Cybersecurity

07 December 2022

TÜV SÜD: cybersecurity trends in 2023

Munich. The cybersecurity measures set in place by companies are being impacted by new laws and regulations in addition to geopolitical and economic crises. Continued training remains one of the key success factors. TÜV SÜD identifies the latest cybersecurity trends for 2023.

“Cybersecurity risks are one of the top risks faced by companies”, says Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) at TÜV SÜD. “The importance of investments in cybersecurity has been boosted by the threat landscape, combined with new regulations and their implementation. Small and medium-sized enterprises (SMEs) in particular will focus more on the cost-efficiency of cybersecurity solutions in the future”, explains Ethiraj. The following cybersecurity trends and developments will move into the foreground in 2023:

Cybersecurity Trends in 2023
TÜV SÜD
Cost-effective Cybersecurity Solutions
Implementation of Cybersecurity Regulations
Stronger Focus on Critical Infrastructure (KRITIS)
Target-Group Training
Digital Trust through Standardisation

Cost-effective cybersecurity solutions

2023 will see a rise in demand for reasonably priced and effective security solutions and services, as a tangible demonstration of the uncertainty arising from the general economic situation as well as the negative impacts of the Covid-19 pandemic and the war in Ukraine. Small and medium-sized enterprises (SMEs) will be particularly careful to make targeted use of their IT security budget and thoroughly scrutinise the cost-effectiveness of cybersecurity measures. To strengthen cybersecurity along the supply chain, suppliers should no longer be burdened with a host of different cybersecurity requirements. Instead, cybersecurity requirements should be standardised and standards adopted at global level wherever possible.

Implementation of cybersecurity regulations

With some national and international cybersecurity acts and regulations already in place, we are now moving to the implementation phase. Some examples: The EU Directive on the Security of Network and Information Systems (NIS) will be replaced by the NIS 2 Directive, which will impose stricter supervisory and reporting measures and adopt harmonised sanctions throughout the EU. The draft European Cyber Resilience Act (CRA) is the first EU-wide legislation to establish mandatory cybersecurity requirements for equipment and products with digital elements. The EU delegated regulation supplementing the Radio Equipment Directive (RED) will apply from August 2024 onwards, making cybersecurity mandatory for all wireless equipment such as mobile phones, tablets or smart watches. The USA has seen a rising number of cybersecurity-implementing regulations, causing US authorities such as CISA to work on the implementation of cybersecurity requirements that apply across several industries. However, an aspect common to all regulations is that companies need to check whether they fall under their scopes and how to implement the relevant changes in the most efficient way. In view of international implementation, standards and third-party certification will play an even greater role in the future than they have to date.

Stronger focus on critical infrastructure (KRITIS)

The numbers of phishing, malware and ransomware attacks are rising, a trend that is set to continue in the near future. In view of the growing professionalism of cyber-attackers and virtual warfare, protection of critical infrastructure continues to take centre stage. This applies above all to highly sensitive sectors such as energy supply and health care. One of the key factors in President Biden’s national security strategy is cyber-resilience. Germany plans to adopt an umbrella act aimed at the protection of critical infrastructure (KRITIS). The purpose of this act is to establish minimum requirements that apply across all sectors to strengthen the resilience of the infrastructure system.

Target-group-oriented training

The human factor continues to be the weak link in the cyber security chain, with employees comprising the third major component next to technology and processes. So far, the focus has been on general awareness training for entire workforces. In the future, there will be an increasing trend towards training measures for specific target audiences and their needs, addressing areas including the requirements of specific sectors like automotive engineering or the medtech industry. Experts and executives, too, require regular continued training on cyberthreats and on how to act and behave correctly.

Digital trust through standardisation

Building digital trust in AI is an important key factor. In view of this, norms and standards are growing increasingly important. In as far as regulations are concerned, the EU Commission presented the Artificial Intelligence Act in April 2021. Given this, stakeholders must now start to engage in discussions on AI certificates and certification standards enabling them to establish IT environments that offer maximum security. Standardisation organisations such as ISO (International Standards Organisations) have already started working on this. The industrial sector is likewise working on the development of proposals and solutions for possible AI labels. One example is the Charter of Trust, a cybersecurity alliance formed by global companies which includes TÜV SÜD among its members. Ensuring growing trust in digital technologies is a key aspect in the development and use of AI applications.

Podcast on Cybersecurity Trends 2023

For more background on Cybersecurity Trends 2023 listen to Episode 62 of TÜV SÜD's Safety First podcast. The interview with Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) TÜV SÜD, is available here or wherever podcasts can be found.

Information about TÜV SÜD's services in the area of IT security can be found at: https://www.tuvsud.com/cybersecurity.

Note for editorial staff: The press release and illustration are available on the Internet at www.tuvsud.com/newsroom.

Media Relations

Sabine Krömer	Tel.	+49 (0) 89 / 57 91 – 29 35
TÜV SÜD AG	Fax	+49 (0) 89 / 57 91 – 22 69
Corporate Communications	Email	sabine.kroemer@tuvsud.com
Westendstr. 199, 80686 Munich	Internet	www.tuvsud.com

Founded in 1866 as a steam boiler inspection association, the TÜV SÜD Group has evolved into a global enterprise. More than 25,000 employees work at over 1.000 locations in about 50 countries to continually improve technology, systems and expertise. They contribute significantly to making technical innovations such as Industry 4.0, autonomous driving and renewable energy safe and reliable. www.tuvsud.com/presse