



Vorsprung durch Sicherheit

Wie man mit Datenschutz seine Mitbewerber aussticht

In den vergangenen Jahren hat die Dienstleistungsbranche harte Einschnitte bei den Umsätzen und Margen hinnehmen müssen. Viele Callcenter-Dienstleister versuchen daher, ihr Profil zu schärfen, um sich am Markt besser zu positionieren.

Die Value Proposition¹ vieler Anbieter verspricht exzellente Qualität und umfangreiche Schulungskonzepte für Mitarbeiter, die beste und modernste technische Ausstattung, ausgeklügelte Controlling-Instrumente zur optimalen Steuerung der Einheit und zusätzliche Vorzüge aus dem Leistungs-Portfolio wie Beratung.

Aber reicht das wirklich aus, um sich von den Wettbewerbern abzuheben?

Eine hervorragende Möglichkeit, sich zu positionieren und sich wirklich vom Wettbewerb zu unterscheiden, ist der Bereich Datenschutz. Leider wird der Datenschutz in Deutschland noch immer sehr „stiefmütterlich“ behandelt, obwohl in den vergangenen Jahren immer wieder Skandale die Öffentlichkeit erschütterten. Die Gesetzgebung wurde verschärft und Verbraucher ebenso wie Auftraggeber sind kritischer hinsichtlich des Umgangs mit personenbezogenen Daten geworden. Insbesondere die Callcenter-Branche gerät zunehmend unter Druck, sich von den „schwarzen Schafen“ des Marktes zu distanzieren. Es gilt, das Vertrauen von Auftraggebern zu bewahren oder neu zu gewinnen.

„Eine wertvolle und vertrauensbildende Maßnahme ist die Implementierung eines so genannten Information-Security-Management-Systems² (ISMS) nach der DIN ISO/IEC 27001, der höchsten internationalen Zertifizierung im Bereich Datenschutz und Informationssicherheit.“, sagt Christian Sonntag, der heute als Berater für die ProfiTel Consulting tätig ist. Er blickt zurück auf mehr als fünf Jahre Erfahrung mit einer der komplexesten ISO-Normen, der DIN ISO/IEC 27001.

Auf die Frage, wie viel eine solche Norm an Wettbewerbsvorteil ausmacht, antwortet Christian Sonntag: „Wo ist der Return of Investment? Mal ehrlich, das kann keiner sagen! Aber aus Erfahrung kann ich bestätigen, dass dieses Siegel eine unheimliche Zugkraft auf potentielle Neukunden ausübt. Ich habe es selbst damals bei der Affinion International GmbH³ erlebt, wo ich die Verantwortung für den operativen Bereich hatte und verantwortlich für die Implementierung dieser Norm war. Man hat automatisch einen unwahrscheinlich großen Vertrauensvorsprung gegenüber der Konkurrenz. Das habe ich jüngst wieder bei meinem letzten Kunden bemerkt, bei dem ich diese Norm implementiert habe. So eine Zertifizierung stellt ein echtes Differenzierungs-Merkmal dar.“

Das stimmt, denn kaum ein Unternehmen der Callcenter-Branche besitzt eine Zertifizierung nach DIN ISO/IEC 27001. Es gibt nur wenige rühmliche Ausnahmen wie zum Beispiel die erwähnte Affinion International GmbH, ein Spezialanbieter für Kundenbindungsprogramme im Finanzdienstleistungssektor

oder die TAS⁴ aus Leipzig. Dabei eignet sich das Thema Datenschutz & Informationssicherheit wie kaum ein anderes, um es als Callcenter-Dienstleister vertrieblisch zu besetzen und zu nutzen. Denn der Umgang mit sensiblen Kundendaten gehört zum Tagesgeschäft. Ob beim Erfassen von Kundendaten in CRM-Systemen⁵, dem Empfangen und Aufbereiten von Daten oder bei der Eingangspost- und Response-Verarbeitung. Überall spielen digitale oder physische Daten eine Rolle. Und in kaum einer Branche kommen so viele Systeme und Programme zum Einsatz, die alle eine potentielle Gefahrenquelle sind.

