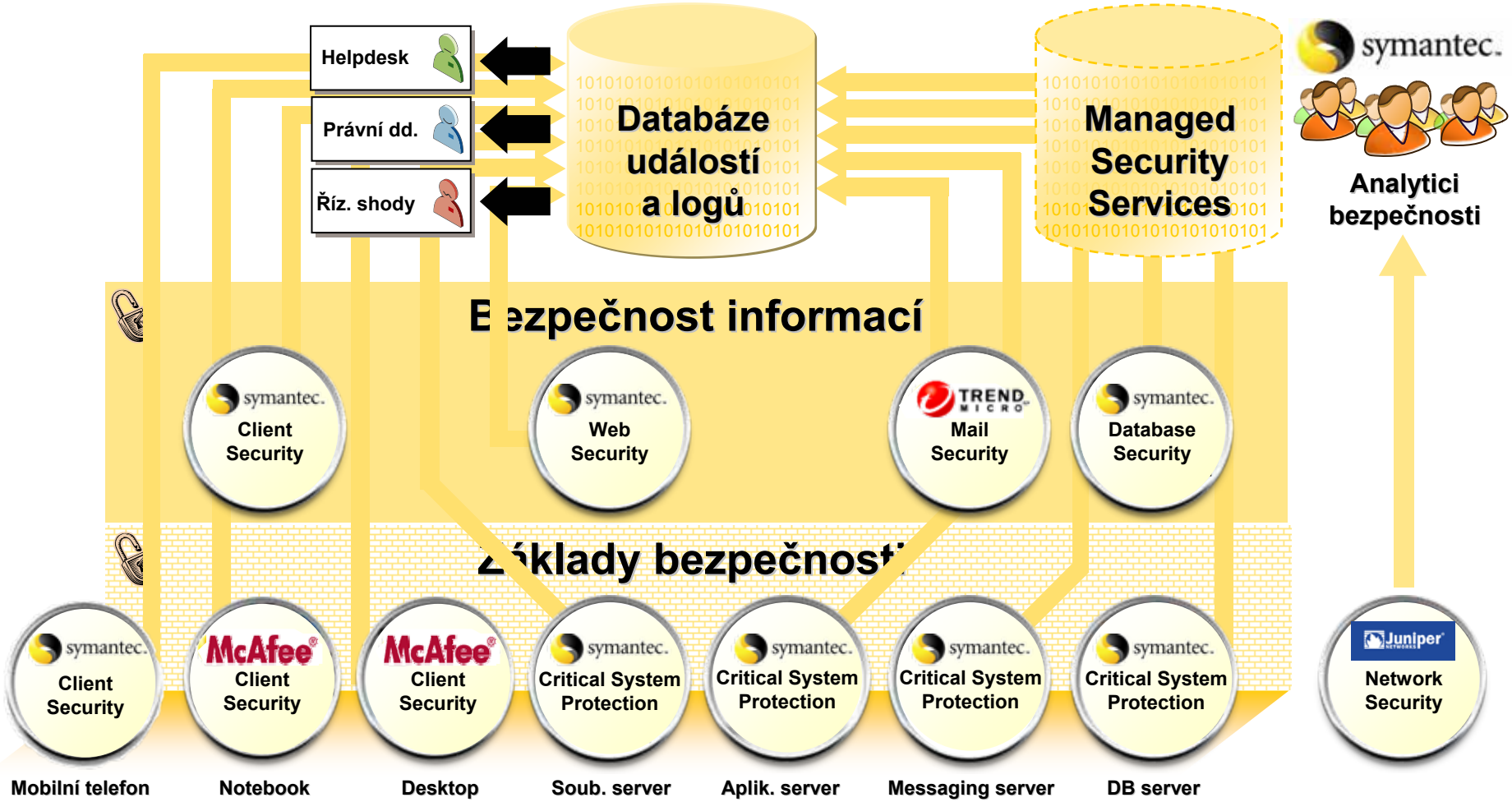


symantec.

