IT-Management

Datensicherheit gewährleisten

Zertifizierung nach ISO 27001

19. Oktober 2007

Verlässliches Sicherheitsmanagement entwickelt sich insbesondere für IT-Dienstleister zu einem wichtigen Vertriebsargument. Auch andere Branchen, die sensible Daten verwalten, müssen sich mit dem Thema auseinander setzen. Eine international anerkannte Möglichkeit, Kunden und Geschäftspartner von der Sicherheit der anvertrauten Daten zu überzeugen, ist ein nach der ISO-Norm 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS).

Die vier einzelnen Zyklen in einem ISMS: der Demingkreis.

Quelle: Easynet

Um ein Zertifikat nach der ISO-Norm 27001 zu erhalten, muss ein Unternehmen zunächst ein Informationssicherheits-Managementsystem einführen, das jederzeit die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen auf angemessenem Niveau sicherstellt. Als erstes werden die hierfür notwendigen Sicherheitsvorkehrungen ermittelt.

Im Falle der Vertraulichkeit sieht dies beispielsweise folgendermaßen aus: Zum Schutz der Informationen werden diese üblicherweise in vier Geheimhaltungsstufen unterschieden. Je nach Bedarf ist eine Information damit als öffentlich, intern, vertraulich oder streng geheim klassifiziert. Öffentlich verfügbare Informationen werden von einem zertifizierten Unternehmen anders gehandhabt als streng geheime Daten. Der Umgang mit diesen Informationen ist vom Unternehmen genau festgelegt und muss durch ISO 27001 definierte Voraussetzungen erfüllen. Jede Sicherheitsmaßnahme greift hier in die nächste. Das Sicherheitsniveau wird also durch das schwächste Glied der Kette bestimmt.

Vertraulichkeit im Netz und vor Ort

Um beispielsweise die höchstmögliche Vertraulichkeit sicherzustellen, müssen Rechenzentren, Systeme und Netze gleichermaßen gesichert sein: Die Daten werden dabei nur in hochwertiger Verschlüsselung über so genannte Virtual Private Networks (VPNs) übertragen. Firewalls schützen alle Rechner im Verbund vor unberechtigten Zugriffen. Standardanwendungen benötigen dafür regelmäßige Überprüfungen gegen alle bekannten Sicherheitslücken. Zudem unterliegt der physikalische Zugriff auf die IT strengen Auflagen, die sich etwa durch eine Zutrittskontrolle zum Gebäude durchsetzen lassen. Üblicherweise findet vor den eigentlichen Rechenzentrumsräumen eine weitere, noch intensivere Überprüfung statt.

Sofern nichts anderes vereinbart wurde, unterliegen sämtliche Kundenanforderungen den höchsten Vertraulichkeitsstufen. Verantwortung und Sensibilität aller Beteiligten sind Grundvoraussetzung, um diesen Anspruch zu erfüllen. Ein hohes Kompetenzniveau ist dafür unerlässlich. Die Mitarbeiter des Service-Providers Easynet beispielsweise werden deshalb kontinuierlich fachlich geschult und im sicheren Umgang mit den Informationswerten sensibilisiert.

Verfügbarkeit ist eine Frage der Systemstruktur

Die zweite Sicherheitsdimension neben der Vertraulichkeit ist die Verfügbarkeit der Daten. Sie wird in erster Linie durch eine leistungsfähige Netz- und Systemstruktur garantiert, die auch Belastungsspitzen problemlos verkraftet. Dazu kommen eine mehrfache Redundanz bei Servern und Leitungen sowie eine unabhängige Stromversorgung, die das Rechenzentrum bei Stromnetzstörungen in Betrieb hält. Auch Warnsysteme für Server und Gebäude, die Performance-Abfälle anzeigen und infrastrukturelle Notfälle wie Feuer oder eintretendes Wasser frühzeitig melden, tragen zu einer hohen Datenverfügbarkeit bei.

Informationsintegrität erfordert Absicherung

Die Informationsintegrität ist als dritte Komponente eines sicheren Informationsmanagements ebenso bedeutend wie Vertraulichkeit und Verfügbarkeit. Sie hängt in erster Linie von hochwertigen Datenspeichern und angemessenen Backup-Konzepten ab. Ein übliches Verfahren ist beispielsweise ein wöchentliches Full-Backup bei täglicher Aufzeichnung der Veränderungen. Für darüber hinausgehende Sicherheitsansprüche können kundenindividuelle Lösungen entwickelt werden.

