EKRAN

CASE STUDY

Featured story: Finance

UKRSIBBANK
BNP PARIBAS GROUP

Audit of remote administrators accessing critical endpoints

Ukrsibbank Case Study
Remote Administrator Audit

UKRSIBBANK
BNP PARIBAS GROUP

CUSTOMER

Ukrsibbank is a subsidiary of international BNP Paribas group holding position in the Top 10 financial services institutions of Ukraine. UkrSibbank serves about 2 million retail clients. Due to its strategic partnership with BNP Paribas, UkrSibbank can be named as the most robust and stable bank in Ukraine. Bank takes care steadily of innovations, new services and technologies adoption.

CHALLENGE

Ukrsibbank serves more than 400 branches, 1000 ATM, and millions of individuals and corporate accounts all over Ukraine. The Bank uses outsourcing services working with the skilled specialists, in particular to maintain its server infrastructure and back-end software environment.

This practice implies security concerns related to remote access of third-party administrators to the critical infrastructure end-points enabling configuration changes, potential backdoor injections, changes in availability, and potential breach to the sensitive data.

Those critical endpoints are also accessed remotely by the in-house administrators, whose work also needs thorough security audit.

The security department of Ukrsibbank insisted to have an exhaustive remote administrator activity audit solution enabling complete reconstruction of any action performed on the critical endpoints and quick incident response.

SOLUTION

Ukrsibbank specialists conducted detailed research of the privileged user activity audit tools available on the market and chose Ekran System to be installed on the servers accessed by third-party subcontractors' staff.

The main benefits resulting in Ekran System winning this bid were:

- Universality: the solution provided cross-platform audit for Windows, Citrix, and Linux servers;
- Easy-to-analyze yet informative video format. The security specialists of the bank are skilled administrators and can quickly reconstruct the issue watching the sequence of the user actions on the screen. Additional log details, like executed commands with parameters, provide all necessary details;
- Strong protection of the monitoring process. As the level of required security is extremely high, the security personnel must be sure that the monitoring process is unstoppable even by the skilled administrators with high access privileges. Ekran System provides protection at all levels.

One more reason to choose Ekran System was the favorable flexible licensing, which enabled painless risk-free pilot deployment on the limited number of Windows and Linux servers, before considering an option of global system installation.