Security Information and Event Management (SIEM) im zusammen Spiel mit einem SOC (Security Operations Center)

Sicherheit verbessern und Datendiebstahl vorbeugen. Wichtige technische Funktionen aktueller SIEM-Lösungen. Analyse der verschiedenen Loesung's Anbieter. Echtzeit-Informationen und -Intelligenz nutzen. Magement von externen Loesungen. Workshops intern und Extern.
Im SOC werden alle Funktionen und Informationen, einschlieslich eines Ticket Systems und Change Management, sogar real estate Ueberwachung und Sicherheit zusammengefasst.
Dazu gehoert auch Fokus auf Planung, Ressourcen-, Risiko- und Change-Management, Erfahrung beim Umgang mit Teams aus verschiedenen Fachbereichen, Zusammenfassung aller Kompetenzen, taeglicher Management Report an die Vorgesetzten, Dokumentation usw.

Sicherheit mit Intelligenz

IT und Unternehmensnetzwerke werden permanent angegriffen, meist muss man sich darüber im Klaren sein, dass Angreifer auch bereits im eigenen Netzwerk sind. Das ist auch ganz unabhängig von der Firmengröße. Die Frage ist, was man daraus macht. Nicht zuletzt deshalb gehört SIEM zu den tragenden Säulen einer Sicherheits- und Verteidigungsstrategie.
Angriffe kommen nicht nur von der IT Seite, sondern auch durch taegliche Bedrohungen wie Einbruch und Diebstahl innerhalb des Unternehmens.
Dabei nimmt die Dynamik und Komplexität der Bedrohungslage permanent zu. Vielleicht kommen die Angreifer über genutzte Cloud-Services oder mobile Endgeräte – das macht die Lokalisierung nicht einfacher.

Ein guter Zeitpunkt, das Thema SIEM nochmals auf den Prüfstand zu stellen und sich mit der aktuellen technischen Situation vertraut zu machen. Oftmals sind bereits Teillösungen im Einsatz oder die bestehenden decken nicht mehr die Realität ab – Stichwort Cloud- Infrastrukturen. Zudem zeigen sich Angreifer und Angriffsmethoden im höchsten Maße flexibel und innovativ. Daher muss ein entsprechendes Sicherheitssystem ebenfalls dynamisch und intelligent agieren.
Aktuelle SIEM-Lösungen können in den gesammelten Daten versteckte Hinweise aufspüren und über Threat Intelligence Feeds mit aktuellen Bedrohungen abgleichen. Das Zusammenspiel von Analyse, Intelligenz und Echtzeit-Informationen von außen hat einen weit höheren Stellenwert als zu Beginn der SIEM-Entwicklung.
Gute Gründe, die Auswahl oder den Einsatz der eigenen SIEM-Lösung einmal zu hinterfragen.
Hierfür finden Administratoren wie Sicherheitsverantwortliche in diesem E-Handbook hilfreiche Informationen, wie sich die Technologie funktional und das Angebot der Anbieter entwickelt.

SIEM-Technologie deckt unautorisierte Zugriffe auf

Informationssysteme mit Passwort- Authentifizierung auszustatten ist eine gängige Praxis. Diese Portale sind oft über das Internet öffentlich zugänglich. Allerdings sind die Ausnutzung von Anmeldedaten, zufällig erratene Passwörter und Brute-Force-Angriffe immer noch die häufigsten Methoden für Einbrüche in ein Firmennetzwerk. Security Information and Event Management (SIEM) hilft Unternehmen dabei, Datendiebstahl durch derartige Einbruchsmethoden zu vermeiden. Setzt ein Unternehmen Appliances mit Passwortauthentifizierung (wie zum Beispiel VPN-Geräte, Webserver, SSH und ähnliche Technologien) ein, sollte es die Einbruchsbekämpfung auf Vordermann bringen.
Das gilt besonders dann, wenn Anmeldeportale über das Internet erreichbar sind. Automatisches Login-Tracking kann beim Aufspüren von schädlichen Aktivitäten helfen.
Das gilt nicht nur für außerhalb, sondern auch innerhalb des Firmennetzwerks. SIEM ist speziell dafür geschaffen, um diese Aufgabe zu bewältigen. Die Technologie sammelt und analysiert erfolgreiche und missglückte Anmeldeversuche auf verschiedenen Systemen. Damit lässt sich ermitteln, wenn Angreifer Zugangsdaten von Benutzerkonten übernommen haben.
Die von SIEM benötigten Daten für ein erfolgreiches Monitoring sind relativ unkompliziert. Alle Log-Dateien von Systemen, die Authentifizierungsaufzeichnungen enthalten, müssen gesammelt werden. Weiterhin ist es wichtig, sowohl erfolgreiche als auch missglückte Anmeldeversuche von allen Systemen, Geräten und Applikationen zu sammeln. Missglückte Anmeldeversuche sind ein Indikator, dass die Security-Systeme Ihre Arbeit gut machen.
Erfolgreiche Anmeldungen enthüllen dagegen, dass jemand Zugriff auf die Systeme hat. Eine erfolgreiche Anmeldung sollte aber nicht mit „autorisierter Zugriff" gleichgesetzt werden. Gestohlene Passwörter und schnelle CPUs für das Knacken von verschlüsselten Passwortdateien sind keine Seltenheit mehr.

