STUDIOSUS REISEN SCHÜTZT SENSIBLE DATEN MIT INDEVIS SOC AS A SERVICE

Als Anbieter von hochwertigen Studienreisen muss Studiosus täglich sensible Kundendaten mit Partnern auf der ganzen Welt austauschen. Eine besondere Herausforderung sind dabei die Legacy-Buchungssysteme, die in der ganzen Reisebranche zum Einsatz kommen. Um Cyberbedrohungen schnell zu erkennen, setzt Studiosus auf Google SecOps und indevis SOC as a Service (SOCaaS).

Ob die Kulturschätze der Toskana entdecken, den Wüstenwind Marokkos in den Haaren spüren oder buddhistische Tempel in Nepal erkunden: Wer mit Studiosus verreist, sammelt unvergessliche Erlebnisse. Das Münchner Familienunternehmen, das 1954 mit einer Bustour durch den Balkan startete, ist heute der führende europäische Anbieter von Studienreisen. 1.000 Routen in über 100 Ländern stehen aktuell im Programm. Neben der Kernmarke zählen auch die Töchter Studiosus Gruppenreisen, Marco Polo Reisen und Hauser Exkursionen zur Unternehmensgruppe. Markenzeichen von Studiosus sind nicht nur die hochqualifizierten Reiseleiterinnen und Reiseleiter, sondern auch ein exzellentes Sicherheits-Management. Dr. Frank Miedreich, Head of IT bei Studiosus erklärt: „Neben der Sicherheit auf Reisen rückt für uns die Cybersicherheit immer mehr in den Fokus. Wir möchten hier dieselben hohen Maßstäbe ansetzen wie bei unseren Reisen und wollten unser Security-Profil daher schärfen."

HOHER SCHUTZBEDARF IN DER REISEBRANCHE

Als Reiseveranstalter muss Studiosus Daten mit einer Vielzahl von Partnern auf der ganzen Welt austauschen, sei es mit Hotels, Busunternehmen oder Flug-gesellschaften. Wie fast alle Organisationen in der Branche nutzt das Unternehmen dafür die einschlägigen und seit Jahrzehnten etablierten Buchungs- und Flugreservierungssysteme. Über diese Tools werden hochsensible personenbezogene Daten der Gäste übermittelt, denen besonderer Schutz zukommen muss: Wenn es Cyberkriminellen z. B. gelingen würde, eine Flugbuchung mitzulesen, könnten sie nicht nur Zahlungsdaten abgreifen. Sie würden auch erfahren, wo eine Person wohnt, wo sie hinfliegt, wie lange sie abwesend ist und ob sie gegebenenfalls gesundheitliche Einschränkungen hat. Das sind kritische Informationen, die sich hervorragend für kriminelle Machenschaften ausnutzen lassen. Um böswilligen Akteuren keine Angriffsfläche zu bieten, setzt Studiosus hier auf höchste Sicherheitsstandards und kontinuierliche Verbesserungen.

EXPERTE FÜR URLAUB SUCHT EXPERTE FÜR CYBERSECURITY

Um sensible Daten zu schützen, beschloss Studiosus, ein SIEM (Security Information and Event Management) einzuführen und die IT-Umgebung mit einem modernen Security-Monitoring zu überwachen. Dafür suchte das Unternehmen nach einer geeigneten Lösung und einem kompetenten Partner. „Wir sind Experten für Urlaub, nicht für Cybersicherheit", erklärt Dr. Frank Miedreich. „Es wäre für uns ein riesiger Invest gewesen, uns selbst in das Thema Security Operations Center (SOC) einzuarbeiten. Die Kollegen von Google haben uns dann indevis empfohlen." Studiosus arbeitet bereits seit einiger Zeit erfolgreich mit Google zusammen und ist gerade dabei, die IT-Infrastruktur mit Google Cloud Platform (GCP) zu modernisieren. Daher nahm das Unternehmen die Empfehlung gerne an und traf sich mit den Münchner Security-Spezialisten. „Wir haben uns von Anfang an gut beraten und verstanden gefühlt", so Dr. Miedreich. „indevis hat uns eine maßgeschneiderte Lösung präsentiert, mit der wir uns gut aufgehoben fühlen. Als Familienunternehmen streben wir außerdem eine langfristige, stabile Zusammenarbeit an. Mit indevis stimmt einfach die Chemie."