Für viele Unternehmen der Callcenter-Branche wird Datenschutz zum existenziellen Thema. „Insbesondere die Callcenter-Dienstleister sollten alles dafür geben, die ihnen anvertrauten Informationen Dritter bestmöglich zu schützen.“, erklärt Christian Sonntag. „Das gilt speziell für die operativen Bereiche, in denen zur Auftragsabwicklung mit Fremddaten gearbeitet wird.“

Die Norm ist erstmals 2005 erschienen und aus dem „British Standard“ BS 7799-2 hervorgegangen. Sie ähnelt sehr stark dem IT-Grundschutz-Standard nach BSI. „Im Kern steht der Aufbau eines ISMS (Information-Sicherheits-Management-Systems).“, erklärt Sonntag. „Das ISMS ist ein umfassendes Management-Tool, um Risiken, Schwachstellen und Sicherheitszwischenfälle

zu analysieren, zu bewerten und zu managen und angemessene Gegen- und Korrekturmaßnahmen zu ergreifen. Dabei soll das ISMS auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfbarkeit, Instandhaltung sowie kontinuierliche Verbesserung der Informationssicherheit abdecken.“

■ LEIDER WIRD DER DATENSCHUTZ IN DEUTSCHLAND NOCH IMMER SEHR „STIEFMÜTTERLICH“ BEHANDELT

■ SO EINE ZERTIFIZIERUNG STELLT EIN ECHTES DIFFERENZIERUNGS-MERKMAL DAR

■ FÜR VIELE UNTERNEHMEN WIRD DATENSCHUTZ ZUM EXISTENZIELLEN THEMA

1: engl. für Nutzenversprechen oder Wertversprechen

2: Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrecht zu erhalten und fortlaufend zu verbessern.

3: Pionier, Marktführer und Full-Service-Anbieter im Bereich des Mehrwert-Marketing

4: Dienstleister für ganzheitliches Dialogmarketing

5: Dies sind Applikationen, Softwarelösungen und Computerprogramme, die als primäres Ziel haben, Unternehmen bei der Umsetzung von mehr Kundenorientierung und Kunden-Beziehungs-Management zu unterstützen.

■ STRATEGISCH KLUG AGIERT DAS UNTERNEH- MEN, WELCHES SICH IN PUNCTO DATENSCHUTZ UND INFORMATIONSS- SICHERHEIT RECHTZEITIG POSITIONIERT

Dabei geht es in den Richtlinien der ISO-Norm und des ISMS nicht nur um den Schutz personenbezogener Daten, sondern vielmehr um eine ganzheitliche Betrachtung des Themas Sicherheit. „Von den Anforderungen der Dokumentation über die Risikobewertung und den Plan der Risikobehandlung, der Klassifizierung von Daten und Informationen, dem Umgang mit Bedrohungen und Schwachstellen, Personalthemen und dem großen Bereich der IT-Themen bis hin zur physischen Sicherheit, dem Management von Zwischenfällen, Notfallplanung und einigen anderen rechtlichen Themen wie z. B. dem Urheberrecht regelt die Norm sämtliche Betriebsabläufe.“, sagt Christian Sonntag. Mit ihren mehr als 130 Vorgaben zählt die Norm zu den umfassenden und komplexeren Regelwerken.

Für die Implementierung eines solch komplexen Management-Systems sollten in Abhängigkeit zur Firmengröße mindestens 12 bis 18 Monate eingeplant werden. Dabei spielt es auch eine große Rolle, welche Basis an Sicherheitsvorkehrungen und Change-Prozessen ein Unternehmen bereits mitbringt. „Klar, wenn ein Unternehmen schon über eine hervorragende IT-Organisation und erprobte Change-Prozesse verfügt und sich in der Vergangenheit bereits um sicherheitsrelevante Fragen gekümmert hat, ist dies ein enormer Vorteil bei der Implementierung.“, verrät Christian Sonntag. Letztlich sind dann „nur“ die Prozesse in Richtlinien, Policies und Arbeitsanweisungen zu dokumentieren. Neben der Dokumentation gilt es jedoch, die Prozesse zu verankern und in die Köpfe der Mitarbeiter zu bekommen. Die Mitglieder des Sicherheitskomitees, welches monatlich zusammenkommt, müssen sich aufeinander einspielen und eine gemeinsame Linie finden.

