Mittelstand-Digital
Zentrum
Chemnitz

PRAXISBEISPIEL

DIGITALISIERUNGSBEISPIEL

Schwachstellenanalyse in Unternehmensnetzwerken

Ausgangssituation

Die WoGe-Service GmbH stellt als Dienstleister u. a. die IT-Infrastruktur für verschiedene medizinische Einrichtungen bereit und ist damit auch für die IT-Sicherheit verantwortlich. Die Anforderungen an die Datensicherheit, insbesondere im Gesundheitswesen, verlangen eine permanente Kontrolle der eingesetzten Hard- und Software im Netzwerk. Die Digitalisierung geht dabei mit einer stetig wachsenden bzw. komplexen IT-Infrastruktur einher. Im Unternehmen sind ca. 50 Hardware-Hauptkomponenten vorhanden. Wenn auch mit einem gewissen Aufwand verbunden, gestaltet sich die Gewährleistung eines guten IT-Sicherheitsniveaus im Software-Bereich durch entsprechende Updates noch relativ einfach. Bei der eingesetzten Hardware sind die Prozesse dagegen komplexer und damit aufwendiger.

„Trotz aller vorhandenen To-do-Listen ist solch ein Tool für eine Schwachstellenanalyse einfach eine tolle Unterstützung. Ich war schon gespannt, wie wir unsere Hausaufgaben als Admin gemacht haben."

Sascha Dupuis, IT-Administrator der WoGe-Service GmbH

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum Chemnitz

PRAXISTIPP

Zielstellung

Das grundlegende Ziel des Projektes bestand in der Analyse der bestehenden IT-Infrastruktur, um eine bestmögliche IT-Sicherheit im vorhandenen Unternehmensnetzwerk aufzubauen bzw. zu gewährleisten. Hierbei standen insbesondere die Hardware sowie deren Systemkomponenten im Fokus. Ein weiteres Ziel war, dass durch das Projekt Erfahrungen gesammelt werden bzw. Know-how erworben wird, um Prozesse zu etablieren, die der ständigen Kontrolle und Aufrechterhaltung einer hinreichenden IT-Sicherheit in einem Netzwerk dienen.

↑ Server mit geöffneten Festplattenschächten

Vorgehen

In einem ersten Schritt führten die Verantwortlichen der WoGe-Service GmbH mit dem Sicherheitstool Mittelstand (www.SiToM.de) eine Selbsteinschätzung des vorhandenen IT-Sicherheitsniveaus durch. Dies erfolgte für insgesamt 14 Bereiche wie z. B. Verantwortlichkeiten, Datensicherung und Notfallmanagement eine Ist-Aufnahme der Organisation der IT-Sicherheit.

Als Zweites stand eine Analyse unter Nutzung der IoT (Internet of Things)-Suchmaschine Shodan im Mittelpunkt. Shodan ermittelt, welche konkreten Angaben bzgl. der vorhandenen IT-Infrastruktur für Außenstehende erkennbar sind. Diese Suchmaschine stellt u. a. geöffnete Ports dar und erkennt ggf. vorhandene Schwachstellen.

Abschließend führten wir mit dem mobilen Demonstrator „CVE-Scanner“ ein Schwachstellen-Scan in dem Unternehmensnetzwerk durch. Bei einem solchen Scan werden Schwachstellen in den Kategorien „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“ ermittelt und in einem Bericht zusammengefasst. Der Bericht dient den IT-Verantwortlichen dazu, Maßnahmen zur Verbesserung der IT-Sicherheit zu definieren und umzusetzen. Außerdem kann der Bericht als Basis für den Aufbau bzw. eine Verbesserung der Dokumentation herangezogen werden.

Lösung

Die Analyse des IT-Sicherheitsniveaus mittels SiToM zeigte, dass das Unternehmen im Managementbereich bereits recht gut aufgestellt ist. Sowohl die Aspekte der IT-Sicherheit als auch die Fragestellungen mit Blick auf den Datenschutz werden durch zahlreiche technische und organisatorische Maßnahmen beachtet und sind durch entsprechende Regelungen bzw. Maßnahmen gut umgesetzt.

Der Check mit der Suchmaschine Shodan ergab als einziges Ergebnis, dass das Netzwerk der WoGe-Service GmbH über diese Suchmaschine nicht zu sehen ist - also ein positives Ergebnis. Dazu wurde die feste IP-Adresse des Internetanschlusses verwendet.

Bei dem Schwachstellen-Scan im Unternehmensnetzwerk mit dem mobilen Demonstrator „CVE-Scanner“ wurden insgesamt 81 Netzwerkkomponenten identifiziert, von denen 71 Komponenten geprüft werden konnten. Die Ergebnisse hinsichtlich der ermittelten Schwachstellen wurden entsprechend der o. g. Kategorien in einem Bericht zusammengefasst. Der Bericht wurde 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.

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