Intelligentes Monitoring

SIEM-Lösungen im Einsatz

Kai-Oliver Detken

Um Dienste- und Netzverfügbarkeit kontinuierlich zu überwachen, ist heute eine Vielzahl von Monitoring-Systemen verfügbar und im Einsatz. Sie ermöglichen die vorausschauende Überwachung aller aktiven Server- und Netzkomponenten und sind daher in der Lage, Ausfälle zu melden, bevor sie zustande kommen. Allerdings lassen sie die IT-Sicherheit bzw. IT-Compliance dabei außen vor. SIEM-Systeme (Security Information and Event Management) gehen einen Schritt weiter: Sie analysieren alle Events der Netzumgebung, um die IT-Sicherheit der Unternehmensumgebung zu überprüfen, Risiken kenntlich zu machen und gegebenenfalls Gegenmaßnahmen zu empfehlen.

Heute sind Unternehmensnetze durch eine Vielzahl von Sicherheitskomponenten gegenüber Sicherheitsangriffe von außen geschützt. Allerdings werden durch die sukzessive Einführung von Sicherheitskomponenten kontinuierlich Insellösungen geschaffen, da diverse Hersteller involviert sind. Jede Insel ist dabei in der Lage, den Sicherheitsgrad des Unternehmens auf die eigene Funktionalität hin zu analysieren bzw. entsprechende Logfiles zur Verfügung zu stellen. Leider werden die Informationen aber nicht konsolidiert und zusammenhängend untersucht, da die Sicherheitskomponenten nur in den seltensten Fällen mit anderen kompatibel sind oder Schnittstellen zum Datenaustausch zur Verfügung stellen. Somit bleiben Angriffe verborgen, die nicht unmittelbar einen Alarm auslösen bzw. es kommt zu einer Vielzahl von „False-Positives"-Meldungen, die manuell untersucht werden müssen.

Der IT-Administrator ist demnach gut ausgelastet, wenn er alle Sicherheitssysteme gleichermaßen analysieren und die Logdaten miteinander vergleichen will (*Bild 1*). Monitoring-Systeme wie Icinga (Nagios) helfen ihm immerhin dabei, nicht den Überblick über seine Dienste, Server- und Netzkomponenten zu verlieren und rechtzeitig Alarme zu erhalten, bevor der kritische Zustand von den Anwendern bemerkt wird. Allerdings wird hier nur auf die Verfügbarkeit Wert gelegt und nicht auf die IT-Sicherheit. Hierüber kann der IT-Administrator lediglich eine subjektive Aussage treffen.

Abhilfe soll ein SIEM-System schaffen, das die Sicherheitslogs konsolidiert und Schadensfälle sammelt. Der Ansatz: Ein Unternehmen legt fest, welche Vermögenswerte (Asset) es schützen will, damit die Gegenmaßnahmen hierfür abgeschätzt und kontinuierlich analysiert werden können. Anhand der Sammlung der Events kann die Reduktion der Eintrittswahrscheinlichkeit eines Schadensfalls gemessen werden und in eine Risikoabschätzung einfließen. Das ermöglicht die Optimierung des Risikomanagements, ohne die Verfügbarkeit im Netz zu reduzieren, im Gegenteil. Die Umsetzung eines SIEM-Systems ist allerdings nicht einfach und kann einige Zeit in Anspruch nehmen.

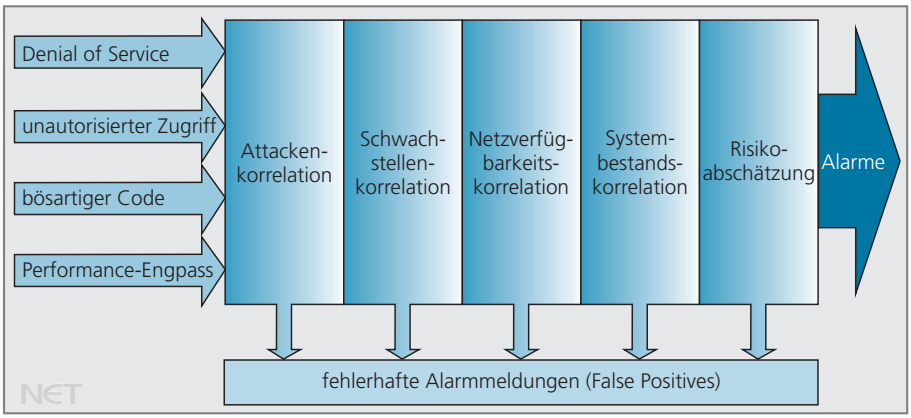

Bild 1: Korrelation von diversen Quellen zur Kontrolle und Visualisierung

SIEM-Technik

Ein SIEM-System besteht aus diversen Modulen (*Bild 2*):

