Einzelheftpreis € 15,-

4/2008 Februar April Juni August Oktober Dezember

IT-SICHERHEIT
Fachmagazin für Informationssicherheit und Compliance

IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Compliance

„Das Unmögliche möglich machen!"

Im Interview: Helmut Heptner, Geschäftsführer bei Acronis Germany

Anbieterübersicht: NAS-Server

Schutz der informationellen Selbstbestimmung
Im Exklusiv-Interview: Prof. Peter Gola, Vorstands-vorsitzender der GDD

Speichersicherheit:
- Backup, Archivierung und Compliance
- E-Mail-Management
- Unified Archiving

Ausfall- und Prozesssicherheit:
- Von Desaster Recovery zu Business Continuity
- Enterprise Rights Management

DATAKONTEXT www.datakontext-press.de

Konvergenz von Security und Compliance

Zwei Seiten einer Medaille

Die Aufgabenstellungen hinsichtlich Sicherheit und Compliance werden die IT-Landschaft so lange dominieren wie sensitive Daten über Kunden, Mitarbeiter, Patienten und Finanztransaktionen ausgetauscht oder gespeichert werden. In der Vergangenheit haben sich die Sicherheitsteams mit dem Schutz der Daten beschäftigt und die Compliance-Verantwortlichen sich auf die Kontrolle der Nutzung fokussiert. Allerdings sind beide Disziplinen in der Praxis zwei Seiten der selben Medaille. Richtlinien und Vorschriften unterstützen weltweit diese Sichtweise und verlangen, dass Sicherheits- und Compliance-Bereiche zusammenarbeiten. Auch wenn diese Herangehensweise für viele Organisationen eine Herausforderung darstellt, bietet ein integriertes Vorgehen eine Reihe von Vorteilen wie Kostenreduktion, verbesserte Effizienz, höhere Sicherheit und Kontrolle der Einhaltung von Richtlinien.

Eine steigende Anzahl von Regularien führt zu einer immer komplizierteren Organisation. Aus den USA stammen etwa Sarbanes-Oxley (SOX), der Payment Card Industry Data Security Standdard (PCI DSS), California Senate Bill 1386 (CA SB1386), der Health Insurance Portability and Accountability Act (HIPAA), der Graham-Leach-Bliley Act (GLBA) und andere. In Europa gibt es daneben etwa die European Data Protection Directive (DPD) oder den Basel Capital Accord (Basel II). Die Anforderungen einiger dieser Richtlinien sind eher vage. Der Prozess, die Anforderungen mit der individuellen IT-Infrastruktur abzugleichen, ist ein ziemlich entmutigendes Projekt. In diesem Beitrag soll PCI DSS als Beispiel dienen, um eine Orientierungshilfe für eine breite Palette an Vorschriften zu geben.

Schutz und Kontrolle sensitiver Daten

Organisationen müssen ihre Daten schützen und sicherstellen, dass jeder Zugriff auf jede Nutzung von sensitiven Informationen kontrolliert wird. Bei PCI handelt es sich um Kreditkarteninformationen, andere schließen Informationen wie Gesundheitsdaten, Mitarbeiterinformationen oder Geschäftszahlen ein. PCI verlangt, dass Unternehmen die Daten der Kreditkarteninhaber schützen und postuliert, dass Logging-Mechanismen und die Fähigkeit, Anwenderaktivitäten zu verfolgen notwendig sind. Des Weiteren müssen Prüfberichte angelegt und gesichert werden, ohne dass eine Veränderung möglich ist. Die entsprechenden Daten werden häufig von ERP, CRM, E-Commerce und anderen Anwendungen abgerufen. Deswegen adressieren die Regularien mehrere Ebenen der IT-Infrastruktur, von der Datenbank über die Applikation bis zum Web-Interface.

Weil die Richtlinien zunehmen, ist eine isolierte Herangehensweise für IT-Sicherheit und Richtlinienkonformität nicht möglich. Unternehmen brauchen einen rationelleren und effizienteren Mechanismus, um die vielfältigen Anforderungen an Security und Compliance zu erfüllen. Nur mit einem abgestimmten Prozess lassen sich mehrere Anforderungen gleichzeitig erfüllen. Ein derartiger Anwendungsdaten- und Compliance-Lifecycle kann aus vier einfachen Schritten bestehen: Identifikation und Beurteilung, Definition von Kontrollen und Policies, Überwachung und Durchsetzung sowie Messung.

Erster Schritt: Identifikation und Beurteilung

Zunächst müssen die Systeme identifiziert werden, die sensitive Daten speichern. Anschließend erfolgt eine Risikobeurteilung. Aus der Sicherheitsperspektive müssen Konfigurationsprobleme aufgedeckt werden, die Schwachstellen verursachen oder nicht in der Lage sind, diese zu schließen. Aus der Compliance-Perspektive müssen die Probleme ermittelt werden, die die Systemintegrität unterminieren, die notwendig ist, um Unternehmensrichtlinien (Policies) zu etablieren und Datennutzungskontrollen aufzusetzen. Zum Beispiel warnt PCI davor, vom Hersteller bereitgestellte Voreinstellungen für Systempasswörter und andere Sicherheitsparameter zu verwenden um sicherzustellen, dass Systeme keine Hintertüren besitzen, die dazu geeignet sind, Sicherheits-, Prüfungs- oder Kontrollfunktionen zu umgehen.

