

Übersicht und Kontrolle bringt Informationssicherheit

Unternehmen sehen sich heute immer stärker neuen Herausforderungen gegenüber. Sie müssen immer komplexere Systeme wirtschaftlich managen und dabei oft auch steigende Compliance Anforderungen erfüllen. Zusätzlich sind Maßnahmen gegen zunehmenden online Betrug gefordert. Eine wesentliche Unterstützung bringen hier Lösungen für SIEM – Security Information and Event Management.



SIEM Lösungen schaffen Übersicht in komplexen IT-Strukturen durch benutzerspezifische Ansichten aller relevanten Ereignisse

Die IT-Welt hat sich in den letzten Jahren stark verändert. Immer mehr Daten eines Unternehmens sind auf unterschiedliche Standorte verteilt. Im gleichen Maß wie dadurch der Überblick erschwert wird, steigt auch der Missbrauch von Daten an und Hacking wird kommerzieller. Beim Conficker Wurm Befall war das bereits deutlich zu sehen; in kürzester Zeit legte er viele kritische Systeme lahm. Der Rund-um-die-Uhr-Betrieb muss aber für wichtige Transaktionen gewährleistet sein. Denn viele Unternehmen bieten Shopping Portale an, Plattformen wie eBay oder PayPal werden immer beliebter, und viele Bankkunden wickeln ihre Überweisungen bereits mit Online Banking ab. Der Überblick über die dafür erforderlichen komplexen Systeme, ist nur noch mit Hilfsmitteln möglich.

Compliance: Vertrauen ist gut, Kontrolle ist besser

Unternehmen stehen heute vor umfangreichen und weiter wachsenden Anforderungen an Compliance, wie sie unter anderem in SOX, PCI oder ISO 27001 beschrieben sind. Nur, wer kann schon ausreichend sicher sein, dass organisatorische Vorgaben wie Passwortpolicy auch eingehalten werden? Wird erkannt, ob generische Administrator Accounts mehrfach benutzt werden oder nicht mehr notwendige Zugriffsberechtigungen wieder entfernt werden? Um Missbrauch erkennen zu können, fehlt oft die Kontrolle und Transparenz über diese Art von Aktivitäten.

SIEM schafft Transparenz

Im Jahr 1999 kam die neue Technologie SIEM erstmals auf den Markt. SIEM steht für „Security Information and Event Management“ und ist die Kombination von SIM und SEM Lösungen. SIM beinhaltet das Reporting historischer Daten und Forensik. Um aber bei bedrohlichen Vorfällen rasch reagieren zu können, ist die Echtzeit-Analyse von Ereignissen wichtig; das ermöglicht SEM. Da kritische Ereignisse nur mit einer Gesamtsicht auf das Netzwerk erkannt werden, steigt der Bedarf an SIEM; und das nicht nur für Organisationen, die Compliance Anforderungen erfüllen müssen, auch für alle anderen Unternehmen ist diese Lösung von enormem Nutzen.

Bacher Systems EDV GmbH, 1100 Wien, Clemens-Holzmeister-Straße 4, Tel.: +43.1/60 126-0, Fax: +43.1/60 126-4, E-Mail: info@bacher.at

Newsletter 1/2009

Informationen für IT-Sicherheit und IT-Infrastruktur

10 Vorteile einer SIEM Lösung

1. Zentrale Sicht auf alle Events im Unternehmen: Ein Mitarbeiter setzt viele Aktivitäten, er führt zum Beispiel Buchungen durch, hat Zugriff auf Kundendaten im CRM-System, versendet Mails, benützt eine Zutrittskontrollkarte ins Lager, etc. All diese Aktionen in unterschiedlichen Systemen können vom Administrator gesamtheitlich gesehen und in Beziehung zueinander gebracht werden. Aus Datenschutzgründen ist sichergestellt, dass Benutzernamen nur im Verdachtsfall mittels Vieraugen-Prinzip lesbar sind.

2. Einheitliches Werkzeug: SIEM wird nicht nur von den Security Analysten genutzt, um einen gesamthaften Überblick zu ermöglichen, sondern auch von der Support-Abteilung, um das Netzwerk zu überwachen. Durch rollenbasierende Berechtigungen erhalten die Anwender unterschiedliche Zugriffsrechte auf Loginformationen des SIEM-Systems.

3. Effizienteres Troubleshooting: Bei Bedarf sieht der Servicedesk auf Knopfdruck, warum zum Beispiel der Mail-Dienst plötzlich nicht mehr funktioniert, und das nicht nur auf Netzwerk- sondern auch auf Applikationsebene.

