The increasing threat of cyber crime

Every two months, Prof. Dr. Thorsten Arnhold, IECEx Chairman 2014-2019, provides an update on developments within the organisation.

In the last couple of years, the number of news stories involving cyber attacks has continuously increased. Considering the fact that for the past two years the public focus has been pretty much dominated by COVID-19, it is obvious that the real extent of cyber criminal threats is much larger and more serious than the public realises. According to the US consulting company Purplesec, cybercrime as a whole has increased by 600% since the beginning of the pandemic. Another study by KPMG says that the damage of cyber crime was equal to 0.9% of the global GDP in 2010 and it is expected that this figure will increase by 1.24 % in 2030.

Some notorious examples of cyber crime in recent years include the 2017 "WannaCry" trojan malware which infected private and commercial computers around the world. This was followed by the "NotPetya" malware which infected, among others, the Maersk shipping company and the transport service provider TNT Express. The damage for these two companies alone was US$300 million (Source: Bundeskriminalamt Germany).

In May 2021, Colonial Pipeline in the US was attacked by ransomware. The pipeline network is one of the largest in the United States. Colonial Pipeline's operations had to be stopped for several days with an immediate effect on oil prices.

About one month later, there was another cyber attack. This time the target was an ERP and management software. The effects were especially severe in Sweden, a country with almost no use for cash in daily life. The consequences have been severe with hundreds of supermarkets, petrol stations and other institutions having to close for days.

The methods used by cyber criminals are becoming ever more dynamic and sophisticated. What we see is an ongoing and intensifying competition between the development of appropriate protection methods and the adoption of these new methods by the criminals followed by new attacks carried out with more efficient "cyber weapons". Obvious indications of this process are the increasing and more frequent update requests by internet security providers for our private computers and the increasingly "professional" look and feel of the camouflage for spyware, ransomware etc.

A couple of years ago it was easy for normal users to identify emails carrying such malware due to spelling mistakes and strange trademarks etc. These times are gone. Nowadays it is hard to distinguish between a serious message and a fake. Furthermore, the carriers of such programs have multiplied. Beside the classical email attachments, we now see infiltration paths via social media, private chats, video games and similar services. I think that especially in the West, we have to consider such developments with our ever-ageing societies in mind!

Another development concerns me as well. The Internet of things may have many positive effects for the efficiency and the flexibility of industrial processes, but we must not forget the intrinsic consequence caused by machines, ships, trains, energy supplies and other industrial facilities which are interconnected by IT and OT.

Considering all these developments and the potential consequences, I am wondering more and more about the low public interest and the lack of attention given to this issue by the media compared with other "hot topics".

The IEC has given much higher priority to cyber security. Here it is a major topic, driven by the strong conviction that there are only global solutions for these serious issues!

The standard ISO/IEC 27001 is about powerful methods to reduce information security risks, including threats, vulnerabilities, and impacts. Furthermore, it gives valuable hints on designing controls to protect the confidentiality, integrity, and availability of data, as well as for regulating access to critical information systems and networks.

ISO/IEC 27001 is now also part of the approved process scheme that provides for the independent assessment and issuing of an international IECQ certificate of conformity for organisations that have demonstrated compliance. The new IECQ ISMS facility assessments under the IECQ AP scheme ensure a focus on the key technical and administrative elements that provide confidence that the requirements of ISO/IEC 27001 have been met.

For cyber physical systems, the focus is on protecting the safety, integrity, availability, and confidentiality (S-I-A-C) of a diverse range of traffic, ranging from life-critical patient data requiring immediate delivery and response to general administrative data.

International standards provide solutions to many of these challenges as well. IEC 62443 is designed to keep cyber physical systems running. It can be applied to any industrial environment, including critical infrastructure facilities, such as power utilities or nuclear plants, as well as in the health and transport sectors.

The industrial cybersecurity programme of the IECEE – the IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components – tests and certifies cybersecurity in the industrial automation sector. The IECEE Conformity Assessment Scheme includes a programme that provides certification to standards within the IEC 62443 series (www.iec.com). ■