Compliance-Management leicht gemacht

logpoint

Compliance-Management leicht gemacht

Log- und Compliance-Management in einer Lösung

Das Management der Security-Infrastruktur unter Einhaltung aller Compliance-Richtlinien ist eigentlich eine ganz einfache Aufgabe - mit LogPoint.

Compliance Management – eine herausfordernde Aufgabe

Die Realisierung der Security Compliance ist normalerweise eine sehr zeitintensives und teueres Unterfangen. Unternehmen müssen nicht nur die Anforderungen hinsichtlich Auditing und Controlling erfüllen. Enorme Datenmengen an Log-Dateien müssen dafür unter Einhaltung aller relevanten gesetzlicher Vorgaben verarbeitet werden.

Diese Aufgaben sind nicht nur kostenintensiv und kompliziert. Fehlende oder fehlerhafte Ergebnisse führen zu Geldbußen, zu Kosten für entsprechende Veröffentlichungen, Strafverfahren und Imageschäden und können so zu enormen finanziellen Verlusten führen.

Log Management – ein schöner Schein

Grundsätzlich wurden Compliance-Richtlinien definiert, damit Sie durch verlässliche Informationen zusammen mit dem entsprechenden Reporting über den Zustand der Security stets im Bilde sind. Dies ist zur Absicherung eines jeden Unternehmens absolut notwendig. Compliance-Vorgaben variieren jedoch und setzen die Speicherung aller gesammelten Event-Logs voraus.

Ein Log-Management ist überhaupt die Voraussetzung dafür, dass die Compliance eingehalten werden kann. Gleichzeitig ist es der erste Schritt hin zu einer effektiven Security-Strategie. Durch die Auswahl und die Fokussierung auf die wichtigen Probleme können Sie sehr einfach alle Compliance-Vorgaben umsetzen.

LogPoint – schnell, einfach, effektiv

Jahrelange Erfahrung im Bereich Compliance-Management führte zur Entwicklung von LogPoint. Mit LogPoint setzen Sie alle Vorgaben im Compliance-Bereich schnell, einfach und effektiv um.

Sicherheitsvorgaben unterscheiden sich von Unternehmen zu Unternehmen – aber sie basieren immer auf den gleichen grundsätzlichen Regeln. LogPoint A/S hilft Ihnen mit LogPoint, die täglichen Aufgaben bei der Umsetzung dieser Regeln zu erfüllen.

- Automatisches Sammeln aller netzwerkweit vorhandenen Event-Informationen
- Speicherung aller Event-Logs für umfassende Security-Audits
- Schnelle Antworten bei Bedrohungen durch Identifikation, Sanierung und Reporting
- Alarme bei Verstößen gegen Compliance-Richtlinien
- Überprüfung der Funktionstüchtigkeit aller Kontrollmechanismen
- Vergleichen von Datenvolumina und Events zur Aufdeckung potentieller Probleme
- Dokumentierung von Vorfällen und Reporting von Audits
- Out-Of-The Box, standardisiertes Compliance

ISO 27001 Compliance

Optimale Security-Information

Die International Organization for Standardization, ISO 27001, hat Vorgaben definiert, welche als Empfehlung für ein optimales Security-Management gelten. Dabei ist es wichtig zu erwähnen, dass ISO27001 Sicherheitsempfehlungen für ein beispielhaftes Security Information Management enthält.

- Nicht berechtigte Anwender dürfen keinen Zugriff auf unternehmenskritische Systeme und vertrauliche Informationen haben.
- Daten und Prozesse dürfen nicht veränderbar sein und müssen vollständig vorhanden sein
- Informationen und Daten müssen immer überprüfbar sein

Sicherheitslösungen

Gemäß dieser auf dem ISO 27001 basierenden Verhaltensregeln für das Information Security Management müssen Kontrollmechanismen für die gesamte IT-Infrastruktur eingeführt werden. In Übereinstimmung mit dem Communications & Operations Management und dem operativen Information Security Incident Management müssen alle Bereiche der IT umfassend überwacht und analysiert werden können.

