axivia

Workshop Informationssicherheit

Aktuelles Top-Thema: ArcSight Express

- **Security Information Management**
- **Security Event Monitoring**
- **Log-Management**

Die IT-Landschaften werden täglich komplexer und die Zahl der zu überwachenden Daten und Systeme wächst permanent. Oft bleiben neben dem Tagesbetrieb keine Ressourcen um präventiv Log-Einträge oder (Sicherheits)Ereignisse zu analysieren, zu bewerten und zu managen.

Dies geschieht wenn überhaupt oft reaktiv nach einer Störung oder einem Ausfall. Systematische Auswertung bzw. Echtzeit-Korrelation findet in der Regel nicht statt und oftmals existiert sogar noch nicht einmal ein vernünftiges Logging, geschweige denn eine zentrale Log-Sammlung. Somit werden Symptome eines drohenden Ausfalls oder eines Sicherheitsvorfalles nicht erkannt und deren Vorkommnis nicht durch frühzeitig eingeleitete, präventive Maßnahmen verhindert.

Schlimmer noch: Selbst eine Analyse zur Verhinderung eines erneuten Eintritts der gleichen Störung scheidet dadurch aus.

Seehotel Niedernberg

Donnerstag, 01.10.2009 ab $12^{\underline{00}}$ Uhr

ArcSight™

Parallel dazu erhöht sich der Druck seitens Gesetzeslage und Verträgen mit Kunden oder Partnern permanent. Oft werden Informationen über diese Anforderungen nicht von der Unternehmensführung zur IT übermittelt. Falls doch, gilt es sich einvernehmlich mit den Datenschutzbestimmungen und den derzeit in der Organisation eingeführten Regelungen zur Protokollierung und Auswertung auseinanderzusetzen um Rechtsverstöße zu vermeiden.

Wenn anschließend die Anforderungen klar definiert sind, gilt es nun mit geeigneten Regelungen und zu guter Letzt natürlich mit technischen Hilfsmitteln und Systemen eine Lösung für diese weitreichende Aufgabenstellungen zu finden.

Hierzu gibt es eine Fülle von Produkten auf dem Markt. Doch nur wenige sind in der Lage, nahezu alle Anforderungen im Bereich von Logging, Reporting und Event Management **in Echtzeit** aus einer Hand abzudecken. Die Kür sind rollenspezifische Ansichten der aktuellen Sicherheitslage und des Status inkl. Compliance-Views für verschiedene Regularien und Standards wie ISO27001 oder PCI-DSS.

Speziell für den schnellen Einstieg mit überschaubaren Einführungskosten und Betriebsaufwand hat ArcSight das neue **ArcSight Express** als „kleinen Bruder“ des bewährten ESM (Enterprise Security Manager) auf den Markt gebracht.

Wir geben Ihnen einen tiefen Einblick, welche Möglichkeiten Ihnen die **ArcSight** Produkte bieten.

Wir freuen uns auf Ihre Teilnahme!

FAX-Anmeldung: 06022 - 50872 20

Anmeldung zum Tagesseminar

am Donnerstag, 01.10.2009

im Seehotel Niedernberg

Bitte beachten: Die Anmeldungen werden in der Reihenfolge des Eingangs berücksichtigt!

Die Teilnahme am Workshop ist **kostenlos**.
Jeder Teilnehmer erhält Informationsmaterial.

Informationen zum Veranstaltungsort finden Sie unter http://www.seehotel-niedernberg.com/

Name / Vorname

Firma / Position

Telefon / Telefax

E-Mail

Datum / Unterschrift

axivia GmbH - Industriering 7 - 63868 Großwallstadt 06022/50872 0 – info@axivia.de

12^{00} Uhr — Registrierung+ Mittagessen - Buffet

13 ^{30} Uhr — Logging, Reporting, Event Management
Einführung und Begriffsklärung

- Security Event Managmnt./Monitoring (SIEM)
- Typische Log-Quellen, Architektur
- Normalisierung, Aggregation, Korrelation
- Alerting, Monitoring, Reporting
- Abgrenzung zum klass. Netzwerkmonitoring

Reinald Kempf, axivia GmbH

13 ^{45} Uhr — ArcSight Produkte

ArcSight Logger – Log-Management par excellence

inkl. live Demo

- Vorinstallierte Appliance - ready to start -
- Performance ohne Kompromisse
- günstige, effektive Speicherung
- extrem schnelle Log-Sammlung
- Log-Aggregation
- schnelle und intuitive Analyse
- revisionssicher
- 275+ Standard APIs
- skalierbar
- Compliance-Packages

15 ^{00} Uhr — Kaffeepause

ArcSight Express - Event Korrelation in Echtzeit
Security Information + Event Management. (SIEM)

inkl. live Demo

- Vorinstallierte Appliance - ready to start -
- Sammlung, Kategorisierung, Korellation von
- Aktivitäten in Netzwerken und Applikationen
- Rechtzeitige Erkennung ungewöhnlicher Aktivitäten um Schäden zu vermeiden
  - Verbreitung von Würmern über Firewalls
  - Verbreitung von Viren über Desktops
  - Hackerzugriff auf das Netzwerk
  - Benutzer mit P2P Anwendungen
  - Remote Access durch das VPN
- Alarmierung und automatisierte Aktionen
- Verstehen, welche Systeme behandelt werden müssen
- Real-Time Monitoring und Benachrichtigung
- Intelligente Reaktion
- Workflows und Dokumentation

Frank Lange, ArcSight Deutschland

16 ^{15} Uhr — Q&A

16 ^{30} Uhr — Ausklang in der Lounge

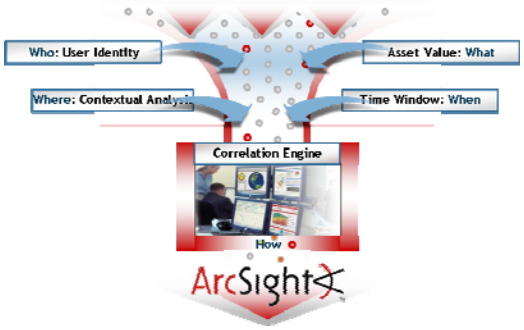
Problem: Risiken sind nicht sichtbar

- zu viele Geräte im Netz
- zu viele verschiedene Gerätetypen
- zu viele Systeme im Internet

„Alles sieht aus wie -eins von vielen-“

„Wir wissen noch nicht einmal, ob wir angegriffen werden“

„Wir kennen die Auswirkungen dieses Problems nicht“



Problem: zu schwierig, „Compliance“ darzustellen

- zu viele Daten
- zu viele Formate
- zu schwierig zu konsolidieren
- zu teuer zum speichern und zum archivieren

„Selbst die einfachsten Untersuchungen erfordern meine besten Mitarbeiter“

„Wir verlieren zu viel Zeit um uns auf ein Audit vorzubereiten“

„Wir können die Log-Daten vieler Jahre nicht aufbewahren“