

Presse-Information

25. März 2004

IT-Security: Vertrauen ist gut – Zertifizierung ist besser

Mit dem IT-Grundschutzzertifikat des BSI wird IT-Security zum wettbewerbswirksamen Gütesiegel / Günstigere Kredit-Konditionen und Versicherungsbeiträge / IT-Dienstleister SAP SI auf CeBIT mit BSI-Zertifikat ausgezeichnet

Köln, 25. März 2004. Kunden von Outsourcing-Dienstleistern müssen enormes Vertrauen aufbringen. Durch die weitgehende Übergabe von internen Daten an einen Dritten geht ihnen die eigene Kontrolle nahezu vollständig verloren. Der Outsourcer versichert zwar einen sorgfältigen und sicheren Umgang mit den Daten. Der Kunde weiß jedoch nicht, ob der Anbieter tatsächlich alles Notwendige tut, um den Verlust der ihm anvertrauten Kundendaten wirkungsvoll und nachhaltig zu verhindern. Er kann sich nicht sicher sein, ob die Mitarbeiter geschult sind im Umgang mit Sicherheitsvorkehrungen, ob Dateien vor den Händen Dritter sicher sind oder ob das Gebäude vor Einbruch geschützt ist. Vertrauen allein ist hier zu wenig.

„Vor allem Outsourcing-Dienstleister, aber auch andere Unternehmen, werden zunehmend von Kunden und Geschäftspartnern vertraglich verpflichtet, IT-Sicherheit zu garantieren – ohne dass hierzu klare Parameter definiert sind“, erklärt Detlef Krings, Leiter Consulting der INFODAS GmbH aus Köln, einem auf Sicherheitsberatung spezialisierten Systemhaus. Denn bestehende Prüfnormen greifen hier zu kurz. So umfasst die managementorientierte BS-7799-Methodik hauptsächlich die Etablierung der oberen Hierarchien im Unternehmen. Das Personal ist in vielen Fällen aber die größte Schwachstelle bei der IT-Sicherheit. „Nicht Viren oder Hacker sind das Hauptrisiko für die IT im Unternehmen“, so Krings. „Neben Feuer und Diebstahl stellen nicht hinreichend sensible bzw. ungeschulte Mitarbeiter das größte Risikopotential dar. Deshalb ist es eine Frage des wirtschaftlichen Überlebens, den Gebäudeschutz und die richtige Mitarbeiterschulung bei der Zertifizierung zu berücksichtigen.“ Ein Zertifikat, das es bisher nicht gab.

Günstige Kreditkonditionen und Versicherungsbeiträge

Um diese Lücke zu schließen, hat das „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) ein neues Qualifizierungs- und Zertifizierungsschema eingeführt – kurz: „IT-Grundschutz-Zertifikat“. Dabei wird der innerhalb einer Organisation erreichte Stand an IT-Sicherheit gemäß IT-Grundschutz transparent nach außen dargestellt. Die Überprüfung beinhaltet Organisation, Personal, IT und Infrastruktur und bezieht sich auf die drei Sicherheitsaspekte Verfügbarkeit, Vertraulichkeit und Integrität in einem ausgewählten IT-Verbund eines Unternehmens. Grundlage für das Prüfverfahren bilden die bereits bewährten und ständig aktualisierten Richtlinien des IT-Grundschutz-Handbuchs. „Das BSI-Grundschutz-Zertifikat berücksichtigt erstmals alle Faktoren, die für IT-Sicherheit relevant sind“, erklärt Krings. „So wird z.B. nicht nur überprüft, ob die Mitarbeiter richtig geschult werden, sondern auch, ob Räume und Türen genügend lange gegen Feuer und Rauch geschützt sind.“

Mit dem IT-Grundschutz-Zertifikat kann IT-Sicherheit als Gütesiegel eines Unternehmens dargestellt werden. Dies ist nicht nur ein Wettbewerbsvorteil. Auch Banken und Versicherungen achten bei der Vergabe von Krediten und Beitragsberechnungen zunehmend auf den Faktor IT-Security. Laut einer kürzlich von der „Security for Business GmbH“ veröffentlichten Umfrage unter Firmenkundenberatern von Finanzinstituten wären 39 Prozent bereit, Zinsnachlässe bei Krediten zu gewähren, wenn ein

„anerkanntes IT-Security-Zertifikat“ vorhanden ist. Die kommenden Kreditvergaberichtlinien nach „Basel II“ werden diesen Trend noch verstärken.

