Key and integrated components of Security concept

Monitoring: across all sections of data networks – L2 monitoring, L3/L4 traffic monitoring

Behavioral analysis of network: automatic detection of security and operating incidents

Network access control: restricting of access only for authorized devices

SIEM: complex evaluation and management of informational security

SOC: Consecutive security operation centres, cooperation with CSIRTs

First step for application of the Concept in the organization is always security analysis, which allows to map out current situation and propose concrete solutions.

Fulfilment of the IT infrastructure Security concept

In Czech Republic is engaged a number of subjects in issues of monitoring IT systems and applications, supervisory tools and managing of information security. There are also specialized manufacturers whose technologies enables effective realization of introduced concept. These are the products:

FlowMon (INVEA-TECH): solution for monitoring, analysing data in network traffic and automatically identification of operating and security incidents

MoNet (NOVICOM): a tool for advanced IT infrastructure monitoring across all sections of SLA continuous evaluations

AddNet (NOVICOM): a tool for address planning and controlled access into the network with integrated services DHCP, DNS, Radius

APM (FerretApps): a tool for monitoring of applications

Referred group of producers complements another member of the NSM Cluster, company **AXENTA**, with their know-how and knowledge in Security management process and practical experiences with the implementation of tools for Log management and SIEM systems from world renowned manufacturers.

The indisputable advantage of Czech manufacturers are mutual interconnection and compatibility of individual systems. Due to the mutual integration is for example possible to indicate security incident recorded by using FlowMon ADS at MoNet dashboard and appropriate device directly disconnect by using AddNet. The event is recorded in Log management and classified in SIEM where is finally projected in the reporting. The concept of active network security is an example how to secure the IT infrastructure of the organization in accordance with current legal standards and high effectivity. The concept is only recommended attitude. Application itself of the individual components into a specific computer system organization need to be addressed individually as required by the top management of the organization and demands of the network.