Customer Reference

ČEZ Group

Energy provider meets extreme security requirements

“SCB BROUGHT MUCH MORE THAN WE EXPECTED: IT IS NOT ONLY AN AUDITING SOLUTION, BUT AN ADVANCED AUTHORIZATION AND OCR SEARCH TOOL, AS WELL. WITH SSB YOU GET A REAL LOG MANAGEMENT TOOL WITHOUT THE NEED TO KNOW LINUX/UNIX, UNLIKE WITH OTHER TOOLS ON THE MARKET.”

Ing.Pavel Hejduk, Head of ICT Security Department, ČEZ ICT Services.

The ČEZ Group is one of the largest energy companies in Eastern and Southern Europe. The main business strategy of ČEZ Group is production, distribution and sale of electricity and heat. It employs 30,000 employees and operates in 10 countries in the region. The company group has about 9.3 million customers. At present, in terms of the number of customers, ČEZ Group is on the 7th place among the top energy companies in Europe. ČEZ ICT Services is a subsidiary of ČEZ, which provides information and telecommunications services for the entire group.

High security standards in the nuclear power plant

ČEZ faced with a large increase of IT devices to be monitored. In addition, the company was under pressure to increase work efficiency and reduce the number of employees at the same time. It also needed to improve the security of the document-management system of a special team. This team selects the general contractor for building the new blocks of the nuclear power plant in Temelín. The team members work on VDI-clients to access a SharePoint-application to collect, process and evaluate all documents arriving from tender candidates. ČEZ management specified strict IT and legal security requirements against this system to avoid legal disputations or possible lawsuits later. Consequently, ČEZ needed a heavyweight solution to meet two key expectations – advanced management of logs and audit of privileged users.

“OUR MAIN GOAL WAS TO PREVENT LEAKAGE OF INFORMATION OR ANY ACTION, WHICH WOULD HARM OUR IT SYSTEM. THESE INCIDENTS COULD HAVE LED TO CHOOSE ANOTHER CONTRACTOR FOR BUILDING THE NEW BLOCKS OF THE POWER PLANT, WHICH REPRESENTED A GREAT SECURITY RISK FOR US.” – *adds Mr. Pavel Hejduk, Head of ICT Security Department, ČEZ ICT* Services.

Strict log management and audit requirements

In the beginning, ČEZ ICT Services used the BalaBit syslog-ng Open Source Edition logging solution as part of their SIEM solution. Later they upgraded the log management component of the SIEM to a trusted logging infrastructure based on syslog-ng Premium Edition. However, requirements for this project were different:

- web-GUI,
- fast log search,
- easy backup/archive of logs,
- WORM (Write Once Read Many) log storage,
- encryption and time stamping of logs and
- High Availability (HA) support.

In terms of auditing, ČEZ required a single tool capable of authorizing administrators and recording administrative sessions. The support of all standard remote administration protocols - SSH, Citrix ICA and RDP - was an additional requirement. Since ČEZ did not have an internal solution to meet these expectations, they started to look for a commercial solution.

The Solution - Combination of BalaBit technologies

As ČEZ were using syslog-ng logging products with great satisfaction, they chose the BalaBit syslog-ng Store Box (SSB) appliance for log management purposes. In addition, except the BalaBit Shell Control Box (SCB) activity monitoring appliance, they did not find any competitive offering for transparently auditing privileged users. The planning, testing and implementation took 2 months. The new BalaBit solutions have been in productive operation since July, 2012.

THE IMPLEMENTED SYSTEMS

ČEZ uses a high-availability SSB cluster to collect the log messages of their production systems including 250 log source hosts. An additional SSB virtual appliance was also purchased (the virtual appliance runs on VMware ESX platform) for testing and development. To collect logs from Windows servers, ČEZ deployed the syslog-ng Agent for Windows with TLS encryption and mutual authentication.

For auditing privileged users, a high-availability SCB cluster has been implemented. SCB audits and monitors the administrative access to more than hundred servers and external communication stations (communication stations are special thin clients with strict policies, such as controlled email for example). An additional SCB virtual appliance was also purchased for testing purposes.

The new systems serve 150 users and 50 thin clients simultaneously, monitor eight IT and security administrators and protect 100 servers in 3 environments (production, test, development). Supported by strict SLA, the production environment is “hermetically” separated from the outside world (no Internet, no phones, no papers, etc.)

IMPLEMENTATION PARTNER – AXENTA A.S.

AXENTA a.s. was founded in 2009. Founders have been working in ICT since 1997. AXENTA clients include companies from the TOP 10 Czech companies, government institutions and several private companies from various business sectors. AXENTA consultants work for major customers in the Slovak Republic, as well. Employees have many years of professional experience with information security environments.

AXENTA has been working on common projects with ČEZ ICT Services and ČEZ Group since 2009. AXENTA has already closed several successful projects with the ČEZ Group in the field of implementation and development of a complex SIEM system.

AXENTA
Bezpečnost informací je pro nás na prvním místě!

Results - Highly secure operation, fast forensics

The SSB log server appliance was easy to deploy and configure. Archiving logs to WORM media and fast log search is a perfect combination for ČEZ security experts for daily operations management and forensics investigations, as well. Indexing of logs based on B-trees* results in really fast searching for any parts of the VDI-client and Active Directory server logs.

syslog-ng Store Box

> "SSB IS A LOG MANAGEMENT TOOL, IT EXACTLY DOES LOG MANAGEMENT. MANY COMPETITORS ARE TALKING ABOUT LOG MANAGEMENT, BUT, ACTUALLY, THEIR SOLUTIONS ARE ABOUT EVENT MANAGEMENT. IF YOU HAVE FOR EXAMPLE 40 TYPES OF LOGS, IMPLEMENTATION OF AN EVENT MANAGEMENT SOLUTION IS A PAINFUL AND TIME-CONSUMING EXERCISE. IN THE SAME SCENARIO, SSB CAN BE IMPLEMENTED IN A FEW DAYS."
>
> *- says Mr. Hejduk.*

BalaBit Shell Control Box

SCB was a bit harder to implement, but easy to operate. ČEZ benefits not just from its primary function (user authorization, audit and record sessions), but from a secondary one, as well: it provides complete documentation and replay of all configuration changes performed by implementation partners and internal administrators.

> "WITH ITS TRANSPARENT MEN-IN-THE-MIDDLE ARCHITECTURE, SCB IS A UNIQUE PRODUCT ON THE MARKET. SUPPORT OF SSH/ICA/RDP/HTTP(S) AUDITING AND REPLAYING, AS WELL AS OCR-BASED INDEXING AND SEARCHING IN A SINGLE BOX IS AMAZING."
>
> *– concludes Mr. Hejduk.*

** B-tree is a tree data structure that keeps data sorted and allows searches, sequential access, insertions, and deletions in logarithmic time. The B-tree is optimized for systems that read and write large blocks of data. It is commonly used in databases and file-systems.*

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe. More information: www.balabit.com

Learn More

- Shell Control Box overview
- syslog-ng Store Box overview
- Request a SCB online demo
- Request a SSB online demo
- Request a callback for SCB
- Request a callback for SSB