KPMG

Jaké bezpečnostní problémy můžeme očekávat

Jiří Vondrášek

Prezentace na konferenci Security 2010

AUDIT ▪ TAX ▪ ADVISORY

Úvod

Jak můžeme charakterizovat současnost

- Současné IS jsou závislé na produktech několika výrobců
- Často spoléháme na výrobce a jejich bezpečnostní opravy
- Nemáme zdroje na zjištění zranitelností vlastními silami
- Informace o zranitelnostech a odhalených bezpečnostních nedostatcích se rychle šíří a útočníci/průnikáři je dokáží obratem využít
- Neumíme se předem patřičně připravit protože nevíme na co

Zdroje informací o zranitelnostech a odhalených bezpečnostních nedostatcích

- **informační služby specializovaných pracovišť jednotlivých výrobců**
  - Microsoft Security Advisories (http://www.microsoft.com/technet/security/advisory/default.mspx)
  - Bugzilla@Mozilla (http://bugzilla.mozilla.org/query.cgi)
  - Apple security updates (http://support.apple.com/kb/HT1222)
  - Oracle Technology Network Critical Patch Updates and Security Alerts (http://www.oracle.com/technology/deploy/security/alerts.htm)
  - další…

Zdroje informací o zranitelnostech a odhalených bezpečnostních nedostatcích

- **Informační služby specializovaných nezávislých organizací/agentur**
  - Security Focus (http://www.securityfocus.com/vulnerabilities)
  - National Vulnerability Database (http://nvd.nist.gov/home.cfm)
  - CoreLabs IT Security Research: Vulnerability Advisories (http://www.coresecurity.com/content/corelabs-advisories)
  - Internet Storm Center - SANS Institute (http://isc.sans.org/newssummary.html)
  - Security Tracker (http://www.securitytracker.com/startup/index.html)
  - US-CERT Technical Cyber Security Alerts (http://www.us-cert.gov/cas/techalerts/)
  - a další …

Praktické problémy s využitím informačních zdrojů

1. problém — Mám jistotu, že jsem z dostupných zdrojů schopen včas získat informace o všech zranitelnostech a odhalených bezpečnostních nedostatcích, které jsou relevantní k situaci, ve které se nachází informační systém, za jehož bezpečnost jsem zodpovědný?

2. problém — Jsou informace o zranitelnostech a odhalených bezpečnostních nedostatcích relevantní k produktům, které jsou použity v informačním systému, za jehož bezpečnost jsem zodpovědný?

3. problém — Jak zamezit zneužití zranitelností a bezpečnostních nedostatků zjištěných touto cestou v informačním systému, za jehož bezpečnost jsem zodpovědný?

4. problém — Jak závažné mohou být dopady, pokud se zranitelnost nebo odhalený bezpečnostní nedostatek vyskytuje v informačním systému, za jehož bezpečnost jsem zodpovědný?

5. problém — Mohu se nějak efektivně připravit na budoucí ještě neodhalené zranitelnosti a bezpečnostní nedostatky?