In Verbindung mit dieser Aufgabe müssen Unternehmen feststellen, welche Anwender in welcher Art normalerweise auf sensitive Daten zugreifen. PCI schreibt vor, den Zugriff auf Ressourcen und Karteninhaber-Informationen auf diejenigen Personen zu begrenzen, die im Rahmen ihrer Aufgabe einen derartigen Zugang benötigen. Diese Information ist notwendig, um die Grundsätze des legitimierten Verhaltens zu verstehen und Policies sowie Kontrollen zu etablieren. Die Nutzung von Werkzeugen für die Identifikation und den Prüfungsprozess reduziert den damit verbundenen Aufwand erheblich. Dazu sind mehrere Fähigkeiten unerlässlich:

Abb. 1: Vier Schritte, um Sicherheit und Compliance zu erreichen, Quelle: Imperva

Mit seinen Securesphere-Appliances adressiert Imperva den Markt für Application-Security und Compliance. Foto: Imperva

Mitgelieferte Handlungsanweisungen für „Best-Practice-Security" und Richtlinienverletzungen, automatische Erkennung der Anwenderaktivitäten, um Zeit zu sparen und legitimierte Änderungen vorzunehmen, ausreichendes Berichtswesen, um Daten nach Anwender, Datenbankobjekt oder anderen Faktoren zu gruppieren sowie eine Multi-Vendor-/ Multi-Versions-Umgebung um sicherzustellen, dass das Werkzeug über verschiedene Datenbanksysteme hinweg arbeitet.

Zweiter Schritt: Kontrollen und Policies

Der zweite Schritt besteht in der Definition von Sicherheitsregeln und Prüfkontrollen sowie der Durchsetzung von Datennutzungspolicies. Wiederum gibt das Beispiel PCI detailliertere Orientierungshilfen. Der Standard behandelt Verfolgungs- und Auditierungsanforderungen sowie Zugangskontrollen. Er fordert, dass alle Aktivitäten im Zusammenhang mit kritischen Daten und Systemen ausschließlich durch bekannte und autorisierte Anwender durchgeführt und bis zu diesen zurückverfolgt werden können. Policies müssen ausreichend detailliert sein, um Sicherheit zu garantieren, gleichzeitig aber auch flexibel genug, um Veränderungen der Verantwortungsbereiche und der Infrastruktur zu ermöglichen. Policies und Kontrollen sollten eine Reihe von Bereichen definieren: Die Tabellen, auf die jeder Nutzer zugreifen darf, Tabellen, die sensitive Daten beinhalten und einen stärkeren Schutz benötigen, Anwender, die privilegierte Rechte besitzen, eine Beschreibung der Arbeitsabläufe für jeden Anwender (Tabellen und Operationen), Abfragen, die Applikationen für den Zugriff auf Datenbanken benutzen sowie die Zeitpunkte und Applikationen des Zugriffs auf die Datenbanken.

Dritter Schritt: Überwachung und Durchsetzung

Sobald die Policies und Kontrollen aufgesetzt sind, müssen alle Datenbankaktivitäten überwacht und die Policies durchgesetzt werden. Es ist wichtig festzustellen, wer die Policies einhält oder verletzt. Beim Auftreten einer Verletzung muss sichergestellt sein, dass die Alarmierungs- und Durchsetzungsmechanismen wie vorgesehen arbeiten. Die bereitgestellten Informationen müssen gleichzeitig umfassend und detailliert genug sein, um Entscheidungen über individuellen Policies zu treffen und die übergeordnete Kontrolle der sensitiven Daten zu ermöglichen.

Sowohl das Security- als auch das Compliance-Personal benötigen entsprechende Reports, um Abweichungen einfach zu erkennen und auf die individuellen Transaktionen zurückzuverfolgen. Compliance-Verantwortliche prüfen in der Regel auf einer periodischen Basis, wohingegen die Sicherheitsverantwortlichen gemeinhin an Echtzeit-Daten interessiert sind. Bei PCI müssen sowohl Compliance als auch Security angesprochen werden. So ist vorgeschrieben, dass Logs mindestens täglich kontrolliert werden und dass Alarme in Echtzeit stattfinden.

Schritt vier: Messung

Der vierte Schritt zeigt den sichtbaren Output der Aktivitäten der ersten drei Schritte und gibt Feedback auf den ersten. Die Berichtsfunktionen müssen Informationen klar in den Formaten präsentieren, die von Sicherheits- und Auditpersonal, dem Management oder anderen Organisationen erwartet werden, die mit der Prüfung der Security- und Compliance-Standards beauftragt sind. Im Hinblick auf die Compliance sollten mitgelieferte Reports mehr als eine Richtlinie adressieren können. Zudem sollte die Möglichkeit bestehen, individuelle Berichte zu erstellen. Hinsichtlich der IT-Security müssen diese Berichte eine Identifikation und Überwachung verdächtiger Aktivitäten oder im Bedarfsfall schützende Aktivitäten ermöglichen.

