Security Audits bringen mehr Sicherheit in die IT

Durch ihre Vernetzung steigt die Verwundbarkeit von IT-Systemen sprunghaft an. Diesem Umstand gilt es auch im Hinblick auf die strengeren rechtlichen Rahmenbedingungen Rechnung zu tragen. Damit werden regelmässige Security Audits zur Pflicht. *Andreas Wisler*

Andreas Wisler
ist Geschäftsführer und Sicherheitsspezialist bei der GO OUT Production GmbH, welche IT-Sicherheits-Überprüfungen und -Beratungen durchführt.
wisler@goout.ch

Eine sichere IT-Infrastruktur mit PC, Netzwerk und Internet ist heute für viele Geschäftsbereiche von zentraler Bedeutung. Immer häufiger sind Mensch und Maschine auf ständig verfügbare Informationen angewiesen. Fallen die Informationssysteme aus oder gehen Daten verloren, hat dies gravierende Folgen für die gesamte Firma. Im schlimmsten Fall steht das ganze Unternehmen still.

Es ist daher wichtig, Informationen und die nötige technische Infrastruktur vor Ausfällen und Manipulationen zu schützen. Mitarbeiter müssen gezielt geschult werden, um Fehler bei der Bedienung der IT zu minimieren. Doch nicht nur die technischen Mittel und die Mitarbeiter gilt es zu beachten, sondern auch die immer strengeren rechtlichen Rahmenbedingungen. Das Management einer Unternehmung kann belangt werden, wenn einer angemessenen Sicherung der IT nicht Rechnung getragen wird. Banken überprüfen im Rahmen des Basel-II-Ratings die IT-Sicherheit ihrer Kunden. Und Wirtschaftsprüfer beurteilen die Systeme zur IT-Sicherheit ihrer Auftraggeber. Die IT-Sicherheit ist zu einem wichtigen Element des Risikomanagements geworden.

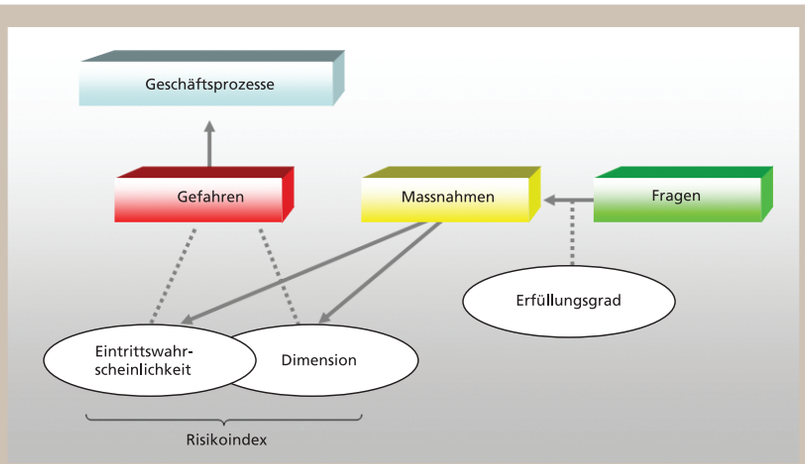
> ***«Immer häufiger sind Mensch und Maschine auf ständig verfügbare Informationen angewiesen.»***

> ***«Professionelle Security Audits zeigen auf, wie es um die IT-Sicherheit steht.»***

Professionelle Security Audits zeigen auf, wie es um die IT-Sicherheit von Unternehmen steht. Dabei genügt es nicht, nur die technischen Mittel einer Firma zu prüfen. Wichtig sind auch die Aspekte Organisation und firmeninternes Know-how. Ein Security Audit deckt Schwachstellen und Sicherheitslücken von Informationssystemen auf und ist damit ein wesentlicher Bestandteil für die Sicherung der Wettbewerbsfähigkeit eines Unternehmens.

Insbesondere sollten folgende zwei Anforderungen an Security Audits beachtet werden:

- Wiederholbarkeit
  Security Audits sollten nicht nur einmal und sporadisch durchgeführt werden, sondern ein Prozess sein, der die IT-Sicherheit in regelmässigen Abständen überprüft. IT-Umgebungen ändern sich heute fast täglich. Was heute aktuell ist, ist in einer Woche bereits wieder veraltet. Wenn Firmen wachsen, ändern sich die Anforderungen an Hardware und Software. Ein Security Audit sollte daher besonders nach grösseren organisatorischen oder technischen Veränderungen wiederholt werden. Bei einem solchen Audit werden nicht nur die veränderten oder neuen Bereiche angeschaut, sondern das System als Ganzes. Folgende Fragen sollten beantwortet werden: Welche Konsequenzen haben die Veränderungen? Entstehen dadurch neue Schwachstellen? Welche Änderungen ergeben sich für die Organisation? Security Audits werden nach standardisierten Kriterien durchgeführt. Dadurch sind die Resultate reproduzierbar.
- Objektivität und Neutralität
  Security Audits müssen objektiv und neutral sein. Ein standardisiertes Vorgehen liefert immer dieselben Resultate – unabhängig davon, wer die Überprüfung durchführt. Der Standard BS7799 («Code of Practice») oder das Grundschutzhandbuch des BSI bieten eine solide Grundlage, um diese Anforderungen zu erfüllen.



