Juli 2018
Marion Lewalski

Whitepaper

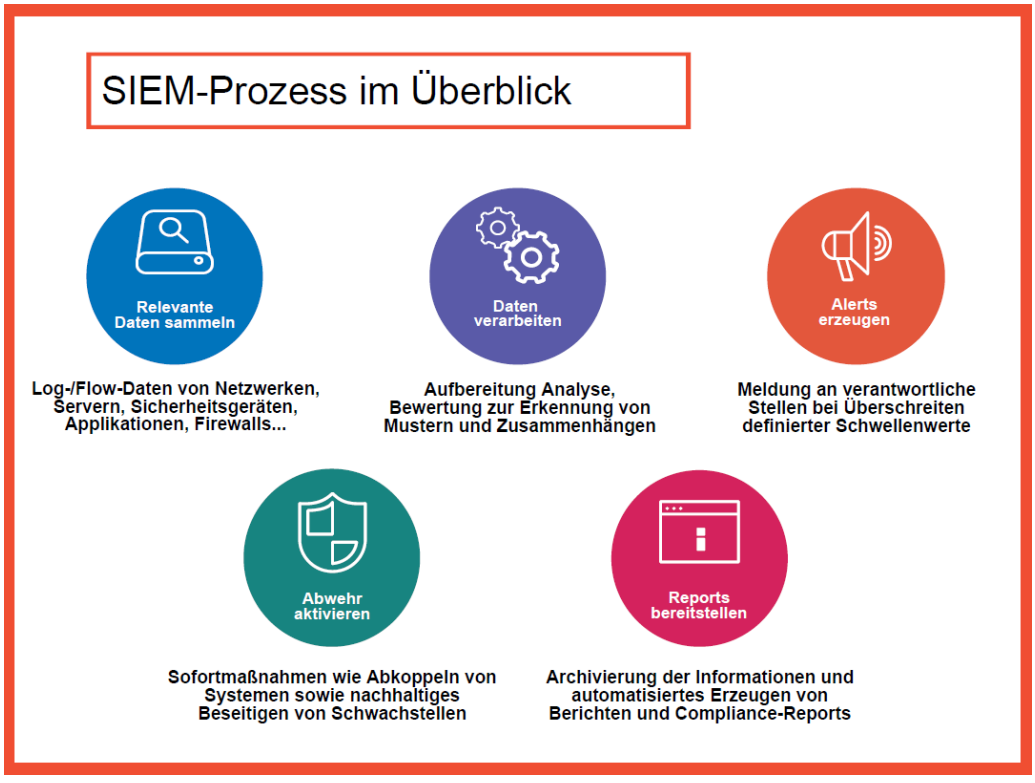
Information Security und Event Management als Service (Security Operation Center)

Sicherheitsrisiken mit Outsourcing flexibel im Griff

Managed Security Services – ein Markt im Aufschwung

Der Markt für IT-Security ist und bleibt auf Wachstumskurs. Für 2018 geht das Analystenhaus Gartner davon aus, dass die weltweiten Ausgaben in diesem Bereich gegenüber dem Vorjahr um acht Prozent ansteigen.[1] Ein großer Teil der Budgets fließt dabei in die Sparte der Managed Security Services (MSS). Eine Mehrheit von 66 Prozent der europäischen Unternehmen setzt in Sachen IT-Sicherheit bereits auf MSS-Provider, weitere 24 Prozent planen, dies künftig zu tun.[2]

Externe Hilfe ist besonders dann gefragt, wenn es um die Erkennung und Prävention von Sicherheitsvorfällen geht. So ist es für Unternehmen angesichts stetig wachsender Datenmengen zusehends schwieriger, hier den Überblick zu behalten. Lösungen und Dienstleistungen für Security Information und Event Management (SIEM) sollen Abhilfe schaffen. Das Anwendungsspektrum reicht von der Erfassung und Verarbeitung von Daten über Alarmfunktionen und Reporting bis zur Risikobehebung (siehe Schaubild).



[1] Quelle: www.gartner.com/newsroom/id/3836563

[2] Pierre Audoin Consultants: Studie „Managing Security in the Digital Era“, 2017

Hinter dem wachsenden Bedarf an sogenanntem Managed SIEM stehen eine Reihe von Ursachen.

Die 5 Hauptgründe für den Fokus auf SIEM als Service

1. Fachkräftemangel

Für Unternehmen wird es immer schwerer, offene Stellen in der IT zu besetzen. So fehlen laut einer repräsentativen Studie bis 2022 auf dem europäischen Arbeitsmarkt 350.000 Fachkräfte für IT-Security.[3] Die Mehrheit der CIOs sehen in diesem Mangel an qualifizierten Mitarbeitern inzwischen bereits das größte Sicherheitsrisiko für ihre Firma.[4] Ein möglicher Ausweg aus dem Personalengpass ist die Beauftragung externer Spezialisten.

