

# Sicherheitslücken schließen

## Managementsysteme für IT-Sicherheit



Im Oktober 2009 berichtete die Internetseite „netzpolitik.org“ über Sicherheitsprobleme bei „Libri“, einem Online-Marktplatz für Buchhändler. Bei den Libri-Konten vieler Händler war der Login-Name identisch mit dem Passwort. Als Login-Name wurde eine mehrstellige Zahl verwendet. Mitarbeitern von „netzpolitik.org“ gelang die Anmeldung bei einigen Konten der mehr als 1.000 Händler. Laut Bericht konnten sie sämtliche Daten der jeweiligen Online-Vertriebsgeschichte nachvollziehen. Zuvor war bekannt geworden, dass durch eine Lücke im System von „libri.de“ der unautorisierte Zugriff auf mehrere tausend Rechnungen von Kunden möglich war.

### Lagebericht zur IT-Sicherheit

Dieses Beispiel ist kein Einzelfall. Der „Lagebericht zur IT-Sicherheit in Deutschland 2009“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigt, dass die IT-Sicherheit bei Verwaltungen, Unternehmen und Privat anwendern erheblich bedroht ist. We-

sentlicher Grund: Die Internetkriminalität nimmt zu und wird immer professioneller. Schadprogramme werden immer ausgefeilter und effektiver, die Zahl der Angriffe auf die Systeme nimmt zu, Sicherheitslücken in Betriebssystemen und Anwendungen werden immer schneller ausgenutzt. Darüber hinaus entstehen durch die zunehmende Vernetzung und insbesondere die Anbindung an das Internet neue Bedrohungen.

Andererseits ist das Bewusstsein der Anwender für IT-Sicherheit gestiegen: Betriebssystem-Updates werden häufiger durchgeführt und IT-Sicherheitstechniken konsequent angewendet. Das Informationssicherheitsmanagement (IS-Management) gerät immer stärker in den Fokus der Unternehmensführung. IT-Systeme sind inzwischen nicht mehr Beiwerk, um bestimmte Arbeiten schneller zu erledigen, sondern sie bilden die Basisinfrastruktur der Geschäftsprozesse. Diese Integration in das operative Geschäft eines Unternehmens erfordert auch ein professionelles Handeln zur Absicherung und Aufrechterhaltung der IT-Dienste.

Mit einem IS-Management werden Unternehmen auch gesetzlichen und aufsichtsrechtlichen Anforderungen gerecht. Beispielhaft sei hier die Finanzbranche mit den Mindestanforderungen an das Risikomanagement genannt. Bei den Automobilzulieferern ersetzt eine Zertifizierung des IS-Managements die Sicherheitsüberprüfung durch die Abnehmer.

## IS-Management

Das BSI definiert IS-Management: „Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung [...] Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Diese Planungs-, Lenkungs- und Kontrollaufgabe wird [...] als IS-Management bezeichnet.“

Aus dieser Definition werden insbesondere drei Grundprinzipien deutlich. Erstens ist es das Ziel des IS-Managements, ein angemessenes Sicherheitsniveau zu erreichen und aufrechtzuerhalten. Insofern ist eine Risikoabschätzung erforderlich, mittels welcher die bestehenden Sicherheitsrisiken beurteilt werden können, und es sind angemessene Schutzmaßnahmen zu treffen. Unter wirtschaftlichen Rahmenbedingungen lassen sich nicht alle Risiken eliminieren. Es müssen Entscheidungen hinsichtlich der Risikoakzeptanz getroffen und von der Unternehmensführung verantwortet werden.

Zweitens handelt es sich beim IS-Management um einen allumfassenden Ansatz, der alle Beteiligten einschließt. Dabei ist insbesondere zu berücksichtigen, dass Informationssicherheit nicht alleine durch den Einsatz von Technik sichergestellt werden kann, sondern

auch der Faktor Mensch Berücksichtigung finden muss.

Drittens ist IS-Management eine Planungs- und Lenkungsaufgabe, die einem immerwährenden Prozess unterliegt und möglichst nah an die Unternehmensführung angebunden werden muss. Dieser Prozess beinhaltet die Bereiche „Planung“, „Umsetzung“, „Wartung“ und „Erfolgskontrolle“, sodass zu jedem Zeitpunkt ein angemessenes Sicherheitsniveau gewährleistet ist.

Zum Aufbau eines Managementsystems für Informationssicherheit (ISMS) ist zunächst eine Grundsatz- bzw. Zielbildung erforderlich. Dies erfolgt in der Regel mittels einer Sicherheitsleitlinie. Nach der Festlegung der grundsätzlichen Ziele erfolgt eine Planungsphase, in der Strategien und Pläne ausgearbeitet werden. Anschließend werden in einer Organisationsphase notwendige Aufgaben an verantwortliche Personen verteilt, damit wird die Umsetzung strukturiert. Abschließend erfolgt eine Kontrolle der umgesetzten Maßnahmen. Die beschriebenen Aufgaben sind naturgemäß Querschnittsaufgaben. Zwangsläufig auftretende Kompetenzüberschneidungen dürfen nicht zu isolierten Betrachtungen führen, welche die IT-Sicherheit gefährden.

Um das allgemeine Ziel sicherer Informationen zu erreichen, werden für das IS-Management Schutzziele definiert, die sich an den Grundwerten der Informationssicherheit (siehe Kasten) orientieren. Diese abstrakten Ziele werden durch die Anwendung von technischen oder organisatorischen Schutzmaßnahmen angestrebt. Dabei ist zu beachten, dass ein vollständiges Erreichen der Schutzziele in der Regel nicht durchgesetzt werden kann. Insofern sieht das IS-Management ein angemessenes Sicherheitsniveau vor.

Beim Aufbau eines ISMS kann man auf Spezialisten im genossenschaftlichen Verbund zurückgreifen. Diese unterstützen die Unternehmen von der Entwicklung über die Implementierung

## Grundwerte der Informationssicherheit nach BSI

1. Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
2. Verfügbarkeit: Dem Benutzer stehen die Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
3. Die Integrität ist gewährleistet, wenn es nicht möglich ist, Informationen unautorisiert und unbemerkt zu verändern.

## Weitere Grundwerte

- Authentizität: Die Überprüfung der Identität mittels charakteristischer Eigenschaften erlaubt es, die Echtheit und Glaubwürdigkeit eines Objekts festzustellen.
- Kann ein Nutzer im Nachhinein die Ausführung von Aktionen nicht abstreiten, gewährleistet ein System Verbindlichkeit.
- Die Einhaltung rechtlicher Erfordernisse (z. B. Schutz personenbezogener Daten entsprechend des BDSG) ist erforderlich.

bis hin zur Aufrechterhaltung des ISMS. Durch einfache Audits und Prüfungen entsprechend den IDW-Prüfungsstandards kann die Ordnungsmäßigkeit der IT nachgewiesen werden.

Der Nutzen eines wirkungsvollen ISMS zusammengefasst: Kunden und Lieferanten kann der verantwortungsvolle Umgang mit Informationen nachgewiesen werden. Die Aufwendungen der Risikovorsorge sind für alle Beteiligten transparent. Das Risikopotenzial wird reduziert und mit den verbleibenden Risiken wird bewusster umgegangen. Die Chancen werden erhöht, dass die Leistungserbringung trotz eines Schadensfalls fortgesetzt werden kann.

Ein Beitrag von  
**Paul Heitmann**