CUSTOMER CASE STUDY

Sichere Brautradition dank moderner Cybersecurity

Als Unternehmen mit langer Tradition und entsprechend historisch gewachsenen Strukturen muss die IT-Abteilung von Früh sehr unterschiedliche IT- und OT-Strukturen betreuen. Deshalb sind eine effektive digitale Infrastruktur und die Absicherung aller Systeme eine zentrale Herausforderung.

SOPHOS

Cölner Hofbräu FRÜH

Industrie
Lebensmittel/Brauerei

Nutzer
280

Sophos-Partner
H&G Hansen und Gieraths EDV Vertriebsgesellschaft mbH

Sophos-Lösungen
Sophos Firewall
Sophos NDR
Sophos MDR
Sophos ZTNA

Die bisherige, gute Zusammenarbeit mit Sophos legte den Grundstein für eine umfassende Modernisierung und flexible Ausrichtung der Cybersecurity-Architektur, in deren Rahmen viel Wert auf eine zentrale Steuerung sowie die Einbindung eines externen SOC-Teams gelegt wurde. Mit dem 24/7-Schutz ließ sich zudem die Voraussetzung für eine Cyberversicherung realisieren.

Seit 1904 ist die Cölner Hofbräu P. Josef FRÜH KG als lokaler Arbeitgeber mit heute über 500 Mitarbeitern in Köln verwurzelt. Eigengeführt in 5. Generation, definiert sich das Familienunternehmen über Tradition, Kultur, Braukunst und herzliche Gastlichkeit. Mit jährlich 350.000 gebrauten Hektolitern Früh Kölsch gehört das Unternehmen somit zu den drei größten Kölsch-Brauereien.

Das Stammhaus am Dom mit rund 1.200 Sitzplätzen im Innenbereich und großem Biergarten mit 200 Sitzplätzen, das moderne Eden Hotel mit 86 Zimmern gleich nebenan, vier weitere eigengeführte Brauhäuser in den Veedeln mit rund 270 Mitarbeitenden in Küche, Service und Verwaltung sorgen für deftige Speisen und echte kölsche Gastlichkeit.

„Die Cybersecurity-Lösung von Sophos sorgt bei uns für ein durchweg positives Sicherheitsgefühl und hat zudem positive Business-Auswirkungen wie den erfolgreichen Abschluss einer Cyberversicherung."

Gino Link
Leiter IT

Die Herausforderung

Die IT-Infrastruktur von Früh ist aufgrund der sehr unterschiedlichen, historisch gewachsenen IT- und OT-Strukturen anspruchsvoll. So müssen Anlagen-PCs mit älteren Betriebssystemen an den Produktionsstandorten ebenso abgesichert werden wie die IT in der Verwaltung, Hotellerie und Gastronomie. Das IT-Team ist deshalb auf eine übersichtliche und einheitliche Security-Strategie angewiesen, die zukunftssicher ist und zugleich ein zentrales Monitoring über alle wichtigen Ebenen bietet. Durch den großen Einfluss des OT-Bereichs auf den IT-Alltag muss das Unternehmen seine Strukturen und Ansätze immer wieder neu überdenken, um den steigenden Anforderungen der Digitalisierung zu entsprechen. Die zunehmende Gefahr durch moderne Cyberattacken machte eine Anpassung der Kommunikationskanäle noch einmal dringender und erhöht zudem die Notwendigkeit einer Reaktion und Überwachung auch außerhalb der Geschäftszeiten. Eine Herausforderung, die ebenfalls im Zusammenhang mit dem Abschluss einer Cyberversicherung essenziell war.

