G DATA CyberDefense

Case Study

Thalia stärkt seine Cyberabwehr: Warum MXDR für IT-Verantwortliche unverzichtbar ist

Thalia

Branche:
Omnichannel-Buchhändler im deutschsprachigen Raum

Umfang:
6.500 Mitarbeitende in rund 380 Buchhandlungen in der DACH Region

Standort:
Hagen, Deutschland

Herausforderung

- Rund-um-die-Uhr-Überwachung der gesamten IT
- Managed Security Service
- Schlanker Prozess zur Verteilung von Updates

Lösung

- G DATA 365 | MXDR (Managed Extended Detection and Response)

Vorteile

- 24/7-Überwachung an 365 Tagen im Jahr der IT-Systeme
- Sofortige Reaktion bei Störfällen
- Ressourcenschonende Verteilung von Updates

Eine hohe Verfügbarkeit der IT ist nicht nur im Onlinegeschäft eine zentrale Voraussetzung für wirtschaftlichen Erfolg. Auch im klassischen Buchhandel setzt Thalia auf eine hochverfügbare IT für Bestellungen. Um das gesamte Netzwerk vor Cyberattacken oder anderen Ausfällen zu schützen, nutzt das Familienunternehmen Managed Extended Security Services von G DATA CyberDefense: G DATA 365 | MXDR.

Die Thalia Bücher GmbH ist der marktführende Buchhändler im deutschsprachigen Raum. Rund 6.500 Mitarbeiterinnen und Mitarbeiter arbeiten an den zentralen Standorten in Hagen, Münster, Berlin, Aachen und Linz sowie in den rund 380 Buchhandlungen. Durch einen Onlineshop und die eigene App ist Thalia zudem digital stark vertreten. Mit seiner Omni-Channel-Strategie ermöglicht das Unternehmen Kundinnen und Kunden den Einkauf zu jeder Zeit über alle Kanäle hinweg. Für die enge Verzahnung von klassischem Buchhandel und Digitalgeschäft hat Thalia eine umfangreiche IT-Infrastruktur etabliert. Das digitale Herz dieser Infrastruktur schlägt in einem hybriden Rechenzentrum und Cloud Umgebung. Jede Bestellung im Onlineshop oder in einer Buchhandlung sowie die Anbindung der Kassensysteme laufen hier zusammen. Die hochverfügbare digitale Umgebung ist ein maßgeblicher Erfolgsfaktor für Thalia.

„Für Thalia steht die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen an erster Stelle“, sagt Moundji Merabet, Senior Manager Retail IT bei Thalia, der für die IT in den Buchhandlungen verantwortlich ist. „Wir müssen sicherstellen, dass unsere Systeme rund um die Uhr verfügbar sind. Insbesondere die Daten unserer Kundinnen und Kunden.“ Den Verantwortlichen ist bewusst, dass eine Unterbrechung oder ein Ausfall der IT-Infrastruktur weitreichende Folgen für Unternehmen haben kann – von finanziellen Einbußen bis hin zum Verlust von Kunden und dem Ruf des Unternehmens. Mit dem konstanten Unternehmenswachstum der letzten Jahre registriert der Omnichannel-Buchhändler auch eine Zunahme der Angriffsversuche.

Managed Security für mehr IT-Sicherheit

Schnell erkannten die Verantwortlichen, dass eine reine technologische Aufstockung nicht zum gewünschten Ziel führt. So waren die Anforderungen an eine neue Lösung schnell gefunden: Es brauchte einen Managed-Security-Service mit einem Security Team, dass an sieben Tage in der Woche

„Wir können uns auf wesentliche IT-Aufgaben konzentrieren und wissen, dass ein versierter Partner für die IT-Sicherheit sorgt.“

Moundji Merabet
Senior Manager Retail IT | Thalia Bücher GmbH

rund um die Uhr die Systeme von Thalia überwacht. Um bei Verdachtsfällen direkt und schnell reagieren zu können. „Wir orientieren uns sehr stark am BSI-Grundschutz und der ISO 27001, um den Schutz unserer Daten und Prozesse zu gewährleisten. „Um unsere IT jedoch dauerhaft abzusichern, haben wir entschieden, mit einem erfahrenen IT-Security-Unternehmen zusammenzuarbeiten, das auch entsprechende Ressourcen für uns vorhält“, sagt Moundji Merabet. Gerade kleinere und unauffällige Anomalien im Netzwerk infolge unterschiedlichster Angriffe lassen sich von Fachleuten besser und schneller aufdecken. Aber auch Social-Engineering-Versuche oder Ransomware-Attacken erkennen Security Analystinnen und Analysten frühzeitig. Erster Ansprechpartner war die G DATA CyberDefense AG, deren Sicherheitslösung Thalia bereits seit mehr als 20 Jahren einsetzt. „Wir haben ein jahrelanges und vertrauensvolles Verhältnis zu G DATA. Daher war es naheliegend, zunächst bei unserem Partner nachzufragen, ob er eine Lösung anbieten kann“, erklärt Moundji Merabet. „Außerdem waren unsere Ansprechpersonen mit unseren Anforderungen und auch mit den Besonderheiten des Netzwerkes vertraut.“ Tatsächlich traf G DATA mit seinem Managed-Extended-Detection-and Response-Angebot G DATA 365 | MXDR genau die Vorgaben von Thalia, sodass sich die Verantwortlichen entschieden, die Zusammenarbeit fortzusetzen und auszubauen.

