ANWENDERBERICHT

Hochleistungs-SIEM als Service

noris network

Die noris network AG mit Hauptsitz in Nürnberg bietet ihren Kunden maßgeschneiderte ITK-Lösungen in den Bereichen IT-Outsourcing, Managed Services, Cloud Services und Colocation. Ihr Primärgeschäft besteht im Aufbau und Betrieb von Hochsicherheitsrechenzentren, darunter auch die Rechenzentren Nürnberg Süd und München Ost, die zu den modernsten und energieeffizientesten Rechenzentren Europas zählen. Vor allem anspruchsvolle Kunden aus der Finanzbranche und Unternehmen, die großen Wert auf IT-Sicherheit legen, nehmen die Leistungen von noris in Anspruch. Sie ist nach ISO 20000-1, ISO/IEC 27001 und ISO 9001 zertifiziert und bietet für ihre Rechenzentren die höchsten Sicherheits- und Schutzklassen. Das inhabergeführte Unternehmen wurde 1993 gegründet und hat heute zirka 350 Mitarbeiter. 2018 betrug der Umsatz 70 Millionen Euro.

Bereits seit Langem sammelt noris Daten zur Performance, Ressourcen-Verbrauch und Security in ihren Rechenzentren. Deshalb hatte sie schon immer damit geliebäugelt, auch ein eigenes Security Information and Event Management System (SIEM) aufzubauen, um Daten zusammenführen und intelligent auszuwerten. Sie wollte das SIEM nicht nur selbst nutzen, sondern auch ihren Kunden als neuen Service anbieten.

Auf der Suche nach der besten Lösung

Zunächst evaluierte noris zahlreiche Lösungen. Sie hatte dabei hohe Anforderungen. Das System sollte mandantenfähig sein und sich verteilt betreiben lassen. Verschiedene Log-Quellen und externe Systeme wie Sandboxing und Antivirus sollten sich schnell und zuverlässig einbinden lassen. Außerdem wollte noris gerne auch eigene Parser nutzen, und Daten sollten in Reinform im RAW-Format verfügbar sein. Im Hinblick auf die DSGVO war wichtig, dass personenbezogene Daten anonymisiert werden können. Darüber hinaus spielte auch das Preis-Leistungsverhältnis eine Rolle, und wie schnell und einfach sich das System bereitstellen und automatisieren lässt. Am Ende entschied man sich für FortiSIEM von Fortinet. Michael Ibe, Team Leader SOC bei noris, erklärt: „FortiSIEM hat uns in allen Punkten überzeugt. Dazu kommt, dass die Lösung dank des Security-Fabric-Konzepts von Fortinet reibungslos mit vielen Perimeter-Systemen zusammenarbeitet. Nicht umsonst stammen 85 Prozent der Perimeter-Systeme, die wir an unsere Kunden verkaufen, von Fortinet.“

“FortiSIEM bietet genau das, was wir brauchen: eine schnelle und zuverlässige Einbindung von Log-Quellen, Mandantenfähigkeit und Anonymisierung von Daten. Wir können eigene Parser schreiben und Reports automatisiert generieren. Zudem arbeitet die Lösung dank des Security-Fabric-Konzepts reibungslos mit vielen Perimeter-Systemen zusammen.”

– *Michael Ibe,*
Team Leader SOC bei noris

Eckdaten

Kunde: noris network AG

Branche: IT-Dienstleister

Standort: Nürnberg

Gründliche Vorbereitung – Deployment in einer Woche

noris erwarb eine FortiSIEM Subscription mit 20.000 EPS (Events per Second). Die Einführung begann mit einer gründlichen organisatorischen Vorbereitung. Zunächst ermittelten die Spezialisten, welche Log-Quellen die wichtigsten Informationen liefern – etwa Firewalls, VPN-Konzentratoren, Authentifizierungssysteme und diverse Linux- und Windows-Server. Anschließend klärten sie mit der Rechtsabteilung und der Personalabteilung, wo es gesetzliche Vorgaben oder Compliance-Richtlinien gab. Gemeinsam mit dem Betriebsrat und der Geschäftsleitung wurden entsprechende Betriebsvereinbarungen mit Geheimhaltungsklauseln und Zusatzvereinbarungen entwickelt, etwa im Hinblick auf Pentesting und das Erfassen von personenbezogenen Daten.

