Anomalieerkennung leicht gemacht

Ziel ist die Erhöhung der Unternehmenssicherheit

Kai-Oliver Detken

Heutige Sicherheitssysteme basieren in den meisten Fällen auf Mustererkennung, um sicherheitskritische Vorfälle mitzubekommen. Dies kann aber nur gelingen, wenn vor einem Ereignis dieses schon bekannt ist. Ein „Hase-und-Igel"-Spiel beginnt, das oftmals vom Angreifer gewonnen wird. Daher ist eine Anomalieerkennung, die anhand von Sicherheitsvorfällen selbstständig lernt, wertvoller. Im Folgenden ein Überblick über Forschungsansätze und Herstellerlösungen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Jedes Unternehmen, unabhängig von der Größe, besitzt heute eine IT-Infrastruktur, die zumindest mit Antivirenlösungen, Firewalls, Monitoring- und Backup-Systemen gesichert ist. Oftmals kommen Remote-Zugänge über ein VPN-Gateway hinzu, die es externen Mitarbeitern ermöglichen, von außen sicher auf das Unternehmensnetz und seine Dienste zuzugreifen. Sind höhere Ansprüche vorhanden, so wird auf Zugangskontrolle mittels Network Access Control (NAC) oder Angriffserkennung über Intrusion-Detection- (IDS) und Intrusion-Prevention-Systeme (IPS) gesetzt. Allerdings sind die verschiedenen Systeme oft als Insellösungen implementiert, insbesondere, wenn sie nicht vom gleichen Hersteller kommen. Das erschwert auch die Erkennung von Angriffsmustern.

Aus diesem Grund sind sog. SIEM-Systeme (Security Information and Event Management) entwickelt worden, um systemübergreifend den aktuellen Sicherheitsstatus auswerten zu können. Über sie lassen sich auch Richtlinien definieren, anhand derer Vorfälle zu Compliance-Anforderungen überwacht werden können. Idealerweise beziehen SIEM-Lösungen auch andere Sicherheitssysteme über Schnittstellen ein und werten vorhandene Logs aus. Oft fehlen allerdings Möglichkeiten, eine automatisierte Bearbeitung von relevanten Sicherheitsvorfällen abzubilden. Ebenso sind die Systeme meist nur von Systemexperten konfigurierbar. Dies soll durch das Forschungsprojekt Clearer geändert werden.

Das Clearer-Projekt

Ziel des Clearer-Projekts (www.clearer-project.de) war es, eine automatisierte Überwachung und Steuerung von Compliance-Aspekten in der IT auch für kleinere Unternehmen auf Open-Source-Basis zu ermöglichen. Hierzu findet eine Vernetzung von Sicherheitssystemen wie NAC, IDS und Schwachstellenscanner statt, um auch Logdaten weiterer Systeme auswerten zu können. Dadurch kann festgestellt werden, ob das Unternehmen definierte Richtlinien eingehalten oder verletzt hat. Über die SIEM-Funktionalität lassen sich Angriffe und Verstöße permanent erkennen, bewerten und entsprechend priorisieren. Anschließend können bei relevanten Events Reaktionen eingeleitet oder IT-Administratoren sowie Compliance-Beauftragte informiert bzw. bei Ausübung ihrer Arbeiten unterstützt werden. Der Aufbereitung aller gesammelten Daten fällt dabei eine wichtige Rolle zu, um bei erfolgten Angriffen eine einfachere Forensik zu ermöglichen.

Die zentrale Sammlung aller sicherheitsrelevanten Informationen muss dabei die Anforderungen der Nachvollziehbarkeit und Nachweisbarkeit erfüllen. Auditoren sollen durch das System in der Lage sein, eine Compliance-Statuskontrolle einfacher durchzuführen, während IT-Administratoren von verständlichen Handlungsempfehlungen profitieren. Auf der einen Seite entsteht so eine große Datenmenge, um im Auditfall die korrekte Funktion des Systems nachweisen zu können, auf der anderen Seite sollten nur die relevanten Informationen den Nutzer erreichen. Ebenso soll das System auf den aktuellen Zustand der IT-Umgebung eingehen können und anhand der vorliegenden Daten weiter lernen, Anomalien erkennen und diese melden. Eine Zielsetzung ist, dass das IT-Compliance-Regelwerk dynamisch angepasst werden kann, um auf neue Bedrohungsszenarien schnell reagieren zu können. Dafür wurden verschiedene Szenarien definiert, die künftig weiter ausgebaut werden sollen.

