

Sicherheit als Schlüsselfaktor für Compliance

Rechtens und sicher

Von Frank Sommerfeld, Geschäftsführer von Equant in Deutschland

Neue Gesetze wie Sarbanes Oxley, IAS, Basel II oder auch die Grundsätze zum Datenzugriff und Prüfbarkeit digitaler Unterlagen (GDPdU) zwingen Unternehmen, ihr Informationsmanagement und die Informationsverarbeitung drastisch zu verändern - vielleicht für immer. Archivierung und Retrieval von Dokumenten, das Security-Management und die Einhaltung der entsprechenden Gesetze (Compliance) machen das Betreiben komplexer IT-Systeme noch schwieriger.

Hierzu hat Equant im dritten Quartal dieses Jahres eine Studie unter CIOs in 860 Unternehmen in Deutschland, Skandinavien, der Schweiz, Großbritannien, Italien, Belgien und im osteuropäischen Raum durchgeführt, um mehr über die Sicherheitslage und gesetzliche Regelungen in großen multinationalen Firmen zu erfahren. Für einen sehr großen Prozentsatz (44 Prozent) gehört Compliance Management und Auditing sowie Security Incident-Reporting beziehungsweise -Handling bereits zum Unternehmensalltag. Die Sicherheits-Akkreditierung findet in Europa nur bei neun Prozent der Befragten Beachtung - bei zwei Dritteln steht dieses Thema gar nicht auf der Agenda. Regulatory Compliance-Programmen zur Umsetzung von Sarbanes-Oxley oder European Privacy-Richtlinien wird mittelmäßige Aufmerksamkeit zuteil: 44 Prozent arbeiten an diesen Programmen - 31 Prozent kümmern sich darum noch gar nicht.

Was ist Compliance eigentlich genau?

Unter Compliance versteht man die Einhaltung aller internationaler oder nationaler Gesetze und Vorschriften wie beispielsweise Sarbanes-Oxley Act, Basel II oder OMB Circular A-123. Für Unternehmen wird es zunehmend wichtiger, diese Aufgaben zu erfüllen – sonst drohen Wettbewerbsnachteile oder schlimmstenfalls signifikante Strafen. Proaktive, umfassende und konsequente Compliance-Maßnahmen können zu Effizienzsteigerungen und Kostensenkungen beitragen.

Zentraler Bestandteil vieler Richtlinien ist die langfristige Aufbewahrung und rasche Bereitstellung von Unternehmensdaten beziehungsweise -dokumenten.

Wer die damit verbundenen Kosten in den Griff bekommen will, sollte sich mit einer mehrstufigen Speicherarchitektur und „artgerechten“ Datenhaltung befassen. Das bedeutet, dass sich Daten problemlos in andere Prozesse einbinden lassen, damit Arbeitsabläufe unterstützt werden können, in denen einzelne Informationsabläufe nahtlos verzahnt sind. Langzeitarchivierung muss - auch im Hinblick auf physikalische, elektronische und hybride Speicherung - angemessen und wirtschaftlich vertretbar sein. Manipulationen und Veränderungen der archivierungsrelevanten Daten nach deren Erstellung müssen ausgeschlossen oder zumindest dokumentiert und reziprok abzuwickeln sein. Durch eine Rückwärtsabwicklung aller Vorgänge muss der ursprüngliche Zustand jedes einzelnen Datensatzes und der Dokumente zu rekonstruieren sein. Dies bezieht sich auf strukturierte und unstrukturierte Daten sowie auf die zugehörigen Metadaten. Bei rechtskritischen Daten sollte gewährleistet sein, dass sicherheitstechnische Maßnahmen, wie etwa digitale Signatur oder Authentifizierungs-Stempel, einbezogen werden. Netzwerksicherheit ist dabei ein wichtiger Schlüsselfaktor: Das Netzwerk bildet das Rückgrat für die Aufbewahrung und den Austausch von Unternehmensinformationen und darf nicht zur potenziellen Fehler- oder Gefahrenquelle werden.

Angesichts der Bemühungen um die viel diskutierten Sicherheitsrichtlinien kommen Investitionen in die Informationssicherheit vergleichsweise noch zu kurz. Davon geht das Information Security Forum (ISF) aus. Demnach rechnen viele ISF-Mitglieder damit, gut zehn Millionen Dollar für die Einrichtung der gemäß Sarbanes-Oxley (SOX) vorgeschriebenen IT-Security-Kontrollen ausgeben zu müssen. Für die Informationssicherheit wesentliche Aspekte wie Business Continuity und Disaster Recovery würden von SOX allerdings so gut wie ignoriert, warnt das ISF. Wichtig sei daher, Compliance in eine umfassendere IT-Sicherheits- und Corporate-Governance-Strategie einzubetten. Es bestehe zudem die Gefahr, dass Richtlinien die ganze Aufmerksamkeit auf sich ziehen und von dringlicheren Sicherheitsbedrohungen ablenken. Es dürfe nicht dazu führen, dass Organisationen einen Compliance-anstelle eines Risiko-orientierten Ansatzes verfolgen, der letztendlich die Informationssicherheit aufs Spiel setzt.

Ein sicheres Unternehmensnetzwerk ist das A und O einer jeden Sicherheitsstrategie. Ein zentralisierter Ansatz im Bezug auf die Netzwerksicherheit garantiert eine umfassendere Kontrolle, reduziert die Risiken und verbessert die Netzwerktransparenz und somit die Sicherheit. Hier müssen Sicherheitslösungen greifen, die auf ein komplexes Netzwerk mit einer

Vielzahl von Applikationen zugeschnitten sind. Die Anforderungen vervielfachen sich mit der Anzahl der Standorte. Das Sicherheitsrisiko steigt mit neuen Anwendungen wie Web Services oder sonstigen mobilen Applikationen. Experten sind sich einig, dass sich ein Unternehmen nur mit einer ganzheitlichen IT-Security-Lösung, die mit gesetzlichen Vorschriften Hand in Hand geht, absichern kann.

