DIGITALISIERUNGSBEISPIEL

Schwachstellen im Unternehmensnetzwerk identifizieren

Ausgangssituation

Das Unternehmen Hch. Kettelhack GmbH & Co. KG in Rheine hat ca. 100 Beschäftigte und ist Hersteller von Spezialtextilien. Produziert werden unter anderem Hochleistungsgewebe für Berufsbekleidung sowie langlebige Bettwäsche für Hotels, Kliniken und Pflegeeinrichtungen. Die ständig zunehmende Digitalisierung der Prozesse und die damit verbundene Vernetzung von Verwaltung und Produktion fordern ein entsprechendes IT-Sicherheitsniveau im Unternehmen. Störungen in den Prozessen müssen vermieden werden.

Die Anforderungen an die Datensicherheit insbesondere im Zusammenhang mit den Produktionsprozessen verlangen eine permanente Kontrolle der eingesetzten Hard- und Softwaresysteme im Netzwerk. Die allgemein zunehmende Digitalisierung zeigt sich nicht nur darin, dass immer mehr Prozesse digitalisiert werden, sondern auch in einer wachsenden bzw. komplexen IT-Infrastruktur. Im Unternehmen sind ca. 250 Hardwaresysteme vorhanden. Das notwendige IT-Sicherheitsniveau kann im Software-Bereich zumeist durch Updates noch relativ einfach gewährleistet werden. Bei der eingesetzten Hardware sind die Prozesse dagegen komplexer und damit aufwendiger.

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Zielstellung

Vorrangiges Ziel des Projektes war die Identifizierung von eventuell vorhandenen Schwachstellen in der bestehenden IT-Infrastruktur, um eine bestmögliche IT-Sicherheit im Unternehmensnetzwerk aufzubauen bzw. zu gewährleisten. Im Fokus lagen insbesondere die Hardware sowie deren Systemkomponenten. Zudem sollten die IT-Verantwortlichen durch das Projekt Erfahrungen sammeln und Know-how ausbauen können, um Prozesse zu etablieren, die der ständigen Kontrolle und Aufrechterhaltung einer hinreichenden IT-Sicherheit in einem Netzwerk dienen.

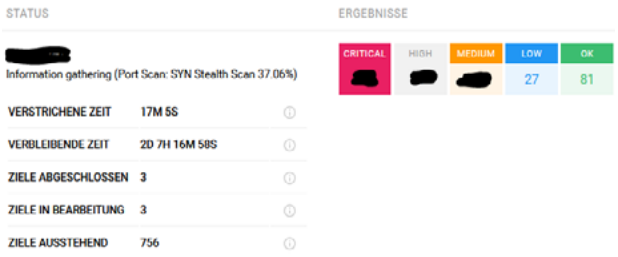
Vorgehen

In einem Vorort-Termin wurde mit dem mobilen Demonstrator „CVE-Scanner“ des Mittelstand-Digital Zentrums Chemnitz ein Schwachstellen-Scan im Unternehmensnetzwerk durchgeführt, das aus mehreren getrennten IP-Bereichen besteht. Der Scan ermittelt Schwachstellen in den Kategorien „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“ und fasst sie in einem Bericht zusammen. Dieser dient den IT-Verantwortlichen dazu, Maßnahmen zur Verbesserung der IT-Sicherheit zu definieren und umzusetzen. Außerdem kann der Bericht im Zusammenhang mit der Inventarisierung von Komponenten als Basis für den Aufbau bzw. einer Verbesserung der Dokumentation herangezogen werden.

Da für den Internetanschluss des Unternehmens mehrere feste IP-Adressen verwendet werden, wurde für eine weitere Analyse die IoT (Internet of Things)-Suchmaschine Shodan eingesetzt. Damit kann festgestellt werden, welche konkreten Angaben bezüglich der vorhandenen IT-Infrastruktur für Außenstehende zu erkennen sind. Die Suchmaschine ermittelt u. a. geöffnete Ports und erkennt mögliche vorhandene Schwachstellen.

Ergebnisse

Der Schwachstellen-Scan mit dem mobilen Demonstrator „CVE-Scanner“ identifizierte ca. 200 prüfbare Netzwerk-



Durchführung des Schwachstellen-Scans © Enginsight GmbH/ tti Magdeburg GmbH

komponenten. Für weitere konnten zwar IP-Adressen ermittelt werden, jedoch keine tiefergehende Prüfung erfolgen. Das heißt, dass bei diesen Systemkomponenten auch vermeintliche Angreifer keine Möglichkeit haben, Informationen zu möglichen vorhandenen Schwachstellen zu erhalten, da entsprechende Ports und Dienste nicht freigegeben sind.

Die Ergebnisse wurden in einem Bericht zusammengefasst und den IT-Verantwortlichen zur Auswertung übergeben. Auf Basis des Berichtes wurden in Abhängigkeit der erforderlichen Dringlichkeiten Maßnahmen definiert und zeitnah umgesetzt, so dass die Sicherheit des Netzwerkes erhöht werden konnte.

Der Check mit der Suchmaschine Shodan ergab unter Verwendung der festen IP-Adresse des Internetanschlusses, dass zwei Ports offen sind: die Verwendung für die E-Mail-Kommunikation und für eine sichere Datenübertragung über ein verschlüsseltes Netzwerk.

„Wir haben eine sehr gute eigene IT-Abteilung, die sich kontinuierlich um die Themen IT-Sicherheit und Datenschutz kümmert. Dennoch besteht gerade bei historisch gewachsenen IT-Strukturen die Gefahr der Betriebsblindheit. Ein objektiver, kritischer Blick von außen ist daher sehr sinnvoll und beruhigend.“

Joan Kettelhack, Assistent der Geschäftsführung

Mittelstand-Digital Zentrum Chemnitz
c/o Technische Universität Chemnitz
09125 Chemnitz
0371 531-19935
info@digitalzentrum-chemnitz.de

Roland Hallau
0391 74435-24
roland.hallau@digitalzentrum-chemnitz.de

digitalzentrum-chemnitz.de