Proaktives Compliance-Management

Ein rationeller Ansatz für Websicherheit und die Einhaltung gesetzlicher Vorschriften

Proaktives Compliance-Management

Einleitung: Wer immer hinterherhinkt, kann nicht proaktiv sein

Gesetze und Vorschriften aller Art werden immer strikter, zahlreicher und ihre Einhaltung entsprechend schwieriger. Laut einer Umfrage der IT Policy Compliance Group, die sich die Unterstützung von IT-Sicherheitsexperten bei der Einhaltung von Vorschriften und Richtlinien zum Ziel gesetzt hat, müssen 70 Prozent der Befragten die Vorschriften mehrerer Gesetzgeber, vertragliche Vereinbarungen und Branchenstandards einhalten.[1]

Gleichzeitig werden IT-Budgets gekürzt, da Unternehmen aufgrund der schwierigen Wirtschaftslage um Kostensenkung bemüht sind. Die Nutzung cloudbasierter Services erschwert das Compliance-Management zusätzlich. Angesichts dieser Probleme und chronischen Zeitmangels sind in vielen Unternehmen mehrere, nicht aufeinander abgestimmte Checklisten für die Einhaltung der verschiedenen Vorschriften im Einsatz.

Dieser taktische, reaktive Ansatz kann nicht nur unnötige Kosten verursachen, sondern auch zu Unzulänglichkeiten bei der Überprüfung, häufigeren bzw. längeren Ausfallzeiten und einem erhöhten Risiko von Datenverlusten führen. Um den ständig strenger werdenden Vorschriften voraus sein, statt ihnen immer hinterherzuhinken, benötigen Unternehmen Lösungen zur Umsetzung eines proaktiven Ansatzes, der ständige Vorschriftsänderungen einplant, statt nur auf sie zu reagieren.

Die Einhaltung aktualisierter Vorschriften

Viele Unternehmen tun sich noch immer schwer mit der Einhaltung der zahlreichen Vorschriften, die im Laufe der vergangenen zehn bis fünfzehn Jahre in Kraft getreten sind. Das Bundesdatenschutzgesetz, die europäische Datenschutzrichtlinie 1995/46/EG, der Sarbanes-Oxley-Act (SOX) für in den USA notierte Aktiengesellschaften und der „Payment Card Industry Data Security Standard“ (PCI) für Unternehmen, die Zahlungen per Kreditkarte akzeptieren, sind nur einige der scheinbar endlosen Vorschriften, die Unternehmen einhalten müssen. Inzwischen wurden und werden viele dieser Vorschriften aktualisiert und dabei teilweise erheblich verschärft bzw. geändert, wie in Tabelle 1 zu sehen ist. Infolgedessen wird Sicherheitsexperten in Unternehmen zunehmend bewusst, dass ein isolierter, auf Checklisten beruhender Ansatz für die Sicherheit und Einhaltung von Vorschriften nicht flexibel genug ist, um mit dieser Entwicklung Schritt zu halten.

Tabelle 1: Beispiele aktualisierter Vorschriften und ihrer Auswirkungen auf die IT-Sicherheit und -Compliance

Vorschrift	Jahr	Anforderungen bzw. Auswirkungen
BASEL II	2009	Banken müssen Verschlüsselungstechnik einsetzen, um das Risiko der Preisgabe bzw. Änderung vertraulicher Daten bei der Speicherung oder Übertragung zu mindern.
FISMA 2.0	2010	Alle US-amerikanischen Behörden müssen die lückenlose Überwachung ihrer Informationssysteme in ihr IT-Sicherheitsprogramm aufnehmen. Die CIOs der Behörden müssen vor Ablauf des Steuerjahres 2012 Software für die ununterbrochene Überwachung der Netzwerksicherheit implementieren.
PCI DSS 2.0	2011	Dieser neue Standard für die Sicherheitssoftware für Zahlungen per Kreditkarte ist seit Anfang 2011 verfügbar und seit Anfang 2012 verpflichtend vorgeschrieben.
HITECH Act	2011	Einrichtungen des Gesundheitswesens, Versicherungen, Verrechnungsstellen und ihre Geschäftspartner müssen bis Ende 2015 die verfügbare Technik für elektronische Patientenakten „sinnvoll nutzen“. Im Fall einer Sicherheitsverletzung müssen Unternehmen alle betroffenen Personen innerhalb von 60 Tagen benachrichtigen. Nur „nicht entzifferbare“ (d. h. durch starke Verschlüsselung geschützte) Daten sind von dieser Regelung ausgenommen.

