

# Jaké bezpečnostní problémy můžeme očekávat

Jiří Vondrášek

Prezentace na konferenci Security 2010

# 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 nedostacích 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 nedostacích

- **informační služby specializovaných pracovišť jednotlivých výrobců**
  - Microsoft Security Advisories (<http://www.microsoft.com/technet/security/advisory/default.msp>)
  - 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 nedostacích

- **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?

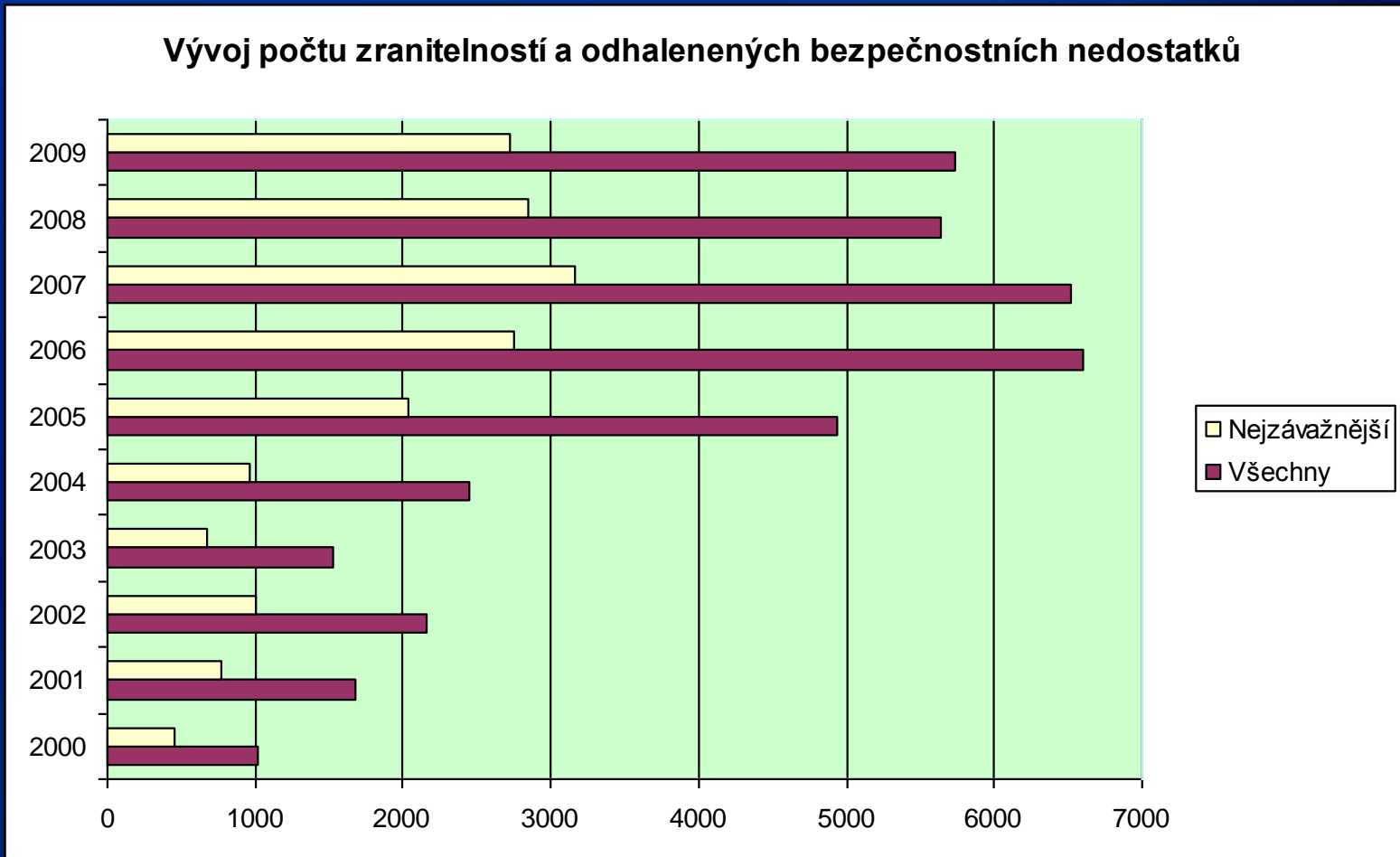
# Východiska pro využití informačních zdrojů

- **System 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, platform a balíčků 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>)
- **System 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

