Link: https://www.computerwoche.de/a/wie-aus-daten-informationen-werden,2354632

Das Compliance Log Warehouse

Wie aus Daten Informationen werden

Datum: 10.12.2010
Autor(en): Klaus Manhart

Egal ob Transaktionsdaten oder falsche Logins - die in Logfiles gespeicherten Daten sind für jedes Unternehmen ein wertvoller Informationsschatz. Doch der ist nur schwer zu heben -sind die Daten doch meist dezentral über den ganzen Betrieb verteilt. Abhilfe inklusive einer Gesamtsicht auf die Unternehmens-IT verspricht das Compliance Log Warehouse.

IT-Systeme in Unternehmen wie PCs, Server, Router, Firewalls oder Applikationen produzieren heute eine Unmenge an Daten. Die werden in der Regel in Log-Files gespeichert. Dazu gehören so unterschiedliche Informationen wie SAP-Transaktionsdaten, Buchungsdaten, Fail Logons, Aufzeichnungen von Datenbankänderungen oder Event-Logs von Betriebssystemen und Anwendungen.

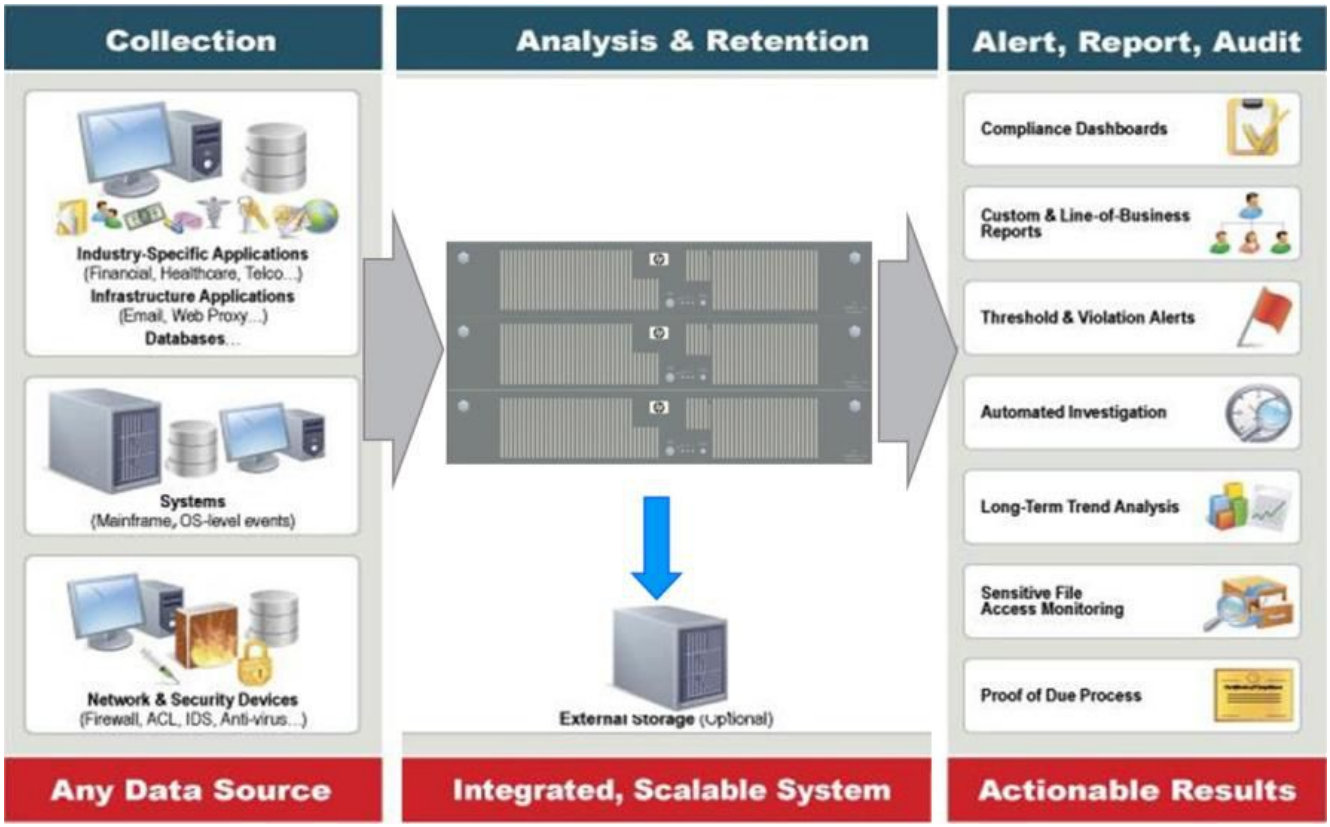
Viele Unternehmen nutzen diesen Datenschatz heute und analysieren die Logfiles. IT-Sicherheit und das Monitoring von Netz- und User-Aktivitäten gehören zu den klassischen Anwendungen von Log-Daten-Analysen. Schließlich sind Ereignisdaten wie Event-Detection und die Nachverfolgung verdächtiger Aktivitäten wichtig für die Security und Gewährleistung einwandfreier IT-Prozesse. So könnte beispielweise der Versand von E-Mails mit kritischen Anhängen außerhalb der Geschäftszeiten auf Datendiebstahl verweisen.

