The Governmental Computer Security Incident Response Team

https://csirt.gov.pl/cee/arakis-gov-system/78,ARAKIS-GOV-system.html
2021-12-09, 02:11

ARAKIS-GOV system

ARAKIS-GOV is an early warning system reporting threats arising on the Internet. The system has been developed by the IT Security Department of the Polish Internal Security Agency in cooperation with the CERT Polska team operating within the NASK organization. It was established in order to support the existing security measures protecting IT resources of public administration as a result of extending the ARAKIS system created by the CERT Polska by an additional functionality.

ARAKIS-GOV is not a typical security system. By no means could it replace functionalities of standard network security systems, such as a firewall, antivirus software or IDS/IPS.

Nevertheless, taking into account its specific nature, ARAKIS-GOV may well be applied as a supplement of the above mentioned systems, providing data about:

1. new (global) threats arising on the Internet, including:

    newly detected self-propagating threats of the worm type;

    new types of attacks observed from the level of numerous localizations;

    activity trends for network traffic on individual ports;

    activity trends for viruses disseminated via electronic mail;

2. local threats connected with a specific secured localization:

    lack of up-to-date antivirus vaccine;

    infected hosts in the external network;

    leaky borderline configuration of the firewall systems

    scanning attempts of the public address space both from the Internet and the internal network

Additionally, tools implemented in the system make it possible to compare statistics of network traffic viewed from the level of a protected localization with a global picture coming from all the installed sensors as well as imaging the geographical location of the suspected traffic. It is unique to the ARAKIS-GOV system that it does not in any way monitor the content of the data exchanged by the secured institution with the Internet. It is possible due to the fact that system sensors are installed beyond the secured internal network of the institution, on the Internet side.