Eigenverantwortung Cybersecurity

Chemie ist die Leidenschaft und die Kernkompetenz des Unternehmens Ursa-Chemie am Standort Montabaur. Es bietet hier ein Full-Service-Gesamtpaket: von der Prozessentwicklung über Rohstoffbeschaffung, Produktion, Qualitätskontrolle bis hin zu logistischen Dienstleistungen. Foto: Ursa-Chemie

Prävention Die neue Studie des Verbands Bitkom belegt: Unternehmen können mit geeigneten Methoden Hackerangriffe abwehren oder zumindest den Schaden begrenzen. Ursa-Chemie aus Montabaur berichtet über durchgeführte und geplante Maßnahmen im Unternehmen.

Von Gudrun Heurich

Cybercrime betrifft nicht nur Konzerne – jeder Betrieb kann zum Ziel werden und ist gefordert, sich zu schützen. Bisher ist Ursa-Chemie in Montabaur, Experte auf dem Gebiet der Full-Service-Lohnfertigung chemischer Produkte, zum Glück von Cyberattacken verschont geblieben. „Dennoch schätzen wir die Wahrscheinlichkeit, dass wir Opfer von Angriffen werden könnten, als hoch ein“, bekennt Geschäftsführer Andreas Möller und fügt hinzu: „Wir wissen, dass Cybercrime ein großes Schadensrisiko – auch der mittelständischen Industrie – darstellt.“ Das Unternehmen hat daher einiges auf den Weg gebracht, um dieses Risiko möglichst gering zu halten, wie Möller berichtet.

So wurde eine leistungsfähige Hardware-Firewall etabliert, die das Netzwerk überwacht (zum Beispiel den Datenstrom für das Internet) und den externen Zugriff auf das Unternehmen regelt. Dies umfasst ebenso eine Next-Gen-Antivirussoftware auf Clients (PCs, Notebooks) und Servern, die den Schutz vor unbekannter Malware anhand von Verhaltenserkennung sicherstellt, sowie die Nutzung von Mehrfachauthentifizierung, die zusätzliche Einmalpasswörter generiert und diese per Smartphone-App, SMS oder Telefonanruf übermittelt. „Dies ist vor allem wichtig bei IT-Systemen, die von außerhalb des Unternehmensnetzwerks erreichbar sind oder einen externen Zugriff auf das Unternehmensnetzwerk ermöglichen wie den VPN-Tunnel für das Homeoffice“, so der Geschäftsführer. Die sogenannte Mehrfachauthentifizierung bietet durch die zweite Hürde einen zusätzlichen Schutz.

Darüber hinaus ist eine aktive Freigabe des Fernzugriffs von Dritten, beispielsweise dem IT-Dienstleister, auf die IT-Systeme erforderlich. Dritte haben generell keinen unbeaufsichtigten Fernzugriff auf die IT-Systeme, auch nicht für Wartungsarbeiten oder Supportfälle. Der Fernzugriff muss aktiv angefragt und durch die IT-Abteilung temporär freigeschaltet werden. Der Fernzugriff deaktiviert sich vollautomatisch nach einer gewissen Zeitspanne.

„Die wichtigste Maßnahme, zu der wir allen Unternehmen raten, ist: Datensicherung, Datensicherung und noch mal Datensicherung – mindestens einmal täglich“, sagt Möller. „Wir haben schon vor einiger Zeit ein erweitertes Datensicherungskonzept etabliert und nutzen modernste Datensicherungssoftware und -hardware. Die Sicherungskopien der Datensicherungen befinden sich an verschiedenen Orten im Unternehmen.“ Wichtig sei auch, dass eine Offlinedatensicherung, also eine Kopie der Sicherung, vom Unternehmensnetzwerk getrennt aufbewahrt wird, beispielsweise auf einer externen USB-Festplatte, die mindestens täglich gewechselt wird und nie dauerhaft mit dem System verbunden ist.

Die Mitarbeitenden müssen in den aktiven Schutz einbezogen werden, betont der Geschäftsführer. Daher werden im Unternehmen regelmäßig Mitarbeiterschulungen zum Thema Datenschutz und Datensicherheit durchgeführt. Bei einer Livedemonstration wurde den Mitarbeitenden gezeigt, wie schnell ein moderner PC Passwörter hacken kann, die Teilnehmer waren sehr überrascht, dass es meist nur wenige Sekunden dauerte.

