Mehr Sicherheit im Netzwerk mit Splunk

bluecue unterstützt die GASCADE auf dem Weg zur ISO 27001 Zertifizierung durch effiziente Datenauswertung in Splunk.

Die GASCADE Gastransport GmbH hat ihr gesamtes EDV-Netzwerk inklusive IT-Security neu aufgebaut. Als Betreiberin einer Kritischen Infrastruktur nach BSI-Kritisverordnung ist sie zudem verpflichtet, sich nach ISO-Norm für Informationssicherheits-management zu zertifizieren. Um den hohen Anforderungen gerecht zu werden, implementierte das Unternehmen Splunk Enterprise als Plattform für die Systemüberwachung und holte sich einen IT-Experten an Bord, der die Norm selbst schon erfüllt: die bluecue consulting GmbH & Co. KG.

„Für die ISO-Zertifizierung gibt man sich als Unternehmen selbst Compliance- und IT-Security-Richtlinien", erklärt René Golembewski, IT-Sicherheitsbeauftragter der GASCADE. „Der Auditor überprüft diese und schaut gleichzeitig, ob die Richtlinien eingehalten werden, wie, wann und wo sie geprüft und in welcher Form sie dokumentiert werden."

Um diese Anforderungen erfüllen zu können, ist ein guter Überblick über sämtliche Vorgänge in der IT-Struktur Voraussetzung. „Ich wollte wissen: Wie läuft meine Infrastruktur und was passiert in meinem Netzwerk?", erinnert sich Golembewski und installierte daraufhin zunächst die kostenlose Testversion von Splunk – eine Big-Data-Lösung, mit der große Datenmengen gesammelt, beobachtet und ausgewertet werden können. „Nach einer Woche hatte ich alle Gewerke, die mich zu der Zeit interessierten, in meinem Splunk, konnte sie grafisch auswerten und sehen, was vor meiner Haustür eigentlich passiert. Das ging wirklich schnell und einfach. Splunk ist sehr intuitiv."

bluecue für die Expertise

Doch für die ISO-Zertifizierung muss nicht nur die Bedrohungslage des Unternehmens analysiert werden: Wie ist das Spam-Aufkommen? Wer scannt das Unternehmen? Wer greift das Unternehmen an? Sind Trends erkennbar? „Es geht dabei auch um Berechtigungen in der IT-Infrastruktur", erklärt Denis Roehr, IT-Experte von bluecue. „Welcher Mitarbeiter darf worauf zugreifen und zu welchen Zeitpunkten? Über welche VPN-Verbindung wird auf das Netzwerk zugegriffen und welche Veränderungen werden durchgeführt?"

Um diese Informationen mit Splunk auswerten zu lassen, musste das gesamte Active Directory der GASCADE an die Monitoring-Lösung angeschlossen werden. „Dafür brauchten wir Hilfe von einem Experten", sagt Golembewski. „Denn obwohl Splunk generell sehr einfach zu bedienen ist, ist das sogenannte Data-Onboarding mitunter kompliziert. Dafür wurde uns bluecue als sehr guter deutscher Splunk-Partner empfohlen."

Gesagt, getan. Die Experten von bluecue schlossen das Active Directory an, erstellten die ersten Dashboards und sorgten dafür, dass in kürzester Zeit in Splunk sämtliche Informationen des User-, Access- und Identity-Managements abgebildet wurden und gleichzeitig gegen die selbstgesetzten Compliance- und IT-Security-Richtlinien geprüft werden konnten.

„Dadurch, dass bluecue selbst schon nach ISO 27001:2013 zertifiziert ist, wussten die Experten genau, auf welche Informationen im Active Directory es ankommt, und haben uns diese zielgenau beschafft", freut sich Golembewski über die gute und unkomplizierte Zusammenarbeit. Als Nächstes möchte er auch die Sicherheitslösung Kaspersky an Splunk anbinden und auswerten. Ein Projekt, bei dem bluecue die GASCADE ebenfalls unterstützen wird, denn die Rolle von bluecue ist „eine vollumfängliche Unterstützung bei allen Fragen zum Thema Splunk – architektonisch und betrieblich", so Golembewski.

Hohe Sicherheit in sicherheitskritischen Umgebungen

Die Vorgabe durch die Bundesnetzagentur zur ISO-Zertifizierung kommt nicht von ungefähr. Als Betreiber einer der größten

„Dadurch, dass bluecue selbst schon nach ISO 27001:2013 zertifiziert ist, wussten die Experten genau, auf welche Informationen im Active Directory es ankommt, und haben uns diese zielgenau beschafft. Es hat nicht lange gedauert, da hatten wir alles, was wir sehen wollten."

