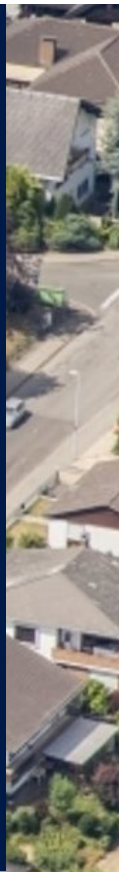
Cybersicherheit aus einer Hand

Mit 14 Schulen und 16 weiteren Außenstellen wie Sozialraumbüros, Deponien, Kfz-Servicestellen oder das Gesundheitsamt mit verschiedensten Ansprüchen muss das IT-Team der Kreisverwaltung Bad Dürkheim ein weit vernetztes IT-System managen. Aufgrund der Verwaltung sensibler Daten und Dienste bestehen sehr hohe Anforderungen an die Datensicherheit. Gleichzeitig müssen die vorhandenen Ressourcen und Budgetmittel optimal eingesetzt werden, um die interne Administration effektiv zu entlasten und gleichzeitig höchstmöglichen Schutz vor aktuellen Bedrohungen zu garantieren. Sophos bietet mit seinem Cybersecurity-Ökosystem inklusive zentralem Management und einem modernen MDR-Service optimale Rundum-Sicherheit bei geringstmöglichem Management und Kostenaufwand.



Auf einen Blick

Kreisverwaltung Bad Dürkheim

Industrie
Kommunale Verwaltung

Website
www.kreis-bad-duerkheim.de

Sophos-Partner
SHC Netzwerktechnik GmbH

Nutzer
700

Sophos-Lösungen
Sophos MDR
Sophos EDR
Sophos XDR
Sophos XGS
Sophos Access Points

„Das Cybersecurity-Ökosystem von Sophos bietet uns alle Facetten, die wir benötigen, um der gesamten Infrastruktur inner- und außerhalb unseres Netzwerks höchstmöglichsten Schutz zu bieten.“

Jens Preßler, Referatsleiter IT

Der Landkreis Bad Dürkheim ist im Zuge der Verwaltungsreform in Rheinland-Pfalz 1969 aus Teilen der ehemaligen Kreise Neustadt und Frankenthal entstanden. In 48 Gemeinden leben heute rund 132.000 Menschen auf einer Fläche von knapp 600 km2. Jeweils zur Hälfte prägen Wald und Weinbaulandschaft mit dem Siedlungsband der Deutschen Weinstraße den Landkreis Bad Dürkheim. Aktuell sind ca. 900 Mitarbeiter und Mitarbeiterinnen beim Landkreis beschäftigt. Neben dem eigentlichen Haupthaus unterhält der Landkreis ca. 35 weitere Außen- und Nebenstellen wie u.a. das Gesundheitsamt Neustadt, Sozialraumbüros sowie Kfz-Außenstellen und die Kreisvolkshochschule.

Die Herausforderung

Die besondere Bedeutung kritischer Infrastrukturen für die Grundversorgung der Bevölkerung und die daraus resultierenden, erhöhten Sicherheitsanforderungen, um einen Ausfall als Folge von Cyberangriffen zu verhindern, führen dazu, dass die eine effiziente und schlagkräftige Cybersecurity-Strategie weit oben auf der IT-Prioritätenliste der Kreisverwaltung Bad Dürkheim steht.

Cyberkriminelle machen sich permanent neuere Technologien zunutze, um Schwachpunkte anzugreifen. Für IT-Teams wird es immer schwieriger, Cyberbedrohungen rechtzeitig zu identifizieren, zu untersuchen und dagegen vorzugehen, denn die Angriffsvarianten verändern sich ständig. Aufgrund der immer komplexeren Gefahrenlage, die Organisationen kaum noch komplett überblicken und meistern können, hat die Kreisverwaltung Bad Dürkheim beschlossen, auf das Cybersecurity-Ökosystem von Sophos zu setzen, dass den Schutz von Endpoints und Netzwerk synchronisiert und zudem erfahrene Threat Hunter mittels eines dedizierten Managed-Security-Services bereitstellt. Im Fokus der Strategie stehen dabei die 24/7-Überwachung durch externe Experten, die Absicherung auch vor neuartigen Cyberangriffen und ein zentrales Management mit einem Dashboard für alle Anwendungen.

