

Wie die GFA GROUP mit **G DATA 365 | MXDR** ihre IT-Sicherheit auf ein neues Level hebt

Herausforderung

- Zunehmende Bedrohungslage: Wachsende Zahl an Systemen und Mitarbeitenden trifft auf immer ausgefeiltere Angriffsmethoden
- Steigende Anforderungen durch Cyber-Versicherungen und regulatorische Vorgaben
- Fehlende personelle Kapazitäten für ein eigenes 24/7 Security Operations Center (SOC)

Lösung

- G DATA 365 | MXDR als ganzheitliche, gemanagte Security-Lösung [↗](#)

Vorteile

- 24/7-Security-Monitoring durch Fachleute
- Nahtlose Integration, hohe Systemstabilität und keine False Positives
- Zukunftssicherheit hinsichtlich Compliance und Bedrohungslage



Branche:

Internationale
Entwicklungszusammenarbeit



Umfang:

700 Clients



Standort:

Hamburg, Deutschland

GFA SysCom sorgt als IT-Rückgrat der GFA GROUP für stabile digitale Strukturen für sich selbst und die Unternehmen der Unternehmensgruppe. Um sich wirksam gegen Cybergefahren abzusichern, hat sich das Team für die Managed-Extended-Detection-and-Response-Lösung von G DATA CyberDefense entschieden. Eine Lösung, die unsichtbar, aber hochwirksam im Hintergrund arbeitet.

Mit ihren rund 1.800 festen und freien Mitarbeitenden weltweit realisiert die GFA GROUP Projekte der Entwicklungszusammenarbeit um die Lebens-

bedingungen in den Empfängerländern nachhaltig zu verbessern. Die Expertise der Unternehmen erstreckt sich über ein weites Spektrum und reicht von Beratung zu Landwirtschaft und Ressourcenschutz, Gesundheit, Privatsektorentwicklung, Wasserversorgung und öffentliche Verwaltung, bis hin zu Zertifizierungen. Für den reibungslosen IT-Betrieb sorgt der interne IT-Dienstleister, die GFA SysCom. Das Unternehmen stellt für die Projekte moderne und sichere IT-Werkzeuge auf dem aktuellen Stand der Technik zur Verfügung. Dabei kümmert sich das Team um alle technischen Belange, die in diesem Zusammenhang auftreten: vom Betrieb der IT-Infrastruktur bis zur Entwicklung der individuellen Anwendungen.

„Auch die Zusammenarbeit zwischen G DATA und unserem Administratoren-Team hat hervorragend geklappt. Der Angriff wurde binnen Sekunden abgewehrt und die Systeme noch am selben Tag bereinigt und gepatcht wieder in Betrieb genommen.“

Teamleiter IT-Administration | GFA SysCom

Mehr Sicherheit? Nur als Managed-Lösung

Die Anforderungen an IT-Security haben sich massiv verändert, nicht zuletzt durch die wachsende Bedrohungslage und neue regulatorische Vorgaben wie die NIS-2-Richtlinie. Aber auch Cyber-Versicherungen machen klare Vorgaben: Sie setzen aktive Detection-Maßnahmen voraus. Für einen strategischen Wechsel sorgten auch die typischen Herausforderungen vieler mittelständischer IT-Abteilungen: begrenztes Budget, fehlende Expertise und Fachkräftemangel. Der Trend geht hin zu einer Sicherheitslösung, die nicht nur reagiert, sondern Angriffe erkennt, bevor sie Schaden anrichten – und das rund um die Uhr. Die GFA SysCom suchte deshalb ein Angebot, das nicht nur technologisch überzeugt, sondern auch operativ entlastet wie eine Managed-Extended-Detection-and-Response-Lösung, kurz MXDR.

Gesucht: Verlässlich, Managed, Made in Germany

Die Kriterien für die Marktanalyse waren klar definiert: Die Lösung sollte nicht nur die Anforderungen der Cyber-Versicherung erfüllen und die gesam-

te IT-Infrastruktur rund um die Uhr überwachen. Zusätzlich sollte sie sich auch einfach in die bestehende Infrastruktur integrieren lassen und die Vorgaben der DSGVO vollumfänglich erfüllen. Dabei präferierten die Verantwortlichen schon früh einen europäischen oder deutschen Anbieter mit einem erstklassigen Support. „Wir haben uns bewusst gegen eine technische Lösung entschieden, die wir selbst betreiben. Dafür fehlt uns im Alltag die Zeit und die personellen Ressourcen“, so der Teamleiter IT-Administration bei der GFA SysCom.

Auswahlprozess: Fundiert und zukunftsorientiert

Im Auswahlprozess standen mehrere Anbieter zur Diskussion. Am Ende überzeugte G DATA mit einem ganzheitlichen Konzept und dem bereits etablierten Vertrauensverhältnis, denn die GFA SysCom nutzte vorher die G DATA Virenschutzlösung.