Konkret messbare Vergabekriterien

Die jüngste IT-Grundschutz-Auszeichnung erfolgte auf der CeBIT: Dort nahm der Leiter des Geschäftsbereichs Hosting der „SAP Systems Integration AG“ (SAP SI), Uwe Ripprich, das Zertifikat aus den Händen des BSI-Präsidenten Udo Helmbrecht entgegen. Das Untersuchungsgebiet bei SAP SI umfasste das System-Management und -Monitoring von der Kundenschnittstelle über Backbone-, Router- und Firewallstrukturen bis hin zum Application Hosting auf circa 400 Servern in drei hochverfügbaren Rechenzentren. Rund 100 Unternehmen lassen derzeit ihre IT-Lösungen bei der SAP SI betreiben, darunter Zulieferer der Automobilindustrie, Handelsunternehmen und nicht zuletzt Kunden aus dem Gesundheitswesen, die einen hohen Schutzbedarf fordern.

Für die INFODAS-Auditoren Gerhard Weck und Frank Reiländer war das SAP SI-Projekt die zweite erfolgreiche Auditierung eines großen Rechenzentrums in kürzester Zeit. Erst im Herbst vergangenen Jahres war der Geschäftsbereich Application Hosting der TDS Informationstechnologie AG in Neckarsulm, einem weiteren großen SAP-Hoster, erfolgreich vorbereitet und geprüft worden.

Die Auditierung eines komplexen IT-Verbunds dauert dabei – mit Erstellung und Prüfung des Audit-Reports - nicht länger als vier Wochen; das gesamte Projekt allerdings bis zu sechs Monate. Der Grund: Der eigentlichen Auditierung geht ein ausführlicher Basis-Sicherheitscheck voraus. Anhand von bis zu 700 Fragen wird dabei ein Soll-Ist-Vergleich erstellt. Fällt das Ergebnis in Teilen negativ aus, kann noch nachgerüstet werden. Erst wenn alle erforderlichen Maßnahmen umgesetzt wurden, beginnt die eigentliche Auditierung. Der ermittelte Umsetzungsstatus wird dabei stichprobenartig vor Ort überprüft. Stimmen die Ergebnisse mit den Angaben überein, erhält das Unternehmen das IT-Grundschutz-Zertifikat für zwei Jahre. Nach Ablauf dieser Zeit kann es durch eine Wiederholungsprüfung verlängert werden.

Das „Zwei-Auditoren-Modell“

„Wie schon bei früheren Projekten hat sich auch bei der Auditierung bei SAP SI unser Zwei-Auditoren-Modell bewährt“, erklärt Krings. Das Prinzip: Da der mit der Zertifizierung beauftragte Auditor innerhalb der vergangenen zwei Jahre in dem zu zertifizierenden Unternehmen nicht beratend tätig gewesen sein darf, bereitet ein zweiter Auditor das Unternehmen auf das Zertifikat vor. Er führt den Basis-Check gemäß den Prüfkriterien durch, deckt Missstände auf und berät das Unternehmen bei deren Behebung. Der Prüf-Auditor findet für das Zertifikats-Audit ein Unternehmen vor, das seine Hausaufgaben gemacht hat. Das beschleunigt den Zertifizierungsprozess erheblich. Unnötige Unterbrechungen und Nachprüfungen, wie sie bei einer Vorbereitung ohne lizenzierten Auditor häufig vorkommen, können vermieden werden. „Eine solche ganzheitliche Begleitung des Zertifizierungsprozesses wird aus Gründen der Planungssicherheit immer öfter gewünscht“, erklärt Krings. „Denn gerade in Zeiten enger Budgets ist das Bedürfnis nach klarer Kalkulation und Investitionssicherheit besonders groß.“