Um die bisherigen Aktionen noch weiter auszubauen, plant Ursa-Chemie diverse Maßnahmen, zum Beispiel den Ausbau der Trennung der IT-Netze von Produktion, Administration und Büros, die teilweise bereits vorhanden ist. „Ziel ist die weitere Abschottung der Netzwerke unserer Produktionsanlagen und unserer IT-Administration vom ‚normalen‘ Büronetzwerk, um die kritische Infrastruktur im Unternehmen noch mehr zu schützen“, erklärt Möller. Dies soll mit zusätzlichen internen Hardware-Firewalls umgesetzt werden. Weiterhin soll es eine Einschränkung der Nutzung von Microsoft-Cloud-Diensten wie OneDrive, Outlook Online oder Sharepoint geben. Diese Dienste sollen nur noch auf Geräten nutzbar sein, die durch das Unternehmen freigegeben wurden. Separate Admin-Benutzer sollen für unterschiedliche Systeme benannt werden und eine Trennung von Domänen-Administration und der Administration für Server und Clients wird angestrebt. In der Vorbereitung sind außerdem sogenannte Penetrationstests. In diesen Tests versucht ein beauftragter Hacker, in die IT-Infrastruktur einzudringen und mögliche unentdeckte Schwachstellen offenzulegen.

„Wenn wir auch schon ganz gut aufgestellt sind, gibt es immer noch Optimierungsbedarf“, stellt Möller fest. „IT-Sicherheit kostet natürlich Geld, doch hier sollten Unternehmen nicht an der falschen Stelle sparen.“

Andreas Möller, Geschäftsführer von Ursa-Chemie in Montabaur, ist sich bewusst, dass auch sein Unternehmen jederzeit Opfer von Cyberattacken werden kann. Daher investiert er einiges in die IT-Sicherheit. Foto: Ursa-Chemie

Weiterbildung zum Informationssicherheitsbeauftragten

Die **IHK Koblenz** bietet einen Onlinelehrgang zum **Informationssicherheitsbeauftragten** (IHK) an. Der Zertifikatslehrgang vermittelt die erforderlichen Fähigkeiten, um den IT-Sicherheitsbedarf im Unternehmen zu ermitteln und passende Konzepte zu entwickeln. Er richtet sich auch an kleine und mittlere Unternehmen, die insbesondere in der Zusammenarbeit mit größeren Unternehmen zunehmend ihre IT-Sicherheitsvorkehrungen nachweisen müssen.

Zielgruppe sind Fach- und Führungskräfte, die sich mit dem Thema Informationssicherheit und der Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) befassen wollen.

Es sind keine Voraussetzungen notwendig. Datenschutz- und IT-Grundkenntnisse sind von Vorteil.

Weitere Information unter:
www.ihk-akademie-koblenz.de, Kursnummer 587ITSB

Das Ministerium für Soziales, Arbeit, Gesundheit und Demografie Rheinland-Pfalz fördert die Teilnahme aus Mitteln des Europäischen Sozialfonds Plus durch den sogenannten **QualiScheck Rheinland-Pfalz.** Weitere Information unter: www.berufliche-weiterbildung.rlp.de

Zum Unternehmen

Name: UCM Ursa-Chemie GmbH (Die UCM Ursa-Chemie ist eine Ausgründung der Zschimmer und Schwarz GmbH & Co. Chemische Fabriken, Lahnstein, und der Ursapharm Arzneimittel GmbH, Saarbrücken)

Gegründet: 1970

Geschäftsführer: Andreas Möller, Dr. Michael Müller

Sitz: Montabaur

Mitarbeitende: 62

Kernkompetenz: Full-Service-Lohnfertigung chemischer Produkte

Weitere Information:
www.ursa-chemie.de

Die Beschäftigten müssen in den Schutz des Unternehmens einbezogen werden. Regelmäßige Schulungen zum Thema Datensicherheit sind angebracht. Auch die Ausbildung eines Mitarbeitenden zum Informationssicherheitsbeauftragten kann ein wesentlicher Beitrag sein. Die IHK Koblenz bietet diesen Kurs an. Foto: Mikolette Moller/peopleimages.com/stock.adobe.com