Durch Zertifizierung nach ISO/IEC 27001 die Sicherheitslücken schließen, Kunden überzeugen und dem Wettbewerb immer einen Schritt voraus sein

„Wenn wir nicht mit sicheren, standardisierten Systemen arbeiten, können wir Kunden verlieren. Deshalb haben wir uns für den Weg der Zertifizierung entschieden. Wir wollten optimale Verfahren schaffen und unseren Kunden aus der freien Wirtschaft und staatlichen Institutionen kommunizieren, dass wir der zuverlässige, ausfallsichere Partner sind."

Bill Millar,
Head of Security,
Infrastructure Outsourcing Services,
Capgemini UK

Kundenziele

- Verbesserte Sicherheit
- Schutz der Kundenvermögenswerte sowie der Ressourcen und der Mitarbeiter
- Bessere Wettbewerbsvorteile
- Glaubwürdige Zusicherung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen

Kundennutzen

- Verbesserte Sicherheit und hohe Glaubwürdigkeit für das Unternehmen Capgemini UK und seine Kunden
- Best-Practice-Nachweis (Zertifizierungsurkunde) für die Kommunikation an potenzielle und bestehende Kunden
- Erhöhtes Sicherheitsbewusstsein und Unterstützung in Management und Belegschaft
- Verbesserung von Sicherheitsdokumentation und -Reporting

Hintergrund des Kunden

Capgemini ist das größte Unternehmen für IT-Dienstleistungen in Europa und weltweit führend bei Beratung, Technologie, Outsourcing und Local Professional Services.

Das Unternehmen mit Hauptsitz in Paris besteht seit 45 Jahren als unabhängige Gesellschaft und ist in mehr als 40 Ländern und 100 Sprachen tätig. 2012 betrug der Umsatz 10,3 Mrd. Euro.

Warum die Zertifizierung?

Sicherheit ist ein wichtiger Baustein, von dem die gesamte Capgemini-Gruppe abhängt: Der Schutz der unternehmens- und kundeneigenen Vermögenswerte, von Ressourcen und Menschen ist letztendlich auch ein Wettbewerbsvorteil.

Zu den wichtigsten Sicherheitsrisiken gehören traditionelle Bedrohungen wie Unfälle, Naturkatastrophen und Angriffe von Hackern auf Computersysteme, aber auch neue „Bedrohungen" wie erhöhte staatliche Regulierung und strengere Anforderungen der PIN-Card-Branche.

Bill Millar, Head of Security für das Geschäft Infrastructure-Outsourcing-Dienstleistungen von Capgemini in Großbritannien erklärt, „Wenn wir die Vorschriften nicht erfüllen, riskieren wir hohe Geldbußen und gehen Gefahr, unser Image nachhaltig zu schädigen. Sicherheit ist auch für unsere Kunden ein wichtiges Thema geworden. Wenn wir nicht mit robusten Systemen arbeiten, können wir Kunden verlieren. Deshalb haben wir uns für den Weg der Zertifizierung entschieden. Wir wollten optimale Verfahren schaffen und unseren Kunden aus der freien Wirtschaft und staatlichen Institutionen kommunizieren, dass wir der zuverlässige, ausfallsichere Partner sind."

Millar identifizierte eine Reihe von Maßnahmen, die von Capgemini UK ergriffen werden mussten, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen und die Geschäfte erfolgreich zu führen. Er legte fest, dass diese Maßnahmen pragmatisch, geschäftsorientiert, risikobasiert, ganzheitlich, systematisch und kosteneffizient sein müssen sowie sich nach den Vorschriften des Kunden oder von Capgemini richten sollten.

Unter Berücksichtigung dieser Überlegungen strebte das Unternehmen eine Zertifizierung nach der Informationssicherheitsnorm ISO/IEC 27001 an, die eine umfassende Herangehensweise an Informationssicherheit bietet.

Vorteile

Capgemini UK berichtet über eine Reihe von Vorteilen durch die Zertifizierung nach ISO/IEC 27001, einschließlich verbesserter Sicherheit für das Unternehmen und seine Kunden, Zusicherung von Best Practices gegenüber neuen und bestehenden Kunden, verbessertes Sicherheitsbewusstsein und Begeisterung unter den Mitarbeitern und Verbesserung von Sicherheitsdokumentation und -Reporting.

