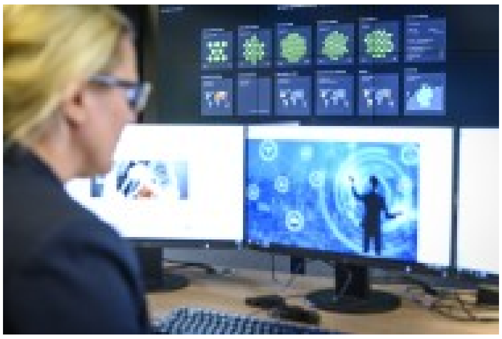
TÜVRheinland®

TÜV Rheinland: Cybersecurity decides on the stability of societies

02/06/2020 | Cologne



TÜV Rheinland, a leading international provider of testing, inspection and certification services, today released its seventh annual report on Cybersecurity Trends for 2020. The report is a collaboration between many of TÜV Rheinland‘s leading Cybersecurity experts globally, and discusses seven key Cybersecurity trends which will be important to be aware of in 2020. These include attacks on smart supply chains, threats to medical equipment and weaknesses in real-time operating systems.

Seven Cybersecurity Trends for 2020 by world-leading professionals

The developments in the area of Cybersecurity are alarming. As the number of smart devices in private households increase, so do the opportunities for cyber criminals to attack. Uncontrolled access to personal data undermines confidence in the digital society. The logistics industry and private vehicles are increasingly being targeted by hackers. TÜV Rheinland’s Cybersecurity experts view these trends as critical to understand in 2020. "From our point of view, it is particularly serious that cybercrime is increasingly affecting our personal security and the stability of society as a whole," explains Petr Láhner, Business Executive Vice President for the business stream Industry Service & Cybersecurity at TÜV Rheinland. "One of the reasons for this is that digital systems are finding their way into more and more areas of our daily lives. Digitalization offers many advantages - but it is important that these systems and thus the people are safe from attacks."

UNCONTROLLED ACCESS TO PERSONAL DATA CARRIES THE RISK OF DESTABILIZING THE DIGITAL SOCIETY
GDPR
Too much data, too little transparency
The hidden problem of third parties
TÜVRheinland®
Precisely Right.

Uncontrolled access to personal data carries the risk of destabilizing the digital society

In 2017, Frenchwoman Judith Duportail asked a dating app company to send her any personal information they had about her. In response, she received an 800-page document containing her Facebook likes and dislikes, the age of the men she had expressed interest in, and every single online conversation she had had with all 870 matching contacts since 2013. The fact that Judith Duportail received so much personal data after several years of using a single app underscores the fact that data protection is now very challenging. In addition, this example shows how little transparency there is about securing and processing data that can be used to gain an accurate picture of an individual's interests and behavior.

SMART CONSUMER DEVICES ARE SPREADING FASTER THAN THEY CAN BE SECURED
Smart devices are becoming ubiquitous and powerful

Smart consumer devices are spreading faster

than they can be secured

Smart speakers, fitness trackers, smart watches, thermostats, energy meters, smart home security cameras, smart locks and lights are the best-known examples of the seemingly unstoppable democratization of the "Internet of many Things". Smart devices are no longer just toys or technological innovations. The number and performance of individual "smart" devices is increasing every year, as these types of device are quickly becoming an integral part of everyday life. It is easy to see a future in which the economy and society will become dependent on them, making them a very attractive target for cyber criminals. Until now, the challenge for Cybersecurity has been to protect one billion servers and PCs. With the proliferation of smart devices, the attack surface could quickly increase hundreds or thousands of times.

THE TREND TOWARDS OWNING A MEDICAL DEVICE INCREASES THE RISK OF AN INTERNET HEALTH CRISIS
TÜVRheinland®
Precisely Right.

The trend towards owning a medical device increases the risk of an Internet health crisis

Over the past ten years, personal medical devices such as insulin pumps, heart and glucose monitors, defibrillators and pacemakers have been connected to the Internet as part of the "Internet of Medical Things" (IoMT). At the same time, researchers have identified a growing number of software vulnerabilities and demonstrated the feasibility of attacks on these products. This can lead to targeted attacks on both individuals and entire product classes. In some cases, the health information generated by the devices can also be intercepted. So far, the healthcare industry has struggled to respond to the problem - especially when the official life of the equipment has expired. As with so many IoT devices of this generation, networking was more important than the need for Cybersecurity. The complex task of maintaining and repairing equipment is badly organized, inadequate or completely absent.

Vehicles and transport infrastructure are new targets for cyberattacks

Through the development of software and hardware platforms, vehicles and transport infrastructure are increasingly connected. These applications offer drivers more flexibility and functionality, potentially more road safety, and seem inevitable given the development of self-propelled vehicles. The disadvantage is the increasing number of vulnerabilities that attackers could exploit – some with direct security implications. Broad cyberattacks targeting transport could affect not only the safety of individual road users, but could also lead to widespread disruption of traffic and urban safety.

Hackers target smart supply chains and make them “dumb”

With the goal of greater efficiency and lower costs, smart supply chains leverage Internet of Things (IoT) automation, robotics and big data management – those within a company and with their suppliers. Smart supply chains increasingly represent virtual warehousing, where the warehouse is no longer just a physical building, but any place where a product or its components can be located at any time. Nevertheless, there is a growing realization that this business model considerably increases the financial risks, even with only relatively minor disruptions. Smart supply chains are dynamic and efficient, but are also prone to disruptions in processes. Cyberattacks can manipulate information about deposits. Thus, components would not be where they are supposed to be.

THREATS TO SHIPPING ARE NO LONGER JUST A THEORETICAL THREAT BUT A REALITY
TÜVRheinland®
Precisely Right.

Threats to shipping are no longer just a theoretical threat but a reality

In 2017, goods with an estimated weight of around 10.7 billion tons were transported by sea. Despite current geopolitical and trade tensions, trade is generally expected to continue to grow. There is ample evidence that states are experimenting with direct attacks on ship navigation systems. At the same time, attacks on the computer networks of ships used to extort ransom have been reported. Port logistics offers a second, overlapping area of vulnerability. Many aspects to shipping that can be vulnerability to attack such as ship navigation, port logistics and ship computer network. Attacks can originate from states and activist groups. This makes monitoring and understanding a key factor in modern maritime Cybersecurity.

Vulnerabilities in real-time operating systems could herald the end of the patch age

It is estimated that by 2025 there will be over 75 billion networked devices on the Internet of Things, each using its own software package. This, in turn, contains many outsourced and potentially endangered components. In 2019, Armis Labs discovered eleven serious vulnerabilities (called "Urgent/11") in the real-time operating system (RTOS) Wind River VxWorks. Six of these flaws exposed an estimated 200 million IoT devices to the risk of remote code execution (RCE) attacks. This level of weakness is a major challenge as it is often deeply hidden in a large number of products. Organizations may not even notice that these vulnerabilities exist. In view of this, the procedure of always installing the latest security updates will no longer be effective.

Contact for media inquiries: Norman Hübner
Phone: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland is a global leader in independent inspection services, founded nearly 150 years ago. The group maintains a worldwide presence of more than 20,000 people; annual turnover is EUR 2 billion. The independent experts stand for quality and safety for people, technology and the environment in nearly all aspects of life. TÜV Rheinland inspects technical equipment, products and services, oversees projects, and helps to shape processes and information security for companies. Its experts train people in a wide range of careers and industries. To this end, TÜV Rheinland employs a global network of approved labs, testing and education centers. Since 2006, TÜV Rheinland has been a member of the United Nations Global Compact to promote sustainability and combat corruption.

Website: www.tuv.com