Sebastian Pohl is an advocate of timely prevention in Cybersecurity Matters

Many companies are still too lax when it comes to the security of their own information. After all, we read or hear about serious cyberattacks on company systems almost every day. These attacks are motivated by the fact that huge quantities of valuable and confidential information are generated and processed on a daily basis. This data – stored not only on internal servers and devices, but also in external data centers – now represents an organization's greatest asset. It therefore has to be protected.

In multiple studies, the German Insurance Association (GDV) has determined that almost one in four small or medium-sized retail or logistics companies has been targeted by cyberattacks. In many cases, the criminals' work is made easier by outdated systems, limited awareness of the problem, and inadequate precautions.

In my own experience, the risks and vulnerabilities are downplayed, not taken seriously enough, or consciously ignored at many companies and organizations. According to a representative Forsa survey of 300 wholesale/retail and transport companies carried out on behalf of the GDV, almost two thirds of respondents (63%) underestimate the risk to their own company.

Almost every company has vulnerabilities in terms of information security, with the responsible officers often unaware of the problem. The Hiscox Cyber Readiness Report 2022 indicates that cyberattacks in Europe cause damage of approximately €19,000 on average – a figure that is significantly higher than the rest of the world.

There is also no end in sight; on the contrary, experts anticipate that cybercrime will rise by a loss amount of more than €5.8 trillion by 2028. It is also estimated that up to 33 billion online accounts will be misused by the end of 2023, which equates to an average of 97 cybercrimes an hour.

The question is therefore not whether a company will fall victim to a cyberattack, but when.

Given these statistics, it is astonishing that only slightly more than half of companies in Germany 54 % have an emergency plan with written procedures and ad hoc measures to deal with cyberattacks. This was one of the findings of a 2022 study carried out by IT industry association Bitkom, which also showed that larger companies are better prepared than smaller ones. Firms with 100 to 500 employees 71 % and those with 500 and more employees 78 % have damage limitation processes in place much more often than smaller companies with ten to 99 employees 51 %.

According to the survey, companies need to make up lost ground in terms of raising employee awareness of the topic. 61 percent conduct regular training on the topic of information security, with no difference between larger and smaller companies in this regard. A further 13 percent plan to offer training, but one in four companies 25 % still intend to forgo training in the future.

"The question is not whether a company will fall victim to cybercrime, but when."

Despite preventive measures such as backup servers and the raising of employee awareness, any company can still fall prey to cyberattacks. But even in the event of an attack, damage can be limited by suitable preparation, e.g., regular backups and a functioning risk management system.

Here, it is worth remembering that an investment in preventive measures often costs far less than the damage incurred by a potential attack.

Sebastian POHL has been at DEKRA for more than five years. Having started out in the IT division, he specialized in information security and cybersecurity two years ago. As a Business Line Manager for Information Security & Cybersecurity and an Auditor in the Audit Service Division, where he is responsible for the Strategic Development and Implementation of ISMS Information Security Management System) standards, such as ISO 27001 (Information Security), TISAX (Trusted Information Security Assessment Exchange), and CSMS (Cybersecurity Management System) standards.

DEKRA Audit

Mail **audit@dekra.com**
Web **www.dekra.com/en/audit/**