Mehr IT-Sicherheit in weltweit verteilten Rechenzentren.

Die LANXESS AG ist ein führender Spezialchemie-Konzern mit Sitz in Köln. Mit mehr als 50 Produktionsstandorten für Spezial- und Feinchemikalien, hochwertigen Zwischenprodukten sowie Kunststoffen und Kautschuken in knapp 30 Ländern und mehr als 16.000 Mitarbeitern ist das Unternehmen rund um den Globus vertreten. Das vielfältige Produktportfolio erfordert den Einsatz sehr unterschiedlicher chemisch-technischer Verfahren und Rezepturen – geistiges Eigentum, welches es zu schützen gilt. Ein hohes Niveau in der Informationssicherheit ist für den Konzern daher eine wesentliche Grundvoraussetzung für den unternehmerischen Erfolg.

Umfassende IT-Sicherheitsanalyse

Um herauszufinden, wie verwundbar die konzerneigenen Rechenzentren gegenüber gezielten Hacker-Attacken sind, beauftragte der Chemie-Spezialist TÜV Rheinland mit der Durchführung einer umfassenden IT-Sicherheitsanalyse. Im Anschluss daran entschloss sich LANXESS, das Computer Security Incident Response Team (CSIRT) hinzuzuziehen, eine Expertengruppe des TÜV Rheinland. Ziel war es, das Risiko einer Kompromittierung durch gezielte und komplexe Angriffe („Advanced Persistent Threats“, kurz APT) so weit wie möglich zu reduzieren.
Eine wichtige Anforderung dabei war es, das Problem kontinuierlich und nachhaltig zu adressieren: Die interne IT sollte technologisch und personell befähigt werden, komplexe Angriffsmuster zu erkennen und diese im Rahmen von Service Management Prozessen zu analysieren und effektiv behandeln zu können.

Die Umsetzung der Service Prozesse durch das CSIRT basiert auf dem Einsatz sogenannter Sensor-Systeme. Hierbei werden relevante Teile des Netzwerksverkehrs permanent analysiert.
Im Rahmen einer unabhängigen Anbieterauswahl entwickelte TÜV Rheinland zunächst eine Vorauswahl von zu evaluierenden Lösungen für Sensorsysteme.
Um Performance und Qualität dieser Sicherheitssysteme im jeweiligen Zusammenspiel mit der bestehenden LANXESS Infrastruktur zu überprüfen, integrierte TÜV Rheinland diese Testsysteme in das Produktivnetzwerk von LANXESS.
Im nächsten Schritt analysierten die Experten des CSIRT den laufenden Netzwerkverkehr und unterzogen die von den Testsystemen verdächtigen Ergebnisse einer kritischen Prüfung.

TÜV Rheinland unterstützt Sie im Fall eines Angriffs schnellstmöglich mit seinem Computer Security Incident Response Team (CSIRT). Das CSIRT ist eine hochqualifizierte und schnelle Eingreiftruppe, vergleichbar mit einer Feuerwehr, die Ihnen bei der Analyse und Bekämpfung einer Cyber-Attacke hilft. Weitere Informationen hierzu finden Sie unter: www.tuv.com/csirt

www.tuv.com/csirt

LANXESS Energizing Chemistry

TÜVRheinland®
Genau. Richtig.

CSIRT als Managed Security Service.

Globale Logistik als Herausforderung

Eine der großen Herausforderungen im Rahmen der Implementierung technologischer Lösungen ist erfahrungsgemäß die globale Logistik – man denke nur an die unterschiedlichen Einfuhr- und Zollbestimmungen oder die lokale Rechnungsstellung. Mit Standorten in derzeit 69 Ländern hat TÜV Rheinland den Vorteil, für internationale Projektanforderungen auf professionell eingespielte Teams und Prozesse sowie lokale Kompetenzen zurückgreifen zu können. Auch im Fall von LANXESS sorgte TÜV Rheinland in allen Rechenzentren weltweit für die reibungslose Umsetzung der integrierten Sicherheitslösung aus einer Hand.

Aufbau des notwendigen Know-Hows

Doch Technologie alleine ist nicht ausreichend, damit sich Unternehmen gegen Hacker-Attacken wehren können. Damit das zuständige Team aus den gewonnenen Daten künftig auch die richtigen Schlussfolgerungen zieht, baut TÜV Rheinland bei LANXESS intern das Know-how zur Qualifizierung und Behebung von IT-Sicherheitsvorfällen auf. Während dieser Lernphase von Sicherheitsvorfällen wird der CSIRT-Service als Managed Security Service erbracht. „Durch die an unseren Anforderungskatalog geknüpfte Anbieterauswahl für eine Ergänzung unserer globalen IT-Sicherheitsinfrastruktur haben wir einen wichtigen und großen Schritt im Wettrennen mit Cyberkriminellen getan. TÜV Rheinland hat uns dabei mit einem kompetenten und jederzeit erreichbaren Projektteam unterstützt und die Mitarbeiter erfolgreich für den Umgang mit den neuen Systemen qualifiziert.“ erläutert Udo Nelken, Leiter Technical Support bei LANXESS.

Mehr über TÜV Rheinland und unsere Leistungen rund um die Abwehr gezielter, komplexer Angriffe und Einsatz des CSIRT-Teams unter: www.tuv.com/apt

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
service@i-sec.tuv.com

www.tuv.com/informationssicherheit

LANXESS Energizing Chemistry

TÜVRheinland®
Genau. Richtig.