DIGITALISIERUNGSBEISPIEL

Verschlüsselte Daten nach einem Sicherheitsvorfall wiederherstellen

Ausgangssituation

Die IT-Sicherheit ist ein wesentlicher Erfolgsfaktor bei allen Digitalisierungsbestrebungen. Denn durch Ransomware können z. B. Unternehmensdaten vollständig verschlüsselt und ihre Verfügbarkeit verhindert werden.

Das in diesem Praxisbeispiel von einer Malware betroffene Unternehmen wurde 1992 gegründet und bietet seitdem unterschiedliche Beratungsdienstleistungen für Unternehmen und Handwerksbetriebe an. Neben Daten aus dem Buchhaltungsbereich werden umfangreiche, kundenspezifische Datenbestände verwaltet. Eine Datensicherung erfolgt täglich auf zwei unterschiedlichen Datenträgern, die getrennt voneinander aufbewahrt werden. Ausgangspunkt der unerwünschten Datenverschlüsselung war eine Phishing-Mail mit dem Betreff „Rechnung“. Auf Grund einer kurz zuvor ausgelösten Bestellung wartete man im Unternehmen tatsächlich auf eine Rechnung per E-Mail und so wurde trotz entsprechender Schulungen ein Link angeklickt, der nicht die Rechnung beinhaltete, sondern Schadcode aus einer Dropbox-Cloud geladen und ausgeführt hat.

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

Mittelstand-Digital
Zentrum Chemnitz

PRAXISBEISPIEL

Zielstellung

Nach Feststellung der Datenverschlüsselung bestand das Ziel in der schnellstmöglichen Wiederherstellung aller verschlüsselten Datenbestände bzw. der vollständigen IT-Infrastruktur. Bei den zu planenden Arbeiten zur Beseitigung der Schäden musste insbesondere darauf geachtet werden, dass die Ursachen bzw. Quellen für die Verschlüsselung in Form des ausführbaren Schadcodes beseitigt werden, so dass keine Gefahr vor einer erneuten Ransomware-Attacke durch diesen Schadcode bestand.

Vorgehen

Die unternehmensinternen IT-Verantwortlichen trennten zunächst alle Internet- sowie Netzwerkverbindungen, fuhren die Systeme herunter und informierten den externen IT-Dienstleister. Nach einer Analyse des Sicherheitsvorfalls wurden gemeinsam die einzelnen Arbeiten besprochen und verteilt. Der IT-Dienstleister übernahm die Überprüfung und Wiederherstellung der vorhandenen 13 virtuellen Server-Systeme inklusive der Rücksicherung des aktuellsten Datenbestandes auf den Daten-Server. Die beiden internen Administratoren übernahmen den Check der einzelnen Arbeitsplatzrechner mit einer aktuellen Rescue-DVD (Schadware-Check). Den Rechner, über den die Phishing-Mail bzw. die Ransomware eindrang, setzten sie vollständig neu auf, um ein Restrisiko auszuschließen.

Lösung

Das Unternehmen konnte sowohl die Datenrücksicherung als auch die Wiederherstellung der kompletten IT-Infrastruktur in einem Zeitraum von weniger als 9 Stunden erfolgreich durchführen. Die eingesetzten Antiviren- und Firewall-Lösungen konnten die Datenverschlüsselung zwar nicht verhindern, aber das Gesamtpaket der im Unternehmen vorhandenen bzw. realisierten IT-Sicherheitsmaßnahmen war die entscheidende Basis für die erfolgreiche Bearbeitung des Sicherheitsvorfalls. Wesentliche Punkte waren:

- Vereinbarung der Leistungen und Reaktionszeiten in einem IT-Dienstleistervertrag
- Festlegungen zu IT-Verantwortlichkeiten
- regelmäßige, kontrollierte Datensicherung
- Einsatz von geeigneter Schutzsoftware
- Dokumentation der Soft- und Hardwaresysteme
- Aufbau eines Notfallplans

Die Auswertung des Vorfalls führte darüber hinaus zu folgenden Erkenntnissen bzw. konkreten Maßnahmen:

- Vorhandene Schutzsoftware/Technik war korrekt konfiguriert.
- Trotz regelmäßiger Schulungen lag menschliches Versagen vor.
- Der Vorfall hätte bei der Polizei bzw. LKA angezeigt werden sollen.
- Für eine tiefer gehende Analyse des Vorfalls hätten die Rechner nicht ausgeschaltet werden dürfen. Eine Trennung vom Netzwerk bzw. vom Internet hätte ausgereicht.
- Nach dem Sicherheitsvorfall wurde zur Minimierung der Bedrohungen aus dem Internet neben dem E-Mail-Proxy auch ein Web-Proxy implementiert.

„Die Verschlüsselung bzw. die Wiederherstellung der IT-Infrastrukturen hat uns zwar gezeigt, dass die getroffenen Maßnahmen für solche Vorfälle und auch das installierte Notfallmanagement gut funktioniert haben, aber auch, dass der Mensch nach wie vor ein entscheidender Faktor bei dem Thema der IT-Sicherheit in den Unternehmen ist.“

interner Administrator des Unternehmens

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