CONTINUM

DIE KRITISCHEN TAGE NACH EINER CYBERATTACKE: EIN FALLBERICHT

VON JULIAN SAYER

Julian Sayer,
Vorstand bei der Continum AG. Foto: ZVG

Mehr als zwei Drittel der deutschen Unternehmen waren 2021 von erpresserischer Schadware betroffen. Zu diesem Ergebnis kommt die neue Sophos-Studie „State of Ransomware 2022“. Das durchschnittlich gezahlte Lösegeld in Deutschland ist demnach um fast das Doppelte auf 253.160 Euro angestiegen. Allerdings nicht in folgendem Fall, den Continum jüngst begleitet hat.

Mitte März 2022 war ein großes deutsches Unternehmen mit mehreren tausend Mitarbeitern Ziel einer Cyberattacke. Alle Unternehmens-Server wurden verschlüsselt, und die Angreifer forderten Lösegeld. Ein IT-Mitarbeiter des Unternehmens handelte sehr geistesgegenwärtig. Er sicherte in letzter Minute manuell die ERP-Datenbank („Enterprise Resource Planning“) auf einer externen Festplatte und veranlasste dann den Shutdown aller Server. Das konnte zwar nicht mehr das Verschlüsseln der Server und der gesamten Back-up-Dateien verhindern. Aber die manuelle externe Datensicherung gab Anlass zur Hoffnung in dem Super-GAU.

Unmittelbar nach dem Cyberangriff schaltete das Unternehmen das Landeskriminalamt (LKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein und stellte Strafanzeige. Das ist wichtig, denn eine Strafanzeige ist die Grundlage für etwaige Versicherungsansprüche.

Die Situation nach der Attacke: Das Unternehmen hatte eine IT-Infrastruktur im eigenen Rechenzentrum, die verschlüsselt und so nicht mehr zu gebrauchen war. Darüber hinaus gab es eine oder mehrere Sicherheitslücken, über die die Angreifer sich Zugang zu den Systemen verschafften, sowie eine Produktion, die durch fehlende IT-Unterstützung fast komplett stillstand. Hier kam Continum ins Spiel. Man beschloss, die unternehmenskritische ERP-Umgebung ins Continum Rechenzentrum auszulagern beziehungsweise dort neu aufzubauen.

Einen Tag nach dieser Vereinbarung und sieben Tage nach dem Cyberangriff stand die benötigte Infrastruktur im Continum-Rechenzentrum bereit, und der mühsame Wiederaufbau des ERP-Systems konnte beginnen. Ein Vorteil dabei: Das ERP-Systemhaus konnte viele kundenindividuelle Systemteile noch rekonstruieren.

Fünf Wochen nach dem Angriff startete das ERP-System wieder mit einer begrenzten Anzahl von Usern. Die während des Shutdowns angefallenen manuellen Auftragsdaten wurden mit großem Aufwand im ERP-System nacherfasst. Sechs Wochen nach dem Angriff konnte man zum Normalbetrieb des ERP-Systems übergehen. Ab diesem Zeitpunkt lief es wieder richtig, und alle Benutzer hatten wie gewohnt Zugriff darauf.

Fazit: Durch die fokussierte und enge Zusammenarbeit aller Beteiligter konnte das ERP-System des angegriffenen Unternehmens in Rekordzeit ins Continum Rechenzentrum verlagert und dort wieder live geschaltet werden. Alle Kunden des betroffenen Unternehmens zeigten ein hohes Maß an Solidarität in der Krisensituation und sind diesem erhalten geblieben.

Julian Sayer ist Vorstand für Vertrieb, Marketing und Entwicklung des Freiburger Hostingunternehmens und Cloud Solution Providers Continum AG. Als AWS und Microsoft Azure Partner versteht sich die Continum AG als Anwalt des Kunden und unterstützt Unternehmen auf dem sicheren Weg in die Cloud.