DIGITALISIERUNGSBEISPIEL

Härtung eines Netzwerks für ein sicheres ERP

Ausgangssituation

Der B2B-Handel mit Produkten der Antriebs- und Wälzlagertechnik ist ein wettbewerbsintensiver Markt. Die Schulz Kugellager GmbH beschäftigt aktuell acht hoch spezialisierte Mitarbeitende. Mit der Geschwindigkeit des Marktes und der Kundschaft mitzuhalten, stellte die bislang genutzte IT-Infrastruktur vor größere Herausforderungen.

Kundenkommunikation, Bestellprozesse über persönliche Kanäle der Mitarbeitenden, aufwendige Produktrecherchen, manuelle Angebots- und Rechnungsstellungen oder Materialbewirtschaftung – das Team der Schulz Kugellager GmbH musste dringend den immensen internen Kommunikations- und Abstimmungsbedarf reduzieren. Die automatisierte Auftragsverarbeitung verspricht eine zügigere Bearbeitung der Kundenbedarfe.

„Wir haben durch die konzertierte Zusammenarbeit mit den Experten aus Mittelstand-Digital in kurzer Zeit einen großen Schritt in Richtung unserer passgenauen Digitalisierung gemacht – zum Beispiel unsere identifizierten Sicherheitslücken zügig geschlossen."

Timo Sauerländer, Gesellschafter & Prokurist der Schulz Kugellager GmbH

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

In dieser Situation nahm der Geschäftsführer an einer kostenfreien Digitalisierungssprechstunde des Mittelstand-Digital Zentrums Zukunftskultur teil. Im Gespräch wurden die Möglichkeiten einer Unterstützung durch das Mittelstand-Digital Netzwerk in den verschiedenen Handlungsfeldern aufgezeigt und diskutiert.

Zielstellung

Ziel des Projektes war die Optimierung der gesamten Prozesslandschaft. Die Basis für dieses Gesamtvorhaben stellte eine optimal funktionierende und sichere IT-Infrastruktur dar. Um die bestmögliche IT-Sicherheit in dem vorhandenen Unternehmensnetzwerk aufzubauen bzw. zu gewährleisten, sollte eine Schwachstellenanalyse der IT-Systeme durchgeführt werden – unabhängig von einer evtl. notwendigen Erweiterung der vorhandenen IT-Infrastruktur. Neben diesem Check der Hard- und Softwarekomponenten stand auch die Awareness der Belegschaft im Fokus. Außerdem konnten 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.

Vorgehen

Für das Handlungsfeld der IT-Sicherheit stimmten wir gemeinsam mit dem IT-Dienstleister zunächst in einem Online-Termin die Vorgehensweise ab. Bei einem Vor-Ort-Termin mit dem mobilen Demonstrator „CVE-Scanner“ führten wir einen Schwachstellen-Scan des Unternehmensnetzwerks 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 im Zusammenhang mit einer Inventarisierung von Komponenten als Basis für den Aufbau bzw. eine Verbesserung der Dokumentation herangezogen werden.

In Anlehnung an den BSI-Leitfaden IT-Sicherheit besprachen die Beteiligten während des Scans die aktuellen technischen und organisatorischen Maßnahmen für die IT-Sicherheit. So konnten sie Ansätze für mögliche Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus identifizieren. Zusätzlich nahm die Geschäftsführung mit Hilfe des Sicherheitstools Mittelstand (SiToM.de) eine Selbsteinschätzung bzgl. des vorhandenen IT-Sicherheitsniveaus vor.

Ergebnisse

Der Schwachstellen-Scan des Unternehmensnetzwerks mit dem mobilen Demonstrator „CVE-Scanner“ erkannte 14 prüfbare Netzwerkkomponenten mit einigen kritischen Sicherheitslücken und weiteren Schwachstellen mit hohem bzw. mittlerem Risiko. Die Auswertung ergab, dass für 90 % der ermittelten Schwachstellen allein ein zur Datenspeicherung/-sicherung eingesetztes Network Attached Storage (NAS) verantwortlich ist und z. B. Zugangsmöglichkeiten durch entsprechende Weboberflächen ermöglicht. Die Ursachen lagen hauptsächlich in fehlenden Updates.

Insgesamt zeigte sich ein befriedigender Zustand der Hardware. Entsprechende Updates können eine Vielzahl der Schwachstellen bzw. Sicherheitslücken beheben. Wir stellten dem Unternehmen eine vollständige Übersicht der Ergebnisse zur Verfügung. Zusammen mit dem ebenfalls eingebundenen IT-Dienstleister werden die sich daraus ableitenden Maßnahmen nun abgestimmt und eingeleitet.

Die Auswertung des Gesprächs anhand des BSI-Leitfadens sowie der Ergebnisse der Selbsteinschätzung mittels SiToM ergaben, dass einige technische und organisatorische Maßnahmen wie bspw. ein optimiertes Benutzer-/Rechte-Konzept, weiterführende Dokumentationen und Regelungen zum Einsatz externer Datenträger sowie zielführende Schulungen des Personals zur weiteren Erhöhung des IT-Sicherheitsniveaus beitragen können.

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