Co-Managed SIEM

Gemeinsam Cyber-Bedrohungen den Garaus machen

Ein Security Information and Event Management (SIEM) ist ein wirksames Tool, um die Cyber-Security zu erhöhen; doch für viele, gerade kleinere Unternehmen ist gerade das eine schier unüberwindbare Hürde. Denn Implementierung und Betrieb erfordern hohe Ressourcen: Budget, Zeit, aber auch Expertise, die nicht immer alle vorhanden sind. Hier greift der Ansatz des Co-Managed SIEM. Dabei wird das SIEM individuell mit einem Dienstleister aufgebaut, sodass Unternehmen flexibel entscheiden, welche Leistungen sie selbst erbringen können und welche sie extern managen lassen möchten.

Die Digitalisierung aller Unternehmenszweige schreitet unaufhaltsam voran. Im gleichen Maße steigt jedoch auch die Wahrscheinlichkeit von IT-Sicherheitsbedrohungen. Cyberkriminelle suchen unaufhörlich nach Sicherheitslücken in IT-Systemen und Netzwerken, um wertvolle Daten, sensible Firmeninterna oder vertrauliche Informationen abzugreifen. Ein SIEM (Security Information and Event Management) kann hier Schutz bieten: Es versetzt Unternehmen in die Lage, umfassend sicherheitsrelevante Daten zu sammeln, sie in einem zentralisierten Repository zusammenzuführen und anhand vorher definierter Use Cases automatisiert Auffälligkeiten und Regelverstöße zu erkennen. So kann das IT-Sicherheitsteam dank SIEM schneller auf Cyberbedrohungen aller Art reagieren. Denn die Zeit, die bis zur Identifizierung einer akuten Bedrohung benötigt wird, die Meantime to Detect, lässt sich deutlich reduzieren. Gerade bei kritischen Angriffen stellt dies einen entscheidenden Vorteil dar.

Allerdings: Vollständig inhouse umgesetzt, ist ein SIEM für Unternehmen kosten- und ressourcenintensiv und verlangt eine komplexe Verwaltung. Immense Datenmengen müssen von den internen IT Security-Spezialisten täglich ausgewertet werden. Oft fehlen Unternehmen die Ressourcen, die für den Aufbau und die Pflege eines SIEM unabdingbar sind - fachliche Expertise, technische Voraussetzungen oder die entsprechende Manpower. Die Lösung kann ein Co-Managed SIEM-Ansatz darstellen, bei dem ein SIEM in Zusammenarbeit mit einem externen Dienstleister realisiert wird. Der Dienstleister übernimmt zum Beispiel die Überwachung der SIEM-Meldungen, aktua-

lisiert die Lösung und stellt Berichte und Protokolle bereit. Idealerweise ist das Dienstleistungsportfolio modular aufgebaut und lässt sich flexibel an die Kundenanforderungen anpassen.

Die Vorteile des Co-Managed SIEM-Ansatzes

Ein teilweise oder vollständig extern gemanagtes SIEM bietet einige Vorteile. Denn je mehr Daten innerhalb eines Unternehmens generiert werden, desto komplexer gestaltet sich die Erkennung von aktuellen Bedrohungen. Jedes SIEM liefert zunächst mehr oder weniger qualifizierte Alarme: Die User – in der Regel SOC Analysten – müssen in der Lage sein, Warnmeldungen nicht nur zu überwachen, sondern auch zu bewerten und auf tatsächliche Bedrohungen angemessen zu reagieren. Ein externer Dienstleister kann das mit seiner Expertise oftmals professioneller leisten als die Inhouse-Mannschaft.

Eine weitere Herausforderung im Betrieb eines SIEM liegt in der Besetzung der verschiedenen Rollen: Von der Überwachung von Logquellen über die Entwicklung von SIEM Content bis hin zu Incident Response und Threat Hunting funktioniert die Technologie nur dann, wenn alle Positionen ideal besetzt sind und, einem Zahnrad gleich, ineinandergreifen. Von einem Unternehmen ist dies ohne die Unterstützung durch externe Cyber Defense Experten nur selten vollständig umsetzbar. Gerade in Betrieben, die nur über ein kleines IT-Sicherheitsteam verfügen, birgt ein internes SIEM-System außerdem die Gefahr von Kapazitätsengpässen: Denn damit der effiziente Einsatz des SIEM gelingt, müssen Netzwerke und Systeme rund um die Uhr und an 365 Tagen im Jahr überwacht werden. Mit einem Co-Managed SIEM lassen sich diese Aufgaben auslagern. Das eigene IT Security-Team hat dann genügend Freiraum, um schnell und effizient auf akute Probleme reagieren zu können.

Hinzu kommt: Ein internes SIEM kann je nach Unternehmensgröße Kosten im sechsstelligen Bereich produzieren. Mit der Anschaffung allein ist es nämlich nicht getan - danach muss das SIEM zeitnah in die IT-Architektur des Unternehmens implementiert werden. Schulungen und Trainings des SIEM Teams kosten Zeit und Geld und im Anschluß daran muss der stabile Betrieb mit Überwachung, Auslastung und Wartung gewährleistet sein. Ein extern gemanagtes SIEM limitiert diese initialen Kosten. Ausgaben für Schulungen, Wartungen und Sicherheitspatches entfallen sogar vollständig.

Den richtigen Partner für das Co-Managed SIEM auswählen

Durch die Zusammenarbeit mit einem externen Partner kann ein erstklassiges SIEM entstehen, wenn all diese Faktoren optimal bedient werden können. Bei der Auswahl sollten Unternehmen daher das Angebot des jeweiligen Cyber Defense Spezialisten genau unter die Lupe nehmen. Ganzheitlich ist es dann, wenn es die Bereiche Security Monitoring, Incident Response, Content-Entwicklung und -pflege sowie Plattformbetrieb und Logquellen-Überwachung abdeckt.