Um diese Vorgaben zuverlässig und kostengünstig zu erfüllen, muss eine automatisierte Lösung folgende Aspekte abdecken:

- Umfassende Korrelation aller Daten
- Genaueste Analysemöglichkeiten
- Detailliertes, ISO 27001konformes Reporting

LogPoint und ISO 27001

Die strengen Vorschriften zur ISO 27001-Compliance benötigen eine ausgefeilte Strategie des Security Compliance Managements. Sowohl Security Information und Event Management (SIEM) als auch Log Management müssen abgedeckt werden. LogPoint bietet diese Voraussetzungen – es ermöglicht das Sammeln und Analysieren von Log-Daten und schützt Applikationen und Datenbanken vor internen Bedrohungen. Zusätzlich liefert LogPoint verarbeitbare Informationen zur Security- und ISO 27001-Compliance über alle im Unternehmen vorhandenen Daten in Echtzeit.

Mit der LogPoint SIEM-Lösung können Sie ein permanents Risiko-Management durchführen und erfüllen gleichzeitig alle Sicherheitsvorgaben einschließlich ISO 27001.

Mehr als nur eine Log Management-Lösung

Ein Log Management, das die definierten Kontrolleinrichtungen und die erwarteten Compliance-Resultate liefert, ist eine wichtige Grundlage für ISO 27001-Vorgaben. Während gängige Log Management-Lösungen nur das Sammeln, Speichern und die Reports allgemeiner Event Logs übernehmen, bietet Ihnen LogPoint deutlich mehr.

Dank der vielschichtigen, patentierten Korrelationstechnologie wird aus dem Log Management heraus ein tiefer Einblick in die unternehmensweite IT-Umgebung möglich. Durch die Verknüpfung aller Logs ermöglicht LogPoint einen umfassenden und klar verständlichen Überblick über Events, Struktur und Trends in Echtzeit. Auf diese Weise können mögliche Bedrohungen gestoppt werden, bevor diese sich zum echten Problem entwickeln.

LogPoint erstellt ferner analytische Verknüpfungen aller auffälligen Ereignisse der Vergangenheit. Die standardisierten und kategorisierten Ereignisse oder Events ermöglichen sodann die schnelle, auf Analysen basierende Reaktion in Echtzeit.

Effektives Security Compliance Management

LogPoint ist eine effective Security Compliance Management Suite mit der alle sicherheitsrelevanten Vorgaben einschl. ISO 27001 komplett abgedeckt werden können.

- Zeit- und Ressourcen-Einsparung bei der Umsetzung von Compliance-Vorgaben
- Überwachen und messen der Effektivität der PCI Compliance Kontrollmechanismen
- Informationen über Third-Party Audits und Compliance-Tests
- Sicheres Erfassen und Speichern von Event Logs als revisionskonforme Beweissicherung
- Korrelation der Events von Devices und Applikationen
- Erkennen der Bedrohungslage und der Compliance-Abweichungen in Echtzeit
- Sofortige Alarmierung bei Abweichungen von Richtlinien und Kontrolleinstellungen
- Out-Of-The-Box, standardisierte Berichte und Regeln zu ISO 27001

Weitere Informationen:

www.logpoint.com

logpoint

Sarbanes-Oxley Act (SOX) Compliance

SOX – optimale Security-Richtlinien & proaktives Risiko-Management

Das Sarbanes-Oxley Act (SOX) wurde entwickelt, um den Schutz von Investoren durch den Einsatz von genauen und verlässlichen Informationen über Unternehmen im Einklang mit bestehenden gesetzlichen Vorgaben zu gewährleisten. Die SOX-Standards müssen strikt eingehalten werden. Bei Nichteinhaltung drohen Strafen.

