G DATA advanced analytics

Case Study

Incident Response bei der Westfalen Gruppe: G DATA hilft beim Wiederanlauf der IT und gibt Hinweise zu sicherem Betrieb

Herausforderung

- Wiederaufbau der IT nach einer Ransomware-Attacke
- Wirksame IT-Sicherheitsmaßnahmen identifizieren und umsetzen

Lösung

- Incident Response
- Regelmäßige Penetration Tests

Vorteile

- Klare Kommunikation und Vorgaben zur Bewältigung des IT-Notfalls
- Reibungsloser Wiederaufbau und Rückkehr zum Normalbetrieb
- Penetration Tests sorgen für höheres IT-Sicherheitsniveau, indem Schwachstellen in Systemen und Fehler bei Konfigurationen vermieden werden

Westfalen

Branche:
Industrial Gases & Services, Energy Solutions und Mobility

Umfang:
2.000 Mitarbeitende

Standort:
Deutschland und Europa

Nach einer Ransomware-Attacke war die Westfalen Gruppe aus Münster gezwungen, Teile ihrer IT-Infrastruktur neu aufzubauen. Den IT-Notfall nutzte das Unternehmen als Chance für einen Neuanfang und baute die IT-Landschaft noch sicherer wieder auf. Bei der Rückkehr zur Normalität setzte die Westfalen Gruppe auf die fachliche Expertise von G DATA Advanced Analytics.

Der 21. Januar 2021 nimmt in der hundertjährigen Geschichte der Westfalen Gruppe einen im negativen Sinne besonderen Platz ein. Denn an diesem Tag offenbarte sich den Verantwortlichen, dass sie Opfer einer Cyberattacke waren. Den Anfang machten mehrere Server im lokalen Rechenzentrum in der Unternehmenszentrale in Münster, die nicht mehr erreichbar waren. Eine erste Prüfung förderte eine Erpressernachricht zutage: „Sie wurden verschlüsselt. Treten Sie mit uns in Kontakt. Gegen Zahlung einer Lösegeldsumme geben wir Ihre Systeme wieder frei."

„IT ist natürlich auch in unserem Unternehmen ein zentrales Element des Geschäfts und maßgeblich für sehr viele Prozesse", sagt Andreas Eckey, Information Security Officer bei der Westfalen Gruppe. „Der Angriff hatte damals massive Auswirkungen auf die gesamte Organisation." Schnell zeigte sich, dass das interne Rechenzentrum inklusive der Back-up-Landschaft ausgefallen war. Die virtuellen Maschinen der Daten- und Anwendungsserver waren verschlüsselt und zahlreiche Dienste wie Drucken, Scannen oder WLAN nicht mehr nutzbar. Nicht betroffen waren die SAP-Systeme mit den Geschäftsdaten, die bei einem externen Partner gehostet werden, sowie weitere Cloud-Anwendungen wie beispielsweise MS Office-Dienste. Glücklicherweise blieb das KRITIS-relevante Tankstellen-Netz ebenfalls unberührt. Dieses führt die Westfalen Gruppe in einem separierten Netz mit besonderen IT-Sicherheitsmaßnahmen.

Als Familienunternehmen mit 100-jähriger Geschichte ist die Westfalen Gruppe europaweit an zahlreichen Standorten vertreten. Zu den Geschäftsfeldern zählen Industrial Gases & Services, Energy Solutions und Mobility.

„Die Zusammenarbeit war hervorragend. Gerade die klare Kommunikation und das schlüssige Maßnahmen-Konzept haben für eine Grundstruktur in der stressigen Situation gesorgt.“

