Der Einsatz von Informatikmitteln, und die elektronische Verarbeitung von Daten ist heute selbstverständlich und hilft der Hotelindustrie die Geschäftsprozesse zu automatisieren und Informationen für eine optimale Gästebetreuung zu erhalten.

Schon immer hatten Diskretion und der Schutz der Privatsphäre in der Hotellerie einen hohen Stellenwert. Mit dem Einsatz der Informatik stellt sich für alle eine neue Herausforderung die Daten und Informationen zu schützen.

Der Einsatz der Informatik erfordert ein Umdenken im Umgang mit dem Schutz von geschäftskritischen Daten. Während es für jedermann leicht verständlich und nachvollziehbar war, wie man vor 20 Jahren sensitive Dokumente und Daten durch Einschliessen schützte, hat sich die Fähigkeit den Schutz von Daten und Informationen in komplexen Informatikumgebungen sicherzustellen, auf einige wenige Experten reduziert.

Die Herausforderung in der Hotelindustrie

In der Hotelindustrie hat der Einsatz der Informationstechnologie enorm zugenommen und es existiert kaum mehr ein Geschäftsprozess, der nicht in irgendeiner Weise durch die Informatik unterstützt wird. Von der ersten Kontaktaufnahme, über den Aufenthalt bis hin zur Pflege der Kundenbeziehungen werden Daten gesammelt und bereinigt und in nutzbare Informationen gewandelt um schlussendlich als Hilfsmittel und Entscheidungshilfen für das Management zu dienen. Alles mit dem Ziel, einen effizienten, konkurrenzfähigen Betrieb und optimale Kunden- und Gästezufriedenheit sicherzustellen.

Durch die Tatsache, dass in der Vergangenheit verhältnismässig wenig Wert auf Sicherheit bei der Entwicklung und Einführung von Informatiksystemen in der Hotellerie gelegt wurde, besteht ein nicht unerhebliches Risiko, dass durch Informationssicherheitsverletzungen grosse Schäden entstehen können. Diese können finanzieller wie juristischer Art sein oder können sich negative auf das Image auswirken.

Die globale Vernetzung zu Fremdsystemen wie Reservationssysteme, Internet, E-Mail etc. sind weitere Elemente die die Komplexität und die Verwundbarkeit erhöhen. Ständig sich vergrössernde Speicherkapazitäten zu geringem Preis, eingesetzt in portablen Geräten, sowie die Tatsache, dass Softwarehilfsprogramme frei zur Verfügung stehen, können Missbräuche begünstigen. So kann man sich leicht vorstellen, dass bei Verfehlungen in der Vergabe von Zugriffsrechten oder durch „Hacking“ die komplette Datei aller Gäste eines grossen Hotels leicht innerhalb weniger Minuten auf einen „Mini Memory Stick“ kopiert werden kann. Solche Szenarien sind beängstigend, denn neben sensitiven Daten von Gästen würden auch mühsam und aufwendig erarbeitete Informationen in falsche Hände geraten. Oftmals können solche Sachen schwer verfolgt werden, da fast oder gar keine Spuren hinterlassen werden.

Informationen sind ein wichtiger Erfolgs- und Wettbewerbsfaktor für ein Hotel und müssen entsprechend geschützt werden muss. Informationen können in verschiedenen Formen existieren. Sie können unter anderem auf Papier gedruckt, elektronisch verarbeitet und gespeichert, verteilt auf elektronischem Weg oder per Post oder ganz einfach in der zwischenmenschlichen Kommunikation vorkommen. Ziel der Informationssicherheit ist das Sicherstellen von Vertraulichkeit, Integrität und Verfügbarkeit.

Eine Informationssicherheit wird erreicht, wenn ein entsprechendes Regelwerk eingeführt und praktiziert wird, welches aus organisatorischen wie auch technischen Massnahmen besteht. Alle Massnahmen jedoch werden Ihre Wirksamkeit verlieren, wenn die Informationssicherheit nicht von höchster Managementstelle unterstützt und gefördert wird.

Der ISO 17799 Standard

Ein guter Leiffaden um eine Informationssicherheit einzuführen, bietet der ISO Standard 17799. Der Standard hat seine Wurzeln in Großbritannien wo er 1995 als British Standard BS7799 entwickelt wurde und Empfehlungen zur Gestaltung eines Informations-Sicherheits-Management-Systems (ISMS) beinhaltete. Der Standard ist inzwischen international anerkannt als ISO 17799 und beinhaltet eine Reihe von Steuerungsbereichen (Controls) und Kontrollobjekten. (Control Objects), beides zusammen auch bekannt unter dem Ausdruck „ISO 17799, Code of Practice".