SIEM-BEZUGSREGELN UND ALARMIERUNG

Eine SIEM-Bezugsregel lässt sich nutzen, um Teile des Monitoring-Prozesses für System-Logins und Authentifizierung zu automatisieren. Hier sind einige Beispiele für Bezugsregeln, die effizientes Zugriffs-Monitoring ermöglichen:

• Angriff auf ein einzelnes System, wenn der Angreifer alle Zugangsdaten auf diesem System ausprobiert.
• Eine Reihe von mehreren missglückten Anmeldeversuchen, auf die plötzlich ein erfolgreicher folgt.
• Angriff mittels Authentifizierungreihe (der Angreifer probiert die Zugangsdaten auf allen Systemen).
• Erfolgreiche Anmeldung zu ungewöhnlichen Tageszeiten. Das kann auf den Anwender oder das System bezogen sein.
• Erfolgreiche Anmeldung von ungewöhnlichen Orten. Auch das kann sich auf Anwender oder Systeme beziehen.

ANSICHTEN UND REPORTS

Zu den nützlichen Berichten und Dashboard- Ansichten für diese Anwendungsfälle gehören:
• Die wichtigsten Systeme mit missglückten Anmeldeversuchen.
• Das Verhältnis von erfolgreichen und missglückten Anmeldeversuchen.
• Der Trend zu missglückten Authentifizierungen.
• Anwender, von denen missglückte Anmeldeversuche auf mehreren Systemen verzeichnet sind.

Berücksichtigen Sie, dass Reports kein Ersatz für die Alarmfunktion sind. In vielen Fällen werden bösartige Aktivitäten von Menschen aufgedeckt, die die Berichte auswerten. Die Reports finden in erster Linie Neues, Ungewöhnliches oder Verdächtiges. Die Häufigkeit der Durchsichten variiert von monatlich, bis hin zu wöchentlich oder sogar täglich. Letzteres ist ideal und manchmal, wie zum Beispiel von der PCI DSS, vorgeschrieben. Solange Ihr Unternehmen mit der Häufigkeit der Durchsicht zufrieden ist, ist das akzeptabel. Hier ist zum Beispiel die Zeit zwischen einem Vorfall und dessen Entdeckung gemeint. SIEM-Technologie kann Daten automatisch sammeln und einen Alarm senden, wenn Angreifer die Passwörter raten. Allerdings muss innerhalb des Unternehmens sichergestellt sein, dass SIEM effiziente Vorfallsreaktionsprozesse und -prozeduren verfolgt. Diese müssen natürlich zunächst einmal existieren.
Wir sprechen hier von Alarmierung für eine weitere manuelle Analyse und entsprechenden Gegenmaßnahmen. Letztere sind in einigen Fällen mithilfe von DLP oder andere Firewall und Datenfilterprodukten automatisiert. Ein solides Verständnis für normale Log-Messbasen und typische Aktivitäten ist außerdem hilfreich. Dazu bedarf es aber nicht nur SIEM, sondern auch eines erfahrenen Mitarbeiters und am wichtigsten ein gut und Enterprise gerechtes, strukturiertes SOC (Security Operation Center) wo alle Informationen , Clients, DatenCenter, externe Serice Provider, Stakeholder usw. Zusammengefasst und analysiert werden, fuer eine schnelle Reaktion auf ein Sicherheits Problem.
Neben SIEM, dem Sammeln von Log-Dateien und der Analyse von Berichten, sollten für ein effizientes Serverzugriffs-Monitoring weitere Verfahren zum Einsatz kommen. Was passiert zum Beispiel, wenn der System-Administrator feststellt, dass sich ein Anwender von zwei verschiedenen Orten gleichzeitig anmeldet? Hat dieser Administrator die Berechtigung, Sitzungen zu terminieren? Kann er Konten deaktivieren, mit dem Vorgesetzten des Anwenders Kontakt aufnehmen oder andere Gegenmaßnahmen ergreifen? Solche Verfahren machen diese Aktionen reproduzierbar, schnell, effizient und helfen beim Tracking.