In der nächsten Phase sah sich noris noch einmal alle benötigten Log-Quellen im Detail an und prüfte, ob das Konzept schlüssig war oder ob Informationen fehlten. Dann ging es an die Planung der Infrastruktur. Dabei arbeiteten zwei Fach-Teams zusammen: Das Netzteam ermittelte, welche Komponenten erforderlich waren und welche IP-Range man abdecken wollte. Das Security-Team legte die nötigen Firewall-Freischaltungen fest. Nachdem die Änderungen vom unternehmenseigenen Change Advisory Board genehmigt waren, baute noris die Infrastruktur auf. Da alles virtualisiert sein sollte, waren auch die Spezialisten der VMware-Farmen beratend involviert. Die eigentliche Bereitstellung von FortiSIEM erfolgte dann innerhalb von einer Woche.

Schnellere Analyse und einfache Anbindung von Kunden

noris hat nun alle wichtigen Daten aus verschiedenen Quellen in einem zentralen System im Blick. Michael Ibe freut sich: „Wir sind viel schneller geworden bei der Analyse von Problemen und sehen sofort, ob ein System gefährdet ist. Außerdem hilft uns FortiSIEM, Fehlkonfigurationen und Lücken in Prozessen aufzudecken. Dadurch können wir nachjustieren und unsere Infrastruktur noch sicherer machen."

Dank FortiSIEM kann der IT-Dienstleister seinen Kunden jetzt SIEM als Shared Service und Managed Service als eigenständige noris-Produkte anbieten. Im Shared-Modell profitieren alle – ob Großkonzern oder kleiner Mittelständler – von denselben leistungsfähigen SIEM-Funktionen. Jeder kann selbst entscheiden, wie viele EPS er buchen und welche seiner Datenquellen er anbinden möchte. Alles, was der Kunde benötigt, erhält er mit einer Device-Lizenz. Sie umfasst sowohl die SIEM-Plattform als auch die Wartung. Unternehmen müssen sich also nicht um Einzellizenzen für Indicators of Compromise oder Ressourcen auf der VMware-Farm kümmern.

Entscheidet sich ein Kunde für SIEM als Managed Service, übernimmt noris auch die komplette Risikoanalyse und Bewertung der Findings. Sie erstellt Berichte, überwacht das System rund um die Uhr und alarmiert den Kunden unmittelbar, falls ein Sicherheitsvorfall eintritt.

Ein Türöffner für neues Geschäft

Derzeit ist noris damit beschäftigt, die vorhandenen Daten noch mit Mikrodaten aus zusätzlichen Datenquellen anzureichern, um externe und interne Sichtweisen miteinander zu verbinden. Außerdem geht es ans Finetuning, um die Incident-Bearbeitung zu optimieren: Daten werden aufbereitet, Unschärfen und False Positives bereinigt und Parser angepasst oder neu geschrieben. Künftig möchte der IT-Dienstleister die Orchestrierung und Automatisierung im Bereich Security noch stärker vorantreiben.

Mit FortiSIEM ist noris für die Zukunft gerüstet. Außerdem fungiert die Lösung als Türöffner, um neues Geschäft zu generieren. Durch die enge Partnerschaft mit Fortinet entstehen Synergien, sodass Fortinet Kunden, die sich für ein Shared SIEM oder Managed SIEM interessieren, auch gerne einmal an noris weiter verweist.

Business Impact

- Zentraler Blick auf alle wichtigen, sicherheitsrelevanten Daten
- Schnelle und einfache Bereitstellung und Automatisierung
- Schnelle Analyse von Vorfällen und Aufdecken von Fehlkonfigurationen
- Mandantenfähige Lösung ermöglicht neue Geschäftschancen

Lösungen

- FortiSIEM Subscription mit 20.000 EPS

FORTINET

www.fortinet.de

November 26, 2019 4:06 PM

557202-0-1-DE

Sheldon:Fortinet:2019-11-557202-cs-Noris-Teal:cs-Noris-teal-A4