IT-Sicherheit für kleine und mittlere Unternehmen

Über 99 Prozent der Unternehmen in Deutschland sind dem Bereich der kleinen und mittleren Unternehmen (KMU) zuzuordnen und stellen somit einen wesentlichen Faktor für den Erfolg der deutschen Wirtschaft dar. Viele wirtschaftliche Prozesse – insbesondere auch im öffentlichen Bereich – hängen mittelbar oder unmittelbar von der Leistungsfähigkeit dieser Unternehmen ab. Im Zeitalter elektronischer Geschäftsprozesse ist eine funktionierende und sicher aufgestellte IT eine Voraussetzung für diese Leistungsfähigkeit.

Laut dem Bericht des Statistischen Amts der Europäischen Union (Eurostat) „E-commerce in Europa“

- nutzen 96% aller KMU Computer
- haben 67% aller KMU einen Internetzugang
- haben 65% aller KMU eine eigene Website

Laut dem Institut für Mittelstandsforschung (IfM) Bonn wird das Internet u.a. noch benutzt für

- die Vernetzung von Unternehmensteilen
- interne Automatisierung
- externe Automatisierung (B2B)

Das BSI Bundesamt für Informationssicherheit stellte 2011 eine Studie zum Thema Informationssicherheit in kleinen und mittleren Unternehmen vor. Daraus ergaben sich vielfältige Handlungsempfehlungen:

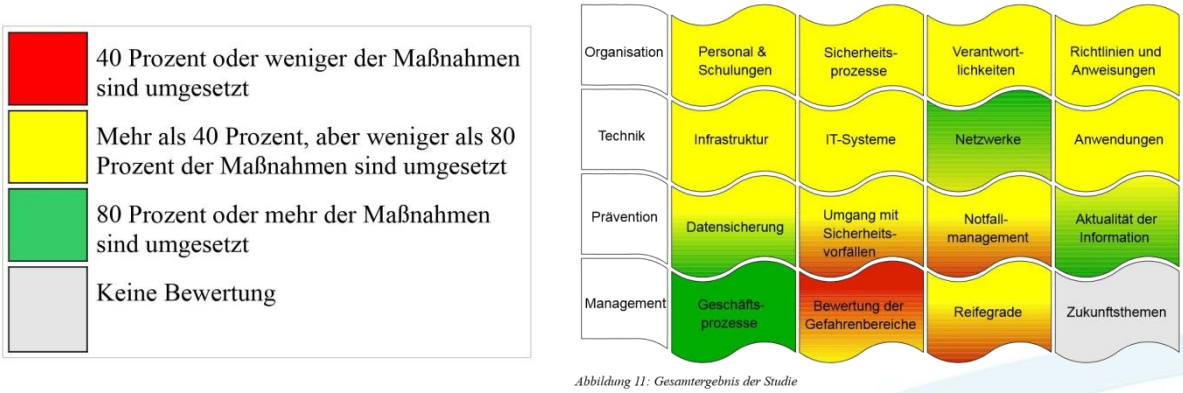


Abbildung 11: Gesamtergebnis der Studie

Quelle: BSI Sicherheitsstudie 2011

Ergebnis: In den Themengebieten Bewertung von Gefahrenbereichen, Behandlung von Sicherheitsvorfällen und Notfallmanagement – **besteht sofortiger Handlungsbedarf!**

Ein Nichthandeln, Abwarten und Aussitzen kann verheerende Auswirkungen haben wie:

- **Störung des Geschäftsbetriebes bis hin zum existenzgefährdenden Stillstand**
- **Verlust des technologischen Vorsprungs**
  - Wirtschaftsspionage über Netzanbindungen, Laptops, PDAs und Mobiltelefone
  - Wissensabfluss durch Mitarbeiter (Zugriff auf Daten, Speichermedien, Wissensmanagement)
- **Verlust der Wettbewerbsfähigkeit**
  - Störung / Ausfall der Produktion durch Schadsoftware, fehlende Redundanzen von Hardware, fehlende Datensicherung
  - Störung / Ausfall der Kommunikation mit den Kunden, Zulieferern oder der internen Kommunikation (Web-Server Verfügbarkeit, E-Mail Verfügbarkeit, Ausfall des Online Support)
  - Einbußen bei der Produkt- / Dienstleistungsqualität (Verfügbarkeit von Netz, IT, Servern, Client für Lieferanten, Lagerhaltung, Auslieferung und Abrechnung)
  - Störung / Ausfall der gesamten IT (Datenverlust, Verlust der Datenintegrität)
- **Verlust der Finanzierung durch Banken**
  - Verschlechterung des Ratings bei fehlendem IT Konzept für Produktion, Controlling und Finanzsystem
  - Unzureichende Hard- und Softwarekonfiguration
    Verlust des Vertrauens der Banken in die Unternehmensleitung (Stichwort: KonTraG, Organisationsverschulden des Vorstandes / Geschäftsführers)

Sind Sie vorbereitet? Wir können helfen!

