

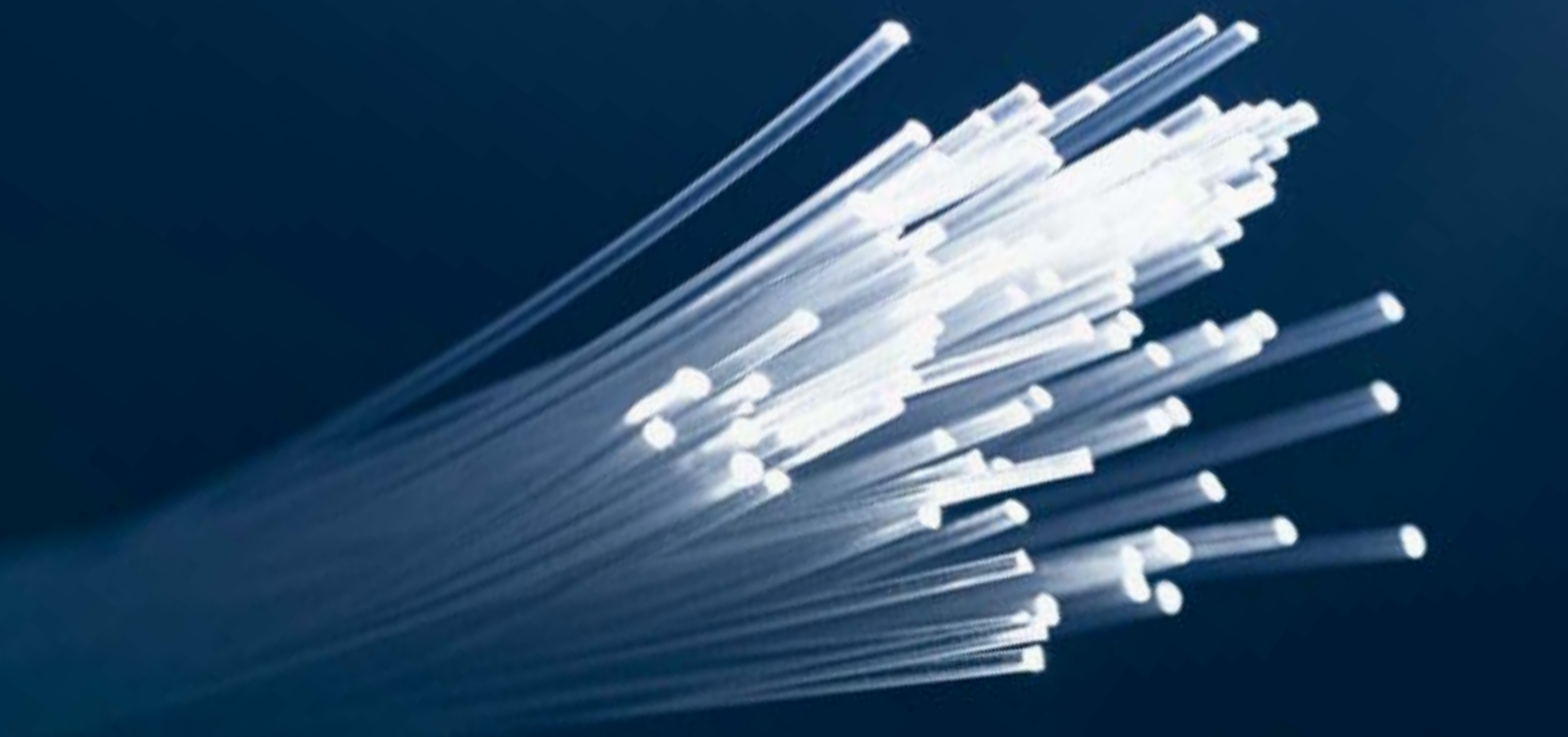
The background of the entire page is a deep blue gradient. Overlaid on this are several thick, dark blue fiber optic cables that curve and loop across the frame. At the ends of these cables, there are bright, glowing white points of light, suggesting signal transmission or data flow.

Report
IT-Umfrage 2004

KPMG Innsbruck-Linz

INHALT

KPMG Business Services – Information Risk Management	3
Vorwort	4
Das Procedere	5
Resümee Umfrage zur IT-Sicherheit	6
Erfahrung mit IT-Sicherheit	8
Unsere Dienstleistungen	13



KPMG BUSINESS SERVICES INFORMATION RISK MANAGEMENT (IRM)

Der Einsatz von Informationstechnologien birgt neben vielen Chancen auch ein großes Risikopotential.

Chancen nutzen ...

Die internen Prozesse in Unternehmen erfolgen heute fast ausschließlich IT-gestützt und auch der externe Geschäftsverkehr wird in zunehmendem Maße digital abgewickelt.

... und Risiken erkennen.

Mit dem Einsatz der Informationstechnologie sind jedoch auch bestimmte Risiken verbunden, die zum Gefahrenpotential für den unternehmerischen Erfolg werden können.

Mit Information Risk Management unterstützt Sie KPMG Business Services, die technischen, organisatorischen und personellen Voraussetzungen zu schaffen, um Ihre IT-Risiken zu identifizieren, zu kontrollieren und zu steuern.

Als kompetenter Partner sowohl für die Abwicklung ganzheitlicher Projekte im Rahmen des zentralen Managements von IT-Infrastruktur und Network-Security als auch auf den sicherheitsrelevanten Gebieten minimieren wir das Risiko und geben Ihnen Sicherheit.

Vertrauen Sie auf unsere interdisziplinären Teams von erfahrenen Beratern, Branchenexperten und IT-Spezialisten!



