



Management- Forum

Persönliche Einladung

Sicherheit ganzheitlich betrachtet

Mit Beiträgen von:

Gerhard Brandstätter (META Group),
Herfried Geyer (Siemens Business Services),
Erich Scheiber (CIS-CERT), **Helmut Stärker** (OVE)

Moderation: Edmund Lindau (Computerwelt)

Dienstag, 4. Mai 2004, 9.00 – 12.00 Uhr
Siemens Business Services, Seminarraum, 2. Stock,
Dietrichgasse 27–29, 1030 Wien
Bei freiem Eintritt

COMPUTERWELT
SIEMENS



CON
CONSULTING
EVENTS
COMMUNICATIONS
TRAINING
ECT

Umfassende Informationssicherheit

Informationen sind Werte, die genauso wie die übrigen Geschäftswerte wertvoll für eine Organisation sind und infolgedessen in geeigneter Weise geschützt werden müssen. Maßnahmen zur Informationssicherheit schützen Ihre sensiblen Daten. Sie soll die Aufrechterhaltung des Geschäftsbetriebs sicherstellen, geschäftsschädigende Einflüsse niedrig halten sowie die Investitionsrentabilität und die Geschäftsgelegenheiten maximieren.

Informationen können in vielen Formen vorliegen. Sie können ausgedruckt, auf Papier geschrieben, elektronisch gespeichert, auf dem Postweg oder elektronisch übertragen, in Filmen gezeigt oder in Gesprächen mündlich weitergegeben werden. Informationen sollten unabhängig von der dargebotenen Form, der gemeinsamen Nutzung oder Speicherung immer angemessen geschützt werden.

Informationssicherheit wird im Wesentlichen verstanden als Sicherung der

(a) Vertraulichkeit: Sicherstellung des Zugangs zu Informationen nur für Zugangsberechtigte;

(b) Integrität: Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden;
(c) Verfügbarkeit: Sicherstellung des bedarfsorientierten Zugangs zu Informationen und zugehörigen Werten für berechnete Benutzer.

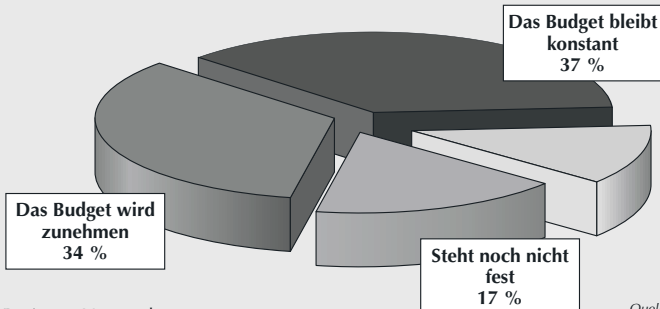
Informationssicherheit wird durch die Implementierung von geeigneten Maßnahmen erzielt, die Politik, Praktiken, Verfahren, Organisationsstrukturen und Softwarefunktionen sein können. Diese Maßnahmen sind zur Erfüllung der spezifischen Sicherheitsziele der Organisation festzulegen.

Motivation Informationssicherheit

Informationen und die sie unterstützenden Prozesse, Systeme und Netzwerke sind wichtige Geschäftswerte. Ihre Vertraulichkeit, Integrität und Verfügbarkeit können wesentlich zur Erhaltung von Wettbewerbsvorsprung, Liquidität, Rentabilität, Einhaltung gesetzlicher Vorschriften und Geschäftsansetzen beitragen.

Organisationen und ihre Informationssysteme und -netzwerke sehen sich

Wie wird sich Ihr IT-Security-Budget im Jahr 2004 gegenüber 2003 entwickeln?



Basis: 98 Unternehmen

Quelle: META Group Österreich

Sicherheitsbedrohungen unterschiedlichster Herkunft, einschließlich Computertrevirus, Spionage, Sabotage, Vandalismus, Feuers oder Überschwemmung, gegenüber. Gefahrenquellen wie Computerviren, Hacker und „Denial of Service“-Angriffe werden immer verbreiteter, anspruchsvoller und raffinierter.

