

# Řešení ochrany databázových dat

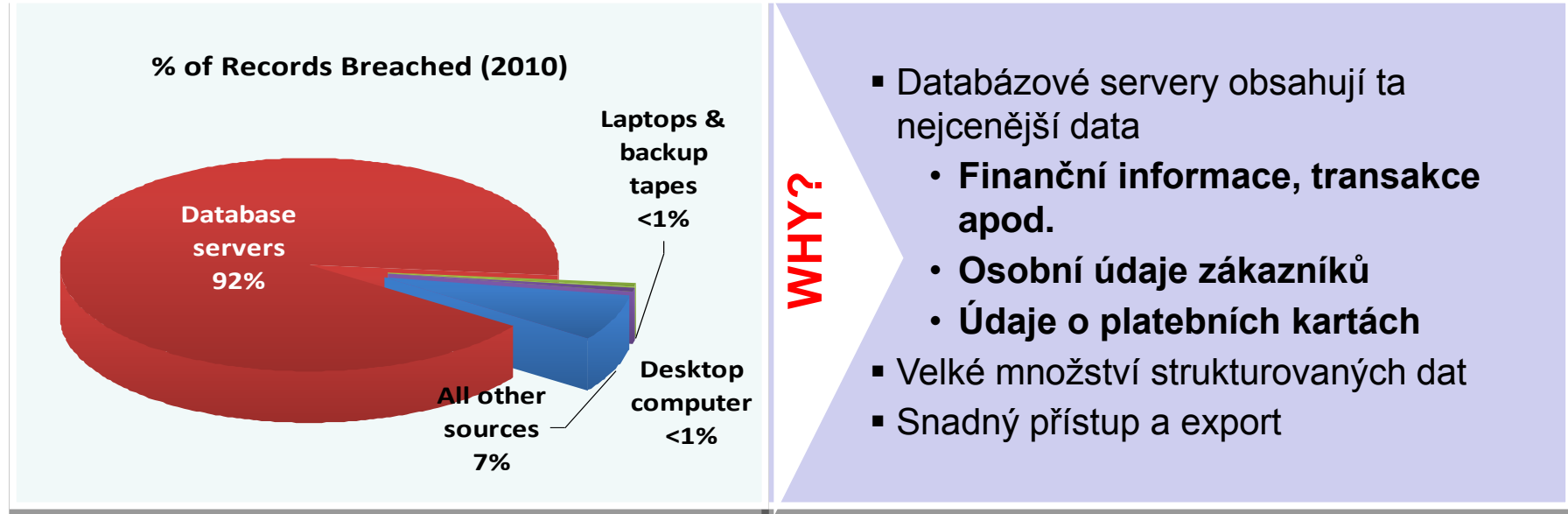
Projekt Raiffeisenbank CZ

Aleš Tumpach CISA

April 25, 2016



# Pokud dojde k bezpečnostnímu incidentu, informace v databázi jsou nejčastějším cílem útoku



**“Because that’s where the money is.”**

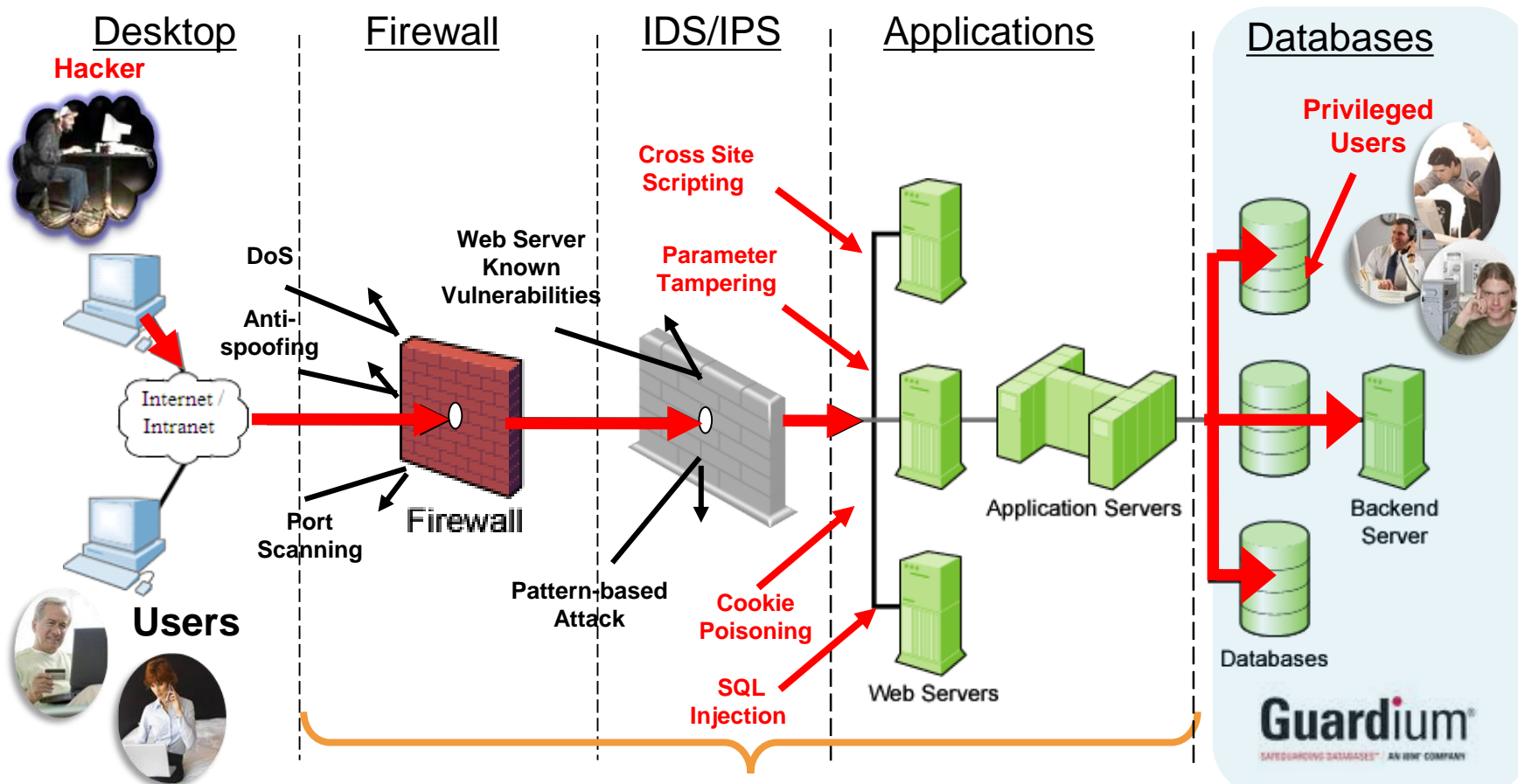
- Willie Sutton

# Situace v bankovním prostředí před projektem ochrany dat na úrovni databáze

- 2 vrstvá architektura představuje zvýšené bezpečnostní riziko
- Nutný přístup uživatelů nejen přes aplikace, ale i přímo do databáze