Professionelle Security Audits helfen, kritische Geschäftsprozesse vor IT-Risiken zu schützen

Auch beim Ablauf eines Security Audit ist darauf zu achten, dass der folgende Prozess strikte eingehalten wird:

1) Bedürfnisaufnahme

Die Vorbereitungen für eine Sicherheitsüberprüfung sind entscheidend. Sie bilden die Basis für die Analyse der IT-Sicherheit in einem Unternehmen. Zuerst wird der Ist-Zustand untersucht: Wie sieht die Struktur der Firma aus? Welche Mittel werden eingesetzt? Welche Prozesse zeichnen das Unternehmen aus? Sind Verbindungen zu einem externen Arbeitsplatz oder Aussenstellen vorhanden? Im nächsten Schritt werden die Ziele der Organisation untersucht: In welche Richtung soll sich das Unternehmen entwickeln? Welche Schwachstellen und Probleme sind bereits bekannt? Die Geschäftsleitung gibt dabei mit einer Liste kritischer Geschäftsprozesse die Leitplanken vor. Die IT-Leitung erweitert die Liste mit den dazugehörenden Applikationen und beschreibt die kritischen Systemabhängigkeiten.

2) Dokumentation

Bevor ein Audit durchgeführt werden kann, müssen die Strukturen und Prozesse einer Firma bekannt sein. Nur so können Schwachstellen erkannt und praktikable Lösungen gefunden werden. Folgende Unterlagen gilt es zu prüfen:

- IT-Strategie (evtl. mit Sicherheitskonzept)
- Regelung
- Mitarbeiterreglement
- Notfallkonzept
- technische Unterlagen zu Hardware, Software, Backup und Netzwerkaufbau

Mit der Bedürfnisaufnahme und dem Studium der Dokumentationen bereiten sich die Auditoren genau auf das Unternehmen und seine individuelle Situation vor.

3) Audit

Die Organisation wird in drei Schritten komplett untersucht:

- Fragenkatalog
  Auf Basis der BS7799/2, der ISO-Norm 17799 oder des Grundschutzhandbuchs des BSI erarbeitet der Auditor einen detaillierten Fragenkatalog. Er stellt technische und organisatorische Massnahmen zusammen, die den gewünschten Sicherheitsstandard ermöglichen, und leitet davon Fragen ab, die Rückschlüsse über den Fortschritt der Realisierung geben sollen. Die Fragen werden anschliessend in folgende Gruppen eingeteilt: Ebene der Geschäftsleitung (IT-Strategie, IT-Sicherheitskonzept, Mitarbeiter- und Notfallplanung), der IT-Verantwortlichen (Hard- und Software, technische Mittel, Backup) und der Mitarbeiter (Basiswissen, Sicherheitsverständnis).

«Ein Security-Audit sichert die Wettbewerbsfähigkeit eines Unternehmens.»

- Rundgang
  Im Rundgang unterzieht der Auditor sämtliche IT-Mittel der Organisation einem umfassenden Check. Zum Rundgang gehören die Untersuchung der Server- und Netzwerkumgebung, die Analyse des Mitarbeiter-Know-how sowie die Überprüfung aller IT-relevanter Arbeitsplätze.
- Technische Kontrolle
  Verschiedene Tools schliessen die Kontrolle der IT ab. Es geht darum, die Dokumentationen auf den neusten Stand zu bringen, Abweichungen zu erfassen und die Konfiguration der Server zu kontrollieren (Benutzer, Rechte, Patchstand, bekannte Schwachstellen etc.). Diese Tests werden sowohl im internen Netzwerk als auch von aussen durchgeführt. Wichtig für die technische Kontrolle ist auch die sichere Konfiguration von Firewall und Internetzugang (VPN).

4) Resultate

Die Auswertung der Antworten, die auf einem umfassenden Fragenkatalog beruhen, erlaubt Rückschlüsse auf bereits umgesetzte Massnahmen und zeigt mögliche Verbesserungen oder Lösungen für die IT-Sicherheit auf. Je professioneller der Fragenkatalog ist, desto grösser ist die Chance, alle Sicherheitslücken in einem IT-System zu entdecken und schliesslich zu beheben.

5) Auswertung

Die Verflechtungen in komplexen IT-Systemen sind vielschichtig. Die Auswertung des Fragenkatalogs aus den Security Audits wird in einer Datenbank abgebildet. Daraus entwickelt der Auditor einen Gefahrenkatalog. Den so erfassten Gefahren wird ein Risikoindex zugeordnet, der die Dimension der Gefahr und die Eintrittswahrscheinlichkeit misst. Noch nicht umgesetzte Massnahmen sind in der Datenbank speziell hervorgehoben und werden je nach Gefahrendimension und Dringlichkeit geordnet.

6) Umsetzung

Die Datenbank zeigt als Resultat eine Reihe von Massnahmen, die es für die Gewährleistung der IT-Sicherheit umzusetzen gilt. Nicht alle sind gleich dringlich – einige davon jedoch kritisch. Bei der Umsetzung der einzelnen Massnahmen muss das IT-System als Ganzes betrachtet werden. Ändert man die Konfiguration von Element A, kann dies grosse Auswirkungen auf die Elemente C und D haben. Daher ist die Umsetzungsreihenfolge von grosser Bedeutung. Entscheidend für eine erfolgreiche Umsetzung ist, dass die Massnahmen zielgerichtet und in nützlicher Frist umgesetzt werden und genügend Ressourcen zur Verfügung stehen – personelle wie finanzielle.

7) Nutzen

Vier Wochen nach der Bedürfnisaufnahme stehen die Resultate des Security Audit zur Verfügung. Ein reichhaltiges Arbeitshandbuch hilft bei der Beseitigung der entdeckten Schwächen und Sicherheitslücken. Eine detaillierte Beschreibung der einzelnen Massnahmen und Mittel erleichtert die Umsetzung im Betrieb. Wichtig ist, dass das Unternehmen mit den vorhandenen Werkzeugen den grössten Teil der Massnahmen in Eigenregie umsetzen kann.