

# *DatenUnsicherheit*

**für MS SQL Server und Azure**

**Elmar Bergmann**

# Who am I

- Elmar Bergmann
- Mehr als 10 Jahre in der IT-Sicherheits-Branche
- Penetration Tester, Forensics, Malware, Security Architekt & Design
- McAfee, Virgin Media & Mobile, Metropolitan Police London, Deutsche Bank, HSBC

Kontakt Daten: [NetSec.Source@gmail.com](mailto:NetSec.Source@gmail.com)

<https://uk.linkedin.com/in/elmarbergmann>

# Agenda

- Beispiele von Hacking-Fällen
- wie sie entstehen
- und warum
- Die Bösen: Russen, Chinesen, Skriptkiddies? Oder doch die "seriöse" Konkurrenz?
- Datenbanksicherheit allgemein und mit MS SQL Server
- MS Azure und SQL Azure vs. Sicherheitsbedenken
- Tipps und Tricks für die eigene Arbeit und für Kunden

# Hacking-Fälle in jüngster Vergangenheit

- Adobe
- Homedepot
- Staples
- LinkedIn
- Yahoo
- Sony
- Morgan Stanley
- JP Morgan

## 2 MILLION ONLINE ACCOUNTS HACKED

Report by **Trustwave**

**NOV 2013**

USA, Germany, Singapore

57% of these were Facebook accounts.

## ADOBE HACKED

### 38 MILLION ACCOUNTS AFFECTED

San Jose, USA

Hackers breached into customer accounts and stole usernames and passwords.

**OCT 2013**

Debit and credit card information of **2.9 million** accounts compromised.

## MALWARE Attack on YAHOO!

Great Britain, France, Romania

**JAN 2014**

Thousands of Yahoo! users were hacked and its servers were made to send out malware into user systems.

## NSA'S SECRET DIVISION Hacks Computers Globally

Report by **DER SPIEGEL**

USA, Germany

**DEC 2013**

Top secret division of National Security Agency called 'Tailored Access operations' (TAO) alleged to be stealing data by inserting 'invisible back door spying devices into computer systems'.

## 1 MILLION SONY PLAYSTATION ACCOUNTS HACKED

**JUN 2011**

When Sony took legal action, hackers stole account information from Sony Pictures in retaliation.

**SONY PICTURES**

## STUXNET BOTNET ATTACK

100,000 computers affected.

**2010**

Nuclear installations in Iran were hacked into and attacked by a computer worm, stuxnet.

Iran

## BURGER KING TWITTER ACCOUNT HACKED

McDonalds @BurgerKing

**FEB 2013**

BURGER KING'S USA official Twitter account. Just got hacked by McDonalds because the wrapper flipped -> 'FREEDOM IS FAILURE'.

## CREDIT CARDS & CUSTOMER INFO HACKED

### TARGET 40 million customer accounts hacked

USA

**NOV 2013**

**27**

**15**

## Fake Tweet on 'Obama, Explosions' CAUSES MARKET CRASH

Loss: **\$136 million**

**AP** The Associated Press Breaking: Two Explosions in the White House and Barack Obama is injured.

**APRIL 23 2013**

## SYRIAN ELECTRONIC ARMY HACKS skype's TWITTER ACCOUNT

**JAN 2014**

SEA hacked Skype's social media programs, its Twitter account and official blog.

# Wer sind die Hacker?

- Script Kiddies
- Hacker
- Malware-Autoren
- Organisiertes Verbrechen
- Konkurrenz
- Regierungen





