Eine Welt, in der jeder einen angemessenen Platz zum Leben hat!

Bereits seit 2004 unterstützen wir pro Quartal wechselnde Hilfsorganisationen. Die Vorschläge hierzu kommen aus den Reihen unserer Mitarbeiter. Im zweiten Quartal 2009 ging unsere Spende an Habitat for Humanity International. Die Organisation engagiert sich in über 100 Ländern und baut dort mit Hilfe von Spenden sichere und angemessene Unterkünfte für arme Familien und organisiert den Wiederaufbau in Katastrophengebieten. Freiwillige aus aller Welt helfen dabei. Die Häuser werden nicht verschenkt. Interessierte Familien, die den Auswahlprozess erfolgreich durchlaufen haben, erhalten ein gering verzinstes oder sogar zinsloses Darlehen zur Finanzierung ihres Hauses. Diesen Kredit können sie über viele Jahre, entsprechend ihren Möglichkeiten, zurückzahlen. Außerdem arbeiten alle zukünftigen Eigentümer beim Hausbau mit und helfen ihren Nachbarn in gleicher Situation. Auf allen fünf Kontinenten wurden so mehr als 300.000 Häuser gebaut und mehr als 1,2 Millionen Menschen konnte geholfen werden.

Weitere Informationen finden Sie unter www.habitat.org

Jedes Jahr gibt es in Tadschikistan bis zu 5000 Erdbeben. Habitat for Humanity hilft den Menschen, ihre Häuser wieder bewohnbar zu machen.

atsec wird vom PCI Security Standards Council als PA-QSA akkreditiert

München – Das PCI Security Standards Council hat atsec information security als Payment Application Qualified Security Assessor akkreditiert. Damit ist atsec befugt, Zahlungsanwendungen auf die Einhaltung der Vorgaben des PA-DSS zu überprüfen. atsec hat alle geschäftlichen, technischen und administrativen Anforderungen, die eine PA-DSS-Zertifizierung erfordert, erfüllt.

Das Ziel des PA-DSS ist es, Softwareentwicklern dabei zu helfen, sichere Zahlungsanwendungen zu programmieren, die keine unerlaubten Daten (z. B. den kompletten Magnetstreifen, Prüfsumme und PIN-Nummern) speichern und zudem den Anforderungen des PCI DSS genügen. Der Standard ist relevant für Zahlungsanwendungen, die verkauft, publiziert oder lizenziert werden.

Fiona Pattinson, Director Business Development and Strategy, sagte dazu: „Wir sind stolz darauf, die PA-QSA-Akkreditierung erreicht zu haben, deren Anforderungen sehr komplex und detailliert waren – sowohl für uns als Firma als auch für die beteiligten Personen. Wir freuen uns darauf, mit unseren Kunden und dem PCI SSC die Sicherheit von Zahlungsanwendungen zu verbessern."

atsec verfügt über langjähriges Know-How im Bereich der IT-Sicherheit sowie in der Anwendung von IT-Sicherheitsstandards und der Evaluierung von Organisationen, Produkten und Computersystemen.

atsec ist vom PCI SSC als Qualified Security Assessor (QSA) akkreditiert und damit befugt, PCI DSS-Assessments in Europa, China und den USA durchzuführen.

atsec hat weitreichende Erfahrung mit der Durchführung von Quellcode-Beurteilungen, FIPS 140-2-Tests, Algorithm Validation, SCAP und Penetrationstests.

atsec hat eine große Zahl von Sicherheitsaudits für Kunden aus den verschiedensten Geschäftsfeldern (z. B. Telekommunikation, Energie, Banken und Militär) durchgeführt.

atsec hat Common Criteria-Labore (ISO/IEC 15408 and 18045) in drei Ländern: in Deutschland, Schweden und in den USA.

Falls Sie weitere Informationen wünschen, besuchen Sie bitte die PCI SSC Website (https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml) oder senden Sie uns eine E-Mail an pa-dss@atsec.com.