„Das Sicherheitskomitee besteht aus je einer Person pro relevanter Abteilung und befasst sich mit allen Fragen rund um das Thema Sicherheit. Es ist aber auch zuständig bei Bekanntwerden von Zwischenfällen. Dann hat es die Aufgabe, diese

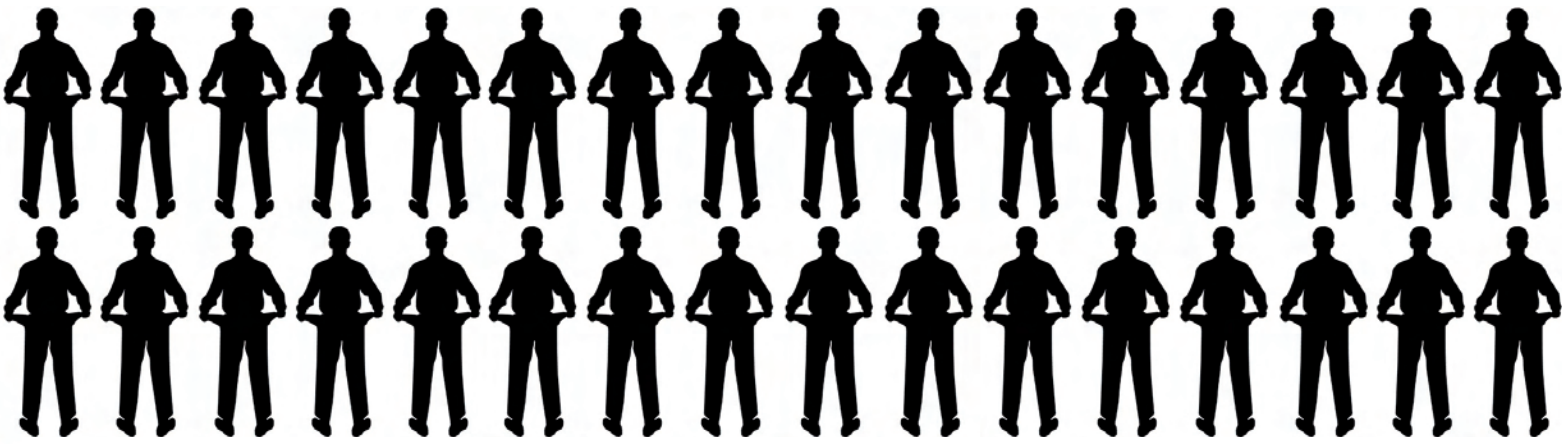
aufzuklären bzw. kurz- und langfristige Gegenmaßnahmen zu ergreifen, falls ein akutes Risiko für die Sicherheit besteht. Es beschäftigt sich mit der Auswertung und Messung der Effektivität des ISMS. Hierzu sind Kriterien festzulegen. In regelmäßigen Abständen können so die Geschäftsleitung und die Mitarbeiter über Trends und Entwicklungen der Sicherheit im Unternehmen informiert werden.“, so Christian Sonntag. „Kommunikation mit dem Team ist einer der wichtigsten Erfolgsfaktoren eines ISMS. Ohne interne Kommunikation und Training haben Sie nicht die Aufmerksamkeit und Wachheit der Mitarbeiter, um die ständig vorkommenden kleinen Zwischenfälle ans Tageslicht zu befördern. Und ohne externe Kommunikation haben Sie nicht die Aufmerksamkeit Ihrer potentiellen Neukunden. Also tue Gutes und sprich darüber! Dann zahlt es sich aus.“, schließt Sonntag mit einem Augenzwinkern.

