Customer reference

Leibniz Supercomputing Center (LRZ)

Protecting Personal Data and Simplifying Access Management

"SCB PROVIDED US CLEAN AUDITING AND A SECURE, CENTRAL POINT FOR ACCESS MANAGEMENT."

- Dr. Christoph Biardzki, Head of IT Infrastructure, Server and Service Group, LRZ.

Founded in 1962, the Leibniz Supercomputing Center (LRZ) is one of the oldest computing centers in Germany which provides services to scientific and academic communities in Munich, Germany. Major services include operating the Munich Scientific Network and running IT-Applications. LRZ also operates the fastest supercomputer in Europe and no. 4 in the world.

The Challenge

PROTECTING STUDENT RECORDS

LRZ is an institution which traditionally operates an open, scientific environment and usually does not process any sensitive data. However, recently LRZ was requested to host a complex web application which requires a much more stringent approach to IT security than usual, as it directly handles personal data of hundreds of thousands of study applicants. The regulations to protect sensitive personal records required LRZ to implement a process for preventing unauthorized data copies.

Previously, the administrators of the institution used SSH-based access with a password or a SSH key to reach the servers. However, administration and audit of these accesses was a very complex task as there were countless access controls regulating who is allowed to do what from where and on which server. Consequently, LRZ had to find a solution to easily and securely control and audit access to (Linux) servers storing personal data. This new concept required the separation of server administration and access management roles, as well.

The Solution

CENTRAL ACCESS CONTROL WITH SCB

In the planning phase, LRZ experts considered different concepts, such as stricter control over all SSH-enabled workstations or the implementation of a Linux-based gateway server. Finally, they chose the BalaBit Shell Control Box activity monitoring appliance. “We decided to buy SCB because it acts as a central access control point to our servers. In addition, compared to a Linux server-based gateway, SCB provides gateway functionality without admins needing to have a shell account on a gateway server.” – says Dr. Christoph Biardzki, LRZ’s Head of IT Infrastructure, Server and Services Group.

LRZ issued a smartcard with an embedded public key to each administrator. The public keys stored on smartcards were entered on SCB and administrators were granted access rights based on group membership on SCB. SCB uses the stored SSH keys to login to the target servers. Target systems include Novell SLES-servers and NetApp filers. As only SCB is allowed to access target servers via SSH, securing and auditing network firewalls has become very easy, as the rule sets only include SCB and not, like before, many different workstations.

Testing and implementation took approximately one month. Now, SCB is in productive operation protecting LRZ’s critical servers and storage systems. It currently controls 10 administrators and 100 servers of the institution. Furthermore, there are plans at LRZ to extend SCB operation for additional systems such as network components.

Key SCB benefits for LRZ

- Central point for access management
- Cheap smartcard-based, two-factor authentication
- Ability to record all activities on servers
- Ability to track sensitive data and file transfers
- Ability to allow or deny server access
- Use of multiple encryption keys for audit trails
- Simple, effective high-availability solution

The Results

SECURE ACCESS MANAGEMENT, CALM WORKER’S COUNCIL

SCB helped LRZ to implement several IT security best practices like clean assignment of access roles, secure two-factor authentication and auditing. It also helped to make access administration easier as most access rules are stored centrally and the rest is identical and thus easily auditable on all servers. Additionally SCB discourages potential internal attackers to attempt pulling out data from critical servers.

“Most importantly, the turnkey appliance approach made our system less complex. In addition, SCB provided smooth integration with $10 smartcards to get a fully functioning two-factor authentication. Last but not least, the use of multiple encryption keys* for audit trails made easier to us to get implementation approval from the worker’s council (“Betriebsrat”) which in Germany has to agree all measures which could be used to monitor employees. SCB ensures they are involved if audit logs have to be checked.” – concludes Dr. Biardzki.

*SCB can use multiple keys to encrypt the audit trails. In this case, multiple decryption keys are needed to replay the audit trails, so a single auditor on his own cannot access every information about LRZ systems.

About BalaBit

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring, trusted logging and proxy-based gateway technologies to help protect customers against internal and external threats and meet security and compliance regulations. BalaBit is also known as “the syslog-ng company”, based on the company’s flagship product, the open source log server application, which is used by more than 650,000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the second fastest-growing IT Security company in the Central European region according to the Deloitte Technology Fast 50 (2010) list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Our R&D and global support centers are located in Hungary, Europe.

More information here: www.balabit.com

Learn more

- Shell Control Box homepage
- SCB Use Case – Control internal IT Staff
- Request access to SCB online demo
- Request a callback