1. Symantec: „Financial Information Security and IT Risk Management“, 2008, http://eval.symantec.com/mktginfo/enterprise/brochures/b-brochure_financial_services_10_2008_14163207.en-us.pdf

Fragmentierte Gesetzgebung: wenn die Internetsicherheit wild um sich greift

Im Jahr 2003 wurde in Kalifornien das Gesetz SB1386 über die Meldepflicht für IT-Sicherheitsverletzungen verabschiedet. In rascher Folge führten auch andere US-Bundesstaaten ähnliche Regelungen ein und heute hat nahezu jeder Bundesstaat ein Äquivalent zu dem kalifornischen Gesetz SB1386. In Massachusetts sind beispielsweise Unternehmen und Personen, die persönliche Daten speichern bzw. nutzen, gesetzlich dazu verpflichtet, einen Plan zum Schutz dieser Daten schriftlich auszuarbeiten und regelmäßig zu überarbeiten.[2] Diese fragmentierte Gesetzgebung erschwert Unternehmen, die in mehreren Bundesstaaten tätig sind, die Einhaltung gesetzlicher Auflagen.

Die Richtlinie 1995/46/EG[3] des Europäischen Parlaments zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist ein weiteres Beispiel für eine Regelung, die unterschiedliche Gesetze nach sich zog. Die Richtlinie diente als Grundlage für die Ausarbeitung nationaler Gesetze über die Datensicherheit und den Datenschutz in allen EU-Mitgliedsländern.

Zur Einhaltung dieser Gesetze müssen Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen, um die unautorisierte und rechtswidrige Verarbeitung, den Verlust bzw. die Zerstörung persönlicher Daten zu verhindern. Diese Datenschutz- und Datensicherheitsgesetze verbieten auch die Übertragung persönlicher Daten in ein Land oder Gebiet außerhalb des Europäischen Wirtschaftsraums, in dem die Rechte und Freiheiten von Personen hinsichtlich der Verarbeitung persönlicher Daten nicht ausreichend geschützt sind.

Mehrere Staaten weltweit haben Datenschutz- und Datensicherheitsgesetze verabschiedet, um ihren Bürgern den Zugang zu europäischen Märkten zu erleichtern. Da viele dieser Gesetze sich an dem von der EU-Richtlinie 1995/46/EG vorgegebenen Rahmen orientieren, ist diese zum internationalen De-facto-Standard für den Schutz persönlicher Daten geworden. Fast alle diese Gesetze schreiben die Nutzung technischer Hilfsmittel wie beispielsweise der Verschlüsselung zum Schutz persönlicher Daten vor Diebstahl, Verlust und unautorisierter Preisgabe vor.

Tabelle 2: Beispiele für Gesetze für Datenschutz und -sicherheit weltweit

Land	Gesetz	Jahr
Argentinien	Gesetz zum Schutz persönlicher Daten	2000
Chile	Gesetz zum Schutz des Privatlebens	1999
Hongkong	Verordnung zum Schutz persönlicher Daten[4]	1996
Japan	Gesetz zum Schutz persönlicher Daten	2003
Taiwan	Gesetz zum Schutz persönlicher Daten bei der computergestützten Verarbeitung	1995
Singapur	Grundlage für den Datenschutz[5] (Gesetzesvorlage)	2012
Südafrika	Gesetz über elektronische Kommunikation und Transaktionen[6]	2002
Südkorea	Gesetz zur Förderung der Nutzung von Informations- und Kommunikationsnetzen und der Informationssicherheit[7]	2002
Indien	Regeln für die Informationstechnik (angemessene Sicherheitsmaßnahmen und -verfahren zum Schutz vertraulicher persönlicher Daten und Informationen)[8]	2011

2. Commonwealth of Massachusetts, „201 CMR 17.00 Compliance Checklist“, Dezember 2009, http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf
3. Europäische Union, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, November 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML
4. G&A Management Consultants Limited, „Privacy of Personal Data in Hong Kong“, http://privacy.com.hk/
5. ZDNet Asia, „S'pore sets data protection law for 2012“, 16. Februar 2011, http://www.zdnet.com/spore-sets-data-protection-law-for-2012-2062206733/
6. Parlament der Republik Südafrika, „Electronic Communications and Transactions Act, 2002“, 31. Juli 2002, http://www.internet.org.za/ect_act.html
7. United Nations Public Administration Network, „Act on Promotion of Information and Communication Network Utilization and Information Protection“, 31.Dezember 2001, http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN025694.pdf
8. BNA International Global Law Watch, „Analysis: Data Privacy in India“, 23. Mai 2011, http://www.globallawwatch.com/2011/05/analysis-data-privacy-rules-in-india/

