

Warum das Landratsamt Breisgau-Hochschwarzwald auf **G DATA 365 | MXDR** setzt



Herausforderung

- 24/7-Überwachung der IT
- Einhaltung DSGVO und BSI-Grundschutz

Lösung

- G DATA 365 | MXDR [↗](#)

Vorteile

- 24/7-Überwachung des IT-Netzwerkes an 365 Tagen im Jahr
- Zusammenarbeit mit deutschsprachigem Support

**Branche:**

Kommunale Verwaltung für 250.000 Bürgerinnen und Bürger

**Umfang:**

1.900 Angestellte
2.300 Clients

**Standort:**

Breisgau-Hochschwarzwald,
Deutschland

Das Landratsamt Breisgau-Hochschwarzwald verwaltet in der IT sensible Bürger- sowie Sozialdaten und setzt deshalb auf höchste IT-Sicherheit. Mit Managed Extended Detection and Response (MXDR) von G DATA schützt die Behörde ihre mehr als 2.000 Clients und Server rund um die Uhr. Wie der Roll-out verlief, welche Anforderungen entscheidend waren und warum die Zusammenarbeit mit G DATA überzeugt, erfahren Sie in dieser Case Study.

Der Landkreis Breisgau-Hochschwarzwald mit rund 270.000 Einwohnerinnen und Einwohnern liegt im Südwesten Baden-Württembergs. Das Landratsamt verantwortet vielfältige Aufgaben in seiner Funktion als kommunale Kreisbehörde und untere staatliche Verwaltungsbehörde. Das Spektrum reicht von Abfallwirtschaft, Sozial- und Jugendhilfe über Straßenbau und Baurecht sowie Gesundheits- und Umweltschutz bis hin zum Schulwesen und Ausländerbehörde. Hinter all diesen Leistungen steht eine komplexe IT-Infrastruktur, die On-Premises betrieben wird: Zwei eigene Rechenzentren in Freiburg, über 2.000 Clients und zahlreiche Fachanwendungen, die den Bürgerinnen und Bürgern digitale Services ermöglichen. Insgesamt 70 Mitarbeitende kümmern sich

um alle Belange der IT, insbesondere um die Digitalisierung der Verwaltung. Aber nur fünf mit dem Fokus auf IT-Sicherheit und Compliance.

„Die IT ist für uns der Motor einer modernen Verwaltung“, sagt Manuel Seifer, IT-Administrator und verantwortlich für die technische IT-Security beim Landratsamt. „Gerade weil wir mit hochsensiblen Bürger- und Sozialdaten arbeiten, braucht es ein Höchstmaß an Sicherheit und Verlässlichkeit.“

Mit Managed Security zu mehr Sicherheit

Auch die öffentliche Verwaltung rückt zunehmend ins Visier von Cyberkriminellen. Im Breisgau-Hochschwarzwald registrierte das IT-Team wiederholt Angriffsversuche – ohne größere Auswirkungen. „Wir hatten manchmal schlicht Glück, dass wir Indicators of Compromise frühzeitig erkannt haben und Angriffe ins Leere liefen“, erinnert sich Seifer. „Das ist aber keine nachhaltige IT-Sicherheitsstrategie. Daher wollten wir die Sicherheit systematisch auf ein neues Level heben.“ Hinzu kommt: Erfolgreiche Cyberattacken auf Städte oder kommunale Dienstleister haben gezeigt, welche gravierenden Folgen der Ausfall der IT für Verwaltung und die Bevölkerung hat.



„Wir haben in Feedbackgesprächen unsere Kritikpunkte offen angesprochen. Und G DATA hat schnell reagiert und Lösungen gefunden. Das hat uns das Gefühl gegeben: Wir sind bei einem Partner, der nicht nur liefert, sondern auch zuhört und Lösungen findet.“

Manuel Seifer

IT-Administrator | Landratsamt
Breisgau-Hochschwarzwald

Daher war schnell klar, dass der klassische Endpoint- und Virenschutz allein nicht mehr ausreicht. Folgerichtig war der Schritt zu einer Managed-Extended-Detection-and-Response-Lösung (MXDR), die rund um die Uhr Angriffe erkennt, blockiert und analysiert – auch außerhalb der klassischen Bürozeiten. Schon zu diesem Zeitpunkt entschieden sich die Verantwortlichen für eine gemanagte Lösung. Also ein Angebot, das moderne Technologien mit Dienstleistung kombiniert und versierte Fachleute die Systeme überwachen. Sie schauen im Zweifel auch genauer hin und entscheiden, was zu tun ist. Ein Grund für den Systemwechsel: Eine 24-Stunden-Überwachung der IT konnte das Landratsamt mit eigenem Personal nicht etablieren. Dafür fehlt es an Angestellten, aber auch an dem erforderlichen Spezialwissen.

Klar definierte Anforderungen

Im Vorfeld des Auswahlprozesses hatte das Landratsamt klare Kriterien formuliert. Dazu gehörte eine 24/7-Überwachung und Reaktion, um alle Clients und Server auch abends und am Wochenende zu schützen. Zudem sollten Angriffe durch automatisierte Abwehrmechanismen unmittelbar eingedämmt werden. Eine weitere Anforderung: Die Angriffsversuche sowie die Reaktion sollten gut

nachvollziehbar sein. Die Präferenz lag dabei auf einem europäischen Anbieter, der die Einhaltung der DSGVO sicherstellt, sowie die Vorgaben des BSI-Grundschutzes einhält. Und nicht zuletzt sollten Aktionen transparent und nachvollziehbar sein.

