Ein Fallbeispiel aus der Praxis: Telefonbau Arthur Schwabe GmbH & Co. KG (TAS)

Zertifizierung der Informationssicherheit – Warum und wie?

AUTOR: THOMAS SCHMIDT

Die Unternehmenszentrale von TAS in Mönchengladbach (Quelle: TAS)

Die Beweggründe für eine Zertifizierung der Informationssicherheit in einem Unternehmen können vielfältiger Natur sein: Unternehmerisches Eigeninteresse, Kundenanforderungen oder auch die Wettbewerbsfähigkeit auf dem Markt bringen Unternehmensleitungen dazu, die eigene Informationssicherheit zertifizieren zu lassen. Durch eine Zertifizierung der Informationssicherheit wird eine kontinuierliche Informations-/Datensicherheit im Unternehmen verankert. Zudem lassen sich sowohl geschäftliche Risiken als auch die Gefahr einer individuellen Haftung der Geschäftsführer reduzieren.

Der Autor dieses Beitrags, ***Thomas Schmidt***, ist Chief Information Security Officer (CISO) und Datenschutzbeauftragter der Telefonbau Arthur Schwabe GmbH & Co. KG (TAS) in Mönchengladbach.

Kontakt: tschmidt@tas.de

Eine Zertifizierung ist ein Qualitätsnachweis für die Informationssicherheit im Hinblick auf die gewünschten Schutzziele „Verfügbarkeit", „Integrität" und „Vertraulichkeit". Durch die Etablierung einer Zertifizierung werden Einrichtung, Umsetzung, Aufrechterhaltung sowie die fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS; engl.: Information Security Management System) in einem Unternehmen sichergestellt.

Welche Zertifizierung ist für mein Unternehmen die richtige?

Bevor sich ein Unternehmen für eine Zertifizierung ihrer Informationssicherheit entscheidet, sollte Klarheit über die Art und den Umfang der Zertifizierung geschaffen werden, denn davon abhängig ist der passende Standard für die Zertifizierung zu wählen.

Bekannte Standards der Informationssicherheit

Bei der Umsetzung einer Zertifizierung hat ein Unternehmen die Wahl zwischen folgenden unterschiedlichen Standards (Beispiele):

- ISO 27001
- BSI IT-Grundschutz
- Sicherer IT-Betrieb (SITB)
- VdS 3473

ISO 27001 und BSI IT-Grundschutz

Die ISO 27001 ist eine Norm der „International Organization for Standardization" mit insgesamt 130 Sicherheitsmaßnahmen („Controls"). Sie ist in der ISO 27002 im Detail beschrieben und ein internationaler Standard zur Einrichtung eines ISMS.

Der BSI IT-Grundschutz ist eine vom Bundesamt für Informationssicherheit (BSI) entwickelte Vorgehensweise zur Analyse sowie zur Verbesserung der Informationstechnik.

Eine ISO-27001-Zertifizierung auf Basis des BSI IT-Grundschutzes fordert neben den ca. 130 Controls beispielsweise auch, dass entsprechende Maßnahmen des BSI-Grundschutzkataloges erfüllt werden müssen. Als Richtwert für das Zertifikat dient eine Erfüllungsquote von 82 Prozent.

SITB (Sicherer IT-Betrieb)

SITB (Sicherer IT-Betrieb) ist ein vom ehemaligen Sparkassen-Informatik-Zentrum (SIZ) entwickelter

Informationssicherheitsstandard für die Rechenzentren der Sparkassen, welcher in den vergangenen Jahren auch für andere Branchen angepasst wurde.

VdS 3473

Die Richtlinie VdS 3473 ist ein Standard zur Umsetzung von Informationssicherheit in kleinen und mittelständischen Unternehmen (KMU) und ist aufwärtskompatibel zu ISO27001 und IT-Grundschutz.

Mit den Cyber-Richtlinien 3473 reagierte VdS auf die wachsende Bedeutung der Informationssicherheit gerade für KMU. Die Richtlinien VdS 3473 enthalten Mindestanforderungen an die Informationssicherheit insbesondere für KMU, ohne Unternehmen organisatorisch oder finanziell zu überfordern, und sind branchenneutral gehalten. Die umzusetzenden Maßnahmen der VdS 3473 konzentrieren sich auf das technisch und organisatorisch Wesentliche für KMU und sind daher für die meisten Organisationen direkt und praxisnah umsetzbar.