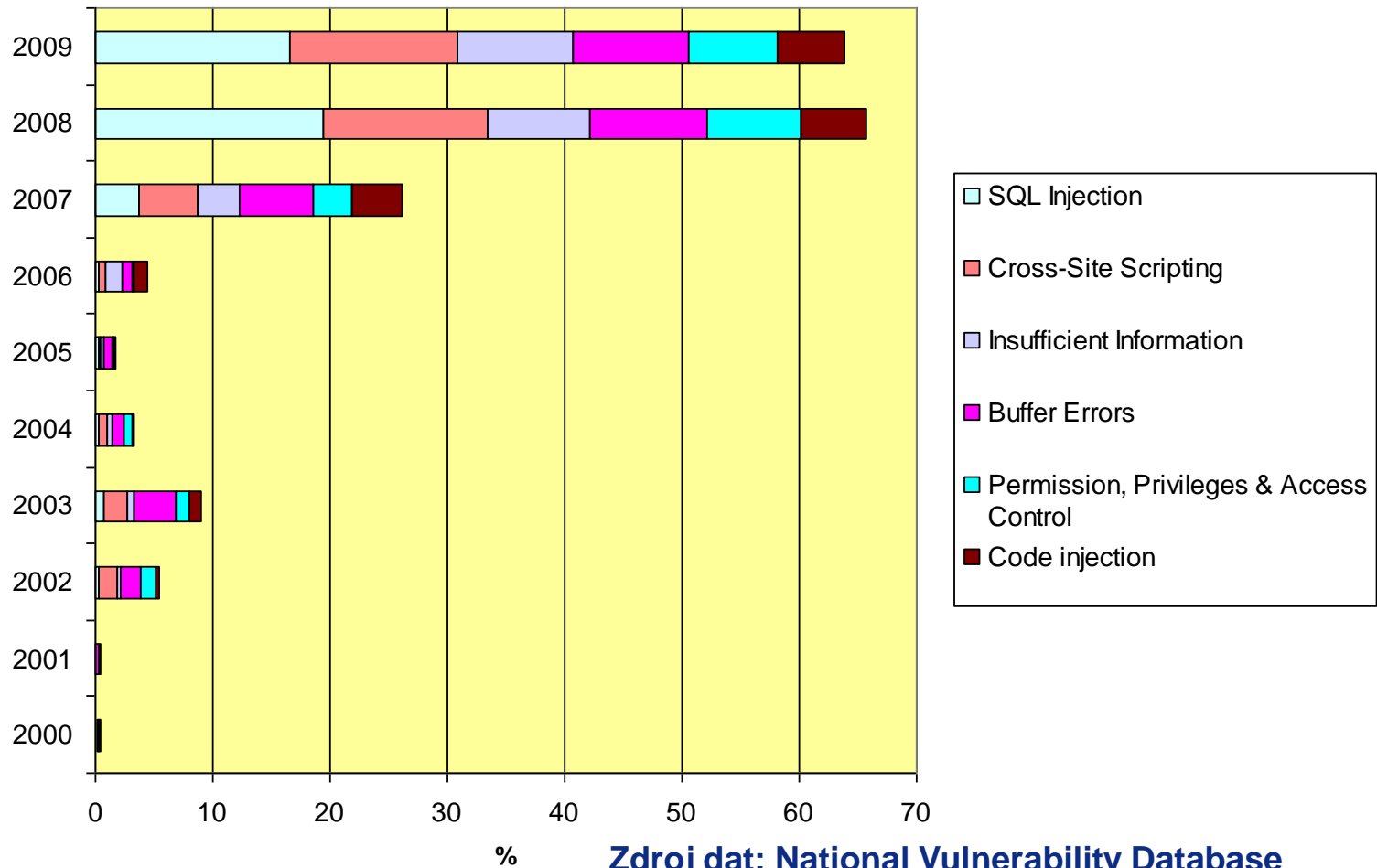


Zdroj dat: National Vulnerability Database

