CASE STUDY Notfall-Management Ransomware Attacke

IT-Ausfälle bedrohen schnell Bilanzen oder gar Existenzen von Unternehmen. Risiko-Management, unternehmenseigene Richtlinien und gesetzliche Anforderungen fordern daher wirksame Maßnahmen, um Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme und Daten auch im Falle einer Cyberattacke zu gewährleisten.
Für Continum ist IT-Sicherheit die Maxime des alltäglichen Handelns. Kontinuierliche Zertifizierungen nach ISO 27001 und den strengen Standards der Kreditkartenindustrie (PCI-DSS) garantieren ausgereifte Prozesse und Werkzeuge im Bereich Cyber Security.

KUNDENPROFIL

Unser Kunde ist ein seit über 80 Jahren europaweit führender Anbieter von qualitativ hochwertigen Pipettierhilfen. Zu den Kunden des Unternehmens zählen u.a. Branchen wie Pharmazie, Chemie, Lebensmittel und Getränke. Der Mittelständler unterhält mehrere europäische Tochtergesellschaften und beschäftigt ca. 2000 Mitarbeiter.

AUSGANGSSITUATION

Ransomware Angriffe haben in den letzten Jahren stark zugenommen. Die Art der Notfälle, die bei IT-Systemen auftreten können, werden zunehmend komplexer und Cyberattacken immer raffinierter. Ein neuer Erpressertrend besteht darin, nicht nur die Vernichtung aller Datenbestände eines Unternehmens oder einer Institution anzudrohen, sondern auch deren Backups.
Unser Kunde hatte kein ausreichende Notfallmanagement für den Ernstfall. Das Unternehmen wäre im Falle eines Angriffs auf die Unternehmens-IT nicht mehr in der Lage gewesen, zu operieren.

ANFORDERUNGEN

Unser Kunde möchte auf feindliche Ransomware Attacken umfassend vorbereitet und in der Lage sein, mögliche Schäden zu begrenzen sowie im Ernstfall handlungsfähig zu bleiben. Der Notfallplan sollte IT-Sofortmaßnahmen konkret beschreiben sowie Geschäftsfortführungspläne und Wiederanlaufpläne enthalten. Ebenso sollte enthalten sein, wie Geschäftspartner im Notfall informiert werden.

LÖSUNG

Da es im Notfall erforderlich ist, dass sowohl Notfallhandbuch als auch weitere kritische Daten schnell zugänglich sind, müssen diese zwingend außerhalb der Unternehmens-IT aufbewahrt werden. Nur so kann sichergestellt werden, dass diese Informationen nach einem Angriff für den Krisenstab des Unternehmens tatsächlich noch verfügbar sind.
Im vorliegenden Fall wurde aus diesem Grund ein einfacher Notfallblog, ein Mailsystem sowie ein Dokumentensafe, in dem das Notfallhandbuch und weitere wichtige Dokumente liegen, für unseren Kunden auf der Continum Infrastruktur bereitgestellt.
Sollte der Kunde Ziel eines Ransomware-Angriffs werden, wird der Notfallblog sowie das unabhängige Mailsystem aktiviert und die Geschäftspartner unseres Kunden über den Krisenstatus informiert.

Der Zugriff zur Pflege des Notfall-Blogs sowie zum Dokumenten-Safe ist ausschließlich für die zuvor definierten Mitarbeiter des Krisenstabs und für Schlüsselpersonen des Unternehmens vorgesehen. Der Zugang ist über eine 2-Faktor Authentifizierung abgesichert.

ERGEBNIS

- Notfallblog, Dokumentensafe und unabhängiges Mailsystem befinden sich im hochsicheren, nach ISO/IEC 27001 zertifizierten Rechenzentrum der Continum AG in Deutschland. Sie unterliegen damit dem strengen Bundesdatenschutzgesetz der Bundesrepublik Deutschland und der EU-DSGVO.
- Nur die Mitglieder des Krisenstabs des Unternehmens können auf Notfallblog, Mailsystem und Dokumentensafe zugreifen. Der Zugang ist durch 2-Faktor Authentifizierung abgesichert.
- Im Ernstfall kann auf vorgefertigte Krisenabläufe zugegriffen werden und Geschäftspartner werden über den Krisenstatus des Unternehmens zuverlässig informiert.
- Das Unternehmen kann sich beruhigt auf das Kerngeschäft konzentrieren. Im Ernstfall bleibt das Unternehmen weiterhin handlungsfähig und kann besonnen handeln.

GERNE BEANTWORTEN WIR IHRE FRAGEN | + 49 - 761 - 217 111 - 20 | vertrieb@continum.net