Zusätzlich zum ISO 17799 gibt es den British Standard BS 7799-2:2002 welcher neben dem „Code of Practice" zusätzlich die Spezifikationen für die Entwicklung, Einführung und Pflege eines Informations-Sicherheits-Management-Systems (ISMS) beschreibt. Unternehmen können sich nach diesem Standard zertifizieren lassen und dadurch folgende Ziele erreichen.

- Kunden können darauf vertrauen, dass ihre Informationen sicher und geschützt sind
- Die Kosten für einen Sicherheitsvorfall können beträchtlich sein. Die Zertifizierung reduziert durch regelmässige Kontrollen externer Personen das Risiko eines Schadenfalls.
- Mit der Zertifizierung demonstriert ein Unternehmen, dass die entsprechenden Gesetze und Verordnungen befolgt werden.
- die Zertifizierung zeigt das Engagement eines Unternehmens in diesem wichtigen Bereich.

Eine Zertifizierung, ist aber nicht zwingend notwendig, ausser der Markt oder die Kunden verlangen danach. In vielen Fällen ist die Einführung eines ISMS nach den Richtlinien des Standards ein guter Start, und eine Zertifizierung kann später in Erwägung gezogen werden.

Der Standard stellt 10 Steuerbereiche zur Verfügung. Darin eingeschlossen sind 30 Kontrollobjekte und insgesamt 127 Kontrollpunkte. Die gesamte Dokumentation des Standards ist auf dem Internet zu vernünftigen Preisen erhältlich. Nachfolgend sind die Steuerbereiche zusammengefasst.

1. Sicherheitspolitik: Darin werden die geforderte Unterstützung des Managements sowie die Anforderungen an das Entwickeln einer Security Policy definiert.

2. Organisation der Sicherheit: Gibt Hinweise über Organisationsformen, Verfahren und Methoden zum Betreiben eines ISMS. Das Verhalten zu Dritten (Outsourcing) ist darin ein wichtiger Punkt.

3. Einstufung und Wertung Informationswerte: Gibt Hilfestellung bei der Bestandesaufnahme (Inventar) und Klassifizierung von Informationen und Objekten.

4. Personelle Sicherheit: Beschreibt Massnahmen zur Minimierung von Risiken durch menschlichen Irrtum, Betrug, Missbrauch, Diebstahl. Die Ausbildung und die Bildung einer Sicherheitskultur innerhalb der Unternehmung sind wichtige Teile dieses Steuerbereiches.

5. Physische und umgebungsbezogene Sicherheit: Vorgaben und Richtlinien um den Zugang für Unberechtigte auf jegliche Art von Informationen und Einrichtungen zu verhindern.

6. Betrieb und Kommunikation: Darin werden Richtlinien für einen stabilen und sicheren Betrieb der Informationsverarbeitung gegeben. Die Minimierung des Systemausfallrisikos sowie die Sicherung von Informationen sind ebenfalls Bestandteil

dieses Steuerbereiches. Ein wichtiger darin beschriebener Teil ist der sichere Datenaustausch mit Partnern.

7. Zugriffskontrolle: Massnahmen um einen sicheren und kontrollierten Zugriff auf Daten, Informationen, Netzwerke, Anwendungen etc. zu gewährleisten. Besondere Aufmerksamkeit gilt der Informationssicherheit bei Mobilcomputing.

8. Systementwicklung und -wartung: Hinweise um sicherzustellen, dass bereits bei der Systementwicklung oder beim Kauf von Software auf Sicherheitsaspekte geachtet wird. Ebenfalls wird darauf eingegangen wie Sicherheitsaspekte bei Projekten und Supportaktivitäten berücksichtig werden sollen.

9. Kontinuierlicher Geschäftsbetriebs: Darin werden Hinweise gegeben wie vorbeugende Massnahmen gegen die Unterbrechung von Geschäftsprozessen eingeführt werden sollen. (Contingency Planning)

10. Einhaltung der Verpflichtungen: Darin wird beschrieben welche Massnahmen zur Vermeidung von Verfehlungen bei gesetzlichen oder vertraglichen Verpflichtungen getroffen werden sollen. Weiter werden die internen Pflichten beschrieben, um die Informationssicherheit zu gewährleisten. Es wird spezifiziert wie Audits durchgeführt werden sollen.

Zusätzlich zu den Steuerbereichen wird im Standard ausführlich darauf eingegangen wie das Management von Informationssicherheit aufgebaut werden muss und welche Prozesse dazu notwendig sind. Dazu gehören

1. Allgemeine Anforderungen an ein ISMS: Darin wird ausführlich beschrieben wie ein ISMS aufgebaut, eingeführt, unterhalten und ständig verbessert werden muss. Hinweise werden gegeben wie ein Risikomanagement aufgebaut werden soll, und wie die identifizierten Risiken behandelt werden müssen.