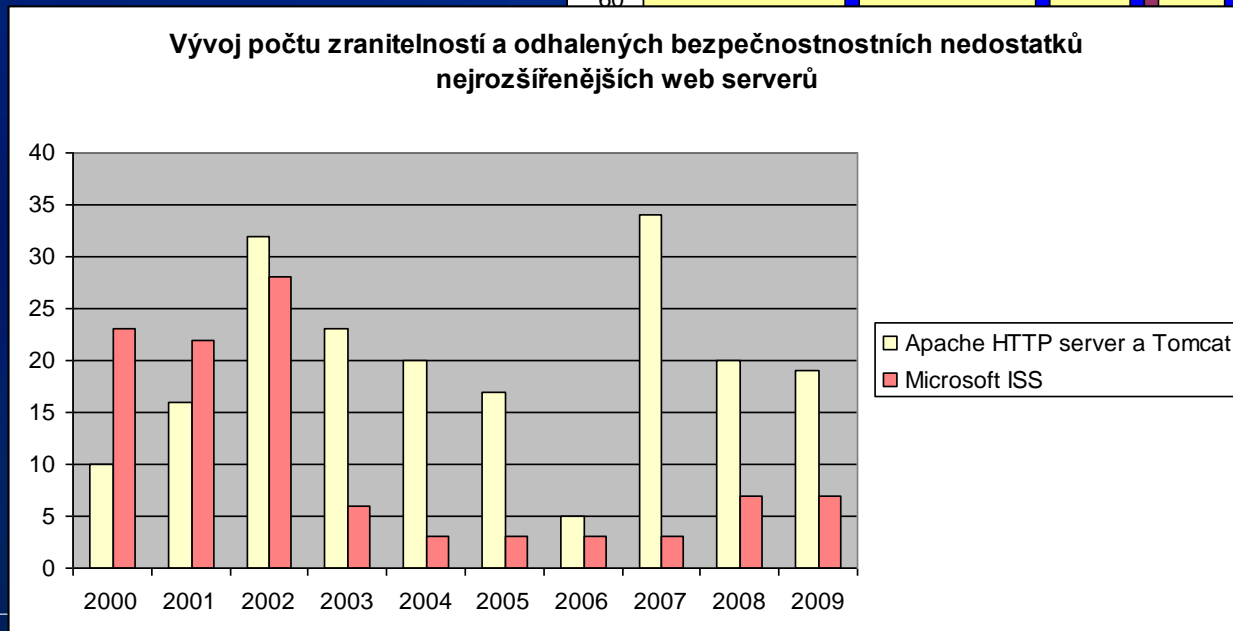
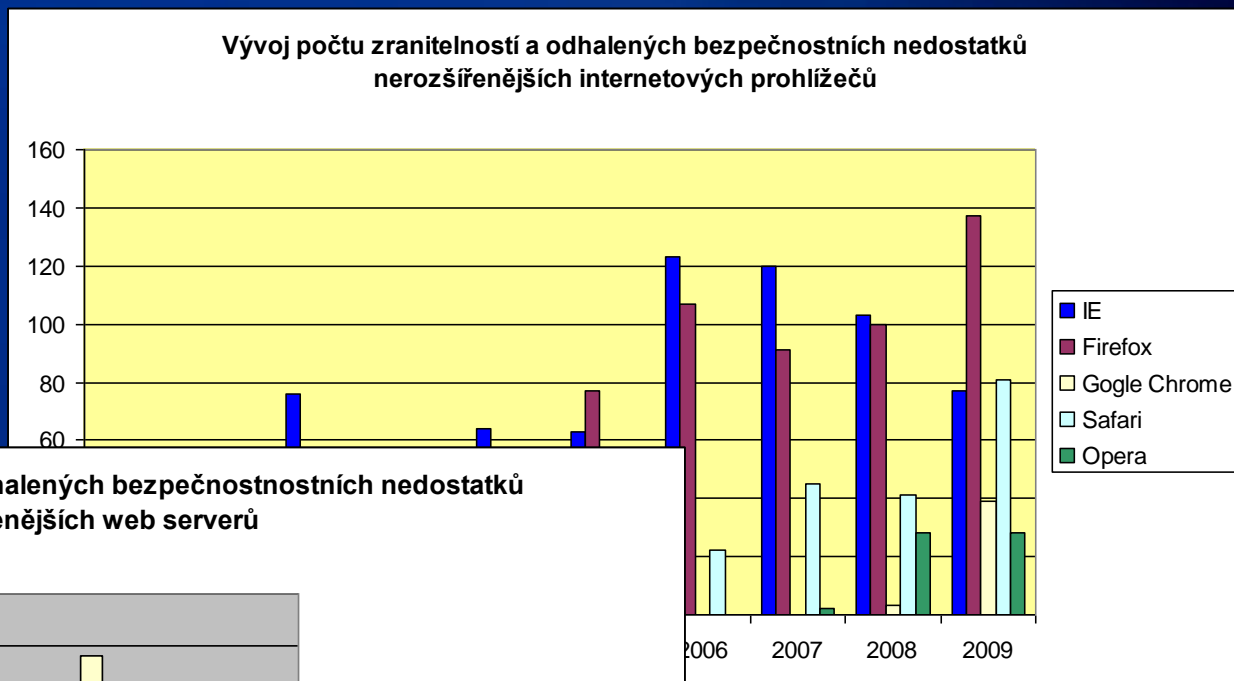


