G DATA advanced analytics

Case Study

IT-Notfall beim Autohaus Kruft: G DATA stellt IT-Sicherheit auf die Probe und sorgt für **verbessertes Schutzniveau**

Herausforderung

- Bewertung der IT-Infrastruktur hinsichtlich der vorhandenen Abwehr- und Sicherungsmaßnahmen
- Identifizierung von Verbesserungsmaßnahmen und Handlungsempfehlungen zur Erhöhung des Sicherheitsniveaus

Lösung

- Incident Response von G DATA Advanced Analytics
- Adversary-based IT-Security Assessment von G DATA Advanced Analytics

Vorteile

- Professionelle Bewertung des aktuellen IT-Sicherheitslevels
- Zusammenarbeit mit ausgewiesenen IT-Sicherheitsfachleuten

Kruft

Branche:
BMW-Vertragshändler

Umfang:
Mehr als 50 Mitarbeitende

Standort:
Oberhausen, Deutschland

Nach einer Cyberattacke entschied sich das Autohaus Kruft aus Oberhausen, die gesamte IT-Infrastruktur neu aufzusetzen. Im Zuge der Neugestaltung des Netzwerks wollte der BMW-Vertragshändler das Niveau der IT-Sicherheit deutlich erhöhen und sich von historisch gewachsenen Altlasten befreien. Dabei setzte das Autohaus auf externe Unterstützung von G DATA und nutzte nach dem Neuaufbau auch das Beratungsangebot.

Auch mit gut eingerichteten technologischen Schutzmaßnahmen gibt es keine hundertprozentige Absicherung vor Cyberattacken. Dabei machen sich Cyberkriminelle immer wieder Schwachstellen in Anwendungen und Systemen zunutze, um in IT-Infrastruktur einzudringen. Anfang 2021 nutzten Angreifergruppen massiv **Zero-Day-Sicherheitslücken in Exchange-Servern** aus, also dem Hersteller bis zu diesem Zeitpunkt völlig unbekannte Sicherheitslücken. Von dieser Schwachstelle waren zum damaligen Zeitpunkt zehntausende Unternehmen betroffen. Zu den Opfern gehörte auch das Autohaus Kruft. Trotz der bestehenden Schutzmaßnahmen erhielten Cyberkriminelle Zugang zum Netzwerk und haben unter Ausnutzung mehrerer Schwachstellen die IT-Systeme mit Schadcode kompromittiert. Nach dem Wiederanlauf beschloss das Unternehmen, dass sich ein derartiger Vorfall nicht wiederholen sollte. Schnell entschieden sich die Verantwortlichen die IT-Infrastruktur neu aufzubauen. Der Autohändler beauftragte im Anschluss die IT-Sicherheitsfachleute von G DATA Advanced Analytics mit einem Wirksamkeitstest für die IT-Sicherheit.

Schnell handeln und Schaden eingrenzen

Kaum hatte der IT-Dienstleister aus dem Münsterland, der das Autohaus seit Jahren betreut, das Ausmaß des IT-Notfalls erkannt, handelte das Unternehmen sofort. Das Autohaus entschied sich, zunächst alle Rechner vom Netz zu trennen und professionelle Unterstützung zur Bewältigung des Falls hinzuzuziehen. Besonders erfreulich war, dass der zentrale Server nicht von der Cyberattacke

„Dank der Expertise der G DATA Advanced Analytics GmbH konnten wir die Sicherheit unserer IT stark verbessern. Dass ein solch komplettes Leistungsspektrum von der G DATA angeboten wird, ist schon besonders, gerade im Vergleich zu anderen IT-Dienstleistern.“

Philipp Sporckmann, Marketingverantwortlicher Autohaus Kruft

betroffen war, wodurch keine Kundendaten in die Hände der Angreifer gelangen konnten. Außerdem konnte dadurch der Wiederanlauf der Systeme signifikant beschleunigt werden. Gleichzeitig informierten die Verantwortlichen das Landeskriminalamt und auch die Zentrale von BMW über den Vorfall.

Arbeiten ohne IT

Für die mehr als 50 Mitarbeitenden bedeutete die Cyberattacke einen massiven Einschnitt in den Arbeitsalltag. Aber aufgrund des frühzeitigen Erkennens und des schnellen Handelns konnte ein vollständiger Stillstand des Autohauses verhindert werden. „Im gesamten Unternehmen sind Prozesse vollständig digitalisiert, beim Fahrzeugverkauf genauso wie bei unseren Serviceangeboten oder in der Werkstatt“, beschreibt Philipp Sporckmann, Marketingverantwortlicher beim Autohaus Kruft, die Situation. „Viele vertraute und eingespielte Prozesse konnten wir in den folgenden Wochen nur analog, also mit Papier und Stift, erledigen. Später konnten wir eingeschränkt auch cloudbasierte Anwendungen wieder nutzen.“