IMPRESSUM

atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com
Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG: DE205370914
Verantwortlich für den Inhalt:
Matthias Hofherr (Anschrift wie oben)

AKTUELLE MELDUNG

atsec und Red Hat erreichen JBoss Enterprise Application Platform Common Criteria Zertifizierung

Pünktlich zu unserem ersten Newsletter können wir eine weitere Erfolgsmeldung verkünden. Red Hat's JBoss Enterprise Application Platform hat die Zertifizierung nach Common Criteria EAL 2 erfolgreich durchlaufen.

mehr zum Thema http://www.atsec.com/01/atsec-news.html

atsec NEWS 08/09
the information security provider

Sehr geehrte Damen und Herren,

herzlich willkommen zum ersten atsec Newsletter. Ab jetzt werden Sie von uns vierteljährlich interessante Neuigkeiten aus der Welt der IT-Security erhalten. Wir freuen uns auf Ihr Feedback.

Zentraler Bestandteil unseres Newsletters wird ein Fachartikel zu einem ausgewählten Thema sein. Den Auftakt bildet in der aktuellen Ausgabe ein Beitrag zum Thema „Security Monitoring" von unserem Mitarbeiter Ralf Wienzek. Der Beitrag erläutert Ihnen die Wichtigkeit von Security Information- und Event Management Systemen (SIEM) für eine auf Sicherheit und Compliance bedachte IT-Infrastruktur.

Weltweit wird der Gesamtverlust für Unternehmen durch externe und interne Angriffe auf Informationssysteme auf 100 Milliarden Dollar geschätzt mit steigender Tendenz.

Aktuelle Meldungen, unsere Firma betreffend, finden Sie auf der Rückseite. Wir freuen uns besonders, als neu akkreditierter PCI Payment Application Qualified Security Assessor (PCI PA-QSA) unser Portfolio um eine weitere Dienstleistung erweitern zu können. Detaillierte Informationen hierzu finden Sie auf Seite 4.

Zusammen mit dem Newsletter erhalten Sie unser „IT-Sicherheitsstandard-Planetarium", das die Beziehung zwischen vielen IT-Sicherheitsstandards verdeutlicht.

Falls Sie Fragen oder Anregungen haben, erreichen Sie uns unter der E-Mail-Adresse *newsletter@atsec.com*. Diese Mailadresse steht Ihnen auch zur Verfügung, falls sie den Newsletter gerne per E-Mail bestellen möchten.
Ihre Meinung ist uns wichtig!

Viel Spaß beim Lesen und herzliche Grüße von atsec

Gerald Krummeck,
Director,
atsec information security GmbH

Falls Sie den atsec Newsletter in Zukunft nicht mehr erhalten möchten, senden Sie bitte eine E-Mail mit dem Betreff „unsubscribe" an newsletter@atsec.com.

Unsere Leitsätze

Wir kennen unser Geschäft
atsec kennt die weltweite Informationssicherheitsbranche gut. Mit unserem multinationalen Team fühlen wir uns überall auf der Welt zu Hause. Wir sind ein Unternehmen mit globaler Reichweite. Wir leisten exzellente und pünktliche Arbeit.

Wir handeln integer
IT Sicherheitsconsulting und Evaluierungen setzen ein Höchstmaß an Integrität und Vertrauenswürdigkeit voraus. All unsere Angestellten sind verpflichtet dies unseren Kunden gegenüber einzuhalten. Wir widmen uns uneingeschränkt der Aufgabe, die höchste Qualität pünktlich zu liefern.

