Press Release

Add value.
Inspire trust.

IT security

29 October 2020

TÜV SÜD announces cybersecurity trends in 2021

Munich. The "new normal" is forcing companies to reconsider their existing plans, structures and processes and to seek out new solutions, including in cybersecurity. The experts from TÜV SÜD Sec-IT keep companies and their IT security departments up to date with the important trends and developments to look out for next year.

"The new normal requires companies to implement a change process", explains Stefan Vollmer, Chief Technology Officer (CTO), TÜV SÜD Sec-IT. "Large parts of the workforce will continue to practice mobile working and working from home in the future. Use of remote access to business data and applications stored in the cloud will continue to rise. Access management solutions, the associated time and effort expended on data protection and, of course, IT security for working from home must be aligned to this new normal." Against the backdrop of this development, the experts from TÜV SÜD Sec-IT expect the following cybersecurity trends in 2021:

Cybersecurity Trends in 2021
TÜV SÜD
Workforce gap – automation can help
Cloud security is increasingly vital
Improve supply chain security
Standards are the backbone of security
Automated phishing
Data protection still crucial

1. Workforce gap – automation can help

   Qualified IT security experts were at a premium even before the coronavirus pandemic hit. The (ISC)² Cybersecurity Workforce Study from 2019 estimates the global workforce gap at 4 million. In view of these estimates, companies must increasingly seek out automated solutions to relieve the workload of their existing staff and ensure that resources are focused better on protecting against new threats and developing new strategies, while leaving minor tasks to be automatically completed by the system.

2. Improve supply chain security

   Lockdowns and new regulations have forced suppliers in particular to explore new avenues and restructure existing processes. Circumstances are pressuring manufacturing industries into digitising a growing number of sub-processes, or even entire processes. Smart connectivity and remote control of multiple devices via the Internet of Things (IoT) will evolve into an important factor in this context. To protect these IoT devices against cyberattacks, their design and development and their security need to be standardised so that they can be tested and certified against objective criteria.

3. Cloud security is increasingly vital

   To simplify remote access and mobile working, many companies are moving their applications and services into the cloud. As a consequence, these platforms require higher levels of protection. One way of enhancing security in the cloud is to seek prior analysis and advice from third-party experts. However, subsequent regular and extensive penetration tests are imperative to check the cloud solution for potential vulnerabilities.

4. Automated phishing

   Quantity over quality is still the watchword of cybercriminals. In keeping with this, the wide phishing net cast by cybercriminals using email and social media will continue to figure among the biggest threats to companies. Employees must be made aware of these risks and the scams used by fraudsters, and learn how to handle these threats in dedicated security awareness training. A report published by Cofense in 2019 outlines the extent to which automation also makes good sense in defence of cyberattacks.

5. Data protection still crucial

   As the degree of digitisation grows, so too do the responsibilities for protecting the collected and stored data, which present a challenge for small and medium-sized enterprises. Companies thus need not only ensure the best possible protection for these data, but also be familiar with the key data-protection requirements laid down in the EU GDPR. In the case of larger companies, external advisory services or the outsourcing of responsibility to an external data protection officer (DPO) may be helpful.

6. Standards are the backbone of security

   The EU regulation “EU Cybersecurity Act” came into effect in June 2019. It establishes the regulatory framework for the EU-wide security certification of products, services and processes. According to this regulation, ICT products must comply with standardised security requirements from the earliest stages of design and development as well as in production (“security by design” and “security by default”). Uniform standards on this basis enable certification to be performed by an independent and impartial third party.

More information about the services of TÜV SÜD Sec-IT GmbH can be found at https://www.tuvsud.com/en/services/cyber-security.

Note for editorial staff: The press release and high-resolution photo can be found on the Internet at www.tuv-sud.com/newsroom.

Media Relations:

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