MASSGESCHNEIDERTE LÖSUNG AUS CLOUD-SIEM UND MANAGED SERVICE

Studiosus entschied sich für den Managed Security Service indevis SOC as a Service (SOCaaS). Technisches Herz ist die Cloud-native Plattform Google SecOps, die eine

Studiosus

ECKDATEN

Kunde: Studiosus Reisen
Branche: Tourismus
Hauptsitz: München
Mitarbeiterzahl: ca. 290
Umsatz 2024: 259.170.000 Euro

PROJEKT UND VORTEILE

+ indevis SOCaaS auf Basis der Cloud-nativen Plattform Google SecOps (früher Google Chronicle)
+ Anbindung von Logdatenquellen in einer heterogenen, hybriden IT-Landschaft
+ Absicherung von Legacy-Systemen durch maßgeschneidertes, kontinuierliches Security-Monitoring
+ Schnelle, präzise Bedrohungs-erkennung, die individuell auf die speziellen Anforderungen von Studiosus zugeschnitten ist
+ Kontinuierliche Beratung zur weiteren Optimierung der Security

indevis GmbH
Koppstraße 14
81379 München

Tel. +49 (89) 45 24 24-100
Fax +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de

„indevis hat unsere Cybersecurity auf ein neues Level gebracht, sodass ich nachts ruhig schlafen kann. Ich muss mir keine Sorgen mehr machen, dass sensible Kunden- und Unternehmens-daten gefährdet sind."

Dr. Frank Miedreich, CIO bei Studiosus

ÜBER DIE INDEVIS GMBH

Die ISO 27001 zertifizierte indevis GmbH mit Sitz in München bietet seit 1999 IT-Sicherheits-, Datacenter- und Netzwerklösungen, flankiert von professionellen Consulting-, Management- und Support-Dienst-leistungen. Dabei erfüllt indevis sowohl die Anforderungen der Wirtschaft als auch die von öffentlichen Behörden und Hochschulen.

Als einer von Deutschlands führenden Managed Security Service Providern ist indevis der Partner für IT Security und Netzwerktechnik für Unternehmen jeder Größe und Branche – denn IT-Sicherheit muss strategisch geplant werden.

Dabei ist indevis nicht nur in München und Umgebung vertreten: Unsere Mitarbeiterinnen und Mitarbeiter sind an Standorten in ganz Deutschland aktiv.

indevis
Sicherheit in einer vernetzten Welt

SIE WOLLEN MEHR ERFAHREN?

Unsere Experten beraten Sie gerne und unterstützen auch Sie dabei, Ihre Cybersicherheitsstrategie zu optimieren. Kontaktieren Sie uns:

+49 (89) 45 24 24-100
sales@indevis.de
www.indevis.de

TÜV SÜD ISO 27001

kosteneffiziente, leistungsfähige SIEM-Lösung mit SOAR-Funktionalität (Security Orchestration, Automation and Response) bietet und Security-Prozesse automatisieren kann. In einen Cloud-Data-Lake fließen die Logdaten aller angeschlossenen Systeme ein, werden korreliert und KI-unterstützt analysiert. Google stellt die SecOps-Plattform als SaaS bereit. Das indevis-SOC-Team überwacht die Warnmeldungen, führt tiefere Security-Analysen durch und verständigt Studiosus sofort, wenn etwas Kritisches auffällt.

