„Nur die Paranoiden überleben“
Andy Grove, Intel

Sicher?

SQL Server Sicherheit
SNEK, 12. – 13.3.2016, Nürnberg

2

Wer nutzt den Standard Port 1433 für die SQL Server Installation?

Wer nutzt die gemischte Authentifizierung im SQL Server?

Wer betreibt eine Web Anwendung z.B. Share Point Server in seiner Organisation?

5

Gibt es in Ihrer Organisation einen IT-Sicherheitsbeauftragten?

6

Wird in Ihrer Organisation regelmäßig ein Audit durchgeführt?

Gibt es in Ihrer Organisation eine Passwort Policy, z.B.
- regelmäßige Änderung
- Komplexitätsregel

Wird die Policy auch auf Dienstkonten angewendet?

Über mich

Vortragsziel

- Vermittlung technischer Informationen
- Sensibilität für das Thema Sicherheit erzeugen

So?

```
<connectionStrings>
  <add name="MyLocalSQLServer"
       connectionString="Initial Catalog=aspnetdb;
       data source=localhost;
       Integrated Security=SSPI;"
       providerName="System.Data.SqlClient"/>
</connectionStrings>
```

... oder so?

```
<connectionStrings
     configProtectionProvider="RsaProtectedConfigurationProvider">
     ...
     <CipherData>
          <CipherValue>R7cyuRk+SXJoimz7wlOpJr/YLeADGnwJVcmElHbrG/
             B5dDTE4C9rzSmmTsbJ9Xcl2oDQt1qYma9L7pzQsQQYqLrkajqJ4i
             6ZQH1cmiot8ja7Vh+yItes7TRU1AoXN9T0mbX5HAxm0O3X/285/M
             dXXTUlPkDMAZXmzNVeEJHSCE=
          </CipherValue>
     </CipherData>
     ...
     <CipherData>
        <CipherValue>d2++QtjcVwIkJLsye+dNJbCveORxeWiVSJIbcQQqAFofhay1wMci8FFlbQWtti
          RYFcvxrmVfNSxoZV8GjfPtppiodhOzQZ+0/QIFiU9Cifqh/T/7JyFkFSn13bTKjbYmHObKAzZ+
          Eg6gCXBxsVErzH9GRphlsz5ru1BytFYxo/lUGRvZfpLHLYWRuFyLXnxNoAGfL1mpQM7M46x5YW
          RMsNsNEKTo/PU9/Jvnh/lT+GlcgCs2JRpyzSfKE7zSJH+TpIRtd86PwQ5HG3Pd2frYdYw0rmlmlI9D
        </CipherValue>
      </CipherData>
       ...
</connectionStrings>
```

Themen

- Allgemeines
- Instanz-Sicherheit
- Wege-Sicherheit
- Datenbank-Sicherheit

Allgemeines

- Der Umgang mit sensiblen Daten
- Der technologische Wandel
- Der Faktor Mensch
- Die Aufgabe

Technologien

- Column Encryption
- Transparent Database Encryption (TDE)
- Data Masking
- Row Level Security
- Always Encrypted
- Kerberos, NTLM
- Windows / SQL Server Authentication
- SSL/TLS, HTTPS, IPSec
- Zertifikate
- AES, 3-DES, SHA2
- ...

Prozesse

- Passwortwechsel
- Rolling Keys / Key Rotation / Key Management
- Überwachung
- ...

Compliance

- PCI DSS: The Payment Card Industrie Data Security Standard (kurz: PCI)
- HIPAA: Health Insurance Portability and Accountability Act
- STIG: Security Technical Implementation Guide
  - DoD: United States Department of Defense
  - DISA: Defense Information System Agency
- ...

It‘s a Beautiful Day

SQL Server Dienstkonto

- lokales Systemkonto
- Netzwerkdienstkonto
- Virtuelles Konto
- Lokales Benutzerkonto
- Managed Service Account
- Group Managed Service Account
- Domänenbenutzerkonto

Auswahlkriterien

- Prozess: Regelmäßige Passwortänderung
- SQL Server im Cluster
- SQL Server Multi-Instanzumgebung
- Kerberos
- Delegierung
- „The principal of least privilege“
- „Separation of Duties“ (SoD)

Managed Service Account

- Wird im Active Directory verwaltet
- Automatische Passwortänderung
  - Zyklus: 30 Tage
  - Kann geändert werden
- Wird einem Computer exklusiv zugeordnet
- Keine interaktive Anmeldung möglich
- Service muss die Nutzung von MSAs unterstützen
- Automatisches SPN Management

Demo:
Managed Service Account

Hinweise MSA (1)

- New-ADServiceAccount legt standardmäßig einen gMSA an!
  - Parameter: -RestrictToSingleComputer für MSA
- „Key not found“ / „Schlüssel ist nicht vorhanden“
  - Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10)
- Add-ADComputerServiceAccount ordnet den MSA einem Computer zu
  - Ausführung auf dem betreffenden Server!