„Das Risiko, von einer gezielten Cyberattacke betroffen zu sein, ist heute so hoch wie noch nie. Dank Sophos MDR können wir eine permanente Überwachung aller Systeme durch Experten realisieren und auf Gefahren sofort reagieren."

SJens Preßler, Referatsleiter IT

Die Lösung

Die Kreisverwaltung Bad Dürkheim hatte bereits in der Vergangenheit gute Erfahrungen mit den Security-Lösungen von Sophos gemacht, und entschied sich daher, auf ein Gesamtpaket aus einer Hand zu setzen.

Um den zunehmenden Cyberbedrohungen entgegenzuwirken, empfahl der Systemhauspartner SHC, in einem ersten Schritt einen zusätzlichen Bedrohungsschutz mit Sophos Intercept X mit XDR einzusetzen. Die Lösung erkennt automatisch potenzielle Bedrohungen und bietet einen optimierten Schutz, selbst gegen hochentwickelte und komplexe Cyberbedrohungen. Die gesamte Verwaltung und Steuerung von XDR erfolgt, wie auch bei allen anderen Sophos-Lösungen, in der zentralen Management-Konsole Sophos Central.

Dieses System wurde anschließend durch Sophos MDR um eine Managed-Security-Variante erweitert. Aufbauend auf dem bestehenden XDR-Schutz fusioniert das Angebot maschinelles Lernen mit Expertenanalyse, um das Auffinden von Bedrohungen zu verbessern, Warnmeldungen gründlicher zu untersuchen und gezielter bei der Eliminierung von Gefahren zu agieren. Der MDR-Service von Sophos bietet Organisationen ein 24/7 verfügbares Sicherheitsteam, das gezielte Maßnahmen ergreift, um selbst hochkomplexe Bedrohungen zu neutralisieren.

Das Ergebnis

Die Vorteile des Cybersecurity-Ökosystems von Sophos liegen für Referatsleiter Jens Preßler auf der Hand: „Nach der Umstellung können wir uns nun auf eine Überwachung rund um die Uhr durch externe Profis verlassen, die Sicherheitsvorfällen auch am Wochenende im Blick haben und gegebenenfalls schnell reagieren können." Zudem profitiert das IT-Team von einer umfangreichen und effizienten Überwachung und Verwaltung aller ins Netzwerk eingebundenen Geräte.
Die benutzerdefinierte Regelung für Firewalls und Endpoints ermöglicht zudem eine sehr gezielte Steuerung der Zugangsmöglichkeiten für unterschiedliche Mitarbeiter und damit eine Reduzierung der Angriffsfläche.

Neben den bereits bestehenden Security-Lösungen steht nun zudem eine zusätzliche Lösung zur automatischen Erkennung und Priorisierung sowie Reaktion auf potenzielle Bedrohungen zur Verfügung. Machine Learning sorgt dank Sophos XDR dabei für die Identifizierung verdächtiger Ereignisse und weiterführende Cyber-Security-Funktionen dienen der Analyse und Reaktion auf potenzielle Sicherheitsbedrohungen. Die Threat Hunter aus dem Sophos-MDR-Team sorgen für die menschliche Komponente, die aus heutigen Cybersecurity-Lösungen aufgrund der immer professionelleren Angriffe nicht mehr wegzudenken ist. Als Managed Service sorgen die Experten nicht nur dafür, auf Vorfälle zu reagieren, sondern sie senken gleichzeitig die Wahrscheinlichkeit eines Vorfalls.