Defizite existierender IT-Toolkits

Die in Datenbanken vorhandenen Prüfwerkzeuge sind unzureichend bei der Erfüllung der Anforderungen der Compliance-Richtlinien. Zum Beispiel stellen die Prüf-Logs der Datenbanken, die für geschäftskritische Anwendungen wie Oracle E-Business Suite, Peoplesoft oder SAP zum Einsatz kommen, nicht immer Informationen über die verantwortliche Person für jede Datenbanktransaktion bereit. Für Audit und Security gibt es eine Reihe von Schlüsselanforderungen: Unabhängigkeit von der zu prüfenden Datenbank, Identifikation des verantwortlichen Anwenders für jede Aktivität, Detailtiefe, Erfassung aller Aktivitäten sowie Identifikation grundlegender Abweichungen von Policies und Durchsetzungsmechanismen. Neue Systeme für Data Activity Monitoring (DAM) stellen ein integriertes Framework zur Automatisierung des vierstufigen Datensicherheits- und Compliance-Lebenszyklus bereit und überwinden die Defizite, die bei reinen Compliance- oder Security–Werkzeugen bestehen. Eine Reihe von Herstellern bietet derartige Produkte an, jeweils mit einer geringfügig anderen Herangehensweise. Entsprechende Lösungen sollten grundlegende Funktionen erfüllen.

Dazu zählt die Fähigkeit, einzelne Anwender zu identifizieren und ihre Aktivitäten genau zurückzuverfolgen, die Fähigkeit zur Pflichtentrennung – entsprechende Produkte müssen die Datenbankaktivitäten verfolgen ohne die Datenbank für den eigenen Betrieb zu benötigen, die Fähigkeit, Compliance-Berichte über eine Vielzahl von Richtlinien hinweg zu erstellen sowie die Fähigkeit, sowohl zu Audit-Logging als auch zu Echtzeit-Alarmierung durchzuführen.

Darüber hinaus ist die Erkennung von grundlegenden Abweichungen und Policy-

Verletzungen sowie eine detaillierte Information darüber unerlässlich, ebenso wie die Kombination aus manuell anpassbaren und automatisch gelernten Policies. Dies vereinfacht den Roll-Out und das kontinuierliche Management. Die Möglichkeit, legitimierte Änderungen an Applikationen und Datenbanken zu erkennen, befreit von konstantem manuellen Tuning. Nicht zuletzt sollten diese Produkte transparent ohne irgendwelchen Einfluss auf die IT-Infrastruktur arbeiten.

Web-Anwendungen

Datenbankkontrollen können via Web-Applikationen untergraben werden. Angreifer können mittels Applikationen unerkannt auf eine Datenbank zugreifen, tatsächlich auch als Applikation. Unter der Maßgabe des privilegierten Zugangsstatus von Applikationen würde diese Aktivität nicht als verdächtig eingeschätzt und durch traditionelle Datenbankprüfwerkzeuge nicht erkannt. Deshalb gibt es bei PCI die Wahl – entweder wird eine Application-Layer Firewall installiert oder der Applikationscode wird durch eine Organisation überprüft, die auf Anwendungssicherheit spezialisiert ist. Auch wenn Code-Reviews im Prinzip eine gute Sache sind, so ist doch die Beauftragung von Consultants zur Prüfung des gesamten Anwendungscodes kostspielig und bietet nicht den kontinuierlichen Schutz, den eine Application Firewall offeriert.

Autor

Shlomo Kramer,
President und CEO von Imperva

Shlomo Kramer gilt als einer der Pioniere der Firewalls. Bereits 1993 war er Mitbegründer von Check Point und war dort bis 2003 Mitglied der Geschäftsführung. In dieser Zeit entstanden unter seiner Federführung die Produkte FireWall-1, VPN-1 und FloodGate-1. Als Investor und Aufsichtsratsmitglied hat sich Shlomo Kramer an der Gründung von IT-Security-Unternehmen wie Palo Alto Networks, Serendipity Technologies und Trusteer beteiligt. Seit der Gründung von Imperva konzentriert sich Kramer auf das Thema Sicherung von Anwendungsdaten.

„Die Bedrohungslandschaft hat sich in den letzten Jahren vollständig verändert", so Kramer. „Früher waren Hacker vor allem durch ihre Egos getrieben. Heute geht es in erster Linie um den Profit. Es gibt organisierte Verbindungen und einen schwarzen Markt für gestohlene Informationen wie Kreditkarten oder persönliche Daten. Das schürt auch die Versuchung für interne Mitarbeiter." Shlomo Kramer wurde für sein Engagement mehrfach ausgezeichnet. Network World wählte ihn zu einer der 20 Persönlichkeiten, die das Netzwerk-Business verändert haben, in diesem Jahr wurde er als CEO of the Year von SC Magazin gewählt.