Schatzkammern fürs 21. Jahrhundert

Ein Informationssicherheits-Management-System ist ein wichtiger Eckpfeiler für nachhaltigen Kanzleierfolg

Von Heiko Haffmans

Früher war längst nicht alles besser, aber zumindest vieles leichter. Die Aufbewahrung von Schätzen zum Beispiel: Vier solide gemauerte Wände, eine schwere Eichentür und ein grimmig dreinblickender Mann mit Axt – fertig war die Schatzkammer. Unternehmen, die heute ihre Reichtümer schützen wollen, müssen wesentlich mehr Aufwand betreiben. Denn das Gold des Informationszeitalters sind – wer hätte das gedacht – Informationen. Und diese sind schwerer zu schützen und wesentlicher leichter zu verlieren als tonnenschwere Goldkisten.

Informationswirtschaft (Symbolbild): Jedes Unternehmen besitzt einen riesigen Pool an Informationen – doch wie schützt man diesen Schatz?

Schätze sichern

Informationssicherheit ist daher ein zentrales Thema für den betriebswirtschaftlichen Erfolg und die juristische Absicherung eines Unternehmens beziehungsweise einer Kanzlei. Dabei geht es nicht allein um die Sicherheit personenbezogener Daten gemäß dem Bundesdatenschutzgesetz. Und auch der Schutz der IT-Systeme vor Viren und Trojanern ist nicht alleiniger Fokus: Datenschutz und IT-Sicherheit sind vielmehr wichtige Aspekte von Informationssicherheit, aber eben nur zwei Punkte von vielen.

Informationssicherheit umfasst alle Gesichtspunkte, die zur Sicherung von Unternehmens-Know-how und sensiblen Daten notwendig sind. Und das schließt das Wissen um Prozesse, Projekte, Vertriebsnetze, Partnerschaften und Patente mit ein – egal, ob sie schriftlich und elektronisch dokumentiert sind oder nur im Erfahrungsschatz der Mitarbeiter verankert. Hierdurch betrifft das Thema Informationssicherheit zahlreiche Unternehmensbereiche: Vom Organisationshandbuch über die Firewall bis hin zur Schulung der Mitarbeiter.

Wenn Experten über Informationssicherheit sprechen, diskutieren sie in der Regel folgende drei Aspekte: Vertraulichkeit, Verfügbarkeit und Integrität von Information:

Vertraulichkeit – bewahrt ein Unternehmen die Informationen, die vertraulich behandelt werden müssen, entsprechend abgesichert auf?

Bei dieser Frage geht es nicht nur um technische Maßnahmen wie den IT-Schutz, sondern vor allem um organisatorische Prozesse. Denn die häufigsten Probleme in diesem Bereich entstehen durch menschliches Fehlverhalten.

Verfügbarkeit – sind Informationen, die für den Betrieb des Unternehmens beziehungsweise der Kanzlei als Arbeitsgrundlage unverzichtbar sind, ständig verfügbar?

Wichtig ist hier ein sicherer IT-Betrieb mit Maßnahmen wie Datensicherung, IT-Service und -Support. Idealerweise hat das Unternehmen außerdem ein Notfallkonzept, falls ein größerer Schaden auftritt. Genauso muss aber sichergestellt sein, dass Informationen im Fall eines Mitarbeiterausfalls dem Unternehmen zur Verfügung stehen.

Integrität – ist sichergestellt, dass die Informationen, mit denen wir arbeiten, auch korrekt sind?

Dabei geht es um Fragen der Datenmanipulation und auch um fehlerhafte Software, die möglicherweise falsche oder unvollständige Informationen liefert.

Der Weg zum ISMS

Ein sogenanntes Informationssicherheits-Management-System (ISMS) kann helfen, diese drei Aspekte sicherzustellen. Die Grundregel beim Aufbau eines ISMS lautet, dass Aufwand und Nutzen in einer vernünftigen Relation zueinander stehen müssen. Sie sollten sich pragmatisch an den Möglichkeiten des Unternehmens beziehungsweise der Kanzlei orientieren: „In der Branche unterscheidet man zwischen dem Begriff der maximalen Sicherheit und der sogenannten optimalen Sicherheit", erklärt Bernd Huber, Geschäftsführer des Serviceproviders Compus. „Der Versuch, maximale Sicherheit zu erreichen, wäre zu teuer und würde Systeme schaffen, die für die Anwendung in der Praxis gänzlich ungeeignet sind." Daher strebe man nach optimaler Sicherheit: Das bedeutet, dass die Daten so abgesichert sein müssen, dass die Aufwand-Ertrags-Relation für einen Datendieb möglichst abschreckend und die

Aufwand-Risiko-Relation für das Unternehmen akzeptabel ist. Prozesse und IT-Systeme wiederum sollten so aufgesetzt sein, dass die Wahrscheinlichkeit eines Datenverlusts möglichst gering ist, sie aber gleichzeitig gut in den Arbeitsalltag integrierbar sind.