Die entwickelte Clearer-Architektur besteht aus verschiedenen Komponenten (*Bild 1*), die gemeinsam eine Netzanalyse vornehmen:

- MAP-Server/VisITMeta: Zustandsanalyse und Historie des Netzes;
- NAC-Modul: Netzzugangskontrolle sowie Bereitstellung von Infrastruktur- bzw. Zustandsdaten durch macmon NAC;
- SIEM-GUI+: Benutzeroberfläche und Event-Anzeige;
- RabbitMQ: Event Message Broker;
- OpenVAS und Bro: Sensoren zur Ereignisgenerierung;
- MariaDB-Datenbank: Ereignispersistierung;
- Apache Camel: regelbasierte Routing- und Konvertierungs-Engine;
- Esper: Ereigniskorrelation und -bewertung;
- Solr und Banana-GUI: Auditing und gezielte Suche.

Bei der Datenverarbeitung wird eine Trennung von Ereignis- und Zustandsdaten vorgenommen. Das IF-MAP-Protokoll der Trusted Computing Group (TCG) wird zur Kommunikation mit dem zentralen MAP-Server genutzt, der die Zustandsdaten der Infrastruktur verarbeitet. Der Event Message Broker wird hingegen als Message-Queue für die aufkommenden Ereignisse verwendet. Neben der Performance spielen hier auch Compliance-Anforderungen eine entscheidende Rolle. Protokolle und die verwendete Datenbank müssen eine schnelle Schreibleistung aufweisen, um keine Ereignisse zu verlieren. Des Weiteren dürfen Ereignisse nicht verändert werden (Überprüfung der Compliance), und eine Selbstüberwachung ist vorgesehen. Treten Verluste oder Inkonsistenzen auf, müssen diese und der betroffene Zeitraum erkennbar sein.

Die SIEM-GUI+ fungiert als zentrale Oberfläche für den Benutzer des Clearer-Systems (*Bild 2*). Über sie wird die normale Systemfunktionalität genutzt, d.h., es werden die Informationen über die Compliance- sowie Netzzustände angezeigt und konfiguriert. Des Weiteren wurde ein Rollen- und Rechtemanagement integriert, um Administratoren und Benutzer zu trennen. Im Hintergrund wird dabei auf einen LDAP-Server zurückgegriffen. Dies erleichtert die Integration des Clearer-Systems in Infrastrukturen, die bereits einen Verzeichnisdienst verwenden, da so die Benutzer nur in einem System gepflegt werden müssen. Die GUI enthält ein integriertes Ticketsystem, mit dem der Zugriff auf Tickets und Queues über Berechtigungen gesteuert wird. Die Ereignisansicht der Oberfläche bietet künftig Filtermechanismen und Seitenumbrüche zur Aufbereitung der Anzeige, damit auch größere Ereignismengen angezeigt werden können. Eine Vorfälleübersicht ermöglicht mithilfe von Filterfunktionen die einfache Suche nach relevanten Compliance-Ereignissen. Weiterhin kann die Oberfläche zum Verwalten des Regelwerks genutzt werden, indem Parameter der einzelnen Regeln dynamisch verändert werden.

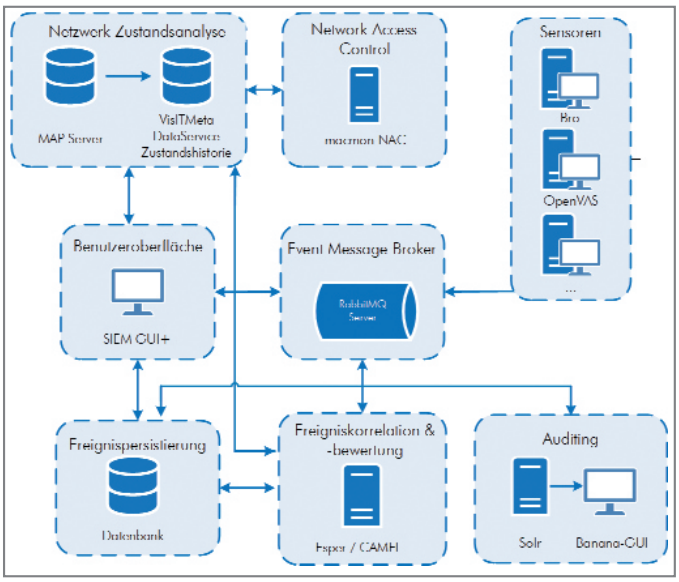

Bild 1: Clearer-Architektur in der Gesamtübersicht

Die interne Kommunikation wird über den RabbitMQ-Message-Broker und das Protokoll Advanced Message Queuing Protocol (AMQP) durchgeführt. Insbesondere Ereignisdaten, Korrelationsergebnisse usw. werden darüber übertragen. Dazu dienen je nach Anwendungsfall verschiedene AMQP-Exchanges und Message-Queues, wodurch eine Nachricht auf einfache Art und Weise an viele interessierte Empfänger geschickt werden kann. Sie müssen lediglich beim RabbitMQ die entsprechenden Message-Queues abonnieren. Um bei einer hohen Anzahl von Ereignissen zumindest die Größe der einzelnen Nachrichten selbst klein zu halten und so den Traffic zu reduzieren, wird der Inhalt der AMQP-Nachrichten im CBOR-Datenformat codiert.

