A smart world needs smart security

As our world swiftly becomes more connected, security demands are taking on an entirely new level of importance. To ward off cyber attacks, industrial gas specialist Linde uses Deutsche Telekom's Cyber Defense and Security Operation Center (SOC) in Bonn.

COPY —— Sven Hansel

Shanghai's metro transports three billion passengers every year, an 8.7 magnitude earthquake in Los Angeles would cause 200 billion US dollars in damage, and residents of São Paulo spend an average of 45 days in traffic jams – the trend toward urbanization can only be maintained with the support of technological advances. It is becoming a key factor to the quality of life. However, it is far from having entered most people's consciousness, so that new thinking in IT security is necessary to promote this technological advance. In short: A smart world needs smart security.

The blueprint of the smart world reveals why this is the case. People are more mobile in the smart world, and so are goods, data, and finances. In addition, trillions of sensors will ensure that the Internet of Things experiences gigantic data growth – data that is becoming a hard currency in new business models and which is at home across the globe, thanks to blockchain technology, for example. This smart world is limitless but should not be unrestrained. The concept of network security enters a whole new dimension here. Because the network is everything, and without a network everything is nothing.

Experts from eco, the Association of the Internet Industry, together with the consultants of Arthur D. Little, examined what this means specifically in terms of volume. The sales volume of the German smart city market alone will increase from 20.4 billion euros in 2017 to 43.8 billion euros in 2022. This is an average annual growth rate of 16.5 percent. "Growth is happening across all market segments, with more than 65 percent of the total smart city market in 2017 comprising the four segments of transportation & logistics, communications services & network security, physical security, and building automation," according to the experts.

Established in 1879, the Linde technology group employs over 60,000 people worldwide in business divisions such as Gas and Engineering.

The growing connectivity of production environments has helped make cyber security a core strategic issue for the multinational technology group.

And this “network security” has nothing to do with what IT security experts commonly mean. Example of Dubai: The metropolis of three million in the already fast-growing United Arab Emirates has ambitious smart city plans, with the goal of reducing CO_2 emissions by 16 percent and car traffic by 8 percent. These measures alone require a batch of more than 150 smart city initiatives and services, from smart traffic lights to online government services. These services themselves are then integrated into an ICT platform with an open and horizontal architecture. Given the degree of interconnectedness of this digital world, it is, therefore, more than logical that new high-performance centers for network security emerge, such as Deutsche Telekom’s integrated Cyber Defense and Security Operation Center (SOC) in Bonn, Germany, one of Europe’s largest and most modern defense centers thwarting cyberattacks.

The experts of Deutsche Telekom analyze one billion security-relevant pieces of data from 3000 data sources every day, almost fully automatically. 30 companies and organizations already rely on SOC, including the Munich-based global corporation Linde (see the interview). At the new Master SOC in Bonn and affiliated locations, around 200 experts monitor the systems of Deutsche Telekom and its customers 24 hours a day, both nationally and internationally. They detect cyberattacks, analyze the attack methods, sustainably protect against attacks, and deduce forecasts of future patterns of attacks. To do so, the Deutsche Telekom experts draw on their many years of experience in combating attacks on their own infrastructure. They have already collected more than 20 million examples of attacks and used them to improve their own systems. A smart team to protect a prospering digital world.

reutter@t-systems.com (Rene Reutter)
ruediger.peusquens@telekom.de
www.linde-worldwide.com
www.t-systems.com/bestpractice/soc

Photos: The Linde Group

Klaus Brenk, Head of Global Security Operations, Linde AG.

Sebastian Mahler, Head of Enterprise Infrastructure, Linde AG

Hybrid safety for Linde

Sebastian Mahler (Enterprise Infrastructure) and Klaus Brenk (Global Security Operations) on their cooperation with Deutsche Telekom's Cyber Defense and Security Operation Center (SOC). The gas and engineering group cherishes the principle of shared responsibility.

COPY —— Sven Hansel

Mr. Brenk, Mr. Mahler, you rely on the protection of Deutsche Telekom's new SOC, why?
Mahler: The sense is that the threat situation is increasing daily. Cyber security has grown to become a top issue, a strategic element right up to the board level. The threat is global and requires effective defense 24 hours a day, seven days a week. If you take the threat seriously, and we do at Linde, then you also have to develop a global strategy against it.
Brenk: ... and this strategy is best implemented with a partner. You have to form alliances nowadays, because well-trained security professionals are hard to come by. Special network expertise is also beneficial. Which is why we work in partnership with Deutsche Telekom.

What does this look like exactly?
Mahler: It's a hybrid model. Our colleagues in Bonn use a security information and event management (SIEM) tool for constant network monitoring. We receive an alarm in real time if the team discovers something suspicious. Our staff then processes the corresponding message. Therefore, SOC is our 1st and 2nd level of support and we cover the subsequent stages.
Brenk: We also benefit from the technological network expertise of Deutsche Telekom. Based on the team's many years of experience in protecting their own network infrastructure and their customers, we appreciate their competence in handling this issue. When it comes to the actual production environment of our systems and machinery, we use our own internal expertise. Things work very well this way. We value both the speed and quality of SOC alarms. We can rely on the expertise, and false alarms are extremely rare.

Network expertise is one thing. To what extent has the quality of attacks played a role in the decision to partner with SOC?
Brenk: It played a big role, definitely. In the smart, digital world, our production environment is becoming increasingly networked, the number of important data for us is growing dramatically, and attacks are also becoming more sophisticated. Today, sabotage tools can be bought in illegal markets, along with tool sets that compromise our equipment. As the number of targets grows, cyber criminals can cause more damage.
Mahler: We are well positioned in the area of Global Security Operations. Nevertheless, our internal resources are finite. Which is another reason we appreciate the support of a competent and capable partner. Especially in the future ...

To what extent?
Mahler: For us, it sent the right message that Deutsche Telekom bundled its entire security expertise in one unit. When cyber criminals learn new tricks, we know that on the other side there is a team of experts always staying one step ahead, for example, using artificial intelligence and machine learning. And we cannot keep pace with such methods on our own, that would be entirely unrealistic. Or in other words: That would not be smart.

reutter@t-systems.com (Rene Reutter)
ruediger.peusquens@telekom.de
www.t-systems.com/bestpractice/soc

Photos: The Linde Group (2), Magna