EXPERT OPINION

Security: It's not *if*, it's *when*

As security threats become more sophisticated and literally every business is a potential target, only a holistic security approach offers the right combination of prevention, detection and protection.

Although cybercrime has been around as long as the Internet itself, its face changed radically over the years. Today, cybercrime has the size and maturity of a true, worldwide industry, run by organized crime and based on proven business models. Social engineering remains an important instrument to trap potential targets. At the same time, purely technical attacks have become industrialized and automated. A wide range of malware, ransomware, DDoS attacks and other malicious solutions are simply available as a service, as if they were regular IT commodities.

Taking measures to keep the bad guys out is no longer enough these days. Prevention, detection and protection go hand in hand. Every business is a potential target. It's no longer "*if or when you are attacked*", but "*did you know you are under attack, and why and by whom*" you are attacked. And of course, when it happens, you need to have the right answer ready. Not just to contain the incident and avoid further damage, but also because the GDPR requires appropriate action. And there's more where that came from, as European law makers are preparing new regulations like the NIS, setting new standards for proper IT and data hygiene.

We practise what we preach

Sopra Steria helps businesses develop the holistic security approach they need. First of all, there is a strong emphasis on prevention. Are the right security processes in place? What about process management and security tools? As a company keeps focusing on its business objectives, we are taking care of all necessary managed security services. At the same time, monitoring is an integral part of our security approach as well. Tools for threat detection enable the organization to immediately take the right measures.

Putting our take on a complete security solution into practise, Sopra Steria implements and integrates the same tools we use to back up our very own security strategy. We practise what we preach. The expertise we have developed in our own backyard of course is extremely helpful to our customers as well. Key tools in our security landscape include LogRhythm, Qualys and CrowdStrike.

Full circle

LogRhythm is a SIEM tool (Security Information & Event Management). It finds the correlation between separate events and sends out alerts accordingly. Qualys helps businesses automate auditing, compliance and protection of their IT systems and web applications, among other things by scanning for vulnerabilities, controlling patch levels and checking technical state compliance. The information is fed back into the SIEM tool to enhance the risk – awareness of the monitoring systems.

Last but not least, CrowdStrike offers endpoint protection and threat intelligence, based on what this next-gen antivirus solution picks up on the network. Following the analysis of the data, the information is fed back into the tool and integrated with the SIEM tool. This way, Sopra Steria's security approach comes full circle…

Would you like to learn more about Sopra Steria's security services? Contact Dirk Nijs, Senior Security Expert

Sopra Steria - Communication & Marketing
bnl-communication@soprasteria.com
www.soprasteria.be

sopra steria