SECURITY

CONNECTIVITY INCREASES THREAT LEVELS

The "Internet of Things" and "Industry 4.0" characterise a development, by which the whole society is penetrated by information and telecommunications technology: people and devices connect via internet, privacy and data protection are becoming increasingly important. The IT, which is the foundation of it all, must therefore have maximum security and protection. Two examples: when hackers attacked the major U.S. bank JPMorgan Chase, they stole data on millions of accounts. According to information provided by the company, 76 million private households and seven million companies were affected. Even Apple's App Store, which was previously thought to be very secure, was also penetrated by hackers. Malware was apparently found in hundreds of apps.

TIME FOR THE IT TO ACT

As both examples show, even companies and organizations that seem to have strong protection still need to fortify their IT security. This is primarily the responsibility of the IT organization, where worry about whether they have taken the right security precautions is the order of the day. Despite constant budget pressures and a potential shortage of IT security experts. According to a representative study, companies need more than 200 days on average to even discover that they've been the victim of an attack.

That's why an IT outsourcing partner is the right choice: a specialist that has access to all the crucial expertise and resources 24/7.

EXPERTISE

Deutsche Telekom and T-Systems employ more than 1,500 security specialists. To identify new attack vectors, the Telekom computer emergency response team (CERT) searches the Internet and the Telekom networks for anomalies. Its unique combination of IT and network security skills means Telekom can cover LANs/WANs, carrier backbones and even mobile networks.

TRANSPARENCY

With more than 180 sensors distributed across the globe, Deutsche Telekom generates a big picture of the current threat level posed by cyber-attacks: These systems, called "honeypots", simulate weaknesses, such as smartphones with vulnerabilities, and provoke hacker attacks – more than a million every day. The information gained from these attacks enables the development of more effective defenses against cyber-crime. An online portal operated by Deutsche Telekom, www.sicherheitstacho.eu, provides insights into this early-warning system.

T · · Systems ·

STRONG SECURITY IS IN OUR CORPORATE GENES

Deutsche Telekom was one of the first DAX-listed companies to elevate the topic of security to the board level, incorporating it in the Data Privacy, Legal Affairs and Compliance department. Telekom also introduced the Privacy and Security Assessment several years ago. This process entrenches the technical security and data protection aspects in development processes early on, deep in the company's DNA. Security is a design factor here.

LEADING SECURITY VENDOR

According to the Experton Vendor Benchmark 2015, Deutsche Telekom is the "measure of all things" for managed security services in Germany. The analysts reported that Telekom has an extremely attractive portfolio and proven competitive strength. The "Security Vendor Benchmark" study also placed Telekom in the "Leader" category in five other areas: Cloud and data center security; backup/archiving/high availability; identity and access management; and IT security consulting & professional services.

T · · Systems ·

2016, T-Systems International GmbH