CCVOSSEL

We know IT.

SUCCESS STORY

Stromnetz Berlin GmbH | CCVOSSEL GmbH

Zentrale Serverhärtung nach CIS-Richtlinien

Bild: Shutterstock / Mikko Lemola

CCVOSSEL

We know IT.

Anforderungen

Unser Kunde, die Stromnetz Berlin GmbH, den wir bereits beim Rechenzentrumsaufbau sowie beim Aufbau eines sicheren Active Directory unterstützt haben, fragte bei CCVOSSEL eine Zusammenarbeit zur Serverhärtung an. Wir kollaborieren hierbei als CIS-Partner eng mit dem Kunden, um sicherzustellen, dass die Anforderungen erfüllt werden und die Systeme optimal funktionieren.

Die gemeinnützige Organisation CIS (Center for Internet Security) fokussiert sich auf die Verbesserung von IT-Security und hat verschiedene Sicherheitsstandards für die Unternehmens- und Organisationsebene entwickelt.

Umsetzung

Für unseren Kunden, die Stromnetz Berlin GmbH, bauten wir 2019 ein Basis-Image für Windows Server, welches das Fundament für alle Systeme bildet. In diesem ist die lokale Serverhärtung bereits integriert, wodurch ein grundlegender Schutz der Server gegenüber Angriffen gewährleistet werden kann.

Da die gesamte Infrastruktur neu aufgebaut wurde, war zunächst eine lokale Serverhärtung notwendig. Auf dieser Basis wurde die Domäne aufgebaut und die Serverhärtung zentral per Gruppenrichtlinie etabliert. Somit ist eine nachhaltige Absicherung der Server gewährleistet und alle neuen Server werden direkt abgesichert.

Die durch CIS bereitgestellten Best Practices beinhalten Empfehlungen verschiedener Kategorien, z.B. User Accounts und Authentifizierung, Netzwerk- und Hostkonfiguration, sowie Security Event Monitoring. Allerdings müssen diese Empfehlungen an die spezifischen Bedürfnisse eines Unternehmens angepasst werden, um eine effektive Security-Lösung abzubilden.

Unsere IT-Security-Consultants stimmen sich individuell mit dem Kunden ab, um eine maßgeschneiderte Lösung zur Anpassung der Settings zu entwickeln. Hier wird höchster Wert auf die Sicherheit gelegt, ohne den Betrieb des Unternehmens zu beeinträchtigen.

Die lokale Serverhärtung hatte jedoch einen Nachteil: Sie konnte durch einen lokalen Admin manuell entfernt werden. Um dieses Risiko und potenzielle Folgen zu minimieren, haben die Experten der CCVOSSEL die lokale Härtung weiterentwickelt und eine zentrale Härtung (via Gruppenrichtlinien) eingeführt. Diese zentralen Einstellungen können über das Active Directory auf alle Server angewendet werden und sind nur durch Domain-Admins änderbar. Dadurch wird die IT-Sicherheit des Unternehmens signifikant erhöht.

Eine Besonderheit der zentralen Serverhärtung ist, dass diese erst nachträglich durchgeführt werden kann. In enger Abstimmung mit dem Kunden werden die benötigten Einstellungen und Änderungen identifiziert und umgesetzt. Durch die Expertise der IT-Security-Consultants von CCVOSSEL waren Betrieb und Security während der Härtung stets im Einklang. Gleichzeitig stehen wir unserem Kunden jederzeit zur Verfügung, um bei

Problemen im Zusammenhang mit der CIS-Härtung zu unterstützen.

Bevor die Server gehärtet werden, führten wir eine eingehende Analyse durch, um den aktuellen Zustand zu erfassen. Nach der Härtung erfolgte eine erneute Überprüfung, um den Unterschied und den Sicherheitszugewinn zu evaluieren.

Fazit & Ausblick

Durch die enge Zusammenarbeit konnten alle beteiligten Personen auf Kundenseite gut einbezogen und auf verschiedene Bedürfnisse geachtet werden. Gemeinsam waren wir so in der Lage, eine bestmögliche Serverhärtung vorzunehmen.

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