Compliance + Cloud-Computing = Komplexität[9]

Für viele CIOs hat Cloud-Computing oberste Priorität.[10] Immer mehr Unternehmen nutzen cloudbasierte Services; Schätzungen von Gartner Research zufolge werden Unternehmen weltweit in den nächsten fünf Jahren insgesamt 112 Milliarden US-Dollar für Cloud-Dienste ausgeben.[11]

Gleichzeitig ergab eine IDC-Umfrage unter IT-Verantwortlichen, dass Cloud-Dienste vor allem mit Sicherheitsbedenken zu kämpfen haben.[12] Gartner Research nennt sieben Bereiche, in denen Unternehmen beim Einsatz von Cloud-Computing mit Sicherheitsrisiken[13] rechnen müssen. Tabelle 3 führt einige Punkte auf, die vor dem Einsatz cloudbasierter Services in einem Unternehmen geklärt werden sollten.

Tabelle 3: Die sieben von Gartner genannten Sicherheitsrisiken beim Einsatz von Cloud-Computing in Unternehmen

Bereich	Problem
Verantwortlichkeit	Unternehmen sind auch dann für die Sicherheit und den Schutz vertraulicher Daten verantwortlich, wenn diese Daten von einem externen Cloud-Anbieter gehostet werden.
Zugriffskontrolle	Unternehmen müssen nachprüfen können, dass ihr Cloud-Anbieter bei der Auswahl seiner Mitarbeiter, der Aufsicht und der Durchsetzung von Zugriffsbeschränkungen die gebotene Sorgfalt walten lässt.
Speicherort der Daten	Viele SaaS-Anbieter nutzen cloudbasierte Speicherlösungen von Drittanbietern wie Amazon, Rackspace usw. Einige Anbieter nutzen auch Rechenzentren außerhalb des Europäischen Wirtschaftsraums. IT-Verantwortliche in Unternehmen sollten Service-Anbieter fragen, wo ihre Rechenzentren sich befinden und ob sie die Erfüllung der relevanten Datenschutzanforderungen garantieren können.
Mehrinstanzenfähigkeit	Da viele öffentliche Clouds von mehreren Kunden gemeinsam genutzt werden, muss der Hosting-Anbieter hundertprozentig garantieren können, dass die Daten und der Netzwerkverkehr der verschiedenen Kunden voneinander getrennt bleiben.
Datenwiederherstellung	Ausfallzeiten in Cloud-Computing-Umgebung können nicht absolut ausgeschlossen werden. Deshalb muss gewährleistet sein, dass der Service-Anbieter alle Daten und Services im Notfall schnell wiederherstellen kann.
Überwachung und Berichte	Die Überwachung und Protokollierung der Vorgänge in einer öffentlichen Cloud ist kompliziert. IT-Verantwortliche in Unternehmen sollten sich von vornherein davon überzeugen, dass ihr Cloud-Anbieter sowohl physischen als auch virtuellen Netzwerkverkehr überwachen, Untersuchungen unterstützen und die für Compliance-Prüfungen nötigen Unterlagen bereitstellen kann.
Datenverfügbarkeit	Manche, häufig neu gegründete, Technologieunternehmen müssen Insolvenz anmelden. Die finanzielle Stabilität möglicher Anbieter und die Portabilität der dort gespeicherten Daten müssen daher eingehend geprüft werden. Ziel ist es, weiterhin auf die eigenen Daten zugreifen und diese auch auf anderen Plattformen nutzen zu können, falls der Anbieter vom Markt verschwindet oder übernommen wird.

9. Commonwealth of Massachusetts, „201 CMR 17.00 Compliance Checklist“, Dezember 2009, http://www.mass.gov/ocabr/docs/idtheft/compliance-checklist.pdf

10. Gartner Research, „EXP Worldwide Survey“, 19. Januar 2010, http://www.gartner.com/it/page.jsp?id=1283413

11. Gartner Research, „Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010“, 22.Juni 2010, http://www.gartner.com/it/page.jsp?id=1283413

12. IDC Research, „New IDC IT Cloud Services Survey: Top Benefits and Challenges“, 15. Dezember 2009, http://blogs.idc.com/ie/?p=730

13. Gartner Research, „Assessing the Security Risks of Cloud Computing“, 3. Juni 2008, http://www.gartner.com/DisplayDocument?id=685308

