

Die Anforderungen von PCI DSS erfüllen

Mit Luminet Insiderdelikte bekämpfen und Konformität herstellen

Eine der größten Herausforderungen für Unternehmen, die sich verpflichten, die Anforderungen von PCI DSS (Payment Card Industry Data Security Standard) zu erfüllen, verbirgt sich in Anforderung 10.2.1 dieses Regelwerks. Diese Anforderung verlangt die „Implementierung automatisierter Audit-Trails für alle Systemkomponenten zur Rekonstruktion ... aller individuellen Zugriffe auf Karteninhaberdaten.“ Anforderung 10.2.2 schreibt ferner vor, dass „alle von einer Einzelperson mit Root- oder Administratorrechten vorgenommenen Aktionen“ in den Audit-Trail aufzunehmen sind.

Warum Audit-Trails schwer zu erstellen sind

Die Konformität mit den Anforderungen von PCI DSS in Bezug auf Audit-Trails ist aus vier Gründen schwer herzustellen:

1. Die meisten Unternehmensanwendungen gleich welchen Alters beinhalten keine Protokollierungsmechanismen, die den Benutzerzugriff auf die Karteninhaberdaten vollständig aufzeichnen könnten. In vielen Fällen protokollieren die Log-Dateien nur Schreibvorgänge, keine Benutzerabfragen und andere reine Lesevorgänge. Um vollständig zu sein, muss ein Audit jedoch auch den Lesezugriff jedes einzelnen Benutzers erfassen.
2. Die einfache Sammlung von Log-Dateien erfüllt möglicherweise bestimmte Auflagen von PCI DSS, nicht jedoch die Forderung nach einem vollständigen Audit-Trail gemäß Anforderung 10.2. Enthalten die Protokolle keine ausreichenden Daten oder enthalten sie nur bestimmte Arten von Aktivitäten, hilft die Log-Dateisammlung bei der Erfüllung von Kapitel 10.2 auch nicht weiter.
3. Die Erstellung einer Inhouse-Lösung würde zeit- und kostenaufwendig sein. In einem großen Unternehmen müssten Tausende von Anwendungsprogrammen geändert, neu getestet und neu implementiert werden. Anschließend hätte man immer noch keine zentralisierte und einfach administrierbare Ansicht dessen, wer genau was und wann in allen Anwendungen und Systemen unternommen hat.
4. Die reine Erfassung von Datenbankaktivitäten stellt ebenfalls keine Konformität her, da die meisten Anwendungen für den Datenbankzugriff eigene Benutzerkennungen verwenden. Unter dem Strich lässt sich die Anforderung nach Protokollierung „aller individuellen Zugriffe“ so nicht erfüllen.

Die gute Nachricht ist, dass es eine Technologie gibt, die diese Herausforderungen bewältigen kann.

Beobachten. Aufzeichnen. Analysieren.

Attachmate Luminet™ wurde mit dem Ziel entwickelt, ein vollständiges Bild aller Benutzerzugriffe auf Kreditkartendaten zu erfassen, um für Audit-Zwecke nicht länger kryptische Log-Dateien manuell durchkämmen zu müssen. Und so arbeitet Luminet:

- **Benutzeraktivitäten beobachten**
Luminet stellt das Instrumentarium zur Definition konfigurierbarer Geschäftsregeln bereit, um verdächtige Verhaltenweisen im Rahmen des Risikomanagements erkennen zu können. Luminet erzeugt bei verdächtigen Verhaltensmustern Warnmeldungen in Echtzeit, um Anomalien unverzüglich auf den Grund gehen zu können.
- **Benutzeraktivitäten aufzeichnen**
Luminet zeichnet alle Benutzeraktivitäten in Echtzeit einschließlich jedes Fensters und jeder Tastenbetätigung auf und erzeugt einen Audit-Trail direkt aus dem Netzwerk. Dieser Audit-Trail umfasst sowohl die Updates als auch alle Lesevorgänge seitens regulärer und privilegierter Benutzer. Luminet speichert diese Informationen in einem sicheren Repository, aus dem man leistungsfähige Volltextsuchläufe in den aktuellen oder aufgezeichneten Aktivitäten durchführen kann. Diese Suchläufe ermöglichen die visuelle Wiedergabe aller für eine Prüfung maßgeblichen Fenster und Tasteneingaben. Konfigurierbare Dashboards, Diagramme und Berichte vermitteln den

