CCVOSSEL

We know IT.

SUCCESS STORY

Energiekonzern | CCVOSSEL GmbH

Konzeption einer sicheren Active Directory-Struktur

Bild: Shutterstock / Mikko Lemola

Anforderungen

Da das Active Directory das Herzstück der IT-Infrastruktur eines Unternehmens darstellt, war es uns und unserem Kunden besonders wichtig, alle relevanten Aspekte mit dem Fokus auf die IT-Sicherheit zu betrachten. Eine spezielle Anforderung unseres Kunden beim sicheren Neuaufbau aller Active Directory Domänen bestand in der Konzeption und Umsetzung des Tier-Models. Dadurch werden die unterschiedlichen Sicherheitsbereiche (Tiers) segmentiert und gegeneinander gegen Kompromittierung abgesichert. Zu den weiteren Anforderungen unseres Kunden zählte neben der Härtung der Domaincontroller auch die Absicherung des Netzwerkverkehrs zum Domaincontroller über LDAPS mittels einer PKI-Infrastruktur.

Umsetzung

Um ein Höchstmaß an Sicherheit auf allen Ebenen zu gewährleisten, wurden die Systeme und Benutzerkonten nach dem erweiterten Tier-Model in verschiedene Bereiche aufgeteilt. Dabei erhält jeder Bereich dedizierte Adminstratorzugänge, sodass beispielsweise bei einem erfolgreichen Hackingangriff auf einen Administrator lediglich Zugriff auf die Clients, nicht aber auf die Server möglich ist. Die Reichweite eines Hackerangriffs wird somit eingeschränkt und das Risiko einer unternehmensweiten Kompromittierung minimiert.

Da Microsoft keine einfache Implementierung des Tier-Models unterstützt, haben die Experten von CCVOSSEL die Anforderung des Kunden über die Nutzung von strukturierten OU-Strukturen, Gruppenrichtlinien und Gruppenstrukturen umgesetzt.

Infolge dieser Anforderung wurde der Aufbau mehrerer gesonderter Zonen nötig, für die jeweils ein eigenes Active Directory konzipiert wurde. So konnte wiederum die Sicherheit der gesamten IT-Infrastruktur verbessert werden.

Weiterhin haben die IT-Security Consultants der CCVOSSEL GmbH die Struktur des DNS geplant und aufgebaut sowie eine sichere Integration dessen in das Active Directory sichergestellt. Außerdem wurde eine Azure Site angebunden und mehrere AD-Sites konzeptioniert. Dabei wurde ein hybrider Ansatz zur Positionierung von Domaincontrollern (on prem und Cloud) in Azure verfolgt.

Zur Härtung der Domaincontroller wurden umfangreiche Härtungsrichtlinien implementiert. Außerdem wurden Richtlinien für mächtige Konten wie administrative und Servicekonten konzeptioniert, was auch für Group Managed Service Accounts erfolgte. Die Projektmitarbeiter von CCVOSSEL konzipierten außerdem die Gruppenrichtlinien zur fundamentalen Absicherung der Infrastruktur.

Speziell für unseren Kunden wurde eine individuelle Schemaerweiterung im Active Directory implementiert.

Schlussendlich konnten alle notwendigen Objekte vom bisherigen AD in das neue, gesicherte AD migriert werden.

Fazit & Ausblick

Dank einer Zusammenarbeit auf Augenhöhe zwischen den Experten der CCVOSSEL und den Projektbeteiligten auf Kundenseite konnte die Active Directory-Struktur sicher konzeptioniert und umgesetzt werden, sodass es jetzt reibungslos und vor allem sicher funktioniert.

CCVOSSEL

We know IT.

Sicherheit

360° Überprüfung und Optimierung Ihrer IT-Sicherheit

Business Solutions

Professionelle IT-Services rund um Ihre Infrastruktur

Softwareentwicklung

Optimierung Ihrer Prozesse durch angepasste Lösungen

CCVOSSEL steht seit über 25 Jahren für professionelle IT-Dienstleistungen

Wir engagieren uns für unsere Kunden und für eine offene Gesellschaft. Unser Fokus liegt dabei in der Absicherung und dem Betrieb von IT-Systemen mit dem Schwerpunkt IT-Sicherheit. Durch den Einsatz interdisziplinärer Teams bestehend aus Administratoren, Beratern, Datenanalysten und Softwareentwicklern ermöglichen wir auch bei komplexen Anforderungen effiziente und moderne Lösungen.

Unsere Kunden

Siemens Bosch Daimler AG
Lufthansa System Network GmbH
Howoge Servicegesellschaft mbH
John F. Kennedy Friendship Center e.V.
Vattenfall Deutsche Bank AG
Gilette Deutschland GmbH & Co. OHG
BMW KPMG Agilent Technologies
Trägerverein des deutschen Presserats e.V.
Sony Europe GmbH G + J Berliner Verlag GmbH
Roche

Kooperationen

Microsoft Partner
Microsoft
Gold Application Development
Gold Datacenter
Silver Messaging

it's.BB
DAS IT-SICHERHEITSNETZWERK BERLIN-BRANDENBURG

SecurITy made in Germany

Allianz für Cyber-Sicherheit

Zertifizierungen

ISO/IEC 27001 zertifiziert www.isocert.de

ISO 9001 zertifiziert www.isocert.de

CCVOSSEL GmbH

www.ccvossel.de | info@ccvossel.de | FreeCall: 0800 2286773 | + 49 30 6098409 – 0

Standort Berlin Prenzlauer Berg | Sredzkistraße 28 | 10435 Berlin

Standort Berlin Tempelhof | Rathausstrasse 48 | 12105 Berlin