- Event Correlation: wichtigste Basisfunktionalität; die vorhandenen Logfiles werden aufgenommen, archiviert, normalisiert und korreliert, um eine Gefährdung zu erkennen;

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

- Network Behaviour Anomaly Detection (NBAD): Anomalien auf Netzebene können erkannt, Kommunikationsverhalten festgestellt und Abweichungen von der Normalität verfolgt bzw. bei Bedarf in die Korrelation der Problemstellung aufgenommen werden;
- Identity Mapping: die Identität des Benutzers wird offenbart, da SIEM diese Informationen aus diversen Quellen bezieht und analysiert; die dahinterliegenden Datenbanken erlauben auch das Suchen nach Identitätsinformationen bezogen auf unterschiedliche Zeiträume;.
- Key Performance Indication: Netzdaten, Logfiles, sicherheitsrelevante Informationen und Asset-Details werden zentral vereint; die IT-Sicherheit wird messbar;
- Compliance Reporting: erfolgt nach bestimmten Regeln, um auch definierte Aussagen zur IT-Sicherheit treffen zu können; alle Events können kontinuierlich ausgewertet werden;
- Application Programming Interface (API): mögliche Integration von Drittprodukten und Bereitstellung generischer Schnittstellen zur Integration nicht bekannter Geräte/Systeme;
- Role Based Access Control: stellt sicher, dass bestimmte Problemstellungen nur von den jeweils verantwortlichen Stellen/Mitarbeitern eingesehen und bearbeitet werden können.

Diese Module machen die Intelligenz eines SIEM-Systems aus, wodurch eine Risikoanalyse in Korrelation mit allen bekannten Events erfolgen kann. Über unterschiedliche Schnittstellen erhält das System Informationen über Assets (z.B. Inventardaten), Sicherheitslücken (Vulnerability, Patch Management) und kann auf die Dokumentation zugreifen. Zusätzliche Schnittstellen wird es zum Helpdesk oder zu Asset-Datenbanken geben. Auch das Zusammenspiel zum vorhandenen NAC-System muss über Schnittstellen ermöglicht werden, damit Netzbenutzer bei Bedarf in Quarantäne geschickt werden können.

Eine SIEM-Lösung sollte daher für die Verarbeitung des Echtzeit-Incident-Management-Prozesses die Möglichkeit bieten, alle Log-Informationen der überwachten Systeme zu sammeln, zu archivieren und auszuwerten. So können mit einer Lösung Sicherheitsinformationen in Echtzeit und historisch durch entsprechende forensische Analysen bearbeitet werden. Das Ergebnis liefert einen guten Überblick über die bestehende Infrastruktur und damit eine objektive Einschätzung der IT-Sicherheit.

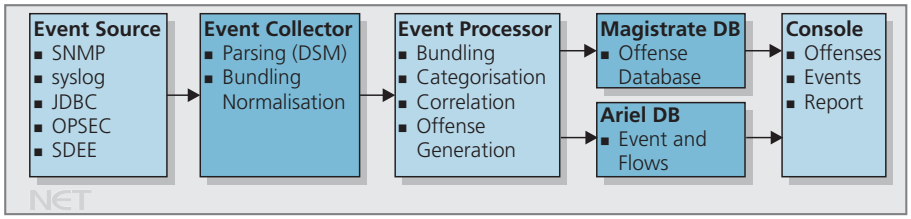

Bild 2: Softwaremodule eines SIEM-Systems

Beispiel Ossim

Das SIEM-System Ossim von Alien Vault gibt es in einer kommerziellen und einer Open-Source-Variante. Beide bieten eine grafische Webbenutzerschnittstelle (GUI, *Bild 3*), in der der Administrator alle notwendigen Konfigurationen durchführen kann. Ebenso ist die Kontrolle und Überwachung von Verfügbarkeit und Funktionsfähigkeit des Ossim-Systems sowie eine komfortable Suche für die Inhalte der Logfiles mittels GUI möglich (*Bild 3*).

Sämtliche Komponenten können durch den Administrator einzeln konfiguriert oder durch eigene Komponenten ersetzen werden. Die Benutzerverwaltung ermöglicht den Einsatz in großen Unternehmens- und Netzumgebungen. Neben den gängigen Informationen wie z.B. Name, Login und Kennwort legt der Administrator genau fest, welche Menüs ein Benutzer sehen und verwenden darf. Auch Assets können so definiert werden, dass sie nicht für alle Benutzer analysiert werden können. Als Asset bezeichnet Ossim Hosts und Netze, die der Administrator vorher dem SIEM-System bekannt machen muss.

