

Der Mensch als Fehlerquelle



Stephan Spieckermann
Geschäftsleitung der
EOS Deutschland GmbH
T. 0 70 66 / 91 43 95 02
stephan.spieckermann@eos-ksi.de

Der zu laxer Umgang mit sensiblen Daten kann jedes Unternehmen in Schwierigkeiten bringen, wie diverse Datenschutzskandale bewiesen haben. Um mögliche Probleme zu vermeiden, sollten Sicherheitslücken aktiv und systematisch aufgespürt und geschlossen werden. Stephan Spieckermann, Geschäftsleiter bei der EOS Deutschland GmbH – Geschäftsbereich B2B, weiß wie dies gehen kann. Im Gespräch mit dem Credit Manager berichtet er über die Erfahrungen von EOS KSI mit der Zertifizierung nach ISO/IEC 27001.

CM: Wie wirkt sich die Zertifizierung nach ISO/IEC 27001 auf die tägliche Arbeit Ihrer Kunden aus und wie profitieren die Kunden von der Zertifizierung?

Spieckermann: Die Zertifizierung betrifft ausschließlich interne EOS KSI-Prozesse: Aus diesem Grund bemerken unsere Kunden in ihrem Tagesgeschäft keine direkten Auswirkungen – ebenso wenig wie man Airbags in einem Pkw bemerkt. Trotzdem profitieren unsere Kunden, denn durch unseren verantwortungsbewussten Umgang mit sensiblen Daten und Informationen vermeiden wir erhebliche Imageschäden und große Umsatzeinbußen sowie schwerwiegende Vertrauensverluste, die aus einem Datenskanal resultieren.

CM: Besteht die Gefahr, dass durch einzelne Maßnahmen die Qualität oder der „Fluss“ der Informationen leidet?

Spieckermann: Nein.

CM: Ist die Zertifizierung ein Wettbewerbsvorteil gegenüber anderen Dienstleistern? Wie ist das Feedback?

Spieckermann: An dieser Stelle würde ich gerne unsere Kunden zitieren. Alfred Stricker, Geschäftsführer HeidelbergCement Shared Services GmbH, erklärte: „Wir begrüßen die ISO-Zertifizierung unseres Geschäftspartners EOS KSI. Und hoffen, dass sich in der Finanzdienstleistungsbranche das Bewusstsein für die Notwendigkeit einer Zertifizierung weiter schärft – ähnlich wie in der produzierenden

Industrie, wo ein Nachweis über zertifiziertes Qualitätsmanagement mittlerweile zur Pflicht gehört und nicht zur Kür.“ Und der Geschäftsführer der Sonepar Deutschland Financial Services GmbH, Matthias Stobbe, sagte: „Wir legen sehr großen Wert auf die Sicherheit unserer Daten und arbeiten ausschließlich mit Dienstleistern zusammen, die unserem Anspruch gerecht werden. Aus diesem Grund schätzen wir die EOS KSI-Zertifizierung, denn sie stellt sicher, dass alle Mitarbeiter des Unternehmens kontinuierlich im sicheren Umgang mit sensiblen Daten geschult werden.“

CM: Können Sie exemplarisch aus Ihrer Sicht besonders „sensible“ Bereiche/Faktoren im Bereich Datensicherheit/Datenschutz benennen? Welches ist die wichtigste Maßnahme um mögliche Sicherheitslücken im System zu erkennen und zu schließen?

Spieckermann: Unser Informationssicherheitskonzept deckt alle relevanten internen Prozesse ab. Dazu gehören Gebäudesicherheit, Daten- und Dokumentensicherheit, EDV-Betriebsicherheit und Datenschutzrichtlinien sowie verbindliche Regelungen für unsere Mitarbeiter. Ich möchte zum Verständnis nachfolgend einige Details aufzeigen: Um umfassende Daten- und Dokumentensicherheit zu gewährleisten, ist unsere Dokumentenbibliothek mit verschiedenen Zugriffsrechten ausgestattet. Mitarbeiter, die lediglich über Leserechte verfügen, können beispielsweise keine Dokumente ändern – für das Ändern von Dokumenten werden

Autorenrechte benötigt. Diese Änderungen oder Ergänzungen werden anschließend durch Mitarbeiter mit Genehmigungsrechten freigegeben. Ein Versionsverlauf sorgt darüber hinaus für die nötige Transparenz und Nachvollziehbarkeit, wer wann was geändert hat.

Dabei ist der „Faktor Mensch“ beim Thema Sicherheit der störanfälligste Bereich, denn in den häufigsten Fällen sind menschliche Fehler der Auslöser für Datenskandale. Aus diesem Grund gelten für alle EOS KSI-Mitarbeiter verbindliche Regelungen, die im Tagesgeschäft für die nötige Sensibilität in Bezug auf Datensicherheit sorgen: Neben einer Bildschirmsperre, die sich automatisch aktiviert, ist jeder Mitarbeiter verpflichtet, beim Verlassen seines Arbeitsplatzes seinen Bildschirm aktiv zu sperren – diese Regelung stellt sicher, dass sensible Daten und Informationen noch nicht einmal für kürzeste Zeit zugänglich sind. Außerdem sind Smartphones und Laptops durch einen Pin sowie einen zusätzlichen Code gesichert. Hinzu kommt die Regelung des leeren Schreibtisches: Alle Dokumente in Papierform oder auf Wechselmedien werden beim Verlassen des Schreibtisches eingeschlossen – dadurch werden unsere Mitarbeiter täglich daran erinnert, mit sensiblen Daten unserer Kunden sorgsam umzugehen. Des Weiteren führen sie vor der Bereitstellung von Daten und Informationen eine sorgfältige Legitimationsprüfung durch: Fordert ein Kunde z.B. telefonisch ein neues Passwort an oder bittet um die Zusendung von kundenspezifischen Unterlagen per Fax, so wird durch diesen Legitimationsprozess seine Identität überprüft und sichergestellt, dass sensible Daten niemals in falsche Hände gelangen. Die Zertifizierung ist ein kontinuierlicher Prozess und sensibilisiert unsere Mitarbeiter fortlaufend, um die ständige Einhaltung der strengen EOS KSI Sicherheitsleitlinien zu gewährleisten.

CM: Wie lief der Zertifizierungsprozess ab?

Spieckermann: Nach der Beauftragung führte der TÜV Rheinland ein Audit mit einer detaillierten Prüfung von internen Prozessen und Nachweisdokumentationen durch und

führte umfassende Gespräche mit Mitarbeitern. Eine Risikoanalyse zeigte Risiken auf und bewertete diese. Auf dieser Grundlage wurden Verbesserungsmaßnahmen abgeleitet. Da unsere Prozesse seit 2007 durch QM definiert werden, mussten nur wenige Punkte optimiert werden – aktueller Hauptaugenmerk lag auf der Regelung informeller Prozesse sowie auf der Schaffung und Verstärkung von Überzeugung und Bewusstsein bei jedem einzelnen Mitarbeiter.

CM: Wie beurteilen Sie die MaDiC?

Spieckermann: Der verantwortungsbewusste Umgang mit Kundendaten sollte eine Selbstverständlichkeit sein – trotzdem häufen sich in letzter Zeit Informations- und Datenskandale auch bei bekannten Unternehmen. Das darf nicht sein! Und aus diesem Grund begrüßen wir alle Maßnahmen und Leitlinien, die auf eine sichere Handhabung von sensiblen Daten und Informationen abzielen.

Das Interview führte Alf Buddenberg.