VORWORT

Eine der größten Herausforderungen für moderne Unternehmen ist die Koordination eines ausgewogenen Risikomanagements. Das unternehmensweite Risikomanagement gehört zu den zeitgemäßen Instrumentarien einer verantwortungsbewussten Unternehmensführung. Die Herausforderung besteht darin, komplexe heterogene Technologien, Richtlinien und Verfahren mit den geschäftlichen Anforderungen in Einklang zu bringen.

Ein perfektes Gleichgewicht wird erreicht, indem die wichtigsten Risikopotentiale erkannt und richtig gesteuert werden. Die häufigsten Probleme sind unerkannte Schwachstellen, Überwachungslücken, steigende Betriebskosten, verlorene Geschäftsmöglichkeiten und Verletzung gesetzlicher Vorschriften. Die gemeinsame Basis für all diese Bereiche stellt die Informations- und Kommunikationstechnologie dar.

Wer seine IT-Systeme gut kennt und diese mit den tatsächlichen Marktanforderungen, die an seine Organisation gestellt werden, objektiv vergleicht, wird eine effiziente und effektive Unterstützung seiner strategischen Geschäftsziele erreichen.

Um Sie bei Ihren Analysen unterstützen zu können, präsentieren wir Ihnen in der vorliegenden Broschüre die Ergebnisse der IT-Umfrage 2004 der KPMG Innsbruck-Linz zum Thema Informationssicherheit in Österreich.

Für weitere Informationen zur Umfrage und auch zu anderen aktuellen Themen wenden Sie sich bitte an Herrn Prokurist Mag. Ing. Markus Oman, Leiter unserer IRM-Abteilung KPMG Business Services Innsbruck-Linz.

Mehr zu unseren IRM-Aktivitäten finden Sie auch auf unserer Homepage unter www.kpmg.at.

Wir danken allen Teilnehmern der Umfrage.

Linz, im Oktober 2004

A handwritten signature in blue ink, appearing to read 'Löffler'.

Dr. Helge Löffler
Partner

A handwritten signature in blue ink, appearing to read 'Mag. Ing. Markus Oman'.

Mag. Ing. Markus Oman
Prokurist



DAS PROCEDERE

IRM Innsbruck-Linz hat im Juni/Juli 2004 eine Umfrage zum Thema Inform@tionssicherheit bei österreichischen Unternehmen aus allen Branchen durchgeführt.

Die Unternehmen wurden auf Grundlage von öffentlich zugänglichen Informationen ausgewählt und hinsichtlich folgender Punkte befragt:

- Einschätzung der Bedeutung von Information bzw Informationssicherheit
- Hindernisse und Probleme eines ausreichenden Informationssicherheitsniveaus
- allgemeine Sensibilisierung gegenüber Informationssicherheit
- angewandte Maßnahmen und Abläufe, um die Informationssicherheit zu erhöhen

Wir stellten uns folgende Hauptaufgaben:

- Schaffung eines Überblicks über die seitens der Unternehmen getroffenen Maßnahmen zur Verbesserung der Verfügbarkeit und der IT-Sicherheit
- Erhebung des Ausmaßes an Beschäftigung mit den vorhandenen IT-Risiken in Unternehmen
- Aktualisierung der IT-Kennzahlen
- Verfolgung neuer Tendenzen der Informationssicherheit

Als Grundlage der Umfrage erhielten die Unternehmen standardisierte Fragebögen, deren Rücklaufquote¹ mit ca 30 % sehr hoch war.

Im Rahmen der Untersuchung wurde „Informationssicherheit“ als Sammelbegriff aller Maßnahmen zum Schutz von unternehmensrelevanten Informationen vor Verlust (Verfügbarkeit), unbefugter Veränderung (Integrität) und unbefugter Kenntnisnahme (Vertraulichkeit) verstanden. Somit wird sichergestellt, dass diese Informationen zum erforderlichen Zeitpunkt nur von berechtigten Nutzern verwendet und nicht gegen die Interessen des eigenen Unternehmens und seiner Mitarbeiter (Corporate Identity) gerichtet werden können.

¹ Obwohl bei der Erarbeitung dieser Veröffentlichung größte Sorgfalt an den Tag gelegt wurde, ist es möglich, dass bestimmte Informationen falsch, unvollständig oder überholt sind. Die Autoren und Herausgeber übernehmen keine Haftung für die Folgen der Handlungen, die auf der Grundlage dieser Veröffentlichung erfolgen. Aufgrund ihres allgemeingültigen Charakters können die in dieser Veröffentlichung enthaltenen Informationen nicht als Hilfsmittel für die Lösung konkreter Probleme herangezogen werden. Die Vervielfältigung und/oder Verbreitung von Teilen dieser Veröffentlichung ist ohne ausdrückliche Genehmigung von KPMG untersagt.



RESÜMEE UMFRAGE ZUR IT-SICHERHEIT

IT entwickelt sich zur Chefsache!

- Information Risk Management ist bzw sollte eine Hauptaufgabe des Managements sein. Das Risikomanagement im Informations- und Kommunikationstechnologiebereich (IKT oder engl ICT) gewinnt stark an Bedeutung. Bei 80 % aller Befragten ist die IT-Abhängigkeit sehr hoch.
- In 80 % der Unternehmen ist die Geschäftsführung bei der strategischen Entscheidung im IT-Bereich involviert.
- Bei 63 % aller Befragten werden die Unternehmensinformationen als streng vertraulich behandelt. Bei 56 % würde es sogar zu einer erheblichen Geschäftsunterbrechung kommen, wenn auf diese Unternehmensdaten nicht mehr zugegriffen werden könnte.

Obwohl die IT ein integrierter und unabdingbarer Bestandteil der Geschäftsprozesse ist, wird diese noch zu ineffizient betrieben!

