Digitalisierung macht Angriffsflächen größer

Security Audit bei der Energie - versorgung Oberhausen

Bildquelle: Energieversorgung Oberhausen AG

Den Hackerangriff auf das Universitätsklinikum Düsseldorf im September 2020 mit seinen gravierenden Folgen hat Stefan Gnaudschun noch in schlechter Erinnerung. Als Koordinator für Informationssicherheit der Energieversorgung Oberhausen arbeitet er ebenfalls für einen öffentlichen Versorger, dessen Funktionieren für die Bürgerinnen und Bürger kritisch ist. Denn werden Kraftwerke durch Cyberattacken lahmgelegt, stellt dies einen massiven Angriff auf die öffentliche Ordnung dar.

*Von Frank Zscheile**

Auch in der Energieversorger-Branche gab es bereits mehrere Fälle von Hackerangriffen. Deren Eindringen und das Stehlen von Daten gilt es um jeden Preis zu vermeiden. Deshalb bedient sich der Oberhausener Energieversorger der Expertise des Sicherheitsspezialisten Werth IT. Diese hat für das Unternehmen im Sommer 2020 einen kompakten Security-Audit durchgeführt. Das Ziel war, die IT-Systeme des Unternehmens auf Herz und Nieren zu überprüfen und einen konkreten Maßnahmenplan zu erarbeiten. Auf Basis dessen kann der Energieversorger jetzt seine IT-Systeme so absichern, dass niemand von außen unberechtigt auf Kundendaten zugreifen kann.

Als betriebswirtschaftliche Standardsoftware setzt der Energieversorger auf SAP, implementiert und betreut von einem SAP-Integrationshaus. Zur Absicherung des Systems kommt das Standard-Security-Toolset der SAP zum Einsatz. „Die IT-Landschaft eines Unter-

*Frank Zscheile ist IT-Journalist in München.

Stefan Gnaudschun, Koordinator für Informationssicherheit der Energieversorgung Oberhausen:

„Überall, wo Digitalisierung stattfindet und dort, wo Prozesse immer ausgefeilter werden, entstehen neue technische Medienbrüche und damit zwangsläufig zusätzliche IT-Risiken. Die Frage ist nicht, ob ein Angriff kommt, sondern nur noch, wann.“

Bildquelle: Energieversorgung Oberhausen AG

nehmens verändert sich aber stetig“, sagt Stefan Gnaudschun, Koordinator für Informationssicherheit der Energieversorgung Oberhausen, „überall, wo Digitalisierung stattfindet, wo Prozesse immer ausgefeilter werden, entstehen neue technische Medienbrüche und damit zwangsläufig zusätzliche IT-Risiken. Die Frage ist nicht, ob ein Angriff kommt, sondern nur noch, wann.“

Audit komplett remote

Zusätzliche Sicherheitsüberprüfungen werden also notwendig. Auf Empfehlung kam das IT-Team des Energieversorgers mit der Werth IT in Verbindung. Diese erhielt den Auftrag für einen Sicherheitsaudit des SAP-Systems. Der Audit dauerte einen Tag und fand komplett remote statt. Eine besondere Prüfsoftware musste dafür nicht im Unternehmen installiert werden. Werth IT führte den Audit mithilfe des Einsatzes ihres „werthAuditor“ durch, einem umfänglichen Werkzeug für professionelle Audits von SAP-Systemen, Durchführung von Penetrationstest-Kampagnen und die effektive Analyse von SAP-Landschaften auf Compliance und Sicherheit. Für die Prüfung ergänzt der Auditor das Equipment der SAP und führt über 2.000 Einzeltests durch. Dazu werden alle relevanten Vorschriften wie beispielsweise der DSAG-Sicherheitsleitfaden und die BSI-Richtlinien herangezogen, die dann checklistenartig abgearbeitet werden. Unzureichende Stellen, sei es bei der Konfiguration oder sonstigen fehlenden Maßnahmen, deckt der Auditor so schnell auf. Auch bei dem Versorger aus Oberhausen fand das Werth-Team einige Schwachstellen im Backend.

Wichtiger Baustein in der Sicherheitsstrategie

Ergebnis des Audits war eine kompakte Maßnahmenliste mit abgestuften Risikostufen nach dem Ampelprinzip. In Form einer Exceltabelle erhielt Stefan Gnaudschun Empfehlungen, an welcher Stelle der Programmierschnittstellen was zu ändern ist, um die Sicherheit der IT-Systeme zu erhöhen. „Nicht ein kleines To-do hier und dort. Sondern man erhält ein Gesamtbild nach einer erkennbaren Testthematik, wie es SAP selbst in dieser Form nicht bietet“, erläutert der Sicherheitsfachmann.
Schwachstellen aufdecken ist das eine – sie dann zu schließen, wird schon wesentlich komplizierter. Dies erledigt das Unternehmen derzeit gemeinsam mit den vorhandenen Partnern in Eigenregie. Ein wirklich neues Konzept ist Privacy and Security by Design, also Datenschutz und Sicherheit durch Technikgestaltung, nicht unbedingt. Angesichts immer komplexerer Prozessverzahnungen zwischen interner IT und dem Internet ist es jedoch aktueller denn je. Stefan Gnaudschun: „Der Service eines externen Sicherheitsspezialisten wie der Werth IT ist deshalb ein wichtiger Baustein in unserer Sicherheitsstrategie.“ *(cr)* @