Monitoring der IT-Sicherheit

SIEM-Systeme mit Intelligenz

Kai-Oliver Detken

Monitoring-Systeme werden in Unternehmen heute zunehmend eingesetzt, um Netz- und Serverkomponenten auf ihre Verfügbarkeit zu kontrollieren. Denn der 24/7-Betrieb muss in den meisten Firmen für fast alle IT-Dienste sichergestellt werden können. Gleichzeitig kann ein Monitoring-System auch als Dokumentationshilfe dienen, da alle IT-Systeme enthalten und übersichtlich aufgelistet werden. Allerdings wird dabei die IT-Sicherheit nicht hinterfragt, die sich ebenfalls negativ auf die Verfügbarkeit auswirken kann. Dies soll sich nun durch sog. SIEM-Systeme (Security Information and Event Management) ändern. Sie geben Auskunft über aktuelle Risiken und entsprechende Handlungsempfehlungen. Problematisch bleibt das automatische Erkennen einer Anomalie.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Der Schwerpunkt eines SIEM-Systems ist die Überwachung und Verwaltung von Benutzerdiensten und -privilegien, Verzeichnisdiensten und Änderungen der Systemkonfiguration sowie die Bereitstellung zur Auditierung und Überprüfung der Vorfälle. Es geht damit einen Schritt weiter als herkömmliche Monitoring-Systeme und bezieht explizit die IT-Sicherheit mit ein. SIEM-Systeme werden daher mittlerweile als eine sehr wichtige Sicherheitskomponente von IT-Infrastrukturen angesehen. Sie kommen bisher allerdings fast ausschließlich in großen Unternehmen zum Einsatz, da ihr Betrieb sehr komplex und kostenintensiv ist.

Aktuelle SIEM-Systeme sind zudem auch nur dann nützlich, wenn Experten in IT-Abteilungen die Sicherheitswarnungen und Ausgaben des SIEM-Systems sinnvoll selektieren und interpretieren können, um dann geeignete Gegenmaßnahmen ergreifen zu können. Das macht den Betrieb in kleinen und mittelständische Unternehmen (KMU) praktisch nicht möglich.

Eine weitere Schwierigkeit liegt in proprietären Datenformaten für Systemereignismeldungen (Events) und deren unterschiedliche Aussagekraft. Dazu müssen Sicherheitskomponenten unterschiedlicher Hersteller miteinander kommunizieren bzw. sich die Ereignismeldungen korrelieren lassen. Erst dann erhält man eine qualitativ wertigere Aussage zur IT-Sicherheit, als wenn man sich auf die Einzelkomponenten verlässt. Dabei spielt der Einsatz von KI-Verfahren (Künstliche Intelligenz) eine immer wichtigere Rolle.

SIEM-Funktionalität

Um sicherheitsrelevante Events unterschiedlicher Güte in einem SIEM-System zusammenzuführen und korrelieren zu können, erbringen sog. Kollektoren (auch Agents genannt) die folgenden Leistungen (*Bild 1*):

- Extraktion: Events sind in Rohform meist Einträge in Log-Dateien oder über das Netz versandte Systemmeldungen. Sie müssen aus den jeweils verwendeten Systemen oder Transportprotokollen extrahiert werden, um sie einem SIEM-System zugänglich machen zu können.
- Homogenisierung/Mapping: Events werden von verschiedenen Diensten erzeugt und aus unterschiedlichen Systemen extrahiert. Um eine Weiterverarbeitung in einem SIEM-System zu gewährleisten, müssen die relevanten Inhalte der einzelnen Events miteinander in Bezug gebracht werden können. Dafür sorgt ein entsprechendes „Umsortieren" individueller Datenfelder in speziellen Event-Formaten in ein standardisiertes, dem SIEM-System verständliches Event-Format.
- Aggregation: Große Mengen gleichartiger Events über einen kurzen Zeitraum würden ein zentrales SIEM-System belasten, ohne einen signifikanten Mehrwert zu erzeugen. Kollektoren aggregieren daher große Mengen gleichartiger Events über einen kurzen Zeitraum (sog. Bursts) zu einem einzigen Event mit höherer Aussagekraft (z.B. Event-Typ, Inhalt und Menge der ursprünglichen Meldungen).