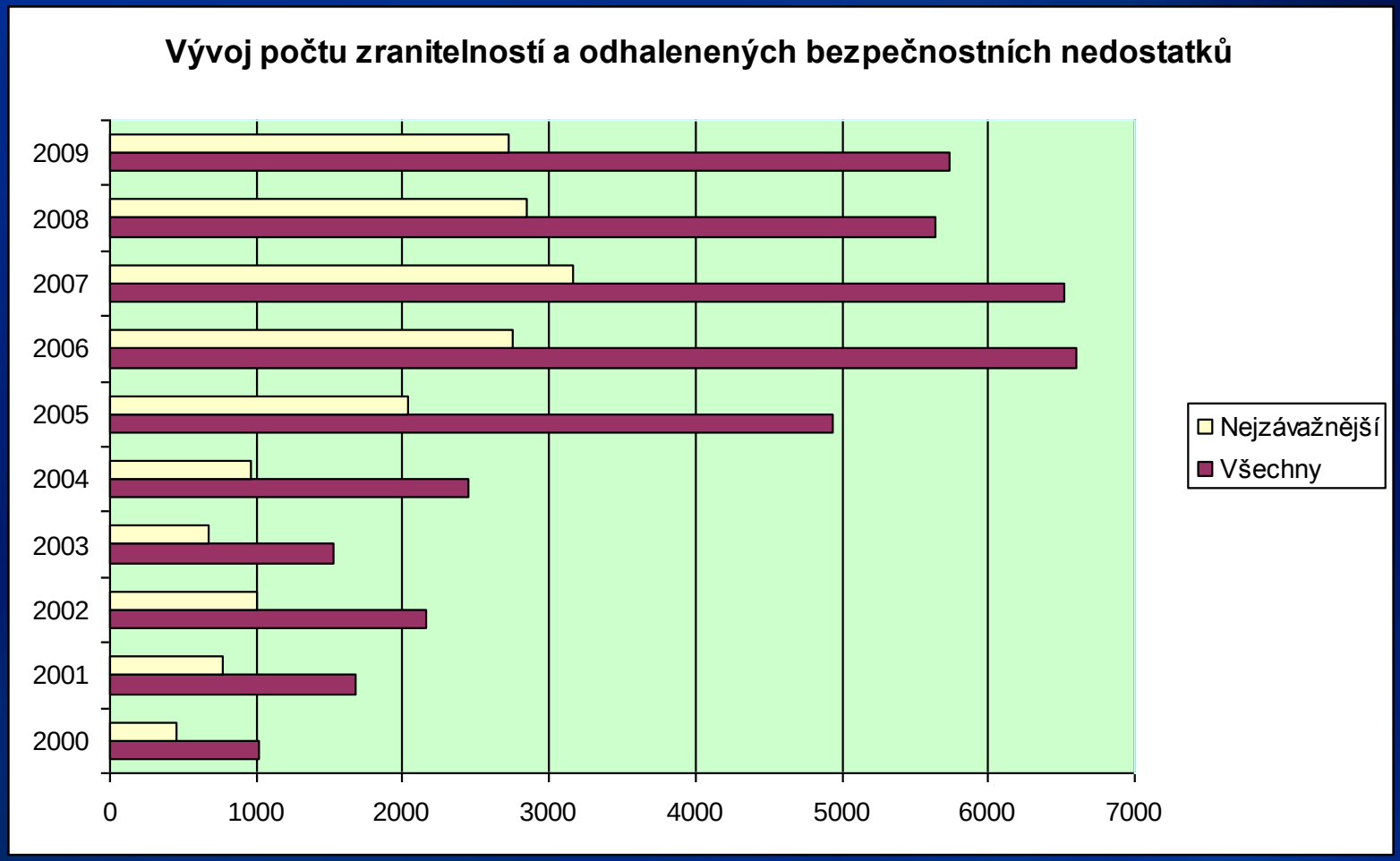
Východiska pro využití informačních zdrojů

- Systém označování zranitelností a odhalených bezpečnostních nedostatků - Common Vulnerabilities and Exposures (CVE) (http://cve.mitre.org/cve/index.html)
- Jmenný systém pro označování komponent informačních systémů, platforem a balíků Common platform enumeration (CPE) (http://cpe.mitre.org/)
- Vyhledávání zranitelností a bezp. nedostatků přes CPE,
- Každý vyhledaný záznam je identifikován pomocí CVE
- Klasifikace zranitelnosti a bezpečnostní nedostatky podle typů slabin - Common Weakness Enumeration (CWE) (http://nvd.nist.gov/cwe.cfm)
- Systém oceňování závažnosti zranitelností a bezpečnostních nedostatků Common Vulnerability Scoring System (http://nvd.nist.gov/cvss.cfm)