Für die Assets benutzt Ossim eine eigene Datenbank, in der diese entweder manuell oder per Scan automatisiert aufgenommen werden können, inkl. Betriebssystem und aktiver Dienste. Bei aktiven Scans wird die WMI-Schnittstelle genutzt, damit Windows-Systeme direkt ausgelesen werden können. Zusätzlich ist OCS NG (Open Computers and Software Inventory Next Generation) in Ossim integriert und kann für kontinuierliche Prüfungen genutzt werden. Das Passive Real-time Asset Detection System (PRADS) ermöglicht die Überwachung von Hosts, Betriebssystemen und Diensten. Dazu aktualisiert es dynamisch die Daten in der Asset-Datenbank.

Neu erkannte Systeme werden automatisch auf Schwachstellen geprüft. Sobald eine solche erkannt ist, wird automatisch ein Ticket generiert, das vom IT-Administrator an verschiedene Benutzer delegiert werden kann. Zusätzlich können Anhänge hinzugefügt und Reaktionen dokumentiert werden.

Die erkannten Dienste und Hosts

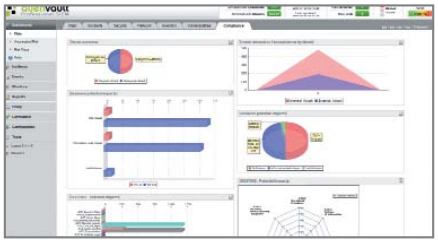

Bild 3: Ossim-Darstellung der Compliance

kann der IT-Administrator durch ein ebenfalls in Ossim integriertes Nagios überwachen, wobei die Konfiguration der Asset-Datenbank entsprechend angepasst werden muss. Allerdings ist nur eine Verfügbarkeitsüberwachung mittels Nagios integriert; weitere Leistungsmerkmale sind bislang nicht vorhanden. Ein weiterer Bestandteil von Ossim ist das Intrusion Detection System Snort, wobei hier ebenfalls nicht alle Funktionen zur Verfügung stehen.

Die wichtigste Funktion von Ossim aber ermöglicht das Auswerten und Analysieren von Sicherheitsvorfällen. Ähnliche Ereignisse werden dabei zu einer einzigen Meldung zusammengefasst. Eine grafische Darstellung des Risikofaktors ermöglicht, dass die Mel-

dungen nach Priorität geöffnet und bearbeitet werden können. Die direkte Umwandlung in Tickets und Weiterleitung an den zuständigen Benutzer erleichtert dabei die Handhabung.

Zwei Forschungsprojekte

Es gibt verschiedene Projekte der IT-Sicherheitsforschung, die sich mit der Entwicklung von SIEM-basierten Systemen beschäftigen. Exemplarisch sollen zwei nationale Projekte genannt werden, die von BMWI und BMBF gefördert werden:

- iMonitor: intelligentes IT-Monitoring durch KI-Ereignisverarbeitung;
- Simu: Sicherheitsinformations- und Ereignismanagement für kleine und mittelständische Unternehmen (KMU).

Im iMonitor-Projekt soll eine neue Form der Ereigniskorrelation entwickelt werden, die automatisiert neue Angriffsvarianten erkennt. Korrelationsregeln werden dabei nicht mehr nur manuell gepflegt. Das heißt, das Erkennen von Anomalien wird mithilfe der Weiterentwicklung von „künstlicher Intelligenz“ (KI) ermöglicht, um nicht nur von einer reinen Mustererkennung abhängig zu sein. Hierfür müssen vorhandene KI-Ansätze optimiert und skaliert umgesetzt werden. Zudem sollen die Sicherheitsvorfälle so formalisiert werden, dass sie auch für andere Systeme verständlich sind und datenschutzgerecht ausgetauscht werden können. Dadurch wäre z.B. eine Kombination mit anderen SIEM-Systemen möglich. Aus den Vorfällen sollen sich auch klare Handlungsempfehlungen ableiten lassen, die den IT-Administrator z.B. über ein Ticket-System erreichen und ihn darauf hinweisen, dass eine Entscheidung getroffen werden muss. Diese Entscheidung wird dann durch das Ticket-System wieder entsprechend dokumentiert und kann für die spätere Auswertung herangezogen werden. Man verspricht sich davon verbesserte Diagnosen gemeldeter Vorfälle. Auf Basis von Icinga (Nagios) wird eine SIEM-Erweiterung entwickelt.

