anykey
going beyond IT

Thomas Schwert

- Key Account Manager bei anykey GmbH
- Seit über 20 Jahren im IT Vertrieb tätig
- Zertifizierter Berater zur Krankenhausstrukturfonds-Verordnung (KHSFV)
- Erfahrungen aus erfolgreichen SIEM-Projekten

Security Information and Event Management: Ereignisse und Bedrohungen immer im Blick

SIEM-Lösungen wie IBM QRadar unterstützen IT-Manager bei der Erkennung, Priorisierung und Reaktion auf Bedrohungen im gesamten Unternehmen. Als integraler Bestandteil einer Zero-Trust-Strategie aggregiert und analysiert SIEM automatisiert die Protokoll- und Datenflussdaten aller Geräte, Endpunkte und Apps, die im Firmennetz aktiv sind. Unser Security-Experte Thomas Schwert erläutert, warum immer mehr Unternehmen ein Security Information and Event Management benötigen und welche typischen Fehler bei der Einführung gemacht werden. Hier ein Interview von Frank Erdle, Freelance IT Journalist mit Thomas Schwert, Key Account Manager bei anykey GmbH.

Was verbirgt sich hinter dem Begriff „Security Information and Event Management“ (SIEM)?

Thomas Schwert: SIEM-Lösungen ermöglichen es Unternehmen, Daten aus den verschiedensten Quellen zu sammeln, zu analysieren und bestimmte Informationen oder Ereignisse sichtbar zu machen. Durch das Aufbrechen von Datensilos wird eine Transparenz für alle angebundenen Systeme und Datenquellen erreicht. Dies schafft die Möglichkeit, Zusammenhänge zu erkennen und nachzuverfolgen.

Warum wird IT-Sicherheit nun auch für viele Unternehmen, die keine kritische Infrastruktur betreiben, zur Kernaufgabe?

Thomas Schwert: Die gesetzlichen Vorgaben haben sich in diesem Bereich in den vergangenen Jahren immer weiter verschärft. Dadurch sind viele Branchen verpflichtet, ihre Informationssicherheit auf ein Niveau anzuheben, das dem technischen Stand der Dinge entspricht. Betroffen sind im Grunde alle Unternehmen, die mit schützenswerten Daten umgehen, also beispielsweise Industriefirmen und deren Zulieferer, aber auch Kliniken und Arztpraxen. Mit dem Einsatz eines SIEM lassen sich Schwach-stellen frühzeitig erkennen, sodass eine deutlich schnellere und bessere Reaktion auf Angriffe erfolgen kann. So wird es für Cyberkriminelle wesentlich schwieriger, in die IT-Systeme einzudringen und sich im Ökosystem auszubreiten.

anykey GmbH
Thomas Schwert
Junkersring 5
D-53844 Troisdorf

t: +49(0)2241-3974 0
f: +49(0)2241–3974–199
e: t.schwert@anykey.de

anykey
going beyond IT

Vorteile einer SIEM Lösung am Beispiel IBM QRadar

+ Echtzeitüberwachung der gesamten IT-Infrastruktur zur Erkennung und Priorisierung von Bedrohungen.

+ Ausgabe und Priorisierung von Warnungen, um die Untersuchungen von Sicherheitsanalysten auf verdächtige Vorfälle mit hoher Wahrscheinlichkeit zu konzentrieren.

+ Effektives Bedrohungsmanagement mit detaillierter Protokollierung von Nutzeraktivitäten und Datenzugriffen zur Einhaltung aller Compliance-Vorgaben.

+ Vielfältige Einsatzmöglichkeiten: on-premise, in der Cloud oder in einer hybriden Umgebung.

+ Inklusive Multi-Tenancy und Master-Konsole, um Managed Service Provider bei der Bereitstellung von kostengünstigen Security-Intelligence-Lösungen zu unterstützen.

+ Optionales Upgrade mit IBM X-Force® Threat Intelligence, um eine permanent aktualisierte Übersicht zu potenziell bösartigen IP-Adressen zu erhalten, einschließlich Malware-Hosts, Spam-Quellen und anderer Bedrohungen.

IBM QRadar

Welche Bausteine muss eine SIEM Software enthalten?

Thomas Schwert: Im Grunde verbirgt sich dahinter eine Plattform, die Informationen sammelt, verarbeitet, speichert und durchsuchbar macht – inklusive einer übersichtlichen Visualisierung. Die verschiedenen Anbieter auf dem Markt liefern zwar vergleichbare Ergebnisse, gehen aber unterschiedliche Wege bei der Verarbeitung. Grundsätzlich benötigt man eine Infrastruktur, also Server und Storage, und die SIEM-Software. Dabei ist es aus technischer Sicht unwesentlich, ob diese im eigenen Rechenzentrum, in der Cloud, hybrid oder als Software-as-a-Service bereitgestellt wird.