Das sichere Unternehmensnetzwerk

Das Hauptproblem unternehmerischer Netzwerke startet mit der eigentlichen Implementierung. Das heißt, ist das Netzwerk schlecht implementiert, kann es nachher auch nicht einwandfrei und sicher funktionieren. Auch die Firewall reicht alleine nicht aus, um absolute Sicherheit zu gewährleisten. Zusätzliches Problem: Ist die Firewall einmal installiert, bleibt sie oft jahrelang sich selbst überlassen, da in der Praxis regelmäßige Updates häufig unterbleiben. Zeitmangel und fehlendes Fachwissen bei Administratoren sorgen darüber hinaus für gefährliche Lücken. Doch selbst eine ständig gepflegte Firewall kann nur eine singuläre Komponente im Sicherheitsmanagement darstellen.

Intrusion Detection Systeme melden den Feind, bevor er Schaden anrichtet. Das Intrusion Detection System (IDS) analysiert den gesamten Datenverkehr und informiert den Netzwerkadministrator oder externen Dienstleister, falls Gefahr droht. Angriffe werden selbst in einem harmlos aussehenden Datenstrom erkannt, weil das IDS automatisch Audit- und Logfiles analysiert und mit Angriffssignaturen bereits durchgeführter Attacken vergleicht. Durch die Anbindung des IDS an die proaktive Alarmzentrale eines Dienstleisters erreicht man selbst bei weltweiten Netzwerken eine 24x7-Überwachung.

Von besonderer Bedeutung zur umfassenden Sicherung des Unternehmensnetzwerkes sind Verschlüsselungs- und Authentisierungsverfahren. Wichtige Daten sollten nur verschlüsselt übertragen und archiviert werden. Zur zuverlässigen Codierung werden zwei weit verbreitete Techniken verwendet: die symmetrische, bei der zum Ver- und Entschlüsseln der gleiche Schlüssel verwendet wird und die asymmetrische Verschlüsselung, die im Gegensatz dazu zwei verschiedene Schlüssel, einen öffentlichen und einen privaten, nutzt.

Neben der Verschlüsselung der übertragenen Daten bietet eine gesicherte Identifikation und Authentisierung wesentlichen Schutz vor dem Missbrauch von Unternehmenssystemen. Dies lässt sich beispielsweise durch Challenge-Response-Verfahren oder durch den Einsatz von Einmalpasswörtern erreichen,

bei denen die sensiblen Informationen nur ein einziges Mal benutzt werden, so dass ein Mitlesen für Hacker uninteressant wird. Außerdem gehören Produkte zum Schutz vor Computerviren zur Grundausrüstung eines Unternehmens mit Internetzugang. Content-Security-Komponenten geben zusätzliche Sicherheit, dass durch E-Mails oder den Webseiten-Besuch keine gefährlichen Inhalte wie Java Applets oder ActiveX eingeschleppt werden. Schließlich ist Vorsicht beim Thema Updates geboten: Wer seine Software nicht immer auf dem aktuellsten Stand hält, ist potenziell anfällig für Angriffe über Sicherheitslücken, die Hersteller mit ihren neuen Updates schließen.

Die menschliche Firewall

Aber bei all den technischen Vorkehrungen darf das Unternehmen eines nicht vergessen: Die Sicherheit eines Unternehmens steht und fällt mit der Sicherheits- und Aufklärungspolitik. Technik und Gefahrenbewusstsein müssen Hand in Hand gehen. Laut der Equant-Umfrage sind sich fast zwei Drittel der Befragten (61 Prozent) dessen bewusst und haben bereits eine unternehmensweite Sicherheitspolitik eingeführt. Lediglich vier Prozent haben bis jetzt noch nicht darüber nachgedacht. 34 bis 38 Prozent führen regelmäßige Security Awareness-Trainings oder IT Risk Management-Programme durch. Die meisten Unternehmen setzen jedoch beim Thema IT-Sicherheit immer noch zuviel Vertrauen in die Technik und vernachlässigen dabei die Kommunikation mit ihren Mitarbeitern. Aufgeklärte Mitarbeiter sind der sicherste Unternehmensschutz.

Sicherheit outgesourct

Um das Thema Sicherheit in den Griff zu bekommen, kann ein Unternehmen intern ein eigenes Security-Team aufbauen und die entsprechenden Produkte für eine Security-Infrastruktur einkaufen oder die Sicherheitsmaßnahmen in die Hände eines externen Experten geben. Letzteres hat vor allem für große Unternehmen zahlreiche überzeugende Vorteile. Unternehmen müssen sich nicht um die Umsetzung gesetzlicher Vorschriften und um den technischen Stand der eigenen Security-Ausrüstung kümmern – ein professioneller Anbieter sorgt dafür, dass alles stets auf dem neuesten Stand ist.

Positiver Zukunftstrend

Nach den Ergebnissen der Equant-Umfrage findet das Thema Sicherheit in Unternehmen mehr und mehr Gehör. Immerhin 87 Prozent der Entscheider in multinationalen Unternehmen wollen im nächsten Jahr mehr Geld für Security-Projekte ausgeben. Damit lässt sich die Grundlage für sicheres



Informationsmanagement und Informationsverarbeitung gemäß Compliance-Anforderungen legen.

Zeichen: 9.602