Die Auswertung von Events wird anhand von Regelsätzen durchgeführt. Die Relevanz der Ergebnisse der Regelauswertung ist aber abhängig von den Eigenschaften bzw. dem Aufbau des jeweiligen Unternehmens. Beispiele hierfür sind primäre und sekundäre Geschäftsprozesse, organisatorische Prozesse, die Bedrohungslage oder eingesetzte IT-Assets. Die Operationalisierung übergreifender Strategien, aber auch bereits das Ableiten von Regelsätzen aus konkreten Sicherheitsrichtlinien stellt für Unternehmen eine Herausforderung dar. Maschinenlesbare Sicherheitsrichtlinien sind kom-

plex und deren manuelle Erstellung erfordert spezifisches Expertenwissen, das nur in begrenztem Maß zur Verfügung steht und dessen Bereitstellung kostenintensiv ist. Ohne ein wirksames Set an Regelsätzen ist ein SIEM-System in seiner Wirkung stark eingeschränkt und erbringt nicht die Leistungen, die dessen Anschaffungs- und Betriebskosten rechtfertigen würden.

SIEM-Einführung und -Arbeitsweise

Die Zielsetzung bei der Implementierung von IT-Sicherheit ist im Grunde genommen relativ einfach: Das Unternehmen und seine Assets sollten nach Schutzbedarfsfeststellung geschützt und die Kosten dieser Schutzmaßnahmen abgeschätzt und in Relation zu der Reduktion der Eintrittswahrscheinlichkeit eines Schadensfalles gestellt werden. Es kann ein positiver Beitrag zum Unternehmensergebnis geschaffen werden, wenn die Optimierung des Risikomanagements ermöglicht wird, ohne dabei die Verfügbarkeit im Netz zu reduzieren – im Gegenteil. Die Umsetzung eines SIEM-Projektes kann durchaus ein bis zwei Jahre dauern.

Damit ein Projekt nicht zu viel Zeit in Anspruch nimmt, ist anzustreben, dass man die Unternehmenswerte vorab definiert, sie in die Sicherheitsstrategie einbezieht und beim Einsatz von IT-Sicherheitskomponenten einen ganzheitlichen Kontext verfolgt. Dieser bezieht auch die Benutzergruppen mit ein, die für die verschiedenen Unternehmensbereiche zuständig sind. So muss z.B. ein Problem für einen technisch Verantwortlichen anders dargestellt werden als für einen kaufmännischen. Zudem dürfen unterschiedliche Arbeitsgruppen nur die für sie bestimmten Bereiche einsehen. Zwar müssen alle Informationen in die Bewertung der Gesamtsicherheitslage einbezogen werden, sensible Informationen aus „Gruppe A" dürfen jedoch nicht in „Gruppe B" auftauchen.

Eine Unterteilung könnte dabei wie folgt aussehen:

- Gruppe A: Netz;
- Gruppe B: Sicherheitskomponenten;
- Gruppe C: Facility Management;
- Gruppe D: Serversysteme.

Das Beispiel einer Gefährdung könnte z.B. so aussehen, dass sich ein Benutzer am Unternehmensnetz über Network Access Control (NAC) authentifiziert und das NAC-System nach Überprüfung der Login-Daten ihm Zugang gewährt. Der Benutzer kann nun auf die Unternehmensdaten zugreifen und geht seiner normalen Arbeit nach. In der Mittagspause nutzt er seinen privaten USB-Stick, der leider einen Virus enthält, der sich umgehend mit einem Server im Netz verbindet. Da eine Anmeldung am NAC-System erfolgt ist, kann der Virus bereits freigeschaltete Applikations-Ports zur Kommunikation nutzen. Die Firewall-Systeme und Switche merken erst einmal nichts Ungewöhnliches.

