

IT SECURITY

Datenschutz, Informationssicherheit und IT-Service-Management sind besonders bei kleinen und mittleren Betrieben oft Stiefkinder. Hingegen Themen, die direkt mit dem Wertschöpfungsprozess zusammen hängen, sind überlebensnotwendig. So ist es nicht weiter verwunderlich, dass in Zeiten mit starken konjunkturellen Schwankungen die Belange der IT Sicherheit keine Priorität haben.

Dass diese dennoch unverzichtbar sind, bleibt unbestritten - lesen wir doch fast täglich über insolvente Firmen, haftende Geschäftsführer und entlassene Mitarbeiter. Verursacht durch riesige Sicherheitslücken oder mangelhafte IT-Prozesse im Unternehmen. Wir sind davon überzeugt, dass Sie als Geschäftsführer oder Abteilungsleiter für diese Themen bereits „sensibilisiert“ sind.

Wir möchten Ihnen unsere Vorgehensweise näher bringen, wie Sie Ihre Informationstechnologie auf lange Sicht sicher und wettbewerbsfähig machen können.

KONTAKT



Comgroup GmbH
Industriepark Würth
Drillberg 6
97980 Bad Mergentheim

Tel. +49 7931 91-6400
Fax +49 7931 91-6401

info_d@comgroup.de
www.comgroup.de

Ansprechpartner:

Matthias Möhring
Tel. +49 170 6337701
matthias.moehring@comgroup.de

Michael Tomas
Tel. +49 7931 91-6570
michael.tomas@comgroup.de



IT SECURITY

**Datenschutz
Informationssicherheits-Management
Zertifizierung nach ISO 27001**

IT SECURITY



MEMBER OF THE WÜRTH  GROUP

Externer Datenschutzbeauftragter

Das Bundesdatenschutzgesetz (BDSG) schreibt vor, dass Unternehmen, bei denen zehn oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten bestellen müssen. Dieser steht für den Schutz allgemeiner Persönlichkeitsrechte von Mitarbeitern und Kunden. Als Voraussetzung für diese Aufgabe beschreibt das Bundesdatenschutzgesetz juristische sowie organisatorische Kenntnisse, didaktische Fähigkeiten und IT Kenntnisse. Neben diesen Voraussetzungen ist noch zu beachten, dass aufgrund der sonstigen betrieblichen Aufgaben keine Interessenskonflikte auftreten dürfen. Sie können als Unternehmen einen internen Mitarbeiter mit dieser Aufgabe betrauen. Häufig ist es jedoch so, dass aus ökonomischen Gesichtspunkten die Bestellung eines externen Datenschutzbeauftragten bevorzugt wird. So können interne Interessenkonflikte ausgeschlossen sowie eine Garantie der Rechtssicherheit gewährleistet werden.

Wir übernehmen für Sie folgende Aufgaben:

- ▶ die Beurteilung organisatorischer und technischer Abläufe hinsichtlich datenschutzrechtlicher Anforderungen
- ▶ die Erstellung eines Datenschutzkonzepts
- ▶ die Erstellung des gesetzlich geforderten Verzeichnisses
- ▶ die Erstellung von Organisationsanweisungen und Richtlinien
- ▶ die Berichterstattung an die Geschäftsleitung
- ▶ die Beantwortung von Anfragen zum Datenschutz von Kunden und Mitarbeitern
- ▶ die Sensibilisierung und Schulung von Mitarbeitern.

Ihr messbarer Erfolg

- ✓ Ressourcen im Unternehmen freisetzen
- ✓ Schulungsaufwand minimieren
- ✓ eventuelle Interessenskonflikte umgehen
- ✓ Nutzung von juristischen Ressourcen

Die Novellierung des Bundesdatenschutzgesetzes:

Ab dem 1. September 2009 bzw. dem 1. April 2010 gelten geänderte Bestimmungen hinsichtlich des Datenschutzes:

- ▶ Es gibt erhöhte Anforderungen an die Auftragsdatenverarbeitung
- ▶ die personalisierte Werbung wird eingeschränkt
- ▶ es gelten erhöhte Transparenzpflichten bei automatisierten Einzelentscheidungen
- ▶ es gibt einen umfassenden Kündigungsschutz für den betrieblichen Datenschutzbeauftragten
- ▶ die Rechte der Aufsichtsbehörden wurden erweitert
- ▶ der Bußgeldrahmen wurde angehoben.



Informationssicherheits-Management

Alle reden über Informationssicherheit. Mit der weltweiten Vernetzung von Firmen, Standorten, Ländern und sogar Kontinenten steigen nicht nur Chancen, sondern auch Risiken. Zunehmende Komplexität und Unübersichtlichkeit der Strukturen sorgen dafür, dass die elektronische Geschäftswelt für Bedrohungen sehr anfällig geworden ist. Gegenmaßnahmen sind meist schlecht aufeinander abgestimmte Insellösungen.