# Datenbank Sicherheit für SQL Server

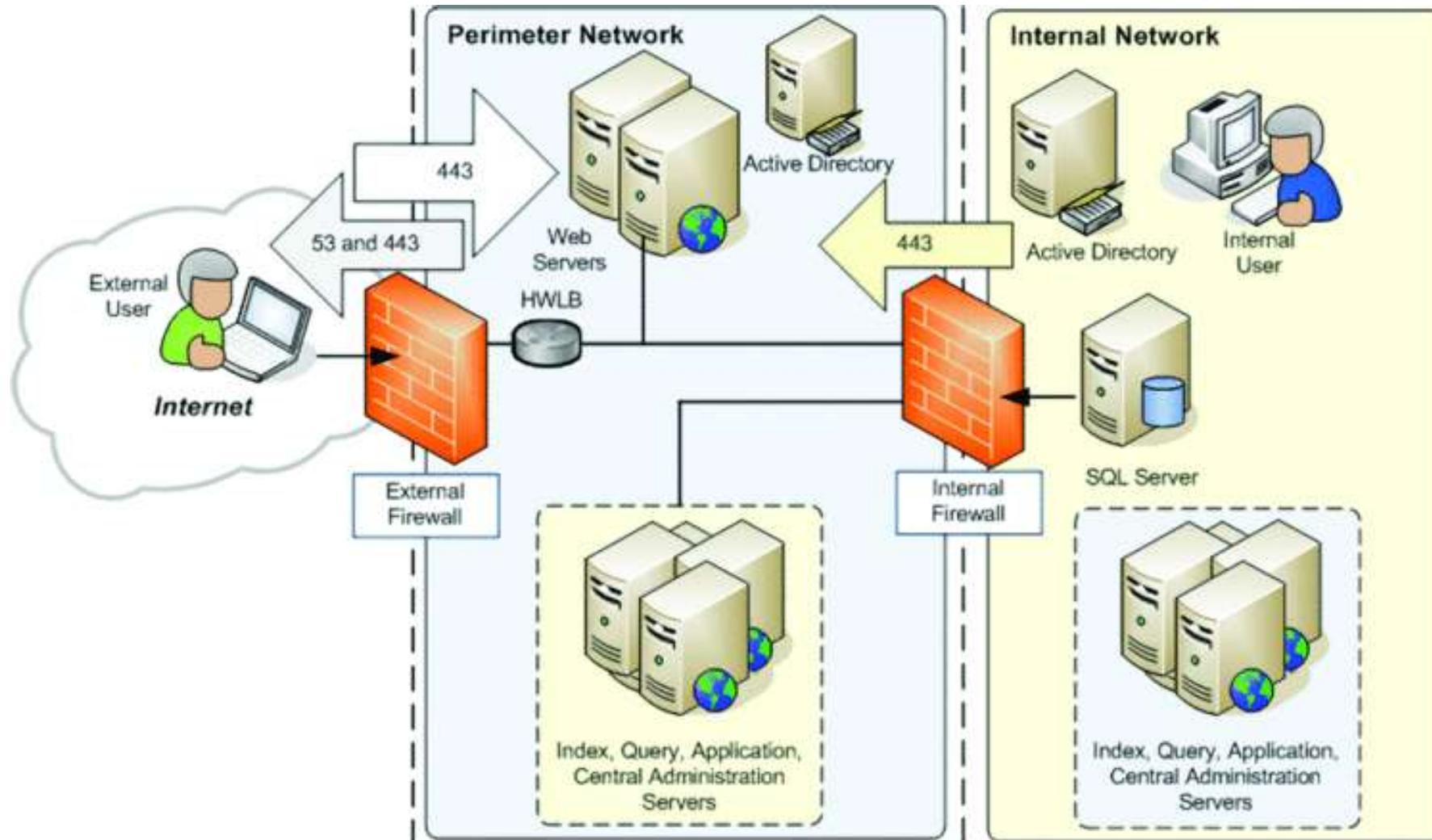
## Übersicht

- Datenbanken im Netzwerk
- Datenbankverschlüsselung
- Kennwörter
- Instanzen
- Datensicherheit
  
- Hacker-Angriffsmethoden

# Datenbank im Netzwerk – Was ist zu beachten?

- Datenbankserver - Position im Netzwerk
- Firewall Konfiguration
- Netzwerkverbindung von Internet
- Netzwerkverbindung von Intern
- NATing
- Daten in Transit

# Datenbank im Netzwerk – Was ist zu beachten?



# Datenbankverschlüsselung – Was ist zu beachten?

- Datenbankverschlüsselung
- Verschlüsselung in Tabellen
- Verschlüsselung von gespeicherten Daten
- Verschlüsselung von Daten im Transit
- Verschlüsselung von Daten via HBAs

# Datenbankverschlüsselung – Was ist zu beachten?

- Verschlüsselungs-Keys – Nie am Datenbank-Server lagern
- Verschlüsselung via Hashing
- Welche Algorithmen sind sicher? Und welche nicht?
- **BEACHTE: JE HÖHER DIE VERSCHLÜSSELUNG DESTO MEHR CPU-LEISTUNG WIRD BENÖTIGT!**

# Datenbankverschlüsselung – Was ist zu beachten?

- Nicht sicher:

- Hashing: MD2-MD5, SHA & SHA1
- Verschlüsselung: DES, RC4, Alles unter 128 Bit Länge

- Sicher:

- Hashing: SHA2 (MSSQL2005), SHA2\_256, SHA2\_512 (MSSQL2012)
- Verschlüsselung: TRIPLE\_DES, TRIPLE\_DES\_3KEY, DESX, AES\_128, AES\_192, AES\_256

# Datenbankkennwort – Was ist zu beachten?

- Starkes Passwort - qerty, Mama01121945, oder doch qPx\*syT%#ma1Or£6
- SQL-Authentifizierung vs. Windows-Authentifizierung
- In Azure ist nur SQL-Authentifizierung möglich

# Instanzen – Was ist zu beachten?

- Was installieren – und wann
- Kennwort wechseln – Policy (alle 30 Tage – oder doch nie?)
- Audits – Failed Logins
- Namensänderung des SA-Kontos
- SA-Konto deaktivieren
- Endpoints Securing
- Minimale Berechtigungen
- Datenbankdatei-Initialisierung (Instant File Initialization)

# Datensicherheit – Was ist zu beachten?

## Berechtigungen

- GRANTing
- DENYing
- REVOKEing
- Column Level
- Row Level

Common User: SELECT, INSERT, UPDATE und DELETE

# Angriffsmethoden – Beispiel SQL Injections

Passiert in WebFrontEnd mit Hilfe eines SQL Commands in einem FORM Field oder URL

