

Der externe IT-Sicherheitsbeauftragte

Dienstleistungsbeschreibung von BDG

<i>Version</i>	: 1.1
<i>Sensibilitätsstufe</i>	: öffentlich
<i>Autorname / Abteilung</i>	: S. Schänzer / BDG
<i>Erstellt am</i>	: 2006-08-16
<i>Freigabe durch</i>	: S. Schänzer / BDG
<i>Zuletzt bearbeitet am</i>	: 2006-10-02
<i>Status</i>	: Freigabe

BDG GmbH & Co. KG
Stolberger Strasse 307
50933 Köln
Tel. +49 (0)221 95 42 31-0
Copyright © 2006 by BDG GmbH & Co. KG

Dieses Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der BDG GmbH & Co. KG unzulässig und wird zivil- und strafrechtlich verfolgt. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Inhalt

1	Ausgangssituation	3
2	Aufgaben eines IT-Sicherheitsbeauftragten	4
3	Organisatorische Grundregeln	5
3.1	Organisatorische Einbindung	5
3.1.1	IT-Sicherheitsbeauftragter als Stabsstelle.....	5
3.1.2	IT-Sicherheitsbeauftragter als Teil der IT-Abteilung.....	5
3.1.3	Externer IT-Sicherheitsbeauftragter	6
4	Dienstleistung von BDG.....	7

1 Ausgangssituation

In Unternehmen mit IT gestützten Geschäftsprozessen gewinnen der Nachweis und die Aufrechterhaltung der Informationssicherheit eine immer größere Bedeutung. Nicht zuletzt verlangen zum Beispiel Basel II, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) und der Sarbanes-Oxley Act (SOX/SOA), dass die Unternehmensführung einen dokumentierten Nachweis über den Status und die Funktionen der Informationssicherheit im operativen Bereich erbringt. Für die Konformität wird ein funktionierender Prozess der Informationssicherheit benötigt, wie er für die erfolgreiche Umsetzung eines Informations-Sicherheits-Management-Systems (ISMS) erforderlich ist. Es ist entscheidend, dass die notwendigen organisatorischen Strukturen für Aufbau, Durchführung, Kontrolle und Anpassung des Sicherheits-Management-Prozesses geschaffen und aufrechterhalten werden.

Die Zertifizierung nach einem Standard wie ISO 27001 ist ideal für den Nachweis der Sorgfaltspflicht der Geschäftsleitung bei der Einhaltung der Informationssicherheit. Eine solche Zertifizierung setzt jedoch voraus, dass ein IT-Sicherheitsbeauftragter (häufig auch als Chief Information Security Officer, kurz CISO bezeichnet) von der Geschäftsführung bestellt wird. Obwohl die Bestellung eines IT-Sicherheitsbeauftragten, im Gegensatz zu einem Datenschutzbeauftragten, bisher noch nicht gesetzlich vorgeschrieben wird, empfiehlt sich der Einsatz eines IT-Sicherheitsbeauftragten selbst für kleinere Unternehmen auch dann, wenn eine Zertifizierung nach einem Standard zur Informationssicherheit nicht angestrebt wird.

Die Verantwortung für die Informationssicherheit eines Unternehmens liegt bei der Geschäftsführung. Ihre Aufgabe ist es, im Rahmen der kaufmännischen Sorgfaltspflicht, möglichen Schaden, der durch Einsatz der Informationstechnik entstehen kann, zu minimieren. Um hier konkrete Maßnahmen einzuleiten, die wirksame Umsetzung zu kontrollieren und damit auch der Sorgfaltspflicht nachzukommen, kann die Geschäftsleitung diese Aufgaben an einen IT-Sicherheitsbeauftragten delegieren.

Die Rolle des IT-Sicherheitsbeauftragten kann durch einen eigenen Mitarbeiter des Unternehmens oder durch einen externen Spezialisten übernommen werden. Die Erfahrung hat gezeigt, dass unternehmens-eigene IT-Sicherheitsbeauftragte in der Regel nicht immer über ausreichend Zeit und Know-How verfügen, um die ihnen übertragenen Aufgabe mit der gebotenen Sorgfalt zu erfüllen. Tatsächlich muss die Rolle des IT-Sicherheitsbeauftragten meistens nebenbei zum Tagesgeschäft wahrgenommen werden. Dies hat zur Folge, dass die Informationssicherheit letztendlich jedem Mitarbeiter selbst überlassen bleibt. Die IT-Mitarbeiter sind jedoch für rein funktionale Aspekte der Informationsverarbeitung im Tagesgeschäft zuständig und verfügen in der Regel nicht über das aktuelle Spezialwissen zur Informationssicherheit. Aus diesem Grund haben die IT-Verantwortlichen kaum die Möglichkeit nachzuprüfen, ob die Unternehmensrichtlinien zur Informationssicherheit eingehalten werden. Definierte Sicherheitsrichtlinien sind somit faktisch wirkungslos. Kommt es aufgrund eines solchen Misstandes zu einem Sicherheitsvorfall in der Informationsverarbeitung, kann die Geschäftsleitung für einen entstandenen Schaden persönlich haftbar gemacht werden.

