Presse-Info

IT-Risiken im Unternehmen aufspüren

Die umfassende Dokumentierung der IT-Sicherheit ist für Unternehmen von existenzieller Bedeutung. Immer neue Gesetze und Vorschriften sehen bei Zuwiderhandlung z.T. empfindliche Strafen vor. Ein neues, internationales IT-Grundschutz-Zertifikat ermöglicht nun erstmals eine umfassende und gleichzeitig praxisnahe Prüfung ...

Köln, 28. September 2006. Immer neue Gesetze und Vorschriften fordern von Unternehmen ein geeignetes IT-Risiko-Management. Sonst drohen z.T. schwerwiegende Konsequenzen. So sind die Geschäftsführer und Vorstände laut „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ („KonTraG“) verpflichtet, die Risiken in ihrem Unternehmen transparent zu machen und zu kontrollieren. Prinzipiell haften sie persönlich für eventuelle Folgen. Auch das auf dem amerikanischen Markt gültige „Gesetz zur Verbesserung der Unternehmensberichterstattung“, der „Sarbanes-Oxley-Act“ (SOX), droht der Geschäftsleitung mit harten Strafen.

Vorgaben von Basel II erfüllen

In Zukunft wird sogar für den Erhalt eines Kredites die nachgewiesene IT-Sicherheit entscheidend sein: Mit Inkraftsetzung der Eigenkapitalvorschriften nach Basel II im Januar 2007 hängt die Kreditvergabe von der Rating-Position eines Unternehmens ab – und diese wiederum auch von dessen IT-Sicherheits-Management. Wer hier seine Hausaufgaben nicht gemacht hat, dem droht eine schlechte Rating-Position und damit geringere Kredit-Chancen.

Um ein böses Erwachen zu vermeiden, sollten Unternehmen rechtzeitig vorsorgen. Wie aber kommt man den IT-Risiken im Unternehmen auf die Spur? Ein einfaches Werkzeug zur Risikoanalyse entwickelte das Bundesamt für Informationstechnik (BSI) Mitte der 90er Jahre: Das Grundschutzverfahren. Der Grundschutz bietet eine Reihe allgemeiner Schutzmaßnahmen, um die häufig auftretenden Risiken zu überprüfen und ggf. zu beseitigen. Mit Hilfe eines Fragenkatalogs wird u.a. kontrolliert, ob der Brandschutz rund um die IT-Anlagen ausreichend ist, ob regelmäßige Back-ups gemacht werden und ob die Mitarbeiter für den Umgang mit sensiblen Daten ausreichend geschult sind.

Gesamte IT mit einem Prüfverfahren

Wegen seiner Praxisnähe und leichten Handhabung wurde das Grundschutzverfahren und das damit verbundene Zertifikat für viele Unternehmen und Behörden schnell zu einem Standard in der IT-Sicherheit – allerdings nur für einen mittleren Schutzbedarf. Höhere Sicherheitsanforderungen, wie sie z. B. bei der Konfiguration eines Internet-Servers benötigt werden, konnten bisher nicht anhand des IT-Grundschutzes berücksichtigt werden. Zudem war das IT-Grundschutz-Zertifikat nicht international anerkannt. Für komplexere IT-Landschaften, wie sie heute in der Regel fast überall vorzufinden sind, und für international tätige Unternehmen waren daher weitere Prüfverfahren notwendig.

Seit Anfang 2006 ist das IT-Grundschutzverfahren nun auch für erhöhte Sicherheitsanforderungen geeignet und international anerkannt. Damit ist es jedem Unternehmen weltweit möglich, die gesamte IT mit einem einzigen Prüfverfahren zu kontrollieren – zum Schutz der eigenen Daten und zur Einhaltung von Gesetzen und Vorschriften.

Das BSI hat für diese so genannte „ISO-Zertifizierung auf Basis von IT-Grundschutz“ das Grundschutzverfahren mit der internationalen Norm ISO 27001 zusammengeführt. Die ISO-Norm war kurz zuvor aus dem britischen

INFODAS - Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestraße 2
50765 Köln
Telefon (0221) 70912-0
Fax (0221) 70912-55
info@save-infodas.de
www.save-infodas.de
infodas@infodas.de
www.infodas.de

Standard BS 7799-2 entwickelt worden und stellt einen Katalog von Anforderungen zur Verfügung, nach denen Unternehmen und Behörden das Management ihrer IT-Sicherheit aufbauen und kontrollieren können. Dabei geht die Norm mit ihren Forderungen zum IT-Sicherheitsmanagement über die Maßnahmen des Grundschutzes hinaus. Die Umsetzung der abstrakt formulierten Anforderungen erwies sich jedoch als schwierig bis unmöglich. Erst durch die Kombination mit dem Grundschutzverfahren wurde ISO 27001 für Unternehmen tatsächlich anwendbar. Ein Anwender hat es mit der Formulierung „Internationaler Standard gepaart mit deutscher Gründlichkeit“ treffend beschrieben.