4. Erkennen von Zusammenhängen: Eine SIEM Lösung enthält bereits viele vordefinierte Zusammenhänge und damit einhergehende Richtlinien, dadurch werden False Negatives reduziert. Wenn zum Beispiel ein Mitarbeiter mit Hilfe seiner Zutrittskarte ins Unternehmen gelangt, so kann er sich nicht

10 Minuten später über eine Internet-Verbindung aus einem anderen Land in die Zentrale einwählen. Jedes für sich wäre unbedenklich, durch die Korrelation beider Ereignisse muss jedoch ein Alarm ausgegeben werden.

5. Dashboard für Online Monitoring: Jeder Rolle werden eigene Ansichten zugewiesen, somit bekommt jeder Administrator oder Analyst genau die Ansicht, die er im Rahmen seiner Verantwortung braucht.

6. Umfassendes Reporting: Aus der Flut an Daten der unterschiedlichen Systeme werden Zusammenfassungen erstellt. Das ermöglicht zum Beispiel Trends zur Auslastung der Systeme abzuleiten, Änderungen an Systemen nachzuvollziehen oder aktuelle Schwachstellen eines Systems aufzuzeigen.

7. Workflow-Unterstützung: Ist ein Vorfall passiert, wird ein vordefinierter Workflow gestartet. In einem Call Tracking System wird automatisch ein Ticket eröffnet, das nach Behebung des Vorfalls, mit Rückmeldung an das SIEM System wieder geschlossen wird. Auf diese Weise ist nachvollziehbar, wann welcher Vorfall bearbeitet und in welcher Zeit er abgeschlossen wurde – damit wird eine wesentliche Compliance Anforderung erfüllt.

8. Erkennen von Anomalien: Das SIEM System bildet Baselines, so genannte durchschnittliche Grundauslastungswerte, sowohl auf Applikationsebene als auch im Netzwerk. Wird nun ein unüblich hoher Netzwerk-Verkehr registriert, oder eine ungewöhnlich

hohe Zahl an Datenbank-Abfragen, so wird automatisch Alarm ausgelöst.

9. Verbindung zwischen IP-Adresse und Benutzer: Zur Verfolgung und Aufdeckung von Online Betrug muss zwischen dem Benutzer und der IP-Adresse ein Zusammenhang hergestellt werden, das heißt: zu welchem Zeitpunkt hat Benutzer X diese Adresse gehabt.

10. Logdateien werden komprimiert gespeichert: Laut SOX müssen Systemlogs bis zu 3 Jahre aufbewahrt werden, mit SIEM wird der Storage Bedarf durch Komprimierung erheblich reduziert.

Damit unterstützt SIEM nicht nur jene Unternehmen, die Compliance Anforderungen erfüllen müssen. SIEM-Lösungen werden für die Betriebssicherheit komplexer IT-Strukturen unerlässliche Hilfsmittel sein.

Trainings bei Bacher Systems

IT-Infrastruktur

Unix Grundlagen der Solaris 10 Betriebssystemumgebung

2.6. - 5.6.2009 / € 1.990,-

Solaris 10 OE Systemadministration I

15.6. - 19.6.2009 / € 2.790,-

Solaris 10 OE Systemadministration II

22.6. - 26.6.2009 / € 2.790,-

Netzwerkadministration für Solaris 10 OE

29.6. - 3.7.2009 / € 2.790,-

IT-Sicherheit

Check Point Security Administration NGX III (R65)

2.6. - 5.6.2009 / € 2.560,-

Intensiv-Workshop: Endpoint Security

9.6. - 10.6.2009 / € 1.150,-

Alle Preise pro Person exkl. MwSt.

Firmenspezifische Kurse auf Anfrage.

Anmeldungen: training@bacher.at

Kursinfos: www.bacher.at/training

Änderungen vorbehalten

Offenlegung gemäß § 25 Mediengesetz; Medieninhaber: Bacher Systems EDV GmbH, Clemens Holzmeister Straße 4, 1100 Wien
 Reg. zu FN 54202i, Handelsgericht Wien, GF: Manfred Köteles, Mehrheitsgesellschafter: Manfred Köteles, Martin Mörtinger
 Unternehmensgegenstand: Handel mit Computer-Soft- und Hardware IT-Beratung; Blattlinie: Verbreitung von Information für sichere IT-Infrastruktur