Darüber hinaus ist zu beachten, dass alle diese Fragen mit jedem einzelnen Anbieter geklärt werden müssen, wenn ein Unternehmen nicht mehr nur einen Cloud-Dienst, sondern mehrere Dienste von verschiedenen Anbietern nutzt. Vermutlich hat jeder Anbieter seine eigene Infrastruktur, seine eigenen Richtlinien und sein eigenes Sicherheitsprofil. Die Kombination derart komplexer Anforderungen an die Vertrauenswürdigkeit mit ebenfalls immer komplexeren gesetzlichen Vorschriften macht ein überall verfügbares und äußerst zuverlässiges Verfahren erforderlich, das die Sicherheit der Daten beim Verschieben in die Cloud, innerhalb der Cloud und aus der Cloud gewährleistet.

Die Notwendigkeit eines rationellen Ansatzes für Sicherheit und Compliance

SSL- und Code Signing-Zertifikate sichern Transaktionen und Daten online durch Authentifizierung, Verschlüsselung und Überprüfung. Aufgrund immer neuer und strengerer gesetzlicher Vorschriften ist die Nachfrage nach Verschlüsselung und Authentifizierung drastisch gestiegen.

Infolgedessen wird die Zertifikatsverwaltung problematisch, da immer mehr Zertifikate benötigt werden und diese im Unternehmen verteilt sind. Die Komplexität kann auch durch Personalwechsel in der IT-Abteilung steigen, wenn dabei die Kontrolle und der Überblick darüber verloren gehen, welche technischen Kontaktpersonen und sonstigen Mitarbeiter Zugriff auf die Zertifikate haben.

Gleichzeitig muss der IT-Betrieb vielerorts mit einem gekürzten Budget auskommen und dennoch für die Einhaltung der internen und externen Sicherheitsvorschriften sorgen. In Tabelle 4 sind einige der spezifischen Probleme, die bei der Verwaltung zahlreicher SSL- und Code Signing-Zertifikate durch eine IT-Abteilung entstehen, zusammengefasst.

Tabelle 4: Probleme bei der Verwaltung von SSL- und Code Signing-Zertifikaten

Bereich	Problem
Überblick und Kontrolle	In großen, räumlich verteilten Netzwerken mit unterschiedlichen Betriebspraktiken fällt es Administratoren schwer, unternehmensweit den Status aller Zertifikate im Auge zu behalten und den Lebenszyklus digitaler Zertifikate effizient zu verwalten. Viele Anbieter stellen kein zentrales Repository zur Verfolgung und Verwaltung ihrer Zertifikate bereit. Die manuelle Erledigung dieser Aufgaben mithilfe von Kalkulationstabellen oder SharePoint ist nicht skalierbar und führt leicht zu Unstimmigkeiten und Mehraufwand.
geschäftliche Verfügbarkeit	Das unbemerkte Ablaufen von Zertifikaten kann zu Betriebsstörungen und zahlreichen Anrufen beim Kundendienst führen. Es kann sogar zu Ausfällen der Online-Systeme von Unternehmen und damit zu erheblichen Umsatzeinbußen kommen. Wenn über einen längeren Zeitraum kein gültiges Zertifikat vorhanden ist, sind eventuell Bußgelder zu zahlen und der gute Ruf des Unternehmens wird geschädigt.
IT-Betrieb	Die manuelle Verwaltung aller SSL- und Code Signing-Zertifikate eines Unternehmens ist umständlich und zeitraubend. Viele IT-Administratoren betreuen heterogene IT-Umgebungen mit verschiedenen Anwendungen und Betriebssystemen, deren Lebenszyklen mit spezifischen Verfahren verwaltet werden müssen. In solchen Fällen ist es oft schwierig, gleichzeitig die Speicherorte und Ablaufdaten aller Zertifikate im Auge zu behalten, insbesondere, wenn Zertifikate von verschiedenen Zertifizierungsstellen verwendet werden.

Deshalb suchen viele IT-Verantwortliche nach Lösungen zur Vereinfachung der Prozesse, Steigerung der betrieblichen Effizienz und Risikominderung.

Proaktive Compliance

Unternehmen, die den immer strengeren Gesetzen und Vorschriften mit einem proaktiven Sicherheitsansatz für ihre Internetpräsenz voraus sein wollen, benötigen eine Lösung der Enterprise-Klasse, mit der sie alle SSL- und Code Signing-Zertifikate über eine einzige sichere Plattform verwalten können. Der folgende Abschnitt ist als Hilfestellung bei der Auswahl der für Ihr Unternehmen am besten geeigneten Lösung gedacht. Darin werden einige wichtige Funktionen beschrieben, die eine solche Lösung unbedingt bieten sollte.