- SQL jazyk je mocný nástroj jednoduše použitelný i pro non IT uživatele, ale při špatném použití může způsobit performance problémy nebo i rozsáhlé poškození dat
- Dostupnost programů pro přímý přístup k DB
- Jednoduchý export velkého množství strukturovaných dat např. do Excelu
- Práva privilegovaných uživatelů, která nelze kontrolovat běžnými DB prostředky
- Chráněná data i v testovacím či vývojovém prostředí bez odpovídajících kontrol

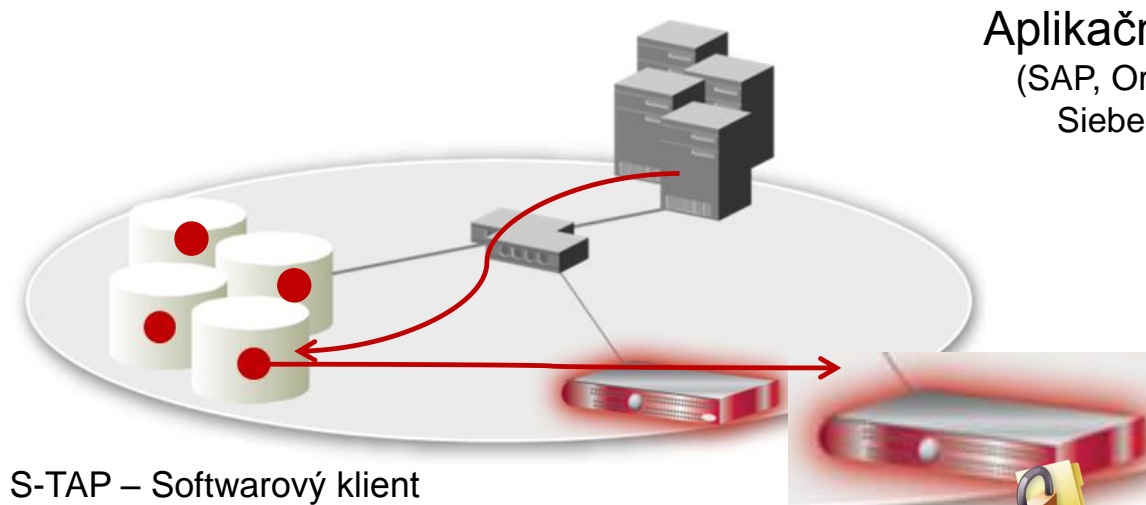
Tato rizika bylo potřeba snižovat jak procesně tak i technickými nástroji