Im Rahmen des Security Monitoring führen die Cyber Defense Analysten des Dienstleisters die Analyse von IT-Sicherheitsvorfällen durch, qualifizieren diese und beraten den Kunden bezüglich passender Gegenmaßnahmen. Mit Hilfe des Threat Hunting werden die Logdaten auf Grund von internen oder externen Vorkommnissen bzw. basierend auf Indicators of Compromise (IOCs) oder erkannter Angriffe anderer Kunden geprüft. Wenn Security Incidents detektiert wurden, schließen sich die Qualifizierung der Vorfälle und Vorschläge für das Incident-Response-Team für Gegenmaßnahmen an. Der IT Security Spezialist SECUINFRA geht dabei in den Schritten Level 1- und Level 2-Analyse vor: Level 1 umfasst die Triage und Erstanalyse von SIEM-Alarmen sowie die Eliminierung von Fehlalarmen und Doppelmeldungen. Relevante Vorkommnisse werden an die Level 2-Analyse eskaliert. Hier erfolgt die detaillierte Analyse und Bewertung der detektierten Ereignisse. Eine Rücksprache mit den Verantwortlichen stellt eine klare Bewertung der Incidents sicher. Die daraus resultierenden Handlungsempfehlungen für das Incident Response Team schließen die Level 2-Analyse ab.

Die zweite, wichtige Säule ist die SIEM Content-Entwicklung und -pflege. Dazu definiert SECUINFRA die benötigten Use Cases abhängig vom Unternehmen und wählt diese aus seiner Use Case Library aus. Auch ihre individuelle Entwicklung mit Log-Policy, SIEM Regeln, Testroutinen und Runbook kann diese Säule umfassen. SECUINFRA hat zum Beispiel mehr als 200 Use Cases auf Basis des MITRE ATT&CK Frameworks entwickelt – die Cyber Defense-Experten erstellen dabei nicht nur die SIEM-Regeln für die einzelnen Use-Cases, sondern entwickeln auch die nötigen Vorgaben für besagte Log-Policy, Testroutinen und Runbooks. In der Folge werden die „End-to-End-SIEM Use-Cases“ implementiert, initial und später regelmäßig getestet und optimiert. Wichtig ist ebenso die kontinuierliche Pflege der Inhalte.

Last but not least sind ein professioneller Plattformbetrieb sowie die qualifizierte Logquellen-Überwachung die Voraussetzungen für einen reibungslosen SIEM-Betrieb. Zu Ersterem gehören unter anderem Release-Planungen, das heißt das Testen und Einspielen von Aktualisierungen, die Kontrolle der Verfügbarkeit der SIEM-Infrastruktur, Fehlerbehebung bei Softwareproblemen der Infrastrukturkomponenten sowie die regelmäßige Kontrolle des Lizenzvolumens. Die Logquellen-Überwachung stellt die Verfügbarkeit und die Qualität der angebundenen Logdaten sicher. Gegebenenfalls werden Anpassungen der Log-Policy durchgeführt oder die Eskalation an den Logquellen-Verantwortlichen übernommen.

Als ideal erweist es sich, wenn ein Partner wie SECUINFRA auch eine Incident Response anbietet: Damit ist er auch dann Ansprechpartner, wenn es tatsächlich zu einem IT-Sicherheitsvorfall kommt. Nachdem die kompromittierten IT-Systeme identifiziert wurden, schließen sich forensische Analysen zur Aufklärung des Tathergangs und zur Beweissicherung an sowie die Unterstützung zur schnellstmöglichen Wiederherstellung des IT-Betriebs.

Die notwendige Infrastruktur

Mit dem flexiblen Co-Managed SIEM-System von SECUINFRA können die benötigten Komponenten innerhalb des Kundennetzwerkes installiert und betrieben werden. Der Kunde stellt dafür die Betriebssystemplattform zur Verfügung, auf der das SIEM Expertenteam mittels Remote-Zugriff das SIEM-System installiert, konfiguriert und betreibt. Alternativ ist es aber auch möglich, dass der Kunde die Plattform eigenständig betreibt und nur durch einzelne Bausteine von SECUINFRA unterstützt wird. Dieses hybride Angebot ermöglicht es, dass die Services entweder vor Ort oder remote erbracht werden können.

Fazit

Ein SIEM-System kann die Zeit bis zur Entdeckung eines IT-Sicherheitsvorfalls maßgeblich verkürzen und die Cybersicherheit relevant erhöhen. Unternehmen mit kleinen Budgets und fehlenden Inhouse IT Security-Experten sind damit aus Gründen fehlender Ressourcen jedoch allein häufig überfordert. Hier kann ein hybrider Co-Managed SIEM-Ansatz flexibel helfen. Dieser erlaubt es, ein SIEM individuell und modular mit

Dienstleistungen nach dem Baukastenprinzip aufzusetzen und zu betreiben. Unternehmen entscheiden dann selbst, welche Leistung sie selbst erbringen und wofür sie externe Unterstützung benötigen. Fehlende Ressourcen und Expertise können so durch die Hinzunahme eines spezialisierten Partners ausgeglichen werden.

Autor: Ramon Weil, Geschäftsführer SECUINFRA

Weitere Informationen: https://www.secuinfra.com/de/services/co-managed-siem/

Pressekontakt:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0)30 5557021 11

sales@secuinfra.com