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