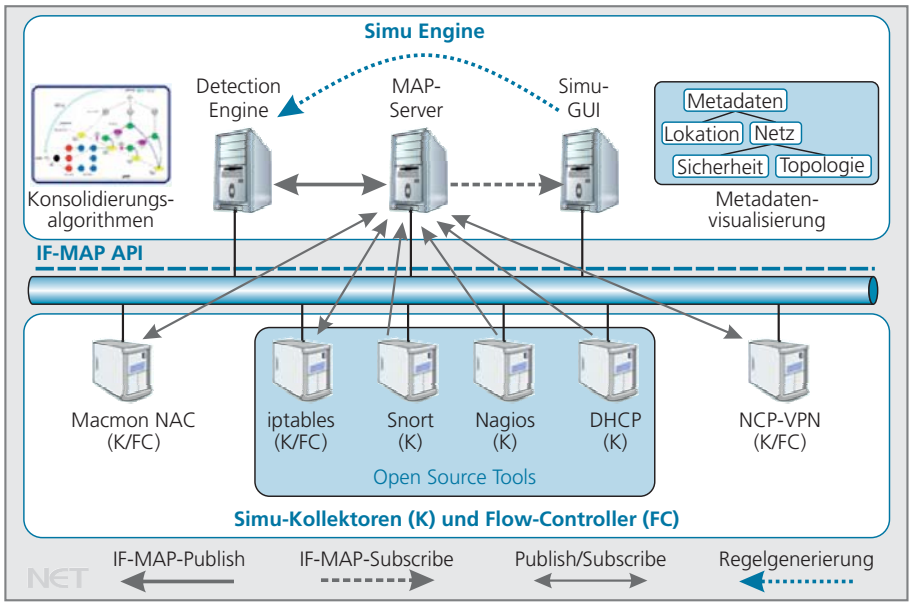

Bild 4: Grundlegende Simu-Architektur

Das Simu-Projekt möchte ebenfalls eine SIEM-Umgebung aufbauen. Allerdings soll die leichte Integrierbarkeit in KMU gewährleistet werden sowie die Nachvollziehbarkeit von relevanten Ereignissen und Vorgängen im Netz gegeben sein. Dabei soll der Aufwand für Konfiguration, Betrieb und Wartung gering ausfallen. Simu setzt auf die Spezifikationen der Trusted Computing Group und stellt das IF-MAP-Protokoll als einheitliches Datenformat und Schnittstelle in den Vordergrund. Darüber tauschen sich die IF-MAP-Clients, die als SIEM-Kollektoren fungieren, mit der Simu-Engine aus. Letztere besteht aus dem zentralen MAP-Server, der die Daten sammelt und korreliert, der Detection Engine und der Simu-GUI (*Bild 4*).

Im Gegensatz zu iMonitor wird das Simu-Projekt nicht auf eine bestehende Monitoring-Lösung aufsetzen und diese um SIEM-Funktionalität erweitern, sondern ausschließlich im Konsortium bereits vorhandene Systeme SIEM-fähig machen. Dabei kommt der Anomalieerkennung eine große Bedeutung zu, weshalb beide Projekte miteinander kooperieren.

Fazit

Es gibt viele Möglichkeiten, um vorausschauendes Netz- und Server-Monitoring zu betreiben. SIEM-Systeme beziehen zusätzlich die IT-Sicherheit ein und ermöglichen eine Risikoabschätzung. Dabei halten allerdings nicht alle SIEM-Systeme das, was sie versprechen. So weist z.B. das Ossim-System Lücken in der Umsetzung auf. Insbesondere die Open-Source-Variante verfügt u.a. nur über eine beschränkte Anzahl von Korrelationsregeln, wodurch die meisten Meldungen kein tatsächliches Ereignis erzeugen, was die Auswertung von Ereignissen erschwert. Eigene Regeln können zwar erstellt werden, erfordern aber wiederum Expertenwissen. Hinzu kommt, dass Ossim nicht alle gesammelten Ereignisse gleichermaßen auswertet. So kann es z.B. passieren, dass Snort einen kritischen Alarm erzeugt, der aber von Ossim nicht beachtet wird.

Um das Zusammenspiel zwischen unterschiedlichsten Sicherheitskomponenten gewährleisten zu können, sollte man sich daher von proprietären Systemen verabschieden und mehr auf offene Schnittstellen achten. Nur so kann ein effektives Zusammenspiel der verschiedenen Komponenten gewährleistet werden. Open-Source-Lösungen besitzen daher einen entscheidenden Vorteil bei der Monitoring- bzw. SIEM-Realisierung. Auch wenn Ossim jetzt noch Mängel ausweist, werden diese wahrscheinlich in absehbarer Zeit geschlossen werden. Allerdings stellen Kosten und Beherrschbarkeit solcher Systeme nach wie vor die Haupthindernisse für die Einführung dar. Forschungsprojekte wie iMonitor und Simu sollen dies zu ändern. *(bk)*