

Sind Sie sicher ?



Ein Gesetz macht die IT-Sicherheit zur Pflicht für das management

Von **Franz-Josef Lang, F.-J. Lang IT-Security Consulting GmbH, München**

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) erzwingt präventive Maßnahmen zur Risikoerkennung. Informationssysteme und Daten müssen in ein Schutzstufenkonzept integriert werden, damit Probleme vorhersehbar werden und Kunden wie Aktionäre keine bösen Überraschungen erleben.

Spektakuläre Unternehmenskrisen führten dem Gesetzgeber vor Augen, daß es um die Kontrollmechanismen und die Risikovorsorge nicht ausreichend bestellt war. Um künftig vor allem die Anleger vor solchen Überraschungen zu schützen, wurde das KonTraG verabschiedet, das am 1. Mai 1998 in Kraft trat. Als Artikelgesetz, das bestehende Gesetze beeinflusst, führte es zu Anpassungen unter anderem im Aktiengesetz (AktG), im Handelsgesetzbuch (HGB) und im Recht der gesetzlichen Abschlußprüfung.

Die Stärkung des Aufsichtsrats, eine höhere Transparenz der Geschäftsabläufe und verbesserte Kontrollmöglichkeiten der Hauptversammlung standen im Mittelpunkt der Reform. Neu geregelt wurde zudem die Zusammenarbeit zwischen Abschlußprüfer und Aufsichtsrat.

Sicherheit als Managementaufgabe

Indem die Vorstände börsennotierter Aktiengesellschaften verpflichtet werden, ein Kontrollsystem zur Früherkennung von Risiken zu etablieren, kommt auf die IT-Abteilungen Arbeit zu. Ein Überwachungsprozeß muß eingerichtet werden, damit sich Entwicklungen, die den Fortbestand der Gesellschaft gefährden können, rechtzeitig erkennen lassen. Risiko-Management, bislang primär im Versicherungs- und Bankenumfeld ein Thema, erstreckt sich nun auf das gesamte Unternehmen: von der Produktion über Kunden- und Lieferantenverhältnisse, externe Marktgegebenheiten und politische Entwicklungen bis hin zur IT.

Damit wird Informationstechnik mehr denn je zur Vorstandssache. Die Geschäftsführung muß sich mit Risiken, Sicherheitsproblemen und Disaster-Management beschäftigen. Auch die interne Revision, die als Kontrollinstanz durch das KonTraG noch mehr Verantwortung erhält, hat ihren Fokus auf die Sicherheit wichtiger Informationen zu richten. Neben den vorhandenen Anwendungen und Datenbanken für die Bewältigung der täglichen Geschäftsabläufe wird auch das vom Gesetzgeber geforderte Überwachungssystem IT-basiert sein.

Die möglichen Gefahren sind vielfältig. Hacker können die Handlungsfähigkeit des Unternehmens durch Manipulation, Weitergabe von Daten oder Zerstörung einschränken - etwa indem sie Kundendaten löschen oder an die Konkurrenz verkaufen. Wie groß diese Gefahr ist, zeigte sich jüngst bei einem erfolgreichen Hackerangriff auf die Datenbestände des FBI.

Denkbar ist aber auch, daß Kriminelle unbemerkt auf wichtige Insider-Informationen zugreifen und über Aktiengeschäfte daraus finanzielle Vorteile ziehen. Verschafft sich ein Eindringling - oder auch ein interner, aber nicht befugter Mitarbeiter - Zugang zum internen Kontrollsystem, liegen die gesamten kritischen Bereiche des Unternehmens ungeschützt vor ihm.

KonTraG und Basel II zwingt zur IT-Risikoanalyse

Die IT muß deshalb auch im Sinne von KonTraG einer genauen Analyse unterzogen werden. Soll das Restrisiko gering gehalten werden, sind Schutzkonzepte zu implementieren, die eine ausführliche Analyse und Bewertung der Daten, der Security-Leitlinien sowie der Kommunikations- und Sicherungsstrukturen voraussetzen.

