INFORMATION SECURITY SOLUTIONS

SIEM: SECURITY INFORMATION & EVENT MANAGEMENT

Effizient Missbrauch verhindern und Compliance sicherstellen

Der Kontrollaufwand von IT-gestützten Tätigkeiten hinsichtlich der Einhaltung von Compliance-Regeln steigt durch zunehmende Komplexität der IT-Landschaft und der Masse von Protokolleinträgen. Gleichzeitig verschärfen sich gesetzliche und regulatorische Anforderungen, sodass Unternehmen der Verpflichtung, jederzeit den Nachweis über eine ordnungsgemäße Nutzung von IT-Systemen führen zu können, nur noch automatisiert nachkommen können.

Jedoch nicht nur der Gesetzgeber fordert beispielsweise durch das Bundesdatenschutzgesetz oder § 203 StGB hinreichende Kontrolle. Unternehmen haben ein vitales, eigenes Interesse, Sicherheitsvorfälle aufzudecken.

„Spionage via Internet kennt keine zeitlichen und sprachlichen Barrieren, sie ist effizient und kostengünstig zugleich. [...] Die zunehmenden elektronischen Attacken auf Computernetze stellen mittlerweile eine größere Gefahr dar als traditionelle Ausspähungsversuche."
Der Verfassungsschutz

Der deutschen Wirtschaft gehen geschätzte 20 bis 50 Milliarden Euro pro Jahr durch Wirtschaftsspionage verloren und das Risiko steigt durch verstärkten Datenaustausch über unsichere Netze.

Die Realität in Unternehmen ...

... reflektiert indessen nicht die Bedrohungslage, die den Verantwortlichen oft unbekannt und nur schwer quantifizierbar ist. Eine Vielzahl von Protokolleinträgen, die die Tätigkeiten einer Person dokumentieren, bleiben daher unausgewertet und eventuelle Sicherheitsvorfälle mithin unentdeckt. Wird im Verdachtsfall dennoch ausgewertet, erfolgt eine oft verspätete Reaktion auf Sicherheitsereignisse, da die Datenflut mangels geeigneter Werkzeuge manuell untersucht werden muss. Ergeben sich dann auch noch „False Positives" (der Verdacht stellt sich als unbegründet heraus) oder bleibt eine forensische Analyse erfolglos, da wichtige Information bereits verloren sind, erscheint der Aufwand womöglich als nutzlos und zukünftig nicht erforderlich.

Doch nicht nur zur Schadensbegrenzung sollte schnell gehandelt werden, sondern auch zur Kanalisierung eines bisweilen über das tatsächliche Schadensmaß hinausgehende Medieninteresse, wenn ein „Datenskandal" vermutet wird.

Ist der Bann einmal gebrochen und die Entscheidung für eine automatisierte Auswertung von Protokolleinträgen gefallen, trifft man auf eine scheinbar unüberschaubare Artenvielfalt und Anzahl von Quellen, z. B.

- Firewalls und Intrusion-Detection- und Prevention-Systeme
- Identity & Access Management
- Virenschutz
- Datenbanken
- Netzwerkkomponenten
- Syslog-Server

Die Fragestellung „Wie können Zusammenhänge zwischen Protokolleinträgen, die auf ein Sicherheitsereignis hindeuten, angesichts der Menge und Vielfalt von Daten überhaupt erkannt und verständlich dargestellt werden?" liegt nahe.

Die Antwort geben Ihnen die Berater von Sopra Steria Consulting.

Der Lösungsansatz heißt …

… „Security Information & Event Management" (SIEM). Wenngleich SIEM allzuoft auf eine Software reduziert wird, ist es doch ein Managementsystem, welches zunächst die unternehmensspezifischen Anforderungen erfasst, diese mittels Tool-Unterstützung umsetzt und das zugrundeliegende Regelwerk dann kontinuierlich verbessert.

