

REFERENZ · PRODUZIERENDES GEWERBE

Nach dem Ransomware-Angriff: Forensik, Gutachten und Neuaufbau – vom 100-Mbit-Netz zum 25-Gbit-Backbone

Ein produzierendes mittelständisches Unternehmen aus dem Raum Mannheim verlor bei einem Ransomware-Angriff Teile seiner Buchhaltung. Wir haben den Angriff forensisch aufgearbeitet, die Rekonstruktion technisch begleitet und die Infrastruktur von der Glasfaser bis zum Serverraum neu aufgebaut. Die Zusammenarbeit besteht bis heute.

Eckdaten

Branche	produzierendes mittelständisches Unternehmen
Standorte	Verwaltung und mehrere Produktionshallen im Raum Mannheim, ein weiterer Standort in Baden-Württemberg
Unsere Rolle	Forensik und Gutachten → Begleitung der Rekonstruktion → Bestandsaufnahme → Neuaufbau → laufende Betreuung
Ausgangsnetz	100 Mbit/s am Sternpunkt, Komponenten teils über 15 Jahre alt
Neues Netz	Glasfaser-Backbone, Core 25 Gbit/s, Switches untereinander 10 Gbit/s
Sicherheit	sechs getrennte Netzbereiche, Firewall mit VPN zwischen den Standorten, Angriffserkennung rund um die Uhr
Dauer des Neaufbaus in diesem Projekt	rund fünf Monate
Datensicherung	Standard des Hauses in fünf Stufen, Wiederherstellungstest alle zwei Monate
Zusammenarbeit	besteht bis heute

Ausgangslage: Ein Angriff auf eine Anlage, die lange niemand angefasst hatte

Das Unternehmen fertigt im Raum Mannheim in mehreren Hallen, die Verwaltung sitzt auf demselben Gelände, dazu kommt ein weiterer Standort in Baden-Württemberg. Die IT war über viele Jahre gewachsen, eine dokumentierte Wartung gab es nicht. Als die Ransomware zuschlug, traf sie auf eine Umgebung, die ihr kaum etwas entgegensetzte.

Der schwerste Schaden lag nicht bei den Rechnern, sondern in der Buchhaltung: Ein Teil der Daten war verloren und musste im Nachgang aufwendig rekonstruiert werden. Wie lange so

etwas dauert, lässt sich vorher kaum planen. Es kostet Zeit und Geld, und fehlende Buchhaltungsdaten können Haftungsfragen für die Unternehmensleitung aufwerfen. Was dazu gehört, beschreibt unser Fachbereich Verfahrensdokumentation.

Nachdem der Betrieb notdürftig wieder lief, konnte der bisherige Dienstleister die Betreuung nicht mehr leisten. Wir haben übernommen.

Bei der Übernahme fanden wir eine Verkabelung aus den frühen 2000er-Jahren, teils frei durch den Raum geführt, ohne Kabeltrassen. Gigabit-Switches hingen an 100-Mbit/s-Verteilern am Sternpunkt – das ganze Netz lief so schnell wie sein langsamstes Glied. Einzelne Komponenten waren defekt, viele älter als 15 Jahre. Der Serverraum hatte ein offenes Rack, keinen Potenzialausgleich und eine Klimatisierung, die im Sommer nicht mehr reichte.

Viele Unternehmen wechseln ihren IT-Partner erst, wenn etwas passiert ist. Gewohnheit ist verständlich – aber teuer.

Stufe 1: Aufklären und aufarbeiten

Bevor etwas neu gebaut wird, muss klar sein, wie der Angreifer hereingekommen ist. Sonst baut man ihm dieselbe Tür noch einmal.

Forensische Analyse: Einfallstor, Ausbreitung, Zeitachse und betroffene Systeme rekonstruiert. Das Ergebnis steht in einem schriftlichen Gutachten.

Verschlüsselte Datenträger aufbewahrt: Die verschlüsselten Festplatten haben wir gesichert und verwahrt – als Beweismittel und für den Fall, dass es später ein Entschlüsselungswerkzeug gibt. Das kommt vor, wenn Ermittler die Schlüssel einer Tätergruppe sicherstellen und veröffentlichen.

Meldungen und Versicherung: Die Meldung an Polizei und Datenschutzaufsicht und die Abstimmung mit der Cyberversicherung haben wir begleitet.

Neu aufgesetzt statt bereinigt: Kompromittierte Systeme wurden neu installiert, alle Zugangsdaten erneuert.

Buchhaltungsdaten rekonstruiert: Die technische Rekonstruktion haben wir übernommen: Datenbestände wiederhergestellt, Fragmente zusammengeführt, Lücken dokumentiert. Die steuerliche Würdigung und alle Korrekturen lagen beim Steuerberater des Unternehmens.