EIN SORGFÄLTIGES ONBOARDING IST ENTSCHEIDEND

In einem Kick-off-Meeting klärte indevis zentrale Fragen: Welche Logdatenquellen von Studiosus müssen angebunden werden? Was sind die wirklich geschäfts-kritischen Systeme, auf die das SOC-Team besonders achten sollte? Wie ist die Netzwerkarchitektur aufgebaut und wie arbeitet Studiosus? All diese Faktoren spielen eine wichtige Rolle, um Bedrohungen zuverlässig zu erkennen. Wenn z.B. Netzwerkzugriffe von ungewöhnlichen Orten zu ungewöhnlichen Zeiten erfolgen, könnte das ein Hinweis für einen Cyberangriff sein. Außerdem definierten die Partner die Meldewege: Wer soll bei welcher Kritikalitätsstufe verständigt werden? Wer ist außerhalb der Geschäftszeiten zu benachrichtigen?

ANBINDUNG DER HETEROGENEN LOGQUELLEN

Bei der Anbindung der Logquellen war die Mitarbeit des internen IT-Teams gefragt: Es musste die Daten bereitstellen und Firewall-Regeln anpassen, damit die Verbindung zur SIEM-Plattform hergestellt werden konnte. Mit Unterstützung von indevis gelang es Studiosus, diese Hürde zu meistern. Im nächsten Schritt kümmerten sich die Security-Spezialisten um die Integration der Daten in Google SecOps. Dabei koordinierten sie sich auch mit den SAP- und GCP-Dienstleistern von Studiosus. Eine besondere Herausforderung bestand in der heterogenen, hybriden Systemlandschaft, die neben 40 Jahre alten Legacy-Systemen auch moderne Cloud Services umfasst. Während sich Letztere einfach über APIs in Google SecOps einbinden lassen, musste indevis für die bestehende Endpoint-Security-Lösung WithSecure (früher F-Secure) eigens einen Parser entwickeln. Dieser übersetzt die Daten, sodass die SIEM-Plattform sie versteht und auswerten kann.

ANPASSUNG DES REGELWERKS AN INDIVIDUELLE ANFORDERUNGEN

Eine weitere Herausforderung bestand in der Anpassung der automatisierten Prüfprozesse, anhand derer die SecOps-Plattform Bedrohungen erkennt. indevis stimmte dieses Regelwerk genau auf die Studiosus-Umgebung ab. Zur Absicherung der Legacy-Systeme mussten u.a. spezielle Prozesse entwickelt werden. Außerdem führte indevis ein Finetuning durch, um die Zahl der Fehlalarme zu minimieren und die Bedrohungserkennung zu präzisieren. Denn anfangs gab das SIEM viele Standard-Warnmeldungen aus, die aber im Studiosus-Kontext harmlos waren. Nach drei Monaten Feinjustierung konnte der SOC as a Service schließlich in den Regelbetrieb übergehen.

GESCHÄFTSKRITISCHE SYSTEME SIND GESCHÜTZT – UND ES GEHT WEITER

Die wichtigsten Logquellen sind jetzt angebunden, die noch fehlenden folgen in Kürze. Dr. Frank Miedreich ist zufrieden: „indevis hat unsere Cybersecurity auf ein neues Level gebracht, sodass ich nachts ruhig schlafen kann. Ich muss mir keine Sorgen mehr machen, dass sensible Kunden- und Unternehmensdaten gefährdet sind." Die geschäftskritischen Systeme von Studiosus werden jetzt kontinuierlich überwacht und die Bedrohungserkennung permanent an neue Anforderungen angepasst. Außerdem beraten die Security-Spezialisten auch über den SOC as a Service hinaus, weisen auf Sicherheitsprobleme hin und geben zum Beispiel Tipps zum Umgang mit Schwachstellen. In wöchentlichen Meetings tauscht sich das indevis SOC-Team mit dem internen IT-Team aus.

Künftig will Studiosus die Zusammenarbeit mit indevis weiter ausbauen, so Dr. Miedreich: „Die Bedrohung durch Cyberangriffe wächst. Daher müssen wir auch in der Cybersecurity immer besser werden und die Informationssicherheit zum fundamentalen Baustein der IT-Architektur machen. Bei allem, was wir in der IT ändern oder neu entwickeln, müssen wir die Sicherheit mitdenken. Daher möchte ich indevis von Anfang an beratend hinzuziehen."