Eine clevere Verteidigung:
Überdenken Sie den Einsatz Ihrer SIEM-Produkte
SIEM bildet eine zentrale Rolle beim Sammeln von Daten und Überwachen der Netzwerkaktivität.

Unternehmen brauchen dynamische Verteidigungssysteme, die bösartiges Verhalten identifizieren, selbst wenn dieses Verhalten noch nie zuvor gesehen wurde. Schließlich sind diese Attacken für den Großteil der gefährlichen Zero-Day-Attacken verantwortlich, die täglich Schaden in IT-Umgebungen verursachen. Eine Schlüsselrolle in einer Verteidigung fällt den Produkten der Kategorie Security Information and Event Management (SIEM) zu. SIEM bildet eine zentrale Rolle beim Sammeln von Daten und Überwachen der Netzwerkaktivität.
Leider haben SIEM-Produkte dank problematischer Implementierungen und zu großen Versprechungen von Herstellern eine angekratzte Reputation. Viele SIEM-Lösungen wurden ausgerollt, um Compliance-Richtlinien zu erfüllen, wenige Unternehmen nutzen tatsächlich das Potential der Systeme vollkommen aus.
Die zweite Generation der SIEM-Produkte könnte das ändern. Die erweiterten Analyseund verbesserten Auswertungsfunktionen für gesammelte Daten bedeuten, dass eine größere Anzahl von Aktivitäten überprüft und in Kontext gesetzt werden kann. So lassen sich auffällige Aktivitäten in Echtzeit aufspüren.

DATENMENGEN MIT SIEM ÜBERPRÜFEN

Unternehmen erstellen kolossale Datenmengen:
E-Mails, Dokumente, Interaktionen in Social- Media-Netzwerken, Audio, Netzwerkdatenverkehr, Clickstreams. Hinzu kommen systemnahe Ereignisse: Log-Dateien, auf die zugegriffen wird, Änderungen in der Registry und Prozesse, die gestartet und gestoppt werden.
Systeminformationen, etwa zum Prozessor und Ausnutzung des Speichers, können ebenfalls nützlich sein, um unerwartete Veränderungen im Status der Systeme zu erkennen. Die schiere Masse an Daten, die ein System verarbeiten muss, zeigt, wie wichtig die Skalierungsfähigkeiten, Analysefunktionen und die Unterstützung

