Management Bulletin

AUSGABE 09.2008

INHALT

Informationssicherheits-System auf hohem Niveau

EFKON wurde nach ISO 27001 zertifiziert

Information ist ein zunehmend bedeutender Produktionsfaktor. Die Funktionsfähigkeit und Verfügbarkeit der informationstechnischen Systeme und Netze sowie die Vertraulichkeit und Integrität der Geschäftsprozesse, Produktspezifikationen, Fertigungsverfahren und Daten sind vielfachen Gefahren ausgesetzt: Technische Fehler, Prozessfehler, Fehlverhalten, Sabotage, Spionage, Naturschäden, etc. Dies kann zu Imageverlust, wirtschaftlichem Schaden oder im Extremfall zur Gefährdung des Unternehmens, der Menschen und der Umwelt führen.

Um solchen Gefahren wirkungsvoll zu begegnen, hat das Management der EFKON AG die notwendigen organisatorischen, technischen und personellen Maßnahmen ergriffen.

Durch ein effizientes Informations-Management sollen auch die Kosten für die Informationssicherheit gesenkt und drohende finanzielle und Imageschäden vermieden werden.

Mittels einer erfolgreichen Zertifizierung des **I**nformations-**S**icherheits-**M**anagement-**S**ystems (ISMS) durch das Zertifizierungsinstitut SGS (siehe auch Seite 4) konnte von unabhängiger Stelle nachgewiesen werden, dass das eingeführte System dem Best Practice sowie internationalen Normen entspricht.

Um die Wirksamkeit des Systems und die laufende Weiterentwicklung sicherzustellen, werden jährlich externe Überprüfungsaudits durchgeführt.

Die globalen Informationssicherheitsziele von EFKON sind

- Hohe Verlässlichkeit des Handelns, insbesondere in Bezug auf Vertraulichkeit, Richtigkeit und Rechtzeitigkeit
- Gewährleistung des Vertrauens der Öffentlichkeit in das Unternehmen
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen

Für den Kunden bedeutet das, dass

- alle Informationen per System strengstens vertraulich behandelt und transportiert werden
- die informationsrelevanten Risiken im Unternehmen minimiert sind
- Informationen und IT-Systeme im höchsten Ausmaß verfügbar sind

Gegenstand der Informationssicherheit sind alle Arten von Informationen, insbesondere elektronische, schriftliche, mündliche, fernmündliche sowie E-mails, Telefaxe und Zeichen.

Dr. Helmut Rieder, CEO der EFKON AG und oberster Verantwortlicher des Information Security Management-Systems

Über einen Zeitraum von einem halben Jahr wurde das Informationssicherheitssystem von EFKON intensiv entwickelt und aufgebaut:

Das Management hat eine detaillierte Informationssicherheits-Politik diskutiert und verabschiedet. Von den IT-Zugangsregelungen, den physischen Zutrittskontrollen, der Need-to-know-Policy, den personellen Maßnahmen über die Vermeidung von Informationsmonopolen bis hin zum Business Continuity Management und der Notfallsplanung wurden alle wichtigen Sicherheitspunkte geregelt.

Ein wichtiges Element war auch die Einführung des Risikomanagements und die Durchführung einer tief greifenden Risikoanalyse. Anhand einer mehr als 300 Seiten langen Sicherheits-Checkliste wurden vorhandene Risiken identifiziert. Für jedes Risiko wurde ein Maßnahmenplan zum Abbau des Risikos erarbeitet und die Umsetzung dazu eingeleitet.

Um der Informationssicherheit im Unternehmen einen hohen Stellenwert zu geben und auf eine breite Basis zu stellen, wurde das **I**nformation **S**ecurity **C**ommittee ins Leben gerufen. Die Teilnehmer dieses regelmäßig arbeitenden und entscheidenden Gremiums sind Manager aller Bereiche und involvierte Mitarbeiter (IT, Personal, Recht, Systems & Products, Facility Management, etc.).

Die zentrale operative Verantwortung für das ISMS liegt beim Information Security Officer. Er koordiniert und kontrolliert das Sicherheitssystem und ist in dieser Funktion direkt dem Vorstand unterstellt.