Viele wollen oder müssen über die Logfile-Analyse aber auch sicherstellen, dass Unternehmens- und Legislative-Richtlinien erfüllt werden, etwa auf dem Gebiet Compliance. Auch die IT im eigenen Haus lässt sich damit optimieren, zeigt die intelligente Auswertung von Logs doch präzise und in Echtzeit Fehlerquellen in den IT-Systemen an.

Studien wie etwa die des **SANS-Instituts**[1] zeigen, dass die Logfile-Analyse inzwischen ihren festen Platz als wichtiges Instrument für IT-Sicherheit und Betrieb in den Unternehmen hat. Laut der fünften Studie des SANS-Instituts sammeln inzwischen 99 Prozent aller Unternehmen Logfiles oder planen die Einführung von Log-Management.

CLW - Die Gesamtsicht auf die IT

Die strategische Nutzung von Log-Daten setzt zunächst ihre lückenlose und zentrale Sammlung voraus. Nur dann führen Analysen zu verlässlichen Ergebnissen, anhand derer sich unternehmensübergreifende Maßnahmen definieren und durchsetzen lassen. Der umfassende Blick auf die IT wird in der Praxis allerdings durch die dezentrale Datenhaltung erschwert. Dadurch dass die Log-Daten normalerweise abteilungsspezifisch gespeichert werden geht der Überblick über die gesamte IT-Infrastruktur verloren. Man bekommt immer nur punktuelle Bilder, keine Gesamtsicht auf die IT.



Das CLW sammelt und integriert Daten aus verschiedenen Quellsystemen und bietet gleichzeitig Analyse- und Reportingfunktionen.

Eine Lösung dafür, die richtigen Informationen zeitnah im Datenmeer zu finden und dabei vor allem eine globale Sicht auf die gesamte Unternehmens-IT zu gewährleisten bietet das Compliance Log Warehouse (CLW) von HP. Die modular ausbaubare, aus Server, Datenbank plus Software bestehende Appliance sammelt alle Logdaten zentral in einem großen Data Store. Die Daten werden per Push- und Pull von allen erzeugenden Quellsystemen abgeholt. Die Installation eines Agenten im Quellsystem ist nicht notwendig.

Je nach Betriebssystem bzw. Applikation werden zum Anzapfen der Quellsysteme unterschiedliche Methoden genutzt. Im Unix-Umfeld können die Log-Informationen direkt von den Quellen in das CLW geschrieben werden. Für SAP wurden spezielle, von SAP zertifizierte Module entwickelt, die in die SAP-Systeme integriert werden. Mit ihnen können die SAP Audit Logs und die Statistik Logs abgeholt und das Security- und Transaktions Monitoring übernommen werden. Damit haben SAP-Anwender eine 360 Grad Sicht auf ihr komplettes SAP und ihre kundenspezifischen Anwendungen.

Schnell integriert - Datensammlung über Adaptoren

Die Daten werden über eine Schnittstelle, die Adaptoren, integriert. Über 180 Adaptoren für alle gängigen IT-Systeme sind bereits im CLW enthalten. Die unterstützte Palette reicht von diversen Betriebssystemen, über Applikationssysteme, Datenbanken bis hin zu Netzwerkkomponenten wie Firewalls oder IDS. Da die Adaptoren mit relativ geringem Aufwand zu erstellen sind lassen sich auch nicht marktübliche Quellsysteme an das CLW schnell anschließen.

