Customer

ORANGE

Industry

Telecommunications/ISP

Challenges

- *Network traffic visibility (based on NetFlow) for troubleshooting*
- *Detection of attempts to crack passwords to standard access mechanisms*
- *Detection of DDoS attacks*
- *Detection of traffic anomalies*

Solution Benefits

- *Full IPv4/6 traffic visibility*
- *Easy detection of attacks on network services*
- *Detection of DNS and NTP traffic anomalies*
- *Detection of malicious activities and applications*

Deployed Products

- *Flowmon Collector*
- *Flowmon ADS ISP*

Contact

www.orange.pl

Orange Polska S.A.

Orange Polska is a member of the international group France Telecom and one of the largest telecommunication operators in Poland and Central and Eastern Europe. It is the biggest Polish provider of broadband high-speed Internet with the widespread mobile network covering whole Poland. The company provides professional B2B telecommunication services including commercial and regulated ones. Within the company there is established a specialized unit Orange Poland CERT (Computer Emergency Response Team), which is responsible for the safety of Internet users of this network provider.

Infrastructure

After the investments in 2014, the operator's network equipment is ready to establish connections at 100 Gbps speed. Orange Polska has added new fiber optic lines under the use of the mobile network and the introduction of new standards for data transmission to expand 4G LTE network capabilities.

Orange team required a suitable solution to:

- Visualize and analyze network traffic with high intensity (10Gbps or more),
- observe network traffic characteristics according to particular applications, subnets, communication between servers,
- the solution should enable traffic visibility and detailed analysis of the data collected up to a year back.

Flowmon Solution Deployment

Due to the need for high system performance, long-term storage of data and the possibility of using additional modules, a hardware Flowmon collector was deployed. Data for the analysis is provided by the network using NetFlow. The collector stores the data for the desired period of time, provides visualization, analysis and reports for network engineers. It is the central point with Anomaly Detection System module so it is used also by the security engineers. The solution analyzes generated flows and reports potentially dangerous network attacks and events or anomalies. Therefore it makes possible to see unwanted network communication and violations of safety rules in activity caused by malware or viruses.

Customer Review

Robert Grabowski, Security Expert of ICT systems at Orange Polska, summarizes Flowmon solution deployment as follows:

"*Flowmon solution is widely used in our company both by network and security engineers. Everyone receives the most important information necessary for his work. ADS is used to quickly detect sources of security incidents and to increase protection of our customers. The most beneficial is an automatic detection of attacks and traffic anomalies with detailed information about particular events, including involved flows. This functionality decreases the time needed to evaluate potential risks so we can focus on other important activities knowing that everything is under control.*"