Press Release

Cybersecurity 2023: Cloud security is key issue for companies

[Essen, Germany, 07. November 2022] **What challenges do companies currently face regarding security? What is their cybersecurity strategy for the future? And what role does digital sovereignty play in this? To answer these and other questions, the research and consulting company IDC surveyed more than 300 companies on behalf of secunet Security Networks AG as part of the "Cybersecurity in the German-speaking markets 2022" study.**

The results show that cloud security is the most important strategic security topic for 34% of companies in 2022 and 2023. Ranked second to fifth are secure backups/disaster recovery (20%), data security (19%), security awareness training (15%) and identity & access management (14%).

Along with the strategic issues, there are also the top cybersecurity challenges faced by companies. Nearly two-thirds of respondents say their security landscapes have become more complex over the past twelve months. In addition, 69% expect complexity to increase further over the next twelve months. The top five security challenges for companies in Germany, Austria and Switzerland are security complexity (24%), data protection/privacy (21%), ransomware attacks (19%), cybersecurity skills shortage (18%) and security of networked environments (16%). Fifty-seven percent of respondents agree that they already have an urgent shortage of cybersecurity personnel or will have one in the coming year.

Digital sovereignty is becoming more important

The economic and political situation has made the issue of digital sovereignty more important for three out of four companies. For 26%, it is "much more important" with strategic implications, and for another 49%, it is at least "more important" with implications for day-to-day business. This also means that many companies see numerous benefits

Press Release

in digital sovereignty. For example, it helps respondents to shape their own transformation in a self-determined way, to strengthen the trust of customers and other stakeholders, and to promote collaboration with partners in increasingly digital ecosystems (60% each).

The top 5 most common digital sovereignty challenges for companies are protecting and gaining visibility of data in clouds (31%), the cost of evaluating and adopting new technology (29%), expertise in dealing with cloud contracts and skilled employees to understand and implement individual digital sovereignty requirements (27%), the availability and cost of local compliance officers (25%), and dealing with competing requirements between regional and national jurisdictions (24%).

Ransomware attacks are on the rise

According to the IDC study, 72% of companies in the German-speaking markets have been affected by ransomware. 40% have even seen an increase in cyberattacks over the past twelve months. Looking ahead, half of the respondents (50%) expect the number of attacks to increase even further. If a ransomware attack occurred, only 50% of companies were able to successfully defend against it.

"To remain competitive and successfully develop their own business model, companies must respond to technological innovations and act with digital sovereignty," analyzes Frank Sauber, Global Head of Sales & Business Enablement, secunet Security Networks AG. "Besides self-determination and independence, this also means freedom of choice, for example in terms of providers, data protection or transparency. This gives companies more influence over what happens to their data and ultimately enables them to better protect themselves against cybercrime, sabotage or espionage. Companies are already complaining about the lack of skilled personnel and the complexity of the security landscape - this can only be mastered with independent partners and secure services."

About the study:

Press Release

The study "Cybersecurity in the German-speaking markets 2022" was conducted as a primary market survey by IDC in September 2022. Using a structured questionnaire, 306 companies in the German-speaking markets, consisting of Germany, Austria and Switzerland, with at least 50 but almost exclusively more than 100 employees were surveyed across all industries. Security managers who are involved in strategic security planning, security-related investment and technology decisions, or security operations took part in the survey and can therefore provide well-founded information on their companies' current and future cybersecurity strategies.

All results of the study can be found at the following link (only available in German language): https://www.secunet.com/studie-cybersecurity-in-dach-2022

Press contact

Patrick Franitza
Spokesman

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen/Germany
Phone +49 201 54 54-1234
Fax +49 201 54 54-1235
E-mail: presse@secunet.com
http://www.secunet.com

secunet – Protecting Digital Infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed in the SDAX and generated revenues of around 337 million euros in 2021.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

Further information can be found at www.secunet.com.