COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/warum-it-compliance-so-schwer-faellt,2504551

Die Bedenken der Anwender

Warum IT-Compliance so schwer fällt

Datum: 08.02.2012
Autor(en): Matthias Zacher (IDC)

Unternehmen belassen es bei IT-Sicherheit oft mit Teilumsetzungen. Dafür gibt es zwar gute Gründe. Doch werden sie damit Compliance-Anforderungen nicht gerecht, schreibt Matthias Zacher von IDC in seiner Kolumne.

Foto:

Die Abwehr von Angriffen auf die IT und Daten sowie der Schutz und die Beseitigung von Schwachstellen gestalten sich zunehmend komplexer und aufwendiger. Eine bisher geschlossene, nach außen abgeschottete Unternehmens-IT mit festen Ein- und Ausgängen wird abgelöst von losen Gebilden mit einer Vielzahl von Zugriffspunkten, temporären Beziehungen und oftmals unbekannten Akteuren. Die Grenzen zwischen der eigenen IT und den Systemen und Services Dritter werden immer undeutlicher.

Aktuell sind die meisten Unternehmen jedoch in Produktions- und Lieferketten eingebunden und der Datenaustausch innerhalb solcher Gebilde findet zwischen vernetzten Informations- und Kommunikationssystemen statt. Es liegt daher auf der Hand, dass solch ein Gesamtsystem nur so sicher ist wie das schwächste Glied innerhalb der Kette.

Welche gesetzlichen Anforderungen es gibt

Matthias Zacher ist Senior Consultant bei IDC in Frankfurt. Foto: IDC

Seit mehr als zehn Jahren unterliegen IT-Verantwortliche einem mehr oder minder starken Regulierungsdruck. Von allen Seiten werden Unternehmen mit neuen Gesetzen, Standards und Richtlinien penetriert. Beispielsweise von der EU-Kommission, der Bundesregierung oder unterschiedlichen Industriekonsortien. Zu den Gesetzen und Richtlinien, die für IT-Verantwortliche in Deutschland relevant sind, zählen das Bundesdatenschutzgesetz, die EU Direktive 136, die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (**GDPdU**[1]) oder das Telekommunikations- und Telemediengesetz.

Hingegen haben folgende Regularien einen eher breiten und generellen Ansatz. Sie zeigen auf Basis von Best Practice und erprobten Katalogen sichere Wege und Abläufe für die Implementierung und die Nutzung von Informationstechnologie auf:

Bestehende Best Practice Regularien

- Payment Card Industry Data Security Standard (PCI DSS)
- Information Technology Infrastructure Library (ITIL)
- Control Objectives for Information and Related Technology (Cobit)
- International Organization for Standardization (ISO) 2700x
- Statement on Auditing Standards (SAS) 70
- IT-Grundschutz

Die Sicht auf Compliance deutscher IT-Verantwortlicher unterscheidet sich nur marginal von der Betrachtungsweise in anderen europäischen Staaten. Wie eine Umfrage von IDC im Sommer 2011 gezeigt hat, ist für knapp 60 Prozent der dort befragten Unternehmen das Thema Compliance "Außerordentlich wichtig" oder "Sehr wichtig". Damit bewegen sich deutsche Unternehmen im Durchschnitt hinsichtlich der Bewertung des Themas.

Der Regulierungsdruck auf einzelne Branchen ist unterschiedlich groß. Zu den Industrien in Deutschland, die besonders stark reguliert sind, zählen derzeit die Telekommunikationsbranche, Financial Services und das Gesundheitswesen. Insbesondere für Financial Services sind aufgrund der sich häufig ändernden internationalen und nationalen Gesetzeslage weitere Anpassungen der IT an die Regelungen zu erwarten. Ein Schwerpunkt liegt nach wie vor in der Risiko-Analyse.

Die Unternehmen sind heute nicht mehr in der Lage, gesetzliche Anforderungen ohne Unterstützung von Informationstechnologie umzusetzen. Das betrifft die Übermittlung, den Nachweis und die Speicherung von Daten einschließlich solcher Aspekte wie Nachvollziehbarkeit, Identität und Zugriffsmanagement oder Zweckbindung.

Compliance wird nur dann in hohem Maße erreicht, wenn in Unternehmen die vorhandenen Frameworks oder Kataloge vollständig implementiert oder umgesetzt werden. Hier zeigen sich häufig noch deutliche Lücken. Nach Einschätzung von **IDC**[2] ergibt sich aber ein zweischneidiges Bild: Viele Unternehmen neigen dazu, mit Teilumsetzungen, beispielsweise bei IT-Grundschutz, IFS oder PCI-DSS zu starten. Sie beginnen in der Regel mit aus ihrer Sicht leicht zu erfüllenden Anforderungen. Dadurch wird aber nur ein Basis-Schutz erreicht, der jedoch hohen Schutzanforderungen nicht genügt.

Viele Unternehmen tun sich schwer, weitere Kriterien, die meistens anspruchsvoller sind, zu erfüllen; entweder weil sie einen Basis-Schutz als ausreichend erachten, ihnen die benötigten Fachkräfte fehlen oder sie schlichtweg kein Budget bereitstellen können.

Allerdings gibt es noch einen weiteren Aspekt, der aus unserer Sicht als kritisch anzusehen ist: Nationale Gesetzgeber setzen EU-Recht häufig zögerlich in nationales Recht um. Somit sind Unternehmen gezwungen, mit der Implementierung in ihre Lösungen zu warten. Mitunter hat dies knappe Projekt-Timelines oder offene Teilprojekte zur Folge.

Compliance ist grundsätzlich ein sich erneuernder und wiederholender Prozess, der in bestimmten zeitlichen Abständen Evaluationen, Upgrades von Policies oder die Einführung neuer bzw. aktualisierter Lösungskomponenten erfordert. Viele Anwender verzichten bewusst auf vollständige Implementierungen, insbesondere dann, wenn diese regelmäßig offizielle Audits und Prüfungen nach sich ziehen. Insbesondere kleinere Unternehmen beschreiten den Weg zu einer umfassenden Implementierung von Regularien und Richtlinien eher in kleinen Schritten.

Fazit

Aus Sicht von IDC müssen Unternehmen Compliance und IT Sicherheit zunehmend unter einem gesamtheitlichen Ansatz betrachten. Nur dann ist die IT-Abteilung in der Lage, die Businessanforderungen sicher zu unterstützen. Bei der Umsetzung von Regularien dürfen deutsche Unternehmen nicht auf halbem Wege stehen bleiben. Sie müssen zudem beachten, dass Compliance ein kontinuierlicher Prozess mit einer Vielzahl von organisatorischen, prozessualen und technologischen Aspekten ist.

Matthias Zacher ist Senior Consultant bei IDC in Frankfurt.

Der Beitrag erschien zuerst bei unserer **Schwesterpublikation CIO**[3].

Links im Artikel:

[1] **https://www.cio.de/schwerpunkt/g/GDPdU.html**
[2] **https://www.cio.de/schwerpunkt/i/IDC.html**
[3] **https://www.cio.de/strategien/methoden/2293391/**