Customer

SLOVENSKÁ sporiteľňa

Industry

Financial Services

Challenges

- *An extensive WAN network including more than 150 branch facilities, 100+ independent LANs and two data centres*
- *Existing monitoring was unable to provide sufficient information for network management and security*
- *A lack of information about the operation and the benefits of events occurring on the internal network solution*

Solution Benefits

- *Network visibility, including a detailed overview of the behaviour of users and devices in the network*
- *Increased security for computer networks and controlled access to ICT resources was established*
- *More effective management and supervision of the network*
- *Assistance with troubleshooting and resolving network problems*

Deployed Products

- *Flowmon collector*
- *Flowmon probes*
- *Flowmon ADS*

Contact

www.slsp.sk

Slovenská Sporiteľňa

Slovenská Sporiteľňa is the leading savings bank of Slovakia with the longest history in the country. In 2001, the company become part of the strong financial group Erste Bank der oesterreichischen Sparkassen AG. Slovenská Sporiteľňa is one of the largest banks in the country with nearly 2.4 million clients and more than four thousand employees. It is the market leader in providing retail loans and deposits. It also holds primacy in the number of ATMs and branches, operating 292 branches and 17 corporate centres.

Situation

The company‘s network department solves dozens of tasks relating to management of the regular IT infrastructure on a daily basis. From an IT security perspective, there was a lack of necessary visibility into the existing network infrastructure. Therefore, a request for data network traffic monitoring implementation with the following requirements arose:

- complete WAN monitoring (branch network across the whole of Slovakia),
- detailed LAN monitoring, including two data centres and DMZ,
- effective administration and supervision of the network, assistance with troubleshooting and resolving network issues,
- network traffic analysis and evaluation for the purposes of detecting security incidents and anomalies

Flowmon Solution Deployment

The company´s requirements have been resolved by the distributed Flowmon solution consisting of:

- a central 12TB Flowmon collector,
- four virtual Flowmon probes that have been implemented in areas where monitoring QoS / VoIP parameters, or localities with no devices with NetFlow data export capability, was necessary,
- 25 active elements exporting NetFlow data to the central collector.

The solution mentioned above is fully integrated with the SIEM system using internal syslog messages, for the purposes of single site collection and evaluation of security incidents. As above, the Flowmon logic set up multiple correlation rules, and together with Flowmon output operates Incident Management under the existing processes.

Customer Review

Jan Adamovsky, CISO of Slovenská Sporiteľňa, evaluates the deployment of the Flowmon solution:

"Flowmon provides us with network visibility which we had previously lacked. Thanks to the integration with standard security incident process management, we have increased our ability to identify incidents and react in a timely manner."