Um externe Sensoren wie z.B. OpenVAS oder IDS Bro (Nachfolger von Snort) an den Message-Broker anzuschließen, werden entsprechende Komponenten benötigt, die die Daten in das Clearer-eigene Format konvertieren und die Kommunikation mit dem Broker übernehmen. Für viele Tools, die ihre Ereignisdaten über Logs zur Verfügung stellen, kann das Modul DECOmap verwendet werden, das in einem anderen Forschungsprojekt entstand (www.simu-project.de). Bei anderen Sensoren kommen speziell auf diesen Sensor zugeschnittene Entwicklungen zum Einsatz. Im Fall von OpenVAS wird ironvas von der Hochschule Hannover verwendet, was zusätzlich ermöglicht, OpenVAS-Scans über entsprechende AMQP-Nachrichten durch das Clearer-System selbst zu starten. Somit kann automatisch geprüft werden, ob eine erkannte

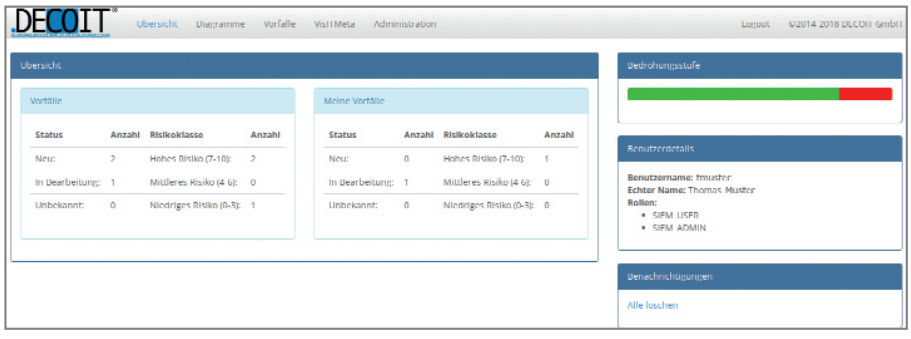

Bild 2: Oberfläche der SIEM-GUI+

Schwachstelle nach einer gewissen Zeit behoben wurde.

Die Ereigniskorrelation ist einer der zentralen Bausteine des Clearer-Systems. Diese arbeitet mit den Rohdaten der verschiedenen Sensoren, erkennt in diesen mithilfe eines Regelwerks bestimmte Muster und erzeugt daraus vordefinierte, abstrahierte Informationen. Diese werden in einem weiteren Schritt bewertet und von der Policy-Engine genutzt, um sicherheitsrelevante Vorfälle und im Speziellen Verletzungen von Compliance-Regeln zu erkennen. Für die Ereigniskorrelation und als Bewertungs-Engine wurde die CEP-Engine Esper ausgewählt, deren umfangreiche Korrelationsmöglichkeiten die Bewertung erleichtern. Durch die universelle Ausrichtung und Abfragesprache von Esper ist die Korrelation unterschiedlicher Ereignisse gegeben. Außerdem bietet Esper Zeitfenster und Operatoren zur Korrelation von Ereignissen aufgrund der zeitlichen Reihenfolge an. Weiterhin erlaubt sie die Verwendung von Variablen in Statements.

Die technische Umsetzung der Policy-Engine erfolgt ebenfalls über Esper. Dabei gestalten sich die Anforderungen im Vergleich zu der Bewertungs-Engine nicht wesentlich anders: Die Policy-Engine nimmt die bewerteten Ereignisse von Esper entgegen. Wie diese benötigt auch die Policy-Engine den Zugriff auf IF-MAP-Zustandsdaten und auf aktuelle sowie ggf. vergangene Ereignisdaten. IF-MAP-Daten werden in der ersten Umsetzung nur gelesen. Der größte technische Unterschied zur Bewertungs-Engine liegt in der Reaktion auf Ereignisse, auf die eine Aktion erfolgen muss. Außerdem kann die Anzeige des Compliance-Status über eine direkte Anbindung oder den Umweg über die Datenbank realisiert werden.