Über PCI DSS

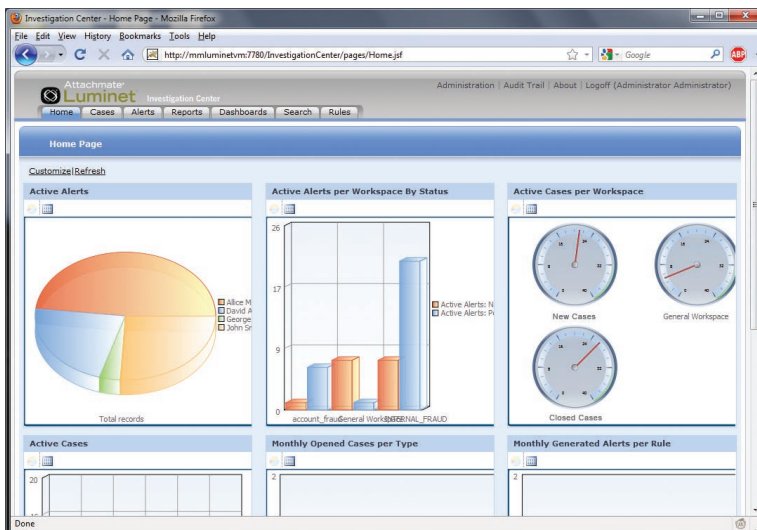
Der Payment Card Industry Data Security Standard (PCI DSS) wurde vom PCI Security Standards Council entwickelt und wird von diesem auch verwaltet (pcisecuritystandards.org). Dabei handelt es sich um ein internationales, offenes Forum, das von führenden Kreditkartengesellschaften zur Definition der Anforderungen an Organisationen geschaffen wurde, die Kreditkartendaten verarbeiten. Ziel ist die Vermeidung von Kreditkartenbetrug und die Schaffung durchgängiger Sicherheitsmaßnahmen unter allen Anwendern von Kreditkartendaten. Der Standard definiert zwölf konkrete Anforderungen, die von jeder Organisation umgesetzt werden müssen, die Kreditkartendaten speichert, verarbeitet oder überträgt.

internen Prüfern auf einen Blick ein umfassendes Bild und versetzen sie in die Lage, Aktivitäten gezielt nachzugehen, die die Konformität mit PCI DSS gefährden könnten.

• Benutzeraktivitäten analysieren

Luminet unterstützt Anwender dabei, zwischen dubiosen Aktivitäten und legitimen Vorgängen zu unterscheiden. Ein interaktives Werkzeug erkennt übergreifende Muster unter Mitarbeitern und Abteilungen sowie über diverse Anwendungen hinweg. So ist es möglich, bei verdächtigen Verhaltensweisen unverzüglich einzugreifen.

Luminet setzt anwendungsübergreifend auf drei Strategien: Benutzeraktivitäten beobachten, aufzeichnen und analysieren. So entsteht ein lückenloser Audit-Trail aller individuellen Zugriffe auf sensible Informationen, wie beispielsweise Kreditkartendaten. Ohne den Einbau weiterer Kontrollen oder irgendwelche Änderungen am Programmcode sind Anwender mit Luminet in der Lage, einen vollständigen Audit-Trail zu erstellen, der dazu beiträgt, die Anforderungen 10.2.1 und 10.2.2 von PCI DSS zu erfüllen.



Überwachung wichtiger Aktivitätsgrößen mit anpassbaren Dashboards.

Luminet: Beobachten. Aufzeichnen. Analysieren.

Luminet, die Softwarelösung zur Bekämpfung von Insiderdelikten, setzt anwendungsübergreifend auf drei Strategien: Benutzeraktivitäten beobachten, aufzeichnen und analysieren. Luminet führt eine genaue und belegbare Überwachung der Anwendungen durch und erstellt daraus aussagekräftige Informationen als Grundlage für fundierte Entscheidungen.

Die wichtigsten Merkmale im Überblick:

- Agentenlose Architektur
- Übergreifende Überwachung
- Warnmeldungen in Echtzeit
- Visuelle Wiedergabe von Anwendungsfenstern
- Google-ähnliche Suchfunktion
- Grafische Link-Analyse
- Unterstützung von Legacy-Anwendungen
- Fallbearbeitung
- Individuelle Dashboards und Berichte

Über Attachmate

Attachmate ist ein führender Hersteller von fortschrittlichen Softwarelösungen für Terminalemulation, Modernisierung von Legacy-Systemen, Managed File Transfer und Enterprise Fraud Management. Attachmates Technologie unterstützt Unternehmen bei der Erweiterung, Verwaltung und Absicherung ihrer IT-Systeme. Das Unternehmen zählt 65.000 Kunden weltweit. www.attachmate.de



Hauptsitz
1500 Dexter Avenue North
Seattle, Washington 98109
TEL +1 206 217 7500
FAX +1 206 217 7515

Europäische Zentrale
Niederlande
TEL +31 172 50 55 55
FAX +31 172 50 55 51

Österreich
TEL +43 1 595 4335 0
FAX +43 1 595 4335 11
www.attachmate.at
info-at@attachmate.com

Schweiz
TEL +41 43 399 2090
FAX +41 43 399 2099
www.attachmate.ch
InfoCH@attachmate.com

Deutschland
TEL +49 89 99 351 0
FAX +49 89 99 351 111
TEL +49 2102 4965 0
FAX +49 2102 4965 65
www.attachmate.de
info-de@attachmate.com

Weitere Niederlassungen von Attachmate finden Sie unter www.attachmate.de.