Hinweise MSA (2)

- Install-ADServiceAccount zur Einrichtung des MSA auf dem Server
- Test-ADServiceAccount zur Prüfung der Einrichtung auf dem Server
- Reset-ADServiceAccountPassword zur manuellen Erneuerung des Passwortes auf dem Server
  - Gilt nicht für gMSAs!
- Uninstall-ADServiceAccount
- Remove-ADServiceAccount

Hinweise MSA (3)

- Einrichtung der Delegierung über ADSIEdit!
  - Attribut: msDS-AllowedToDelegateTo
  - Hinzufügen der SPN‘s

Hinweise Dienstkonto

- lokale Admin Rechte?
  - Nein!
  - Fehlermeldungen im Ereignisprotokoll prüfen
- Zugriffsrechte auf Datenverzeichnisse?
  - Nein!
  - Zugriff erfolgt über das virtuelle Konto
- Identisches Konto für alle SQL Server Dienste?
  - Nein!
  - SQL Server Instanzen verwenden eigenes Konto

Demo: Dienstkonto

Wegeverschlüsselung

- Verschlüsselung der Kommunikation zwischen Client und Server
- Verfahren: SSL/TLS
  - Seit 29.1.2016: TLS 1.2 Support für 2008 und größer)
- Konfiguration erfolgt pro SQL Server Instanz
  - Achtung: Neustart des Dienstes notwendig!
- Konfiguration:
  - Jede Verbindung wird verschlüsselt
  - Nur wenn der Client die Verschlüsselung anfordert

Zertifikatsanforderung

- Zertifikat wird abgelegt im
  - Zertifikatsspeicher des lokalen Computer
  - Zertifikatsspeicher des aktuellen Benutzers
- Aktuelle Uhrzeit liegt im Gültigkeitszeitraum
  - Zertifikate haben eine definierte Laufzeit!
- Zertifikat zur Serverauthentifizierung
  - Enhanced Key Usage Property: 1.3.6.1.5.5.7.3.1
- Subject Property
  - Common Name = Hostname oder FQDN des Servers
  - Cluster: Hostname oder FQDN des virtuellen Servers

Demo: Wegeverschlüsselung

Database Security

- dbo and SET TRUSTWORTHY ON
- Code Signing
- Always Encrypted (SQL Server 2016)

Demo:
dbo and SET TRUSTWORTHY

dbo and SET TRUSTWORTHY

- Mitglieder der Gruppe db_owner dürfen Prozeduren anlegen, die in einem anderen Benutzerkontext ausgeführt werden
- Wenn TRUSTWORTHY gesetzt ist, können Zugriffe im Benutzerkontext des Eigentümers ausserhalb der Datenbank ausgeführt werden
- Das funktioniert auch dann, wenn das SA Konto gesperrt wurde!

Code Signing

- Vermeidung von SET TRUSTWORTHY ON
- Signieren einer Prozedur mit einem Zertifikat oder einem asymmetrischen Schlüssel
- Erstellen eines Anmeldekontos auf Basis des Zertifikates
- Setzen der Zugriffsrechte für das Anmeldekonto

Demo:
Code Signing

Zusammenfassung

- SQL Server Sicherheit ist eine kontinuierliche Aufgabe
- Es geht nicht nur um sensible Daten, auch die Instanz selbst kann das Ziel sein
- Wir bewegen uns in einer komplexen technischen Umgebung. Kleine Änderungen können große Auswirkungen haben
- Verlassen Sie sich nicht auf andere Schutz-mechanismen, ergänzen Sie diese durch weitere Maßnahmen

Fragen?

```
SELECT ExtendedTime
FROM SpecialEvent
WHERE
     Domain = ‘Security‘;
```

Let us never lose the lessons we have learned

Back log

Tools (1)

- Überwachung
  - ApexSQL (www.apexsql.com)
  - Idera (www.idera.com)
  - Nessus (www.tenable.com)
  - Netwrix (www.netwrix.com)
- Security Test
  - sqlmap (www.sqlmap.org)
  - Kali (www.kali.org)

Tools (2)

- Analyse
  - Wireshark (www.wireshark.org)
  - Process Monitor (https://technet.microsoft.com/en-us/sysinternals/bb896645.aspx)
- Konfiguration
  - SQL Server Configuration Manager for Kerberos

Links (1)

- www.derekseaman.com
  - Infos zu SQL Server in virtueller Umgebung
  - Anleitung zum Aufbau einer PKI Infrastruktur (Lab)
- http://sqlity.net/
  - Infos zu SQL Server, speziell auch zu Sicherheit
- http://www.sommarskog.se/grantperm.html
  - Giving Permissions through Stored Procedures
- http://malwaremusings.com
  - Python Skript zur Analyse eines TDS Streams

Links (2)

- www.darkoperator.com
  - Attacking MSSQL with Metasploit
- http://blog.netspi.com
  - Diverse Einträge zum Thema „Hacking SQL Server“