Sicher in die mobile Zukunft mit Sophos

Als größter Mobilitätsclub Österreichs deckt der ÖAMTC vielfältige Aufgabengebiete ab und arbeitet entsprechend mit einer sehr heterogenen Systemlandschaft. Umso wichtiger ist die kompetente Absicherung dieses Systems gegen Cyberangriffe, in dessen Rahmen die Implementierung einer flexiblen und zugleich ausbaufähigen IT-Sicherheitsstrategie eine zentrale Rolle spielt. Sophos ermöglicht den effektiven Schutz der Endpoints als „Last Line of Defense" und realisiert mit seinem XDR-Angebot gleichzeitig einen weiteren wichtigen Wunsch der IT-Abteilung: möglichst viele Angriffsszenarien automatisch zu erkennen und damit Attacken verhindern zu können – und das, ohne das Team zusätzlich zu belasten.

Auf einen Blick

ÖAMTC

ÖAMTC - Österreichischer Automobil-, Motorrad- und Touring Club

Branche
Service

Webseite
www.oeamtc.at

Anzahl der Nutzer
3.200

Sophos-Partner
JT-Computer

Sophos-Produkte
Sophos Intercept X with XDR (Endpoint und Server)

„Sophos hat uns mit seinem Gesamtpaket überzeugt: Stabilität, ein hoher Schutzgrad und die zentralen Management-Features machen den Unterschied zur Konkurrenz aus.“

Christoph Pertl, IT Security Officer

Der ÖAMTC ist der größte Mobilitätsclub Österreichs und arbeitet aktiv in einem weltweiten Netz von Mobilitätsclubs mit. Er ist ein wirtschaftlich und parteipolitisch unabhängiger Verein. Für den ÖAMTC steht die Dienstleistung für seine 2,4 Millionen Mitglieder im Mittelpunkt: Der Club ist Ansprechpartner in allen Fragen rund um Mobilität – im Alltag wie in Notsituationen – und Förderer der Interessen seiner Mitglieder. Unter dieser Prämisse sind rund 4.000 Mitarbeitende im Einsatz für Menschen und Mobilität.

Die Herausforderung

Der ÖAMTC hat durch seine föderale Struktur und vielfältigen Aufgabengebiete eine sehr heterogene Systemlandschaft. In der Folge sind viele unterschiedliche Geräte und IT-Systeme im Einsatz, um den Anforderungen eines umfassenden Serviceleisters gerecht zu werden. Entsprechend wichtig ist die kompetente Absicherung dieses Systems gegen Cyberangriffe, in dessen Rahmen die Implementierung einer flexiblen und zugleich ausbaufähigen IT-Sicherheitsstrategie eine zentrale Rolle spielt. Primäres Ziel war deshalb, den Endpoint als „Last Line of Defense“ mit effektiven Tools auszustatten, eine gute Visibilität zu erhalten und bei einem Sicherheitsvorfall schnell und effizient Maßnahmen einleiten zu können. Zweiter Fokus lag darauf, möglichst viele Angriffsszenarien bereits automatisch zu erkennen und damit zu gewährleisten, potenzielle Attacken schon im Keim zu ersticken. Außerdem musste die Lösung nicht nur verschiedene Betriebssysteme unterstützen, sondern auch unterschiedlichste Deployments wie klassische Endpoints, Server, Terminalserver oder VDI sowie den Einsatz in virtualisierten Umgebungen ermöglichen.

Die Lösung

Aufgrund dieser Ziele zur Neuausrichtung der IT-Security-Strategie und den langjährigen, guten Erfahrungen mit Sophos entschied sich der ÖAMTC zusammen mit seinem IT-Partner JT-Computer für Sophos Intercept X with XDR zum Schutz seiner Endpoints und Server. Die Lösung erfasst neben Endpoint- und Server-Informationen auch Netzwerk-, E-Mail-, Cloud- und mobile Datenquellen und liefert mit diesem umfassenden Bild der aktuellen Cybersicherheitslage im Unternehmen die Lösung für eine zentrale Anforderung der IT-Security-

Strategie. Zudem werden dank Machine Learning verdächtige Ereignisse erkannt und entsprechend ihrer Dringlichkeit fortlaufend priorisiert. Darüber hinaus bietet die Lösung weiterführende Cyber-Security-Funktionen zur automatischen Erkennung, Analyse und Reaktion auf potenzielle Sicherheitsbedrohungen und kann auf die Expertise der Sophos X-Ops-Experten bauen. Dies ermöglicht eine deutliche Verringerung des Workloads, denn je mehr Bedrohungen durch XDR abgewehrt werden, desto weniger Vorfälle müssen vom IT-Administrator untersucht werden.