Die Lösung

Zu Beginn der Modernisierung führte das IT-Team zusammen mit IT-Partner H&G und Sophos eine komplette Systemanalyse durch, bei der alle eingesetzten Sicherheitslösungen auf den Prüfstand gestellt und bewusst der gedankliche Wechsel von traditionellen IT-Sicherheitsarchitekturen hin zu modernen Strategien vorgenommen wurde. Die Analyse machte schnell klar, dass die immer schnellere Entwicklung im

Bereich der Digitalisierung, die zudem durch die umfangreichen OT-Systeme noch einmal auf ein höheres Level gehoben wird, nur durch ein flexibel erweiterbares Sicherheitssystem inklusive zentraler Steuerung in den Griff bekommen werden kann.

Um den zunehmenden Cyberbedrohungen wirksam entgegenzuwirken, empfahlen die IT-Experten als zusätzlichen Bedrohungsschutz Sophos MDR einzusetzen. Aufbauend auf dem bestehenden Schutz 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. Der MDR-Service von Sophos bietet Organisationen ein 24/7 verfügbares Sicherheitsteam, das gezielte Maßnahmen ergreift, um selbst hochkomplexe Bedrohungen zu neutralisieren.

„Sophos hat uns aufgrund der einfachen Verwaltung und hohen Sichtbarkeit überzeugt. Das zusammen mit dem super effizienten MDR-Service realisiert für uns eine sichere IT-Infrastruktur."

Gino Link
Leiter IT

Das Ergebnis

Allen voran hat die IT-Security-Abteilung nach der Umstellung eine ganz neue Sichtbarkeit über ihre Systeme und kann diese zentral managen. Auch der Arbeitsaufwand für das IT-Team hat sich aufgrund der effektiven Funktionsweise und Homogenisierung der Sophos-Produkte stark verringert. Die Konsolidierung in Sachen Administration und Monitoring über die zentrale Plattform Sophos Central entlastet die Mitarbeiter entscheidend – bei gleichzeitig besserer Überwachung und leichterer Auswertung der eingehenden Sensorik.

Aufgrund der intuitiven Managementfunktionen und Unterstützung durch H&G erfolgte die Migration auf die neue Lösung ohne große Ausfallzeiten und stellte zu jeder Zeit einen sicheren Betrieb von Produktion, Hotellerie und Gastronomie sicher.

Last but not least konnten aufgrund des eingeführten MDR-Services neben einer für die IT-Mitarbeiter sehr beruhigenden 24/7-Überwachung durch Threat-Hunting-Experten auch die Voraussetzungen für den erfolgreichen Abschluss der anvisierten Cyberversicherung erfüllt werden. Das externe SOC-Team von Sophos kann im Bedrohungsfall sofort eingreifen – rund um die Uhr und an 365 Tagen im Jahr. Mit dem neuen System kann das IT-Team zudem auf eine deutlich bessere und höhere Informationsdichte und Telemetrieanalyse zugreifen und somit fundiert Entscheidungen in Sachen Cybersicherheit treffen.

Der Partner

H&G Hansen und Gieraths EDV Vertriebsgesellschaft mbH

Die H&G Hansen & Gieraths EDV Vertriebsgesellschaft mbH ist ein bundesweit tätiges, familiengeführtes IT-Systemhaus mit Sitz in Bonn. Seit 1986 unterstützt H&G Unternehmen und öffentliche Auftraggeber bei der Analyse, Planung, Implementierung und Absicherung moderner IT-Systeme. H&G bietet ganzheitliche Lösungen für digitale Arbeitsumgebungen, Business Continuity und die sichere Transformation von Geschäftsprozessen.

Dabei ist Informationssicherheit ein zentraler Bestandteil der Unternehmensstrategie: H&G betreibt ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheits-managementsystem (ISMS), das alle Standorte und Prozesse umfasst. Mit ganzheitlichen IT-Security-Lösungen und Managed Services von Firewall über Endpoint-Schutz bis Secure Printing sorgt H&G für widerstandsfähige, sichere IT-Infrastrukturen – zuverlässig und zukunftsorientiert.

Mehr Infos unter www.hug.de

Mehr Informationen unter www.sophos.de

2025-12-18 CCS-DE (NP) CRE-4071