Die Daten aus den Sourcen werden in einer speziellen Datenbank gesammelt und für jeden Quelltyp separat abgespeichert. Das hat den Vorteil, dass extrem hohe Komprimierungsfaktoren bis 40:1 gegenüber relationalen Datenbanken möglich sind. Mit den 2 TB Storage in der Grundversion können damit Daten im Umfang von 10 TB und mehr abgelegt werden.

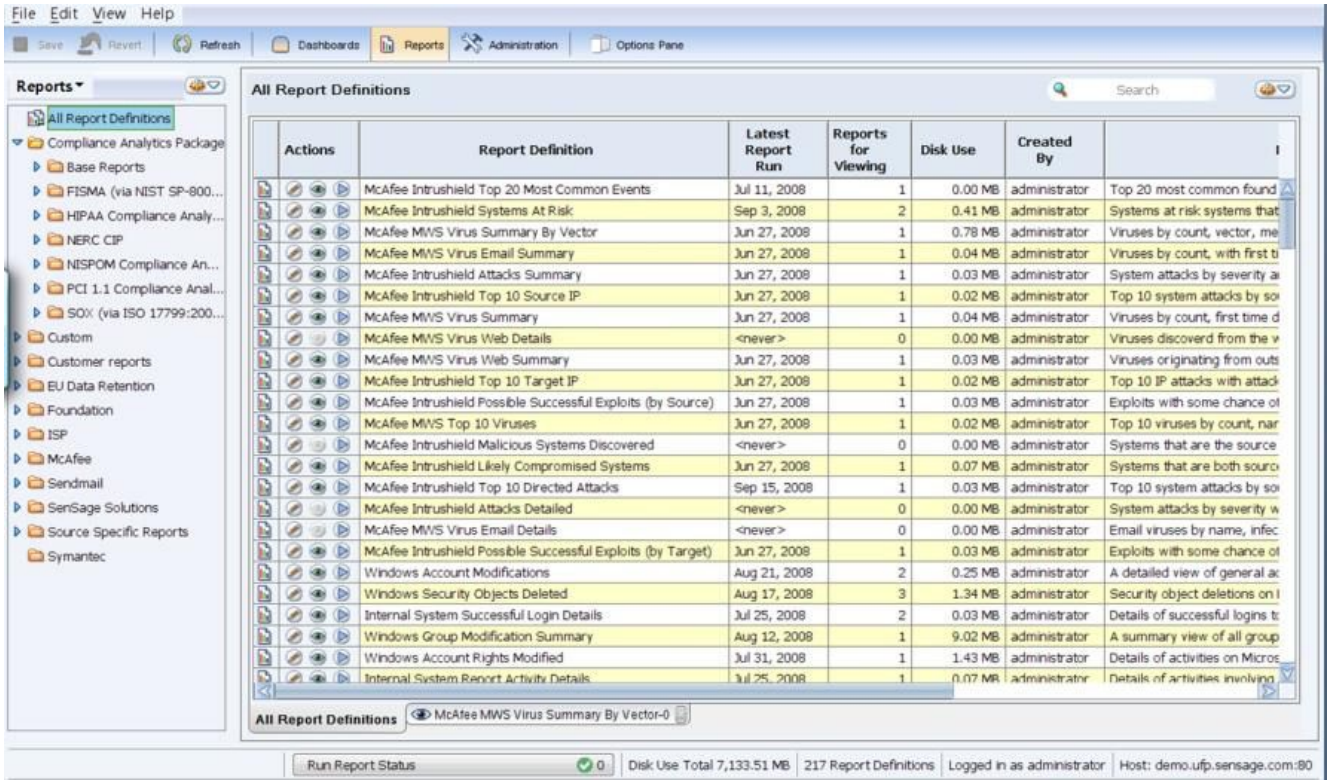
Ein wichtiger Aspekt der Compliance betrifft die Sicherung der Daten. Diese müssen entsprechend der unterschiedlichen Vorschriften elektronisch archiviert werden. Dabei ist zu gewährleisten, dass die Daten nicht verändert oder gelöscht werden können. Die im CLW gesammelten Daten werden deshalb weder indiziert noch normalisiert, sondern im Original der Quellen im CLW abgelegt.

Um die Daten vor Veränderung zu schützen werden Hash-Algorithmen eingesetzt. Desweiteren sorgt die Verschlüsselung der Daten für einen zusätzlichen Schutz. Somit gibt es keine Möglichkeit, die Daten zu überschreiben oder sonst wie zu manipulieren - die Gerichtsverwertbarkeit ist vollständig gewährleistet.