IT-Sicherheitsdatenbank SAVe® vereinfacht Umsetzung

Der Umfang und die Komplexität der bei dem Prüfverfahren zu beachtenden Gefährdungen und Maßnahmen können allerdings – ebenso wie auch schon beim Grundschutzverfahren – enorm sein. Erleichtert wird die Untersuchung durch den Einsatz eines datenbankgestützten Werkzeuges. So ist die IT-Sicherheitsdatenbank SAVe® der Infodas GmbH eine der ersten Lösungen, die bereits für das neue Prüfverfahren ausgerichtet ist. SAVe® ist bereits seit Jahren bei der Überprüfung nach IT-Grundschutz im Einsatz und hat sich schon viele Male bewährt. Z.B. erleichtern grafische Auswertungen der erfassten Daten das Auffinden von Lücken bei der IT-Sicherheit. Die Konsistenzkontrollen sorgen für eine hohe Qualität der Daten und verringern dadurch die Notwendigkeit zu Nachbesserung beim Zertifizierungsaudit.

Ein solches Audit ist dann notwendig, wenn die überprüfte Sicherheit auch nach außen dokumentiert werden soll – z.B. für ein Rating. Hat das Unternehmen bereits alle Anforderungen nach Grundschutz erfüllt, ist ein Audit nur mit geringem Aufwand verbunden. Dies zeigte sich bei den ersten Zertifizierungen mit dem neuen Prüfverfahren. Untersuchungsobjekte waren die IT eines großen SAP Outsourcing Rechenzentrums und eines kommunalen Verkehrsträgers. Die Auditierung hatten Auditoren der Infodas GmbH ausgeführt, des führenden deutschen Spezialisten für IT Security Management. In den genannten Fällen konnten die Audits in jeweils drei bis vier Tagen vor Ort abgeschlossen werden. Die Audit-Berichte ließen sich durch Nutzung des Werkzeugs SAVe® innerhalb weniger Tage erstellen.

Wenn ein Unternehmen seine IT-Sicherheit mit dem neuen Zertifikat dokumentiert, beweist es, dass es ein Sicherheitsniveau erreicht hat, das dem aktuellen Stand der Technik entspricht, und dass damit ein funktionierendes IT-Risikomanagement vorhanden ist. Damit sind die Vorgaben von Basel II, Sarbanes-Oxley und KonTraG wirkungsvoll umgesetzt.

Über die INFODAS GmbH

INFODAS gehört zu den innovativen deutschen mittelständischen Systemhäusern für Sicherheitslösungen und Risikomanagement. INFODAS unterstützt eine ganzheitliche IT-Sicherheits-Beratung durch die IT-Sicherheitsdatenbank SAVe®. Die aktuelle Version SAVe® V4.0 basiert auf den BSI-Standards 100-1 bis 100-3, berücksichtigt die Anforderungen der ISO 27001 und unterstützt vollständig die ergänzende Risikoanalyse nach IT-Grundschutz. Grundlage der Maßnahmenempfehlungen sind die IT-Grundschutz-Kataloge Stand Dez. 2005.

Innerhalb der Business Unit IT Security konzipiert und auditiert INFODAS IT-Sicherheitsprozesse und IT-Sicherheitsorganisationen, entwickelt geeignete Notfallvorsorge-Programme, gestaltet und überprüft den Datenschutz innerhalb der Organisation und stellt externe Datenschutzbeauftragte zur Verfügung. Als Erweiterung der SAVe®-Software bietet INFODAS eine Verfahrenshilfe für die Umsetzung des Datenschutzes und der Datensicherheit in Unternehmen. Das auf der Sicherheitskonzeption aufbauende Risikomanagement und -controlling unterstützt bei der Umsetzung der Anforderungen des KonTraG und der Vorgaben von BASEL II.

Unter Leitung der beiden ISO 27001-Auditoren Gerhard Weck und Frank Reiländer konnte INFODAS die beiden ersten Zertifizierungen des neuen Verfahrens erfolgreich abschließen. Das erste Zertifikat wurde für einen kommunalen Verkehrsträger ausgestellt. Mit der SAP Systems Integration AG konnte eine der bisher größten Grundschutz-Zertifizierungen auf den ISO-Standard erweitert werden. INFODAS arbeitet langjährig erfolgreich mit dem BSI bei Anwendung und Fortschreibung des IT-Grundschutzes zusammen.

INFODAS GmbH
Gesellschaft für Systementwicklung und
Informationsverarbeitung mbH
IT Security
Rhonestraße 2
D-50765 Köln
Ansprechpartner: Frank Reiländer
Telefon: +49 (221) 7 09 12-85
E-Mail: security@infodas.de
Web www.save-infodas.de

Pressekontakt:

Eva Wagenbach
möller pr
Tel.: +49(221) 80 10 87- 88
Mobil +49(174) 980 1375
E-Mail: ew@moeller-pr.de