Smarte Welt benötigt smarte Sicherheit.

Die rasant zunehmende Vernetzung katapultiert die Sicherheitsbedarfe in eine neue Dimension. Zum Schutz vor Cyberattacken nutzt der Industriegase-Spezialist Linde das Cyber Defense and Security Operations Center (SOC) der Deutschen Telekom in Bonn.

TEXT —— Sven Hansel

Drei Milliarden Fahrgäste befördert Shanghais Metro jedes Jahr, 200 Milliarden US-Dollar Schaden würde ein Erdbeben der Stärke 8,7 in Los Angeles verursachen, und 45 Tage verbringt ein Bewohner in São Paulo jedes Jahr im Stau – der Trend zur Urbanisierung lässt sich nur noch mit technologischem Fortschritt aufrechterhalten. Er wird zum Schlüsselfaktor für ein lebenswertes Leben. Indes ist noch längst nicht ins Bewusstsein eines jeden vorgedrungen, dass für diesen technologischen Fortschritt auch neues Denken in der IT-Security notwendig ist. Kurz: Smart World braucht zwingend Smart Security.

Warum das so ist, offenbart der Bauplan der smarten Welt. Menschen sind hier mobiler, aber auch Güter, Daten und Finanzen. Billionen an Sensoren werden darüber hinaus dafür sorgen, dass im Internet der Dinge ein gigantisches Datenwachstum herrschen wird. Daten, die zu einer harten Währung in neuen Geschäftsmodellen werden und die, etwa durch die Blockchain, überall auf der Welt zu Hause sind. Diese smarte Welt ist grenzenlos – darf aber nicht zügellos sein. Der Begriff Netzwerksicherheit bekommt hier eine ganz neue Dimension. Denn das Netz ist alles, ohne Netzwerk ist alles nichts.

Was das in Bezug auf das Volumen konkret heißt, haben die Fachleute des Internetverbands eco gemeinsam mit den Consultants von Arthur D. Little untersucht. So wächst allein das Umsatzvolumen des deutschen Smart-City-Marktes von 20,4 Milliarden Euro im Jahr 2017 auf 43,8 Milliarden Euro im Jahr 2022. Das entspricht einem durchschnittlichen jährlichen Wachstum von 16,5 Prozent. „Das Wachstum erfolgt über alle Marktsegmente hinweg, wobei mehr als 65 Prozent des gesamten Smart-City-Marktes 2017 die vier Segmente Transport und Logistik, Kommunikationsdienste und Netzwerksicherheit, physische Sicherheit sowie Gebäudeautomatisierung ausmachen“, so die Fachleute.

1879 gegründet, beschäftigt der Technologiekonzern Linde unter anderem in den Geschäftssparten Gas und Engineering heute weltweit mehr als 60 000 Mitarbeiter.

Und diese „Netzwerksicherheit“ hat so rein gar nichts damit zu tun, was IT-Security-Experten landläufig darunter verstehen. Beispiel Dubai: Die Drei-Millionen-Metropole in den ohnehin stark wachsenden Vereinigten Arabischen Emiraten hat ambitionierte Smart-City-Pläne, möchte derart den CO_2-Ausstoß etwa um 16 Prozent und den Autoverkehr um acht Prozent reduzieren. Und allein diese Maßnahmen benötigen bereits ein Bündel von mehr als 150 Smart-City-Initiativen und -Services, vom smarten Ampelsystem bis hin zu Onlinebehördendiensten. Diese Dienste sind ihrerseits wiederum eingebunden in eine ITK-Plattform mit offener und horizontaler Architektur. Angesichts des Vernetzungsgrades dieser digitalen Welt ist es deshalb mehr als logisch, dass neue Hochleistungszentren für Netzsicherheit entstehen wie beispielsweise das integrierte Cyber Defense and Security Operations Center der Telekom in Bonn, eines der größten und modernsten Abwehrzentren Europas gegen Cyberattacken.

Eine Milliarde sicherheitsrelevante Daten aus 3000 Datenquellen analysieren die Fachleute der Telekom dort jeden Tag nahezu voll automatisiert. 30 Unternehmen und Organisationen setzen bereits auf das SOC, darunter auch der Münchner Weltkonzern Linde (siehe Interview nächste Seite). Rund 200 Experten überwachen im neuen Master-SOC in Bonn und an den angeschlossenen Standorten national und international im 24-Stunden-Betrieb die Systeme der Telekom und die ihrer Kunden. Sie erkennen Cyberangriffe, analysieren die Angriffswerkzeuge, schützen nachhaltig vor Angriffen und leiten daraus Prognosen über zukünftige Muster von Attacken ab. Dabei greifen die Telekom-Experten auf ihre jahrelange Erfahrung in der Bekämpfung von Angriffen auf die eigene Infrastruktur zurück. Mehr als 20 Millionen Beispiele von Attacken haben sie bereits gesammelt und zur Verbesserung der eigenen Systeme eingesetzt. Ein smartes Team zum Schutz einer prosperierenden digitalen Welt.

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

Nicht zuletzt die gerade im Produktionsumfeld zunehmende Vernetzung macht Cybersecurity für den weltweiten Technologiekonzern zum strategischen Topthema.

Fotos: The Linde Group

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

Fotos: The Linde Group (2), Magna