Schnell informiert - Analysen und Berichte

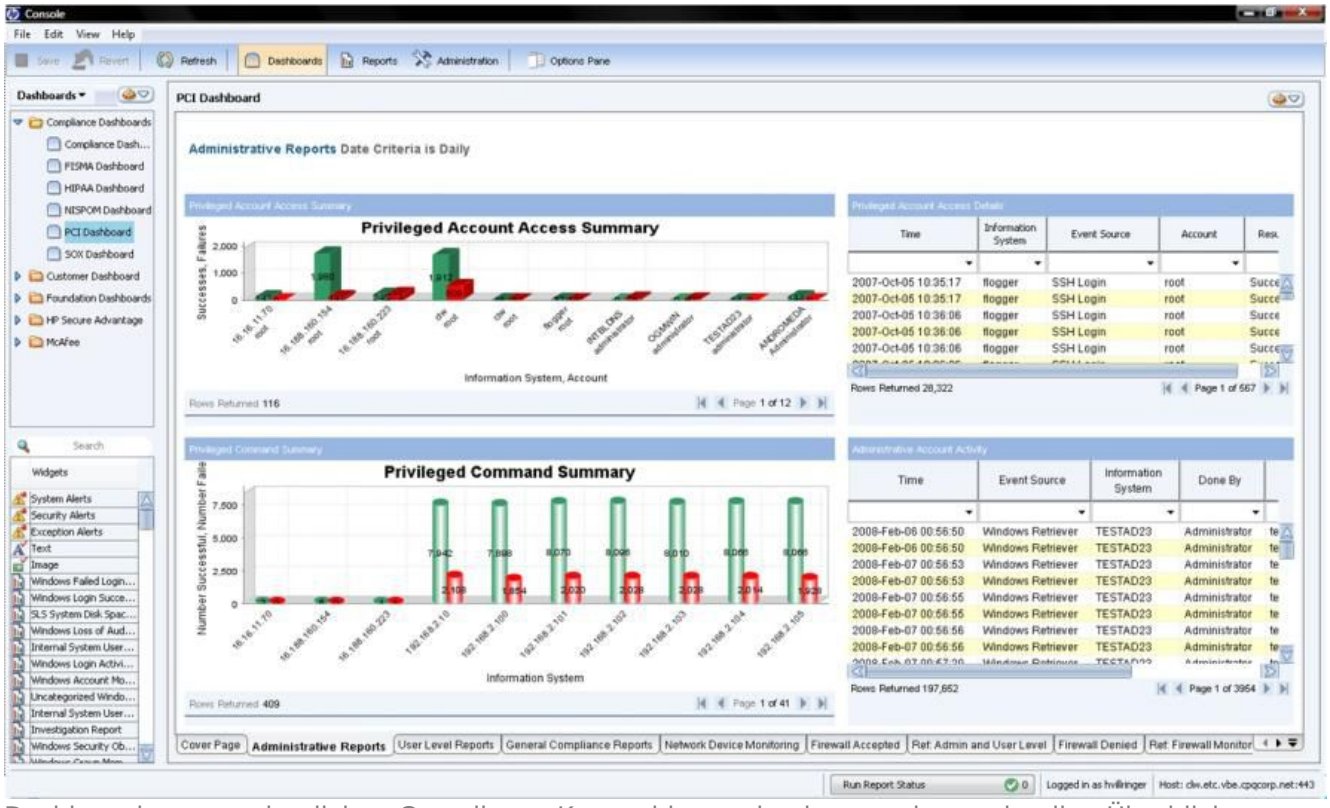
Neben der Datensammlung und der Langzeitarchivierung ermöglicht das CLW zahlreiche Analysen und Reports. Für Berichte oder spontane Abfragen durchsucht das CLW Milliarden Daten in wenigen Minuten. Individuelle Berichte lassen sich damit schnell und einfach generieren. Die Reports können über ein GUI oder über komplexe, individuell gestaltbare SQL Queries generiert werden.

Unterstützt werden Anwender dabei durch vorgefertigte Analysen gemäß üblicher Compliance-Vorschriften wie dem Sarbanes-Oxley Act, dem Payment Card Industrie Mandat oder der European Data Retention Directive für Telekommunikationsunternehmen. In entsprechenden Menüs werden dem User die für ein Compliance Mandat relevanten Informationen zur Verfügung gestellt. Speziell für SAP-Umgebungen beinhaltet CLW ein umfangreiches Repository an vorbereiteten Reports. Mit ihnen lassen sich bequem SAP relevante Auswertungen wie Processcontrol- oder das Risikomanagement zentral unter einer Oberfläche durchführen.