heterogener Quellen sind, wenn Sie SIEMProdukte der nächsten Generation wählen. Die Werkzeuge, um diese Daten auszuwerten und zu visualisieren, sind ein anderer Punkt, den Sie in jedem Fall beachten sollten. Zudem sollten Sie die Möglichkeit, Aktionen aufgrund der erstellten Analysen ausführen zu können, berücksichtigen. SIEM-Systeme müssen über eine „adaptive Intelligenz" verfügen, um diese Daten komplett nutzen und die in den Unternehmensdaten versteckten Hinweise aufspüren zu können.
Anders gesagt, das System (SOC) muss lernen, welches Verhalten zum normalen Arbeitsalltag gehört und welche Vorfälle auf einen Zwischenfall hinweisen. Die Systeme müssen außerdem in der Lage sein, Angriffsmuster zu identifizieren, selbst wenn diese Attacken über einen längeren Zeitraum stattfinden. Das Erstellen der SIEMRegeln ist ein sukzessiver Prozess, allerdings können Produkte, die sowohl regelbasiert wie auch ohne Regeln arbeiten, die notwendige Zeit bis zu einer funktionierenden Konfiguration enorm verringern. Sie können die Überwachung der Zugriffe automatisieren sowie die Anzahl der False-Positive-Meldungen reduzieren.
Selbstlernende Algorithmen sind zwar noch in ihrer Anfangsphase, aber eine Kombinationaus Überprüfung in Echtzeit mithilfe von Fuzzylogik, Verhaltensanalysen, Algorithmen zu Clustering und einem ausgefeilten Regelwerk kommt einer echten signaturlosen Überwachung ziemlich nah. Die Systeme sind inzwischen gut darin, unerlaubten Zugriff zu entdecken und zu verhindern, während sie zeitgleich normale Aktivitäten nicht beeinträchtigen.
Ebenfalls hilfreich sind Feeds von globalen Sicherheitsanbietern. Diese können Hinweise auf verdächtige Verhaltensweisen geben, selbst wenn diese Aktionen außerhalb des eigenen Netzwerks stattfinden. Setzen Sie auf Feeds, die flexible Informationen liefern, sich leicht ausrollen lassen und mit bereits existierenden Sicherheitsprodukten zusammenarbeiten. Unerlässlich ist die Echtzeitanalyse von strukturierten und unstrukturierten Daten.

CLOUD-BASIERTE STRUKTUREN BERÜCKSICHTIGEN

Unternehmen mit Cloud-basierter Infrastruktur sollten nach Anbietern Ausschau halten, die SIEM-Daten für lokal installierte SIEM-Produkte verfügbar machen können. Das ermöglicht eine einheitliche Übersicht über lokale und in der Cloud vorgehaltene Daten – solange die SIEMDaten des Anbieters mit dem lokal verwendeten System kompatibel sind.
In PaaS-Umgebungen (Platform as a Service) können die IT-Verantwortlichen eigene Agenten installieren, welche die Daten zu den lokal installierten SIEM-Systemen schicken können. Einige Lösungen arbeiten zudem mit den APIs von Software-as-a-Service- Anbietern (SaaS) zusammen, um Daten über mehrere Plattformen hinweg zu sammeln und zentral aufzubereiten. Damit lassen sich Audit- Berichte über alle genutzten Systeme erstellen, die Informationen über lokale und Cloud-basierte Systeme beinhalten.
Beachten Sie aber: Verfügbare Bandbreite, Latenz und Datentransferkosten können die Gegenmaßnahmen gegen bösartige Aktivitäten beeinträchtigen. Das bezieht sich auch auf die Ueberwachung und Administration von Routern, Switches, Firewalls, DMZ, Servers usw. Welche ebenfalls in dem SOC einen Teil der Ueberwachung bilden.
Die wichtigste Funktion einer modernen SIEM/SOC-Lösung ist allerdings der zentrale Überblick über alle gesammelten Informationen. Idealerweise beinhaltet dieser Bericht mögliche Gegenmaßnahmen, so dass Administratoren auf einen Blick sehen können, wo ihre Aufmerksamkeit benötigt wird. Nicht zu vergessen sind Funktionen, mit denen sich die Berichte in verschiedenen Formaten exportieren lassen – unterschiedliche Abteilungsleiter benötigen oft unterschiedliche Ausführungen der Berichte.
Dies kann Prozesse deutlich beschleunigen und es einfacher machen, die richtigen Entscheidungen zu treffen. Beschleunigte Entscheidungsprozesse geschehen nicht nur dadurch, dass SIEM mehr und mehr Informationen zugänglich gemacht werden. Vielmehr müssen auch die Sicherheitsverantwortlichen schnell reagieren und entsprechende Aktionen ausführen. Teams, die auf Zwischenfälle reagieren, müssen mit den jeweiligen Warnungen und Alarmen der SIEMLösung vertraut sein. Sie müssen durchdachte und getestete Prozeduren in petto haben, die bei einem Zwischenfall schnell und effektiv das Problem bekämpfen. Das sorgt nicht nur dafür, dass die richtigen Personen wissen, welche Aktionen sie treffen müssen, sondern auch, dass Gegenmaßnahmen koordiniert ausgeführt werden.
Regelmässige Workshops mit Internen und Externen, sowie Stakeholders sind unabdinglich.

