gebieten. 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.

CI Security Standards Council als ert

urity Standards Council hat atsec information security Qualified Security Assessor akkreditiert. Damit ist atsec lungen auf die Einhaltung der Vorgaben des PA-DSS zu e geschäftlichen, technischen und administrativen An-A-DSS-Zertifizierung erfordert, erfüllt.

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.

AKTUELLE MELDUNG

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

Pünktlich zu unserem ersten Newsletter können wir eine weitere Erfolgsmeldung ver-

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

Un

Wi
ats
for
gut
len
auf
ein
Rei
len

Wi
IT
Eva
Hö
Ver
All
ver
der
wic
der
lität

Wi
un
Uns
hei
zer
lich
Wir
ren
we
noc
Pro

Wi
ats
ter
wa
geb
jem
dig
Una
der
las

y Monitoring

chen waren wir im letzten Monat ausgesetzt? Woher stammten die Angreifer? Was griffsziele? In vielen Unternehmen werden Antworten auf diese oder ähnliche Fra- t. Die Antworten darauf sind häufig tief in den Gigabytes an Log-Daten vergraben, fallen. Ein manuelles Auswerten dieser Datenberge ist nicht praktikabel und eine ung daher unerlässlich.

zung bieten so genannte Securi- nagement (SIEM) Systeme. Sie n verschiedenster Dienste und ren und sie durch geeignete Kor- in Zusammenhang zu bringen. n-Detection Systems, dass ein gegen ein internes System ge- pielsweise nur dann die Sicher- uf diesem System auch tatsäch- wird, der für die durch das An- chwachstelle anfällig ist. Kann es Schwachstellen-Scanners ab- erver S eine verwundbare Appli- as Intrusion-Detection System, nstelle passendes Angriffsmus- bachtet wurde, und meldet zu- all, dass vom Server S eine un- indungsversuchen ausgeht, er- e als Ganzes betrachtet ein sehr über die Signifikanz der analy-

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 Mel- Meldungen in ein einheitliches, nvertieren und das Ergebnis an uleiten. Die verarbeiteten Daten n Quellen wie z. B. Unix/Linux sys- ter, Switches, Firewalls, Intrusion- n-Programmen, Schwachstellen- -Servern, Monitoring-Program-

nisse 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 Nachver-

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 ei- ne effektive Überwachung ihrer Infrastruktur der Kauf eines

die konkreten Bedürfnisse des Kombination dieser Werkzeuge derungen ebenfalls erfüllen.

Die meisten Anwendungen unt mes Ausgabeformat ihrer Audi spielsweise das kostenlose n Detection-System Snort, divers pads, arpwatch sowie relevante rung von Systemzugriffen wie gen von Windows-Systemen kö Werkzeuge im syslog-Format a che Meldungen können auf ein gesammelt und z. B. mittels des „Simple Event Correlation“ (SE laubt die Anwendung nahezu b auf einen textbasierten Eingab wendung eines spezifischen Ala bei Bedarf beliebige Systembef nen. Die anfallenden Daten kön Datenbank abgelegt und über terface dem Benutzer dargeste

Im Vergleich zu den meisten k eine solche Lösung zwar nicht und in der Regel wartungsinten sprechendem Know-how des Pe günstige Lösung zusammenges ten Anforderungen des Unterne

Zusammenfassung

Security Information and Event ein wichtiger Baustein für eine Infrastruktur. Sie ermöglichen e aller anfallender Audit-Daten, und die automatisierte Erzeugu

Die Auswahl eines kommerziell Bevor auf die einzelnen Herste besondere Aufmerksamkeit au taillierte Anforderungserfassun ren möglichen Kandidaten sollte tinstallationen untersucht werd Verwendung abgestimmte Test

Für kleine und mittelständische U. auch das Aufsetzen einer auf sierenden Gesamtlösung, da hi tionalität zu einem geringen Pr