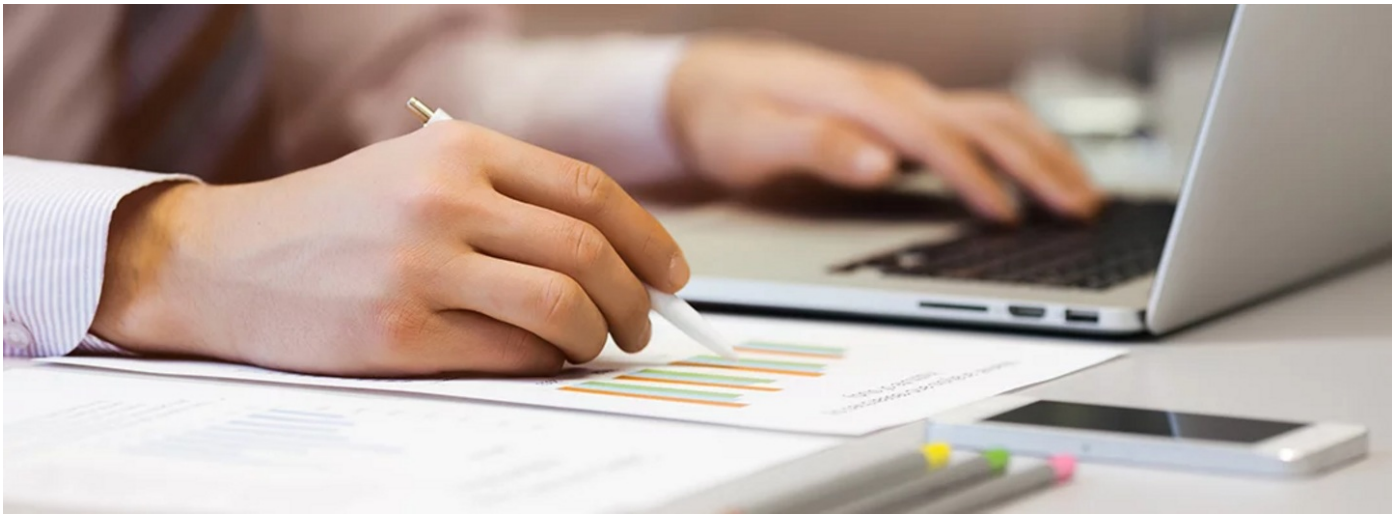

Cybersecurity demands proactive design thinking

2021-10-20 | Munich | Giesecke+Devrient

Cybercrime has become an everyday threat for both private companies and public institutions However, the annual European Cyber Security Month, which takes place in October, is another reminder that there is still far too little investment in the prevention and defense against cyberattacks. In many cases, cybersecurity is still seen as a nuisance. But there is an urgent need for action in this area. After all, cyber security can be a growth driver in the digital age.

Every area of our lives is somehow connected to the digital space. Today, we assume that there exist 30 billion digitally connected devices worldwide – in five years, that number is expected to lie closer to 75 billion. This digitalization push provides us with enormous added value, but it comes at a price. Securing this so-called "massive connectivity" from cyberattacks is therefore emerging as the central pillar in making our society and economy less vulnerable.

Nevertheless, cybersecurity is still often seen as a pesky chore. Yet in such a digital world, companies and institutions should not only to react situationally to attacks, but rather actively analyze threat situations and derive concepts from them at an early stage. That way, organizations can ensure the protection of their systems and the continuity of operations.

Additionally, new trend technologies are regularly entering the market, many of which will be decisive for technological development and the leading economic role. Whether it’s cloud computing, edge computing, the Internet of Things, artificial intelligence or, in the future, quantum computing, data security and cyber resilience are a fundamental part of organization and business models.

"Cybersecurity has moved to the center of corporate and political attention," explains Ralf Wintergerst, CEO of Giesecke+Devrient. "This is not surprising, as incidents like those concerning Kaseya or Solarwinds regularly leave us holding our breath. That is why it should become standard to spend from 15 to 20 percent of the IT budget on increasing IT security, both for companies and government institutions. However, it is just as important to be able to switch from defense mode to active design mode when it comes to security. We need to be active on many fronts."

To actively counter this situation, a holistic approach to cybersecurity is needed, one which takes all of these changes into account and defines prevention strategies. These well-designed defenses at the corporate and institutional level are the basis, but will not be enough. They must be accompanied by a European initiative that establishes cybersecurity as an all-emcompassing concept. There are already many ideas for this, created by both government and private players. The GDPR, which was established two years ago, is the first step in this direction. But Europe needs more. Namely its own, possibly state-supported concept for increasing cyber security and cyber resilience. This way, companies and institutions within the continent can join forces to make themselves strong against latent threats from outside.

About Giesecke+Devrient

Giesecke+Devrient (G+D) is a global security technology group headquartered in Munich. As a partner to organizations with highest demands, G+D engineers trust and secures essential values with its solutions. The company's innovative technology protects physical and digital payments, the connectivity of people and machines, the identity of people and objects, as well as digital infrastructures and confidential data. G+D was founded in 1852. In the fiscal year 2020, the company generated a turnover of 2.31 billion euros with around 11,500 employees. G+D is represented by 74 subsidiaries and joint ventures in 32 countries. Further information: www.gi-de.com.