2 Aufgaben eines IT-Sicherheitsbeauftragten

Die Aufgabe eines IT-Sicherheitsbeauftragten ist die Koordination aller IT sicherheitsrelevanten Maßnahmen eines Unternehmens. Der IT-Sicherheitsbeauftragte muss von der Geschäftsleitung mit der Erstellung und Durchsetzung der Security-Policy und eines Maßnahmenkatalogs beauftragt und ermächtigt werden. Er berichtet direkt an die Geschäftsführung.

Zu den Kompetenzen und Aufgaben eines IT-Sicherheitsbeauftragten gehören im Einzelnen:

- Weisungsbefugnis in Sicherheitsfragen,
- Zugriffsrecht auf alle sicherheitsrelevanten Informationen und Systeme,
- direkter Zugang zu den Mitarbeitern aller Ebenen (inklusive Geschäftsführung) bei sicherheitsrelevanten Ereignissen,
- Verantwortung für Erstellung und Pflege der Security-Policies,
- Information aller für die IT-Sicherheit verantwortlichen Personen (Security Management Team) und damit der Leitungsebene über die Integration und den Ablauf des IT-Sicherheitsprozesses,
- Kontrolle des sicherheitsrelevanten Informationsflusses von Anwendern und Projekten, sowie angemessene Integration dieser Informationen,
- Verantwortung und Übersicht über die Realisierung der ausgewählten IT-Sicherheitsmaßnahmen,
- Gestaltung von Ausbildungs- und Sensibilisierungsprogrammen für die Mitarbeiter,
- Gewährleistung der IT-Sicherheit im laufenden Betrieb (z. B. durch Prüfungen der Einhaltung von IT-Sicherheitsmaßnahmen),
- Leitung von Untersuchungen evtl. auftretender sicherheitsrelevanter Ereignisse.

Neben der Fähigkeit des IT-Sicherheitsbeauftragten Aufgaben zielgerichtet zu definieren und zu delegieren, muss ein IT-Sicherheitsbeauftragter Spezialkenntnisse auf dem Gebiet der IT-Sicherheit mitbringen und mehrjährige praktische Erfahrung auf diesem Gebiet vorweisen können.

3 Organisatorische Grundregeln

Damit die genannten Aufgaben erfolgreich erfüllt werden können, sollten gewisse organisatorische Grundregeln beachtet werden:

- Vermeidung von Rollenkonflikten (z.B. IT-Sicherheitsbeauftragter / Projektleiter / Administrator)
- Trennung der Funktionen von Datenschutzbeauftragtem und IT-Sicherheitsbeauftragtem (vermeidet eine Vermischung der Zuständigkeiten und ermöglicht eine gegenseitige Kontrolle)
- Klare Zuordnung der Verantwortlichkeiten, Kompetenzen und zur Verfügung stehenden Arbeitszeit.
- Verpflichtung zur Organisation und Nachweisführung (Führt zu klaren definierten Aufgaben und Verantwortlichkeiten, sowie nachvollziehbarer Entwicklung des IT-Sicherheitsniveaus)

3.1 Organisatorische Einbindung

Es gibt verschiedene Möglichkeiten, den IT-Sicherheitsbeauftragten in die Organisationsstruktur eines Unternehmens einzubinden. Jede Alternative hat ihre Vor- und Nachteile. Welche Alternative am besten geeignet ist, hängt von der Größe des Unternehmens, seiner Organisationsstruktur, den Prozessabläufen und den personellen Möglichkeiten ab.

Im Folgenden sind einige Möglichkeiten mit ihren Vor- und Nachteilen aufgelistet.