Bestandsaufnahme: Auf ausdrücklichen Wunsch der Geschäftsführung – „alles auf den neuesten Stand“ – haben wir die gesamte IT- und Gebäudeinfrastruktur aufgenommen. Sie war die Grundlage für den Neuaufbau.

Stufe 2: Neu bauen, von der Glasfaser bis zum Serverraum

Gebaut wurde mit Reserven über die heutigen Anforderungen hinaus, damit die nächste Erweiterung keine neue Baustelle wird. Der Neuaufbau dauerte in diesem Projekt rund fünf Monate, bei laufender Produktion.

Glasfaser-Backbone: Verwaltung und Hallen per Lichtwellenleiter verbunden, die längste Strecke misst rund 100 bis 120 Meter. Vom Hauptverteiler aus versorgen drei Unterverteiler die Produktionsbereiche.

Kabeltrassen und Durchbrüche: Trassen in den Hallen bis zum Serverraum neu errichtet, Wanddurchbrüche hergestellt und fachgerecht verschlossen.

Verwaltung neu verkabelt: Brüstungskanäle und S/FTP-Installationskabel der Kategorie 7A (bis 1.200 MHz). Arbeitsplätze mit hohem Datenaufkommen hängen direkt per Glasfaser am Serverraum.

Leistungsstufen: Core-Switch mit 25 Gbit/s, Switches untereinander mit 10 Gbit/s, einzelne Systeme – vor allem der Videospeicher – mit 10 Gbit/s angebunden. An den entscheidenden Stellen ist das die 100- bis 250-fache Bandbreite des alten Flaschenhalses.

Verwaltete Switches: PoE-Switches mit zentralem Management, damit das ganze Netz an einer Stelle überwacht wird.

Serverraum: Geschlossener Serverschrank statt offenem Rack. Potenzialausgleich vom Hauptpotenzialausgleich im Keller bis in den Serverraum im Obergeschoss nachgerüstet, ausgeführt von einem Elektrofachbetrieb in unserem Projekt. Ableitfähiger Bodenbelag mit ableitfähigem Kleber gegen elektrostatische Entladung, Ersatzklimatisierung – kurzfristig mitten im Hochsommer beschafft – und eine USV für Serverraum und Verteiler. Alles nach Stand der Technik.

Getrennte Netze: Verwaltung, Produktion, Videoüberwachung, Zeiterfassung und Zutritt, Sensorik und Gäste-WLAN laufen in getrennten Netzen. Ein kompromittiertes Gerät erreicht nicht mehr das ganze Unternehmen.

Firewall und VPN: Securepoint-Firewall erneuert, verschlüsselte Verbindungen zwischen allen Standorten.

Satelliten-Internet: Ein Standort hatte keine ausreichend schnelle Anbindung. Über Satelliten-Internet arbeiten jetzt alle Standorte vernetzt zusammen.

Angriffserkennung rund um die Uhr: G DATA MXDR überwacht die Endgeräte und Server und schlägt Alarm, wenn sich etwas auffällig verhält – auch nachts und am Wochenende.

Zugang: Mehrfaktor-Anmeldung und getrennte Administratorkonten.

Betrieb: Patch- und Update-Management, Monitoring mit Alarmierung, vollständige Netzwerkdokumentation mit Netzplan, Patchplänen und Kabelbeschriftung, dazu ein Notfallhandbuch.

Mitarbeitende sensibilisiert: Schulung gegen Phishing, damit die nächste gefälschte Mail seltener ankommt.

Produktion: WLAN mit rund zehn Access Points; Temperatursensorik mit Alarmierung und Notfallablauf, wenn Grenzwerte über- oder unterschritten werden.

Video, Zeiterfassung, Zutritt: Mehr als 35 Kameras mit eigenem Speicherserver für eine längere Aufbewahrung, Zeiterfassung in allen Bereichen und am weiteren Standort, biometrische Zutrittskontrolle für die Verwaltung. Videoüberwachung und biometrische Zutrittskontrolle sind datenschutzkonform nach DSGVO umgesetzt.

Datensicherung nach unserem Standard: Fünf Stufen: Sicherung beim Kunden vor Ort, zusätzliche Offline-Sicherung vor Ort, Sicherung ins Partner-Rechenzentrum, stromlos verwahrte Sicherung in unseren Backup-Cluster-Racks in Viernheim, Notfallsystem. Wiederherstellungstest alle zwei Monate außerhalb der Kundenumgebung.

Was tun nach einem Cyberangriff?