Das Ergebnis

Mit der Einführung von Sophos Intercept X with XDR in Kombination mit Sophos Central konnte die IT-Abteilung des ÖAMTC den administrativen Aufwand in Sachen IT-Sicherheit stark reduzieren und gleichzeitig eine bessere Schutzwirkung aufgrund der zusätzlichen Funktionen wie zum Beispiel der gezielten Analyse oder der beschleunigten Reaktion auf Vorfälle realisieren. Der unkomplizierte Rollout im Hintergrund lief ohne die aktive Interaktion mit den Nutzer:innen ab und konnte damit ohne Beeinträchtigung des Tagesgeschäfts abgeschlossen werden. Entscheidend verbessert werden konnten zudem die Verwaltung des Systems und das Threat Hunting aufgrund der Sophos Central Plattform mit seiner übersichtlichen und performanten Oberfläche. „Sophos hat uns mit seinem Gesamtpaket überzeugt: Stabilität, ein hoher Schutzgrad und die zentralen Management-Features machen den Unterschied zur Konkurrenz aus“, so das Fazit von IT Security Officer Christoph Pertl

JT COMPUTER SOFTWARE & HARDWARE

JT-Computer

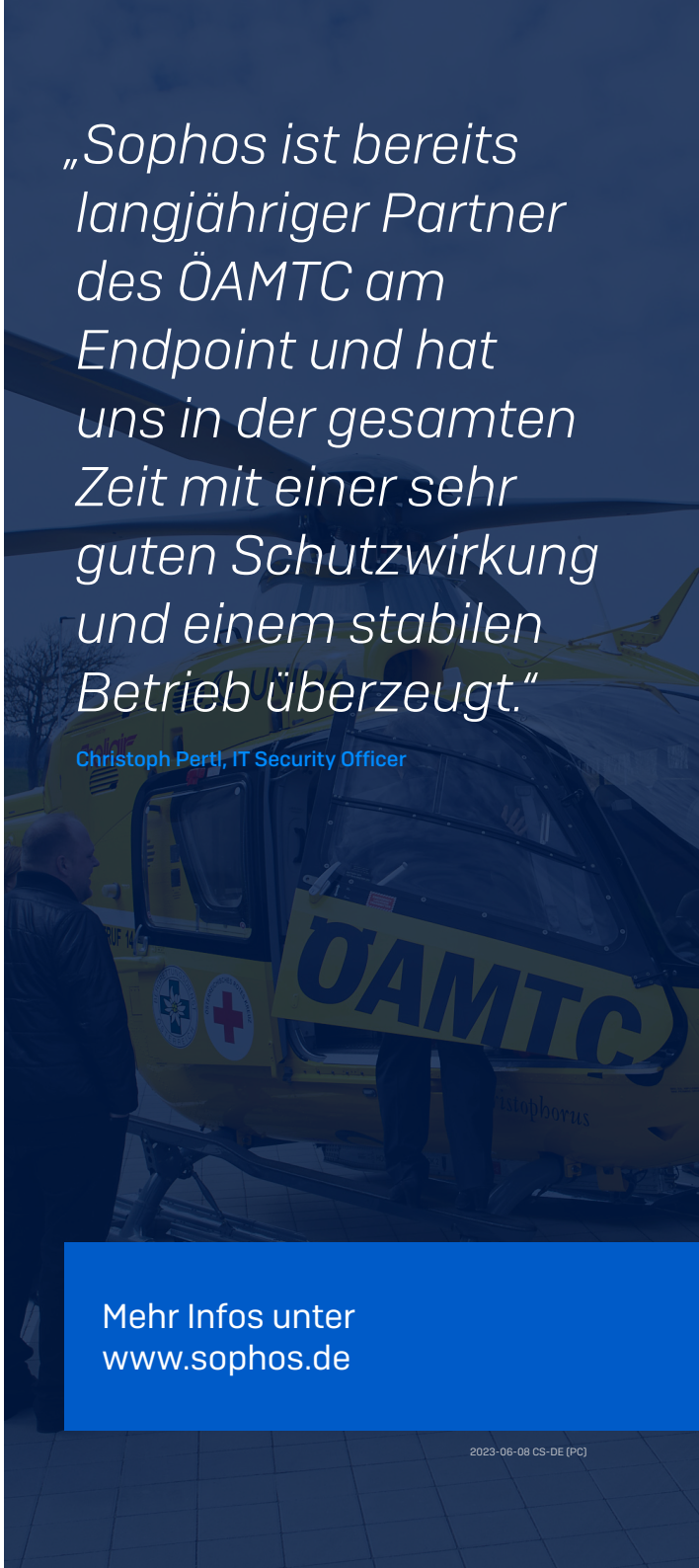
Gemäß der Firmenphilosophie pflegt JT-Computer eine starke Kunden- und Marktnähe und bietet bereits seit über 30 Jahren Individuelle IT-Lösungen im Privat- wie auch im Unternehmensbereich. Die eigene Reparaturwerkstatt garantiert den Kunden zusätzlich eine rasche Serviceabwicklung, eines der vielen Alleinstellungsmerkmale des Unternehmens.

Was 1989 als kleines Familienunternehmen begann, ist heute ein Vorzeigeunternehmen mit 12 Mitarbeitern und vielen Top-Kunden und Partnern. Das Erfolgsrezept ist dabei, funktionierende Lösungen zu optimalen Kosten mit zuverlässigem Service anzubieten – inklusive einer großen Flexibilität, um Trends auf dem Markt rasch umsetzen zu können.

SOPHOS

„Sophos ist bereits langjähriger Partner des ÖAMTC am Endpoint und hat uns in der gesamten Zeit mit einer sehr guten Schutzwirkung und einem stabilen Betrieb überzeugt.“

Christoph Pertl, IT Security Officer



Mehr Infos unter
www.sophos.de

2023-06-08 CS-DE (PC)