- 67 % aller befragten Unternehmen betrachten Informationssicherheit als sehr hohe Priorität und wesentlich für die Erreichung der Unternehmensziele.
- Die Hälfte der Befragten betrachtet ein knappes Budget als das größte Problem bei der Realisierung einer effektiven Informationssicherheit.
- Mehr als ein Drittel kann ihre Anwendungsprogramme nicht an die schnelle Veränderung des Marktes anpassen (System zu starr).
- Interessanterweise ist für 43 % der Unternehmen bzw der Geschäftsführung der Kosten-Nutzen Aspekt nicht transparent, sodass Überlegungen im Bereich Return on Security Investment (ROSI) nicht regelmäßig oder periodisch stattfinden.
- Die Erhöhung der Netzwerksicherheit (57 %) und Sensibilisierung der Mitarbeiter (49 %) sind ebenfalls weitere geplante Maßnahmen.



- 50 % aller Befragten planen als Maßnahme die (Weiter)-Entwicklung einer IT-Strategie², um die Effizienz und Effektivität der IT-Sicherheit zu erhöhen.
- Obwohl 61 % in den letzten drei Jahren Verbesserungen im Internen Kontroll- und Steuerungssystem ergriffen haben, wird in 35 % der Fälle ein Versagen der Verfügbarkeit der Systeme als Faktor für IT-Probleme angegeben.
- Diese Priorisierung der Maßnahmen erscheint vor dem angegebenen Bedrohungshintergrund sinnvoll (Bei 46 % der Befragten war ein Virenbefall einer der maßgeblichsten Probleme in der IT).
- 82 % der Befragten haben kein Kontrollsystem bzw. Intrusion Detection System, welches die internen Datenbewegungen dokumentiert, um Datenmissbrauch vorzubeugen. Von diesen 82 % planen nur 14 % ein solches Kontrollsystem zu implementieren.

Wo liegen somit die Herausforderungen für das Management zum Thema Informationssicherheit?

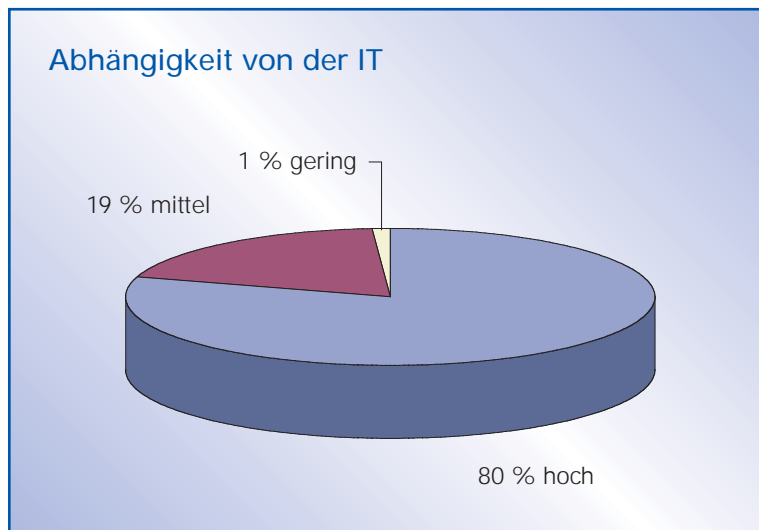
- Erstens muss erkannt werden, dass ein auf längerfristigen Nutzen ausgerichtetes Investitionsverhalten auch im Bereich Informationssicherheit weniger kostet als kurzfristig optimierte Maßnahmen.
- Zweitens sollte das Verhältnis zwischen den wichtigsten Problemen³ und dem Einsatz der Mittel auf die jeweiligen Erfordernisse abgestimmt werden.
- Drittens braucht ein professionelles Risikomanagement im Bereich Informationssicherheit klare und systematische Vorgaben bezüglich der Geschäftsprozesse und der methodischen Umsetzung im täglichen Unternehmensalltag.

² KPMG Anmerkung - Die Erstellung bzw. Weiterentwicklung einer genau auf die Unternehmensziele abgestimmten IT-Strategie und deren kontinuierliche Nachverfolgung ermöglichen einer Organisation, marktgerecht zu investieren und folglich die Betriebsmittel effizienter und effektiver einzusetzen.

³ zB Verfügbarkeit der Systeme, unvorsehbare Kosten, Entwicklungsfähigkeit der Anwendungsprogramme, Viren und so genannte Worms, Verfehlungen eigener Mitarbeiter

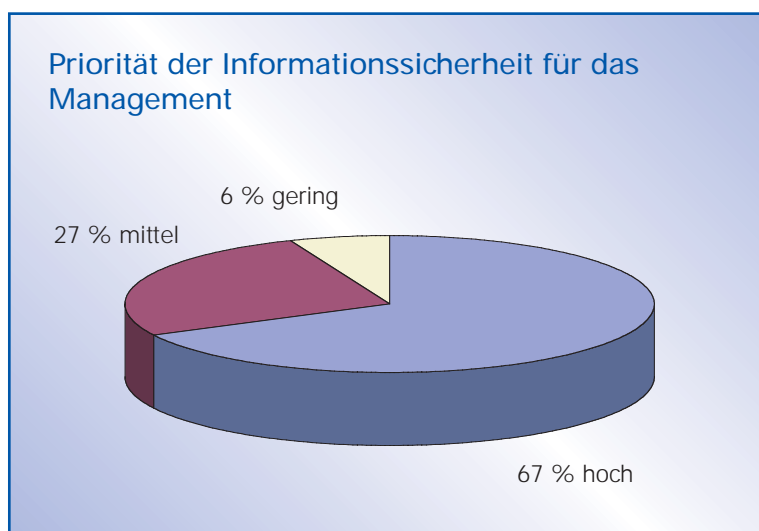
WIRTSCHAFT UND IT

Die Abhängigkeit der Unternehmen von ihrer IT wird als hoch eingeschätzt!



