DAVINCI RECHENZENTRUM

"WE CONNECT PEOPLE, WORLDWIDE"

DAVINCI Rechenzentrum GmbH
O4, 4 · 68161 Mannheim
Edisonstraße 2 · 68519 Viernheim
0621 877 55 990 · post@davinci-rechenzentrum.de

REFERENZ · TECHNOLOGIEUNTERNEHMEN

Totalausfall durch Ransomware – nach acht Stunden wieder arbeitsfähig

Ein großes mittelständisches Technologieunternehmen in Baden-Württemberg stand nach einem Ransomware-Angriff still. Wir wurden ergänzend als zweites IT-Unternehmen hinzugezogen, haben den Angriff rekonstruiert, alle Anlagen bereinigt und den Betrieb innerhalb von acht Stunden wieder hochgefahren.

Eckdaten

Branche	großes mittelständisches Technologieunternehmen
Region	Baden-Württemberg
Lage	Totalausfall durch Ransomware
Unsere Rolle	ergänzend hinzugezogenes Incident-Response-Team, kein Bestandskunde
Leistungen	Angriffsanalyse, forensische Rekonstruktion, Bereinigung, Wiederanlauf
Ergebnis in diesem Fall	wieder arbeitsfähig nach acht Stunden

Ausgangslage: Nichts geht mehr

Ein Ransomware-Angriff hatte die Systeme des Unternehmens verschlüsselt. Kein Zugriff auf Daten, keine Anwendungen, kein geordneter Betrieb – ein Totalausfall. Die bestehende IT-Firma war im Einsatz. Wir wurden ergänzend als zweites IT-Unternehmen hinzugezogen, um die Lage zu klären und den Wiederanlauf zu tragen.

In solchen Stunden entscheidet nicht Tempo allein, sondern Ruhe und Methode. Wer zu früh wiederherstellt, holt den Angreifer womöglich mit zurück.

Was wir getan haben

Die Reihenfolge war fest: erst verstehen, dann bereinigen, dann wieder anlaufen. Angriffsweg und Details nennen wir hier bewusst nicht – sie würden den Kunden erkennbar machen und Angreifern nützen.

Lage klären: Sofort ermittelt, woher der Angriff kam und was genau geschehen war – welche Systeme betroffen sind und welche nicht.

Forensisch rekonstruieren: Den Ablauf des Angriffs nachvollzogen, damit klar ist, wo der Zugang lag und was geschlossen werden muss, bevor irgendetwas wieder ans Netz geht.

Alle Anlagen bereinigen: Jedes betroffene System bereinigt oder neu aufgesetzt – nicht nur die, die auffällig waren.

Kontrolliert wieder anlaufen: Die Anlagen in einer festen Reihenfolge hochgefahren und geprüft. Nach acht Stunden konnte das Unternehmen wieder arbeiten.

Was in den ersten Stunden nach einem Angriff zählt

Die ersten Stunden fühlen sich an, als müsse alles gleichzeitig passieren. Tatsächlich hilft das Gegenteil: eine klare Reihenfolge, eine Stelle, die entscheidet, und keine Wiederherstellung, bevor der Zugang des Angreifers verstanden ist.

Das ist auch der Grund, warum zwei IT-Firmen in einem solchen Fall gut zusammenarbeiten können: Die eine kennt die Umgebung, die andere bringt den Blick von außen und die Erfahrung aus Angriffen mit. Wir wurden ergänzend hinzugezogen – eine Schuldfrage stellte sich dabei nicht.

Ergebnis: arbeitsfähig nach acht Stunden

Innerhalb von acht Stunden liefen die Anlagen wieder, bereinigt und geprüft. Acht Stunden sind der Wert aus diesem Fall – wie lange ein Wiederanlauf dauert, hängt von Umgebung, Sicherung und Vorbereitung ab.

Für IT-Verantwortliche: Ablauf in vier Schritten

- Eindämmung: betroffene Systeme isolieren, Zugänge sperren, Spuren sichern, bevor etwas verändert wird.
- Analyse: Einstiegspunkt und Ausbreitung rekonstruieren; erst danach steht fest, welche Systeme bereinigt und welche neu aufgesetzt werden müssen.
- Bereinigung: alle betroffenen Anlagen, nicht nur die auffälligen; Zugangsdaten erneuern.
- Wiederanlauf: in fester Reihenfolge aus geprüften Sicherungen, mit Kontrolle jedes Schritts; Dokumentation für Versicherung und Meldepflichten.

Projektwerte: Alle Zahlen stammen aus diesem einen Projekt und sind kein allgemeines Leistungsversprechen. Der Kunde bleibt aus Vertraulichkeitsgründen ungenannt. Online mit allen Verweisen: davinci-rechenzentrum.de/referenzen/ransomware-wiederanlauf

---

Ihr Ansprechpartner: **Metehan Kurt**, Geschäftsführer 0621 877 55 990 · post@davinci-rechenzentrum.de