Customer:

BVV Veletrhy Brno

Industry

Organization of trade fairs and exhibitions

Challenges:

- *Large computer network including more than 60 active components (routers/switches)*
- *Complete Wi-Fi coverage of fair area*
- *Traffic statistics collected as summary of data transferred over network interfaces*
- *Difficult identification and investigation of network intrusions and problems by manual data analysis*

Solution benefits:

- *Considerably lowered expenses of network administration*
- *Automation of network administration and security tasks*
- *Tailored to meet actual needs*
- *Excellent price to performance ratio*
- *Easy to extend*
- *Insight into network focused on behavior of users and devices*

Products:

- *FlowMon ADS Standard*
- *FlowMon Probe 2000*

Trade Fairs Brno is the leading brand in trade fairs and exhibitions in Central Europe. The main scope of activity is the organizing of trade fairs and exhibitions. Further activities include organization of accompanying program events along with fairs, as well as the provision of all services that relate to the holding of trade fairs and exhibitions.

Infrastructure

Network in Trade Fairs Brno can be described as cascaded-star configuration. The main device of this network is a central switch, where all the outgoing and incoming traffic goes through and also client – server communication. The second most important switch, where web server is connected, is located in DMZ.

Network infrastructure use only active devices from Cisco. Thanks to this fact it enables the customer to extend Flowmon solution any time by using Cisco ability to generate network traffic statistics – NetFlow; allowing these data to be processed by already implemented **Flowmon ADS**.

Customer challenges

- Effectively check compliance with security policy and laws
- Have a tool for detection and fast analysis of inside and outside attacks
- Detect leaks of sensitive information, social engineering
- Check QoS delivered by suppliers, network and service latencies
- Eliminate undesirable applications and data sharing
- Detect infected devices inside network

Solution

Flowmon Probe 2000's first monitoring port is connected to SPAN port of central switch, while the second port to SPAN port of DMZ switch. These switches are mirroring entire network traffic going through to these monitoring ports.

Flowmon ADS Standard continuously and automatically performs analysis of data collected generating events and reports on the fly.

Customer review

Ing. Heršálek, system administrator stated:

"In the past we have been monitoring our computer network just by collecting information about data volume on IP layer and key protocols. Whenever we want to analyze certain data flow, which we have identified as suspicious, we had to undertake painful way of manual analysis. This way proved to be very problematic especially, as it was extremely time-consuming. Performing this type of analysis we could even miss certain anomalies or attacks, which were distributed into longer time in low intensity. With automatic behavior analysis provided by Flowmon ADS we have now complete real-time overview about attacks and problems in our network and we are able to solve it very effectively."