Zur weiteren Beschleunigung der Auditierung und zur Förderung eines durchgängigen Prozesses sowie einer klaren Abbildung der Rollentrennung zwischen Institution, Prüfer und Zertifizierer, trägt der Einsatz einer speziellen Auditierungs-Software bei. Sie ermöglicht nicht nur den schnelleren Ablauf des Basis-Sicherheits-Checks. Die Prüfergebnisse können zudem transparent dargestellt und unmittelbar für das Zertifizierungsaudit genutzt werden. Bei der TDS- und der SAP SI-Auditierung kam die von der INFODAS GmbH entwickelte IT-Sicherheitsdatenbank SAVE® zum Einsatz.

Da für den überwiegenden Teil der IT-Systeme und -Anwendungen mittlere Schutzanforderungen ausreichend sind, fokussiert sich der IT-Grundschutz auf die Gewährleistung dieses mittleren Schutzbedarfs. Im Bedarfsfall kann das IT-Grundschutz-Verfahren aber auch problemlos um spezifische Risikoanalysen und Sicherheitsmaßnahmen für den Hochschutz ergänzt werden. Außerdem ist es integrativ mit anderen Normen einsetzbar: Es lässt sich als Zwischenschritt zu einer BS-7799/ISO17799-Zertifizierung ebenso umsetzen wie danach. Nicht zuletzt passt es sich IT-Sicherheitsmanagement-

Systemen wie COBIT oder GMITS nahtlos an. Das verliehene IT-Grundschutz-Zertifikat schließt zudem die Empfehlung des „ISO-17799:2000“-Standards ein.

Und schließlich zeichnet sich das IT-Grundschutzzertifikat durch einen großen Praxisnutzen aus: Die möglichst genaue Abbildung der Organisation bzw. der Technik bietet dem Kunden neben der hohen Transparenz eine greifbare Zertifikatsaussage. Sämtliche Zertifikate sind auf der Homepage des BSI einsehbar.

Über die INFODAS GmbH

INFODAS ist ein unabhängiges Software- und Beratungsunternehmen und gehört zu den innovativsten deutschen mittelständischen Systemhäusern. Zu den Schwerpunkten von INFODAS zählt die IT-Sicherheits-Beratung auf Basis der IT-Sicherheitsdatenbank SAVE®. Die aktuelle Version SAVE® V3.1. ist das erste und derzeit einzige verfügbare Unterstützungswerkzeug für das aktuelle Grundschutzhandbuch des BSI (Stand Oktober 2003)

Unter Leitung der beiden IT-Grundschutz-Auditoren, Gerhard Weck und Frank Reiländer, konnte INFODAS im letzten Jahr zielgerichtet den IT-Sicherheitsprozess zahlreicher Kunden gestalten sowie die Grundschutz-Zertifizierungen der „SAP Systems Integration AG“ und der „TDS Informationstechnologie AG“ planen und unterstützen – die beiden umfangreichsten der bislang fünf durchgeführten IT-Grundschutz-Zertifizierungen.

INFODAS arbeitet bereits langjährig erfolgreich mit dem BSI bei Anwendungen und Fortschreibung des IT-Grundschutzhandbuches zusammen. Aktuelles Projekt: Die Restrukturierung des Grundschutzhandbuches 2004. Weiterhin wurde als Erweiterung der SAVE® V3.1- Software eine Verfahrenshilfe für die Umsetzung des Datenschutzes und der Datensicherheit in Unternehmen und Behörden entwickelt.
www.infodas.de