Andreas Eckey, Information Security Officer Westfalen AG

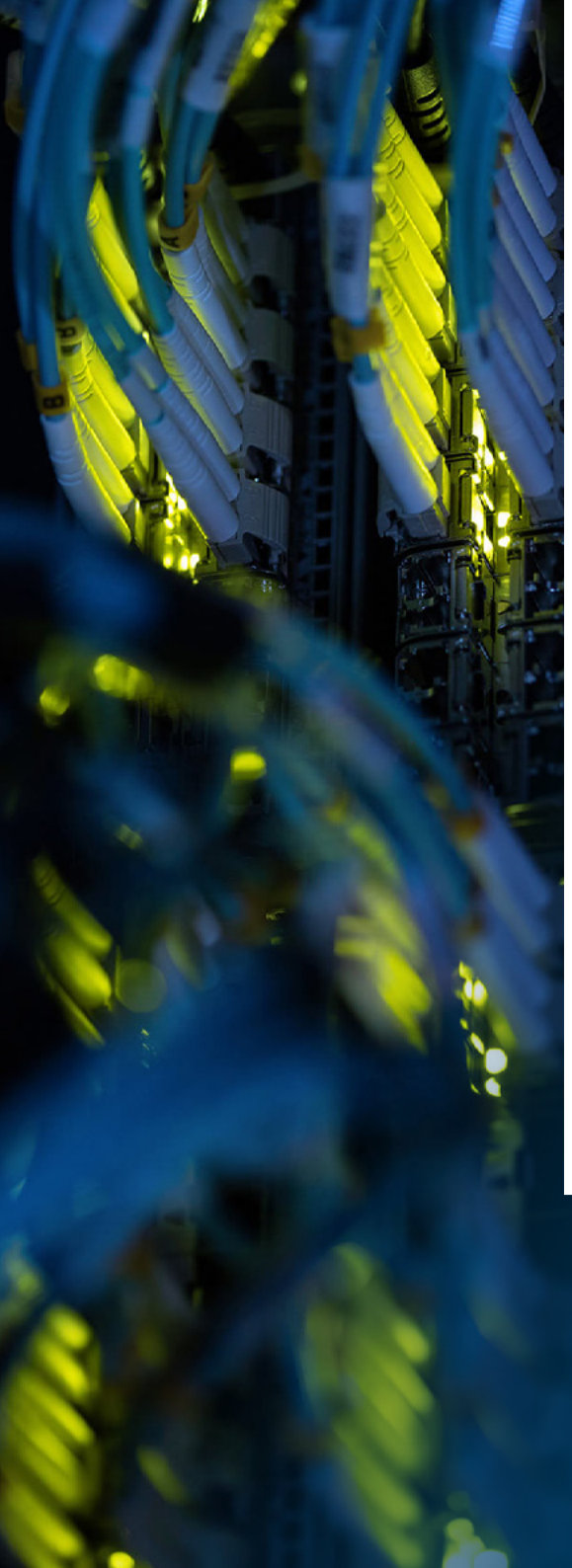
Nicht verhandeln, sondern neu aufbauen!

Umgehend trennten die Verantwortlichen die betroffenen Systeme vom Netz, um weiteren Fremdzugriff zu unterbinden. Im ersten Schritt wurde die Lage ausgewertet und das Unternehmen leitete erste Maßnahmen in die Wege. So konstituierte sich neben einer IT-Taskforce auch ein Krisenteam, in das alle Geschäftsbereiche des Unternehmens einbezogen waren. Zu diesem Zeitpunkt informierte das Unternehmen auch das Landeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Als Folge des Angriffs sah sich die Westfalen Gruppe auch gezwungen, üblicherweise ferngesteuerte Anlagen manuell zu besetzen und im Schichtbetrieb zu arbeiten. Bei der Bewältigung der Cyberattacke priorisierte die IT-Taskforce die Aufgaben unter der Prämisse „Was müssen wir wieder herstellen, um unser Geschäft in allen Bereichen sicherzustellen?“. Aber auch Themen wie die Gehaltszahlung an die eigenen Mitarbeitenden hatte eine hohe Priorität.

Um die Lage wieder unter Kontrolle zu bekommen, entschieden die Beteiligten sich, externe Fachleute hinzuzuziehen. Bei der Wahl eines geeigneten Partners folgte die Westfalen Gruppe dem Rat der Ermittlungsbehörden, ein Unternehmen zu beauftragen, das vom BSI als APT-Response-Dienstleister zertifiziert ist. „Wir haben uns für die Zusammenarbeit mit G DATA Advanced Analytics entschieden, weil G DATA in der IT-Branche schon ein bekannter Player ist“, begründet Andreas Eckey die Entscheidung. „Die Zusammenarbeit war hervorragend. Gerade die klare Kommunikation und das schlüssige Maßnahmen-Konzept haben für eine Grundstruktur in der stressigen Situation gesorgt.“

Der Auftrag an G DATA war klar – angefordert wurden: eine forensische Analyse des Angreifervorgehens, Maßnahmen für einen sicheren Notbetrieb der IT-Landschaft und ein Konzept für einen gefahrlosen Wechsel vom Notbetrieb zum Normalbetrieb.