Kontinuierliche Qualitätssicherung

Sind Vertraulichkeit, Verfügbarkeit und Integrität nach Stand der Technik etabliert, ist die Arbeit jedoch keineswegs abgeschlossen:

Sicherheitsmanagement erschöpft sich nicht in der einmaligen Installation von Schutzmaßnahmen, sondern ist einer kontinuierlichen Qualitätssicherung und -verbesserung verpflichtet. Dies gewährleistet der PDCA-Zyklus (Plan-Do-Check-Act) aus dem Qualitätsmanagement, auch unter dem Namen Deming-Kreis bekannt. Planung und Einführung der Sicherheitsmaßnahmen entsprechen den Phasen „Plan" und „Do". Darauf folgt die Überprüfung der eingeforderten Sicherheitsmaßnahmen, beispielsweise durch interne Audits oder Reviews. Während dieser Checks beginnt bereits die Erarbeitung von Verbesserungsmöglichkeiten, die in der anschließenden Act-Phase umgesetzt werden. Hierfür sind wieder Planung, Umsetzung, Überprüfung und Reaktion notwendig – ein neuer Zyklus beginnt. Der Deming-Kreis ist somit ein wesentlicher Bestandteil des ISMS. Seine Phasen sind in allen Bereichen des Sicherheitsmanagements erkennbar.

Wenn das ISMS nach ISO 27001 zertifiziert werden soll, müssen die im PDCA-Zyklus entdeckten Risiken mit normgerechten Sicherheitsmaßnahmen behoben werden. Diese werden in einer weiteren ISO-Norm beschrieben, der ISO 17799, die aber demnächst in die ISO 27002 übergeht. Sie enthält 134 Maßnahmen oder so genannte „Controls", denen die bisher eingeführten Sicherheitsaktivitäten zugeordnet werden. Deren Umsetzung und die Durchführung weiterer, selbst erstellter Maßnahmen weist das Unternehmen dann durch ein „Statement of Applicability" nach. Dieses hält fest, welche Risiken es mit welchen Controls angeht. Die Wirksamkeit der Maßnahmen ermittelt das Unternehmen in so genannten „Measurements of Effectiveness". Die Dokumentation dieser Measurements dient später als wichtige Informationsquelle für die Zertifizierung.

Der Zertifizierungsvorgang im Detail

Ist ein ISMS der beschriebenen Art erst einmal etabliert, kann das Unternehmen die Zertifizierung nach der ISO-Norm 27001 mit dem Titel „Information Security Management – Specification With Guidance for Use" beantragen. Dieses Zertifikat gilt international als Beleg, dass der Träger das ISMS kompetent umsetzt, und ist somit gerade für Service-Provider ein starkes Vertriebsargument gegenüber sicherheitssensiblen Kunden. In manchen Branchen ist ein zertifiziertes ISMS sogar Geschäftsgrundlage: Beispielsweise müssen die Krankenkassen ihre Eignung zum Schutz der Patientendaten erst mit einer Sicherheitszertifizierung belegen, bevor sie die elektronische Gesundheitskarte einführen dürfen.

Ohne Audit gibt es kein Zertifikat

Unabhängig davon, ob ein Zertifikat zwingend vorgeschrieben oder einfach erwünscht ist: Der Weg zum Sicherheitszeugnis führt über ein so genanntes Audit, in dem das Unternehmen seine IT bewerten lässt. Dazu senden beauftragte, akkreditierte Zertifizierungsstellen ihre Prüfer in das zu zertifizierende Unternehmen. Diese Auditoren überprüfen die Informationstechnologien, ihre Einbindung in die betriebswirtschaftlichen Vorgänge sowie die Einhaltung juristischer Anforderungen wie beispielsweise der jeweiligen Datenschutzvorschriften. Ebenso hoch sind die Anforderungen an die persönliche Integrität der Auditoren. Sie müssen beispielsweise strikte Vertraulichkeit wahren, da sie tiefen Einblick in die Unternehmensstruktur erhalten. Sorgfalt bei der Überprüfung wird vorausgesetzt. Zusätzlich sorgen sie

durch eindeutige Dokumentation dafür, dass ihre Ergebnisse jederzeit verifiziert werden können. Um die Unabhängigkeit und Objektivität des Auditors sicherzustellen, dürfen nur solche Dienstleister eingesetzt werden, die in den vergangenen Jahren nicht als Berater des Auftraggebers tätig waren.

Nach der Auswahl des Prüfers beginnt das Zertifizierungs-Audit. Dieses läuft üblicherweise in mehreren Phasen ab. Zunächst wird grundsätzlich nachgewiesen, dass ein Informationssicherheits-Managementsystem implementiert ist. Erstes und wichtigstes Dokument hierfür ist die Sicherheits-Policy des Unternehmens.

