REGULATORY COMPLIANCE

Shell Control Box Use Case

The Challenge - Increasing Regulatory Pressure

Compliance is becoming increasingly important in several verticals - laws, regulations and industrial standards mandate increasing security awareness and the protection of customer data. Regulations like Sarbanes Oxley Act (SOX), the Payment Card Industry -Data Security Standard (PCI-DSS), ISO 27001, or the Basel II Accord all mandate the strict protection of sensitive information - be it personal data, credit card information, or financial information. For example, SOX mandates CEOs and CFOs to certify that all financial data provided to the auditors is accurate and have not been modified. If a firm fails an audit, management can even be sentenced to prison in case of serious infringements.

Consequently, companies have to increase control over and auditability of their business processes, including the activity of IT administrators or other super-users. Sensitive customer data is usually stored in a database on a central server, and is accessible only via dedicated applications, such as accounting software. However, the server storing the database has to be accessible also by IT administrators for maintenance reasons. Having super-user privileges on the system, these administrators have the possibility to directly access and manipulate the database, and possibly even to erase the traces of such actions from the logs. In addition, with standard log collectors only limited data can be collected and IT auditors would miss critical actions like viewing sensitive data or manipulating specific data. Missing items from the log collection system result in many question marks when an incident occurs. Therefore, organizations must find a reliable solution to be able to audit the actions of their IT administrators in order to ensure compliance.

Key Shell Control Box benefits for regulatory compliance

- control SSH, RDP, VNC, Citrix ICA, Telnet and other protocols
- granular access control policies (e.g. based on support time period or group membership)
- credential store (e.g. automatic password-based authentication)
- two-factor authentication
- 4-eyes authorization
- real-time session following with the possibility of instant termination
- automatic and customizable reporting
- tamper-proof audit trails

The Solution - Independent Audit Device

The BalaBit Shell Control Box (SCB) is a device to control data access: access to the servers where you store your important data. It is a unique solution for controlling and auditing administrator-level access to sensitive databases. The finest granularity of access management helps control who can access what and when. Being an enforcement point for company policies only authorized personal can access critical data. Being independent from controlled servers, it also complements the system and application logs by creating re-playable audit trails of user sessions. By the movie-like replay of actions the troubleshooting and forensics processes accelerate which reduces the operating risks of critical IT systems. The risk of data loss is also reduced, as the implemented SCB device represents both technical and psychological deterrent against malicious access. Using an independent device for auditing is advantageous for the following compliance reasons:

- SCB organizes the audited activities into sessions called audit trails, making easy to review the actions of individual users;
- SCB provides reliable, tamper-proof auditing data even of system administrator accounts who are able to manipulate the logs generated on the servers, and
- SCB allows you to create an independent auditor layer which can control, audit and review the activities of the system administrators, while being independent from them.

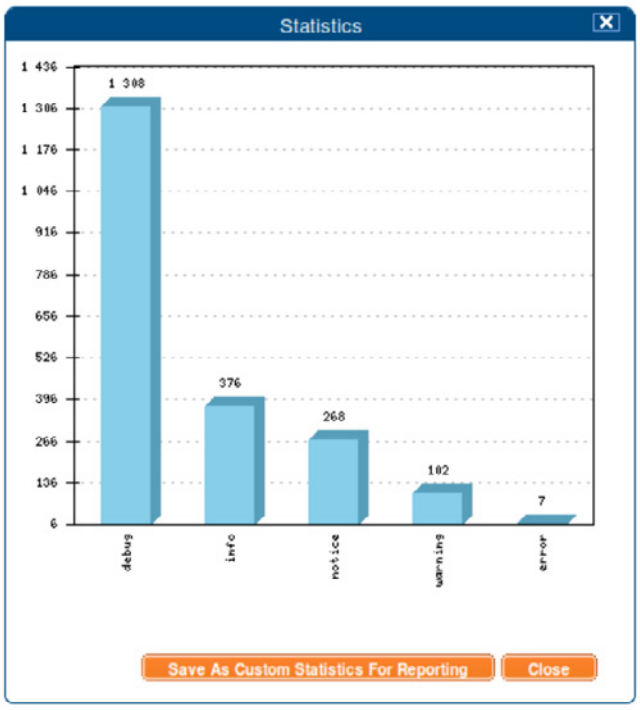

Figure 1. Custom SCB report for compliance

Technical Implementation

SCB is a proxy gateway: the transferred connections and traffic are inspected on the application level (Layer 7 in the OSI model), giving control over protocol features like the authentication and encryption methods or the permitted channels. SCB is an independent device that operates transparently, and extracts the audit information directly from the communication of the client and the server. This prevents anyone from modifying the audited information – not even the administrator of SCB can tamper with the audit trails, which can be time-stamped, encrypted, and digitally signed. For example, SCB records as your administrator configures your database servers through SSH, or maintains your mission-critical SAP application at night.

SCB records the entire network flow between client computers and servers, which also includes keystrokes and mouse events generated by end-users. This means, that even if someone tries to hide some activities (e.g. turns character echoing off in an SSH terminal), commands typed in and executed in an audited connection are still available in the audit trail files. The content of the audit trails can optionally be indexed to make searching for events and automatic reporting possible. To make integration into your network infrastructure smooth, SCB is available both as hardware and virtual appliance, and supports several different operation modes.

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 homepage
- ISO 27001 - Achieve the impossible
- PCI and ISO 27001 compliance and forensics in auditing remote server access
- Creating Value Beyond Compliance
- Shell Control Box SOX Sheet
- Request an evaluation version
- Request a callback