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

Sebastian Mahler, Head of Enterprise Infrastructure, Linde AG.

Hybride Sicherheit für Linde.

Sebastian Mahler, Enterprise Infrastructure, und Klaus Brenk, Global Security Operations, zur Kooperation mit dem Cyber Defense and Security Operations Center (SOC) der Telekom. Der Gas- und Engineering-Konzern wertschätzt das Prinzip geteilter Verantwortlichkeit.

TEXT —— Sven Hansel

Herr Brenk, Herr Mahler, Sie setzen auf den Schutz des neuen SOC der Deutschen Telekom, warum?
Mahler: Die Gefahrenlage wird gefühlt täglich größer. Cybersecurity ist mittlerweile zum Topthema gewachsen, ein strategisches Element bis rauf in die Vorstandsebene. Die Bedrohung ist global und macht eine effektive Abwehr 24 Stunden am Tag an sieben Tagen die Woche notwendig. Nimmt man das Thema ernst, und das tun wir bei Linde, dann muss man auch eine globale Strategie dagegen entwickeln.
Brenk: ... und diese Strategie setzt man bestenfalls mit einem Partner um. Man muss heutzutage Allianzen bilden, denn gut ausgebildete Security-Fachleute sind kaum noch zu bekommen. Darüber hinaus ist eine besondere Netzexpertise von Vorteil. Wir gehen deshalb mit der Telekom arbeitsteilig vor.

Wie sieht das konkret aus?
Mahler: Es ist ein hybrides Modell. Die Kollegen in Bonn nutzen ein Security-Incident-and-Event-Management-Werkzeug (SIEM) für ein ständiges Monitoring der Netze. In Echtzeit bekommen wir einen Alarm, falls das Team etwas Verdächtiges entdeckt. Bei uns bearbeiten die Kollegen die entsprechende Meldung dann weiter. Im SOC erfolgt also der First- und Second-Level-Support, wir decken die darauffolgenden Stufen ab.
Brenk: Dabei kommt uns auch die technologische Netzkompetenz der Telekom zugute. Weil diese Mannschaft jahrelange Erfahrung beim Schutz der eigenen Netzwerkinfrastruktur und ihrer Kunden hat, schätzen wir den kompetenten Umgang mit dem Thema. Geht es dann um das konkrete Produktionsumfeld unserer Anlagen und Maschinen, nutzen wir die internen Kompetenzen. Derart funktioniert das sehr gut. Wir schätzen sowohl die Schnelligkeit als auch die Qualität der SOC-Alarme. Wir können uns auf die Expertise verlassen, Fehlalarme sind extrem selten.

Die Netzwerkexpertise ist das eine. Inwieweit hat aber die Qualität der Angriffe eine Rolle bei der Entscheidung pro SOC gespielt?
Brenk: Selbstverständlich eine ebenso große. In der smarten, digitalen Welt ist auch unser Produktionsumfeld mehr und mehr vernetzt, die Zahl der für uns wichtigen Daten wächst dramatisch, im Gegenzug werden die Angriffe immer ausgefeilter. Sabotagemittel lassen sich heute auf illegalen Märkten erwerben, ebenso Tool-Sets, um unsere Anlagen zu kompromittieren. Die Angriffsflächen wachsen, die Cyberkriminellen können mehr Schaden verursachen.
Mahler: Wir sind im Bereich Global Security Operations gut aufgestellt. Dennoch sind unsere internen Ressourcen endlich. Auch aus diesem Grund schätzen wir die Unterstützung durch einen kompetenten Partner. Vor allem in Zukunft ...

Inwiefern?
Mahler: Für uns war es das richtige Signal, dass die Deutsche Telekom ihre gesamte Securitykompetenz in einer Einheit gebündelt hat. Rüstet die cyberkriminelle Seite auf, dann wissen wir, dass auf der Gegenseite, beispielsweise mit künstlicher Intelligenz und Machine Learning, immer versucht wird, den Kriminellen einen Schritt voraus zu sein. Und solche Methoden können wir allein nicht vorhalten, das wäre realitätsfern. Oder anders ausgedrückt: Das wäre nicht smart.

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