

Stromnetz Berlin GmbH | CCVOSSSEL GmbH

Central Server Hardening According to CIS Guidelines



Requirements

Our client, Stromnetz Berlin GmbH, which we have already supported in setting up a data center and a secure Active Directory, asked CCVOSSSEL to collaborate on server hardening. As a CIS partner, we collaborate closely with the customer to ensure that the requirements are met and that the systems function optimally.

The non-profit organization CIS (Center for Internet Security) focuses on improving IT security and has developed various security standards for the enterprise and organizational level.

Implementation

For our client we built a base image for Windows Server in 2019, which forms the foundation for all systems. Local server hardening is already integrated in this image, which ensures basic protection of the servers against attacks.

Since the entire infrastructure was rebuilt, local server hardening was necessary first. On this basis, the domain was set up and server hardening was established centrally via group policy. Thus, a sustainable protection of the servers is ensured and all new servers are directly secured.

The best practices provided by CIS include recommendations of various categories, e.g. user accounts and authentication, network and host configuration, and security event monitoring. However, these recommendations must be adapted to the specific needs of a company in order to map an effective security solution. Our IT security consultants coordinate individually with

the customer to develop a customized solution to adapt the settings. Here, the highest value is placed on security without compromising the company's operations.

However, local server hardening had one drawback: it could be manually removed by a local admin. To minimize this risk and potential consequences, the experts at CCVOSSSEL have further developed local hardening and introduced central hardening (via group policies). These central settings can be applied to all servers via Active Directory and can only be changed by domain admins. This significantly increases the company's IT security.

Central server hardening can only be implemented retrospectively. The required settings and changes are identified and implemented in close coordination with the customer. Due to the expertise of CCVOSSSEL's IT security consultants, operation and security were always in harmony during hardening. Simultaneously, we are always available to support our customer in case of problems related to the CIS hardening.

Before hardening the servers, we performed an in-depth analysis to assess the current state. After hardening, a recheck was performed to evaluate the difference and the security gain.

Conclusion & Outlook

The close cooperation meant that all the people involved on the customer's side could be well included and attention paid to different needs. Together, we were thus able to carry out the best possible server hardening.



Security

360° Review and optimization
of your IT security



Business Solutions

Professional IT services
around your infrastructure



Software Development

Optimization of your processes
through custom solutions

CCVOSSSEL – well known for professional IT services for over 25 years

We are committed to our customers and to an open minded society. Our focus is on the protection and operation of IT systems with a main emphasis on IT security. Our interdisciplinary teams consisting of administrators, consultants, data analysts and software developers are habituated to finding efficient and modern solutions even for complex requirements.

Our Clients

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

Cooperations



Certifications



CCVOSSSEL GmbH

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

Office Berlin Prenzlauer Berg | Sredzkistraße 28 | 10435 Berlin

Office Berlin Tempelhof | Rathausstrasse 48 | 12105 Berlin