



Sichere Mobilität rund um die Uhr mit dem Cybersecurity-Ökosystem von Sophos

Als Mobilitätsdienstleister im öffentlichen Personennahverkehr mit mehr als 18.000 Fahrgästen täglich ist die Havelbus Verkehrsgesellschaft besonders auf sichere IT-Systeme angewiesen. Die Umstellung auf eine moderne Sicherheitsstrategie war deshalb unumgänglich und mit der Herausforderung verbunden, den Normalbetrieb des Unternehmens aufrechtzuerhalten. Neben modernen Firewall- und Endpoint-Security-Lösungen stand zudem die Realisierung eines SOC-Services rund um die Uhr an 365 Tagen im Jahr im Fokus, der durch Sophos MDR realisiert werden konnte.

Auf einen Blick



Havelbus Verkehrsgesellschaft mbH
Nauen

Branche
Transport und Verkehr

Webseite
www.havelbus.de

Anzahl der Nutzer
220

Sophos-Partner
SHC Netzwerktechnik GmbH

Sophos-Produkte
Sophos Intercept X
Sophos MDR
Sophos XGS Firewall

„In dem Wissen, dass die IT rund um die Uhr an 365 Tagen im Jahr überwacht und geschützt wird, entspannt das Arbeitsumfeld sich sehr. Der MDR-Service durch die Sophos-Experten ist für uns eine riesige Entlastung und die perfekte Alternative zu einem aufwändigen, internen SOC-Team.“

Björn Fritzlär, Sachgebietsleiter EDV

Die Havelbus Verkehrsgesellschaft mbH bietet als Mobilitätsdienstleister in der Region alle Nahverkehrsleistungen aus einer Hand. Mehr als 18.000 Fahrgäste täglich nutzen den Service des Unternehmens. Hauptgeschäftsfeld ist der Linienverkehr und alle damit verbundenen Aufgaben wie die Planung, Durchführung und Verwaltung der Angebote. Das Rückgrat für ein qualitativ hochwertiges und bedarfsgerechtes ÖPNV-Angebot ist die Fahrzeugflotte mit 110 Bussen inkl. 8 Kleinbussen. Weiterhin leistet Havelbus Schüler-, Schienenersatz- und Sonderlinienverkehre für verschiedene Auftraggeber wie die DB Regio AG. 243 Mitarbeiter an drei Standorten (Falkensee, Nauen und Rathenow) machen das Unternehmen zu einem großen Arbeitgeber in der Region.

Die Herausforderung

Die Havelbus Verkehrsgesellschaft stand vor der Umstellung auf Sophos vor der Herausforderung, mit einem unübersichtlichen und nicht auf dem Stand der Technik befindlichen IT-System arbeiten zu müssen. Zudem mussten mehrere HyperV-Farmen, die zum Teil gleiche Server hosteten, umgezogen werden und sollten entsprechenden Schutz erhalten. Die Umstellung stellte auch zeitlich eine Herausforderung dar, da der Normalbetrieb des Busunternehmens weiter gewährleistet sein musste und nebenbei der Umzug auf eine neue Virtualisierungsplattform erfolgte. Im Anschluss war zudem die Einrichtung eines modernen Cybersecurity-Systems mit neuer Firewall und Endpoint-Security vorgesehen, um flexibel und schnell auf zukünftige Herausforderungen reagieren zu können. Die Lösung sollte die BSI-Empfehlung „Stand der Technik“ erfüllen und der IT war es

wichtig, mit Hinblick auf das IT-Sicherheitsgesetz 2.0 sowie EU NIS 2.0 ein aktives Endpoint Detection & Response betreiben sowie einen SOC-Service realisieren zu können.

Die Lösung

Dank der Gespräche mit SHC und Sophos war für Havelbus schnell klar, dass die Verwendung modernster Cybersecurity-Ansätze, die bisher nicht im Fokus des Unternehmens lagen, für ein entscheidendes Plus in Sachen IT-Sicherheit sorgen und zudem die Ansprüche in gesetzlicher und kaufmännischer Hinsicht erfüllen. Die Kombination aus dem Cybersecurity-Ökosystem mit dem SOC-Service Sophos MDR rund um die Uhr konnte keiner der Mitbewerber bieten.