Das CERT-Team (Computer Emergency Response Team) ist eine Gruppe von Mitarbeitern, die die Ursachen von sicherheitsrelevanten Vorfällen sehr zeitnah untersucht, diese aufzeichnet und Hilfestellung bei der Behandlung von sicherheitsrelevanten Vorfällen bietet.

Im Zuge der Einführung wurden unter anderem folgende Maßnahmen umgesetzt:

- **Organisatorische Maßnahmen:** Überarbeitung der Strukturen, Definition informationsrelevanter Prozesse und Kompetenzen, Erarbeitung von Sicherheitsregelungen und Arbeitsanweisungen, Umsetzung der definierten Policies, etc.
- **Personelle Maßnahmen:** Screening neuer Mitarbeiter, Sensibilisierung der Mitarbeiter, Schulung und Entwicklung, Missbrauchsvorbeugung, Kommunikation, etc.
- **Technische Maßnahmen:** Zutrittskontrollen, Überarbeitung der IT-Zugangsregelung und Zugriffe, technische Sicherheitsmaßnahmen, Gebäudetechnik, Maßnahmen bei Hard- und Software, Netzwerke und Kommunikation, Notfallspläne, etc.

Hermann Peitler,

Vorsitzender des Information Security Committee, QMB und Direktor Supply Chain Management

Dietmar Hager,

IT-Leiter und Information Security Officer von EFKON

Rainer Kornberger,

IT-Experte der Firma EFKON

Stefan Hochegger,

Quality Engineer und Leiter des CERT-Teams

Thomas Hediger,

Lead Auditor, ISO 27001 des Zertifizierungs-Unternehmens SGS

Heinz M. Hähnel Geschäftsführer der BSN

Begleiter beim Aufbau des ISMS-Prozesses

Damit alle Mitarbeiter fest in das Informations-Sicherheits-System eingebunden sind,

- haben die Mitarbeiter ein Schulungsprogramm durchlaufen, um sensibilisiert und informiert zu werden.

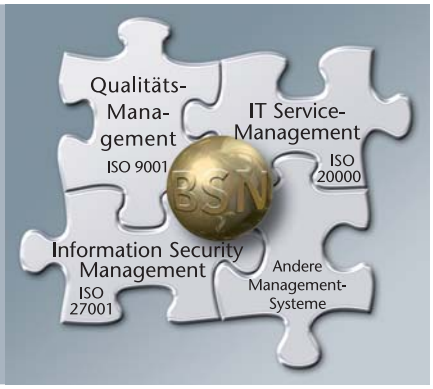
- wurde eine Intranet-Plattform erarbeitet, mittels der alle Mitarbeiter sämtliche notwendigen Informationen über das Unternehmen, die Regelungen, die Geschäftsprozesse und ISMS-Fragen im direkten Zugriff haben.

- wurde eine Informations-Vorfalls-Datenbank erstellt, in die die Mitarbeiter Informationsprobleme eintragen, die vom CERT umgehend bearbeitet werden. Aus Fehlern wird sofort gelernt.

„Ebenso wie beim bereits seit fünf Jahren etablierten Qualitäts-Management-System nach ISO 9001 wurde auch bei der Informationssicherheit der KVP (Kontinuierlicher Verbesserungs-Prozess) eingeführt und wird laufend erfolgreich praktiziert“ stellt Hermann Peitler, Leiter des Qualitätsmanagements, fest.

Der halbjährige Prozess zur Einführung des Informations-Sicherheits-Management-Systems ISMS wurde von dem für Österreich und die CEE-Länder zuständigen Geschäftsführer der BSN Business Solution Network unterstützt.

Nutzen auch Sie die Vorteile der internationalen Normen und Best Practice-Prozesse für Ihr Unternehmen?



Mit einer GAP-Analyse - in der Betriebswirtschaftslehre auch als Lückenanalyse bekannt - können wir schnell und effizient feststellen, inwieweit Sie die Vorteile der internationalen Normen und erfolgreichen Best Practice-Geschäftsabwicklungen zu Ihrem Vorteil nutzen.

Die GAP-Analyse zeigt auf, welche brachliegenden Ertragspotenziale vorhanden sind und wo bedrohliche Risiken bestehen. Nach einer Kurzanalyse erhalten Sie wertvolle Lösungsansätze zur Ertragssteigerung und zur Risikominimierung.