Automatische Durchsuchung

Die manuelle Durchsuchung von Netzwerken ist zwar theoretisch möglich, würde in großen, komplexen Unternehmensumgebungen jedoch zu viel Zeit und Personal in Anspruch nehmen. Wählen Sie deshalb einen Service aus, mit dem Ihr IT-Team Ihr Netzwerk automatisch nach Zertifikaten des jeweiligen Anbieters durchsuchen lassen kann.

Automatisierte Prozesse

Die manuelle Ausstellung, Erneuerung und Installation von SSL- und Code Signing-Zertifikaten ist in Großunternehmen nicht praktikabel. Sie benötigen eine produktivitätssteigernde Lösung, die wichtige administrative Prozesse wie die Genehmigung von Zertifikatsanforderungen und die Weiterleitung dieser Anforderungen an den richtigen Administrator automatisiert und damit den Zeit- und Arbeitsaufwand minimiert.

Warnmeldungen, Berichte und Protokolle

Ein abgelaufenes Zertifikat ist ein Sicherheitsrisiko für Ihre Daten. Deshalb sollten Sie sich für einen Service entscheiden, der Sie über Zertifikate benachrichtigt, die in Kürze erneuert werden müssen. Diese Lösung sollte auch administrative Maßnahmen für ein proaktives Risikomanagement unterstützen.

Flexibilität und Skalierbarkeit

Unternehmensnetzwerke sind dynamische, sich ständig verändernde Umgebungen. Ein Service zur Zertifikatsuche sollte deshalb konfigurierbare Parameter haben, beispielsweise für die maximale Dauer der Suche, die zu durchsuchenden IP-Adressen usw. Der Service sollte darüber hinaus skalierbar sein, um mit zukünftigem Unternehmenswachstum Schritt halten zu können.

Übertragung von Administrationsaufgaben

In einem Großunternehmen sind die Übertragung von Administrationsaufgaben und die damit verbundene Vergabe von Zugriffsrechten unverzichtbar. Wenn Sie mit Ihrem Konto mehrere Geschäftsbereiche bzw. Abteilungen verwalten, benötigen Sie eine Lösung, mit der Sie die angemessenen Rollen für verschiedene Administratoren auswählen können.

Fazit

SSL- und Code Signing-Zertifikate sind für den Erhalt der Sicherheit und die Einhaltung gesetzlicher Vorschriften unverzichtbar. Aufgrund der steigenden Komplexität der Gesetzeslage hat die Anzahl der Zertifikate stark zugenommen. Dadurch sind Services erforderlich, die die unternehmensweite Auffindung und Verwaltung von Zertifikaten vereinfachen.

Ein Thawte Certificate Center Enterprise Account ist hervorragend für mittelständische und große Unternehmen mit vielfältigen Sicherheits- und Compliance-Anforderungen geeignet. Er ermöglicht die automatische Zertifikatsuche und die Einrichtung automatischer Warnmeldungen an Administratoren, wenn Zertifikate ablaufen oder gewartet werden müssen.

Weitere Informationen darüber, wie Sie die Gewährleistung der Sicherheit mit einem Thawte Certificate Center Enterprise Account vereinfachen und gleichzeitig einen umfassenden, proaktiven Ansatz für die Einhaltung verschiedenster Vorschriften umsetzen können, finden Sie unter http://www.thawte.de/ssl/volume-discount-ssl-certificates/index.html

Falls Sie weitere Fragen haben, wenden Sie sich an einen unserer Verkaufsberater:

- **Telefonisch**
  - **USA: +1 888 484 2983**
  - **Großbritannien: +44 203 450 5486**
  - **Südafrika: +27 21 819 2800**
  - **Deutschland: +49 69 3807 89081**
  - **Frankreich: +33 1 57 32 42 68**
- **Per E-Mail an Enterprisesales@thawte.com**
- **Besuchen Sie unsere Website: http://www.thawte.de/ssl/volume-discount-ssl-certificates/index.html**

Mit den renommierten digitalen Zertifikaten des führenden internationalen Online-Sicherheitsexperten Thawte schützen Sie Ihr Unternehmen und bauen so bei Ihren Kunden Vertrauen auf. Seit 17 Jahren bietet Thawte seinen Kunden Stabilität, Zuverlässigkeit, eine bewährte Infrastruktur und erstklassigen Kunden-Support. Deshalb entscheiden sich Kunden weltweit für Thawte als ihren internationalen Sicherheitspartner.

UID 191/2/13