CASE STUDY

Electrolux chooses SGBox to improve the security of its IT infrastructure

Company
Electrolux

Sector
Manufacturing

Implementation
Log Management

Objectives

- To increase IT security
- Fast, accurate research
- Dynamic management of information gathered

"After careful analysis, we chose SGBox as an ideal partner which could be easily integrated into our systems. It has shown itself to be an open log platform, able to gather information from any system type. It is easy to use and quick to implement and is compatible with the entire IT security infrastructure."

Fabrizio Di Narda - Team Leader, IT Security Infrastructure EMEA Electrolux

Electrolux is a global leader in the household appliances and appliances for professional use sector. Every year, the company sells more than 50 million products to consumers of over 150 countries offering innovative solutions developed after in-depth consumer research to meet the wishes of today's consumers and professionals. Electrolux's products include refrigerators, dishwashers, washing machines, kitchen appliances, air conditioners and small household appliances like vacuum cleaners, all sold with brands like Electrolux, AEG, Zanussi and Frigidaire.

In 2014, Electrolux reached a turnover of around €12 billion with a total of 60,000 employees.

In Italy, Electrolux has important production units and around 6,000 employees. It operates through industrial, distribution and service companies both in the household appliances sector, covering the family market, and in the professional appliances sector, serving professional use.

Electrolux Italia SPA produces around 3.8 million household appliances a year in its four factories and also carries out an important innovation role through its Research & Development and Planning laboratories and its Data Center.

Challenge

All the components which make up the ICT security infrastructure of Electrolux generate a large quantity of different logs. These logs are important information and must be stored and converted into a single format which can be handled centrally. If any infringement of the data on the network infrastructure occurs, the log history should be easily accessible and should be able to be correlated to help the system administrator monitor the specific information. Many security components of European sites such as firewall, server proxy or load balancer, generate an enormous quantity of data to be managed centrally.

Electrolux required a system for handling logs centrally which would allow it to reinforce the security of the entire IT infrastructure. When, in the majority of cases, each system produced a proprietary log format, in the case of infringement of data, it would not have been possible to save or access easily all the historic records to find and resolve the problem. This would lead to a delay in the IT infrastructure with a loss of time and money.

Solution Adopted

Electrolux has adopted the SGBox solution, implementing the SG-Log module which allows logs of any format from any source to be gathered. The logs gathered, which are stored in encrypted, original format, are processed to extract the associated events which can be easily analysed in real time or on an historic basis. In this way, it is possible to reach optimum normalisation access and to gather and recognize significant network events such as, for example, errors detected in certain requests by load balancer and reverse proxy. It also enables anomalies to be detected in the number of attacks the network has received, both internally and externally.

> ***"A log management system is obligatory for all the critical components of the ICT security infrastructure in order to reduce the risks stemming from the loss of data"***
>
> **Fabrizio Di Narda -** Team Leader, IT Security Infrastructure EMEA Electrolux

Just as companies do, the network also produces a large number of diverse logs, each one in its own proprietary format. SGBox is able to handle standard syslogs natively as well as being designed to gather logs of all sizes. Having implemented the SGBox module, Electrolux has decided how many logic groups the monitored infrastructure is divided into. Two distinct groups have been created: one to gather information provided by UNIX services and another for the load balancers.

Information gathered in this way is ready to use for all analysis functions available natively on the platform. The SGBox solution is used for log management, running on hardware and logs open at the time of transmission for some devices such as BlueCoat Proxy and Check Point Firewall. It is currently used for managing events for more than 70 devices.

Future Developments

SGBox seems to be a highly efficient solution for the company's aims. By using it, Electrolux has succeeded in achieving a centralised system for managing all information and logs from the entire company network. This has enabled it to increase the security of employees and has reinforced further the capacity of SGBox to predict dangerous incidents even before they happen, saving time and costs on each problem resolved. For the future, Electrolux plans to extend its use of SGBox. The company expects to use the advantages of the server log for correlating events and to use the network monitoring module which was developed to extend the solution to all network devices.