SOX ermöglicht eine proaktive, risikobasierende Überprüfung der internen Kontrollmechanismen börsennotierter Unternehmen. Alle Daten und Applikationen, die der Compliance unterliegen, werden unternehmensweit sowohl auf Applikationsebene als auch auf Netzwerkebene überwacht und gesichert.

Die Einbindung eines echten, richtlinienbasierenden Sicherheitsprogramms ist eine große Herausforderung. Um die Vorgaben von SOX zu erfüllen, müssen Ereignisse nachvollziehbar überprüft und eine nachweisbare Risikominderung erzielt werden. Interne Kontrollen müssen überprüfbar sein, wie z.B.:.

- Logs, Berichte über Ereignisse, Alarme und IDM-Systeme
- Informationen über die Verwendung von Applikationen
- unternehmensweit, über alle Plattformen

Durch ein ordnungsgemäß implementiertes, risikobasierendes Auditing können die SOX-Compliance-Richtlinien besser umgesetzt werden. Bei gleichzeitiger Kostenreduktion werden die Kontroll- und Finanzberichte transparenter.

LogPoint SOX Lösungen

LogPoint ist die kostengünstige Lösung zum proaktiven Risiko-Management von Netzwerken, Systemen, Applikationen, Datenbanken und Anwenderaktivitäten, die allen Vorgaben der SOX-Compliance entspricht. LogPoint liefert ein verlässliches, umfassendes Security-Monitoring und Event-Management für Applikationen, Daten von IT-Systemen im Finanzsektor. Durch den Einsatz dieser effektiven Security Compliance-Lösung ist jedes Unternehmen mit den Werkzeugen ausgestattet, die es braucht, um alle SOX-Auflagen zu erfüllen.

Log Management und mehr

Ein Log Management ist die Grundvoraussetzung zur Umsetzung der SOX Compliance. Es ermöglicht das Sammeln und Speichern von Daten, Reports über Log-Inhalte und stellt darüber hinaus sicher, dass alle getroffenen Kontrollmaßnahmen richtig funktionieren. Dennoch ist das Log Management nur ein Baustein, der die Einhaltung einer SOX Compliance ermöglicht. LogPoint bietet mehr als nur das Sammeln und Speichern von Event-Logs. LogPoint nutzt hoch entwickelte Korrelationsmöglichkeiten und trägt somit dazu bei, dass selbst ausgefeilte Sicherheitsbedrohungen verhindert bzw. minimiert werden.

SOX-Konformität und gesicherte Infrastruktur in einem

Durch den Einsatz von LogPoint werden optimale Sicherheitsvorgaben und ein fortlaufendes Risiko-Management erzielt:

- Sammeln von Daten und Informationen
- Log Management
- Monitoring in Echtzeit
- Identifikation von Bedrohungen
- Schnelle Reaktion
- Flexibles und umfassendes Reporting

LogPoint hilft, die SOX Compliance einzuhalten und ermöglicht:

- Nachweis über durchgeführte Sicherheitsmaßnahmen mittels detaillierter, auditkonformer Dokumentation
- Überwachung und Schutz von Finanzdaten auf Record Level auch wenn diese in Applikationen verschoben wurden
- Zentrales Sammeln und Speichern von Audits über Finanzdaten- und Applikationen in Korrelation mit Netzwerk Security Devices.
- Schnelle Reaktion bei verdächtigen Ereignissen, wie z.B. unzulässige Datenveränderungen, gleichzeitiger Benachrichtigung von Verantwortlichen um Gegenmaßnahmen ergreifen zu können

PCI – "Payment Card Industry" Sicherheitsstandards

PCI Unternehmen, die über Service-Provider handeln und Kreditkarteninformationen speichern, weiterverarbeiten und übermitteln, müssen sehr viele gesetzliche Compliance-Vorgaben erfüllen. Würden diese nicht eingehalten, ware ein Geschäftsbetrieb heute nicht mehr denkbar. Bei Nichteinhaltung wären entsprechende Strafen die Folge.