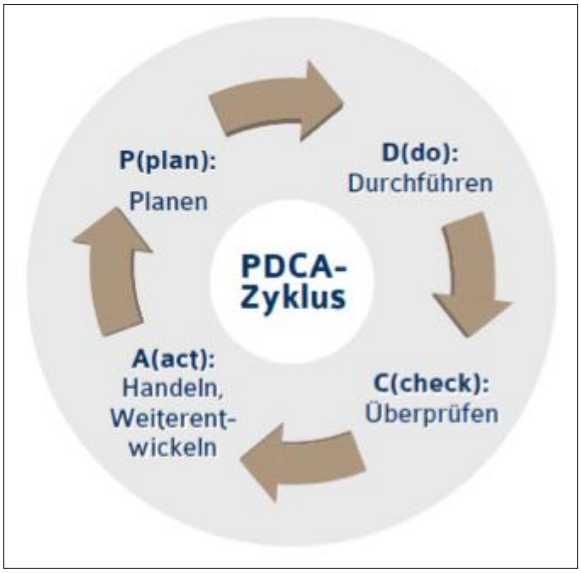
Umsetzung nach dem PDCA-Modell

Die hier genannten Standards der Informationssicherheit beziehen sich bei der Umsetzung auf das PDCA-Modell, dessen Ziel ist es, vorhandenes Verbesserungspotenzial sukzessive auszuschöpfen und so das gewünschte/geforderte Sicherheitsniveau zu erreichen.

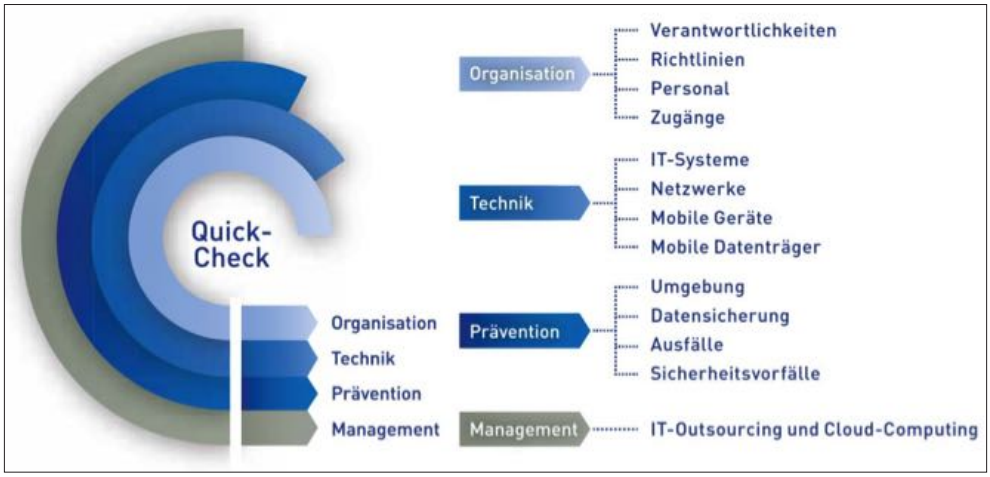
- ❏ Planung und Konzeption (PLAN)
- ❏ Umsetzung der Planung (DO)
- ❏ Erfolgskontrolle, Überwachung der Zielerreichung (CHECK)
- ❏ Optimierung, Verbesserung (ACT)

Warum hat sich die TAS für eine Zertifizierung nach VdS 3473 entschieden?

Im Unterschied zu anderen Standards der Informationssicherheit ist die Richtlinie VdS 3473 kurz und prägnant. Zudem zeichnet sie sich durch eine eindeutige Sprachregelung aus. Trotzdem wird in der Richtlinie VdS 3473 grundsätzlich die gesamte Informationssicherheit eines Unternehmens betrachtet, ohne jedoch die Komplexität anderer Sicherheitsstandards zu beinhalten. Mit der Umsetzung der Zertifi-



Das PDCA-Modell als Schaubild



Übersicht über die im VdS-Quick-Check abgefragten Themenfelder

zierung nach VdS 3473 erhält das Unternehmen eine solide Basis für Informationssicherheit.