SIEM braucht klare Anforderungen …

… im Rahmen eines strikten und fortlaufenden Anforderungsmanagements. Anforderung bedeutet in diesem Zusammenhang zunächst eine klare und umfassende Definition, was ein Sicherheitsereignis darstellt und mit welcher Priorität es verfolgt werden soll. Ist es in einem Unternehmen nicht ungewöhnlich, dass sich Mitarbeiter prinzipiell zu jeder Tages- und Nachtzeit und von jedem Ort der Erde aus mit dem Firmennetzwerk verbinden, kann eine Remote-Einwahl an einem Sonntagmorgen um 3 Uhr in einem anderen Unternehmen bereits als potenzielles Sicherheitsereignis gewertet werden, welches näherer Aufmerksamkeit bedarf. Eindeutiger ist der Fall wohl, wenn ein SIEM feststellt, dass ein Mitarbeiter in einer Unternehmenslokation in Deutschland mit einer SAP-Anwendung arbeitet und sich gleichzeitig versucht, von China ausgehend in das Firmennetzwerk einzuwählen (ein Fall, der übrigens deutlich macht, dass nur eine Korrelation von Ereignissen verschiedener Systeme ein vollständiges Bild liefert).

Weitere Anforderungen stellt das Berichtswesen an ein SIEM. Während ein CIO wohl eher an einem Kurzbericht interessiert ist, der ihm signalisiert, dass das Managementsystem funktioniert und auf alle Sicherheitsereignisse zeitnah und angemessen reagiert wird, möchte ein Administrator ggf. in Abstimmung mit dem Datenschutzbeauftragten oder dem Betriebsrat im Detail sehen, wann auf welchen Systemen in seinem Verantwortungsbereich welche Ereignisse aufgetreten sind. Zum Berichtswesen gehören auch Überlegungen, ob und wie auf Sicherheitsereignisse durch wen reagiert werden soll. Das Prinzip sollte „so schnell wie möglich und angemessen" lauten. Für die Praxis bedeutet das, es gibt Ereignisse, die nur zur Kenntnis genommen werden und evtl. in einer Statistik auftauchen, aber auch Ereignisse, die einen Vorstand um die Nachtruhe bringen und zu denen strenges Stillschweigen vereinbart wird. Es versteht sich von selbst, dass eine Abstimmung des Eskalationsprozesses vor einem Sicherheitsereignis sowohl eine Panikreaktion als auch eine ungebührliche Verzögerung der Aufklärung vermeiden hilft.

Schließlich ist es unerlässlich, sich über Archivierungsanforderungen Gedanken zu machen, wenn man bedenkt, dass in einem Unternehmen täglich durchaus Protokolleinträge im Umfang von Hunderttausenden bis zu einigen Millionen anfallen können (dies kann einem Speicherplatzbedarf von mehreren Gigabyte entsprechen).

