ECHTE SICHERHEITSVORFÄLLE SAUBER
IDENTIFIZIEREN UND ELIMINIEREN

Managed SIEM mit IBM QRadar für die Oldenburgische Landesbank

ConSecur
[security and consulting]

Sicherheitsvorfälle präzise von erlaubten Zugriffen unterscheiden

Die Oldenburgische Landesbank (OLB) hat das Management ihrer Informationssicherheit in die Hände der ConSecur GmbH gelegt. Analysten der ConSecur unterscheiden aus 10.000 Events pro Sekunde Sicherheitsvorfälle präzise von legitimen Ereignissen. Identifizierte Sicherheitsvorfälle lösen in der IT-Abteilung der Bank über das Ticketsystem eine definierte Aktionskette aus, sodass eine Eskalation schnell und strukturiert erfolgen kann. Durch diese Priorisierung von Vorfällen kann die Bank auf Sicherheitsvorfälle in Echtzeit reagieren und damit die Auswirkungen von Bedrohungen innerhalb ihrer kritischen Infrastruktur reduzieren.

Frank Feldmann, IT-Sicherheits- und Datenschutzbeauftragter bei der OLB: „Wir haben eine Struktur geschaffen, mit der wir echte Sicherheitsvorfälle sauber identifizieren und eliminieren können. Die Prozesse im Managed SIEM (Security Information and Event Management) sind so effizient abgestimmt, dass unsere IT-Abteilung und die Analysten der ConSecur Hand in Hand zusammenarbeiten."

Analysten unterscheiden aus 10.000 Events pro Sekunde Sicherheitsvorfälle und erlaubte Zugriffe

Ausgangssituation

Die im Jahr 2018 durch die Fusion der Oldenburgischen Landesbank (OLB AG) und der Bremer Kreditbank AG (BKB AG) entstandene Bank arbeitete mit einem Log-Management-Tool, das alle Vorfälle der im Netzwerk angebundenen Geräte, Endpunkte und Anwendungen protokollierte und speicherte.

Sämtliche Daten sind Frank Feldmann, IT-Sicherheits- und Datenschutzbeauftragter bei der OLB, und seinem Team in einem einfachen PDF-Report zur Verfügung gestellt worden, der mehrere tausend Seiten umfasst hatte.

Für die Korrelation der erhobenen Daten und die präzise Erkennung und Priorisierung von Sicherheitsvorfällen ist dieses Altsystem nicht ausgelegt gewesen.

Mit der Fusion gewann der Aufbau eines SIEM, das Sicherheitsvorfälle erkennt und priorisiert, an Dringlichkeit. Die OLB suchte einen externen Partner, der innerhalb kurzer Zeit eine neue SIEM-Lösung von Grund auf konzipiert, die Manpower für einen dauerhaften Betrieb besitzt und eng mit der hausinternen IT-Abteilung zusammenarbeitet. „Wenn wir ein SIEM erfolgreich umsetzen wollen, brauchen wir die personellen Ressourcen dazu", sagt Frank Feldmann.

Mit diesen Anforderungen suchte die OLB das Gespräch mit der ConSecur GmbH.


„Wir haben eine Struktur geschaffen, mit der wir echte Sicherheitsvorfälle sauber identifizieren und eliminieren können.“
„Uns ist schnell klar gewesen mit ConSecur einen kompetenten Partner für den Aufbau und den laufenden Betrieb eines SIEM zu haben.“
OLB BANK
FRANK FELDMANN, IT-SICHERHEITS- UND DATENSCHUTZBEAUFTRAGTER BEI DER OLB AG

Proof of Concept (PoC) – SIEM-Pilotierung innerhalb von 15 Tagen

Die Anforderungen an das neu zu konzeptionierende SIEM waren die schnelle Bereitstellung eines betriebsbereiten SIEM, die Skalierbarkeit der mit der Bank wachsenden Lösung sowie der operative Betrieb durch spezialisierte Fachkräfte.

Nach Analyse dieser Anforderungen unterbreitete ConSecur der OLB den Vorschlag, ein SIEM mit Security-Monitoring als Pilotprojekt aufzusetzen und die Leistungsfähigkeit des SIEM im laufenden Betrieb live zu demonstrieren. IBM QRadar Security Information and Event Management (SIEM) unterstützt Sicherheitsteams bei der präzisen Erkennung und Priorisierung von Sicherheitsbedrohungen. Das marktführende Tool erkennt IT-Sicherheitsvorfälle verlässlich und minimiert damit das Risiko von Sicherheitsbedrohungen für das Unternehmensnetzwerk.