3.1.1 IT-Sicherheitsbeauftragter als Stabsstelle

Der IT-Sicherheitsbeauftragte hat eine Stabsfunktion außerhalb der Linie und berichtet direkt an die Geschäftsführung.

Vorteile

- Unabhängigkeit von der Fachabteilung
- Kontrollfunktion kann optimal und unabhängig wahrgenommen werden
- Direkter Zugang zur Geschäftsführung
- Keine operative Betriebsverantwortung

Nachteile

- Relativ weit vom operativen Tagesgeschäft und damit auch von den Prozessabläufen entfernt
- Informationssicherheit wird eher als etwas „Externes“ empfunden
- Position fördert Gegensätze statt Integration
- Nicht geeignet für kleinere Unternehmen

3.1.2 IT-Sicherheitsbeauftragter als Teil der IT-Abteilung

Der IT-Sicherheitsbeauftragte ist dem IT-Leiter unterstellt und nimmt ggf. noch weitere Funktionen im IT-Bereich wahr. Er ist in die täglichen Prozessabläufe und aktuellen Projekte häufig besser eingebunden und kann dadurch viele Themen der IT-Sicherheit früher und effektiver einbringen.

Vorteile

- Direkte Einbindung in Prozessabläufe
- Bessere Information über technische und organisatorische Abläufe
- IT-Security wird eher als integraler Bestandteil der IT wahrgenommen

Nachteile

- Position in der Linie schafft Abhängigkeit
- Abhängigkeit kann schnell zu Interessenskonflikten führen
- Kein direkter Zugang zur Geschäftsführung
- Keine ganzheitliche Prüfung der IT möglich, weil Prüfung des eigenen Vorgesetzten

3.1.3 Externer IT-Sicherheitsbeauftragter

Die Funktion des IT-Sicherheitsbeauftragten kann auch von externen Sicherheitsberatern übernommen werden. Dies bietet Unternehmen mit wenig personellen Ressourcen oder fehlendem Fachwissen die Möglichkeit, schnell und bedarfsgerecht kompetentes Berater-Knowhow einzusetzen.

Vorteile

- Unabhängigkeit und Neutralität durch externe Position
- Expertenwissen und Erfahrung aus anderen Unternehmen
- Kontrollfunktion kann optimal wahrgenommen werden
- Bedarfsabhängiger Einsatz möglich
- Entfall der Fortbildungskosten
- Entlastung eigener Ressourcen

Nachteile

- Relativ weit von Prozessabläufen entfernt
- IT-Security wird eher als etwas „Externes“ empfunden

4 Dienstleistung von BDG

BDG stellt Unternehmen auf Wunsch einen externen IT-Sicherheitsbeauftragten, der die Einführung und Aufrechterhaltung festgelegter Sicherheitsziele überwacht und mit vorantreibt. Gerade für kleine und mittelständische Unternehmen ist diese Möglichkeit eine kostengünstige Alternative, weil dadurch personeller Aufwand reduziert wird. Der externe Sicherheitsspezialist von BDG kann im Gegensatz zu einem Mitarbeiter des Kunden wesentlich konfliktfreier auftreten und somit die Sicherheitslage unabhängig und objektiv beurteilen. Die ständige Qualifizierung von IT-Sicherheitsspezialisten entfällt für den Kunden und er kann sich auf sein Kerngeschäft konzentrieren, ohne die Informationssicherheit im Unternehmen zu vernachlässigen. BDG setzt ausschließlich nachweislich qualifizierte Mitarbeiter als IT-Sicherheitsbeauftragte ein und sorgt durch eine fortgeführte Qualifizierung für eine Qualität der Dienstleistung auf höchstem Niveau. BDG bildet für die Verantwortlichen des Kunden einen Single-Point-of-Contact bei Fragen zur Informationssicherheit. Im Gegensatz zu einem unternehmensinternen Beauftragten, verfügt BDG über mehrere Sicherheitsspezialisten und kann so während der Geschäftszeiten eine ständige Verfügbarkeit eines Sicherheitsbeauftragten gewährleisten. D.h. auch im Krankheitsfall und während der Urlaubszeit steht ein kompetenter Ansprechpartner der Geschäftsleitung und den IT-Verantwortlichen zur Seite. Bei Bedarf kann über entsprechende Service Level Agreements auch eine ständige Rufbereitschaft eingerichtet werden. Ziele, Anforderungen und Aufgaben des externen IT-Sicherheitsbeauftragten werden im Vorfeld mit dem Kunden abgesprochen und in Form eines Pflichtenheftes verbindlich schriftlich fixiert, so dass eine klare Vereinbarung geschaffen wird, die dem Kunden eine transparente Leistungs- und Kostenkontrolle ermöglicht. Für BDG ist ein eindeutig definierter Auftrag selbstverständlich, da ein externer IT-Sicherheitsbeauftragter im Einzelfall haftbar gemacht werden kann, wenn er die vertraglichen Pflichten verletzt und dem Kunden dadurch ein Schaden entsteht.