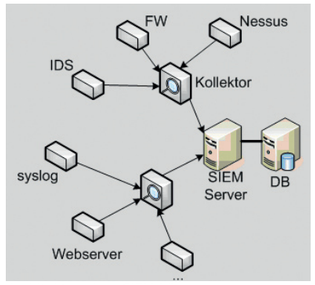
Wir konzentrieren uns auf unsere Kompetenzen
Unsere Berater sind Sicherheitsberater. Als solche konzentrieren wir uns ausschließlich auf Informationssicherheit. Wir beraten zu keinem anderen Thema und wir verkaufen weder Hardware, Software, noch irgendwelche anderen Produkte.

Wir sind unabhängig
atsec gehört seinen Mitarbeitern. Wir sind weder an Hardware- oder Software-Hersteller gebunden, noch werden wir es jemals sein. Unsere Glaubwürdigkeit gründet sich auf diese Unabhängigkeit. Unsere Kunden können sich darauf verlassen, dass wir objektiv sind. Wir haben kein Interesse daran, etwas Anderes als unsere Sicherheitskompetenz zu verkaufen.

Security Monitoring

Wie vielen Angriffsversuchen waren wir im letzten Monat ausgesetzt? Woher stammten die Angreifer? Was waren die Top 10 der Angriffsziele? In vielen Unternehmen werden Antworten auf diese oder ähnliche Fragen regelmäßig benötigt. Die Antworten darauf sind häufig tief in den Gigabytes an Log-Daten vergraben, die im Laufe der Zeit anfallen. Ein manuelles Auswerten dieser Datenberge ist nicht praktikabel und eine automatisierte Auswertung daher unerlässlich.

Eine umfassende Unterstützung bieten so genannte Security Information and Event Management (SIEM) Systeme. Sie sind in der Lage, Meldungen verschiedenster Dienste und Applikationen zu interpretieren und sie durch geeignete Korrelationsregeln miteinander in Zusammenhang zu bringen. Die Meldung eines Intrusion-Detection Systems, dass ein bestimmtes Angriffsmuster gegen ein internes System gesehen wurde, bedroht beispielsweise nur dann die Sicherheit des Zielsystems, falls auf diesem System auch tatsächlich ein Dienst angeboten wird, der für die durch das Angriffsmuster ausgenutzte Schwachstelle anfällig ist. Kann also aus den Meldungen eines Schwachstellen-Scanners abgeleitet werden, dass auf Server S eine verwundbare Applikation A läuft, und meldet das Intrusion-Detection System, dass ein zu dieser Schwachstelle passendes Angriffsmuster gegen den Server S beobachtet wurde, und meldet zudem anschließend die Firewall, dass vom Server S eine unüblich hohe Anzahl von Verbindungsversuchen ausgeht, ergeben diese Einzelereignisse als Ganzes betrachtet ein sehr viel aussagekräftigeres Bild über die Signifikanz der analysierten Ereignisse.



Architektur einer SIEM-Lösung

SIEM-Systeme bestehen im Wesentlichen aus zwei Arten von Komponenten: viele im Netzwerk verteilte Kollektoren und einem zentralen Server (bzw. einem Cluster von zentralen Servern) mit assoziiertem Datenbanksystem. Die Aufgabe der Kollektoren ist es, sämtliche in der IT-Infrastruktur anfallenden Audit-Daten zu sammeln, uninteressante Meldungen auszusortieren, die Meldungen in ein einheitliches, wohldefiniertes Format zu konvertieren und das Ergebnis an den zentralen Server weiterzuleiten. Die verarbeiteten Daten entstammen verschiedensten Quellen wie z. B. Unix/Linux syslog, Windows Event Log, Router, Switches, Firewalls, Intrusion-Detection-Systemen, Antiviren-Programmen, Schwachstellen-Scannern, Authentisierungs-Servern, Monitoring-Programmen, etc. Der zentrale Server führt die Daten sämtlicher Kollektoren zusammen und analysiert den sich ergebenen Gesamtdatenstrom. Dabei können signifikante Einzelereignisse direkt als Sicherheitsvorfall alarmiert werden. Die entscheidende Fähigkeit eines SIEMs ist es jedoch, die zunächst unabhängigen Eingangsdaten zu korrelieren und durch Ableitung zusammengesetzter Ereignisse eine umfassendere und akkuratere Einschätzung der aktuellen Sicherheitslage zu generieren. Im Vergleich zu einer unabhängigen Auswertung der einzelnen Datenquellen wird durch einen geeigneten Abgleich der analysierten Daten untereinander die Rate der Fehlmeldungen (False Positives) in der Regel signifikant reduziert.