2. Steigende Komplexität der IT

Bereits 2016 ergab eine europaweite Umfrage: Zusehends komplexere IT-Landschaften sind der größte Treiber für den starken Anstieg der Arbeitsbelastung in der IT.[5] Als direkte Folge ergeben sich daraus Performance-Probleme, was sich auch auf die Überwachung der Infrastruktur sowie die Identifizierung und Behebung von Sicherheitsrisiken auswirkt. Mit Tools für automatisiertes Netzwerk-Monitoring in Echtzeit und flexiblen SIEM-Services lässt sich hier gegensteuern.

3. Digitalisierung

Menschen, Unternehmen, Geräte – in Zeiten der Digitalisierung ist alles miteinander vernetzt. Mit dem Grad der Vernetzung steigt allerdings auch die Anzahl der Angriffspunkte. SIEM-Systeme zeichnen sich dadurch aus, dass sie auf die Überwachung verschiedener Datenquellen ausgelegt sind und sich flexibel an neue Gegebenheiten anpassen lassen.

„SIEM-Provider sollten Security als Prozess verstehen. Das heißt die bereitgestellte Lösung spiegelt immer die aktuellen Kundenanforderungen wider.“

Martin Viselka, CEO, bw digitronik ag

4. Verschärfte Bedrohungslage

Die Zeiten, in denen Malware relativ wahllos und in großem Stil verbreitet wurde, sind vorbei. Heute richten sich Angriffe meist gezielt gegen zuvor ausgewählte Unternehmen. Immer häufiger geraten dabei kleine und mittlere Firmen ins Visier, da man bei ihnen von geringeren Sicherheitsstandards ausgeht.

Den betroffenen Unternehmen drohen unter anderem Datenklau, Blockade von IT-Systemen und Geldverlust. SIEM-Services bieten zweifachen Schutz: Es lassen sich sowohl Schwachstellen im Security-Bereich proaktiv aufdecken als auch ungewöhnliche Aktivitäten zeitnah erkennen.

Schutz vor neuen Angriffsformen

2017 haben Cyber-Kriminelle ihren Schwerpunkt auf die Durchführung gezielter Ransomware-Attacken verlegt, so der IBM X-Force Threat Intelligence Index 2018. Dabei werden IT-Systeme durch das Einschleusen von Schadsoftware blockiert (zum Beispiel verschlüsselt) und nur gegen Zahlung eines Lösegelds wieder freigeben. Experten gehen davon aus, dass sich diese Angriffsform künftig immer mehr durchsetzt. Wirksamen Schutz bilden Früherkennung und schnelles Reaktionsvermögen.

5. Datenschutz und Compliance

Je restriktiver regulatorische Faktoren werden, Stichwort “EU-Datenschutzgrundverordnung”, desto mehr bietet sich der Einsatz von SIEM an. Entsprechende Lösungen und Services unterstützen Unternehmen bei der Erfüllung der immer anspruchsvolleren Anforderungen. Das beinhaltet die automatische Überwachung der Compliance-Konformität, das Erstellen von Berichten und damit die Erfüllung von Nachweispflichten sowie Alarm- und Benachrichtigungsfunktionen.

[3] Frost & Sullivan: Global Information Security Workforce Study 2017
[4] Ponemon Institute: Befragung zu Top-Sicherheitsbedrohungen in der IT für 2018
[5] Automic: Umfrage zu Gründen für Anstieg der Arbeitsbelastung in der IT, 2016

SIEM-Services nach dem Baukastenprinzip

Nach eigenen Erfahrungen der IT-Dienstleister ist die Skalierbarkeit von Services bei Outsourcing-Entscheidungen ein wichtiges bis sehr wichtiges Kriterium. Dahingehend äußerten sich immerhin 93 Prozent der Anbieter bei einer Befragung durch PricewaterhouseCoopers.[6] Durch die herrschende Marktdynamik und das hohe Tempo in der digitalen Entwicklung setzt sich dieser Trend weiter fort. Für Service-Verträge ergibt sich hieraus die Forderung nach kürzeren Laufzeiten und hoher inhaltlicher Anpassungsfähigkeit. Im Bereich SIEM stehen dabei folgende Leistungsbausteine zur Auswahl:

Technischer Betrieb der SIEM-Lösung
Der Provider implementiert das SIEM-System im Rechenzentrum des Kunden oder stellt Lösungen aus seinem eigenen Bestand zur Nutzung bereit. In jedem Fall liegt der IT-Betrieb in den Händen des Dienstleisters, was auch das Aufspielen von Updates und Upgrades sowie die umgehende Beseitigung operativer Störungen beinhaltet. Das gibt dem Outsourcing-Nehmer die Sicherheit, dass die Software immer hochverfügbar und auf dem neuesten Stand ist.

Incident Response Management
Angriff von außen durch Malware bzw. Cyberkriminelle, interner Anwenderfehler, Datenschutzverletzung oder Sicherheitslücke im Betriebssystem? Incident Response Management beinhaltet das Monitoring der IT-Umgebung sowie eine Bedrohungs- und Risikoanalyse auf Basis der erzeugten SIEM-Alarme. Je nach Bedarf kann die Überwachung rund um die Uhr (24/7) oder zu den üblichen Geschäftszeiten (8/5) erfolgen. Auch in Bezug auf den Leistungsumfang ist eine Staffelung möglich:

Bei der 1st Level Security Analysis handelt es sich um eine reine False Positive-Diagnose. Das heißt es wird festgestellt, ob hinter dem gemeldeten Vorfall tatsächlich eine Bedrohung steht oder nicht.