Důvěra v propojeném světě

Řízení bezpečnosti

Řízení bezpečnostních událostí a incidentů



Řízení zranitelností systémů a aplikací

Řízení shody s politikami

3. Mapování

PCI | Cobit | SOX | ISO | GLBA | NIST | FISMA

1. Vytvoření

- Politika pro nebezpečný kód
- Politika pro shodu konc. bodů
- Politika pro ochranu dat
- Politika pro odezvu na incidenty

2. Distribuce

4. Prověření

Procedurální

Atestace kontrol

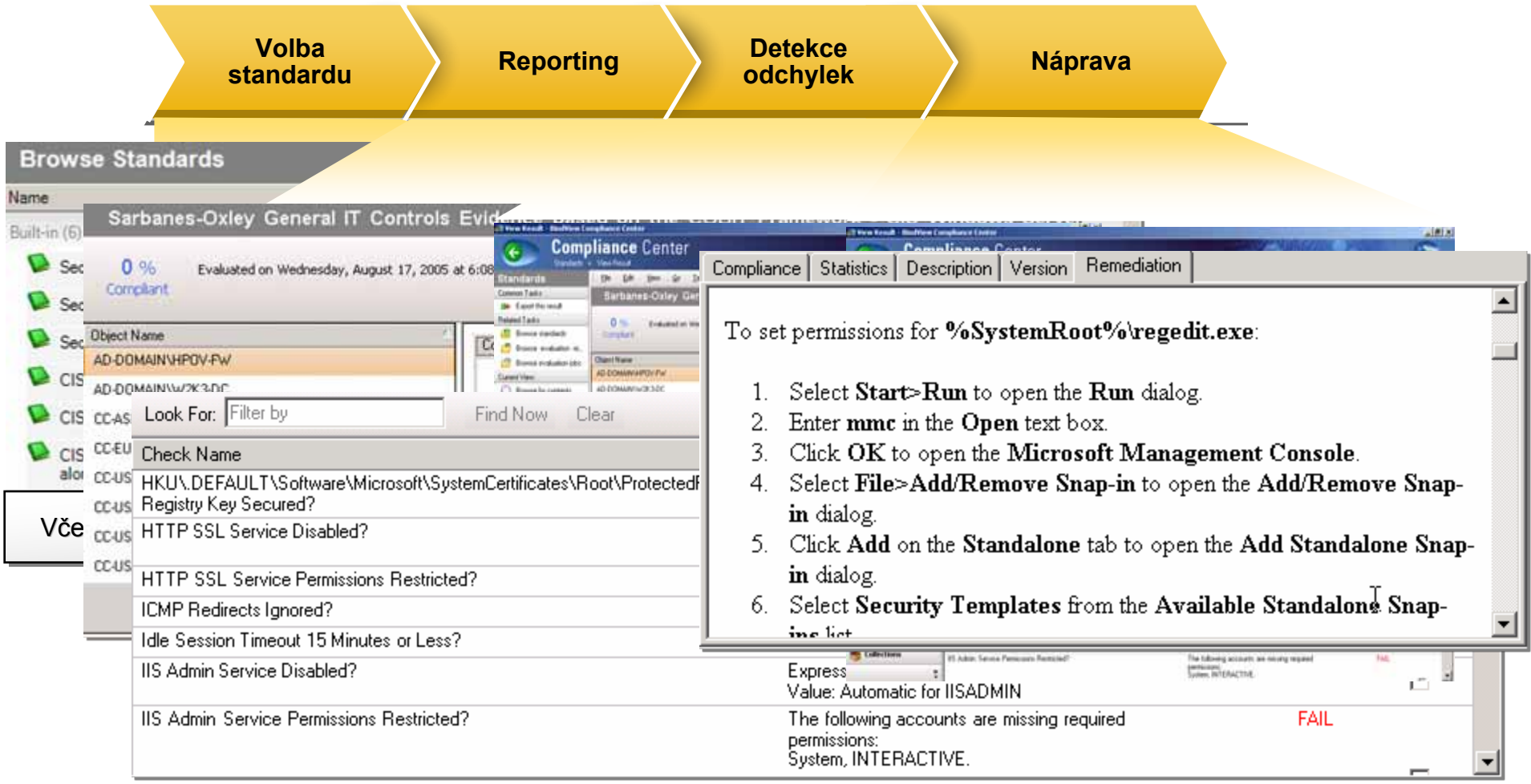
Provozní

Backup | Archiv | Virus | Spam

Infrastrukturní

Zranitelnost, patch, konfigurace, oprávnění

Shrnutí kontrolního cyklu



Pokrytí kompletní bezpečnostní strategie

symantec™

Důvěra v propojeném světě

DĚKUJI za pozornost …