The concept of active security and reliability of IT infrastructure NSMC security concept

Each organization using the ICT tools and technologies solves issues of safety and ensuring the continuity of their processes. The fact, that this is the most actual topic is evidenced by the recent developments in the field of legislation that approved legislation about cyber security law and establishment of the National Centre of cyber security within the National Security Authority Czech Republic. We introduce the concept of active security and reliability of the IT Infrastructure that is based on real needs and the requirements of the law.
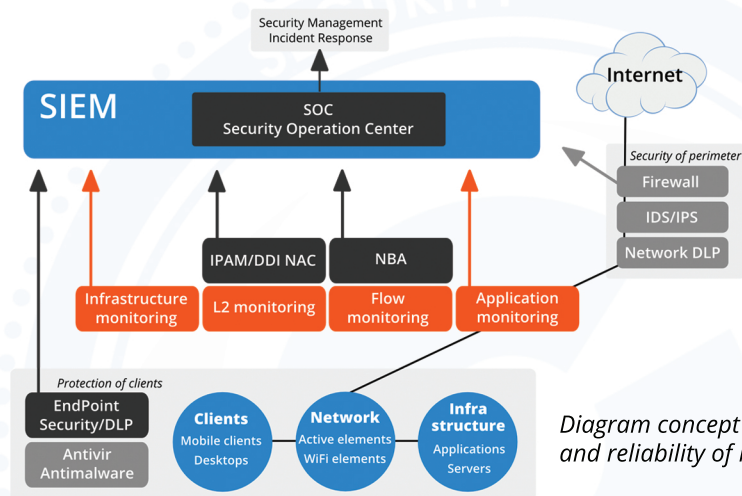

Diagram concept of active safety and reliability of IT infrastructure

The concept respects current functioning and practices of organizations in the field of information technologies and in work with data. It also responds to new requirements that in this area puts valid and also prepared Czech and European legislation.

In the current infrastructure of an organization is added sophisticated monitoring tools and methods. These are further extended by integrated advanced analysis tools for data network traffic (NBA - network behavior analysis) together with tools for complex administration of IP address space and management of access for fixed and mobile devices into the network (IPAM/DDI/NAC). These tools can be properly supplemented by means of complex protection for client stations (End Point Security). Commonplace is coexistence of the safety concept with common components of perimeter protection (firewall, IDS/IPS, DLP, etc..) and clients (antivirus, antimallware, antispam, etc..). Deploying introduced components in practice means that security and reliability becomes a direct attribute of IT infrastructure, and as such it is impossible to bypass or eventually disrupt it.