CCVOSSEL

We know IT.

SUCCESS STORY

Daimler AG | CCVOSSEL GmbH

Server Hardening

Bild: Shutterstock / Mikko Lemola

CCVOSSEL

We know IT.

Anforderungen.

Das Virtual Competence Team Server der Daimler AG, einer der größten deutschen Automobilhersteller und Betreiber vieler heterogener Rechenzentren, suchte nach einer Lösung zur effektiveren Absicherung („Härtung“) aller ihrer Windows-Serversysteme.

Die zu erstellende Lösung sollte in der Lage sein, jeden Server per Knopfdruck vollautomatisch nach standardisierten Vorgaben zu härten und damit gegen Angriffe von Hackern abzusichern.

Das Ziel der Lösung war außerdem enorme Kosteneinsparungen zu erreichen, da zeitaufwendige manuelle Härtungen durch diese Lösung entfallen können. Außerdem kann der Härtungsprozess für alle Systeme als obligatorischer Bestandteil in die zugehörigen Betriebs- und Security-Prozesse integriert werden.

Server Hardening Package

Zur Entwicklung eines Tools zur Serverhärtung dem sogen. „Server Hardening Package“ wurde das Team „Beratung & Sicherheitslösungen“ der CCVOSSEL GmbH beauftragt, welches durch seine langjährige Erfahrung im Umgang mit Windows Serversystemen und durch seine Kernkompetenzen in den Bereichen „Security“ und „Automatisierung“ überzeugen konnte.

Falls es nach der Härtung von bestehenden Systemen mit deren Applikationen zu Funktionsproblemen kommen sollte, wurde außerdem eine Rollback-Funktion integriert, mit der die Härtung bei Bedarf rückgängig gemacht werden kann. Dies war essentiell, da die Funktionalität von Produktionssystemen durch die Härtung nicht eingeschränkt werden durfte.

Nach einer ausgiebigen Testphase wurden die meisten bestehenden Systeme und werden alle neue Windows Server der Daimler AG weltweit mit dem Server Hardening Package bespielt und damit bestmöglich abgesichert.

Entwicklung

Das Verteidigungsministerium der Vereinigten Staaten veröffentlicht in Abstimmung mit Software-Herstellern wie Adobe oder Microsoft Sicherheitskonfigurationsstandards in Form von Guides, den sogenannten Security Technical Implementation Guides. Diese Guides enthalten je Serverversion unterschiedlichste Härtungs-einstellungen, welche gesichtet und exportiert wurden. Die exportierten Daten wurden von den IT-Experten der CCVOSSEL GmbH bewertet und gewichtet und nach der Umsetzbarkeit beim Kunden kategorisiert und priorisiert. Die daraus resultierende Konfigurationsvorlage wird mittels Skripten automatisiert in das Server Hardening Package integriert.

Härtungseinstellungen

Die Konfigurationsvorlage ist dabei so aufgebaut, dass sowohl individuelle Kundenanpassungen als auch brandaktuelle kritische Einstellungen (z.B. zum Schutz gegen Meltdown & Spectre) einfach integriert werden können.

CCVOSSEL
We know IT.

Das Server Hardening Package besteht aus Skripten, die mit Hilfe von Windows-Bordmitteln die rund 600 Härtungseinstellungen, abhängig vom Betriebssystem, injiziert. Die Härtungseinstellungen finden in fast allen Bereichen des Systems statt. Darunter fallen beispielsweise die Bereiche Kennwortsicherheit, Dienste, Netzwerksicherheit, Terminalserver und Protokollierung.

Konkrete Beispiele für die Härtung sind beispielsweise die Deaktivierung von NTLMv1 oder SMBv1. Dabei handelt es sich um alte Schnittstellen, die von Hackern oft zum Angriff missbraucht werden.

Fazit & Ausblick

Mit Hilfe des Server Hardening Package können Windows Server aller Versionen (von Windows Server 2008R2 bis 2016) schnell und einfach auf den aktuellen Stand der Sicherheitsempfehlungen gehärtet werden. Durch die generalisierte Architektur und den strukturierten Aufbau ist es auch möglich, zukünftig erscheinende Versionen von Windows Servern (z.B. Windows Server 2019) oder auch weitere Härtungseinstellungen zu integrieren und auf den Systemen anzuwenden.

Eingesetzte Technologien:

- DoD (United States Department of Defense) STIG Viewer
- Microsoft Excel
- Skripte (Batch, VBS, VBA und Powershell)
- Microsoft Server 2008R2, 2012R2, 2016 und 2019

CCVOSSEL

We know IT.

Business Solutions

Professionelle IT-Services
rund um Ihre Infrastruktur

Softwareentwicklung

Wir optimieren Ihre Prozesse
durch angepasste Lösungen

Sicherheit

Die 360° Überprüfung und
Optimierung Ihrer IT-Sicherheit

Erprobtes Know-how mit Anspruch

CCVOSSEL GmbH steht seit 1996 für maßgeschneiderte IT-Dienstleistungen

Mit unserem erfahrenen Berliner Team und unserem hohen Qualitätsanspruch betreuen wir zahlreiche Konzernkunden bei der Planung und Umsetzung ihrer Digitalisierungsstrategie.
Unsere Kernkompetenzen sind Informationssicherheit und Rechenzentrumsbetrieb nach ITIL, bis hin zur individuellen Softwareentwicklung nach Scrum und dem Thema Reporting und Business Intelligenz.

Unsere Kunden

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

Kooperationen

Microsoft Partner
Silver Application Development
Silver Midmarket Solution Provider

smspasscode

DevExpress™

Auszeichnungen

ISO 9001 zertifiziert www.iqnet.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