Die wichtigsten Funktionen eines SIEMs sind:

- **Echtzeit- und Langzeitüberwachung:**
  Bei ausreichender Dimensionierung werden die eintreffenden Daten in Echtzeit verarbeitet und bei Bedarf einem Sicherheitsanalysten angezeigt. Sämtliche Ereignisse werden in einer dedizierten Datenbank abgelegt und können für längerfristige oder forensische Analysen abgerufen werden. Einige Produkte verwenden auch Data-Mining-Techniken, um in den hinterlegten Daten neuartige Muster zu erkennen.

- **Korrelation:**
  Neben der Bewertung von Einzelereignissen werden diese zusätzlich mit anderen Ereignissen korreliert und dadurch höherwertige, d. h. aussagekräftigere, Ereignisse erzeugt.

- **Visualisierung:**
  Die aktuell eintreffenden Ereignisse werden graphisch aufbereitet und übersichtlich dargestellt. Durch Anwendungen von Filtern können für eine konkrete Analyse uninteressante Ereignisse ausgeblendet und mittels Dashboard-Funktionalitäten nahezu beliebige Übersichtsdiagramme erzeugt werden.

- **Alarmierung, Incident Management:**
  Gibt es genügend viele Hinweise, dass ein Verstoß gegen geltende Vorschriften vorliegt, kann dieser Vorfall umgehend und automatisiert an die zuständigen Stellen innerhalb des Unternehmens gemeldet werden. Die Nachverfolgung der Vorfälle kann ebenfalls durch das SIEM-System selbst geschehen oder von einem dedizierten System übernommen werden.

- **Reporting, Compliance:**
  Aus den in der Vergangenheit aufgezeichneten Ereignissen können nahezu beliebige Reports für unterschiedliche Zielgruppen erzeugt werden. In der Regel bietet das System vordefinierte Berichtsvorlagen für gängige Sicherheitsstandards an; die Generierung eigens definierter Reports ist üblicherweise ebenfalls möglich.

Unternehmensweite Einführung einer kommerziellen SIEM-Lösung

Das Angebot an kommerziellen SIEM-Lösungen ist vielfältig und unübersichtlich. Für eine erfolgreiche Einführung einer SIEM-Lösung in ein Unternehmen ist es unerlässlich, in einem ersten Schritt sämtliche Anforderungen an eine solche Lösung zu erfassen. Insbesondere ist es wichtig, die vorhandene Infrastruktur zu analysieren und eine Liste der in ihr enthaltenen Datenquellen zu erstellen, die von der SIEM-Lösung – möglichst „out-of-the-box" – unterstützt werden müssen. Um die Akzeptanz des Systems zu erhöhen, sollten die Betreiber der später überwachten Systeme in diesen Prozess einbezogen werden. Es gilt auch, den Schutzbedarf der zu analysierenden Daten so zu berücksichtigen, dass beispielsweise eine notwendige Verschlüsselung für die Übertragung von der Datenquelle zum Kollektor durch das SIEM unterstützt wird. Des Weiteren sollte es bereits eine Abschätzung des anfallenden Volumens an Audit-Daten geben, sowie die noch verfügbare Bandbreite im Netzwerk bekannt sein, die für die Kommunikation der SIEM-Komponenten untereinander verwendet werden kann, ohne die Performance des Netzwerks zu beeinträchtigen.