# Fundamentální bezpečnostní kontroly bylo tedy potřeba doplnit o zabezpečení databází



Realita : Tradiční prostředky fundamentální bezpečnosti nemohou zastavit všechny hrozby → Potřeba nasadit poslední vrstvu ochrany na DB úrovni

# Zvolený nástroj - IBM Security Guardium



Aplikační servery  
(SAP, Oracle EBS,  
Siebel, apod.)

GUI - přístup  
založený na roli  
Přístup k auditním  
datům  
(Auditoři, IT security  
specislisté, DBA  
apod.)

S-TAP – Softwarový klient  
(„Lehká“ sonda která kopíruje  
informace do appliance )

Guardium  
Appliance

Zabezpečený auditní  
záznam

- Definování-vyhledávání-klasifikace-monitoring-ochrana dat
- Sběr a normalizace dat pro efektivní ukládání, jedno zabezpečené úložiště, zajištění integrity logů
- Bezpečnostní politiky a parsování jsou konzistentní napříč různými platformami, Oracle, MS SQL, DB2, Hadoop (big data) - škálovatelnost, připraveno na budoucí vývoj
- Podpora oddělení neslučitelných funkcí
- Opravdová ochrana dat, nejen monitoring ale i FW funkce
- Rychlé nasazení, předdefinované politiky a reporty

**Zajištění úplného logování  
činností na databázové úrovni  
včetně mapování koncových  
aplikačních uživatelů vybraných  
aplikací**

**Alerty v reálném čase mohou být  
integrovány se SIEM systémy,  
zaslány do emailu...**

# Projekt nasazení Guardia v Raiffeisenbank

## **První fáze – 2011 (omezený rozsah)**

- Původně součást infrastruktury pro transformační projekt, požadavek na ochranu transakčních a citlivých dat nového core systému
- Nasazení jedné appliance, pasivní monitoring databáze CRM – databáze Oracle
- Postupně připojení dalších Oracle databází v rámci projektů

## **Druhá fáze – 2014/2015 (rozšíření rozsahu)**

- Auditní a regulatorní požadavky na kontrolu kritických aplikací
- Dokoupení druhé appliance
- Připojení databází prvního core systému – Oracle
- Připojení databází druhého core systému – DB2 (AS400)
- Připojení databází treasury aplikací – Oracle

## **Třetí fáze – 2015 (optimalizace a neprodukční prostředí)**

- Auditní a regulatorní požadavky na kontrolu testovacích prostředí s produkčními daty
- Menší objemy dat – oddělení prostředí, využita appliance z první fáze
- Připojení testovacích prostředí cca 20 aplikací včetně výše zmíněných core bankovních systémů

# Konečný stav projektu ke konci roku 2015

## Připojená DB platformy

- Oracle – převažující, cca 90 % všech dat, OS IBM AIX, pár Oracle DB na Windows
- MS SQL na Windows platformě
- DB2 na AS400 platformě
- Celkově cca 60 databází

## Pozitiva projektu

- Pokrytí auditních a regulatorních požadavků na ochranu informací v produkčním i testovacím prostředí
- Rychlé nasazení nástroje, minimální požadavky na IT provoz – minimální degradace výkonu databází, pouze rutinní instalace S-TAP klientů
- Jednoduchost obsluhy, přehledné a intuitivní politiky, reporty, auditní workflow a další nástroje – kompletní obsluha 1 FTE (administrace, tvorba pravidel, politik, reportů, vyhodnocování událostí)
- Mocný nástroj pro kontrolu činnosti privilegovaných uživatelů v databázích
- Otevřenost i pro budoucí požadavky a připojované databázové platformy, konzistentní reporty a auditní politiky – např. vedle Oracle a MS SQL bezproblémové připojení AS400 (DB2) za použití stejných reportů a politik
- Žádné výkonnostní problémy ani na straně DB serverů, sítě či Guardia

## Další plány

- Nasazení funkcionalit FW a anonymizace dat