Das adaptive Cybersecurity-Ökosystem (ACE) von Sophos, das Lösungen für Endpoint, Server und Netzwerk miteinander kommunizieren lässt und

gleichzeitig eine zentrale Verwaltung sowie den Zugriff auf einen gemeinsamen Data Lake zur Analyse ermöglicht, sorgt für grundlegenden Schutz auch vor modernen Cyberattacken. Um zunehmenden, individuellen Cyberangriffen wirksam entgegenzuwirken, empfahlen die IT-Experten von SHC, als zusätzlichen Bedrohungsschutz Sophos Managed Detection & Response (MDR) einzusetzen. Aufbauend auf Sophos Intercept X fusioniert dieser Service maschinelles Lernen mit Expertenanalyse, um das Auffinden von Bedrohungen zu verbessern, Warnmeldungen gründlicher zu untersuchen und gezielter bei der Eliminierung von Gefahren zu agieren

Das Ergebnis

Da zeitgleich mit der neuen Firewall auch die gesamte Netzstruktur überarbeitet wurde, war das Havelbus-IT-Team stark auf die Unterstützung der Partner SHC und Sophos angewiesen und wurde nicht enttäuscht: „Wir waren sehr positiv überrascht, wie einfach es war, den MDR-Service einzurichten und in Betrieb zu nehmen. Hier spielte der tolle Support im Vorfeld eine entscheidende Rolle, und es war sehr einfach, den Mitarbeitenden der IT im Unternehmen den Umstieg auf eine angemessenere Sicherheitslösung schmackhaft zu machen. Die übrige Belegschaft hat aufgrund der reibungslosen Umsetzung so gut wie nichts von der Umstellung mitbekommen“, so Sachgebietsleiter Björn Fritzlar.

Für die größte Entlastung des IT-Teams sorgt nun der MDR-Service durch die Sophos-Experten rund um die Uhr and 365 Tagen im Jahr. Björn Fritzlar zu den Unterschieden: „Anfangs war kein EDR vorhanden, wodurch die IT nicht einmal wusste, wenn irgendwo

etwas aus dem Ruder lief. Als während des Testzeitraums dann die ganzen Informationen verfügbar wurden und ich mit der meisten IT-Sec Erfahrung im Team, von der schieren Menge an Informationen an den Rand der Überlastung getrieben wurde, war schnell klar, dass dies an echte Spezialisten übergeben werden musste. Hier war ich sehr froh, dass die Geschäftsführung dies auch so sah und wir gemeinsam guten Gewissens auf MDR setzen konnten.“



SHC Netzwerktechnik GmbH

Die SHC Netzwerktechnik GmbH ist ein mittelständischer IT-Dienstleister mit einer langjährigen Erfahrung in Bereichen IT-Sicherheit, IT-Infrastruktur, IT-Management und IT-Service. Seit 1991 ist das Team bundesweit von unseren Standorten Frankfurt am Main, Berlin und Köln aus tätig. Der Anspruch ist die optimale Beratung der Kunden. Bei der Auswahl und der Einführung neuer Produkte oder Lösungen ist für SHC die individuelle Ausgangssituation eines jeden Kunden entscheidend. Durch die langjährige Erfahrung kann das Team seine Kunden umfassend aus einer Hand betreuen und begleitet Unternehmen von der Beratung, Projektierung und Beschaffung bis hin zur Integration und Schulung ihrer Mitarbeiter.

Mehr Infos unter www.shc.eu

„Wir waren sehr positiv überrascht, wie einfach es war, den MDR-Service einzurichten und in Betrieb zu nehmen. Der tolle Support durch SHC und Sophos machte hier den Unterschied.“

Björn Fritzlar, Sachgebietsleiter EDV

Mehr Infos unter
www.sophos.de