CUSTOMER CASE STUDY

Mehr Sicherheit, weniger Last: Wie die Kreisverwaltung Alzey-Worms mit MDR echte Handlungsfähigkeit gewinnt

Mit Managed Detection and Response gewinnt die Verwaltung rund um die Uhr Handlungsfähigkeit und stärkt spürbar das Sicherheitsgefühl im Alltag.

SOPHOS

Kreisverwaltung ALZEY-WORMS

Kreisverwaltung Alzey-Worms

Industrie
Behörde

Nutzer
1.220

Sophos-Partner
Kommunalberatung Rheinland-Pfalz GmbH

Sophos-Lösungen
Sophos Managed Detection and Response

Sophos Network Detection and Response

Sophos Managed Risk

Sophos Firewall

Sophos Access Points

Öffentliche Verwaltungen stehen vor einem doppelten Druck: Sie müssen eine wachsende Zahl digitaler Dienste zuverlässig bereitstellen und gleichzeitig eine Bedrohungslage bewältigen, die sich zunehmend professionalisiert. Anders als große Unternehmen verfügen sie jedoch selten über entsprechend ausgebaute IT-Sicherheitsteams. Genau in diesem Spannungsfeld hat die Kreisverwaltung Alzey-Worms ihre Sicherheitsarchitektur neu ausgerichtet – mit dem Ziel, Schutz und Betriebsfähigkeit langfristig sicherzustellen.

Die Herausforderung

Die IT-Struktur der Kreisverwaltung ist breit aufgestellt und historisch gewachsen. Neben klassischen Verwaltungsarbeitsplätzen umfasst sie zahlreiche Fachverfahren für Bürgerdienste sowie angebundene Einrichtungen wie das Kreiskrankenhaus und die Schulen des Landkreises. Insgesamt werden rund 1.400 Clients in unterschiedlichen Organisationseinheiten betrieben – 700 in der Kreisverwaltung selbst, 250 im Kreiskrankenhaus und 450 in den kreiseigenen Schulen – mit jeweils eigenen Anforderungen, aber gemeinsamer Verantwortung für Sicherheit und Verfügbarkeit.

Mit der zunehmenden Professionalisierung von Cyberangriffen wurde deutlich, dass die vorhandenen Mittel nicht mehr ausreichen. Besonders kritisch war dabei weniger die einzelne Technologie als die fehlende Möglichkeit, Bedrohungen durchgängig zu überwachen und schnell zu reagieren.

„Wir haben gesehen, dass andere Verwaltungen erfolgreich angegriffen wurden. Uns war klar, dass wir mit unseren bestehenden Ressourcen nicht in der Lage sind, diese Risiken dauerhaft zu beherrschen – vor allem außerhalb der regulären Arbeitszeiten", so Marc Kramer, ISB, IT-Wissensmanager und IT-Sicherheitsbeauftragter.

Die zentrale Frage war daher nicht nur, welche Lösung eingesetzt wird, sondern wie sich Sicherheitsarbeit trotz begrenzter personeller Kapazitäten organisieren lässt.

„Wir haben gesehen, dass andere Verwaltungen erfolgreich angegriffen wurden. Uns war klar, dass wir mit unseren bestehenden Ressourcen nicht in der Lage sind, diese Risiken dauerhaft zu beherrschen – vor allem außerhalb der regulären Arbeitszeiten."

Marc Kramer, ISB,
IT-Wissensmanager und
IT-Sicherheitsbeauftragter

Die Lösung

Die Kreisverwaltung entschied sich für einen integrierten Ansatz mit Sophos Central sowie Managed Detection and Response (MDR), ergänzt durch Network Detection and Response (NDR), Managed Risk und die bereits vorhandene Sophos XGS Firewall.

Ausschlaggebend war das Zusammenspiel der Komponenten: Statt isolierter Einzellösungen setzt die Verwaltung auf eine Plattform, die Informationen bündelt und Zusammenhänge sichtbar macht. Wichtig war dabei auch, dass sich die Lösung nahtlos in die vorhandene Sicherheitsarchitektur mit der bestehenden Firewall integrieren ließ. Die Beschaffung erfolgte im Rahmen eines Vergabeverfahrens. Ausschlaggebend waren dabei insbesondere die technische Passgenauigkeit und das Zusammenspiel der einzelnen Komponenten.

Gleichzeitig liefert MDR genau die Unterstützung, die intern nicht abbildbar ist: kontinuierliche Überwachung, Einordnung von Vorfällen und schnelle Reaktion – auch außerhalb der Dienstzeiten.

Ein klassisches SIEM kam nicht infrage, denn der operative Aufwand wäre mit den vorhandenen Ressourcen nicht leistbar gewesen. Ebenso wenig überzeugten andere Anbieter am Markt, die entweder Kompatibilitätsprobleme verursacht hätten oder aufgrund der Projektgröße kein Interesse zeigten.

Die Inbetriebnahme erfolgte schrittweise, um den laufenden Betrieb nicht zu beeinträchtigen und die Einführung an die organisatorischen Gegebenheiten der einzelnen Bereiche anzupassen. Für die Kreisverwaltung wurde ein Guided Onboarding genutzt. Die Anbindung weiterer Organisationseinheiten, darunter das Kreiskrankenhaus und die kreiseigenen Schulen, erfolgt schrittweise und unter Berücksichtigung der jeweiligen organisatorischen Anforderungen.

Herausforderungen gab es insbesondere bei der Einführung von NDR, da entsprechende Expertise intern zunächst fehlte. Diese konnte jedoch in enger Abstimmung mit Sophos rasch aufgebaut werden.

> „Das Sicherheitsempfinden hat sich bei uns massiv gesteigert. Wir wären nicht in der Lage gewesen, diese kurzen Reaktionszeiten bei Detection and Response selbst umzusetzen – erst recht nicht außerhalb der Dienstzeiten."
>
> Marc Kramer, ISB, IT-Wissensmanager und IT-Sicherheitsbeauftragter

Das Ergebnis

Heute verfügt die Kreisverwaltung über eine Sicherheitsarchitektur, die technisch zukunftsfähig ist und sich optimal in die Organisation der Kreisverwaltung Alzey-Worms einfügt.

Die IT erhält einen zentralen Überblick über alle relevanten Systeme, von Endpoints und Servern über die Firewall bis hin zum Schwachstellenmanagement mit Managed Risk. Risiken bleiben nicht länger unentdeckt oder unbearbeitet, sondern werden kontinuierlich bewertet und adressiert.

Vor allem aber hat sich eines deutlich verändert: „Das Sicherheitsempfinden hat sich bei uns massiv gesteigert", beschreibt Marc Kramer die Wirkung. „Wir wären nicht in der Lage gewesen, diese kurzen Reaktionszeiten bei Detection and Response selbst umzusetzen – erst recht nicht außerhalb der Dienstzeiten."

Gleichzeitig wird die IT-Abteilung spürbar entlastet. Die permanente Überwachung im Hintergrund schafft Freiräume für strategische Aufgaben – bei gleichzeitig höherem Schutzniveau.

Der Partner: Kommunalberatung RLP

Die Kommunalberatung Rheinland-Pfalz begleitet öffentliche Einrichtungen bei der Auswahl und Umsetzung von IT- und Sicherheitslösungen. Der Fokus liegt auf praxistauglichen Konzepten, die den spezifischen Anforderungen kommunaler Strukturen gerecht werden und sich im laufenden Betrieb bewähren.

Mehr Informationen unter www.sophos.de

2026-06-08 CCS-DE (NP)

SOPHOS