Bei 80 % aller von uns befragten Unternehmen läuft ein Großteil der Prozesse IT-unterstützt ab. Nicht zuletzt auf Grund dieser Tatsache ist in den letzten Jahren ein verstärkter Trend zur Optimierung und Automatisierung der Prozesse zu beobachten. Als Erkenntnis kann daraus abgeleitet werden, dass für alle Organisationen einerseits ein hohes Sicherheitsniveau notwendig ist und andererseits nur qualitativ hochwertige Daten zum Unternehmenserfolg führen.

Mit IT-Sicherheit sollte man nicht experimentieren!



Informationssicherheit hat eine hohe Priorität für das Management. Für 67 % der befragten Geschäftsführer ist die Informationssicherheit sehr wichtig.

Informationssicherheit umfasst die sichere Verarbeitung von Informationen, die als Grundlage für die Entscheidungen des Managements dienen. Weiters ist die IT-Sicherheit ein Faktor, dessen Wichtigkeit für das Überleben des Unternehmens nicht unterschätzt werden darf.

ERFAHRUNG MIT IT-SICHERHEIT

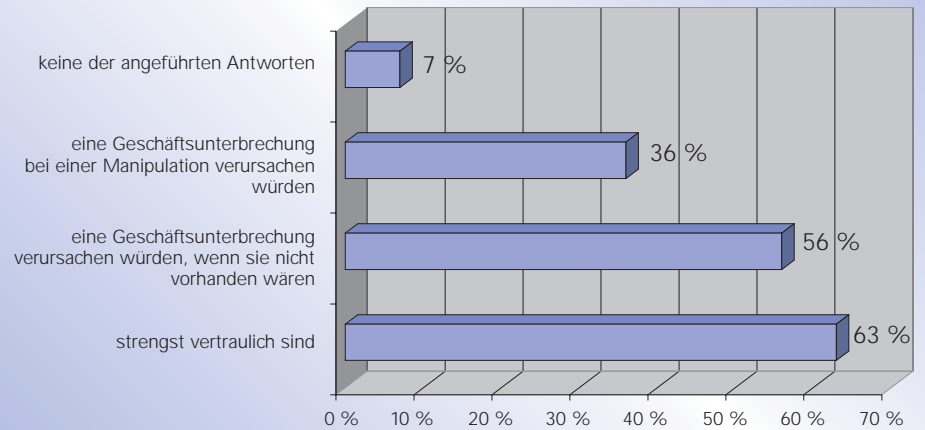
Die drei Grundpfeiler der Informationssicherheit sind Vertraulichkeit, Verfügbarkeit und Integrität.

Eine Gefährdung der Informationssicherheit kann für viele Unternehmen finanzielle Verluste, Imageverlust, Vertrauensverlust oder eine Störung der Geschäftsprozesse bedeuten.

63 % aller Befragten behandeln die Unternehmensinformationen als streng vertraulich. Bei 56 % würde es sogar zu einer erheblichen Geschäftsunterbrechung kommen, wenn auf diese Unternehmensdaten nicht mehr zugegriffen werden könnte.

Die Kontrolle und der Schutz sensibler Daten werden immer

Vertraulichkeit der Daten (Mehrfachauswahl möglich!)



wichtiger, aber auch immer schwieriger.

Information ist heutzutage durch eine ständig wachsende Zahl an

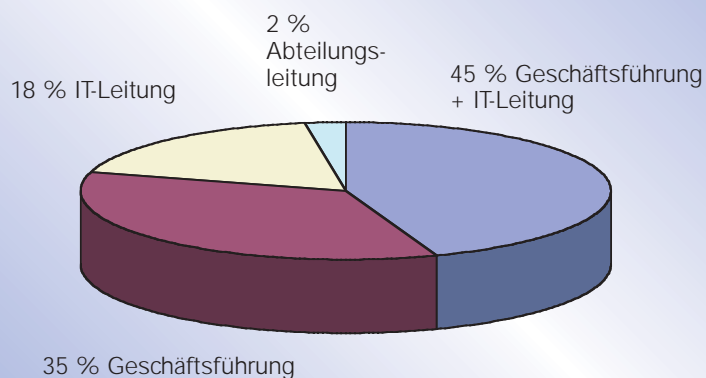
Angriffsszenarien gefährdet (zB Zunahme der Datenübertragungsnetze, Zugänglichkeit der Kommunikationsleitung, zunehmende Terminalanzahl).

IT wird zur Chefsache!

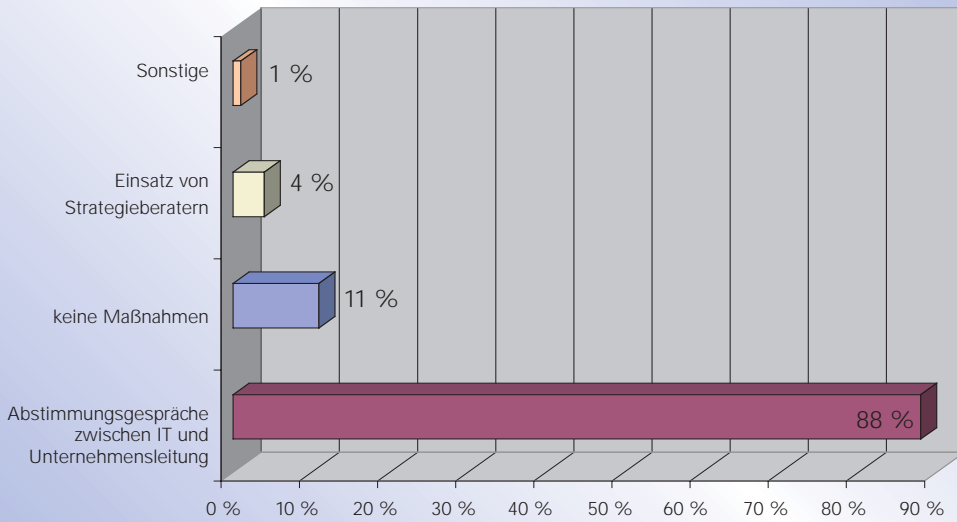
Entscheidungen bezüglich IT-Sicherheit werden bei 80 % aller befragten Unternehmen von der Geschäftsführung oder zumindest unter deren Einbindung getroffen. Selbst in stärker regulierten Branchen geht der Trend hin zum bewussteren „Information Risk Management“ durch die Geschäftsführung.

