HARDENING AND MONITORING

Kaduu AG, Chamerstrasse 172, 6300 Zug, Schweiz, support@kaduu.io, www.kaduu.io

MONITORING & HARDENING OF KADUU SERVERS

All security software is distributed, installed and configured using Playbook Ansible in automated mode.

Centralized installation and configuration of the security software allows us to achieve the unified automation for rapid installation and configuring of any server. After the installation of the protection tools, the system check is performed using Lynis tool.

KADUU server's protection tools

1. All servers have configured Firewall to restrict access to the servers. The access is only allowed for the System Administrator and Support team.

2. Fail2ban daemon is running for protection from brute-force attacks, it is configured to protect SSH.

3. Auditd daemon provides the detailed information about all system events, especially information on security violations that allows to take necessary actions. The event information is available in log files stored locally.

4. Lynis – a flexible tool that is normally executed after installation of a new server and allows to check a new system in the following ways:

- Security audits
- Compliance testing
- Vulnerability testing
- Vulnerability detecting

System hardening

1. Rkhunter – is executed weekly, it is used to scan the server for rootkits, backdoors and possible local exploits. The scanning results are available in log files stored locally.

2. Zabbix agent – is used for monitoring processes and hardware on the Kaduu server.

3. Backup script – is used for encrypting KADUU backups and transferring backups to the backup server.

Monitoring

Properly configured Zabbix agents are running in 24×7 mode on all KADUU servers, they are used for monitoring processes and daemons required for successful operation of KADUU. Zabbix agents keep connection to central stand-alone Zabbix server and report all important events to it. Zabbix server send alarm e-mails to System Administrator and to Support team in case of problems. Based on monitoring alarms System Administrator or Support team immediately react to any problem found, e. g. server crash, network unavailability, insufficient disk space, etc.