In ihr werden die Ziele und Grenzen des ISMS in Einklang mit den Geschäftszielen definiert. Wie diese Sicherheitsziele konkret umgesetzt werden, zeigt dann die Dokumentation. Sie bietet den Nachweis der Maßnahmen, ihrer Überwachung und Überprüfung sowie der Verbesserungen des Sicherheitssystems. Nach dem Review dieser Unterlagen wird im nächsten Schritt die Umsetzung der Maßnahmen überprüft.

Da die Anzahl der Maßnahmen für eine vollständige Kontrolle in der Regel zu groß ist, beschränkt man sich auf Stichproben. Ist das Audit zur Zufriedenheit des Prüfers abgeschlossen, empfiehlt er die Zertifizierung. Hat er Beanstandungen, so erhält das Unternehmen Gelegenheit für Nachbessererungen.

Ein Zertifikat nach ISO 27001 ist längstens drei Jahre gültig und wird jährlich durch sogenannte „Continuing Assessment Visits" überprüft. Sollte sich dabei herausstellen, dass das Informationssicherheits-Managementsystem nicht funktioniert, kann das Unternehmen seine Zertifizierung verlieren. Die Anforderungen eines Continuing Assessment Visits entsprechen denen eines herkömmlichen Zertifizierungs-Audits. Allerdings ist der Aufwand nicht ganz so groß.

Sicherheitsmanagement im Tagesgeschäft

Neben den eigenen Sicherheitsbeauftragten bauen viele Unternehmen dafür auf externe Fachleute, die die Abläufe unvoreingenommen begutachten. Dies können unabhängige Dienstleister sein, jedoch auch Mitarbeiter aus anderen Standorten. International tätige Unternehmen setzen hierfür auch Kollegen aus anderen Ländern ein. Da die ISO 27001 weltweit Gültigkeit besitzt, können diese die Abläufe qualifiziert beurteilen. Sie bringen oft auch einen neuen Blickwinkel ein und liefern wertvolle Anregungen. Zeigen sich Optimierungsmöglichkeiten, befasst sich das Management mit dem Anregungen und stellt die Ressourcen zur Umsetzung bereit.

Nationale und internationale Zertifikate

Obwohl alle Sicherheitskonzepte gleichermaßen auf Vertraulichkeit, Verfügbarkeit und Integrität abzielen, konkurrieren unterschiedliche Zertifikate. Die ISO 27001 hat sich beispielsweise aus einem britischen Sicherheitsstandard entwickelt.

Die Internationale Organisation für Normung (ISO) nahm diesen im Jahr 2000 als ISO 27001 und ISO 17799 in ihr Portfolio auf. Im Jahre 2005 schließlich wurden

beide noch einmal gründlich überarbeitet und bilden somit den Stand des heutigen Tages.

Inzwischen hat sich die Norm international als Standard durchgesetzt. Zurzeit sind weltweit annähernd 4000 Informationssicherheits-Managementsysteme nach ISO 27001 zertifiziert, 70 davon in Deutschland. Hier existiert allerdings neben der ISO 27001 noch ein weiteres relevantes Sicherheitssiegel: eine erweiterte ISO-27001-Zertifizierung nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die ISO- und BSI-Anerkennungen sind inhaltlich kompatibel, wobei das BSI auf dem Basisniveau striktere Vorgehensanweisungen gibt als die internationale Norm. Dagegen macht die ISO bei der Risikoermittlung keinen Unterschied und erfordert schon im Basisniveau eine detaillierte Risikoanalyse.

Mehr als Grundschutzniveau

Jenseits des Grundschutzniveaus entsprechen sich die beiden Sicherheitsgarantien. Dadurch haben die Unternehmen die Möglichkeit, sich für das Zertifikat zu entscheiden, das die Unternehmensphilosophie abbildet.

Dies hat auch für die Praxis Konsequenzen: Easynet als international agierender Service Provider entschied sich zum Beispiel für die weltweit gültige ISO 27001, um auch den Anforderungen ihrer internationalen Geschäftskunden gerecht zu werden.

Weiterführende Links

ISO 27001: http://de.wikipedia.org/wiki/ISO_27001

BSI-ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz: http://www.bsi.de/gshb/zert/ISO27001/ISO27001.htm

Vergleich ISO 27001 sowie ISO 17799 mit BSI-Grundschutz: http://www.bsi.de/gshb/deutsch/hilfmi/Vergleich_ISO17799_GS.pdf