SIEM ERFORDERT RESSOURCEN

Natürlich müssen Sicherheitsteams über dienotwendigen Ressourcen verfügen, um auf die von der SIEM generierten zusätzlichen Warnungen zu reagieren. Wer sich die Zeit nimmt, mithilfe von SIEM ein vollständiges Inventar der verfügbaren Daten zu erstellen und diese zu klassifizieren, erhält ein SIEM-System, das schnell auf etwaige Zwischenfälle reagieren und die entsprechenden Gegenmaßnahme priorisieren kann. Die meisten Produkte bringen passende Programme mit, über die sich das Netzwerk und Endpunkte katalogisieren lassen und die Administratoren eine Menge Zeit sparen können.
Sicherheit ist kein Produkt, sondern ein ständiger Prozess. Eine SIEM-Lösung, die über ausreichend Ressourcen und eine gute Konfiguration verfügt, gibt einen konstanten Überblick über den Sicherheitsstatus, aktuelle Bedrohungen und Schwachstellen. IT-Teams können Probleme schnell erkennen und die wichtigen Systeme vor Angriffen bewahren – das wiederum sorgt dafür, dass geschäftskritische Prozesse weiterlaufen.

Genügend Ressourcen und ordentlich geprüfte Verfahren vorausgesetzt, trägt eine SIEM/SOC-Lösung dazu bei, dass sich die gesamte Sicherheit eines Unternehmens langfristig verbessert.

Technische Neuheiten bei SIEM-Produkten

SIEM-Produkte (und früher IT Sicherheit) sind seit vielen Jahren das Security-Herz vieler Unternehmen. Diese Produkte gewährleisten ein zentrales Interface für Informationen von zahlreichen Security- Systemen. Dabei können sie für Logging und Compliance sowie für Incident Detection und Response genutzt werden. Die SIEM-Technologien (Security Incident and Event Management) haben sich über die Jahre verändert und es ist essentiell, diese Veränderungen beim Aufbau der eigenen SIEM-Strategie zu berücksichtigen.

Hier sind einige Neuheiten, die Administratoren berücksichtigten sollten, wenn sie nach einer neuen SIEM-Lösung suchen oder die Qualität der existierenden SIEM-Produkte bewerten wollen.

BIG DATA

Einer der größten Trends der letzten Jahre war der Übergang von relationalen Datenbanken auf Big- Data-Modelle. Wird SIEM nur als zentralisiertes Logging verwendet, so ist eine Transformation zu Big Data eventuell keine gute Entscheidung, da potenziell Informationen verloren gehen können. Big Data verwendet keine relationalen Datenbanken, so dass nicht gegeben ist, dass jedes gespeicherte Datenbit auch wirklich zurückgeholt
werden kann. Nutzt das Unternehmen SIEM für Incident Detection und Response, so kann ein Big- Data-Modell die Detection-Rate erhöhen, da hier mehr Daten gesammelt und verarbeitet werden, um Muster von Attacken zu finden.

THREAT INTELLIGENCE FEEDS

SIEM-Produkte unterstützen immer mehr die Verarbeitung von Threat Intelligence Feeds. Diese Feeds enthalten Informationen über Indikatoren von Bedrohungen. Dazu gehören unter anderem IP-Adressen, Host-Namen und URLs, die von Hackern genutzt werden. Jeder Feed verfügt über eine Bewertung der Bedrohungsindikatoren. Damit werden beispielsweise der Grad der Bedrohung und die zusätzlichen Metadaten, die der Threat Intelligence Kontext geben, eingeschätzt. Wird ein Threat Intelligence Feed mit SIEM-Daten verwendet, so gewährleistet dies umfassende Informationen und ermöglicht eine schnellere Identifizierung von Vorfällen sowie sichere Reaktionen. Stellen Sie sicher, dass ihre SIEMLösung Threat Intelligence Feeds unterstützt.