Die Bedeutung von Informationstechnologien für das Erreichen von Geschäftszielen wird von 80 % der Firmen als hoch eingeschätzt.

Entscheidungsträger für IT-Investitionen zur IT-Sicherheit



Maßnahmen zur Abstimmung der IT-Ziele mit den Unternehmenszielen (Mehrfachauswahl möglich!)



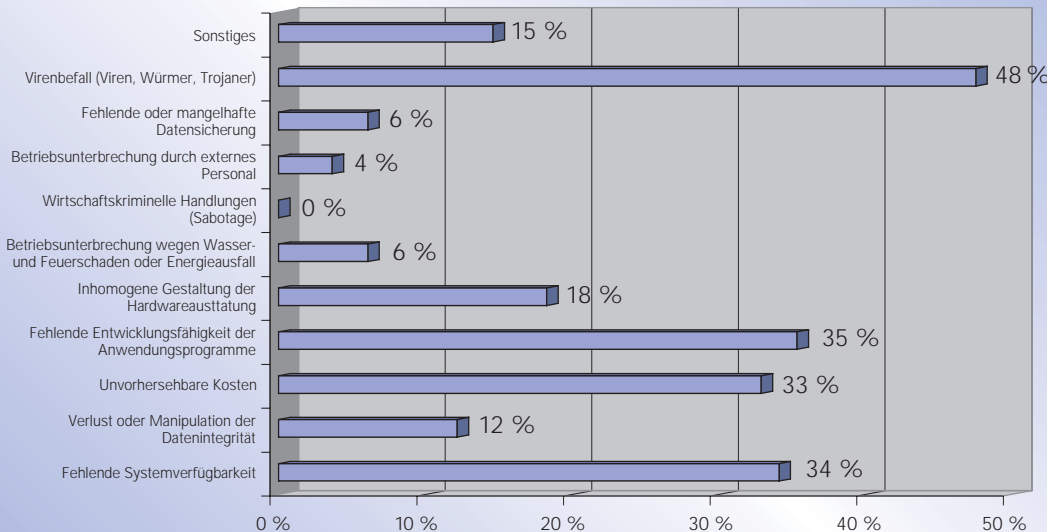
Bei 88 % der Befragten werden Abstimmungsgespräche zwischen IT und Unternehmensleitung zur Definition der IT-Ziele auf die Unternehmensziele durchgeführt.

Nur 4 % der Befragten bedienen sich eines externen Beraters zur Unterstützung bei der Definition der IT-Strategie.

IT-Manager von heute müssen permanent den Graben, der sich zwischen der Erfüllung der strategischen Unternehmensziele und den täglichen operativen Aufgaben auftut, überwinden. Viele Unternehmen umgehen diese Gratwanderung, indem sie etwaige Lücken an Dritte auslagern, wobei sich sofort wieder das Problem des Outsourcing-Managements stellt.

IT-Probleme sind alte Bekannte!

Maßgeblichste Probleme der IT (Mehrfachauswahl möglich!)



Die ersten beiden Punkte stellen externe Problembereiche dar und haben sich in den letzten Jahren kaum verändert. Die beiden letzten Punkte sind unternehmensinterne Probleme, denen durch eine verbesserte Planung entgegengewirkt werden kann. Daraus lässt sich ableiten, dass ein wirksamer Schutz gegen Virenbefall nur durch ein Zusammenspiel von technischen Maßnahmen und einem verbesserten Sicherheitsbewusstsein der Mitarbeiter möglich ist. Mit anderen Worten – es sollte eine auf die Unternehmensziele ausgerichtete IT-Strategie existieren, aus der wiederum die operativen IT-Agenden abgeleitet werden: „Plan your work and work your plan.“

Bei der Problemanalyse der IT trifft man auf „alte Bekannte“:

- Virenbefall
- Fehlende Systemverfügbarkeit
- Schlechte Anpassungsfähigkeit der Anwendungen an die Geschäftsprozesse
- Vermeyntlich unvorhersehbare Kosten