René Golembewski, IT-Sicherheitsbeauftragter der GASCADE

Erdgas-Infrastrukturen in Deutschland versorgt die GASCADE Verbraucher in ganz Mitteleuropa mit Erdgas. Die Gasbestellungen laufen dabei online, stundengenau, 24/7. „Anders als ein Atomkraftwerk, das nur Strom produziert, können wir uns nicht einmauern", erklärt Golembewski. „Unsere gesamte Vermarktungskette läuft über Internetanschlüsse bzw. eine europäische Kapazitätsplattform. Wir müssen also immer online sein und unsere Webserver sind von der ganzen Welt aus erreichbar." Das Unternehmen ist daher möglichen Angriffen von außen kontinuierlich ausgesetzt.

„Die Tatsache, dass wir durch Splunk sehr genau sehen können, was in unserem Netzwerk passiert, wer uns angreift, wo und durch wen Änderungen durchgeführt werden, hat für große Zustimmung auch auf Entscheiderebene gesorgt", resümiert Golembewski. „Deshalb werden wir nun nach und nach weitere Gewerke anschließen." Gleichzeitig hat das Unternehmen viele Veröffentlichungspflichten, denen dank Splunk ebenfalls leicht nachgekommen werden kann.

Eine Lösung, viele Vorteile

Für die GASCADE sind der Betrieb und das Monitoring der eigenen Infrastruktur noch relativ neu. Bis vor kurzem wurde die gesamte IT durch den Mutterkonzern BASF betrieben, musste jedoch aufgrund regulatorischer Vorgaben von dort entflochten werden. „Wir betreiben also jetzt die gesamte IT selbstständig und müssen dementsprechend auch für die IT-Sicherheit sorgen", so Golembewski. „Splunk war einfach eine ideale Lösung, um viele Vorgänge zu automatisieren und gleichzeitig dokumentieren zu können. Ich kann jetzt per Knopfdruck Berichte erstellen und zeigen, dass unsere Policies eingehalten werden. Ich kann unsere Performance analysieren oder das Management von externen VPN-Accounts nachvollziehen – und zwar sowohl in der Vergangenheit als auch live." Gerade in einer hochkomplexen und sicherheitskritischen Infrastruktur wie der von der GASCADE ist dieser Überblick wichtig.

Dass Splunk dabei so einfach einzuführen war, freut Golembewski besonders, aber auch, dass er die erfahrenen Splunk-Experten von bluecue an der Seite hatte. Denn: „Bei uns lief die Splunk-Einführung irgendwie immer nebenbei. bluecue hat aber dafür gesorgt, dass wir sämtliche Anforderungen schnell umsetzen konnten. bluecue hat somit eigentlich unser etwas ‚chaotisches' Projektmanagement in diesem Bereich unterstützt und uns professionell genau die Systemkomponenten implementiert, die wir brauchten."

GASCADE

Die GASCADE Gastransport GmbH ist ein Gemeinschaftsunternehmen von BASF und Gazprom und betreibt ein deutschlandweites Gasfernleitungsnetz. Die Netzgesellschaft mit rund 350 Mitarbeitern bietet ihren Kunden in Mitteleuropa hochmoderne und wettbewerbsfähige Transportdienstleistungen über das unternehmenseigene Hochdruckfernleitungsnetz von über 2.400 Kilometern Länge an.

GASCADE Gastransport GmbH
Kölnische Straße 108–112
34119 Kassel
Telefon: +49 561 934-0
kontakt@gascade.de, www.gascade.de

bluecue by acocon

bluecue Digital Strategies für mehr Spielräume, mehr Möglichkeiten, mehr Wertschöpfung: Collaboration Systems, Flexible Workplaces und IT-Management. bluecue consulting GmbH & Co. KG ist hervorgegangen aus dem Geschäftsbereich „Systems & Services" der acocon GmbH, Bielefeld. Die in 20 Jahren gesammelten Erfahrungen bei digitalen Dienstleistungen setzt bluecue seit Anfang 2013 als eigenständiges Unternehmen für anspruchsvolle Kunden aus der gesamten DACH-Region ein.

bluecue consulting GmbH & Co. KG
August-Schroeder-Straße 4
33602 Bielefeld
Telefon: +49 521 32 90 13-80
info@bluecue.de, www.bluecue.de