Um das Risiko einschätzen zu können, müssen die Daten daraufhin untersucht und bewertet werden, inwieweit ein Verlust oder eine Manipulation den Geschäftsverlauf und den Aktienkurs beeinflussen könnte. Diese Bewertung ist im Regelfall komplex. Neben sofort ersichtlichen und bezifferbaren Schäden, etwa für die Wiederherstellung der Daten, gibt es auch Nachteile, die erst auf den zweiten Blick als Risiko einzustufen sind. Dazu gehört beispielsweise ein schlechterer Geschäftsverlauf, weil das Image Schaden genommen hat.

Einer Bank, bei der Hacker in den Kundenkonten gestöbert oder falsche Transaktionen ausgelöst haben, werden einige Kunden ihr Vertrauen entziehen - auch wenn kein tatsächlicher Schaden entstanden sein sollte. Neue Kunden werden sich schwieriger gewinnen lassen.

Mit einer Risikobewertung ist erst der Grundstein für das Risiko-Management-System gelegt, unabhängig davon, ob es sich um IT oder um betriebliche Risiken in den Bereichen Entwicklung, Produktivität oder Produkthaftung

handelt. Sind die wunden Punkte definiert, ermittelt die Schutzbedarfsanalyse das tatsächliche Gefährdungspotential.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit seinem IT-Grundschutzhandbuch ein Standardwerk für die IT-Sicherheit geschaffen, das ein im Hinblick auf das KonTraG akribisches und umfassendes Vorgehen ermöglicht. Nicht nur die DV-technischen Sicherheitsanforderungen, sondern auch die organisatorischen und gebäudetechnischen Komponenten werden berücksichtigt.

Neben den Schutzmechanismen wie Authentifizierung, Identitätsprüfung oder Firewall weist das Werk auf Standorte, Schutzschranke, Infrastruktur oder Personal hin. Ein Gefährdungskatalog listet mögliche Beeinträchtigungen durch höhere Gewalt, organisatorische Mängel, menschliches und technisches Versagen oder Vorsatz auf. In allen Bereichen lassen sich Gegenmaßnahmen erfassen.

Vorgehensmodelle

Die Verpflichtung zu einem aktiven Risiko-Management (§ 91 Abs. 2 AktG) enthält keine konkreten Vorgaben für die praktische Umsetzung. Es obliegt dem Unternehmen, die maßgeblichen Kriterien zu definieren und Gefahrenpotentiale zu verringern. Das Kunststück liegt immer darin, das sinnvolle und wirtschaftlich richtige Maß zu finden. So bedeuten die Sicherheitsanforderungen, die sich aus der Risikoanalyse ergeben, nicht unbedingten Handlungsbedarf zur hundertprozentigen Absicherung.

Mit Kanonen auf Spatzen zu schießen ist nicht das Ziel des KonTraG. Vielmehr geht es darum, das Restrisiko auf ein vertretbares Maß zu reduzieren und die verbleibenden Gefahren durch geeignete Überwachungsmaßnahmen kalkulierbar zu machen und präventiv zu senken.

An die Datensicherheit werden drei Anforderungen gestellt: Vertraulichkeit, Integrität und Verfügbarkeit. Sie sind getrennt zu betrachten und in ihrer Auswirkung zu bewerten - dies führt zu einem wirtschaftlich vertretbaren Sicherheitskonzept. Die technische Umsetzung kann entsprechend variieren und prägt bei jedem Unternehmen eine individuelle Security-Infrastruktur aus, bestehend aus technischen und organisatorischen Schutzmaßnahmen.

Da jedes System bekanntlich nur durch die begleitende Organisation die gewünschte Schutzwirkung entfalten kann, geht der Implementierung von Hard- und Software die entsprechende Sicherheitspolitik voraus: Festzulegen sind Verantwortlichkeiten, Funktionstrennung, Behandlung sensibler Daten, Benutzerschulung, Passwort- und Key-Management, Datensicherungs- und Notfallkonzepte. Erst dann folgt die technische Umsetzung.