Die Regeln machen den Unterschied …

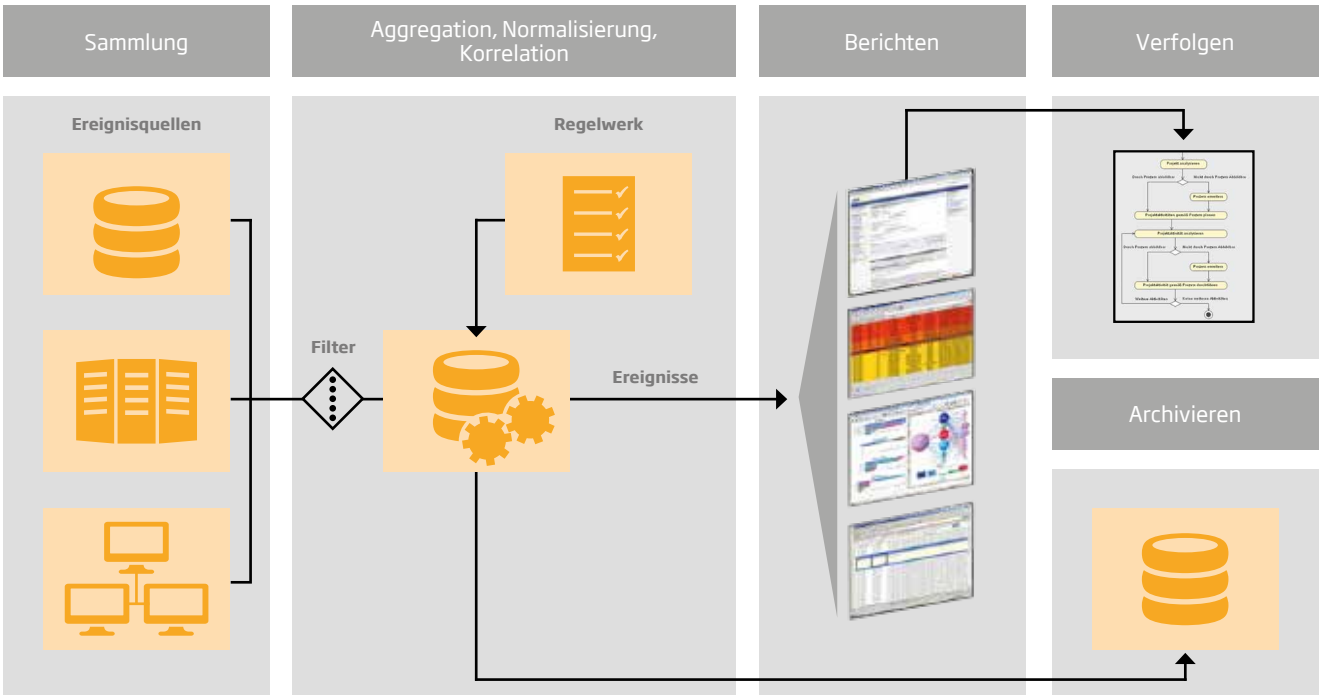
… zwischen einem hilfreichen und einem nutzlosen SIEM-System. In einem SIEM-System werden die Definitionen von Sicherheitsereignissen mithilfe von Regeln etwa der Form „Wenn ein Protokolleintrag mit Eigenschaft A und Protokolleintrag mit Eigenschaft B existiert, dann melde Sicherheitsereignis C mit Wahrscheinlichkeit D" abgebildet. Diese Wahrscheinlichkeit kann beispielsweise aus der Anzahl oder einer Gewichtung von Ereignissen, die auf ein bestimmtes Sicherheitsereignis hindeuten, abgeleitet werden. Ein SIEM-System ermöglicht kein „Plug & Play", denn die Entwicklung eines konsistenten und wirksamen Regelwerkes ist ein kontinuierlicher Prozess, der durch kein Werkzeug automatisiert werden kann; sie erfordert Erfahrung in Bedrohungsszenarien und Risikoeinschätzungen und laufende Anpassung in Orientierung an vergangenen Vorfällen. In jedem Fall sollen die resultierenden Meldungen geeignet sein, die für einen Notruf so wichtigen „W-Fragen" zu beantworten:

- Was genau ist passiert? Z. B. „Wiederholte erfolglose Zugriffsversuche auf geheime Entwicklungsunterlagen"
- Wo ist etwas passiert? System, Anwendung, Netzwerksegment etc.
- Wann ist etwas passiert? Datum, Uhrzeit und Zeitzone.
- Wie ist das Ausmaß? Z. B. „Fünf Benutzer versuchen seit drei Stunden mit 20 Zugriffsversuchen pro Stunde auf Dokumente der Server X, Y und Z zuzugreifen."