Effektive PCI Implementation

Durch die Begrenzung von Budgets und Ressourcen wird die Implementation eines effektiven PCI Compliance-Programms zur wirklichen Herausforderung – dabei ist noch nicht die Rede von der Abwehr von Angriffen und vom Datenschutz. Unternehmen können diese Herausforderung jedoch in einen Vorteil für sich umwandeln, wenn sie statt einzelner Maßnahmen einen laufenden Prozess entwickeln, mit dem sie kontinuierlich Daten sammeln, überwachen, messen, darüber berichten und gleichzeitig alle Compliance-Vorgaben erfüllen.

Mit LogPoint kann die Compliance in PCI-Unternehmen einfach umgesetzt werden – und zwar einfacher und kostengünstiger als erwartet.

Nur Logs zu protokollieren reicht nicht

Die Überprüfung von PCI-Vorgaben und die Aktivierung geeigneter Kontrollmechanismen brauchen mehr als ein Log Management Tool. Im Gegensatz zu anderen Log-Managementlösungen, welche im wesentlichen nur Daten sammeln und Berichte über ungenaue Event-Logs ermöglichen, bietet LogPoint zusätzliche Intelligenz im Security-Umfeld durch eine vielschichtige Korrelationstechnologie.
So werden Event-Logs nicht nur gesammelt und gespeichert – es werden selbst ausgefeilte Bedrohungen erkannt und gestoppt. Treten Ereignisse ein, können Sie diese schnell mit den integrierten Werkzeugen, die sich übrigens nahtlos in Helpdesk-Systeme integrieren lassen, entgegenwirken.

LogPoint für PCI

LogPoint hilft Ihnen, selbst die strengsten PCI Compliance-Richtlinien und anspruchsvollsten Security-Vorgaben umzusetzen.
Mit weniger Zeit und Ressoursen Compliance-Vorgaben erfüllen:

- Überwachen und Messen der Effektivität der Kontrollmechanismen für die PCI Compliance
- Informationsbereitsstellung über Third-Party Auditors für Compliance-Tests
- Sicheres sammeln und speichern von Event-Logs als revisionskonforme Beweismittel
- Korrelation von Event-Daten aller Devices und Applikationen
- Sichtbarmachung aller Compliance-Verstöße in Echtzeit
- Sofortiges Erkennen und Alarmierung bei Abweichungen von Richtlinien oder Kontrollvorgaben
- Out-Of-The-Box, standardisierte PCI Berichte und Richtlinien

Schlußfolgerung

Die aufgezeigten Beispiele zeigen, dass es unmöglich ist, ohne eine Log Management-Technologie die PCI-Vorgaben zu erfüllen. Vollständige Log Daten sind die Voraussetzung für ein funktionierendes Security Management, für Zugriffskontrollen und weiterer sicherheitsrelevanter Bereiche. Ein gut geführtes Log Management ist der beste Schutz bei rechtlichen Auseinandersetzungen, weil im Falle einer gerichtlichen oder forensischen Untersuchung alle notwendigen Daten beweissicher und revisionskonform vorliegen.

LogPoint ist mehr als nur Log Management. Mit LogPoint können Sie immer nachweisen, dass Sie alle relevanten Prozesse Ihrer Compliance-Richtlinien implementiert haben und permanent überwachen – und gleichzeitig schützen Sie mit LogPoint zuverlässig alle sensiblen Daten und Informationen Ihres Unternehmens.

Weitere Informationen:

www.logpoint.com

logpoint

Corporate Headquarters

LogPoint A/S
Aldersrogade 6A
DK-2100 Copenhagen O
Denmark
Tel: +45 70 266 286
Fax : +45 70 266 287
E-mail: info@logpoint.com

LogPoint Deutschland
Bahnhofsplatz 3
D-56410 Montabaur
Deutschland

Tel: +49 (0) 2602 99739-0
www.logpoint.com

Weitere Informationen:

www.logpoint.com