Die Abhängigkeit von Informationssystemen und -diensten bedeutet, dass Organisationen gegenüber Sicherheitsbedrohungen anfälliger sind. Die Verbindung von öffentlichen und privaten Netzwerken und die gemeinsame Nutzung von Informationsressourcen erhöhen die Schwierigkeit, eine effektive Zugangskontrolle sicherzustellen. Der Trend hin zur verteilten Verarbeitung hat die Effektivität einer zentralen, fachlichen Kontrolle geschwächt. „Zugang“ meint hier und im Folgenden sowohl den physischen wie auch den logischen Zugang.

Viele Informationssysteme sind nicht auf Sicherheit hin ausgelegt. Die technisch erzielbare Sicherheit ist begrenzt und sollte durch entsprechendes Management und entsprechende Verfahren unterstützt werden. Die Identifizierung der benötigten Maßnahmen erfordert sorgfältige Planung und Detailgenauigkeit. Beim Informationssicherheitsmanagement ist die Mitwirkung aller Beschäftigten in der Organisation eine Mindestvoraussetzung. Außerdem kann auch die Einbeziehung von Zulieferern, Kunden oder Anteilseignern erforderlich sein. Das Gleiche gilt auch für die Fachberatung durch externe Organisationen. Maßnahmen für die Informationssicherheit sind wesentlich kostengünstiger und effektiver, wenn sie bereits in den Stadien der Anforderungsspezifikation und der Entwicklung integriert werden.

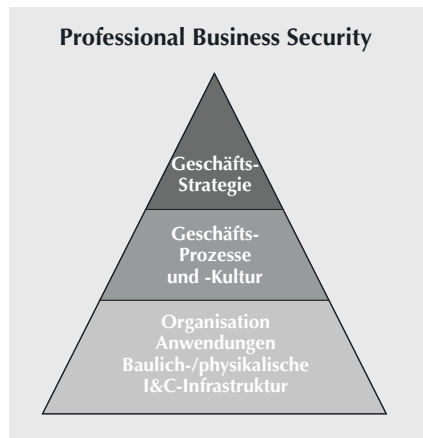
Ein Managementsystem zur Informationssicherheit Wie ist die Umsetzung realisierbar?

Informationssicherheit ist mehr als die Summe der einzelnen Sicherheitsmaßnahmen, dieser Ansatz wird durch das Managementsystem zur Informationssicherheit lt. BS7799 vertreten. Ein Szenario zur Realisierung im Unternehmen.

IT-Security in Österreich 2003 Status, Trends und Strategien in Zeiten knapper Kassen

Rund 60% der großen Unternehmen in Österreich sind der Ansicht, das angestrebte Sicherheitsniveau noch nicht erreicht zu haben. Gesamtheitliche Ansätze und organisatorische Maßnahmen für die Etablierung eines unternehmensweiten IT-Security sind daher nur selten anzutreffen.

Nahezu sämtliche befragte Unternehmen haben Erfahrungen mit Schäden aufgrund Schwächen im Sicherheitssystem. Die Bedeutung eines ausreichenden Sicherheitsniveaus ist daher unumstritten.



Ebenfalls als großes Hemmnis wird die Problematik der Erfolgsmessung von Investitionen in IT-Security gesehen. Traditionelle Return-of Investment (ROI) Verfahren scheitern, da sich der Erfolg von IT-Security nicht zu 100% in monetären Größen messen lässt. Vielmehr muss eine sinnvolle Erfolgsmessung mehrere Faktoren, wie z.B. Einsparungspotentiale, Risikoanalysen oder auch subjektive Einschätzungen der Bedeutung eines hohen Sicherheitsniveaus berücksichtigen.

In Österreich wird ähnlich wie in Deutschland, das Thema IT-Security noch immer primär als technisches Problem gesehen. Organisatorische Maßnahmen treten daher zwangsweise in den Hintergrund. Nur 36% der befragten Unternehmen verfügen über eine schriftlich fixierte Security-Policy.

IT-Security-Budgets werden im Jahr 2004 im Vergleich zu 2003 leicht steigen. 35% der befragten Personen gaben an, dass das Budget für IT-Security im Jahr 2004 steigen wird, 37% der Budgets werden gleich bleiben. Bei 12% der befragten Unternehmen wird von sinkenden Budgets ausgegangen. 12% der Befragten konnten noch keine Angabe über die Entwicklung des Budgets machen. Insgesamt kann damit gerechnet werden, dass sich IT-Budgets im allgemeinen und IT-Security-Budgets in den nächsten Jahren erholen und leicht steigen werden.

