Mittelstand-Digital
Zentrum
Chemnitz

PRAXISBEISPIEL

DIGITALISIERUNGSBEISPIEL

Vorbereitung einer TISAX-Zertifizierung

Ausgangssituation

Ein Hersteller für Automobilkomponenten priorisiert die Digitalisierung seiner Prozesse, um so langfristig seine Wettbewerbsfähigkeit zu garantieren. Basis dafür bildet seine IT-Infrastruktur, die derzeit aus ca. 60 adressierbaren Hardwarekomponenten im Unternehmensnetzwerk besteht. Der IT-Sicherheit kommt eine immer stärkere Bedeutung zu, denn Störungen in den Verwaltungs- und Produktionsprozessen müssen zwingend vermieden werden.

Außerdem fordern die Kundinnen und Kunden aus der Automobilindustrie die Einführung bzw. Umsetzung des sogenannten TISAX Standards. Dieser Standard gehört zu den Informationssicherheitsmanagementsystemen (ISMS) und ist speziell auf die Zulieferindustrie im Automobilbau ausgerichtet.

Zielstellung

Grundlegendes Ziel der Köstler GmbH bestand daher darin, die IT-Sicherheit nicht nur als Grundlage für weitere Schritte der Digitalisierung sondern insbesondere für die Einführung des TISAX-Standards zu erhöhen.

Dazu sollte eine Analyse des Unternehmensnetzwerkes bzw. eine Identifizierung evtl. vorhandener Schwachstellen im Netzwerk durchgeführt werden. Hierfür kam der mobile Schwachstellen-Scanner des Digitalzentrums Chemnitz zum

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

Einsatz. Die identifizierten Schwachstellen wurden nach Schweregrad geordnet und in einem Bericht erfasst. Zur weiteren Feststellung einer optimalen sicheren Konfiguration der vorhandenen Hardware-Komponenten wurde außerdem vorgesehen, die IoT-Suchmaschine Shodan einzusetzen. Die insgesamt ermittelten Ergebnisse dienen den IT-Verantwortlichen dazu, Maßnahmen zur Verbesserung der IT-Sicherheit zu definieren und umzusetzen. Mit Sicht auf den TISAX-Standard sollten die IT-Verantwortlichen durch das Projekt Erfahrungen sammeln und ihr Know-how ausbauen, um Prozesse zu etablieren, die der ständigen Kontrolle und Aufrechterhaltung einer hinreichenden IT-Sicherheit im Netzwerk dienen.

Neben diesem Check der Hard- und Softwarekomponenten stand auch die Awareness der Belegschaft im Fokus. Um zu sensibilisieren und ein höheres Sicherheitsbewusstsein aufzubauen, war eine Schulung zu ausgewählten IT-Sicherheitsthemen vorgesehen.

Vorgehen

Im Zusammenhang mit einer TISAX-Zertifizierung muss zum einen generell ein hohes IT-Sicherheitsniveau nachgewiesen werden, aber gleichzeitig auch deutlich gemacht werden, dass man periodisch (PDCA-Zyklus) daran arbeitet das Niveau weiter zu verbessern.

Ausgehend von diesen Anforderungen des TISAX-Standards bestand im Unternehmen die Herausforderung, Prozesse zu definieren bzw. zu etablieren, die sich dafür eignen, die IT-Sicherheit permanent zu monitoren, um so optimiert Maßnahmen abzuleiten und umzusetzen, die das Niveau entsprechend erhöhen.

Bereits vor dem ersten Vor-Ort-Termin wurden der Zeitrahmen und die Schulungsinhalte sowie technische Parameter für den Schwachstellen-Scan abgestimmt. Ziel der Schulungen war es, die Mitarbeitenden für Bedrohungen zu sensibilisieren. Wichtige Schulungsinhalte waren beispielsweise der Umgang mit Passwörtern und mobilen Datenträgern, sowie relevante Datenschutzthemen.

Bei der Analyse der Hard- und Software vor Ort identifizierte der Schwachstellen-Scanner potenzielle Sicherheitslücken, kategorisierte sie in die Stufen „Kritisch“, „Hoch“, „Mittel“ und „Niedrig“ und fasste sie in einem Bericht zusammen. Mit Hilfe des Berichts können die IT-Verantwortlichen gezielte Maßnahmen zur Behebung der Schwachstellen und zur Verbesserung der IT-Sicherheit ableiten. Zudem können die Erkenntnisse beim Aufbau oder der Optimierung der IT-Dokumentation unterstützen.

Eine weitere Analyse mithilfe der IoT-Suchmaschine Shodan zeigte, welche Informationen über die bestehende IT-Infrastruktur über den Internetanschluss für Dritte sichtbar sind. Die Suchmaschine identifiziert unter anderem geöffnete Ports und mögliche Schwachstellen, wodurch zusätzliche Sicherheitsrisiken aufgedeckt werden können.

Ergebnisse

Unser mobiler Demonstrator „CVE-Scanner“ identifizierte 52 überprüfbare Netzwerkkomponenten. Für weitere Komponenten konnten zwar IP-Adressen erfasst werden, jedoch war eine detaillierte Analyse nicht möglich. Dies bedeutet, dass potenzielle Angreifer ebenfalls keinen Zugriff auf Informationen zu möglichen Schwachstellen erhalten, da die entsprechenden Ports und Dienste nicht freigegeben sind.

Basierend auf den Ergebnissen der Scans wurden notwendige Maßnahmen entsprechend ihrer Dringlichkeit definiert und zeitnah umgesetzt, wodurch die Netzwerksicherheit verbessert werden konnte. Insgesamt zeigte die Untersuchung, dass die Hardware in einem zufriedenstellenden Zustand ist. Viele der identifizierten Schwachstellen und Sicherheitslücken können durch entsprechende Updates oder Patches zeitnah behoben werden.

Der Grundstein für eine erfolgreiche TISAX-Zertifizierung ist somit im Unternehmen gelegt.

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