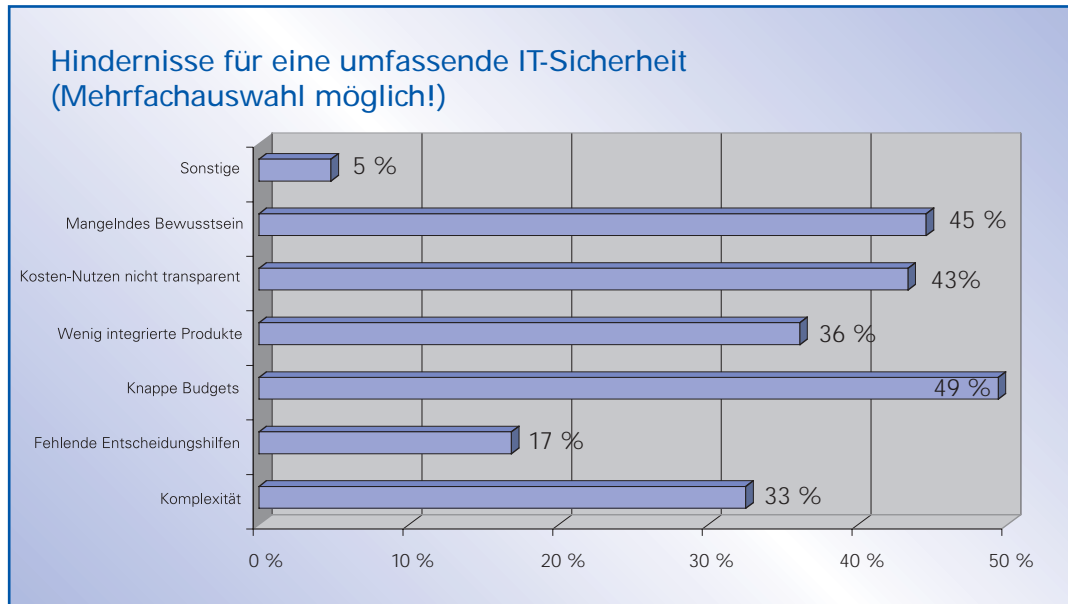
Es ist besser, Deiche zu bauen, als zu hoffen, dass die Flut allmählich Vernunft annimmt.

(Erich Kästner)

Eine wesentliche Voraussetzung für ein erfolgreiches IT-Sicherheitsmanagement ist die realistische Einschätzung der bestehenden Sicherheitsrisiken. Die größte Gefahr hierbei ist, dass eines der folgenden Risikoszenarien nicht erkannt bzw. verkannt wird:

- Logische Datensicherheit: Risiko des Datenverlusts
- Funktionsfähigkeit: Risiko des Systemausfalls
- Physikale Sicherheit: Risiko der Zerstörung des Systems

Weitere Hindernisse am Weg zur optimalen IT-Sicherheit sind jedoch „hausgemacht“, wie aus unserer Umfrage hervorgeht:



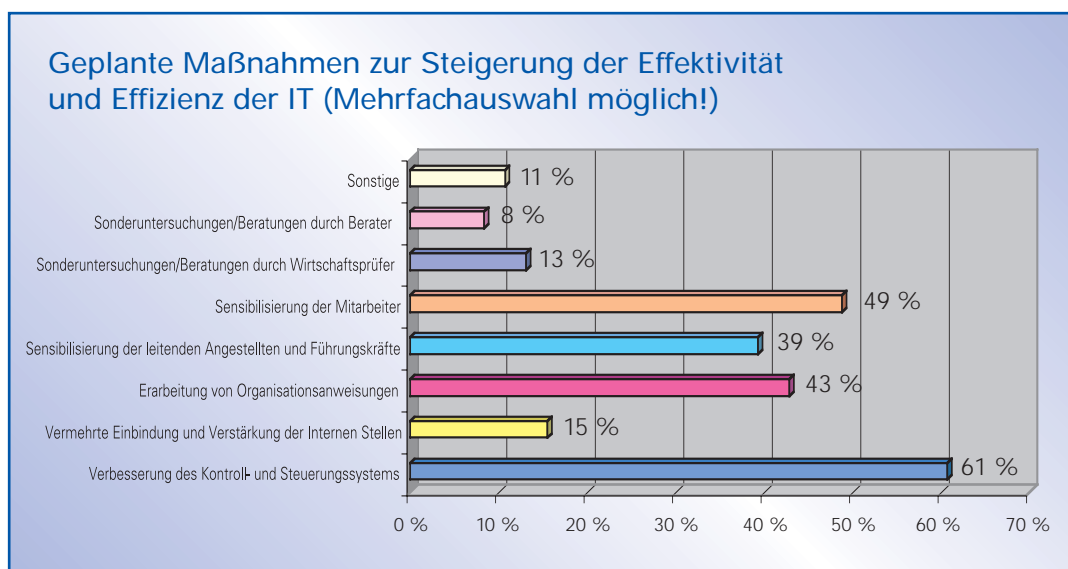
- Knappes Budget (49 %)
- Kosten-Nutzen-Aspekte sind nicht transparent (43 %)
- Mangelndes Bewusstsein (45 %)

Auch in der IT sind langfristige Strategien und gute Management-Informationssysteme gefragt.

Informationssicherheit ist für jedes IT-Projekt, jedes IT-System und alle IT-Benutzer innerhalb einer Organisation von besonderer Bedeutung. Dieser übergreifende Charakter macht es notwendig, entsprechende Rollen mit Kompetenz und auch Verantwortung innerhalb des Unternehmens festzulegen.

