

Compliance dank IT-Security

Gerhard Beeker (CA Deutschland GmbH)

CA schafft mit einer integrierten Software-Suite für das Management der IT-Security wichtige Voraussetzungen dafür, dass Unternehmen die verschärften regulativen Vorschriften einhalten können. Diese "Compliance" ist nicht nur zwingend notwendig – sie lohnt sich auch.

Sicherheit ist eine Grundvoraussetzung für funktionierendes Web-Business, denn anders ließe sich das notwendige Vertrauen zwischen Kunden, Händlern und Herstellern im anonymen Internet gar nicht herstellen. Dabei geht es nicht nur um den strikt kontrollierten Umgang mit sensiblen Anwendungen und Daten, sondern vor allem auch um die wirksame Kontrolle der Identitäten aller handelnden Personen und Organisationen, die im Internet miteinander kommunizieren. Schlagworte wie Phishing oder Identitätsdiebstahl deuten an, welche Problematik dahinter steckt.

Daneben sorgen Finanzskandale, alarmierende Erkenntnisse etwa zu BSE oder Gammelfleisch für Schlagzeilen. Sie haben den Staat, Verbraucherschutz-Organisationen und Wirtschaftsverbände auf den Plan gerufen. Entstanden sind in der Folge eine ganze Reihe neuer Gesetze und verschärfter Vorschriften, die es für die Unternehmen nachweislich einzuhalten gilt. Compliance ist gefragt - mit gravierenden Konsequenzen für den IT-Betrieb.

Die Voraussetzung für IT-Sicherheit und Compliance schaffen integrierte Software-Lösungen, wie sie CA im Rahmen eines Enterprise IT-Managements (EITM) anbietet und weiter entwickelt. Zu ihren Kernelementen zählen eine Integrationsplattform mit Workflow-Engine, Management-Datenbank (MDB), gemeinsamen Richtlinien sowie einheitlicher Benutzerschnittstelle. Auf einer solchen Basis können dann Informationen über Infrastruktur, Prozesse und Mitarbeiter sowie darauf aufsetzende Prozesse zur Unterstützung der Unternehmensziele vereint und vereinfacht werden.

Über diese Integrationsplattform stehen den verantwortlichen Personen alle notwendigen Informationen zur Verfügung. Damit lassen sich die verschiedenen Richtlinientypen überwachen (und falls nötig automatisch Korrekturmaßnahmen einleiten) und die eingeleiteten Korrekturen lassen sich nach verfolgen. Der Effekt: Die kontinuierliche Einhaltung von Regierungs- und Behördenauflagen wird gewährleistet.

Die Netzwerk-, System- und Sicherheitsmanagement-Lösungen, die sich einer solchen Integrationsplattform bedienen, erlauben eine einheitliche Sicht auf alle Aspekte der Infrastruktur und die Zusammenhänge zwischen

IT und den Geschäftsaktivitäten. Aufgrund des einheitlichen Datenformats lassen sich die anfallenden Informationen sach- und fachgerecht zusammenfassen, verdichten und für das „Command Center“ (Steuerpult) eines CIO oder Sicherheitsbeauftragten grafisch aufbereiten. So lässt sich auf einen Blick erkennen, wie es um den aktuellen Compliance-Status steht oder wo Sicherheitsrisiken für die IT lauern.

Für die Compliance eines Unternehmens spielt das **Identity and Access-Management (IAM)** eine zentrale Rolle. Ein Unternehmen muss ja in jedem Fall detailliert nachweisen können, wer wann was in einem Geschäftsprozess gemacht hat. Dazu müssen die Geschäftsprozesse nicht nur lückenlos dokumentiert werden, sondern zusätzlich haben interne Kontrollen auch dafür zu sorgen, dass alle Prozesse transparent und verantwortet ablaufen.

CA unterstützt deshalb beim Identity and Access Management (IAM) ganz gezielt die Einhaltung regulativer Vorgaben, zum Beispiel durch den neuen CA Identity Manager. Er zentralisiert Web-Zugangskontrollen, unternehmensweites Single Sign-on (SSO), Identitätsadministration, User Provisioning, Nutzerverzeichnisse, Identity Federation und Web Services Security. Die gesamte Bandbreite der heterogenen IT-Ressourcen eines Unternehmens wird abgedeckt – darunter Mainframe, Internet, dezentralisierte und mobile Infrastrukturen.

Insbesondere das Management von Nutzeridentitäten – vom Web bis zum Mainframe – kann der CA Identity Manager organisieren. Er vereinheitlicht und vereinfacht die Verwaltung interner und – im Rahmen von Supply Chain- und Customer Relationship Management zunehmend wichtig – auch externer Nutzer und deren Rechte, indem er identitätsbezogene Management-Prozesse über den gesamten "Lebenszyklus" der Nutzer hinweg automatisiert – von ihrem Eintritt als Mitarbeiter ins Unternehmen über sämtliche Beförderungen und Versetzungen bis hin zu ihrer Pensionierung.

Regelmäßige Kontrolle der Nutzerrechte

Müheless kann der Administrator beispielsweise festlegen, dass Nutzerrechte regelmäßig bestätigt werden müssen. So wird sichergestellt, dass Nutzeridentitäten und Zugangsrechte mit den Unternehmensrichtlinien übereinstimmen. Darunter fallen zum Beispiel Zugriffsrechte für sensible Daten wie Gehaltsabrechnungen, die jedes Quartal erneut aktiviert werden müssen, oder auch Zugangsberechtigungen zu weniger kritischen Systemen, die nur einmal jährlich zu aktivieren sind.

Mit eTrust SiteMinder geht CA noch einen Schritt weiter und bietet eine Lösung für das sogenannte Web Access Management, mit der Unternehmen ihren Nutzern einen nahtlosen Zugang zu Web-

Applikationen gewähren können - und zwar sowohl innerhalb eines Unternehmens als auch über Unternehmensgrenzen hinweg. Das ist besonders wichtig bei Applikationen, die Unternehmen gemeinsam mit externen Geschäftspartnern, Lieferanten und Kunden nutzen.

Trotz steigender Nutzerzahlen, sich ausdehnender IT-Infrastrukturen und komplexer werdenden Applikationsportfolios lassen sich auf diese Weise mit gezielter Software-Unterstützung IT-Sicherheit und Datenschutz gewährleisten, ohne dass die Kosten ausufern. Und für das sonst häufig aufwendige Compliance Reporting lässt sich quasi out-of-the-box durch umfassende und einfach anpassbare Reports dokumentieren, dass die Identitätskontrollen etabliert sind – und auch wie vorgesehen arbeiten.