Betroffene Systeme vom Netz trennen, aber nicht ausschalten und nichts löschen – sonst gehen Spuren verloren, die später für Gutachten, Versicherung und Ermittler zählen. Dann Fachleute dazuholen, die den Angriff rekonstruieren, bevor irgendetwas wiederhergestellt wird.

Das BSI empfiehlt Unternehmen, einen Vorfall zu melden und Anzeige bei der Polizei zu erstatten; bei personenbezogenen Daten kommt die Meldung an die Datenschutzaufsicht hinzu, nach Art. 33 DSGVO grundsätzlich binnen 72 Stunden. Die Cyberversicherung will früh informiert werden.

Wie ein Sofort-Einsatz in den ersten Stunden abläuft, zeigt unsere Fallstudie zum Wiederanlauf nach Ransomware in acht Stunden. Dieser Fall hier beschreibt die ganze Strecke danach.

Warum wir verschlüsselte Festplatten aufbewahren

Verschlüsselte Datenträger wirken wertlos. Sie sind es nicht. Die Initiative No More Ransom – getragen von der niederländischen Polizei, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität bei Europol und IT-Sicherheitsunternehmen – stellt Entschlüsselungswerkzeuge kostenlos bereit, wenn Schlüssel einer Ransomware-Familie bekannt werden. Das Verzeichnis wächst.

Nicht jede Ransomware lässt sich entschlüsseln, und niemand kann sagen, ob und wann es für eine bestimmte Variante ein Werkzeug gibt. Wer die Platten aufbewahrt, behält diese Möglichkeit – und hat das Beweismittel, falls es zu Ermittlungen kommt.

Ergebnis: Aus dem Notfall wurde eine dauerhafte Zusammenarbeit

Aus einer Anlage ohne Wartung ist eine dokumentierte, überwachte Infrastruktur mit Reserven für Wachstum geworden.

Der Angriffsverlauf ist aufgeklärt und im Gutachten festgehalten, die Buchhaltungsdaten sind technisch rekonstruiert.

Die Standorte arbeiten stabil vernetzt, die Produktion ist mit WLAN, Sensorik und Alarmierung abgesichert, und die Datensicherung wird regelmäßig zur Probe wiederhergestellt.

Die Zusammenarbeit besteht bis heute.

Was andere daraus lernen können

- **Rekonstruieren kostet mehr als vorsorgen** Teuer wird ein Angriff, wenn sich die Sicherung nicht zurückspielen lässt. Was die Verfahrensdokumentation zu Datensicherung und Wiederherstellung verlangt.
- **Wiederherstellbarkeit nachweisen** Eine Sicherung zählt erst, wenn die Wiederherstellung geprobt und protokolliert ist.
- **Fehlende Wartung ist kein Sparposten** Was ein Ausfall pro Stunde wirklich kostet – zum Nachrechnen.
- **Den IT-Partner wechseln, bevor etwas passiert** Wie eine Übernahme vom bisherigen Dienstleister abläuft, auch über Nacht.
- **Erste Schritte im Ernstfall** Was in welcher Reihenfolge geschieht, wenn es passiert ist.

Für IT-Verantwortliche: die Architektur im Überblick

- Glasfaser zwischen Verwaltung und Hallen (längste Strecke rund 120 m), ein Haupt- und drei Unterverteiler.
- Core-Switch 25 Gbit/s, Uplinks zwischen den Switches 10 Gbit/s, Videospeicher mit 10 Gbit/s angebunden.
- Verwaltung: S/FTP-Installationskabel Kategorie 7A in Brüstungskanälen; datenintensive Arbeitsplätze per Glasfaser.
- Verwaltete PoE-Switches mit zentralem Management; sechs getrennte Netzbereiche.
- Securepoint-Firewall, verschlüsselte Standortverbindungen, ein Standort über Satelliten-Internet angebunden.
- G DATA MXDR, Mehrfaktor-Anmeldung, getrennte Administratorkonten, Patch-Management, Monitoring mit Alarmierung.
- Serverraum: geschlossener Schrank, Potenzialausgleich (Elektrofachbetrieb), ableitfähiger Boden, Ersatzklimatisierung, USV.
- Dokumentation: Netzplan, Patchpläne, Kabelbeschriftung, Notfallhandbuch.
- Datensicherung in fünf Stufen, Wiederherstellungstest alle zwei Monate.
- Bewusst nicht genannt: Adressbereiche, Netzkennungen, Gerätemodelle, Firmwarestände und Standorte einzelner Geräte.

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-forensik-neuaufbau

Ihr Ansprechpartner: **Metehan Kurt**, Geschäftsführer

0621 877 55 990 · post@davinci-rechenzentrum.de