Press Release

Cybersecurity 16 November 2021

TÜV SÜD: cybersecurity trends in 2022

Munich. Cybercrime-as-a-Service (CaaS), growing consumer and industry awareness and supply-chain security feature among the major cybersecurity trends in 2022. The increasing professionalism of cybercriminals in the field of ransomware is also confronting companies with the need to make appropriate preparations.

“Ransomware attacks in 2021, among them Kaseya, SolarWinds and Colonial Pipeline, yet again hammered home the importance of integrating cybersecurity into corporate culture and implementing it across the supply chain”, explains Sudhir Ethiraj, Global Head of Cybersecurity Office (CSO) at TÜV SÜD. “In addition, cybercrime has evolved into a service and thus ransomware is now generally available as ‘cybercrime as a service (CaaS)’ – and even includes technical support. Cybercriminals have used 2021 to reposition themselves, hone their professionalism and expand their activities into new fields. Given this, SMEs, industry and authorities now need to respond accordingly.” In line with these developments, TÜV SÜD’s security experts predict the following cyber-security trends for 2022:

Cybercrime as a Service (CaaS)

Today, ransomware is marketed by cybercriminals in a similar manner to regular software, thus creating a new business model. In return for payment of a licence fee, criminals can buy malware that even includes technical support services. This market will continue to grow. Companies need to respond proactively and step up their investments in employee training and awareness and in the security of their technical infrastructure.

Cybersecurity awareness: Consumers' eyes are being opened

Attacks on large companies and infrastructure have shown that cybersecurity measures adopted by industry in fields such as IIoT are lagging significantly behind the methods of the attackers. In this area, it is in the industry's own interest to heighten its awareness of risks and threats and work together to develop standards that help to improve resilience against attacks. Cybersecurity is also playing an increasingly central role in purchase decisions by consumers seeking connected devices like IoT equipment, smartwatches and other wearables.

Supply chain: Uniform safety standards

However, past incidents have shown that still greater awareness of cyberthreats is imperative, particularly along the software development supply chain. In addition, there is a need for shared standards for software security such as those demanded by the Charter of Trust, a global cybersecurity alliance of which TÜV SÜD is an active member. Manufacturers should motivate their business partners and suppliers by helping them to comply with the new regulations.

Global harmonisation: Working together for more cybersecurity

"Standards are the backbone of cybersecurity" is a motto that needs to be implemented at international level and requires cross-border collaboration. Industry and lawmakers must respond by working together to establish harmonised minimum requirements which deliver cybersecurity "ex works" for products and services across industries and technologies. Uniform and generally valid cyber-security standards will enable the security level to be strengthened.

Digital trust: Protection of AI, automation and algorithms

AI and automation help companies to perform activities such as optimising processes and analysing their own data traffic to detect attacks, data leakage or data theft at an early stage. However, these technologies are only as reliable as their underlying algorithms. Companies and organisations thus need to exercise prudence when it comes to the protection of these technologies. After all,

cybercriminals are also making increasing use of AI for their own purposes. Fundamental standards addressing the cybersecurity of AI can support the protection of infrastructure and data integrity.

Information about TÜV SÜD's cybersecurity services 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.tuv-sud.com/newsroom.

Media Relations:

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

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