“/orderhistory.aspx?id=25; delete from Orders,”

SELECT \* FROM Orders WHERE OrderID=25; delete from Orders;

Exec master.dbo.sp\_makewebtask

“\\web1\wwwroot\tables.html”, “select \* from information\_schema.tables”

<http://example.com/app/accountView?id=' or '1'='1>

# Angriffsmethoden – SQL Injections - Verhindern

- Nutzung einer sicheren API, die den Aufruf von Interpretern vermeidet oder eine typ-gebundene Schnittstelle bereitstellt
- Keine API soll dynamisches SQL verwenden – nur wenn keine andere Möglichkeit besteht
- Applikation soll keinen Zugang zu Tabellen oder Views haben – nur wenn absolut nötig
- Alle Datenbank-Aufrufe sollen parametrisiert sein, anstelle von inline dynamic SQL
- Eingabeprüfung gegen Positivlisten (White List)
- Keiner Anwendereingabe sollte vertraut werden. Alle Eingaben sind verdächtig!

**NICHT NUR KLEINE FIRMEN KÄMPFEN MIT SQL INJECTIONS!!!**

# Andere Angriffsmethoden – OWASP Top 10

OWASP Top 10 – 2010 (alt)	Δ	OWASP Top 10 – 2013 (neu)
A1 – Injection	=	A1 – Injection
A3 – Fehler in Authentifizierung und Session-Management	↗	A2 – Fehler in Authentifizierung und Session-Management
A2 – Cross-Site Scripting (XSS)	↘	A3 – Cross-Site Scripting (XSS)
A4 – Unsichere direkte Objektreferenzen	=	A4 – Unsichere direkte Objektreferenzen
A6 – Sicherheitsrelevante Fehlkonfiguration	↗	A5 – Sicherheitsrelevante Fehlkonfiguration
A7 – Kryptografisch unsichere Speicherung – mit A9 →	↗	A6 – Verlust der Vertraulichkeit sensibler Daten
A8 – Mangelhafter URL-Zugriffschutz – erweitert zu →	↗	A7 – Fehlerhafte Autorisierung auf Anwendungsebene
A5 – Cross-Site Request Forgery (CSRF)	↘	A8 – Cross-Site Request Forgery (CSRF)
<Teil von A6: Sicherheitsrelevante Fehlkonfiguration>	neu	A9 – Verwendung von Komponenten mit bekannten Schwachstellen
A10 – Ungeprüfte Um- und Weiterleitungen	=	A10 – Ungeprüfte Um- und Weiterleitungen
A9 – Unzureichende Absicherung der Transportschicht	↗	Zusammen mit 2010-A7 nun im neuen 2013-A6

# Generelle Cloud-Bedenken

- Einsehbarkeit des angebotenen Services
- Sicherheit
- Daten-Eigentum
- Standards



# Microsoft Azure vs. Security

“Security’s the biggest blocker not just for Azure adoption but for cloud adoption generally,”

Stevan Vidich, director of Windows Azure marketing

# Microsoft Azure vs. Security

- Log Files Problematik – Platform Logs nicht zugänglich
- Sicheres Löschen von Daten in der Cloud
- Code Change und Applikationsupgrades von Microsoft bestimmt
- Microsoft unterstützt nicht jede individuelle installierte Applikation
- Penetration Testing ist Microsofts Angelegenheit – daher keine Einsicht in Wann, Wie oft oder Mit welchen Resultaten
- Azure ist zentral gemanagt via Redmond

# Tipps und Tricks

- Angriffe selber Testen – einige Tools

- Nessus Vulnerability Scanner, Burpsuite, nmap, Wireshark, ZAP Proxy, Netsparker, Metasploit, sqlmap

Beachte: Die Tools ersetzen keinen erfahrenen Pentester! Kein Tool findet alle Schwachstellen! Kein Tool testet alle Sicherheitsbereiche!

- Folge den Best Practices von Microsoft
- Eigener, gehärteter Server für MSSQL
- Immer nur die notwendigsten Berechtigungen vergeben
- Deaktiviere alle nicht benötigten Services, Ports, Benutzerkonten, Berechtigungen
- Ändere Standard-Kennwort, benütze starkes Kennwort und wechsle es regelmässig per Policy

# Tipps und Tricks

- Verfolge konstant die letzten relevanten Sicherheitstipps und Vulnerabilities für MSSQL
- Patche sofort und ständig
- Aktives Loggen von Aktivitäten
- Aktive und periodische Überprüfung von Logdateien
- Wenn möglich Server in eigenes VLAN
- Netzwerk Firewall, Server Firewall, Web Firewall -> NGF (Next Generation Firewall)
- IDS (Intrusion Detection System) / IPS (Intrusion Prevention Systems)
- Anti-Virus und Adware Software

# FRAGEN

# ???

*Elmar Bergmann*

[NetSec.Source@gmail.com](mailto:NetSec.Source@gmail.com)

<https://uk.linkedin.com/in/elmarbergmann>