CLOUD-BASIERTE INTEGRATION

Logging in Multi-Tenant-Clouds (mehrere Nutzer) war bislang eine Herausforderung für SIEM. Mittlerweile gibt es zahlreiche Cloud-basierte SIEM-Services und -Produkte, die Audit-Logs sammeln und an die regulären (nicht-Cloud) SIEM-Server des Unternehmens senden. Einige dieser Cloud-basierten SIEM-Lösungen werden von den gleichen Herstellern angeboten, die auch reguläre SIEM-Angebote offerieren. In diesem Fall ist eine Integration recht einfach. In anderen Fällen benötigt die Firma spezielle Planung und Tests, um zu bestimmen, ob die Daten aus der Cloud sich in kurzer Zeit für das Enterprise-SIEM-System sammeln, verarbeiten und senden lassen, um so Incident Response zu unterstützen.

VERTEILTE ANALYSE

SIEM wurde oft nur als zentrale Log-Verarbeitung betrachtet. Unternehmen können nun aber optimierte Skalierbarkeit gewährleisten, indem individuelle Datensammelstellen (Data Collection Points) ihre eigene Datenanalyse und -verarbeitung durchführen.

Wenn eine SIEMLösung kaum mit dem Workload mithalten kann, so bringt eine verteilte (distributed) Architektur hohen Nutzen. Firmen sollten bei der Auswahl eines SIEM-Produktes diese vier Technologien im Auge behalten – möglicherweise wollen manche SIEM wirklich nur für zentralisiertes Logging nutzen und halten diese Neuheiten für weniger wichtig. Allerdings sollten sich IT-Manager darüber im Klaren sein, wie viel mehr ein SIEM Produkt leisten kann als reines Log-Management. SIEM kann ein wertvolles Tool für die schnelle Entdeckung von Gefahren sein und Daten von Systemen und Vorfällen mit Threat Intelligence gegeneinander abgleichen.

Monitoring, Big Data und MapReduce: So unterscheiden sich SIEM-Anbieter

Neben der veränderlichen Erwartungshaltung von Security-Teams haben SIEM Plattformen auch eine Evolutionsphase durchlebt. Einstige Nischenanbieter, die sich heute in einem belebten Marktumfeld wiederfinden, haben in Reaktion auf die wachsenden Anforderungen von Unternehmen ihre Produkte aufpoliert. Sie haben zudem neue Fertigkeiten etabliert, um sich von anderen Dienstleistern weiter abzusetzen.

Der SIEM-Markt ist alles andere als statisch. Die Marktführer von gestern sind längst nicht mehr die „sichere Bank", die sie einmal waren.

Mannigfaltige Produkte weisen in gleich mehreren Bereichen erweiterte oder verbesserte Möglichkeiten auf. Nachfolgend finden Sie einige Fertigkeiten, die Anbieter gerne nutzen, um auf dem Markt Fuß zu fassen und den Weg in Ihr Netzwerk zu finden.

ANWENDUNGS- UND DATENBANK- MONITORING AUF SIEM-PLATTFORMEN

Die Auswertung von Log-Dateien und das Sammeln von Netzwerkaktivitäten sind Basisfunktionen von SIEM-Plattformen. Ein netzwerklastiger Blick auf Sicherheit hat allerdings nur begrenzten Nutzen. Die Fähigkeit, die Funktionsweise von

Anwendungen zu analysieren und die erwünschte Interaktion der Anwender mit diesen Anwendungen zu ermitteln, kann nicht in der Netzwerkschicht angesiedelt werden. Missbrauch muss im Kontext der Anwendungsfunktion bewertet werden.
Aus genau diesem Grund wurden zusätzliche Möglichkeiten für Datensammlung und -analyse in SIEM-Plattformen integriert – oder in einigen Fällen sogar vollständig mit ihnen fusioniert. Features wie Anwendungs- Monitoring, Datenbankaktivitäts-Monitoring und Dateiintegritäts-Monitoring sind gängige Beispiele für solche Ergänzungen. Diese Features betrachten das Verhältnis zwischen intensiver und normaler Aktivität und können damit sehr viel besser zulässige Aktivitäten von abzuwehrenden Angriffen unterscheiden.

LDAP UND ACTIVE DIRECTORY: IDENTITY-SERVICES-INTEGRATION MIT SIEM
Echte Nutzeridentitäten mit Aktivität verknüpfen zu können, hat viele SIEM-Systemanbieter dazu bewegt, die Integration von Identitäts- Management-Systemen wie Lightweight Directory Access Protocol (LDAP) und Active Directory voranzutreiben. Statt lediglich den generischen Namen eines Dienstkontos (zum Beispiel „App User") oder Benutzerkontos auszugeben, können SIEM-Plattformen diese generischen
Bezeichner mit tatsächlichen Benutzeridentitäten verknüpfen. Dies sorgt für ein klares Bild des Nutzerverhaltens über multiple Benutzerkonten hinweg in verschiedenen Netzwerk-, Dienste- und Anwendungsschichten.

