CCVOSSEL

We know IT.

SUCCESS STORY

A European Power Corporation | CCVOSSEL GmbH

Analysis and optimisation of the Principle of Least-Privilege in the entire corporations infrastructure

Bild: Shutterstock / Mikko Lemola

ISO/IEC 27001 www.isocert.de zertifiziert

ISO 9001 www.isocert.de zertifiziert

CCVOSSEL GmbH

Requirements

An international energy group operates many critical systems and has commissioned us to implement the Principle of Least Privilege (POLP) as part of the optimisation of its IT security. The goal was to constrict all authorisations and user rights to the bare minimum.

Implementation

In close cooperation with the management, the internal IT department and the Security Operation Centre, we have interviewed account owners and developed strategies to mitigate risks. A team of 7 employees has worked remotely over a period of 9 months in a multilingual environment across national borders. Subsequently, we set up processes and designed a procedure that enabled the customer to implement the necessary security measures without interfering with regular operations of the customer's business..

The objective was to prevent potential damage to the IT infrastructure caused by unauthorised persons by reviewing and adjusting existing permissions. An important aspect of this was the removal of administrative permissions from Application Accounts, which in practice are usually equipped with far too many rights. These so-called service accounts are particularly attractive for attackers in any company, as they allow in-depth access to company data and are often poorly secured.

After initial consultations, we conducted a comprehensive risk assessment and developed a checklist. Subsequently, server systems and user accounts were examined for high authorisations and checked whether these could be restricted.

In order to speed up the analysis process, we developed tools to check the account rights automatically. The results were collected and evaluated centrally in a SIEM tool. A second tool enabled us to assign the recommended actions directly to the responsible employees by connecting to Microsoft Teams which also enabled us to track the progress.

Technologies used: PowerShell, Splunk, Microsoft Teams, Microsoft Flow, Microsoft 365, Microsoft Server 2016/2019

Conclusion & Outlook

The tools we developed significantly simplified and accelerated the processes for complying with best practices.

The use of the SIEM system for central data correlation has improved data clarity and made it easier to present the relevant information to the top management.

By minimising authorisations and access permissions to the required minimum, 90% of potential security risks were mitigated, thus significantly increasing overall IT security.

CCVOSSEL

We know IT.

Proven expertise with high standards

CCVOSSEL STANDS FOR RELIABLIE QUALITY IN IT SERVICES SINCE 1996.

With our experienced Berlin based team and our high expectations, we serve numerous customers from a wide range of industries.

Our focus is on Digitalisation and IT Security as well as on individual Software Development.

Our Customers

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

Cooperations

Microsoft Partner
Silver Application Development
Silver Midmarket Solution Provider

sms|passcode

DevExpress™

Certifications

ISO 9001 www.isocert.de zertifiziert

ISO/IEC 27001 www.isocert.de zertifiziert

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