Fachleute für IT-Notfälle

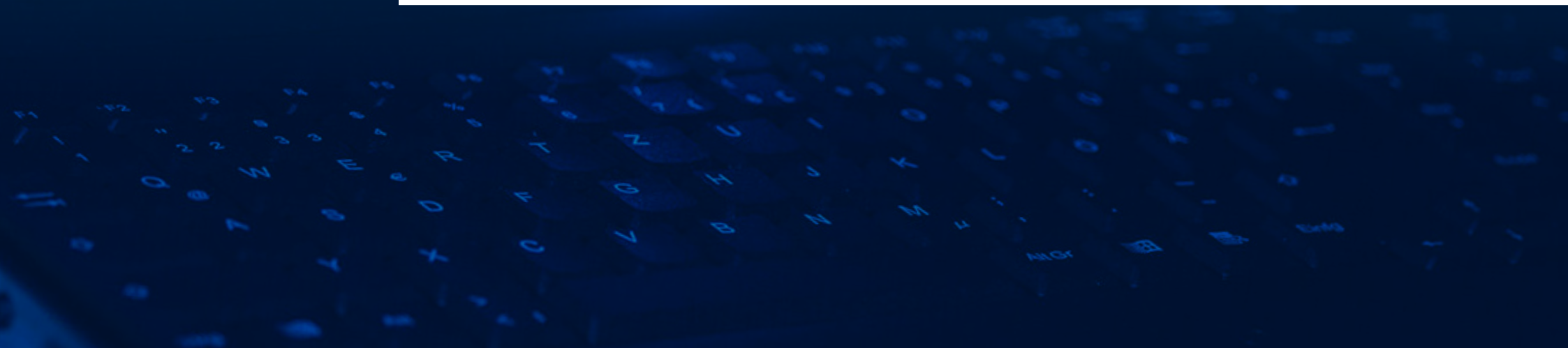
Intern nahm ein dreiköpfiges Notfall-Team, aus IT-affinen Mitarbeitenden, die Arbeit auf, die IT des Autohauses wieder in einen produktiven Zustand zu bringen. Unterstützt wurde das Notfall-Team durch die Fachleute von G DATA Advanced Analytics. Bei der Entscheidung zugunsten des Bochumer Unternehmens zog das Autohaus die Liste der vom BSI zertifizierten APT-Response-Dienstleister zurate und wählte einen regional ansässigen Partner. Denn in Deutschland gibt es nur wenige Unternehmen mit einer derartigen Expertise. „Einerseits ist G DATA Advanced Analytics ein vertrauter Name und ein anerkanntes Unternehmen im Ruhrgebiet, andererseits passt die Zusammenarbeit auch zu unserer Strategie, mit regionalen Partnern zusammenzuarbeiten,“ begründet Philipp Sporckmann die Wahl.

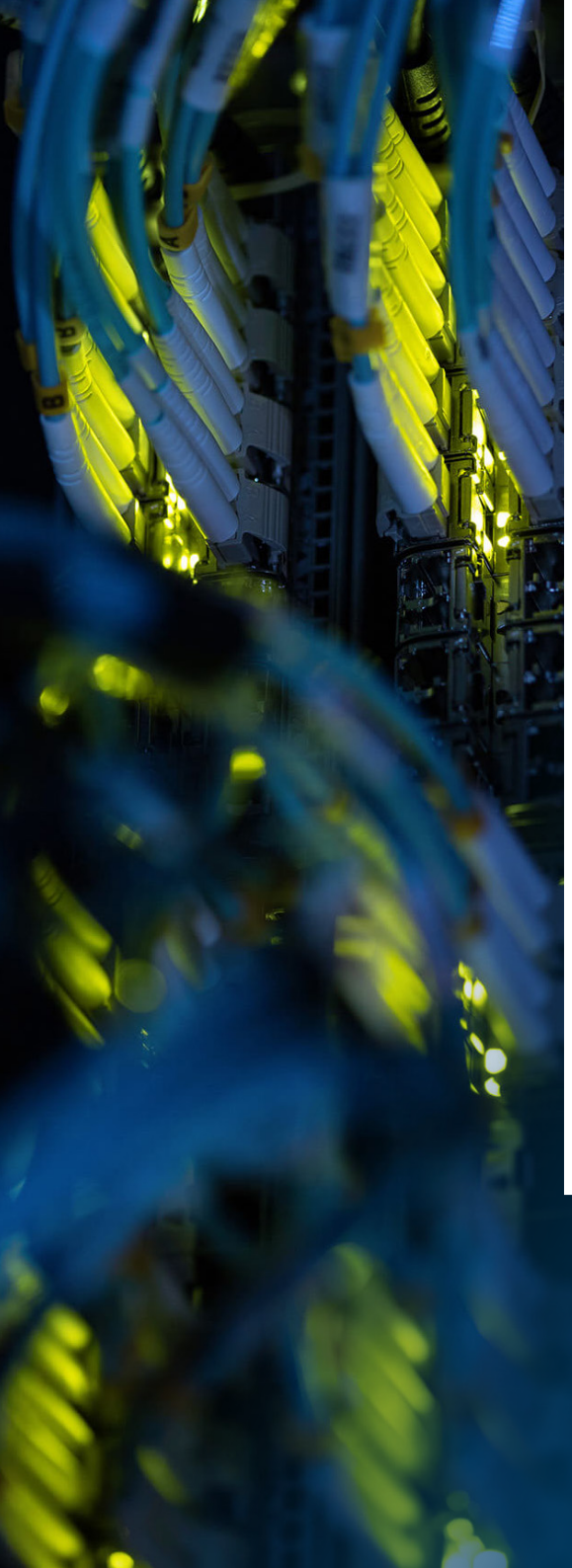
Im Rahmen des Incident-Response-Einsatzes untersuchten Fachleute von G DATA Advanced Analytics die Systeme des Autohauses forensisch, um einklares Bild des Angriffs zu erhalten, damit zugeschnittene Sofortmaßnahmen erfolgen konnten, die auch eine Re-Infektion der bereinigten Systeme verhinderten. Zusätzlich zum Wiederaufbau der IT-Infrastruktur traf die Geschäftsführung weitere Entscheidungen: Alte PCs wurden durch neue Geräte ersetzt und der bereits geplante Umzug der gesamten IT in ein externes Rechenzentrum, in kürzester Zeit vollzogen. Unterstützung erhielt der BMW-Vertragshändler dabei von seinem IT-Dienstleister aus dem Münsterland.

