Bad Tölz setzt auf Cybersecurity as a Service

Bei der Stadt Bad Tölz setzt die IT-Leitung für eine sichere Datenbehandlung seit jeher auf modernste Security-Technologien, wie zum Beispiel Firewalls von Sophos oder Sophos Mobile. Aufgrund ständig neuer und raffinierterer Cyberbedrohungen hat das IT-Team das Thema Security stets auf dem Schirm, damit sowohl der Schutz der eigenen Daten als auch die der Bürger:innen garantiert ist. In Bad Tölz setzt man für einen umfangreichen Schutz mit automatischen Gefahrenerkennung seit Kurzem auf die Lösung Sophos Intercept X mit XDR.

AUF EINEN BLICK

STADT **BAD TÖLZ**

Stadt Bad Tölz

Branche
Kommunale Verwaltung

Anzahl der Nutzer
1.000 Endpoints

Webseite
www.stadt.bad-toelz.de

Sophos-Partner
Hammer Real GmbH

Sophos-Produkte
Sophos Intercept X mit XDR
Sophos MDR

“Mit Sophos Intercept X mit XDR in Kombination mit Firewalls und dem Endpoint-Schutz von Sophos haben wir nun eine Security-Infrastruktur, die uns den höchstmöglichsten Schutz vor Cyberbedrohungen bietet.“

Ithamar Garbe, Leitung Informationstechnik

Bad Tölz ist die Kreisstadt des oberbayerischen Landkreises Bad Tölz-Wolfratshausen. Die Kurstadt liegt an der Isar rund 50 Kilometer südlich von München und zählt gut 19.000 Einwohner. Bei der Stadtverwaltung Bad Tölz arbeiten 230 Mitarbeiter. Die Stadt bietet seinen Bürger:innen neben den städtischen Ämtern ein großes Portfolio an modernen öffentlichen Einrichtungen aus den Bereichen Soziales, Bildung, Kultur sowie Sport und Freizeit.

Die Herausforderung

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. Zudem verwenden Hacker mittlerweile raffiniertere Ausweichtechniken, die es IT-Teams sehr erschweren, Zugriffe rechtzeitig zu entdecken. Aufgrund der immer komplexeren Gefahrenlage, die Organisationen kaum noch komplett überblicken und meistern können, hat die Stadt Bad Tölz beschlossen, die seit zweieinhalb Jahren eingesetzte Lösung Sophos Intercept X mit einer automatischen und erweiterten Gefahrenerkennung zu komplettieren – Sophos Intercept X mit XDR.

Die Lösung

Die Stadt Bad Tölz hatte bereits in der Vergangenheit gute Erfahrungen mit den Security-Lösungen von Sophos gemacht, insbesondere bei der sicheren Internet- und VPN-Anbindung über das eigene Glasfasernetz sowie über Richtfunk mit Hilfe von Sophos Firewalls und Sophos REDs in den Außenstellen. Zudem waren bereits Sophos Mobile für die mobilen Endpoints und der Endpoint-Schutz mit Sophos Intercept X im Einsatz. Diese Lösungen sorgten für die Cybersicherheit der 40 produktiven Server und den Servern in 17 Außenstellen sowie der zwei Hauptrechenzentren und der circa 1.000 mobilen Geräte und Smartphones der Mitarbeiter.

Um den zunehmenden Cyberbedrohungen entgegenzuwirken, empfahl der Münchner IT-Dienstleister Hammer Real GmbH, einen

“Das Risiko, von einer gezielten Cyberattacke betroffen zu sein, ist heute so hoch wie noch nie. Doch für eine permanente Überwachung aller Systeme durch Experten zusätzlich zur automatisierten Security fehlt uns sowohl die Zeit als auch die Manpower. Mit Sophos Intercept X mit XDR haben wir ein effektives Werkzeug an der Hand, das uns automatisch und unmittelbar potenzielle Gefahren und Aktivitäten von Cyberkriminellen aufzeigt, damit wir sofort reagieren können.“