BIG-DATA-ENGINES
In Reaktion auf den stetig ansteigenden Bedarf an schnellem Speicher für große Datenmengen und zwecks Analyse enormer Datenvielfalt nahezu in Echtzeit haben viele SIEM-Anbieter ihre Plattformen weg von der traditionellen relationalen Datenhaltung hin zu nicht-relationalen Big-Data- Engines (wie Hadoop) geführt. Diese Plattformen sind elastischer – sie skalieren deutlich besser als relationale Plattformen – und bieten beispiellose Geschwindigkeit beim Hinzufügen von Daten.
Dies ermöglicht höhere Performanz bei steigender Ereignisanzahl. Die fehlende Unterstützung der Vorteilerelationaler Plattformen (relationaler Speicher, transaktionale Integrität) machen sie mit anderen Vorzügen (intrinsische Hardwareausfallsicherheit, Speicherung flexibler Datentypen) als nur dem schnellen Einfügen von Datensätzen und der besseren Skalierbarkeit wett.

PARALLELVERARBEITUNG
Die Verwendung von MapReduce- Abfragetechnologien erlaubt in Big-Data- Umgebungen umfassende Parallelverarbeitung, welche die Datenanalyse signifikant beschleunigt. Überdies entfällt auch die Notwendigkeit vorheriger Aggregation, Normalisierung und Korrelation der Daten. Die Mapping-Funktion,
intrinsischer Bestandteil der MapReduce-Abfragen, übernimmt die Korrelation, und die Reduction-Funktion vollzieht die Aggregation.Daraus resultiert ein Datenbestand, der nahezu ohne Verzögerung durchsucht werden kann.

Real-time Security Intelligence – mehr als nur SIEM der nächsten Generation
In letzter Zeit ist die Notwendigkeit in den Mittelpunkt gerückt, in Information- Security-Lösungen zu investieren. (Ausbau eines SOC)
Cyberangriffe haben zugenommen, dauernd muss man sich mit internen Herausforderungen plagen und lang anhaltende Angriffe (auch Advanced Persistent Threat, APT genannt) sind wesentlich ausgeklügelter. Dazu kommen noch die Enthüllungen von Snowden und ständig auftauchende Zero-Day-Angriffe. Dadurch hat man von der Veröffentlichung einer Lücke bis zur Reaktion überhaupt keine Zeit mehr. Die Fachwelt ist sich durchaus einig, dass bessere Lösungen notwendig sind.
Unternehmen müssen davon ausgehen, dass sich Angreifer bereits in ihrem Netzwerk befinden. Jede Firma und jeder Anwender ist ein potenzielles Ziel für Cyberkriminelle. Auf der anderen Seite wird es immer schwieriger, die Angreifer ausfindig zu machen, da sie immer ausgefeiltere Methoden verwenden. Außerdem gibt es kein einzelnes Perimeter mehr, wo Organisationen Ihre Security-Systeme platzieren können, um ein Eindringen von außerhalb in das Netzwerk zu verhindern. Möglicherweise sind die Cyberkriminellen über **mobile Geräte** eingedrungen, greifen Cloud-Services an und so weiter.
Die Komplexität nimmt laufend zu.
Auf dem Markt sehen wir den Aufstieg neuer Lösungen. Sie versprechen, den Kunden bei ihren Herausforderungen unter die Arme zu greifen. Sehen wir uns allerdings zunächst die aktuellen Lösungen an, die aber nicht ausreichend sind. Standardmäßige Intrusion Detection Systems (IDS) oder Intrusion Prevention Systems (IPS) sind durch das Konzept eines am Rande befindlichen Gerätes eingeschränkt, wenn es keine wirklich definierte Grenze mehr gibt. Sie sind zudem limitiert, wenn komplexe Angriffsszenarien eine größere Anzahl an Geräten betreffen.
(SIEM) ist immer noch eine Tool-orientierte Herangehensweise, die erhebliche Anpassungen erfordert. Solange Sie diese Systeme nicht ordnungsgemäß konfigurieren können, werden Sie beispielsweise Ihre Erwartungen in einem Security Operations Center (SOC) nicht erfüllen. Brauchen Sie immer mehr Echtzeit-Informationen für die entsprechenden Analysen, sind diese Systeme hinsichtlich Skalierbarkeit möglicherweise eingeschränkt.