2. Management Verantwortlichkeiten: Dieser Teil regelt die geforderte Unterstützung durch das Management, sowie die Zuweisung von Ressourcen. Es wird beschrieben welche Anforderungen an die Ausbildung gestellt werden.

3. Konstante Überprüfung des ISMS: Eine klare Forderung besteht, dass die Wirksamkeit und Effizienz des ISMS regelmässig überprüft wird. Die dazu notwendigen Massnahmen sind beschrieben.

4. ISMS Verbesserungen: Darin werden Hinweise gegeben, wie eine ständige Verbesserung des ISMS durch die Einführung von korrektiven und präventiven Massnahmen sichergestellt werden kann.

Ein Schwerpunkt des Standards ist die Einführung eines Risikomanagement-Systems auf dessen Basis ein Unternehmen die entsprechenden Massnamen zur Risikobehandlung bestimmt.

Die identifizierten Risiken können dann einen typischen Risikomanagementprozess durchlaufen. Das heißt, sie werden an Hand von Wahrscheinlichkeit des Eintritts und Auswirkung im Fall des Eintritts bewertet. Für diese Risiken werden Massnahmen zur Risikominimierung gesucht. Die Maßnahmen mit der höchsten Effektivität und Kosteneffizienz sollen dann realisiert werden.

Zur Einführung eines ISMS für ein Hotel oder eine Hotelgruppe eignet sich der BS 7799-2:2002 ausgezeichnet als Leitfaden. Ohne ein systematisches Management der Informationen gibt es keinen wirksamen Schutz. Rund um den Standard gibt es weitere Leitfäden, die ergänzende Informationen zur Verfügung stellen. Mit dem Standard wird eine „Best Practice" Basis erreicht. Die Zertifizierung nach BS7799-2:2002 wird denjenigen Organisationen helfen, die Kunden darlegen möchten, dass Vertraulichkeit, Integrität und Verfügbarkeit von Informationen stets gewährleistet sind.

Die Spezifikationen und Empfehlungen in den Standards sind generell gehalten und haben für alle Industriebereiche Gültigkeit. Bei der Umsetzung ist darauf zu achten, dass die Vorgaben speziell auf die Hotellerie angepasst werden.

Aufbau eines ISMS in der Hotelindustrie

Für die Einführung eines ISMS empfiehlt sich das durchlaufen folgender Phasen

- Durchführen eines Audits nach dem BS 7799-2 Standard. Der Audit sollte sich über den ganzen Hotelbetrieb erstrecken. Damit werden die Lücken und Verfehlungen aufgezeigt. Ein solcher Audit kann durch einen Experten, mit 2-3 Tagen Aufwand, durchgeführt werden.

- Danach soll eine Risikoanalyse gemacht werden, an Hand derer dann die Massnahmen zur Minimierung des Risikos bestimmt werden. In dieser Phase wird auch bestimmt, welche Restrisiken ein Hotel gewillt ist zu tragen.

- Dann muss sich das Hotel mit der kontinuierlichen Einführung eines ISMS gemäss den Vorgaben des Standards befassen. Dies ist der Prozess der am meisten Resourcen und Zeit benötigt und kann nur bei voller Unterstützung des Managements erfolgreich sein.

- Abschliessend wird wieder ein Audit empfohlen, dessen Resultat verglichen mit dem Initial-Audit, den Fortschritt des Unternehmens bezüglich Informationssicherheit aufzeigen wird.

Der Aufbau eines ISMS ist keine einmalige Tätigkeit, sondern ein fortlaufender Prozess, der das erreichte Niveau sicherstellt und darüber hinaus verbessert. Das Ziel ist, den erreichten Sicherheitsstandard zu wahren, indem neuen Sicherheitsbedrohungen entgegnet wird.

Das Bewusstsein für Informationssicherheit in der Hotelindustrie ist noch nicht sehr weit fortgeschritten. Machen Sie den ersten Schritt und befassen Sie sich mit dem Thema. Informationssicherheit ist „Chefsache" und gehört zu den nicht delegierbaren Pflichten eines Managements. Die Kunden und Geschäftspartner werden es Ihnen danken.

Kontakt

Willi Tinner
Hotel Technology GmbH
Hagenbuchenstrasse 57
CH-8303 Bassersdorf
Telefon: +41 (0)43 537 18 69
willi.tinner@hoteltechnology.com
www.hoteltechnology.com