Die ISO 27001

Möchte eine Kanzlei ein ISMS einführen, muss sie das Rad nicht gänzlich neu erfinden. Zahlreiche Dienstleister bieten Unterstützung bei der Implementierung solcher Systeme in Unternehmen und Kanzleien an. Das wohl führende ISMS stützt sich dabei auf die internationale Norm ISO 27001.

Ursprünglich als Industrienorm konzipiert, wird sie inzwischen zunehmend auch im Mittelstand als Referenzvorgabe eingesetzt. Die Richtlinie definiert, was ein gutes ISMS leisten muss und wie man es aufbaut und betreibt. Sie deckt dabei unter anderem die Bereiche Organisation und Management von Informationssicherheit, personelle, physische und umgebungsbezogene Sicherheit, das Betriebs- und Kommunikationsmanagement sowie die Beschaffung, Entwicklung und Wartung von Informationssystemen ab.

Die Rolle der IT

„Die Absicherung der Informationssicherheit nach ISO 27001 bedeutet, wenn richtig geplant, keinen überbordenden Aufwand", zerstreut Bernd Huber die häufigsten Befürchtung zahlreicher Mittelständler: „Die wichtigsten Themen und Prozesse sollten knapp und einfach dokumentiert werden." Denn nur wenn die Arbeitsanweisungen simpel und übersichtlich gehalten seien, würden sie auch von den Mitarbeitern „gelebt". „Das Schlimmste, was einem Unternehmen passieren kann, ist ein sicherer Prozess, den die Mitarbeiter nicht nutzen, weil dieser an der Arbeitswirklichkeit vorbeigeht", so Huber.

Auch der Aufbau einer sicheren und verlässlichen IT-Infrastruktur ist vom Aufwand her darstellbar: Viele Mittelständler verlassen sich auf einen oder mehrere externe IT-Service-Provider – insbesondere dann, wenn sie selbst keine IT-Abteilung vorhalten können. „Wichtig ist, dass die Dienstleister dieselben oder höhere Standards zur Informationssicherheit erfüllen wie das beauftragende Unternehmen", erläutert Huber: Ansonsten könne es sein, dass man sich eine Sicherheitslücke ins Unternehmen hole.

„Das Schlimmste, was einem Unternehmen passieren kann, ist ein sicherer Prozess, den die Mitarbeiter nicht nutzen."

Sein Fazit: „Wenn sich eine Kanzlei auf das Wesentliche konzentriert – dies jedoch in angemessener Weise, erhält sie eine umfassende Absicherung ihrer Daten", so Huber. „Die Losung muss also lauten: Keep IT simple." ■

Die zehn Gebote der Informationssicherheit

Die Compus Computer GmbH ist eines der führenden IT-Systemhäuser im Großraum München und Systempartner der Datev. Im LSWB-Magazin stellt Geschäftsführer Bernd Huber zehn Grundregeln der Informationssicherheit in Kanzleien auf:

1. Verpflichte deine Mitarbeiter bereits im Arbeitsvertrag zur Informationssicherheit, zum Datenschutz und zur Geheimhaltung. Hier sollte unbedingt definiert sein, dass die Nutzung des Internets ausschließlich dienstlichen Charakter hat.
2. Bestimme einen externen Datenschutzbeauftragten und lade ihn zu regelmäßigen Audits.
3. Schließe eine Datenschutzvereinbarung mit allen relevanten Lieferanten und Dienstleistern.
4. Schließe mit deinen IT-Serviceprovidern Verträge zur Auftragsdatenverarbeitung ab, die sie zur Einhaltung der betriebseigenen Datenschutz- und Informationssicherheitsbestimmungen verpflichten.
5. Stelle sicher, dass der IT-Serviceprovider nach ISO 9001 und zumindest in Grundzügen auch nach ISO 27001 zertifiziert ist. Wichtig: Die gesamte Organisation des IT-Serviceproviders muss zertifiziert sein und nicht nur Teile des Unternehmens, wie etwa nur das Rechenzentrum.
6. Schule deine Mitarbeiter regelmäßig im Hinblick auf Informationssicherheit, IT-Sicherheit und Datenschutz.
7. Etabliere ein Vorschlagswesen in der Kanzlei, um Schwachstellen zu identifizieren und auszuräumen.
8. Strebe für die Kanzlei selbst eine Zertifizierung nach ISO 9001 und ISO 27001 an. Hierdurch kann ein umfassendes Qualitätsmanagementsystem etabliert werden, das weit über Fragen der reinen IT hinausgeht und die Kanzlei als Partner auch sehr anspruchsvoller Mandanten qualifiziert.
9. Etabliere das Managementsystem zur Informationssicherheit als permanenten Verbesserungeprozess und nicht als „Eintagsfliege".
10. Nimm branchenspezifische absichernde Maßnahmen – etwa die Prüfung nach IDW PS 330 für Wirtschaftsprüfer – vor, um die genannten Basisanforderungen zu ergänzen.