Das SIEM-Prinzip …

… ist nun einfach zu verstehen. Es besteht aus sechs Stufen:

- Sammlung: Zunächst werden Protokolldaten von angeschlossenen Zielsystemen gesammelt. Dies erfolgt entweder über spezielle Agenten auf den Zielsystemen oder via Syslog (mit dem klaren Vorteil der Nutzung ohnehin vorhandener Werkzeuge).
- Aggregation: Anschließend werden die Daten an einer zentralen Stelle aggregiert. Hier kann bereits eine Filterung erfolgen in Protokolleinträge, die ausgewertet oder nicht ausgewertet werden sollen. Eventuell verbleiben Protokolleinträge, deren Filterungskriterium einer Klärung bedürfen.
- Normalisierung: Daten aus verschiedenen Quellen haben in der Regel eine unterschiedliche Syntax in Format und Inhalt. Um eine Vergleichbarkeit zu ermöglichen, müssen die Log-Einträge in ein einheitliches Format mit gemeinsamer Semantik gebracht werden.
- Korrelation: Die Anwendung des Regelwerkes ist das Herzstück eines SIEM-Systems, an dem sich der Nutzen entscheidet.
- Berichten/Verfolgen: Die Ergebnisse der Korrelation werden gemäß vorab definierter Berichtsvorlagen dokumentiert, an Meldeprozesse eskaliert und in angeschlossene Prozesse (z. B. Incident Management) eingespeist.
- Archivieren: Den Abschluss bildet eine Archivierung gemäß gesetzlicher oder regulatorischer Vorgaben. Praktikabel ist hier ein abgestuftes Konzept, in dem Daten noch für einige Monate in einem Zwischenarchiv mit schnellem Zugriff gehalten werden, um für eventuell forensische Analysen zur Verfügung zu stehen, bevor sie in ein Langzeitarchiv verschoben werden.



Die Expertise von Sopra Steria Consulting …

… zeichnet sich aus durch:

- Umfangreiche Erfahrung in Technologien, Standards und Produkten
- Starkes Know-how im Design von Prozessen sowie bei der Erstellung von Sicherheits- und Datenschutzkonzepten
- Tiefgreifendes Verständnis der Kundensituation
- Expertise in Branchenspezifika und deren Compliance-Anforderungen
- Produktunabhängige Beratung mit starken Partnerschaften
- Unterstützung bei der Beurteilung und Auswahl von Produktlösungen

Beispiele aus unserem Beratungsangebot sind:

- Unabhängige Beurteilung der bestehenden SIEM-Prozesse auf Basis international anerkannter Standards, z. B. ISO 27001, CobiT etc.
- Vorprojekte zum Scoping von geplanten SIEM-Projekten und zum Proof-of-Concept für eine geplante SIEM-Lösung (prototypisch)
- Erstellung einer SIEM-Strategie und -Grobkonzeption und Implementierung von SIEM-Lösungen inkl. Pilotbetrieb/Migration
- Mitwirkung bei Wirtschaftlichkeitsbetrachtungen sowie Beurteilung von Einsparpotenzial und Return on Security Invest
- Beratungsleistungen und Unterstützung bei der Einführung von SIEM Policies und -Prozessen

Sie möchten mehr über Security Information & Event Management oder unser Leistungsangebot erfahren?

Sprechen Sie uns an, wir beraten Sie gerne!

Über Sopra Steria Consulting (www.soprasteria.de)

Sopra Steria Consulting zählt zu den Top 10 der Business Transformation Partner in Deutschland. Als ein führender europäischer Anbieter für digitale Transformation bietet Sopra Steria mit 36.000 Mitarbeitern in über 20 Ländern eines der umfassendsten Portfolios für End-to-End-Services: Beratung, Systemintegration, Softwareentwicklung, Infrastrukturmanagement und Business Process Services. Unternehmen und Behörden vertrauen auf die Expertise von Sopra Steria, Transformationsvorhaben, die geschäftskritische Herausforderungen adressieren, erfolgreich umzusetzen. Im Zusammenspiel von Qualität, Leistung, Mehrwert und Innovation befähigt Sopra Steria seine Kunden, IT optimal zu nutzen.

A3_18039_1504-SEC-d

Tel.: +49 40 22703-0
www.soprasteria.de