Prozesse müssen etabliert und technische sowie organisatorische Maßnahmen umgesetzt werden, um einen sicheren und anforderungskonformen Betrieb von IT Systemen in kleinen und mittleren Unternehmen herzustellen. Thematische Schwerpunkte sind vor allem **IT-Sicherheit**, **IT-Risikomanagement**, die zugehörigen **IT-Prozesse** und ein effektives **Notfallkonzept**.

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

powered by: ISIS 12 Informationssicherheit für den Mittelstand

apsec applied security

IT-Sicherheit für kleine und mittlere Unternehmen

ISIS12 – Die Lösung für kleine und mittlere Unternehmen

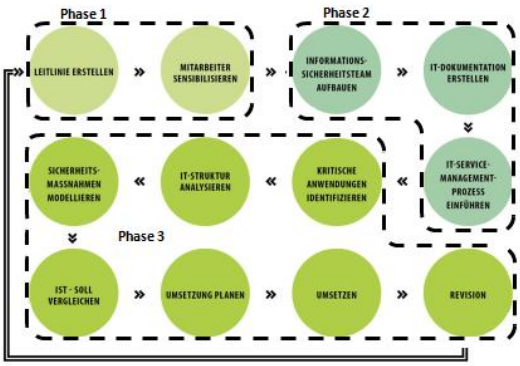
Stärken kombinieren und Vorhandenes nutzen

Der besondere Vorteil von ISIS12 in Bezug auf den Einsatz bei KMU entsteht durch die **konzeptionelle Verbindung der Stärken verschiedener Rahmenwerke**.

Die umfangreichen Maßnahmen der BSI IT-Grundschutzkataloge wurden mit Blick auf die Zielgruppe **reduziert, zusammengefasst und vereinfacht** und ergeben mit den ausgewählten, eher abstrakten, aber strukturierenden Elementen aus der ISO/IEC 2700x einen **klaren, konkret anzuwendenden Leitfaden**.

Die ebenfalls erfolgte Integration der aus der ITIL stammenden IT-Service-Management-Prozesse und der im ISIS12 Vorgehensmodell definierte PDCA-Prozess, führen dann im Ergebnis zu **einem nachhaltigen und dokumentierten Managementansatz** auf strategischer und operativer Ebene.

Aufgrund der in aller Regel bereits vorhandenen, umfangreichen Regelungen und Dokumentationen in den Unternehmen zu den einzelnen Bausteinen, kann eine ISIS12 Implementierung in kleinen und mittleren Unternehmen mit **akzeptablem Aufwand und Ressourceneinsatz und ohne lange Projektlaufzeiten umgesetzt werden.**



Das ISIS12-Vorgehensmodell wurde in drei Grobphasen aufgeteilt. Vor den eigentlichen operativen Schritten, der Entwicklung der Sicherheitskonzeption (Phase 3), gilt es nach der Initialisierungsphase, zuerst die für den weiteren Verlauf notwendigen Voraussetzungen zu schaffen.
Das Vorgehensmodell orientiert sich zwar an der bewährten BSI Grundschutzmethodik, ist aber dennoch ein neuer, für den Mittelstand und Organisationen entwickelter Ansatz.

Zertifizierung macht das verantwortungsbewusste Handeln der Geschäftsleitung nach außen sichtbar

Sobald Sie ISIS12 erfolgreich in Ihrem Unternehmen eingeführt haben und der Schritt 12, die Revision abgeschlossen ist, können Sie sich **von der DQS als Exklusivpartner nach ISIS12 zertifizieren lassen**. Das Zertifikat hat eine Gültigkeit von drei Jahren. In diesen drei Jahren finden zwei Überwachungsaudits statt. Im dritten Jahr kann durch eine Rezertifizierung das Zertifikat neu erteilt werden.

IHR NUTZEN

ISIS12 – **Mindeststandard** für ein **Informationssicherheits-Managementsystem** (ISMS)

ISIS12 – **baut auf bestehende Strukturen im Unternehmen auf**

ISIS12 – ist **überschaubar**, **schlank** gehalten und ein **verständlich** beschriebener 12-stufiger Prozess für die Etablierung eines ISMS

ISIS12 - **eigenständiger Betrieb problemlos möglich!**

ISIS12 – **orientiert sich an ISO 27001/BSI Grundschutz** mit einem speziell für den **Mittelstand angepassten**, auf **unternehmenskritische Anwendungen konzentrierten Maßnahmenkatalog** und kann als **Vorstufe zur ISO/IEC27001- bzw. BSI IT-Grundschutz-Zertifizierung** verwendet werden

ISIS12 – enthält **klar formulierte Anweisungen**, auch zur **IT-Dokumentation** und zum **IT-Service Management** (ISMS und IT-SM werden im Managementprozess integriert)

ISIS12 – **beinhaltet Datenschutz- und Notfallmanagement**

ISIS12 – **werbewirksam zertifizierbar** durch die DQS – Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

Applied Security GmbH • Einsteinstraße 2a • 63868 Großwallstadt
www.apsec.de • info@apsec.de • Fon: +49 (0) 60 22 / 263 38-0

powered by: ISIS 12 Informationssicherheit für den Mittelstand apsec applied security