Trendy zranitelností a odhalených bezpečnostních nedostatků

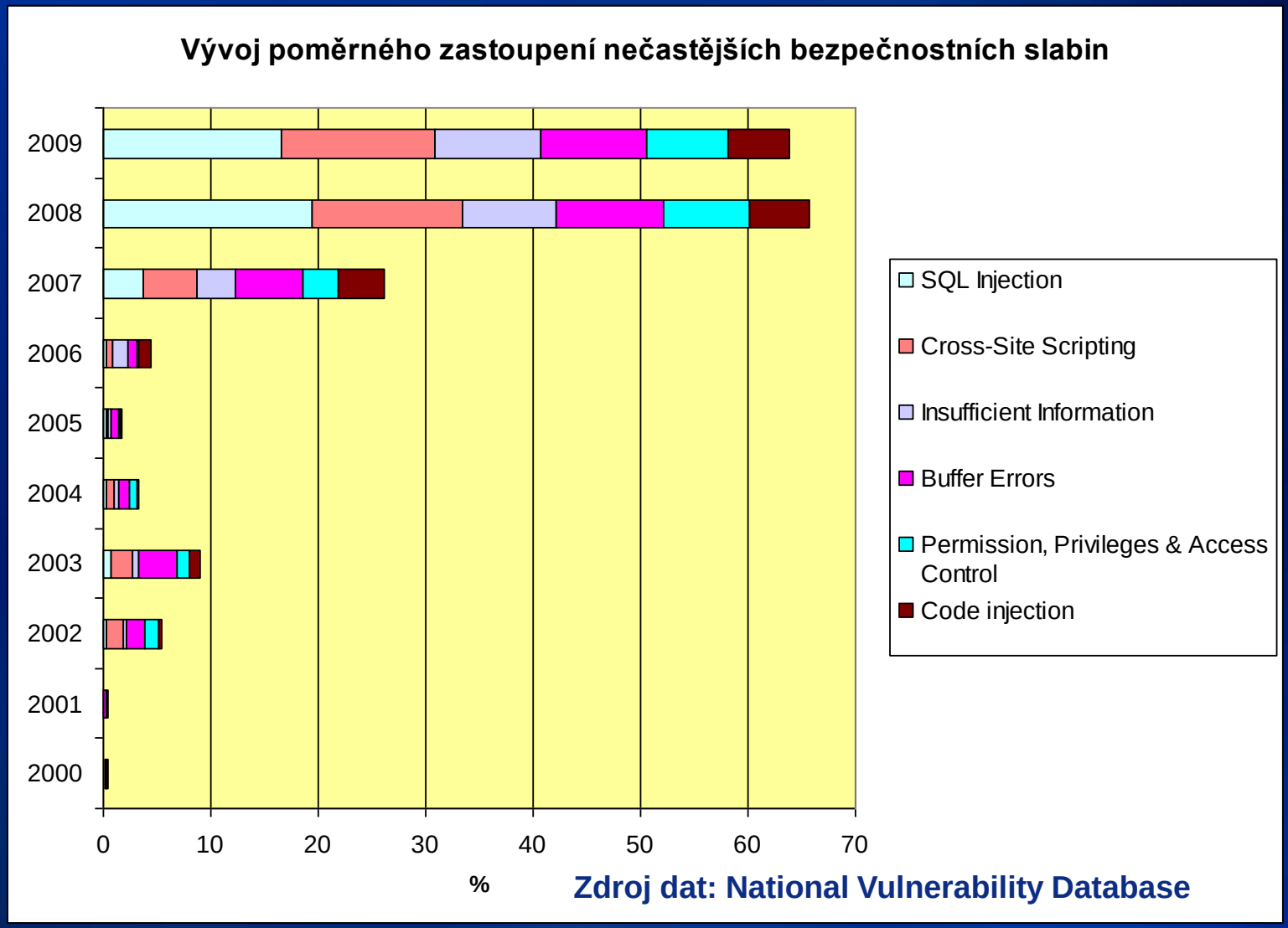
- Poznání trendů může pomoci při přípravě správného zvládnutí budoucích ještě neodhalených zranitelností a bezpečnostní nedostatků.