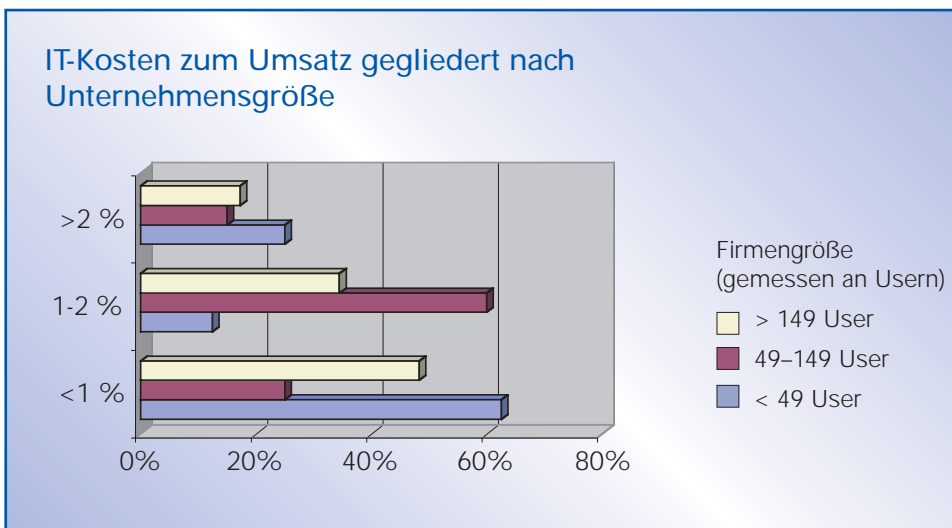
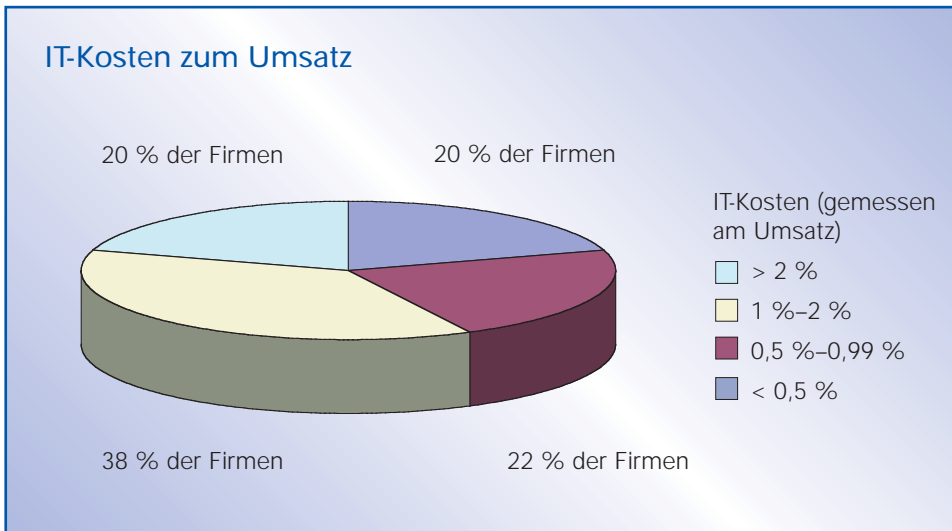
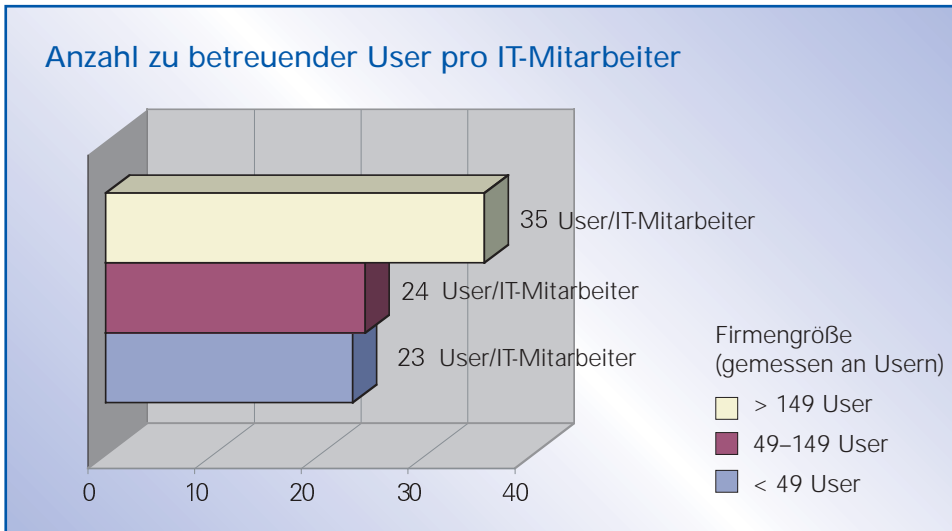
Sicherheitsmanagement ist ein kontinuierlicher Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen sind.

Durch organisatorische, personelle, infrastrukturelle und technische Sicherheitsmaßnahmen



wird ein Standard für das Sicherheitsniveau der IT-Systeme aufgebaut.

Die Servicekosten pro Mitarbeiter sinken mit der Größe des Unternehmens.



Die Servicekosten pro Mitarbeiter sinken mit der Größe des Unternehmens, da größere Unternehmen in der Lage sind Skaleneffekte zu nutzen. Interessant ist hierbei jedoch, dass die prozentuellen Gesamtkosten der IT für manche größere Unternehmen keine sinkende Tendenz ableiten lassen. Dies ist unter anderem damit zu erklären, dass diese Unternehmensstrukturen schon komplexere sowie teurere Applikationssysteme benötigen.

80 % der befragten Unternehmen haben IT-Kosten gemessen am Umsatz von weniger als 2 % und 42 % liegen sogar unter 1 %. Das Bild verändert sich etwas, wenn man die Unternehmen nach der Anzahl der zu betreuenden User schichtet. Unternehmen, die in unserer Studie 49 bis 149 zu betreuende User hatten, weisen die größten prozentuellen IT-Kosten gemessen am Umsatz auf. Auffällig ist zudem, dass jene Unternehmen mit tendenziell hoher Useranzahl und jene mit wenigen Usern sehr geringe Ausgaben für IT aufweisen (unter 1 %). Dass kann einerseits damit erklärt werden, dass gewisse Skaleneffekte genutzt werden können bzw kleinere Unternehmen sich teilweise nur mit dem Notwendigsten ausstatten. Für die Unternehmen im mittleren Bereich sollte ein geeignetes Mittelmaß an Outsourcing und Kompetenzaufbau im eigenen Unternehmen gefunden werden. Dies erreicht man am besten durch eine kompetente und unabhängige externe Unterstützung. Es ist daher nicht nur das Augenmerk auf den Headcount in der IT zu legen, sondern sehr stark auch auf den gewinnbringenden Einsatz der Systeme.