Zahlreiche vordefinierte Reports unterstützen den CWL-Anwender bei der Berichtserstellung.

Zusätzlich zur nachgelagerten Analyse und Auswertung kann eine Echtzeitüberwachung durchgeführt werden. Hierbei können die unterschiedlichsten Meldungen (Events) beim Eintreffen im CLW sofort mit weiteren eintreffenden Meldungen oder bereits gespeicherten Daten korreliert werden. Bei Erkennung eines sicherheitsrelevanten Vorfalls oder bei Abweichung von vordefinierten Grenzwerten und Trends werden weitere Aktionen angestoßen.



Dashboards veranschaulichen Compliance Kennzahlen und geben so einen schnellen Überblick.

Ein fein granulierbares Rechte- und Rollenmanagement für unterschiedliche Usergruppen sorgt beim Reporting für hohe Sicherheit. Dazu stellt das CWL verschiedene Oberflächen für individuelle Usergruppen bereit, in denen Rechte und Rollen festgelegt sind. Diese "Dash-Boards" garantieren, dass alle datenschutzrechtlichen Vorgaben eingehalten werden und jeder Nutzer nur die Daten zu Gesicht bekommt, für die er berechtigt ist. Sollten wirklich einmal Daten gerichtsrelevant werden, können entsprechende Rollen kreiert werden, die es etwa dem Staatsanwalt erlauben, die kritischen Informationen einzusehen.

Das System ermöglicht es auch, unterschiedlichen Konzernbereichen nur die für sie relevanten Sichten auf Daten zu geben und mehrere Unternehmensbereiche in ein zentrales Repository zu nehmen. Wobei der Konzern an sich wieder mit speziellen Rollenberechtigungen eine Gesamtsicht über diese Information bekommen kann.

Mehr Sicherheit mit CLW - Zwei praktische Beispiele

Zwei reale Beispiele aus der Unternehmenspraxis verdeutlichen den konkreten Nutzen des CLW im Bereich Security. Bei der Implementierung von SAP Systemen verwenden Betriebe oft globale Berechtigungen, weil noch nicht fest steht, welcher User welche Berechtigung braucht. Das hat schwerwiegende Nachteile, wenn diese Berechtigungen später im Realbetrieb nicht granular unterschieden und geändert werden. SAP-Rollen mit globaler Berechtigung erlauben es beispielweise Hackern, sich ungehinderten Zugang zu SAP-Systemen zu verschaffen.

Mit dem CLW lassen sich diese Nachteile vermeiden. Über das System kann über eine bestimmte Periode von etwa einem Monat oder einem Jahr mitgeloggt werden, welche Berechtigungen von Usern tatsächlich genutzt werden. Anschließend lassen sich die globalen Berechtigungen reduzieren, so dass jeder User wirklich nur die notwendigen Rechte besitzt. Mit der Möglichkeit, die Rollen zu überwachen und die Zugriffsrechte zu analysieren trägt das CLW deutlich zur Steigerung der IT-Sicherheit bei.

Ein anderes Beispiel, wie mit CLW die Sicherheit erhöht werden kann, sind langsame Attacken. Für gewöhnlich hat ein User drei Login-Versuche. Nach dem dritten Falsch-Login wird der Zugang gesperrt, das System wird zurückgesetzt und der Nutzer muss sich ein neues Passwort geben lassen. Hacker nutzen dieses Procedere für langsame Attacken. Der Angreifer versucht dabei das Login nur zweimal, beim dritten, richtigen Login durch den regulären User wird der Zähler wieder zurückgesetzt. Für die IT sieht alles sauber aus, doch der Hacker kann nach dem Rücksetzen des Zählers immer wieder seine zweimaligen, unbemerkten Login-Versuche starten und das Procedere beliebig oft und unbemerkt wiederholen.

Immer öfter berichten Unternehmen von solchen Attacken, die sich über Monate verfolgen lassen. Ein Log-Auswertungssystem wie das CLW erleichtert die Aufklärung. Es zeigt, dass hier Vorgänge über einen sehr langen Zeitraum stattfinden, die aus dem Windows System nicht herauslesbar sind. Hingegen können CLW-Anwender leicht feststellen, dass aktive Angriffe von intern auf IT-Systeme erfolgen.

Links im Artikel:

[1] **http://www.sans.org/**