Schlanker Update-Prozess

Da der Omnichannel-Buchhändler in der Frozen-Zone zwischen November und Januar nur geringe Änderungen vornimmt, um die Verfügbarkeit und Performance der Systeme im Weihnachtsgeschäft sicherzustellen, konnten G DATA und Thalia sich auf die Projektplanung konzentrieren und den Roll-out der neuen Agents planen. Im Mittelpunkt stand dabei eine zentrale Vorgabe: Da sämtliche Kommunikation im Netz und zu den Läden über gesicherte Verbindungen laufen, brauchte es eine ressourcenschonende Verteilung der Updates für MXDR, die auf jedem der insgesamt 6.000 Rechner installiert sind. Im Normalfall lädt jeder einzelne Agent die Updates für die Anwendung, die Signaturen oder die Regeln der Schutzkomponenten direkt von G DATA Servern herunter. Konkret bestand die Herausforderung darin, die Updates zu verteilen, ohne den Web-Traffic der Buchhandlungen oder des Onlineshops zu beeinträchtigen. Hier konnte G DATA einen bereits bestehenden Caching-Prozess von Thalia zur Verteilung von Updates nutzen, für den dedizierte Server bereitgestellt wurden. So muss jedes Update nur einmal ins Rechenzentrum von Thalia hochgeladen werden. G DATA hat die alternative

G DATA 365 | MXDR

IT SECURITY IST TEAMPLAY

Datenquelle in den Agents entsprechend hinterlegt. Sämtliche Agents fragen die festgelegte interne Downloadquelle an, die den größten Anteil der Anfragen aus dem Cache beantworten kann. Nur wenn eine Datei noch nicht im Cache liegt, ist Download-Kommunikation mit den G DATA Servern im Internet notwendig. Basis für diese Lösung ist die Open Source Software HA-Proxy. „G DATA hat unseren Wunsch sofort umgesetzt“, sagt Moundji Merabet. „Es ist vorteilhaft, dass G DATA eine Lösung zur Updateverteilung mit uns entwickelt hat, die in unseren bereits etablierten Patching Prozessen integriert ist.“

Roll-out mit integriertem Check-up

Unmittelbar nach der Frozen Zone begann der Roll-out von MXDR auf mehr als 6.000 Clients. Das Implementieren der Software gelang ohne größere Probleme. Ein wesentlicher Grund dafür: ein praxisbewährter Implementierungsprozess von G DATA. Dabei stellt der Cyber-Defense-Spezialist Kunden ein Skript zur Verfügung, welches die Kompatibilität der Systeme mit dem XDR-Agent überprüft. Das Tool prüft automatisiert, ob der Rechner einen festgelegten Patch-Status hat. Auf diesem Weg konnten alle Systeme mit alten Windows-Patch-Ständen identifiziert werden.

Direkter Kontakt zum Support

Sechs Monate nach dem Roll-out fällt das Fazit von Thalia positiv aus. Die Systeme werden rund um die Uhr von G DATA mit einem Experten-Team überwacht, die bereits bei geringen Verdachtsfällen umgehend reagieren und verdächtige Systeme vom Netz trennen. Wenn die Mithilfe der Mitarbeitenden erforderlich ist, erhält Thalia klare Handlungsanweisungen, was zu tun ist. „Das Security-Team von G DATA nimmt uns sehr viel Arbeit ab“, sagt Moundji Merabet. „Wir können uns auf wesentliche IT-Aufgaben konzentrieren und wissen, dass ein versierter Partner für die IT-Sicherheit sorgt.“ Ein großer Pluspunkt dabei ist der direkte Kontakt zum Support-Team von G DATA in Bochum. Gerade in stressigen Situationen stört keine Sprachbarriere den Austausch zwischen G DATA und Thalia.

Die Lösung kommt auch in Österreich zum Einsatz, denn die IT-Verantwortlichen sind bestrebt, eine einheitliche IT-Landschaft zu betreiben. Dafür ist auch der Roll-out in der Schweiz geplant. Angesichts der guten Zusammenarbeit überrascht es nicht, dass Thalia die langjährige Zusammenarbeit fortsetzt – getreu dem Motto „Never change a winning team.“

Neugierig, wie auch Sie Ihr Unternehmen mit G DATA absichern können?
Hier erfahren Sie mehr:

gdata.de/business vertrieb@gdata.de 0234 / 9762-170

G DATA CyberDefense