Der Weg zur Zertifizierung nach VdS 33473

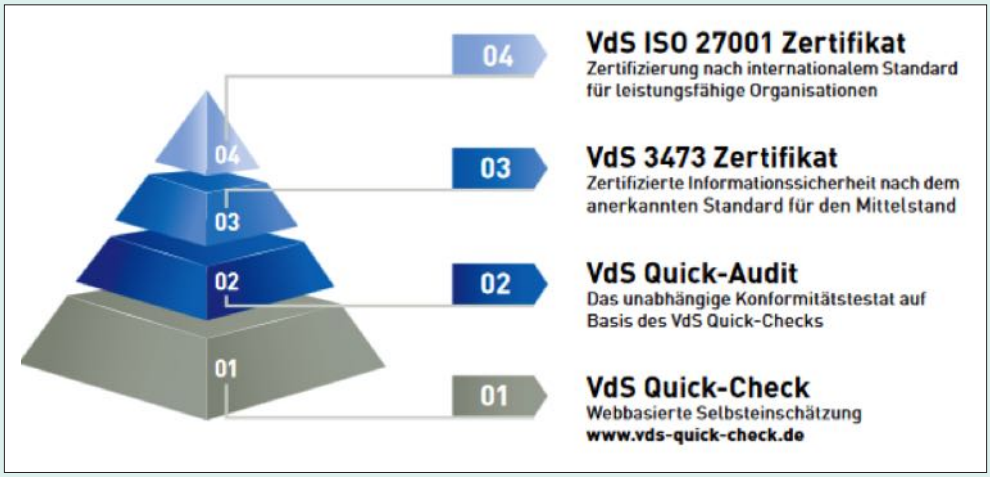
VdS-Quick-Check

Mithilfe des webbasierten Tools VdS-Quick-Check wurde im ersten Schritt ein ersten Überblick des vorhandenen Niveaus der Informationssicherheit erarbeitet. Bei der Durchführung wurde darauf geachtet, dass neben dem IT-Sicherheitsbeauftragten und dem Datenschutzbeauftragten auch die verantwortlichen Mitarbeiter aus dem IT-Bereich mitwirken.

Nur wenn die Know-how-Träger bereits am Anfang mitarbeiten, werden Ressourcen richtig eingesetzt. Auch die Qualität der Ergebnisse ist um ein vielfaches höher. Die Ergebnisse der 39 Fragen werden sowohl in einem einfachen Ampelsystem als auch in einem ausführlichen Bericht dargestellt und haben uns einen ersten Überblick über den Status der Informationssicherheit gegeben.

VdS-Quick-Audit

Mit Unterstützung eines VdS-anerkannten Auditors wurde das Quick Audit mit dem Ziel durchgeführt, die im Quick-Check erarbeiteten Ergebnisse detailliert zu hinterfragen und unter Berücksichtigung der Gegebenheiten vor Ort zum Zeitpunkt des Audits zu bewerten. Daraus sollten korrigierende Maßnahmen erfolgen. Die Durchführung des Audits diente auch als Vorbereitung der geplanten Zertifizierung nach VdS 3473. Im Rahmen dieses Audits wurden die verantwortlichen Mitarbeiter befragt, Räumlichkeiten begangen sowie Dokumentationen als auch relevante/sensible Softwareanwendungen begutachtet. Die aus dem Audit resultierenden Feststellungen wurden risikoorientiert aufbereitet, um uns die Möglichkeit zugeben, die Umsetzung der korrigierende Maßnahmen in ein Projekt zu integrieren.



Der Aufbau der Cyber-Security-Angebote von VdS Schadenverhütung

Zertifizierung

Nach der Umsetzung aller korrigierender Maßnahmen zur Erfüllung der im Quick Audit dokumentierten Feststellungen werden in Q3/2017 im Rahmen eines Zertifizierungsaudits und jährlichen Überwachungsaudits die Konformität mit den Anforderungen der Richtlinien überprüft (SOLL/IST-Abgleich). Sind alle SOLL-Kriterien erfüllt, wird die TAS das VdS-3473-Zertifikat erhalten – als Nachweis gegenüber Kunden und Lieferanten einen angemessenen Informationssicherheitsschutz implementiert zu haben.

Im Rahmen der Zertifizierung werden folgende Themenblöcke bearbeitet, um final die gesamte Informationssicherheit des Unternehmens betrachtet zu haben:

- ❏ Organisation der Informationssicherheit
- ❏ Leitlinie zur Informationssicherheit
- ❏ Richtlinien zur Informationssicherheit
- ❏ Personal
- ❏ Wissen
- ❏ Identifizierung kritischer IT-Ressourcen
- ❏ IT-Systeme
- ❏ Netzwerke und Verbindungen
- ❏ Mobile Datenträger
- ❏ Umgebung
- ❏ IT-Outsourcing und Cloud Computing
- ❏ Zugänge und Zugriffsrechte
- ❏ Datensicherung und Archivierung
- ❏ Störung und Ausfälle
- ❏ Sicherheitsvorfälle

Fazit

Die Zertifizierung nach VdS 3473 ermöglicht es unserem Unternehmen, in den vorhandenen IT-Infrastrukturen mit vertretbarem Aufwand ein angemessenes Sicherheitsniveau aufzubauen und dieses im laufenden Betrieb nachhaltig zu etablieren – ohne organisatorische oder finanzielle Überforderung. Mit der Umsetzung der Zertifizierung nach VdS 3473 erhält das Unternehmen eine solide Basis für Informationssicherheit.