Foto: Consist

Wir unterstützen Sie beim Aufbau einer schlanken und auditsicheren IT-Compliance-Organisation

Compliance 2.0: Effizientere IT-Compliance Audits durch Big-Data-Analyse

Die stetige Zunahme und Veränderung von internen und externen Compliance-Anforderungen bindet vermehrt wichtige Unternehmensressourcen. Die Vorbereitung und Durchführung von beispielsweise MaRisk, PCI DSS oder HIPAA Audits führt zu erhöhten Belastungen der verschiedensten Abteilungen. Consist bietet hier mit der Splunk-Plattform eine Möglichkeit, die neben der schnellen und effizienten Umsetzung der geforderten Änderungen gleichzeitig auch zahlreiche Chancen, Verknüpfungen und Synergien in anderen Bereichen aufzeigt.

Bei aller gebotenen wirtschaftlichen Betrachtung ist eines unstrittig: Bestehende gesetzliche und freiwillige Regulierungen haben zu erhöhter Transparenz und Sicherheit für Unternehmen, Verbraucher, Steuerzahler und weiterer Interessengruppen beigetragen. Dieser Vorteil lässt sich jedoch nur bedingt in der unternehmerischen Bilanz abbilden. Vielmehr ist die Einhaltung solcher Vorgaben eine Grundvoraussetzung, um überhaupt als Anbieter und Geschäftspartner am Markt teilhaben zu dürfen.

Da die Anforderungen an die Compliance absehbar sogar noch zunehmen dürften, gilt es, ein angemessenes Gleichgewicht zwischen Compliance-Konformität und dem notwendigen Aufwand hierfür herzustellen. Diese Gleichung wird für IT-Verantwortliche zusätzlich noch komplizierter, weil sie exponentiell wachsende Datenmengen aus vermehrt heterogenen Quellen integrieren müssen.

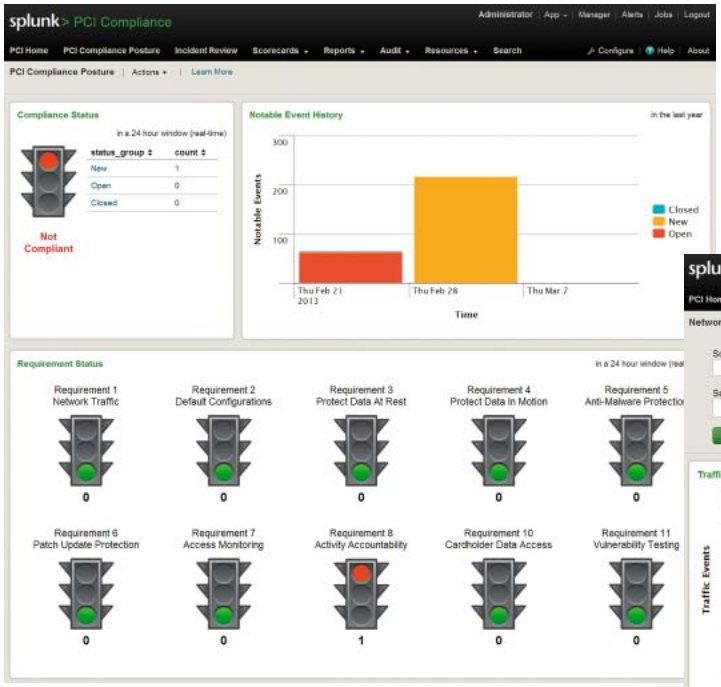
Kurzum: Die Erfüllung höherer Compliance-Anforderungen unter Berücksichtigung komplexer Massendaten muss IT-seitig dem Bedürfnis eines minimalen Ressourceneinsatzes entsprechen.

Das dies möglich ist, soll an den folgenden beispielhaften Szenarien verdeutlicht werden:

Szenario 1: Alle Banken müssen die neuen Mindestanforderungen an das Risikomanagement bis Ende 2013 erfüllen und umsetzen.