Durch unsere ganzheitliche Betrachtungsweise schaffen wir einen deutlichen Mehrwert, gerade für kleinere und mittelständische Unternehmen. Unter "ganzheitlich" verstehen wir, dass nicht ausschließlich die Informationstechnologie eines Unternehmens betrachtet wird, sondern auch deren physikalisches Umfeld, die organisatorische Einbettung sowie die Dokumentation.

Im Vordergrund stehen für uns Begriffe wie Kostenoptimierung, hohes Sicherheitsniveau, individuelle Sicherheitsbedürfnisse, einfache Bedienbarkeit, Flexibilität und Erweiterbarkeit. Dies macht das Management von Informationssicherheit nicht nur schlank sondern auch lebbar.

Unternehmerisches Handeln ohne Risiken ist nicht möglich. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hat durch die Änderung des §91 AktG (das übrigens auch auf GmbH's angewandt wird) die Verpflichtung des Vorstands, für ein angemessenes Risikomanagement und für angemessene interne Revision zu sorgen, explizit formuliert und damit

auch zwei wichtige Attribute eines Information Security-Management-Systems beschrieben. In der Regel wird das Thema Information Security an qualifizierte Mitarbeiter delegiert. Die Verantwortung bleibt jedoch allein bei der Geschäftsleitung.

Wege zur Informationssicherheit

▶ Security Checks

Bei unseren „Security Checks“ werden sicherheitsrelevante Bereiche auf Schwachstellen analysiert und gegebenenfalls Lösungsmöglichkeiten erarbeitet. Da wir Informationssicherheit ganzheitlich betrachten, werden hierbei auch Themen berücksichtigt, die nur indirekt mit der Informationstechnologie zusammenhängen. Somit könnten relevante Themen nicht nur Computer und Netzwerke sondern auch bauliche Absicherung oder etwa Notfallpläne sein.

▶ Security Training

Im „Security Training“ bieten wir Aus- und Weiterbildung auf dem Gebiet der Informationssicherheit. Zu den Teilnehmern gehören Sicherheitsbeauftragte und Sicherheitsmanager oder auch interessierte Neueinsteiger. Verständlicherweise ist die Herstellung und Aufrechterhaltung einer umfassenden Informationssicherheit ein unternehmensweiter Prozess.

Im Anschluss an diese Seminare verfügen die Teilnehmer über die Fähigkeit, ein Informationssicherheits-Management



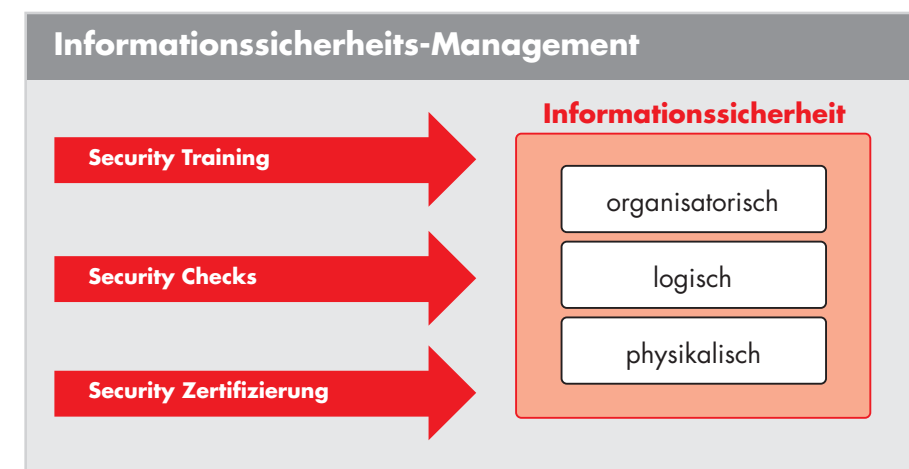
Ihr messbarer Erfolg

- ✓ Sensibilisierung für Sicherheitsdefizite
- ✓ Risikoanalyse der Geschäftsprozesse
- ✓ Erhöhung des Sicherheitsniveaus
- ✓ Kosteneinsparung durch Zentralisierung von Sicherungsmaßnahmen

mentensystem aufzubauen, auf eine eventuelle Zertifizierung vorzubereiten und anschließend aufrecht zu erhalten. Weitere Schwerpunkte des „Trainings“ sind Mitarbeiter-Coaching für Unternehmen, die dieses Sicherheits-Know-how nicht im eigenen Hause vorhalten wollen, bis hin zur Moderation von Security-Workshops, in denen Risikoanalysen oder Sicherheitskonzepte erarbeitet werden.