Nicht nur neu, sondern sicherer

Obwohl das Unternehmen grundsätzlich schnell wieder arbeitsfähig war, dauerte es insgesamt mehrere Monate, bis die Auswirkungen des Vorfalls auf das Tagesgeschäft nicht mehr spürbar waren. Hinzu kam, dass die Geschäftsführung in Abstimmung mit dem IT-Verantwortlichen weitere Maßnahmen realisiert hatte, um das Sicherheitsniveau deutlich zu verbessern.

Dazu zählte unter anderem eine neue Richtlinie für Passwörter sowie das automatische





Sperren der Arbeitsplatzrechner nach einer definierten Zeit. Auch auf technischer Ebene setzte die IT-Abteilung Maßnahmen um und führte eine striktere Segmentierung des Netzwerks ein. Zusätzlich wurde das Berechtigungsmanagement neu konzipiert. Weiterhin definierte die IT Kategorie-Filter und eine Allow-List für das Surfen im Internet, um den Besuch von Webseiten zu unterbinden, die Schadsoftware enthalten oder Login-Informationen von Anwenderinnen und Anwendern abgreifen.

Wirksamkeitstest: Sind wir wirklich sicher?

Nach dem Wiederanlauf der IT und dem Umsetzen der neuen IT-Sicherheitsmaßnahmen war für das Autohaus Kruft die Reise aber noch nicht beendet. Getrieben von der Frage „Wie gut ist unser Schutzniveau?“, beauftragte das Autohaus G DATA Advanced Analytics mit einem Adversary-based IT-Security Assessment. Das Ziel: Eine Bewertung der IT-Infrastruktur hinsichtlich ihrer vorhandenen Abwehr- und Sicherungsmaßnahmen. Dabei sollten die Fachleute nicht nur die organisatorischen Prozesse und Strukturen bewerten, Sicherheitskonzepte prüfen und Verbesserungsmaßnahmen identifizieren, sondern die ausformulierten Aussagen technisch verifizieren. Weiterhin sollten sie Handlungsempfehlungen aussprechen, um das Sicherheitsniveau zu erhöhen. Bei diesem Wirksamkeitstest überprüfte das spezialisierte Team stichprobenartig den Status Quo der IT-Sicherheit und glich diesen mit dem technischen Konzept ab. Zusätzlich erfolgte eine technische Verifizierung der umgesetzten Sicherheitsmaßnahmen in Abhängigkeit ihrer Kritikalität. Bei dieser Herangehensweise lassen sich zusätzlich zu organisatorischen Schwächen wie etwa Fehler im Installationsprozess oder Probleme in der Konfiguration von Sicherheitskomponenten aufspüren.

Während des gesamten Beratungsprozesses haben die Verantwortlichen unter anderem anhand der identifizierten Schwachstellen Hinweise zu weiteren potenziellen Angriffsszenarien und Handlungsempfehlungen zur Mitigierung der verifizierten Schwachstellen erhalten. Dank dieses IT-Security Assessments konnte das Autohaus Kruft seine IT-Infrastruktur erheblich härten und die gesamte IT-Sicherheit auf ein neues Niveau heben.

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

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

G DATA
advanced analytics