# Trend: Jen 6 bezpečnostních slabín se dnes podílí na 65% všech zveřejněných zranitelností

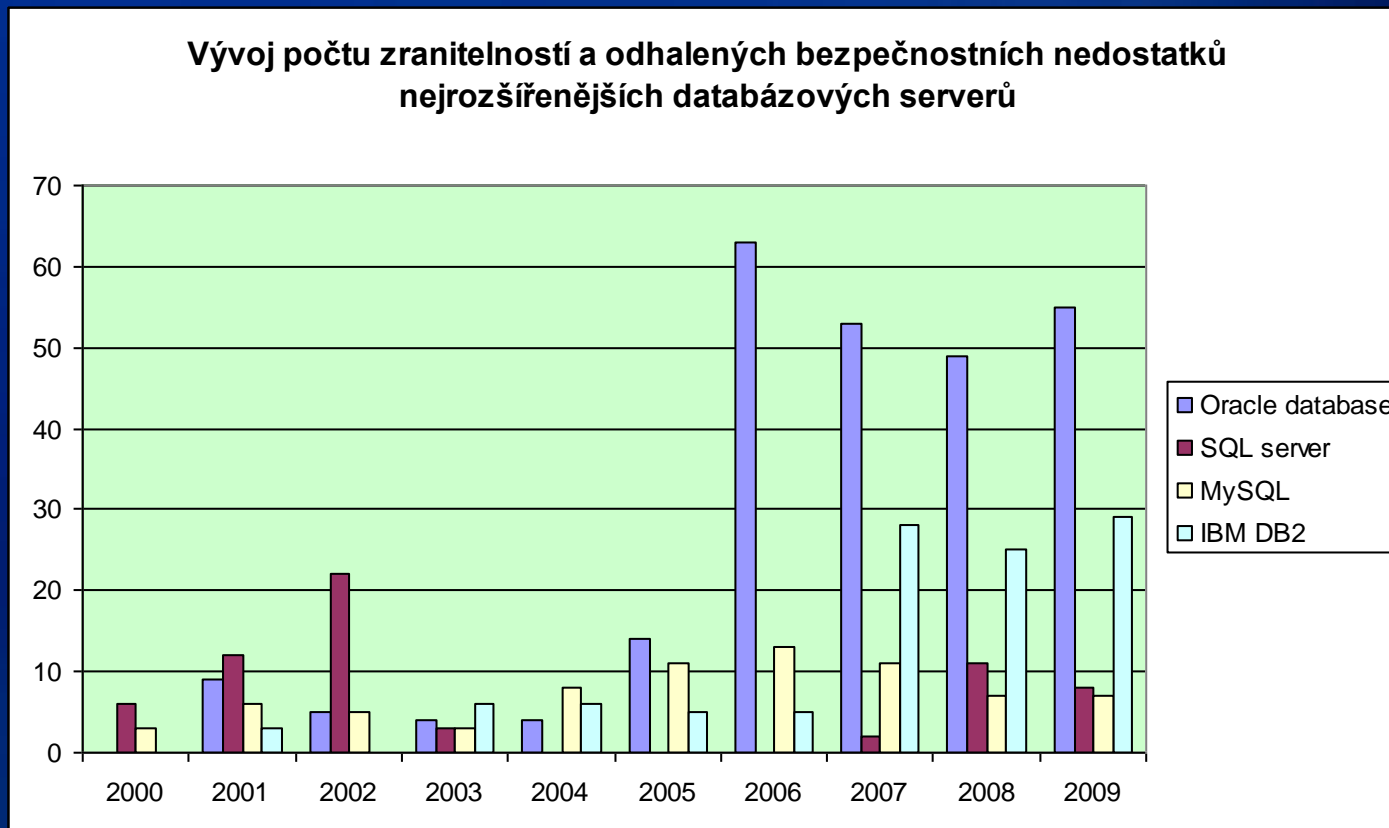
Vývoj poměrného zastoupení nečastějších bezpečnostních slabín



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



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



# 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](mailto:jirivondrasek@kpmg.cz)**

**[www.kpmg.cz](http://www.kpmg.cz)**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Informace zde obsažené jsou obecného charakteru a nejsou určeny k řešení situace konkrétní osoby či subjektu. Ačkoliv se snažíme zajistit, aby poskytované informace byly přesné a aktuální, nelze zaručit, že budou odpovídat skutečnosti k datu, ke kterému jsou doručeny, či že budou platné i v budoucnosti. Bez důkladného prošetření konkrétní situace a řádné odborné konzultace by neměla na základě těchto informací být činěna žádná opatření.