▶ Security Zertifizierung

Im Qualitätsmanagement ist es heutzutage üblich, dass Unternehmen ihre Prozesse nach ISO-Standard zertifizieren lassen. So gibt es auch im Sicherheitsmanagement standardisierte Zertifizierungsmöglichkeiten. Z.B. die ISO 27001 mit der Einführung eines systematischen Managements der Informationssicherheit in Unternehmen. Bei der Implementierung helfen unsere Einführungsseminare, in denen Strukturen und Verfahren der ISO 27001 erläutert werden. Dies ist insbesondere für Unternehmen ratsam, die eine Zertifizierung anstreben.



Zertifizierung nach 27001

Warum eigentlich die ISO 27001-Zertifizierung

Es gibt viele Standards, die sich mit dem Thema "Sicherheit" auseinandersetzen. Einer dieser Standards ist die ISO 27001 – Management von Informationssicherheit.

Durch eine Zertifizierung erlangen Unternehmen die schriftliche Bestätigung, dass Ihre Geschäftsdaten und -prozesse in einen ganzheitlichen Sicherheitsprozess eingebunden wurden. Zunehmend gilt die Zertifizierung eines Informationssicherheits-Management-Systems auch als Qualitäts-Zeichen und bietet somit dem zertifizierten Unternehmen einen nicht unerheblichen Wettbewerbsvorteil. Vor allem in der Automobil- und Pharma-Industrie, die in Deutschland eine Vorreiterrolle haben, geht der Trend verstärkt in Richtung Zertifizierung nach ISO 27001. Nicht zuletzt können zertifizierte Unternehmen auf Dauer Kosten einsparen, da durch die Zentralisierung von Absicherungsmaßnahmen bereits bestehende teure Insellösungen abgelöst werden können.

Der Weg zur Zertifizierung

Schritt 1: Workshop

Jedes neue Projekt braucht qualifizierte Koordinatoren und "Promoter". Daher beginnen wir ein Zertifizierungsverfahren stets mit einem Workshop, in dem den verantwortlichen Personen in Ihrem Unternehmen die Anforderungen aus der ISO 27001 sowie die Erwartungshaltung einer Zertifizierungsstelle näher gebracht werden.

Schritt 2: Risikoanalyse

Bei der strukturierten Risikoanalyse geht es darum, die materiellen und ideellen Werte Ihres Unternehmens zu erfassen und auf deren Schwachstellen hin zu analysieren. Die fruchtbaren Diskussionen, die sich bei diesem Schritt entwickeln, lassen meistens bereits im Vorfeld Schwerpunkte erkennen, die zukünftig angegangen werden sollen.

Schritt 3: Erkenntnisse umsetzen

Durch die gewonnen Erkenntnisse aus der Risikoanalyse lässt sich ein Maßnahmenplan entwickeln, der die Schwachstellen größtenteils beseitigt. Ein Restrisiko wird hier bewusst als fester Bestandteil unternehmerischen Handelns akzeptiert.

Schritt 4: Maßnahmen dokumentieren

Die Maßnahmen werden in einem Informationssicherheits-Management-Handbuch (ISMS-Handbuch) dokumentiert. Dieses Informationssicherheits Management-Handbuch dient später als Arbeitsgrundlage für Ihre Sicherheitskoordinatoren und ist die Basis für die Zertifizierung.

Schritt 5: Desktop Review

Beim Desktop Review wird das ISMS-Handbuch durch uns auf Konformität mit der ISO 27001 geprüft und bewertet. Die Abweichungen werden von uns in einem Abweichungsbericht erfasst und an Sie versandt.

Ihr messbarer Erfolg

- ✓ Schaffung von Wettbewerbsvorteilen
- ✓ Erhöhung der Unternehmenssicherheit: Logisch, physikalisch, organisatorisch
- ✓ Sensibilisierung für das Thema Informationssicherheit
- ✓ Erfüllung gesetzlicher Bestimmungen
- ✓ Nutzung von Optimierungspotenzialen

Schritt 6: Abweichungen beseitigen

Die beim Desktop Review festgestellten Abweichungen können Sie nun beseitigen. Sobald dies geschehen ist, steht einem Zertifizierungs-Audit nichts mehr im Wege.

Schritt 7: Audit

Ein Audit erfolgt in einer Mischung aus Interviews mit kompetenten Gesprächspartnern und persönlicher Betrachtung Ihrer Prozesse durch unsere Auditoren. Während beim Desktop Review lediglich die Dokumentenlage also der "Soll-Zustand" analysiert wird, so untersuchen wir während des Audits, ob dieser letztendlich der Realität entspricht also auch in Ihrem Hause "gelebt" wird.

Schritt 8: Abschluss Zertifizierung

Zum Abschluss der Zertifizierung erhalten Sie von uns eine akkreditierte Zertifizierungsurkunde als Nachweis für Ihr funktionstüchtiges ISMS. Selbstverständlich wird unsere Tätigkeit auch in einem Abschlussbericht dokumentiert, in dem wir alle Punkte festhalten. Auf diese Weise können Sie unsere Bewertungen jederzeit nachvollziehen.