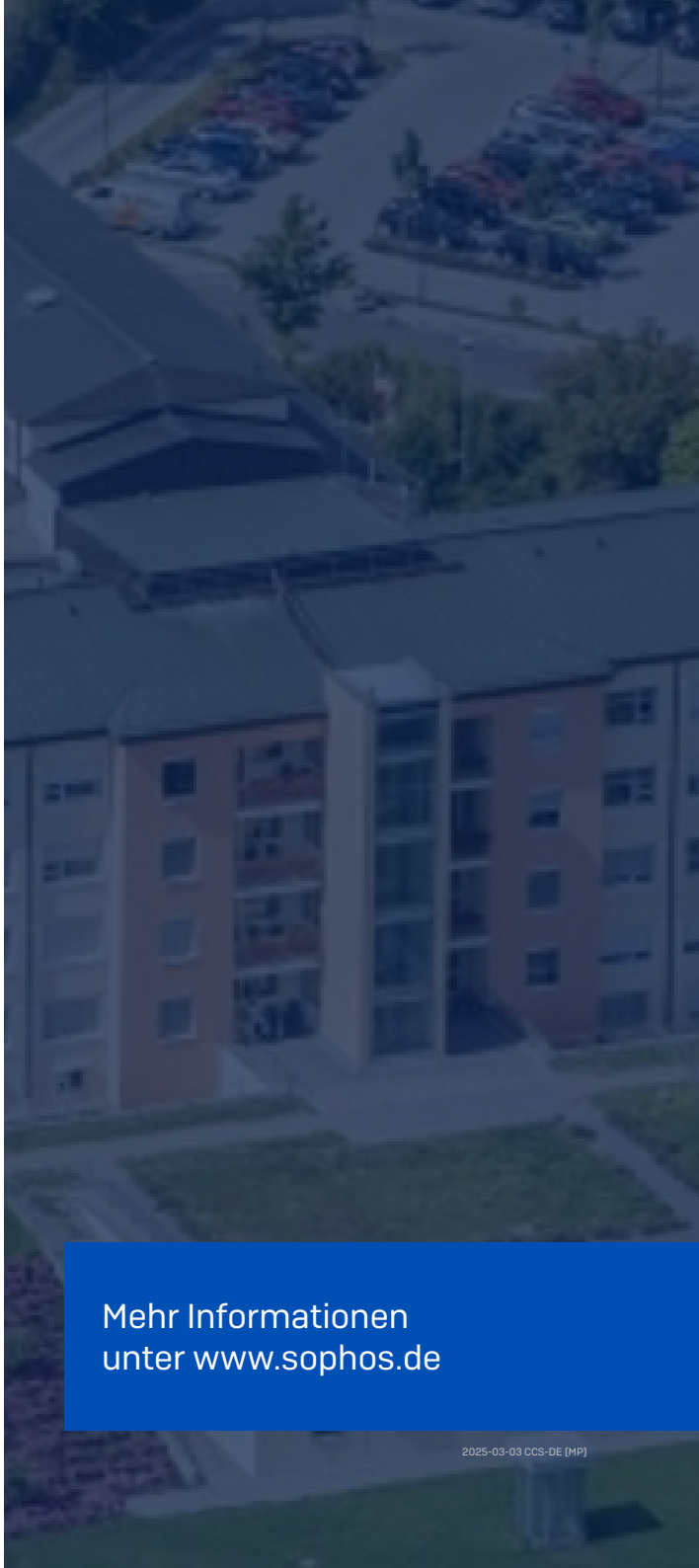
Der Partner

SHC Netzwerktechnik GmbH

Die SHC Netzwerktechnik GmbH bietet als mittelständischer IT-Dienstleister Kundendienste in den Bereichen IT-Sicherheit, IT-Infrastruktur, IT-Management und IT-Service an. Seit 1991 ist das Unternehmen bundesweit von den Standorten Frankfurt am Main, Berlin und Köln aus tätig. Bei der Auswahl und Einführung neuer Produkte oder Lösungen ist für die SHC die individuelle Ausgangssituation eines jeden Kunden entscheidend.

SHC begleitet seine Kunden von der Beratung, Projektierung und Beschaffung bis hin zur Integration und Schulung der Mitarbeiter.

www.shc.eu



Mehr Informationen
unter www.sophos.de

SOPHOS

2025-03-03 CCS-DE (MP)