„Mit der SIEM-Pilotierung konnten wir in einer auf die OLB angepassten Umgebung simulieren, wie das SIEM aufgebaut sein und das Security-Monitoring mit unseren Analysten in der Praxis ablaufen wird“, sagt Jens Wübker, Vertriebsleiter der ConSecur GmbH.

Innerhalb von 15 Tagen stellte ConSecur eine auf die OLB angepasste, betriebsbereite Managed SIEM Lösung vor, die

- die Architektur der SIEM Lösung (Produkte, Lizenzen, Prozesse, Rollen),
- zu überwachende individuelle Use Cases (Risikoszenarien),
- das empfohlene SIEM-Tool QRadar von IBM sowie
- ein arbeitendes Team aus professionellen Security Analysten und Incident Management

beinhaltete.

Der Proof of Concept überzeugten Frank Feldmann und sein Team, die ConSecur GmbH mit dem Aufbau eines SIEM zu beauftragen. „Uns ist schnell klar gewesen, mit ConSecur einen kompetenten Partner für den Aufbau und den laufenden Betrieb eines SIEM zu haben.“

„Uns hat die fokussierte Zusammenarbeit mit der OLB begeistert. Die schnelle Inbetriebnahme des SIEM ist gelungen, weil alle mit dem gemeinsamen Ziel vor Augen an einem Strang gezogen haben.“

STEPHAN ILIC,
CDC MANAGER DER
CONSECUR GMBH

„IBM QRadar ist eine sehr schnell einsetzbare Lösung und unsere erste Wahl, um Sicherheitsvorfälle verlässlich zu erkennen und damit das Risiko von Sicherheitsbedrohungen für Unternehmensnetzwerke zu minimieren.“

JENS WÜBKER,
SALES MANAGER DER
CONSECUR GMBH

SIEM-Umsetzung innerhalb einer Woche – Reduzierung der Lizenzkosten

Die Umsetzung des SIEM sollte in kürzester Zeit erfolgen. Innerhalb von einer Woche hat ConSecur das SIEM betriebsbereit aufgebaut und dabei 800 Log-Quellen wie Firewall, Server, Switche und bankspezifische Anwendungen angebunden und in das Monitoring integriert.

Durch diese neu angebundenen Log-Quellen stieg die Anzahl der Vorfälle (Events) pro Sekunde allerdings unerwartet deutlich an, sodass ConSecur zu einer Anpassung der Lizenzierung riet. Die OLB nutzte IBM QRadar bereits mit einer Lizenzierung nach Events pro Sekunde und folgte der Empfehlung ConSecurs, auf eine Lizenzierung nach virtuellen Servern umzustellen. Dies gelang durch die Verwendung von IBM Cloud Pak for Security.

IBM Cloud Pak for Security ermöglicht darüber hinaus den beliebigen Ausbau von einer SIEM-Lösung hin zu einer umfassenden SOC-Lösung unter Wiederverwendung von vorhanden Security-Tools und Vereinfachung von ganzheitlichen Security-Analysen.

Security-Analysten der ConSecur erkennen und priorisieren Sicherheitsbedrohungen 24/7 und erzeugen Tickets im Ticketsystem, wenn Sicherheitsvorfälle auftreten. Diese Tickets werden mit einer entsprechenden Priorisierung an die Mitarbeiter der IT-Abteilung der OLB weitergeleitet, die Gegenmaßnahmen einleiten.

Fazit – federführende, zielorientierte Umsetzung

Die Oldenburgische Landesbank besitzt eine skalierbare SIEM-Lösung, die Sicherheitsereignisse innerhalb der kritischen Infrastruktur zeitnah und angemessen überprüft.

Nach der Pilotierung und der schnellen Bereitstellung des SIEM haben die Analysten der ConSecur GmbH mit Managed SIEM den laufenden Betrieb übernommen.

„Mir hat sehr gut gefallen, wie ConSecur das Projektmanagement federführend und zielorientiert umgesetzt hat“, sagt Frank Feldmann.

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de