Trend: prakticky polovina zranitelností je hodnocena stupněm nejzávažnější

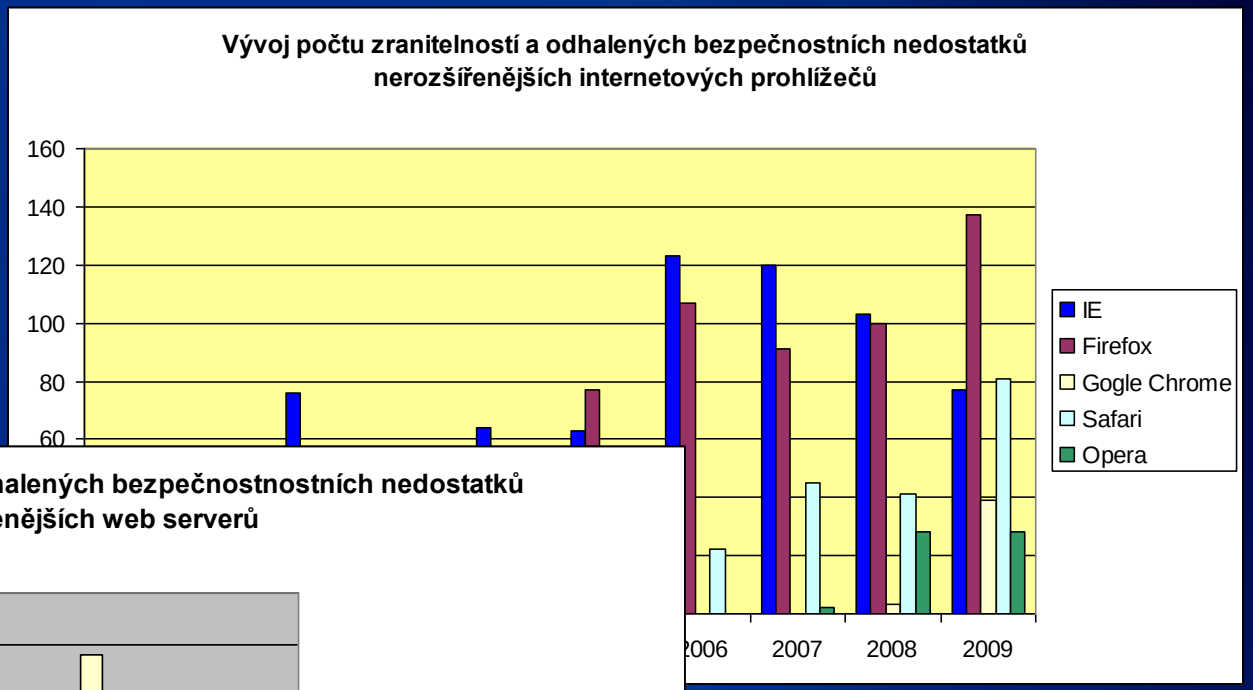


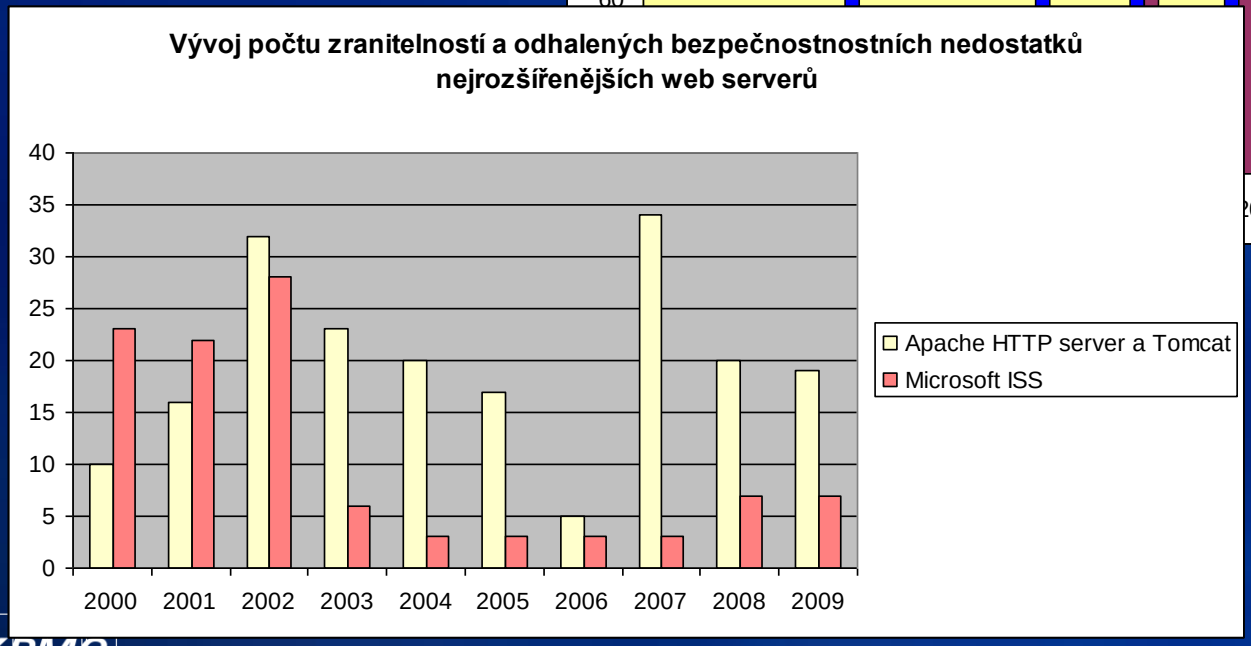
Zdroj dat: National Vulnerability Database

Trend: Jen 6 bezpečnostních slabin se dnes podílí na 65% všech zveřejněných zranitelností



Trend: každý týden je možné očekávat zveřejnění významné zranitelnosti, která postihne váš IS