Da das Landratsamt bereits die Antiviren-Lösung von G DATA CyberDefense nutzte, war das Bochumer IT-Sicherheitsunternehmen der erste Ansprechpartner bei der Suche. Zunächst führten die Verantwortlichen bereits 2024 einen Proof of Concept mit G DATA 365 | MXDR durch, der trotz kleinerer Probleme überzeugte. „Wir haben in Feedbackgesprächen unsere Kritikpunkte offen angesprochen. Und G DATA hat schnell reagiert und Lösungen gefunden. Das hat uns das Gefühl gegeben: Wir sind bei einem Partner, der nicht nur liefert, sondern auch zuhört und Lösungen findet.“, sagt Manuel Seifer. Der enge Austausch, die Weiterentwicklung der Lösung und die Erfahrungen aus dem Pilotprojekt gaben schließlich den Ausschlag für G DATA.

Roll-out: Schritt für Schritt zu mehr IT-Sicherheit

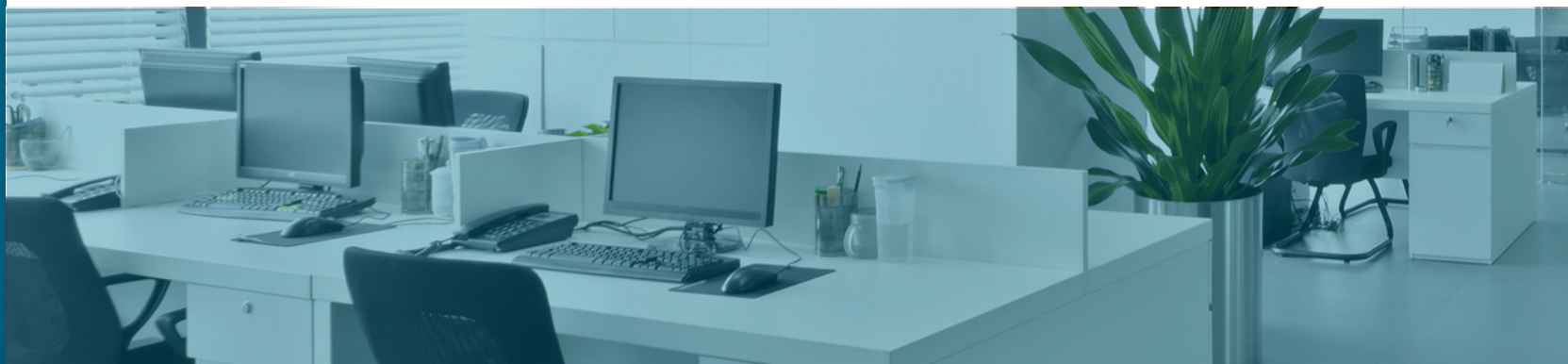
Der Roll-out startete im Frühjahr 2025 und wurde innerhalb von rund vier Monaten abgeschlossen.

Dank der eigenen Software-Verteilung verlief die Umstellung auf über 2.300 Clients und zahlreiche Server reibungslos. Besonderheiten lagen weniger in der Technik als in der Organisation – etwa bei Schulen während der Abiturphase.

„Technisch war der Roll-out unkompliziert“, sagt Seifer. „Die größten Diskussionen gab es über die nötigen Neustarts bei Installation und Deinstallation. Aber größere Stolpersteine gab es nicht.“

Erste Erfahrungen: Stabil und zuverlässig im Betrieb

Heute läuft MXDR stabil und zuverlässig. Alarme werden über den Service Desk als Tickets weitergeleitet, die Expertinnen und Experten gezielt bearbeiten. Das Webportal zeigt auf einen Blick, welche Angriffsversuche erfolgt sind und welche Reaktionen stattgefunden hat. Zusätzlich etablierte das Landratsamt eine eigene Rufbereitschaft für Vorfälle am Wochenende und in den Randzeiten. Allerdings wurde diese noch nicht einmal aktiviert. Ein Beispiel zeigt die Schlagkraft der Lösung: Während einer WebEx-Sitzung erkannte MXDR verdächtige Weiterleitungen auf externe Seiten. Zwar eine Fehlalarmierung, die aber das Vertrauen



G DATA 365 | MXDR

IT SECURITY IST TEAMPLAY



in die Reaktionsfähigkeit stärkte. „Es ist paradox: Eigentlich wünscht man sich, dass nichts passiert. Aber wenn dann doch ein Alarm kommt, zeigt das, wie aktiv das System arbeitet“, so Seifer.

Die Umstellung verlief für die Mitarbeitenden nahezu unbemerkt. Im Client-Bereich gab es keinerlei Beschwerden. Nur im Serverbetrieb mussten einzelne Ausnahmen für Fachanwendungen definiert werden. Für die Mitarbeitenden bedeutet MXDR vor allem eins: Viel Sicherheit.

Zusammenarbeit mit einem guten Partner

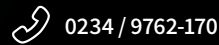
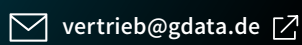
Die Kooperation mit G DATA beschreibt Seifer als partnerschaftlich und konstruktiv: „Das Entscheidende war für uns nicht, dass alles von Anfang an perfekt läuft, sondern wie mit Problemen umgegangen wird. Da fühlen wir uns bei G DATA gut aufgehoben.“ Regelmäßige Abstimmungen stellen sicher, dass die Lösung kontinuierlich optimiert wird. Zudem schätzt das Landratsamt den persönlichen Support durch feste Ansprechpartnerinnen und -partner.

Fazit

Mit G DATA 365 | MXDR hat das Landratsamt Breisgau-Hochschwarzwald den entscheidenden Schritt zu einer proaktiven, rund um die Uhr verfügbaren Cyberabwehr gemacht. „Wir wollten keine Sicherheit auf Glücksbasis, sondern einen echten 24/7-Schutz“, fasst Seifer zusammen. „Mit G DATA haben wir genau das erreicht.“



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



© 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.