Wir werden Ihnen die Ansatzpunkte zeigen,

- **die Kosten zu senken**
- **die Qualität zu steigern**
- **die Effizienz zu erhöhen**
- **die Informationssicherheit zu garantieren**
- **und die Risiken zu minimieren**

Überprüft werden im Zuge der GAP-Analyse drei Management-Bereiche:

1 Qualitäts-Management

Zur Steigerung der Kundenorientierung, der kontinuierlichen Verbesserung Ihres Unternehmens und der Sicherstellung der Zielerreichung ist ein wirkungsvolles Qualitäts-Management erforderlich.

Wie ist die Einhaltung der definierten Qualität Ihres Unternehmens sichergestellt? Wie gut ist Ihr Qualitäts-Management-System? In der internationalen Norm ISO 9001 sind Qualitätsanforderungen definiert, die für die Sicherung, die Weiterentwicklung und die Profitabilität des Unternehmens wichtig sind.

Für Unternehmen, die bereits zertifiziert sind, liefert die externe GAP-Analyse wichtige Hinweise über Optimierungspotenziale. Unternehmen, die noch nicht zertifiziert sind, erhalten Hinweise auf vorhandene Verbesserungsreserven und wie diese gehoben werden könnten.

2 IT Service Management

Eine gut und sicher funktionierende IT mit seinen Services ist heute für den operativen Betrieb des Unternehmens zwingend notwendig.

Die internationalen ISO 20000-Normen und die ITIL-Prozesse geben klare Anforderungen an die IT Services in Ihrem Unternehmen als Best Practice vor.

Die GAP-Analyse zeigt Ihnen, wie weit Ihr Unternehmen die Normen erfüllt und wo es Ansatzpunkte für Verbesserungen gibt. Die Ergebnisse liefern Ihnen konkrete Vorschläge zur Verbesserung und Absicherung Ihres Unternehmens hinsichtlich der Information Technology.

3 Information Security Management

Es gibt eine Vielzahl von internen und externen Informations-Bedrohungspotenzialen und konkrete Gefahren.

Über Wirtschaftsspionage, Hacker, Viren, Einschleichung und interne Probleme wie fahrlässiger Umgang mit Informationen, Informationsverlust, interne Spionage, Ausfall von IT-Systemen, Elementarschäden, Wissensmonopole, unberechtigte Zugänge und Zutritte, etc. reicht die Palette der Informations-Sicherheits-Gefahren. In der ISO 27001 sind die Informations-Sicherheits-Anforderungen definiert. Alle Arten von Informationen sind dabei angesprochen: elektronische, schriftliche, mündliche und fernmündliche Informationen bis hin zu Signalen und Zeichen.

Die GAP-Analyse zeigt Ihnen auf, welchen ungeschützten Risiken und Gefahren im Informationsbereich im weitesten Sinne Ihr Unternehmen ausgesetzt ist.

Durchführung der GAP-Analyse

Die GAP-Analyse wird anhand eines Prüfinstrumentariums durchgeführt. Die Durchführung der Analyse vor Ort dauert – abhängig von der Unternehmensgröße, Komplexität und Lokalisierung – ein bis zwei Wochen. Im Abschlussbericht wird die aktuelle Situation dargestellt und Maßnahmen zur Verbesserung vorgeschlagen.

Nähere Informationen zur Durchführung der GAP-Analyse erhalten Sie von BSN Wien direkt durch unseren Geschäftsführer Herrn Hähnel (Tel +43-1-99460 6490).

Oder senden Sie uns einfach ein E-Mail an office@bsn-ltd.com.

Georg M. Stüttem
BSN-Geschäftsführer

Das BSN-Know-how-Netzwerk

Heinz M. Hähnel
BSN-Geschäftsführer

Netzwerk-Partner (Auszug):

- SGS Austria Controll-Co, Wien-Zürich, und 140 Länder
- BOC Information Technologies Consulting AG, Wien-Berlin-Madrid-Athen-Dublin-Warschau
- MS Marketing GmbH, Oelde
- CAPMEX Unternehmensberatung GmbH, Wien
- Ariadne Consulting Ltd, London-Wien
- LOeCON Management Consulting & IT Services GmbH, Wr. Neustadt
- Evelyn Stein, Kommunikations-Training, Breitenfurt
- Calice & Partners, London-Wien
- BPU s.r.o., Brno
- Lill Consult GmbH, Wien
- CFU C. Flock Unternehmensberatung GmbH, Wipperfürth
- my Vision Management Consulting GmbH, Wien
- Rechtsanwaltskanzlei Fruhstorfer + Günther, Wien
- BSN Business Solution Network Ltd, Birmingham-Oelde-Wien