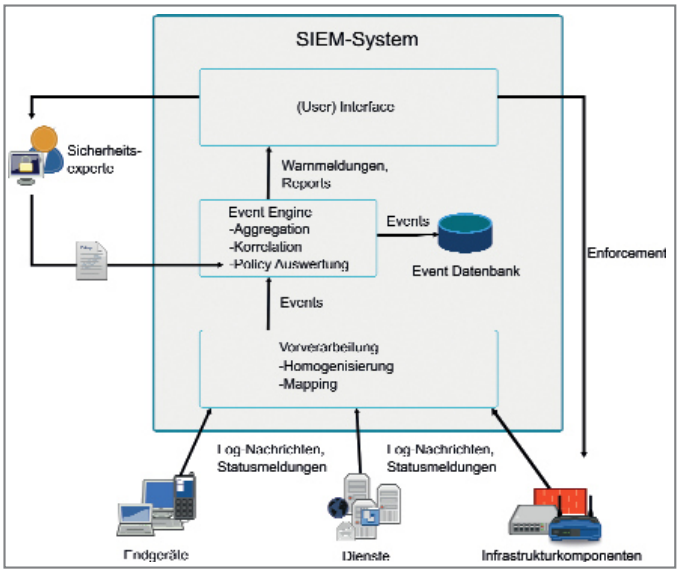

Bild 1: Allgemeiner Aufbau eines SIEM-Systems

Ein SIEM-System hingegen kann z.B. feststellen, dass der Mitarbeiter ungewöhnlich viele Datenpakete durch das Netz schickt oder dass auf Port 80 der Datenstrom SOAP-Traffic enthält. Es informiert daher „Gruppe A" und „Gruppe D". Das Management wird noch nicht informiert, da es noch unklar ist, ob wirklich eine Anomalie vorliegt. Inzwischen ist der Virus weiter aktiv und versucht auf eine Datenbank zuzugreifen. Dabei entstehen viele Fehlauthentifizierungen, die ebenfalls registriert werden. Das SIEM ist nun in der Lage, die beiden Events miteinander zu korrelieren und bewertet das korrelierte Ereignis höher als die Ursprungsereignisse. Neben „Gruppe A" und „Gruppe D" wird jetzt auch das Management informiert, da offenbar ein Angriff erfolgt. Nachdem der Virus erkannt und eliminiert worden ist, wird der Vorfall im SIEM-System dokumentiert, damit spätere Auditoren den Vorfall nachvollziehen können.

Dieses Beispiel zeigt, dass ein übergreifendes SIEM-System mit einer ganzheitlichen Sicht auf das Netzverhalten mehr wahrnimmt als herkömmliche Sicherheitslösungen. Allerdings müssen dazu auch einheitliche Events der unterschiedlichen Sicherheitskomponenten vorliegen, um die Daten entsprechend korrelieren zu können. Genau hier liegt oft die Schwierigkeit bei der Anbindung von SIEM in eine vorhandene Infrastruktur. Hinzu kommt, dass die Anomalie normalerweise automatisch erkannt werden kann, wenn das Normalverhalten bekannt ist. Bisherige Herstellerlösungen arbeiten allerdings hauptsächlich mit Mustererkennung und definierbaren Regelsätzen, so dass es an intelligenten Systemen fehlt.

Forschungsansätze

Die fachlichen Anforderungen an ein SIEM-System orientieren sich am Hauptinformationsfluss, d.h. vom Sammeln über das Verarbeiten der Informationen bis zur Reaktion. Sie müssen Folgendes erfüllen:

- Sammeln von Daten der zentralen Dienste und Netzkomponenten;
- Aggregation dieser Daten zu aussagekräftigen Ereignissen anhand einer flexibel definierbaren Policy;
- Darstellungen der sicherheitsrelevanten Ereignisse in verschiedenen Detailstufen;
- Auslösen von Alarmmeldungen oder gegebenenfalls aktiver Eingriff.

Um angemessene Entscheidungen zu treffen, ist es wichtig, eine aktuelle

und korrekte Wissensbasis über die Geräte, Benutzer und Eigenschaften des Netzes zu besitzen. Diese Informationen müssen zentralisiert und für berechtigte Komponenten zugreifbar sein, damit Bedrohungen miteinander kombiniert werden können. Das BMBF-Forschungsprojekt Simu (**www.simu-project.de**) ermöglicht das Mapping der Metadaten durch ein einheitliches Protokoll namens IF-MAP (siehe NET 9/2014, S. 45). Dadurch lässt sich eine Homogenisierung aller Logdaten durchführen, um eine Korrelation der Daten vornehmen zu können.

Bild 2: Weboberfläche des Personal Dashboards

Zusätzlich muss für eine Anomalieerkennung aber auch der Normalzustand eines Netzes bekannt sein bzw. erlernt werden können. Aktuelle SIEM-Systeme arbeiten allerdings in den meisten Fällen nach Mustererkennung. Ist das Muster nicht bekannt, kann auch der Angriff auf das Unternehmensnetz nicht erkannt werden. Das BMWI-Forschungsprojekt iMonitor (**www.imonitor-project.de**) zeichnet daher eine bestimmte Zeit den Normverkehr des Netzes auf, um Anomalien anhand von Abweichungen mittels Zeitreihenanalyse (KI-Verfahren) erkennen zu können. Dabei werden allerdings auch gewisse Abweichungen toleriert, um die False-Positive-Rate zu verringern.