Thomas Nether, IT-Security Administrator

zusätzlichen Bedrohungsschutz mit Sophos Intercept X mit XDR einzusetzen. Die Lösung wurde vom IT-Team geprüft und nach kurzer Zeit waren Ithamar Garbe und Thomas Nether vom Bad Tölzer IT-Team überzeugt davon, dass XDR der fehlende Baustein in ihrem Security-Konzept ist. Die Lösung erkennt automatisch potenzielle Bedrohungen und bietet einen optimierten Schutz, selbst gegen hochentwickelte und komplexe Cyberbedrohungen. Die Implementierung verlief aus technischer Sicht sehr reibungslos. Nach entsprechender Umstellung und Konfiguration der Firewalls wurde die neue Lösung nach und nach live geschaltet. Die gesamte Verwaltung und Steuerung von XDR erfolgt, wie auch bei allen anderen Sophos-Lösungen, in der zentralen Management-Konsole Sophos Central.

Das Ergebnis

Bei der Stadt Bad Tölz sorgt Sophos Intercept X mit XDR für zusätzliche Sicherheit und Schutz gegen moderne Cyberbedrohungen. Neben den bereits bestehenden Security-Lösungen haben die IT-Profis Nether und Garbe nun auch ein zusätzliches und effizientes Tool zur automatischen Erkennung und Priorisierung potenzieller Bedrohungen an der Hand. Machine Learning sorgt dabei für die Identifizierung verdächtiger Ereignisse und weiterführende Cyber-Security-Funktionen dienen der Erkennung, Analyse und Reaktion auf potenzielle Sicherheitsbedrohungen. Darüber hinaus bietet Intercept X mit XDR die Verfolgung historischer Ereignisse über einen Zeitraum von bis zu 30 Tagen. Dafür werden produktübergreifende Daten im Cloud-basierten Data Lake gespeichert, so das umfassende, kontextbezogen Einblicke möglich sind. Unregelmäßigkeiten, etwa Aktivitäten von Cyberkriminellen im Netzwerk und auf den Endpoints, können erkannt und genau nachvollzogen werden. Dies ist insbesondere dann ein entscheidender Vorteil, wenn die Angreifer eine Attacke vorbereiten und sich vor dem eigentlichen Schlag bereits Tage und Wochen unauffällig im Netzwerk bewegen, um ihre Vorbereitungen für den eigentlichen Angriff zu treffen. Die Lösung ist Teil des Sophos Adaptive Cybersecurity Ecosystems, einer offenen Sicherheitsarchitektur zur Optimierung von Threat Prevention, Detection und Response. Ergänzt werden die Sophos-Lösungen bei der Stadt Bad Tölz durch hoch spezialisierte

MDR (Managed Detection and Response)-Experten. Sie suchen aktiv und 24/7 nach Bedrohungen, um Angreifer zu identifizieren und zu stoppen, bevor sie ihre Attacken ausführen können. Als Managed Service sorgen sie nicht nur dafür, auf Vorfälle zu reagieren, sondern senken gleichzeitig die Wahrscheinlichkeit eines Vorfalls..

Hammer Real GmbH

Die Hammer Real GmbH ist ein Münchner IT-Dienstleister, der auf IT-Security; IT-Dienstleistungen und IT-Consulting spezialisiert ist. Das Unternehmen bietet Unternehmen – von selbständigen Einzelunternehmen bis hin zu mittelständischen Unternehmen – individuell angepasste IT-Lösungen und schafft so ein optimales Arbeitsumfeld für seine Kunden. Darüber hinaus übernimmt der IT-Spezialist auf Wunsch auch alle Aufgaben der IT-Verwaltung – Von der Vertragsabwicklung mit Telekommunikationsdienstleistern über die Wartung bestehender Systeme bis hin zur kompletten Neueinrichtung eines Büronetzwerkes oder die Auslagerung in die Cloud.

www.it.hammer.ag

“Mit Sophos Intercept X mit XDR sehen wir jetzt sofort, wo bei uns potenzielle Bedrohungen lauern, so dass wir sofort reagieren können.“

Ithamar Garbe
Leitung Informationstechnik

Mehr Informationen
unter www.sophos.de

SOPHOS

2022-09-19 CCS-DE (NP)