Wie läuft die Zusammenarbeit mit einem externen IT-Sicherheitsbeauftragten ab?

In einem Vorgespräch werden die Aufgaben und Rahmenbedingung mit dem Kunden abgestimmt und in Form eines Lastenheftes festgehalten. Dieses Lastenheft bildet die Basis für ein durch BDG zu erarbeitendes Pflichtenheft, in dem die vertraglichen Pflichten und Rahmenbedingungen transparent und nachvollziehbar festgelegt werden. In der Regel erfolgt nach Auftragserteilung eine „Einarbeitungsphase“ des IT-Sicherheitsbeauftragten. In dieser Phase findet eine Ist-Aufnahme statt. Bei der Ist-Aufnahme werden alle geschäftskritischen IT-gestützten Prozesse identifiziert und bewertet. Anschließend findet eine Sichtung der vorhandenen Sicherheitsrichtlinien statt. Nach der Ist-Aufnahme wird entschieden, ob die Vorbedingungen für die Tätigkeit eines externen IT-Sicherheitsbeauftragten gegeben sind. Wesentliche Vorbedingungen neben der Unterstützung durch die Geschäftsleitung sind das Vorhandensein einer IT-Security-Policy, Risikoanalyse/-katalog und eines Maßnahmenkatalogs (z.B. in Form von Sicherheits- und Notfallhandbüchern). Falls die Vorbedingungen nicht erfüllt sind, kann BDG dem Kunden dafür gesonderte Angebote unterbreiten. Wurden die Vorbedingungen nach entsprechender Beauftragung durch BDG erbracht, verkürzt sich die „Einarbeitungszeit“ des IT-Sicherheitsbeauftragten erheblich.

Die Aufgaben, die ein externer IT-Sicherheitsbeauftragter von BDG übernimmt, hängen im Detail immer von den spezifischen Anforderungen der Verhältnismäßigkeit für das zu unterstützende Unternehmen ab. Generell übernimmt der externe Sicherheitsbeauftragte

- die Verantwortung für die Pflege und Verwaltung der Security-Policies,
- die Verantwortung für die Pflege und Verwaltung weiterer Sicherheitsdokumente (Notfall- und Sicherheitshandbuch),
- die Information aller für die IT-Sicherheit verantwortlichen Personen,
- die Überwachung des IT-Sicherheitsprozesses (Plan, Do, Check, Act),
- die Sicherstellung des Informationsflusses zwischen Mitarbeitern, IT-Verantwortlichen und Geschäftsführung,
- die Verantwortung und Übersicht über die Realisierung der ausgewählten IT-Sicherheitsmaßnahmen,

-
- die Prüfungen der Einhaltung von IT-Sicherheitsmaßnahmen,
 - die Leitung von Untersuchungen evtl. auftretender sicherheitsrelevanter Ereignisse,
 - die Gestaltung von Ausbildungs- und Sensibilisierungsprogrammen für die Mitarbeiter.

Die Aufgaben des externen Sicherheitsbeauftragten werden bei BDG in einem kleinen Team, bestehend aus mindestens zwei Sicherheitsspezialisten, wahrgenommen, um die nötige Verfügbarkeit sicherzustellen. Diese Sicherheitsspezialisten sind dem Kunden in jedem Fall namentlich und persönlich bekannt. Regelmäßig (meist zweimal im Quartal) findet ein Statusmeeting zwischen IT-Verantwortlichen und den externen Beauftragten der BDG beim Kunden vor Ort statt, um aktuelle Probleme und Änderungen, die Informationssicherheit betreffen zu besprechen. BDG liefert viermal im Jahr einen Quartalsbericht ab, der sowohl die IT-Leitung, wie auch die Geschäftsführung adressieren. Notwendige Tätigkeiten, die nicht als Bestandteil der Rahmenvereinbarung festgelegt wurden, werden durch den IT-Sicherheitsbeauftragten begründet und müssen von der Geschäftsleitung gesondert beauftragt werden.