Woran ist eine hochwertige und zukunftssichere SIEM-Lösung zu erkennen?

Thomas Schwert: Führende Anbieter bieten sehr ausgereifte und vielseitige Lösungen, die aus heutiger Sicht auch zukunftssicher sind. Ein Beispiel ist IBM QRadar mit einer langjährigen Expertise und einem stabilen Unterbau. Wichtige Kriterien für die Auswahl sind auch der Bedarf an Speicher und Rechenleistung sowie der Aufwand für den Betrieb. Hier unterscheiden sich die auf dem Markt verfügbaren Lösungen deutlich. Deshalb sollte man diesem Punkt eine hohe Beachtung schenken.

Wie funktioniert ein Security Information and Event Management in der Praxis?

Thomas Schwert: Zunächst gilt es, die eigenen Ziele zu definieren: Welche Sicherheitsvorgaben sollen erfüllt werden, und welche Use Cases sowie Datenquellen werden benötigt? Danach werden die gewählten Quellen an das SIEM angebunden. Im Anschluss oder parallel dazu werden die Use Cases und die Dashboards eingerichtet. Ab diesem Zeitpunkt erhält man automatisch und nahezu in Echtzeit Informationen zu den überwachten Prozessen und kann automatisierte Aktivitäten anstoßen. Zudem besteht die Möglichkeit, Silo-übergreifend gezielte Suchen durchzuführen, wenn beispielsweise Hinweise auf mögliche Schwachstellen vorliegen und geprüft werden soll, ob diese ausgenutzt wurden.

anykey
going beyond IT

Unsere Expertise

- Mehr als 20 Jahre am Markt mit Fokus auf Consulting
- Mitglied der Allianz für Cybersicherheit des BSI
- Gründungsmitglied des Cyber Security Cluster Bonn e.V.

anykey als Partner

- Erfahrung aus mehr als 1.000 Projekten, davon viele bei Banken, Energieversorgern und anderen kritischen Infrastrukturen
- Erfahrung im Professional Service auch für Hersteller

Leistungen im Bereich SIEM

- Produktauswahl und Konzeption
- SIEM-Einführung
- Schulung
- Beratung zum Erreichen der „SIEM-Reife“
- SIEM as a Service
- Hybridbetrieb
- Unterstützung Eigenbetrieb
- Outtasking/Outsourcing

anykey GmbH
Junkersring 5
D-53844 Troisdorf

t: +49(0)2241-3974 0
f: +49(0)2241–3974–199
e: contact@anykey.de

Für welche Unternehmen ist die SIEM Nutzung als Managed Service in der Cloud interessant?

Thomas Schwert: Eine Managed-Service-Lösung bietet sich für alle Unternehmen an, die keine entsprechenden Ressourcen aufbauen können oder wollen. Der Mangel an Fachkräften ist insbesondere im Bereich der IT Sicherheit enorm. Der Managed Service muss übrigens keine SaaS-Lösung sein. Ein Unternehmen kann auch eigene Softwarelizenzen auf seiner Infrastruktur besitzen und die Betriebsleistung als Service erbringen lassen.

Welche Fehler werden bei der SIEM Einführung gemacht, und woran können entsprechende Projekte scheitern?

Thomas Schwert: Bereitstellung und Betrieb sind sehr komplexe Themen. Viele Hersteller oder Dienstleister werben mit „Out of the Box“ und „Fast Time to Value“, um beim Kunden den Eindruck zu erwecken, dass alles ganz einfach ist. Die Software selbst ist tatsächlich schnell ausgerollt. Doch die Anbindung der Datenquellen und Implementierung von Use Cases erfordert einige Erfahrung. Schließlich müssen sehr viele Abteilungen und Prozesse berücksichtigt werden. Auch der Rückhalt innerhalb der Unternehmensführung ist wichtig. Wir können den Kunden nur raten, sich einen Dienstleister zu suchen, der eine ergebnisoffene Beratung bietet, auch wenn dabei höhere Einstiegskosten entstehen. Auf längere Sicht ist der vermeintlich teurere Anbieter häufig der günstigere.

Viele Verantwortliche, die ein SIEM mit eigenen Mitteln aufbauen wollen, unterschätzen, welches Know-how dafür benötigt wird. Alle uns bekannten Projekte, in denen das versucht wurde, sind gescheitert. Zumal es angesichts des derzeitigen Fachkräftemangels kaum gelingt, erfahrene Spezialisten einzukaufen. In manchen Unternehmen gibt man sich auch damit zufrieden, die regulatorischen Anforderungen zu erfüllen. Davor können wir aber nur warnen: Cybergangstern wird so ungewollt die Arbeit erleichtert. Behalten Sie stets das eigentliche Ziel im Fokus!

Gerne begleiten wir Sie auf Ihrem individuellen Weg zum SIEM.