Die Gewichtung der identifizierten Anforderungen und insbesondere die Auszeichnung von Anforderungen, die auf jeden Fall erfüllt sein müssen (KO-Kriterium), ermöglicht eine anschließende objektive Beurteilung der Kandidaten. Ergibt der Vergleich auf dem Papier keinen eindeutigen Sieger, können die vielversprechendsten Kandidaten mittels einer Testinstallation in der späteren Zielumgebung intensiv getestet werden. Dabei sollten sowohl der Umgang der SIEM-Lösung mit allen vorhandenen Datenquellen als auch ihre Fähigkeit, spezifische, auf die konkrete Einsatzumgebung abgestimmte Korrelationen durchzuführen, praktisch getestet werden. Die Integration in ein vorhandenes Incident Management System sowie die Fähigkeit zur Generierung aller benötigten Reports sollten ebenfalls verifiziert werden.

Installation einer Open-Source SIEM-Lösung

Für viele kleine und mittelständische Unternehmen ist für eine effektive Überwachung ihrer Infrastruktur der Kauf eines kostspieligen kommerziellen SIEM-Produkts nicht notwendig. In der Open-Source-Community existieren verschiedenste Werkzeuge, die bereits Teile der Funktionalitäten einer vollständigen SIEM-Lösung implementieren. Eine auf die konkreten Bedürfnisse des Unternehmens angepasste Kombination dieser Werkzeuge kann die gestellten Anforderungen ebenfalls erfüllen.

Die meisten Anwendungen unterstützen ein syslog-konformes Ausgabeformat ihrer Audit-Daten. Dazu gehören beispielsweise das kostenlose netzwerkbasierte Intrustion-Detection-System Snort, diverse Monitoring-Tools wie p0f, pads, arpwatch sowie relevante Anwendungen zur Gewährung von Systemzugriffen wie SSH. Selbst Systemmeldungen von Windows-Systemen können durch entsprechende Werkzeuge im syslog-Format ausgelesen werden. Sämtliche Meldungen können auf einem zentralen syslog-Server gesammelt und z. B. mittels des frei verfügbaren Werkzeugs „Simple Event Correlation" (SEC) analysiert werden. Es erlaubt die Anwendung nahezu beliebiger Korrelationsregeln auf einen textbasierten Eingabestrom. Ebenso ist die Verwendung eines spezifischen Alarmierungswegs möglich, da bei Bedarf beliebige Systembefehle abgesetzt werden können. Die anfallenden Daten können zudem in einer MySQL-Datenbank abgelegt und über ein entsprechendes Web-Interface dem Benutzer dargestellt werden.

Im Vergleich zu den meisten kommerziellen Produkten ist eine solche Lösung zwar nicht ganz so benutzerfreundlich und in der Regel wartungsintensiver, jedoch kann bei entsprechendem Know-how des Personals eine äußerst kostengünstige Lösung zusammengestellt werden, die die gestellten Anforderungen des Unternehmens vollauf erfüllt.

Zusammenfassung

Security Information and Event Management Systeme sind ein wichtiger Baustein für eine auf Sicherheit bedachte IT-Infrastruktur. Sie ermöglichen eine automatisierte Analyse aller anfallender Audit-Daten, eine zeitnahe Alarmierung und die automatisierte Erzeugung von Berichten.

Die Auswahl eines kommerziellen Produkts ist nicht trivial. Bevor auf die einzelnen Hersteller zugegangen wird, sollte besondere Aufmerksamkeit auf eine umfassende und detaillierte Anforderungserfassung gelegt werden. Bei mehreren möglichen Kandidaten sollten diese im Rahmen von Testinstallationen untersucht werden, indem auf ihre spätere Verwendung abgestimmte Testfälle ausgeführt werden.

Für kleine und mittelständische Unternehmen lohnt sich u. U. auch das Aufsetzen einer auf Open-Source-Produkten basierenden Gesamtlösung, da hierdurch ausreichende Funktionalität zu einem geringen Preis zu erzielen ist.