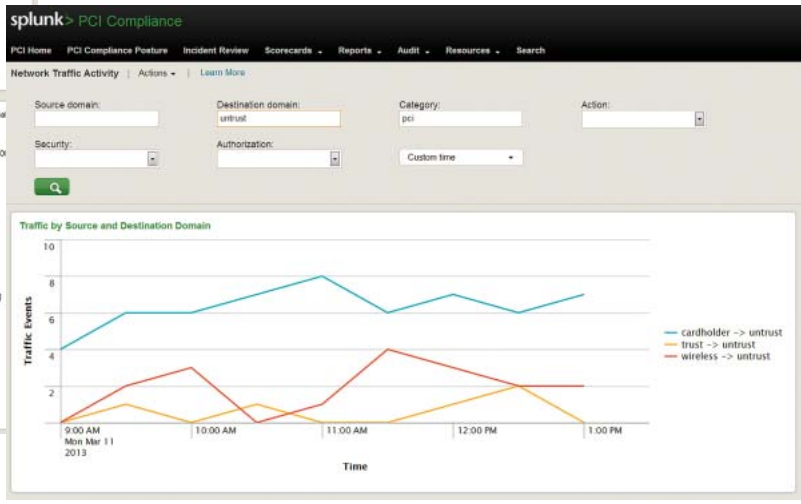
Beginnend im April 2012, aber spätestens mit dem Anschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht zur MaRisk-Endfassung im Dezember 2012, wurden die deutschen Kreditinstitute in Zugzwang gesetzt. Denn bis zum 31.12.2013 gilt es, neben den strukturellen u. a. die Anforderungen an die technisch organisatorische (IT-) Ausstattung (MaRisk AT 7.2) zu erfüllen.

Banken müssen nun also eine Compliance-Organisation etablieren, die neben der bereits existierenden Internen Revision, fachlich und technisch in der Lage ist, bei einer Überprüfung sämtliche



Fotos: Consist

Das Splunk-Dashboard zeigt permanent eine graphische Übersicht über die PCI Compliance. Die „rote Ampel“ weist auf die Störung hin.



Analyse der Störung von nicht vertrauenswürdigen Systemen, die mögliche Sicherheitslücken aufdeckt.

Compliance relevanten Bereiche abzubilden. In der Praxis bedeutet dies, dass beispielsweise permanent alle Log-Daten von Firewalls, Transaktionssystemen, File-, Web- und Mailservern untersucht werden müssen, um bei Auffälligkeiten ebenengerechte Handlungen anzustoßen. Dies ist bei der Komplexität und Vielfalt der heute notwendigen IT-Systeme kaum möglich. Klassische BI- oder DWH-Technologien sind dazu nicht in der Lage, da sie entweder zu langsam sind, Einschränkungen auf wenige Herstellerformate unterliegen oder schlicht nur vorher definierte Abweichungen entdecken können. Damit wird die Compliance und Security bezogene IT-Architektur sehr häufig ein Nebeneinander diverser Anwendungen hervorbringen, welche eine ganzheitliche geschweige denn Echtzeit-Analyse nicht ermöglicht.

Einige Banken haben diese Herausforderung jedoch frühzeitig erkannt und auf die Big-Data-Analyse-Lösung Splunk gesetzt. Getreu dem Motto: „splunk eats everything“ kann Splunk sämtliche strukturierten und unstrukturierten Daten der IT-Infrastruktur „sammeln” und ein Echtzeitbild der physischen und virtuellen Systeme wiedergeben. Im Ergebnis stehen dem Nutzer Dashboards und Reports zur Verfügung, aus welchen schiedensten Formaten in eine PCI-Lösung zu bekommen, ist eine Datennormalisierung nötig. Diese Aufgabe erfordert dauerhafte Wartung und kann aufgrund des stetig steigenden Datenvolumens zu einem Fulltime-Job werden.

Security und Compliance – ein Anwendungsfeld für die Datenanalyse mit Big-Data-Technologien.

er mit wenigen Klicks einen Drill Down in den jeweiligen Bereich durchführen kann. Damit ist auch in Echtzeit ersichtlich, welche Transaktionen unter Umgehung der jeweiligen Nutzerberechtigung veranlasst wurde oder welche Daten um 22.00 Uhr abends auf einen Datenträger kopiert wurden.