Im zweiten Level findet eine erste vertiefte Analyse statt. Es wird geprüft, welche Systemkomponenten betroffen sind und ob sofortiges Handeln, zum Beispiel in Form einer Konfigurationsänderung, erforderlich ist. Passend zum Ergebnis erhält der Kunde entsprechende Handlungsempfehlungen.

Level drei geht noch einen Schritt weiter in Richtung Ursachenforschung. Das beinhaltet zum Beispiel forensische Untersuchungen oder – bei besonders kri-

[6] PwC Schweiz: IT-Sourcing-Studie – die Perspektive der Anbieter, 2015

tischen Fällen – eine Analyse von Daten aus der näheren Vergangenheit, um den Tathergang nachvollziehen zu können.

Vulnerability Assessment/Penetration Testing
Neben den kontinuierlichen Services bieten SIEM-Provider auch proaktive Dienstleistungen an, bei denen Systeme und Netzwerke einmalig oder in regelmäßigen Abständen auf Schwachstellen geprüft werden. Häufige Abnehmer sind etwa Unternehmen aus dem Finanz-, Gesundheits- oder Energiesektor. Die Ergebnisse erhält der Kunde in Form eines technischen Security Bulletins, das Risikopunkte in der IT-Umgebung aufzeigt und Lösungsansätze darstellt.

SIEM plus Service – eine Nutzenbetrachtung

Im Wettlauf mit Cyber-Kriminellen bringen SIEM-Systeme die Anwenderfirmen bereits einen Schritt weiter. Die Lösungen identifizieren Gefahrenpotenziale automatisiert und in Echtzeit. Im Vergleich dazu nimmt die manuelle Ausführung dieser Tätigkeiten das sieben- bis zehnfache an Zeit in Anspruch. Mit der Erkennung von Sicherheitsvorfällen ist es allerdings nicht getan. Der weitaus aufwendigere Teil des Prozesses ist die Analyse der SIEM-Alarme. Um den Bereich in Zeiten einer großen und stark zunehmenden Zahl an Bedrohungen abdecken zu können, benötigen Unternehmen je nach Größe drei bis fünf Security-Analysten – und die sind schwer zu finden. Die Auslagerung dieses manpower-intensiven Parts an externe Spezialisten kann Abhilfe schaffen und zudem die günstigere Alternative darstellen.

SIEM-Services im mittleren Leistungslevel kosten in etwa soviel wie ein Security-Mitarbeiter in Vollzeit.

Martin Viselka, CEO, bw digitronik ag

Schnelles Handeln im Risikofall zahlt sich in weiterer Hinsicht aus. So hat IBM in einer Security-Studie herausgefunden, dass eine langsame Reaktion die Kosten eines Angriffs negativ beeinflusst. Demnach haben Vorfälle, die mehr als 30 Tage dauerten, eine siebenstellige Summe mehr gekostet als diejenigen, die in kürzerer Zeit abgefangen werden können.[7]

Um den Zeit- und Kostenvorteil beim SIEM-Einsatz aufrechterhalten bzw. sogar ausbauen zu können, müssen die Methoden zur Erkennung und Analyse von Sicherheitsrisiken stetig weiterentwickelt werden. In Zeiten einer steigenden Bedrohungslage mit zusehends ausgefeilteren Methoden sowie täglich neuen Malware-Varianten, die sich immer schneller verbreiten, ist dies unabdingbar.

Blick in die Zukunft: Einzug künstlicher Intelligenz in die SIEM-Welt

Es gibt bereits erste SIEM-Lösungen auf dem Markt, die mit künstlicher Intelligenz (KI) ausgestattet sind. Dazu zählt IBM QRadar mit integrierter Watson-Funktionalität. Mithilfe von maschinellem Lernen und kognitiver Intelligenz kann das System darauf trainiert werden, frühzeitig Anomalien im Netzwerk-Traffic zu erkennen und diese auch gleich zu analysieren.

Kommt es bei der Systemnutzung zu Abweichungen von hinterlegten Verhaltensprofilen? Sind Art, Kategorie und Quelle einer eingeschleusten Malware bekannt? Lässt sich eine Verbindung zwischen aktuellen und vergangenen Bedrohungsmustern herstellen? Fragen wie diese lassen sich mit einer solchen Lösung in Sekundenschnelle beantworten und Sicherheitsanalysten erhalten umgehend wertvolle Hintergrundinformationen zum SIEM-Alarm.

Die nächste Stufe der künstlichen Intelligenz im SIEM-Bereich zeichnet sich bereits ab: Künftig soll es mit den Lösungen nicht nur möglich sein, in Echtzeit auf Sicherheitsvorfälle zu reagieren. Bedrohungen sollen vielmehr auch vorausgesehen und proaktiv abgewehrt werden können.

[7] IBM/Ponemon Institute: Studie „Cost of Data Breach“, 2017