



Top-down instead of bottom-up: Cyber security has to be a C-Level priority

2020-11-02

Munich

Giesecke+Devrient

The importance of an integrated IT security strategy is steadily increasing, especially in current pandemic times. The accelerated digitalization in almost all areas of life has broadened the scope of possible attacks by hackers. With isolated bottom-up projects, it is nearly impossible to guarantee a comprehensive high level of security in view of such complex threats, says Giesecke+Devrient (G+D). Instead, a holistic top-down approach is required. Cyber security must become a management priority.

Cyberattacks are increasing in complexity and sophistication. Simultaneously, the IT dependency of companies, public authorities and private individuals continues to grow. The expanded use of cloud services and new developments such as Smart Cities or Smart Homes will drastically raise risk potential once again.

The level of threats presented by internet criminals is high and will remain so. According to the recent special expert report "Cybercrime in times of the Corona Pandemic" from the German Federal Criminal Police Authority: "Due to ongoing threat that the pandemic poses to the state and public life as well as the continuous shift of various aspects of life into the virtual domain, the threat level in cyberspace is considered to be permanently high."
(1)

In recent years, companies have increasingly invested in IT security. Despite all efforts, however, major challenges remain, which require an expansion of existing security concepts. According to the German federal Association for information technology, telecommunications and new media Bitkom, the total damage to the German economy in 2018 and 2019, caused by data theft, sabotage or espionage, is more than 100 billion euros – and the numbers is rising (2).

In many cases, efforts by companies are also insufficient, because singular security measures are often implemented by individual departments, resulting in so-called IT security silos. Isolated solutions that only address a specific security issue - such as perimeter protection or application-related measures - cannot provide a consistently high level of security. Such a bottom-up strategy is not effective and this is why IT security experts have long been pressing for executives to take a holistic approach to the problem.

As a result, a comprehensive IT security strategy must be developed, established and consistently implemented. IT security has to be part of the corporate strategy. And this is where companies need to follow a top-down approach: Only the top management can establish an overarching, sustainable master plan, set priorities, create the essential structures and provide the necessary budgets.

Therefore, the company-wide security strategy and culture must be initiated by the company executives. But of course, such a culture must also be adopted, and consequently the individual employee is also of crucial importance.

Even with the best strategy and use of the latest security solutions, the individual employee remains a potential gateway for phishing emails and social engineering. This occurs, for example, when there is a lack of awareness for cyberattacks and security. Thus, raising employee's perception of potential security threats, scheduling trainings and communicating best practices for the secure use of information technology are indispensable components when implementing a company-wide security strategy. A deep-rooted understanding of cyber security has to be in the mindset of all company employees.

"Especially in these times, cyber security is the decisive success factor for further digitalization. That's why we must both raise awareness and increase our investment in IT security and the corresponding infrastructures," explains Ralf Wintergerst, Chairman of the Management Board and Group CEO of Giesecke+Devrient. "Both tasks clearly fall within the responsibility of the top management."

"And in doing so, an essential point must not be overlooked," Wintergerst continues, "we should view IT security as an opportunity and not as a necessary evil. After all, the security of networks and communication infrastructures is more important than ever."

See:

(1) [Cybercrime special evaluation Corona 2019](#) ■

(2) [bitkom study economic protection](#) ■

About Giesecke+Devrient

Giesecke+Devrient (G+D) is an international Group providing security technology and headquartered in Munich, Germany. Innovations by G+D make the lives of billions of people in the digital and physical world more secure. With its products and solutions, G+D is one of the market and technology leaders in payments, connectivity, identities, and digital infrastructures.

Established in 1852, the company achieved sales of Euro2.45 billion in the fiscal year 2019 and employs 11,500 people. G+D has a presence in 33 countries. Its customer base includes central and commercial banks, mobile network providers, automotive manufacturers, health insurance companies, and governments and public authorities. Further information: www.gi-de.com.