Szenario 2: Neue Anforderungen an die Verarbeitung von Kreditkartendaten.

Log-Management für PCI-Audits und die Umsetzung von Integritätskontrollen ist eine echte technische Herausforderung. Um die Vielzahl von Betriebs- und Sicherheits-Datentypen mit ver-

Dies ist besonders problematisch, wenn benutzerdefinierte Anwendungen in einer virtualisierten Infrastruktur ausgeführt werden.

Einer unserer Kunden nutzt bereits seit beinahe zwei Jahren Splunk sehr erfolgreich im Bereich Webanalyse, also zur Auswertung von Nutzerverhalten im E-Commerce Umfeld sowie der Erfolgsüberprüfung von Marketingaktionen.

Durch den Aufbau des neuen Geschäftsfeldes Mobile Payment, ist es jedoch notwendig auch Kreditkarteninformationen zu verarbeiten. Interne Audits haben bereits gezeigt, dass ein Ad-Hoc-

Nachweis der PCI DSS-Compliance nicht möglich ist. Der Kunde entschied sich daher, auch diesen Bereich mit Splunk zu bedienen. Durch Nutzung der Splunk App für PCI-Compliance 2.0 konnte diese Herausforderung mit einem Aufwand von zwei Personentagen gemeistert werden. Im Ergebnis hat der Verantwortliche des Geschäftsbereiches nun ein Dashboard zur Verfügung, das ihm permanent eine graphische Übersicht über seine PCI-Compliance bietet.

Fazit

Diese beiden Beispiele verdeutlichen zunächst, welches Einsparpotenzial die Big-Data-Analyse-Lösung Splunk bietet. Hierbei ist noch nicht berücksichtigt, welcher Schaden, hervorgerufen durch fehlende Compliance, abgewendet werden kann: Vertrauensverlust von Partnern und Kunden, milliardenschwere Sanktionen wie bei der UBS oder sogar der Entzug der Banklizenz.

Hinzu kommt aber auch, dass Consist und Splunk bereits mehrfach nachgewiesen haben, dass Security und Compliance nur ein Anwendungsfeld darstellt. Splunk wird mittlerweile bei mehr als 4.800 Kunden in über 90 Ländern auch in den Bereichen IT-Operations, Application Management und Business Intelligence eingesetzt. Dies alles ohne Data Warehouse oder vordefinierte Schemata sondern, wie Google, auf Basis von Suchtechnologie.

Nicht ohne Grund ist Splunk von Fast Company im Februar zum viert innovativsten Unternehmen der Welt 2013 gekürt worden und hat dabei in der Kategorie Big Data sogar Platz 1 erreicht.

30 Jahre IT-Erfahrung von Consist und der Technologievorsprung von Splunk ermöglichen selbst konzernweite Proof of Concepts innerhalb von 6-8 Tagen erfolgreich abschließen zu können. Wir freuen uns auf das Gespräch zu Ihren Big-Data-Themen.

Weitere Informationen:

E-Mail: info@consist.de
Web: www.consist.de

Im Fokus: **Big Data**

- Analysieren Sie Ihre Daten, die in den vielen verschiedenen Systemen und Formaten vorhanden sind!
- Verschaffen Sie sich Wettbewerbsvorteile, indem Sie mehr über Ihre Daten wissen und sie zu Ihrem Vorteil nutzen!

Big-Data-Technologien eröffnen neue Möglichkeiten der Ad-Hoc-Analyse sehr großer Datenmengen, nahezu in Echtzeit und quer über unterschiedlichste Datenformate.

Consist unterstützt Sie mit Beratung, Entwicklung konkreter Einsatzszenarien und in der Umsetzung. Unsere zertifizierten Berater setzen hierbei die Big-Data-Analyse-Lösung unseres Partners Splunk ein und verschaffen Ihnen damit einen echten Mehrwert.

splunk>

Foto: fotolia