Safe Wireless Systems for the Industry

Global Spectrum Experience

How an industrial business' network can be accessed via unsafe wireless connections … or how industry could improve its focus on cyber security

The threat to businesses from cyber attacks has increased dramatically. Cyber attacks are directed against companies in all industries worldwide. According to a KPMG study published in May, 88 percent of Swiss companies surveyed were victims of cyber attacks in the last twelve months.[1]

Industry operations are at stake and the legal risks in terms of loss of intellectual property, know-how and customer confidence are tremendous and may endanger business continuity.

"What most industrial companies don't know is that often security loopholes to their intra-company networks are created in-house," says Michael Braun, Managing Director of LS telcom's subsidiary Vision2Comm. In the manufacturing and process industries, automobile and facilities'

industries, operations and production processes are highly reliant on wireless technology and with the introduction and application of 5G to industries this will increase. Robotics, logistics and warehouse management, material flow systems, machine-to-machine communication, RFID technology, network connection for smart meters or transformer stations, water flow control and remote inquiry systems are just some examples of applications that all use and depend on wireless technology.

Michael Braun states, "The question is whether all these wireless connections are safe. Often, cyber security and IT managers are not even aware of all the wireless systems running in a company's premises or factories."

Cyber security is a priority for most businesses and industries and enormous budgets are spent on firewalls to

protect IT-systems and company networks from cyber attacks. "Imagine a house secured by an alarm system, but the backdoor is left open. This is how non-secured wireless systems can present security loopholes to bypass the installed company network's firewall," explains Braun further. "Some may have heard about hackers entering a secured company network via the wireless mouse or wireless keyboard, which sent unencrypted RF packets. This may also happen via radio applications in use at production sites, if they are not secured."

How can industries minimize cyber security threats via radio connections and guarantee the operation of safe and interference-free wireless systems on their premises?

It starts with inventory: industries need to know exactly and at all times, which wireless systems are operating on their premises to make sure they are safe and run without interference.

LS telcom, an expert in frequency management and radio communications technologies, assists industries with concepts for the operation of wireless systems and the safe application of 5G in industrial environments.

LS telcom's support to industries consists of an individual toolbox of measurement systems, frequency and wireless equipments' database systems, analysis software, and services.

First, LS telcom experts carry out an initial inventory by measuring the complete radio frequency environment. This results in an overview of all the frequencies in use and helps to identify and register in a database all wireless systems and technologies in operation at the site. The inventory in the form of measurements and database registration constitutes the prerequisite for IT and radio systems' managers to check each system and identify security loopholes to intra-company IT networks.

The next step in guaranteeing security is continuous radio monitoring of all wireless devices. A "preventive radio network protection system" functions rather like a smoke detector. In the event of defined deviations from the normal network status, for example a new emission from a wireless system that was added without prior registration or any other unusual use, the system automatically generates real-time alerts in the form of emails or text messages and sends them to the monitoring or network surveillance center, via radio or VPN connection. The system operator can analyze these messages by logging into the central control system.

The LS OBSERVER system from LS telcom consists of various fixed, transportable and portable measuring devices, which permanently record the radio frequency spectrum and send the measured data to a control center on demand.

Ad-hoc onsite measurements in case of sudden anomalies or incidences can also be carried out. LS telcom can immediately locate and identify any malfunctioning system or source of interference with the LS OBSERVER handheld measurement device.

"Ultimately, companies should manage their wireless systems' and frequency database on a permanent basis, just as they do for their IT network", confirms Michael Braun.

LS telcom offers frequency and wireless systems' databases, software, measurement equipment, and complete systems for purchase, lease or as a services. As an expert for highly reliable network availability and data transmission security, LS telcom can manage all tasks related to the safe and interference free operation of wireless systems for industries.

[1] Source NZZ, Tino Gaberthüel 31.8.2017, „Cyber-Security als Herausforderung für Unternehmen",
https://www.nzz.ch/meinung/operative-und-rechtliche-risiken-cyber-security-als-herausforderung-fuer-unternehmen-ld.1313539

For further information, please visit our website www.LStelcom.com or contact Info@LStelcom.com.