Sicherheit hat nun auch auf Vorstandsebene einen hohen Stellenwert, führt zu operativer und finanzieller Unterstützung und macht das Thema zu einem wichtigen Bestandteil des Outsourcing-Geschäfts von Capgemini UK. Laut Millar geht es vor allem „nicht nur darum, auf Daten aufzupassen, sondern sich auch um Menschen und physische Sicherheit zu kümmern – es ist nicht nur etwas für Technikfreaks."

Er fügt hinzu: „Mit den Vorteilen, die wir durch die Zertifizierung haben, sind wir sehr zufrieden. Unsere Kunden freuen sich, dass sie nicht selbst externe Auditoren beauftragen und bezahlen müssen – sie nutzen unsere Berichte von BSI, um sich von der Qualität unserer Sicherheit zu überzeugen."

Umsetzung

Die niederländischen und indischen Niederlassungen von Capgemini waren die ersten, die die Informationssicherheitsnorm ISO/IEC 27001 eingeführt haben und „sie haben daraus klare Vorteile gezogen", sagt Millar. Bei der Erstellung von Angeboten beispielsweise haben die Standorte in Großbritannien laut Millar „bei jedem Anlass unzählige Seiten Papier produziert und viel Zeit und Geld dafür aufbringen müssen, unsere Informationssicherheitsnachweise zu belegen. Unsere Kollegen in Übersee haben einfach nur die Nummer ihres ISO/IEC 27001 Zertifikats angegeben. Nicht zuletzt deshalb entschlossen wir uns für die Zertifizierung, damit die Mitarbeiter wieder für andere Tätigkeiten zur Verfügung stehen."

Anfang 2008 hatte Millar dann einen Business Case zusammengestellt, um die notwendige Investition zu begründen, und im Februar desselben Jahres bekam er die Zustimmung des Vorstands, sowohl für die Finanzierung als auch für die Unterstützung. „Es war recht einfach. Der Vorstand fragte tatsächlich, warum wir das nicht schon lange tun", sagt er. Als Kontrollstruktur für das Projekt verwendete er das eigene UK Security Forum von Capgemini, gesponsert vom Chief Financial Officer des Unternehmens, und stellte ein engagiertes Zwei-Personen-Team ein.

Zunächst wurde der Risikoansatz des Unternehmens definiert, dann begann die Kommunikation mit Mitarbeitern und die Gewinnung von Unterstützung durch die Account Leads. Anschließend brachte das Team seine Sicherheitsdokumentation auf den neuesten Stand und fügte neue Bereiche wie z. B. Mobile Security hinzu. Zuletzt startete das Team einen Durchlauf mit Sicherheitsaudits und deckte systematisch die ursprünglich abgegrenzten Bereiche ab.

Die Rolle von BSI

„BSI war von Anfang an durch Beratung zum Umfang des Projekts eine große Hilfe. Es wurde uns vorgeschlagen, den Umfang zu verringern und die Aufgabe 'stufenweise' anzugehen, was sie viel leichter zu bewältigen machte", sagt Millar. „Nachdem wir BSI als Auditor ausgewählt hatten, empfanden wir den Ablauf tatsächlich als sehr unkompliziert, was dann immer noch einen großen Arbeitsanfall bedeutete, jedoch wesentlich strukturierter und unkompliziert."

Er erklärt weiter: „Das externe Audit durch BSI verlief reibungslos, weil wir unsere Hausaufgaben gemacht hatten. Es wurde an uns angepasst durchgeführt, wobei es unsere Hauptaufgabe war, sicherzustellen, dass vom Senior Manager bis zu den Technikern alle richtigen Personen für die Auditoren bereitstanden."

Im November 2008, nur zehn Monate nach dem Beginn des Projekts, gelangte die Outsourcing-Sparte von Capgemini UK an ihr Ziel: Ein nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem war erfolgreich etabliert. Seitdem hat das Unternehmen alle sechs Monate Überwachungsaudits durch BSI geplant und vorbereitet und 2011 eine Rezertifizierung durchgeführt. Zehn seiner 14 Standorte in Großbritannien werden mittlerweile von der Norm abgedeckt.

In Zukunft sind alle drei Jahre weitere Rezertifizierungen erforderlich, und mit der Zertifizierung der letzten vier britischen Standorte sowie der Aufklärung über die Vorteile von ISO/IEC 27001 in anderen Teilen der Gruppe außerhalb Großbritanniens, darunter Polen und Deutschland, sind neue Ziele gesetzt.

bsi.

+49 69 2222 8 9200
info.de@bsigroup.com
bsigroup.de

bsi. ISO/IEC 27001 Informations-sicherheits-management