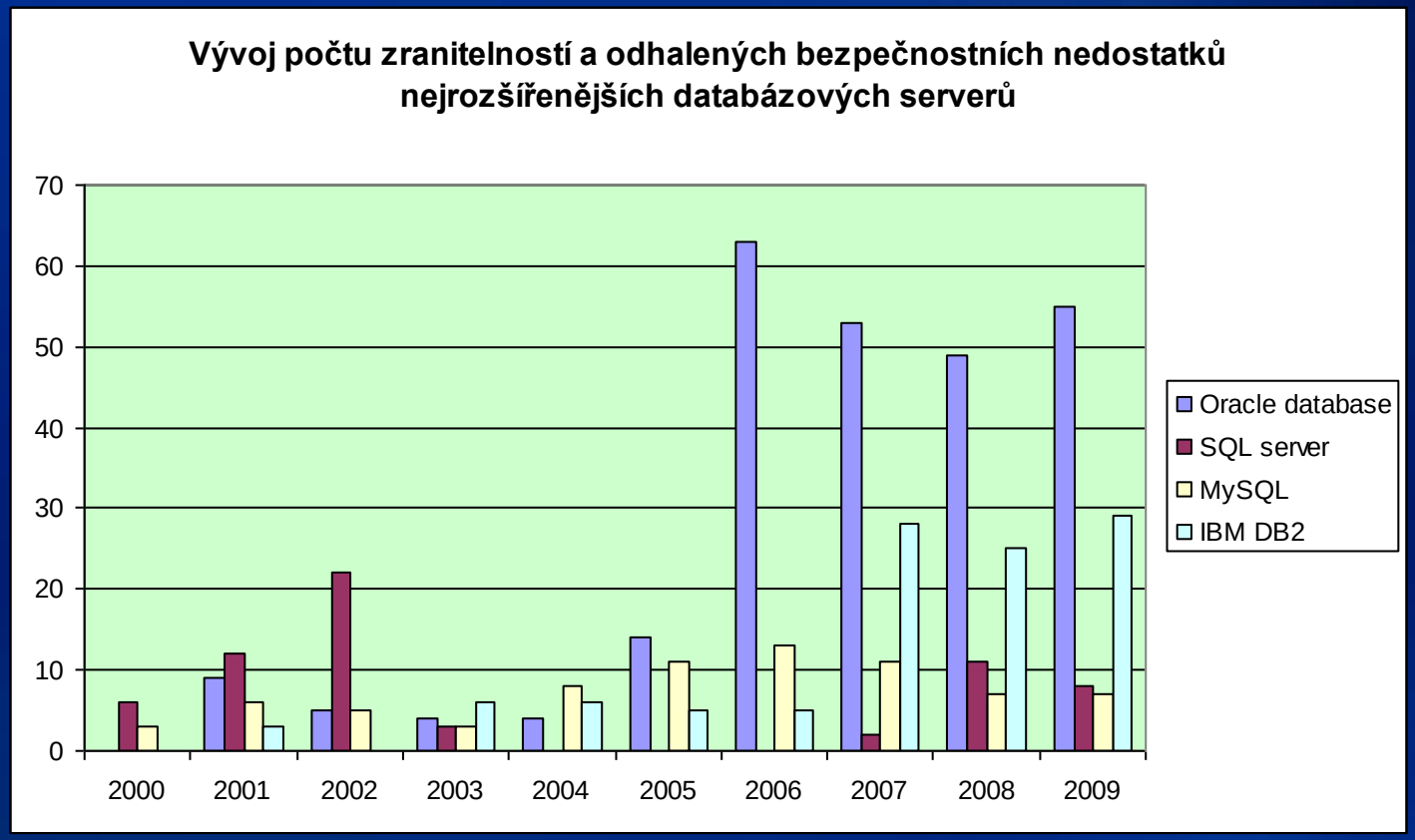




Zdroj dat: National Vulnerability Database

Trend: každý týden je možné očekávat zveřejnění významné zranitelnosti, která postihne váš IS

pokračování



Zdroj dat: National Vulnerability Database

Doporučení

- Je potřeba sledovat a vyhodnocovat informace o nových zranitelnostech a bezpečnostních nedostatcích minimálně jednou měsíčně a nejlépe každý týden, jedině tak lze zajistit přiměřenou a včasnou reakci.

- Pokud nesledujete a nevyhodnocujete informace o veřejně známých zranitelnostech a odhalených bezpečnostních nedostatcích, je jedno, kolik prostředků vynakládáte na bezpečnostní protiopatření. Je třeba si uvědomit, že informace o zranitelnostech a odhalených bezpečnostních nedostatcích se v komunitě průnikářů velmi rychle šíří a ti neváhají je použít.

Jiří Vondrášek

KPMG Česká republika, s.r.o.

+420 222 123 210

jirivondrasek@kpmg.cz

www.kpmg.cz