Kreis Breisgau-Hochschwarzwald

Managed Security für sensible Daten

[22.01.2026] Das Landratsamt Breisgau-Hochschwarzwald verwaltet sensible Bürger- und Sozialdaten – IT-Sicherheit hat hohe Priorität. Die Behörde nutzt eine Managed-Extended-Detection-and-Response-Lösung des Bochumer Sicherheitsspezialisten G Data. Ein Praxisbericht zeigt, welche Anforderungen es gab und wie Zusammenarbeit und Roll-out verliefen.

Der Kreis 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 zu Schulwesen und Ausländerbehörde. Dahinter steht eine komplexe IT-Infrastruktur, die On-Premises betrieben wird: Zwei eigene Rechenzentren in Freiburg, über 2.000 Clients und zahlreiche Fachanwendungen sind die Grundlage digitaler Verwaltungsservices. Insgesamt 70 Mitarbeitende kümmern sich um die IT und die Verwaltungsdigitalisierung – aber nur fünf Personen haben ihren Fokus bei IT-Sicherheit und Compliance. „Gerade weil wir mit hochsensiblen Bürger- und Sozialdaten arbeiten, braucht es ein Höchstmaß an Sicherheit und Verlässlichkeit“, sagt Manuel Seifer, als IT-Administrator auch verantwortlich für die technische IT-Security beim Landratsamt.

„Glück haben“ ist kein Sicherheitskonzept

Die öffentliche Verwaltung rückt zunehmend ins Visier von Cyber-Kriminellen. Erfolgreiche Cyber-Attacken auf andere Städte oder kommunale Dienstleister haben bereits gezeigt, welch gravierende, langfristige Folgen ein Ausfall der IT für Verwaltung und Bevölkerung haben kann. Auch im Kreis Breisgau-Hochschwarzwald registrierte das IT-Team schon wiederholt Angriffsversuche – bisher allerdings 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.“

Managed Security bringt Sicherheit

Es 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). Diese kann rund um die Uhr Angriffe erkennen, blockieren und analysieren – auch außerhalb der klassischen Bürozeiten. Schon frühzeitig entschieden sich die Verantwortlichen für eine gemanagte Lösung, also ein Angebot, das moderne Technologien mit Dienstleistung kombiniert und bei dem 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 erforderlichem 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.

Enger Austausch

Da das Landratsamt bereits die Antiviren-Lösung des Herstellers G DATA CyberDefense nutzte, war das Bochumer IT-Sicherheitsunternehmen der erste Ansprechpartner bei der Suche. Zunächst führten die Verantwortlichen 2024 einen Proof of Concept mit der Angriffsabwehr-Lösung 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.

Erfolgreicher Roll-out

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 für die Mitarbeitenden nahezu unbemerkt. Im Client-Bereich gab es keinerlei Beschwerden, nur im Serverbetrieb mussten einzelne Ausnahmen für Fachanwendungen definiert werden. „Technisch war der Roll-out unkompliziert“, sagt Seifer. „Die größten Diskussionen gab es über die nötigen Neustarts bei Installation und Deinstallation.“ Für Vorfälle am Wochenende und in Randzeiten etablierte das Landratsamt zudem eine eigene Rufbereitschaft. Allerdings wurde diese noch nie aktiviert. Heute läuft MXDR stabil und zuverlässig. Alarme werden über den Service Desk als Tickets weitergeleitet, die Expertinnen und Experten gezielt bearbeiten. Das Webportal zeigt, welche Angriffsversuche erfolgt sind und welche Reaktion stattgefunden hat. Regelmäßige Abstimmungen stellen sicher, dass die Lösung kontinuierlich optimiert wird. Zudem schätzt das Landratsamt den persönlichen Support durch feste Ansprechpartnerinnen und -partner.

()

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Cybersicherheit, G DATA, Kreis Breisgau-Hochschwarzwald