Firewalls allein reichen nicht aus

Firewalls als Barriere zwischen den Netzwerken sind hier nur ein Aspekt. Sie werden ergänzt durch Virens Scanner, Authentisierungsmechanismen zur eindeutigen Feststellung des Benutzers, Signaturen zur Identitätsprüfung sowie der Verschlüsselung, um die Vertraulichkeit der Inhalte zu gewährleisten. Auch Backup-Konzepte oder eine Versicherung der kritischen Restrisiken gehören dazu.

Ergänzend muß unternehmensintern ein Risikobewußtsein geschaffen werden. Das läßt sich nur durch gezielte Kommunikation erreichen, etwa um die Anwender für die Gefährdung durch Viren zu sensibilisieren. Kommunikationskonzepte sind deshalb auch Bestandteil einer Sicherheits-Policy.

Die Aufgabe des von KonTraG geforderten Frühwarnsystems können Intrusion-Detection-Lösungen übernehmen. Sie ermöglichen eine Echtzeitüberwachung der Netzaktivitäten und schützen so vor unliebsamen Überraschungen. In kritischen Bereichen empfiehlt sich das 24-Stunden-Monitoring einer Alarmzentrale. Ebenso muß die Auswertung der Log-Files organisiert werden. Es ist ratsam, eine Checkliste aufzustellen, die beteiligte Personen, Umfang der Auswertungen, Datenschutz etc. beinhaltet. Kontrolliert wird das Schutzkonzept auch durch die interne Revision, die die korrekte Umsetzung der Maßnahmen im Detail überprüfen muß.

Üblicherweise geschieht dies unter anderem durch Security-Audits: Netzwerke und Systeme werden durch vermeintliche Angriffe auf Vertraulichkeit, Integrität und Verfügbarkeit überprüft. Auch das elektronische Kontrollsystem muß sich dem unterziehen.

KonTraG ist damit in besonderer Hinsicht ein Security-Thema. Unbestritten fördert es einerseits den Sicherheitsaufwand im Unternehmen. Andererseits kanalisiert es auch unkoordinierte Vorkehrungen, wie sie in der Praxis bislang oft zu beobachten sind: Firewalls und Verschlüsselungslösungen werden ohne ein differenziertes Konzept eingeführt, Maßnahmen übertrieben und damit zu teuer eingesetzt oder umgekehrt: Es wird an der falschen Ecke gespart.

- Zu Klären:
- Fragestellungen für das IT-Risiko-Management

Für welche IT-Prozesse ist ein Risiko-Management zu implementieren?

Wurde der Ist-Zustand der IT-Security-Leitlinien überprüft? Existieren diese überhaupt so, wie sie von KonTraG gefordert werden?

Wie sind bestehende IT-Security-Prozesse integriert? Erfüllen sie die Anforderungen nach KonTraG?

Welche Sicherungsmaßnahmen wurden für geschäftskritische IT-Prozesse integriert?

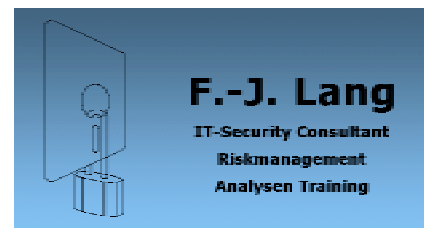
Sind Frühwarnsysteme, bezogen auf KonTraG und IT-Einsatz, installiert?

Informationen

BSI IT-Grundschutzhandbuch

Kostenlose Checkliste für Logfile-Auswertung und Auditing bei info@fjlang.de oder www.fjlang.de

Das noch recht junge Gesetz KonTraG zwingt börsennotierte Aktiengesellschaften zur Risikovorsorge - um Unternehmenskrisen abzuwenden und zum Schutz der Anleger. Ein Risiko-Management-System ist Vorschrift für alle Bereiche, auch für die IT. Punktuelle und meist wenig sichere Schutzmechanismen reichen nicht mehr aus, sie müssen einem integrierten Konzept weichen. Datensicherheit wird zum Vorstandsthema.



**Erfahrung und Qualität bringen Sicherheit !
Partnerschaft für besseres Riskmanagement.**

**F.-J. Lang IT-Security Consulting GmbH
80689 München • Landsberger Str. 302
Tel. 089-904059-16 – Fax –17**