Next-Generation Firewalls (NGFW) sind wiederum ein Randgerät und wie alle anderen aus diesem Bereich auch entsprechend limitiert.

ECHTZEIT-INFORMATIONEN UND -INTELLIGENZ

Services mit Echtzeit-Informationen, wie zum Beispiel über neu entdeckte Zero-Day-Angriffe, liefern wertvolle Informationen. Sie lösen allerdings das Problem nicht. Außerdem stellen sie keine Analysen zur Verfügung, was sich in der internen Infrastruktur abspielt. In der näheren Vergangenheit haben wir allerdings beobachtet, dass immer mehr Anbieter in Richtung integrierter Methoden für Echtzeit-Security- Intelligenz (Real-time Security Intelligence) marschieren und diverse Technologien und Services kombinieren:

Durch Big-Data-Analyse kann man eine große Menge an Daten untersuchen. Als Basis sind sowohl Regeln als auch Muster möglich.

- Unterstützung für sowohl Echtzeit-Analyse als auch Verlaufs- oder rückblickende Analyse. Damit lassen sich neue Ereignisse mit solchen in Verbindung bringen, die irgendwann in der Vergangenheit aufgetreten sind.
- Integration mit existierenden Informationsquellen wie zum Beispiel SIEM-Tools.
- Integration mit Echtzeit-Security- Informationsdiensten, die aktuelle Informationen zu neu entdeckten Security-Herausforderungen liefern.
- Services, die automatisch aktualisierte Regeln und Muster für Analysen bereitstellen – Konfigurationen, bei denen die Kunden beispielsweise ihre „Real-time Security Intelligence"-Systeme nicht manuell auf dem aktuellen Stand halten müssen
- Services, die die Kunden mit Analysen unterstützen. Dazu gehören Dienstleistungen von Experten für die Unterstützung des SOCs.
- Integration mit IT-GRC-Lösungen. Hier werden die identifizierten Herausforderungen aufbereitet und die Risiko- Informationen in Form von Dashboards für IT-Abteilung und Geschäftsleute visualisiert.

Real-time Security Intelligence ist zu einer Mischung aus Services und Software geworden. Sie kombiniert diverse Angebote, die heutzutage zwar existieren, jedoch voneinander getrennt sind. Kunden bekommen damit bessere Einblicke, was in ihren Netzwerken vor sich geht und wie die, derzeitige Sachlage ist. Einige Anbieter stellen sogar die Möglichkeit zur Verfügung, dass man, basierend auf deren analytischen Services, die Netzwerkkonfiguration ändern kann.

NEUE SERVICES, NEUE KOMBINATIONEN

Wir erwarten eine schnelle Entwicklung in diesem Bereich und gehen davon aus, dass noch mehr Services hinzukommen. Großes Potential hat dabei die Zusammenführung von Management- Systemen für Netzwerkkonfiguration mit Realtime Security Intelligence. Somit lassen sich zum Beispiel Firewall- Einstellungen spontan ändern. Ein weiteres Beispiel ist die Integration mit Software Defined Computing Infrastructures (SDCI), um die Konfigurationen von Netzwerk, Storage und virtuellen Maschinen bei der Entdeckung neuer Schwierigkeiten zu ändern. Somit minimieren Sie automatisch und dynamisch die Angriffsoberfläche.

Bei der Entwicklung hin zu Real-time Security Intelligence beobachten wir im Moment, dass sich einige Anbieter mehr auf Big-Data-Security- Analysen fokussieren. Andere wiederum legen den Schwerpunkt auf Online-Services. Aber wir kratzen hier derzeit nur an der Oberfläche. Wie wir uns mit Security beschäftigen, wird sich grundlegend ändern. Weiterhin setzen wir SOCs ein und begeben uns damit weit über die Grenzen von „SIEM der nächsten Generation" hinaus.