# CASE STUDY Systemverschlüsselung durch Cyberangriff

Kürzlich wurde Continum zum Helfer in der Not: ein großes Unternehmen mit mehreren Tausend Mitarbeitern war Opfer eines Ransomware-Angriffs geworden. Das betroffene Unternehmen wendete sich hilfesuchend an unser Partnerunternehmen, einen ERP-Softwarehersteller, und an Continum. Durch fokussierte und engmaschige Zusammenarbeit aller Beteiligten konnte das ERP-System unseres Neukunden in Rekordzeit binnen weniger Wochen aus dem eigenen Rechenzentrum ins Continum Rechenzentrum verlagert und wieder produktiv lauffähig gemacht werden.

## WAS WAR GESCHEHEN?

Mitte März 2022 wurde ein großes deutsches Unternehmen Opfer einer Cyberattacke. Infolgedessen wurden die gesamten Unternehmens-Server verschlüsselt und Lösegeld gefordert.

Geistesgegenwärtig nahm ein IT-Mitarbeiter des Unternehmens in letzter Minute eine manuelle Datensicherung der ERP-Datenbank (ERP = Enterprise Resource Planning Software) auf eine externe Festplatte vor und veranlasste danach den Shutdown aller Server. Leider konnte ein Verschlüsseln der Server und der gesamten Backupdateien durch den Shutdown nicht mehr verhindert werden, die manuelle Datensicherung auf dem externen Datenträger war jedoch das kleine Pflänzchen Hoffnung in dem Super-GAU.
Unmittelbar nach dem Cyberangriff wurde das Landeskriminalamt (LKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeschaltet und es wurde Strafanzeige gestellt. Dieses Vorgehen ist für das geschädigte Unternehmen extrem wichtig, da eine Strafanzeige die Grundlage für etwaige Versicherungsansprüche ist.

Das betroffene Unternehmen hatte nun eine IT-Infrastruktur im eigenen Rechenzentrum, die verschlüsselt und so nicht mehr zu gebrauchen war. Die Produktion kam durch die fehlende IT-Unterstützung nahezu vollständig zum Erliegen. In dieser Ausgangslage kam Continum ins Spiel und es wurde vereinbart, die unternehmenskritische ERP-Umgebung schnellstmöglich ins Continum Rechenzentrum auszulagern bzw. dort neu aufzubauen.

## 7 TAGE NACH ANGRIFF

Bereits einen Tag nach Vereinbarung und somit eine knappe Woche nach dem Cyberattacke hatte Continum die benötigte Infrastruktur aufgebaut und dem Kunden übergeben, sodass mit der Wiederherstellung des ERP-Systems begonnen werden konnte.

## FÜNF WOCHEN NACH ANGRIFF

Nur fünf Wochen nach dem Angriff konnte der Neustart und Betrieb des ERP-Systems mit einer begrenzten Anzahl von Usern sichergestellt werden. Ebenso wurden zusätzlich die während des Shutdowns angefallenen manuellen Auftragsdaten mit großer Anstrengung des Kunden ins ERP-System nacherfasst.

## SECHS WOCHEN NACH ANGRIFF

Eine weitere Woche später konnte endlich zum normalen Betrieb übergegangen werden und alle User erhielten wie gewohnt ERP-Zugriff.

### FAZIT

Hervorzuheben ist insbesondere die hohe Solidarität aller Beteiligten, welche die reibungslose Abwicklung erst möglich machte. Auch die Kunden des betroffenen Unternehmens zeigten ein hohes Maß an Verständnis für die ungewöhnliche Situation. Kein Kunde hat seine Geschäftsbeziehung mit dem in Not geratenen Unternehmen aufgrund des Cyberangriffs beendet.

Der Kunde war vom Einsatz der Continum AG und des ERP-Partners beeindruckt. Das unternehmenskritische ERP-System ging vor vielen anderen betroffenen Systemen (z.B. E-Mail-System) produktiv. Dieser beschriebene reale Fall zeigt, was für grandiose Erfolge erzielt werden können, wenn alle beteiligten Parteien für den maximalen Kundenerfolg zusammenarbeiten!