Anwendungsszenarien

Um die Einhaltung von Compliance-Anforderungen im Unternehmensnetz überwachen zu können, wurden Anwendungsszenarien definiert und implementiert. Denn nur Anforderungen, die das System kennt, kann es auch überprüfen, um Anomalien festzustellen. Zunächst wurden vier Szenarien festgelegt, die nach Bedarf erweitert werden sollen:

- Aktualitäts-Patch-Stand in Windows-Umgebung: Die Updates von Windows-Systemen werden überwacht und Alarmmeldungen ausgegeben, wenn nach einer definierten Zeit offene Sicherheitspatches nicht eingespielt wurden.
- Trennung von Produktions- und Büronetz: Anhand von Netzscans wird auf unterschiedliche Netze Rücksicht genommen und werden Analysen über den Sicherheitszustand durchgeführt.
- Netzverkehr außerhalb der Arbeitszeit;
- Überwachung sensitiver Daten.

Mithilfe dieser Szenarien kann z.B. eine Schwachstelle identifiziert und priorisiert werden. So können Scans automatisch in bestimmten Abständen oder manuell durchgeführt werden. Die Ergebnisse werden dann anhand von Infrastrukturinformationen bewertet und in der SIEM-GUI+ entsprechend angezeigt. Es wird ein Ticket generiert und eine E-Mail mit einer Handlungsempfehlung an den IT-Administrator gesendet. Nach z.B. 30 Tagen wird ein neuer Scan ausgeführt und erkannt, dass die Schwachstelle immer noch existiert. Es wird daher zusätzlich zu dem vorhandenen Ticket eine Compliance-Verletzung gemeldet. Zusätzlich erfolgt eine Protokollierung für die Rückverfolgbarkeit der Compliance. Durch die aktuell verwendeten Tools können Schwachstellen unterschiedlicher Betriebssysteme ermittelt werden. Grundsätzlich wird darauf geachtet, dass die Umsetzung der Szenarien unabhängig vom Zielsystem ist. Dennoch können aber auch Spezialfälle für bestimmte Systeme unterstützt werden.

Herstellerlösungen

Je mehr Anwendungsfälle ein solches System abdeckt, desto „intelligenter" wird es natürlich. Daher war die Zielsetzung von Clearer erst einmal, eine gewisse Basisfunktionalität abzubilden, um anhand neuer Anwendungsszenarien später weiterzuwachsen. Das System soll dabei kontinuierlich lernen, um Anomalien selbst erkennen und einstufen zu können.

Speziell SIEM-Hersteller versuchen, ähnliche Leistungsmerkmale umzusetzen. So bietet Logrhythm eigene Machine-Learning-Algorithmen an, die effektive Sicherheitsanalysen ermöglichen sollen und eine Automatisierung und Orchestrierung beinhalten. Hewlett-Packard geht mit der SIEM-Lösung ClearPass einen ähnlichen Weg. Hier werden ebenfalls das Log-Management vereinheitlicht und Sicherheitsmaßnahmen automatisiert. Wie bei Logrhythm werden auch umfangreiche Bedrohungsanalysen ermöglicht. Über den Policy-Manager lassen sich Richtlinien für Endgeräte definieren und ihre Durchsetzung zentral überwachen. Folglich gibt es auch Herstellerlösungen am Markt, die sich auf Anomalieerkennung spezialisiert haben und selbstlernende Funktionalität besitzen – allerdings nicht auf Open-Source-Basis.

Fazit

Es gibt sehr unterschiedliche Sicherheitssysteme am Markt, die das Sammeln von Informationen und Ereignissen ermöglichen, um Bedrohungen zu erkennen und dadurch auf Schwachstellen reagieren zu können. Zum einen basieren sie meistens auf Mustererkennung, zum anderen decken sie bestimmte Teilaspekte (Monitoring, SIEM, NAC) ab, die nicht unbedingt mit Lösungen anderer Hersteller zusammenspielen. Dadurch lässt sich eine übergreifende Logauswertung nicht immer vornehmen. Hinzu kommt, dass speziell passende SIEM-Lösungen entsprechend kostspielig sind und daher oftmals nur für große Unternehmen infrage kommen. Hier verfolgen insbesondere Logrhythm und Clearpass ein ähnliches Konzept. Die Handhabung ist allerdings für IT-Experten ausgelegt, wodurch die Reaktionszeit verlangsamt wird.

Clearer möchte dies ändern, um auf Sicherheitsvorfälle schneller reagieren zu können. Die zukünftige Entwicklung zu einem Produkt muss allerdings noch zeigen, inwieweit die ursprünglichen Anforderungen sich umsetzen lassen. *(bk)*