Eines ist sicher: Das Thema Datenschutz und Informationssicherheit hat in den letzten Jahren an Bedeutung gewonnen. Immer mehr Unternehmen und Auftraggeber legen großen Wert darauf, ihre Kundendaten in einer sicheren Umgebung zu wissen. Gerade die Dienstleistungsbranche und im Speziellen die Callcenter, die massiv mit personenbezogenen Daten arbeiten, stehen auf dem Prüfstand und müssen ihre Sicherheit dokumentieren. Strategisch klug agiert das Unternehmen, welches sich in puncto Datenschutz und Informationssicherheit rechtzeitig positioniert. Ein vermeintlich kleiner Vorsprung zu Mitbewerbern, der sich angesichts der jüngsten Vertrauensverluste von Auftraggebern als Quantensprung in Sachen Wettbewerbsvorteil erweisen kann. ■

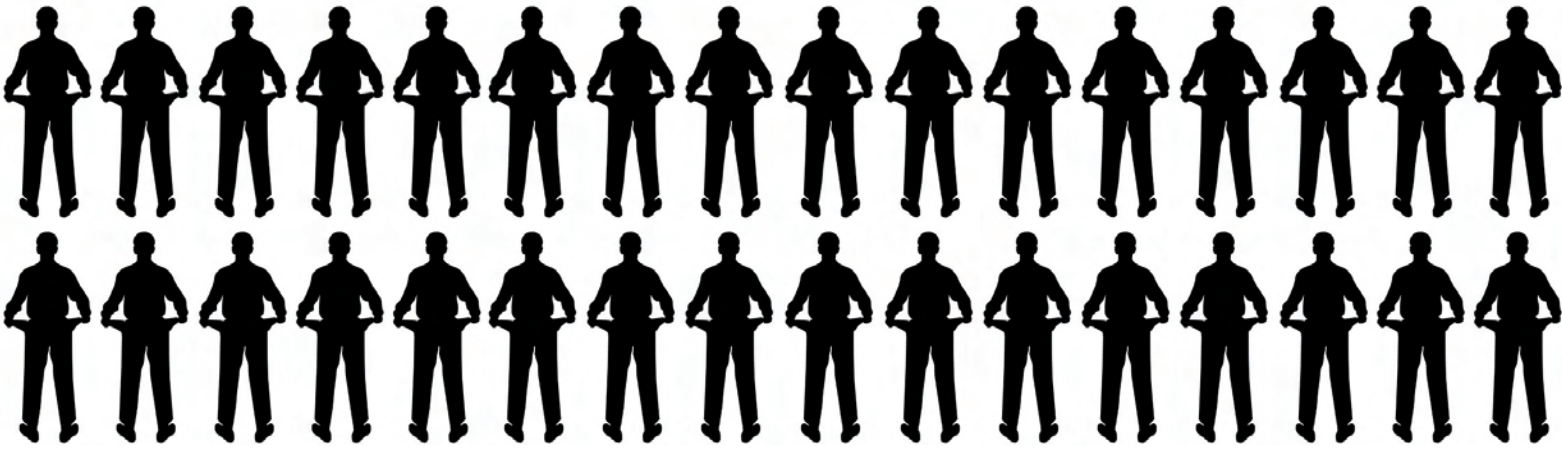


Christian Sonntag

Senior-Berater, profiTel consultpartner GmbH



**Wollen Sie viele, günstige Klicks
auf Ihre Google-Anzeigen?
Dann sind Sie bei uns falsch!**



**Wollen Sie Klicks von potentiellen Kunden?
Wir helfen Ihnen dabei!**



Wir holen das Beste aus Ihrem Budget heraus!

www.die-besserwisser.de

Spezialagentur für Suchmaschinenmarketing (SEM bzw. SEA)