Deutschland und Westeuropa:
Tel.: 0049-2529-948822, email: Georg.Stuettem@bsn-ltd.com

Österreich, CEE, andere Länder:
Tel.: 0043-1-99460-6490, email: Heinz.Haehnel@bsn-ltd.com

Internet: www.bsn-ltd.com

Kapitalmarktexperte: CAPMEX

CAPMEX ist eine unabhängige Unternehmensberatung, spezialisiert auf die Entwicklung des Finanzsektors mit speziellem Fokus auf Banken, Versicherungen, Kapitalmarktinstitutionen und Aufsichtsbehörden. Bis dato führte die CAPMEX erfolgreich 38 Projekte in 21 Ländern durch. Das CAPMEX VisionLab™ ist aktiv im Bereich Entwicklung neuer Produkte und Serviceleistungen. Training stellt bei allen Beratungsleistungen einen fixen Bestandteil dar, um die Nachhaltigkeit der von uns vorgeschlagenen und implementierten Lösungen zu gewährleisten. Auf Grund der großen Nachfrage werden verstärkt auch Beratungsangebote im Bereich Förderwesen und Unternehmens- sowie Projektfinanzierung angeboten.

Geschäftsführer
Hannes Takacs MBA

Österreich: Gabriela Jesacher

Veränderungen im Unternehmen sind immer spannende Herausforderungen.

Während die fachlichen Fragen oft gut konzipiert werden, ist die Umsetzung problematisch. Die Kunst der erfolgreichen Änderung im Unternehmen ist die Erzeugung der Akzeptanz bei den Leistungsträgern.

Hier setzt unsere Partnerin Frau Gabriela Jesacher mit ihrer jahrelangen Erfahrung im systemischen Coaching und Prozessveränderung an.

Gabriela Jesacher,
Coach und Begleiterin
von Organisations-
veränderungen

Netzwerk-Splitter

Europa: BOC

Die BOC-Gruppe (BOC Information Technologies Consulting AG) ist ein Beratungs- und Softwareunternehmen, das sich auf IT-gestützte Management-Lösungen spezialisiert hat. Die weltweit eingesetzten Software-Produkte umfassen u.a. die Bereiche: Strategiemanagement (ADO*score*), Geschäftsprozessmanagement (Adonis) und IT-Service- und IT-Architekturmanagement (ADO*it*)
In 6 Landes-gesellschaften sind über 140 Mitarbeiter beschäftigt.

Mag. Robert Strobl
BOC-Geschäftsführer

International: SGS

Die SGS Austria Controll-Co GmbH gehört zur internationalen SGS-Gruppe. SGS ist Weltmarktführer bei Inspektionen, Prüfungen und Zertifizierungen. In über 140 Ländern ist SGS vertreten und verfügt über das Know how von über 40.000 Mitarbeitern. "Mit über 70.000 zertifizierten Unternehmen ist SGS das führende globale Zertifizierungs-Unternehmen. Von ISO 9001, 14001, 20000, 27001 über VDA und IFS bis TickIT reichen die Zertifizierungs-Felder" betont Dipl-Ing. Hans Strauß mit seiner über 20-jährigen Branchenerfahrung.

Dipl-Ing. Hans Strauß
System & Services
Certification Manager

Kommunikations-Training

Kommunikation am Telefon unterscheidet sich wesentlich von einem persönlichen Gespräch! Oft ist das WIE wichtiger als der Inhalt – positiv formulierte Aussagen ermöglichen es, dass Sie Ihrem Gesprächspartner in guter Erinnerung bleiben. Dafür sorgt unsere BSN-Partnerin Evelyn Stein mit ihrer Seminarreihe „Die hohe Schule des Telefonierens".Maßgeschneiderte, Ihren Anforderungen angepasste Schulungsprogramme (Beschwerde-Management, aktive Gesprächsführung, etc.) werden von Frau Stein für Sie entwickelt.

Evelyn Stein,
Kommunikations-
Trainerin