„Wir haben uns also für ein Produkt-Upgrade aus Deutschland entschieden. Das hat perfekt zu unserer mittelständischen DNA gepasst“, so der IT-Leiter der GFA GROUP. G DATA punktete mit einer

klaren Kommunikation, fairer Preisgestaltung und einem spürbaren Verständnis für die Bedürfnisse mittelständischer Unternehmen.

Der Roll-out: Reibungslos

Vor dem Roll-out führten die Verantwortlichen ein Proof of Concept durch, um mögliche Stolperfallen vorab zu identifizieren. Die anschließende Installation auf allen Clients verlief in den allermeisten Fällen problemlos. Einzelne Herausforderungen – etwa bei älteren Servern oder speziellen Patch-Ständen – waren schnell identifiziert und gemeinsam mit dem G DATA Kundenservice gelöst. „Wir hatten beim Roll-out kleine Hürden, aber keine unlösbaren Probleme. Und wenn etwas war, hat der Support schnell und kompetent geholfen“, berichtet die IT-Administration.

Der Betrieb: Geräuschlos im Hintergrund

Ein Jahr nach dem Roll-out ist die Zufriedenheit hoch: Die MXDR-Lösung läuft im Hintergrund nahezu geräuschlos – ganz im Sinne einer professionellen Sicherheitslösung. Keine False Positives, kein



G DATA 365 | MXDR

IT SECURITY IST TEAMPLAY

Performance-Verlust und keine Beschwerden aus dem Kreis der Kolleginnen und Kollegen.

„No News are good News. Das ist das Beste: Wir wissen, dass jemand mit Expertise drauf schaut und müssen uns nicht selbst um jeden Alarm kümmern“, sagt der IT-Leiter. „Die wenigen Benachrichtigungen, die auftreten, sind präzise und lösungsorientiert – etwa bei Rückmeldungen, die durch den Einsatz spezieller Software oder den Besuch von Webseiten entstehen.“

Zusammenarbeit mit G DATA: Partnerschaftlich und professionell

Bereits von Beginn zeigte sich die hohe Qualität der Zusammenarbeit. Der Support von G DATA in Bochum half nicht nur bei der technischen Umsetzung, sondern passte die Lösung individuell an die Systemlandschaft der GFA GROUP an – etwa mit spezifischen Konfigurationspaketen

für Exchange-Server und andere zentrale Dienste. „Wir sind sehr froh, dass da echte Menschen mit Know-how sitzen, die mitdenken und nicht bloß ein Ticketsystem verwalten“, so der Leiter der Administration.

Der Incident: Schnelle Erkennung, wirksame Abwehr und gründliche Forensik

G DATA 365 | MXDR hat sich bereits in einem Security Incident bewährt. Im Falle des SharePoint CVE-2025-49706 / CVE-2025-49704 hat das Team von G DATA einen Angriff erkannt und die betroffenen Server sofort isoliert. „Die schnelle Erkennung und Abwehr eines Angriffes ist genau der Grund, weshalb wir uns für G DATA 365 | MXDR entschieden haben“, so der IT-Leiter, „Auch die Zusammenarbeit zwischen G DATA und unserem Administratoren-Team hat hervorragend geklappt. Der Angriff wurde binnen Sekunden abgewehrt und die Systeme noch am

selben Tag bereinigt und gepatcht wieder in Betrieb genommen. Was zu einem schwerwiegenden Problem hätte werden können, wurde so zu einer positiven Erfahrung bezüglich der Zusammenarbeit mit G DATA und dem Vertrauen in den Service von G DATA 365 | MXDR.“ Auch den Abschlussbericht von G DATA konnte der CISO so direkt für seinen Bericht verwenden.



Fazit: Sicherheit, die mitwächst


Die GFA SysCom hat mit G DATA 365 | MXDR eine Lösung gefunden, die nicht nur aktuellen Anforderungen gerecht wird, sondern auch mit zukünftigen Herausforderungen wächst. Ob NIS-2, neue Cyber-Bedrohungen oder wachsende Komplexität der IT-Infrastruktur: Die IT-Sicherheit ist so aufgestellt, dass sie mitwachsen kann – sicher, transparent und effizient.



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

 gdata.de 

 vertrieb@gdata.de 

 0234 / 9762-170

© Copyright 2025 G DATA CyberDefense AG. Alle Rechte vorbehalten. Kein Teil dieses Dokuments darf ohne vorherige schriftliche Genehmigung der G DATA CyberDefense AG Deutschland kopiert oder reproduziert werden.

Microsoft, Windows, Outlook und Exchange Server sind eingetragene Marken der Microsoft Corporation. Alle anderen Marken- oder Produktnamen sind Warenzeichen ihrer jeweiligen Eigentümer und sind daher entsprechend zu behandeln.