UNSERE DIENSTLEISTUNGEN

IT-Risikoprofil

Damit Sie die Bedrohungen kennen und geeignete Maßnahmen ergreifen können.

Sie kennen Ihre IT, sämtliche Bedrohungen und Schwachstellen Ihrer Informationssysteme? Wir ermitteln und bewerten auf Basis internationaler Standards wie CobiT und ISO 17799 die Bedrohungen für sämtliche Daten in Ihrem Unternehmen und definieren mit Ihnen gemeinsam alle notwendigen Maßnahmen, damit Sie Ihre Risiken in den Griff bekommen. Gemeinsam bereiten wir Sie damit auf die Einhaltung nationaler und internationaler Vorgaben und gesetzlicher Anforderungen (HGB, DSGVO, BwG, TKG etc) vor.

IT-Revision

Revision zur Verbesserung Ihrer IT-Prozesse.

Ihre IT-Prozesse werden laufend überwacht und durch unabhängige Experten verbessert? Die hohe Anforderung an eine qualifizierte IT-Revision kann die eigenen Ressourcen schnell übersteigen. Unsere auf ihrem Gebiet führenden Experten garantieren Ihnen eine unabhängige Revision, die auf anerkannten Methoden aufbaut. Ihre Risiken und Kontrollen werden gegenübergestellt und deren Angemessenheit evaluiert. Ihre IT-Mitarbeiter profitieren vom externen Know-How und die Geschäftsleitung erhält eine unabhängige Expertise.

Security Management

Wirksame Maßnahmen für die Sicherheit Ihrer Daten.

Angriffe auf interne Firmendaten steigen rasant durch die Öffnung der Unternehmensnetzwerke; besonders E-Commerce Lösungen stehen im Visier von Hackern. Präventiv erarbeiten wir mit Ihnen Maßnahmen, um die Sicherheit Ihrer Daten zu gewährleisten. Dabei analysieren wir - auch mit Hacker-Methoden - die Wirksamkeit bestehender Sicherheitseinrichtungen, bewerten Risiken und planen gemeinsam den Einsatz der für Sie passenden Technologie.



Kontrolle über Ihr ERP-System

Verlässlichkeit, Sicherheit und Ordnungsmäßigkeit durch geprüfte Anwendungen.

Entsprechen Ihre Kernanwendungen den Anforderungen eines internen Kontrollsystems? Das einwandfreie Funktionieren Ihres Enterprise Resource Planning (ERP) Systems ist für die Bewältigung Ihres Tagesgeschäfts unbedingt erforderlich. Egal welches ERP-System Sie einsetzen, ob SAP R/3, Navision oder ein anderes, wir definieren mit Ihnen gemeinsam das erforderliche Kontrollsystem und unterstützen Sie auch bei der Einhaltung von Archivierungserfordernissen. Die internen Kontrollen entsprechen den Grundsätzen der Ordnungsmäßigkeit und geben der Geschäftsführung die Möglichkeit, die Verantwortung zur internen Kontrolle (vgl § 82 AktG sowie § 22 (1) GmbHG) wahrzunehmen.

Geschäftsprozessmanagement

Ihre Geschäftsprozesse optimieren.

Ihre Prozesse laufen optimal und frei von Fehlern? Prozesse durchlaufen typischerweise verschiedene Abteilungen. Diese tauschen über unterschiedlichste Medien Informationen aus, eventuell sogar über verschiedene Systeme. Dadurch entstehen Medien-, Organisations- und Systembrüche, die Ihre internen Abläufe fehleranfällig machen. Notwendige Korrekturen sind kosten- und zeitintensiv. Wir analysieren und optimieren mit Ihnen gemeinsam Ihre Prozesse und wählen ein für Ihre Ansprüche maßgeschneidertes System. So helfen wir Ihnen, Ihre Prozesse zu verbessern und dadurch Kosten zu senken.



IT-Benchmarking

Transparenz und Vergleichbarkeit für IT-Kennzahlen.

Sind Kosten- und Leistungskennzahlen Ihrer IT mit denen Ihres Mitbewerbs vergleichbar? Wir analysieren sowohl Ihre IT-Kosten als auch die Leistungsfähigkeit Ihrer IT und unterziehen die erhobenen Werte einem Benchmark mit vergleichbaren Organisationen. Wir haben Erfahrung in nahezu allen Branchen, in unterschiedlichen Unternehmensgrößen und mit verschiedensten Systemen. Wir machen Kosten und Nutzen Ihrer IT transparent und decken die verborgenen Potentiale zur Leistungssteigerung und Kostensenkung auf.

Ihre Ansprechpartner für
KPMG Innsbruck-Linz:



Dr. Helge Löffler
Partner
Tel (0732) 69 38 - 21 05
Fax (0732) 69 38 - 444
hloeffler@kpmg.at



Mag. Ing. Markus Oman
Prokurist
Tel (0732) 69 38 - 24 24
Fax (0732) 69 38 - 444
moman@kpmg.at



**Globale
Orientierung.**

**Regionale
Präsenz.**

**Für Ihren Erfolg.
www.kpmg.at**

Ob internationaler Konzern, mittelständisches Unternehmen oder öffentliche Verwaltung – KPMG unterstützt Sie mit zukunftsorientierten Strategien und praxiserprobten Lösungen.

Für weitere Informationen zu IRM-Themen:
KPMG, Mag. Ing. Markus Oman, Tel (0732) 6938-2424,
Mobil 0699/12518089, moman@kpmg.at