Durch die Vollverschlüsselung der virtuellen Maschinen (VMs) und das Löschen von Logdaten zur Verschleierung der Angreifenden waren so gut wie keine Spuren auswertbar, was die forensische Aufklärung des Vorfalls massiv beeinträchtigte. Erkennbar war, dass die Cyberkriminellen ein Tool für Penetration Tests (Cobalt Strike) missbraucht hatten, um an hochprivilegierte Administrationsrechte zu kommen und damit die Kontrolle über die Systeme zu gewinnen. Da verschlüsselte Systeme ohne den passenden digitalen Schlüssel nicht entschlüsselt werden können, fokussierten sich die Fachleute auf den Wiederaufbau der Infrastruktur. Die verlorenen Daten konnte das Unternehmen dabei größtenteils aus alten Offline-Back-ups wiederherstellen, denn die aktuellen Back-ups waren ebenfalls verschlüsselt. „Nach der ersten Bestandsaufnahme konnten wir die Datenverluste auswerten und damit auch das Geschäftsrisiko einschätzen“, sagt Andreas Eckey. „Auf dieser Grundlage haben wir gemeinsam mit Vorständen und der Inhaber-Familie entschieden, kein Lösegeld zu zahlen, sondern die betroffene Infrastruktur neu aufzusetzen. Wir wollten das Geld sinnvoll nutzen und haben direkt lang geplante IT-Projekte vorgezogen, zum Beispiel um Altsysteme abzulösen.“



Rückkehr zur Normalität

Rund acht Wochen dauerte der Ausnahmezustand bei der Westfalen Gruppe. In dieser Zeit hatten die Mitarbeitenden des IT-Teams Prozesse etabliert und Systeme stabilisiert, sodass die Kundenversorgung sichergestellt war. Ein wesentlicher Erfolgsfaktor dabei war die Umsetzung eines Zwei-Phasen-Konzeptes mit einem sogenannten „gelben“ und „grünen“ Netz: Das „gelbe“ Netz ermöglichte rudimentäre Arbeiten am Rechner ohne Zugriffsmöglichkeiten auf die Server-Infrastruktur. So konnten die zuvor kurzfristig eingerichteten analogen Notprozesse wenigstens wieder digital stattfinden. Beim Wechsel zum „grünen“, sicheren Netz unterstützte G DATA Advanced Analytics mit ihrer Expertise. Ins „grüne“ Netz durften nur Systeme integriert werden, die neu aufgesetzt wurden und bei denen eine Kompromittierung ausgeschlossen wurde, um eine Re-Infektion zu verhindern. Zusätzlich sind hier noch stärkere Sicherheitsmaßnahmen umgesetzt worden, die das Sicherheitsniveau des neuen Infrastrukturbereichs deutlich erhöht haben. Bei der Bereitstellung sicherer LAN-Strukturen und der Wiederherstellung der Schnittstellen zwischen den Systemen mussten in der Firewall explizite Verbindungen eingerichtet werden. Das war Teil der optimierten Netzwerksegmentierung, um die Angriffsfläche zu verkleinern. Dabei gab es beispielsweise bei den Online-Shops besondere Herausforderungen. Hier setzte die Westfalen Gruppe ein Konzept um, mit der die Firewall sicherstellt, dass ausschließlich gültige Befehle über Webbrowser übergeben werden. Zusätzlich zu den neuen Sicherheitsmaßnahmen wurden die Systeme weiter gehärtet. Auch der Einsatz von USB-Sticks war fortan nicht mehr möglich. Diese Maßnahme stieß auf allen Ebenen auf Verständnis, auch, wenn das die komfortable Benutzbarkeit der Systeme einschränkte. „Mit einschneidenden Erfahrungen des IT-Notfalls war letztlich allen klar, dass niemand mehr mit Papier und Bleistift arbeiten will“, sagt Andreas Eckey.

IT-Sicherheit auf dem Prüfstand

Mit der Rückkehr zur Normalität und dem Ausrollen neuer zukunftsfähiger IT-Lösungen rückten die IT-Verantwortlichen eine zentrale Frage in den Mittelpunkt: „Ist unsere IT wirklich sicher?“. Daher entschied sich die Westfalen Gruppe, ihre Infrastruktur regelmäßig auf Schwachstellen zu überprüfen. Dafür setzten Sie auf die Durchführung von Penetration Tests und weiterhin auf die Expertise von G DATA. „Wir wollen Fehler in der IT-Sicherheit etwa in der Konfiguration der Systeme und Anwendungen frühzeitig erkennen, um direkt gegenzusteuern“, sagt Andreas Eckey. „Weil ständig Updates und Patches notwendig sind, wollen wir bei der IT-Sicherheit nicht mehr hinterherrennen, sondern konsequent vor der Lage bleiben.“ So offenbaren die Tests immer wieder Stellen, wo die IT-Verantwortlichen nachschärfen können – etwa bei der stetigen Absicherung der Passwörter in allen Bereichen oder bei der schnellen Bereitstellung von neuen Software-Updates.

Neugierig, wie auch Sie Ihr IT-Sicherheitsniveau mit G DATA Advanced Analytics weiter erhöhen können? **Hier erfahren Sie mehr:**

www.gdata.de **info@gdata-adan.de** **0234 / 9762-820**

G DATA
advanced analytics