Security Audits

- ▶ Was bringen Security Audits?
- ▶ Optimierungspotentiale durch standardisierte Überprüfungen aufdecken
- ▶ Technische und qualitative Standards für Security
- ▶ Nutzen von regelmäßigen Informations-Sicherheits-Management-System (ISMS) Audits
- ▶ Die Arbeit des ISMS-Auditors – Erfahrungen aus der Praxis
- ▶ ISMS Zertifizierung

Sicherheit – eine kurze Philosophie

- ▶ Mensch
- ▶ Technik
- ▶ Politik
- ▶ Norm

Future Network Eventvorschau Management Foren

16. April 2004

Strategisches Management und innovative Finanzierung – Unternehmen marktorientiert ausrichten und intelligent finanzieren

In Österreich steigt endlich die Innovationsrate. Neue Produkte und Dienstleistungen werden entwickelt. Nicht zuletzt steigt das Wirtschaftswachstum auch hierzulande wieder.

Damit rücken – nach jahrelanger Konzentration auf Kostensenkung – strategische Themen wieder in den Vordergrund, Fokussierung auf das Kerngeschäft, Erhaltung und Ausbau von Kernkompetenzen, Aufbau neuer Vertriebsstrukturen, etc. sind die Themen die viele Unternehmen heute beschäftigen.

Referenten:

Georg Brandner (ICG Infora Consulting Group), **Andreas Reinthaler** (R.W.R. Managementfund Consulting)

18. Mai 2004

Arbeiten/Verkaufen und Lernen als zwei Seiten der Medaille der „Mitarbeiter-Leistung“

Die Zeit für eine von der Arbeitszeit getrennte Lernaktivität fehlt zunehmend. Mitarbeiter brauchen Information zum Zeitpunkt des Problemfalles – Communities of Practice, Action Learning, Learning on Demand u. ä. sind die methodischen Antworten auf den geänderten Context. Arbeit und Lernen verschmelzen.

Größerer Marktdruck erfordert mehr Umsatz – Unternehmenskommunikation als „neuer Lernkanal“ für Kundenbindung und gewünschtes Käuferverhalten. Marktkommunikation und Lernen verschmelzen – der Werbespot wird zum Lernvideo mit der Botschaft „Lerne, welch gutes Produkt ich bin und kaufe mich“. Umgekehrt wird Learning Content über die Darstellung der Lerninhalte hinaus mit motivatorischen Komponenten angereichert und bekommt häufig Fun Charakter – die Identifikation der Mitarbeiter mit dem eigenen Produkt wird erhöht.

Referenten:

Ines Esterkova (OMV CZ), **Julia Michl** (Fachhochschule), **Horst Krieger** (seeyou), **Barbara Saxinger** (BA-CA), **Haider Shnawa** (Microsoft), **Marion Tschirk** (seeyou)

An
Future Network
Kaiserstraße 14/2
1070 Wien
Tel.: (01) 522 36 36-37
Fax: (01) 522 36 36-10
E-Mail: registration@future-network.at
<http://www.future-network.at>

ANMELDUNG

Ja, ich möchte am Management-Forum „Sicherheit ganzheitlich betrachtet“ am 4. Mai 2004 bei freiem Eintritt teilnehmen.

Firma:

Name:

Straße:

PLZ/Ort:

Tel./Fax:

E-Mail:

Oder legen Sie einfach Ihre Visitenkarte bei!
Anmeldeschluss: 30. April 2004

Beschränkte Teilnehmerzahl. Anmeldebestätigung erforderlich.

Das Future Network behält sich vor, Besucher ohne Teilnahmebestätigung abzuweisen.

Senden Sie mir bitte Informationen über das Future Network:

Zielgruppe:

Unternehmensleitung, Sicherheitsverantwortliche, Finanzen, IT-Entscheider, IT-Vorstand, IT-Verantwortliche, Vertreter von Medien, Vertreter der Wissenschaft