Ein Herstellerbeispiel

Ein Hersteller, der bereits relativ viel von den neuen Ansätzen der erwähnten Forschungsprojekte umgesetzt hat, ist Logrhythm. Er bietet eine Komplettlösung an, die aus den drei folgenden Grundkomponenten besteht:

- Log Manager (LM);
- Event Manager (EM);
- Advanced Intelligence Engine (AIE);

Log sowie Event Manager stellen hierbei Datenbanken dar. Der Log Manager empfängt und speichert alle erzeugten Messages und schickt diese zum einen zur Korrelation an die AIE sowie die direkt als Events eingestuften Nachrichten an den Event Manager. Die Anzahl der Log Manager ist nicht festgelegt und kann variiert werden. Dies ist besonders dann sinnvoll, wenn eine sehr große Umgebung vorliegt und dementsprechend die Nachrichtendichte in der Sekunde sehr hoch ist. In einem solchen Fall kann dann ein weiterer Log Manager zur Verteilung der Last hinzugeschaltet werden. Dadurch bekommt man das Big-Data-Problem in den Griff.

Die Advanced Intelligence Engine ermöglicht die automatische und kontinuierliche Analyse der IT-Umgebung. Sie dient ebenfalls zur Verwaltung der Regeln. Über die Knowledge Base können Pakete mit darin enthaltenen Regeln heruntergeladen und anschließend in der AIE aktiviert werden. Diese von Logrhythm erstellten Regeln lassen sich nach vorherigem Klonen bearbeiten und an die eigenen Bedürfnisse anpassen. So ist es ohne weiteres möglich, eine Regel zu schreiben, die z.B. „Failed Logins" erkennt und bei einem anschließenden erfolgreichen Login einen Alarm erzeugt. Bedingungen lassen sich logisch miteinander kombinieren, so dass auch komplexe Regeln erstellt werden können.

Das SIEM-System kann über eine Weboberfläche zentral verwaltet werden. Hierüber werden sämtliche Konfigurationen des Systems vorgenommen. Dabei werden die Events aggregiert und übersichtlich im Personal Dashboard angezeigt (*Bild 2*).

Logrhythm bietet zudem die Möglichkeit, bei der Regelerstellung anzugeben, wie wahrscheinliche „False Positives" und wie hoch der mögliche Einfluss von Geräten innerhalb des Netzes auf die Detektion sind. Diese Werte fließen dann mit in den Algorithmus ein und haben Einfluss auf die Warnstufe. Dadurch kommt dieser Ansatz einem KI-Verfahren schon sehr nahe, da das System laufend lernt.

Fazit

Im Gegensatz zu traditionellen SIEM-Lösungen nutzt die AIE von Logrhythm die Log- und Event-Managementfunktionen dazu, sämtliche Daten in Bezug zueinander zu setzen. Dies bezieht sich nicht nur auf die vorab gefilterte Untermenge von Sicherheitsereignissen. Die Regeln der AIE leiten Daten aus über 70 verschiedenen Metadatenfeldern ab, die wiederum relevante Daten für die Analyse und Korrelation liefern. Zudem kann auf alle forensischen Daten zugegriffen werden.

Die Korrelation aller Daten und die Mustererkennung mit automatischer Verhaltens- und Statistikanalyse bietet so eine mehrdimensionale Analysefunktion. Durch die Kombination von statistischer und heuristischer Analyse mit dem Whitelisting des erwünschten Verhaltens ermöglicht Logrhythm es Unternehmen, ein Normalverhalten zu erlernen. Dies wird im Zusammenspiel mit der Korrelation der Daten und der Mustererkennung ermöglicht. Durch diese Funktionalität wird auch eine große Zahl an „False Positives" vermieden, so dass relevante Ereignisse besser erkannt und analysiert werden können.

Es wurden daher bei Logrhythm bereits Teile der Forschungsansätze der Projekte iMonitor und SIMU erfolgreich umgesetzt. Einfacher muss allerdings allgemein bei SIEM-Systemen die Handhabung werden, damit sie nicht nur ausschließlich von IT-Sicherheitsexperten bedient werden können. Erst dann werden sie auch für KMU eine interessante Sicherheitslösung sein. *(bk)*