Angemessen, praktisch und konkret

Informationssicherheit im Unternehmen hört nicht mit der Datensicherung auf. Für die komplexe Thematik drängt sich eine umfassende Betrachtungsweise auf. Technische Risiken sind genauso ernst zu nehmen wie menschliches Versagen, höhere Gewalt oder gar kriminelle Handlungen wie Diebstahl und Hacking.

VON WOLFGANG SIDLER*

Sobald ein Unternehmen Daten erfasst oder Informationen speichert, muss auch die Frage der Sicherheit geklärt werden – unabhängig von Art und Grösse der Organisation. Mit steigenden Investitionen in Netzwerktechnologien steigt der Bedarf an Sicherheitsmassnahmen weiter. Diesbezügliche Kosteneinsparungen werden allzu schnell durch Ausfallzeiten, Datenwiederherstellung oder sogar Wirtschaftsspionage wieder eingebüsst. So ergab eine Studie der Gartner Group, dass über 70 Prozent der Schweizer Unternehmen durch Attacken und Systemausfälle schon einmal erhebliche finanzielle Verluste zu beklagen hatten.

Gefahren lauern überall. Die Bedrohungen, denen Informationen ausgesetzt sind, haben vielseitige Ursprünge:

► *Höhere Gewalt:* Feuer, Blitz, Sturm, Überschwemmung, Personalabgänge, Krankheiten.

► *Technisches Versagen:* Netzwerkausfall, Ausfall Disk-Systeme, mangelnde Kompatibilität, Softwarefehler.

► *Menschliches Versagen:* Fehlmanipulation, fehlende Sensibilisierung, Übermüdung.

► *Vorsätzliche Handlungen:* Hacking, Diebstahl, Spionage, Erpressung, Missbrauch von Daten, Viren.

Für grosse und kleine Unternehmen heisst dies ganz klar, dass die IT-Sicherheit weit über den täglichen Backup hinausgeht. Gerade auch die Sensibilisierung von Geschäftsleitung und sämtlichen Mitarbeitenden auf die oben genannten Risikofaktoren ist von grosser Bedeutung.

Vertrauen ist gut – Kontrolle ist besser

Die Weiterentwicklung der Informationstechnik (IT) wird zu einem erheblich erweiterten Einsatz informationstechnischer Systeme führen. Dadurch nimmt die Abhängigkeit von Verwaltung und KMU von einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit informationstechnischer Systeme zu. Gleichzeitig ist mit der Zunahme von Bedrohungen zu rechnen, welche die *Vertraulichkeit, Verfügbarkeit und Integrität* der Daten (IT-Sicherheit) gefährden. Vertrauenswürdige und sichere Geschäftsprozesse sind jedoch entscheidende Erfolgsfaktoren:

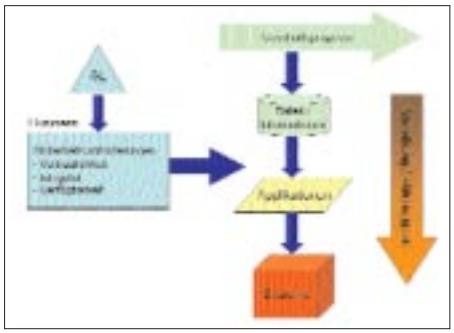
► Welche kritischen Abläufe bestimmen den Geschäftserfolg?

► Welche Informationen werden heute und in Zukunft unbedingt für die Geschäftsabläufe benötigt?

► Welche relevanten Risiken bestehen für die unternehmenskritischen Informationen?

► Welche Sicherheitsziele sind für die kritischen Informationen im Unternehmen gesetzt?

Gefahren wie bösartige Programme oder das Ausspionieren des Nutzungsverhaltens sind die Schattenseiten dieser weltweiten Vernetzung. Der Selbstschutz wird deshalb immer bedeutender. Das persönliche, verantwortungsvolle und aufmerksame *Verhalten* bei der Nutzung der IT-Infrastruktur ist deshalb der entscheidende Faktor. Die wahre Herausforderung stellt die Umsetzung und erfolgreiche Durchsetzung der entsprechenden IT-Security-Weisungen dar.

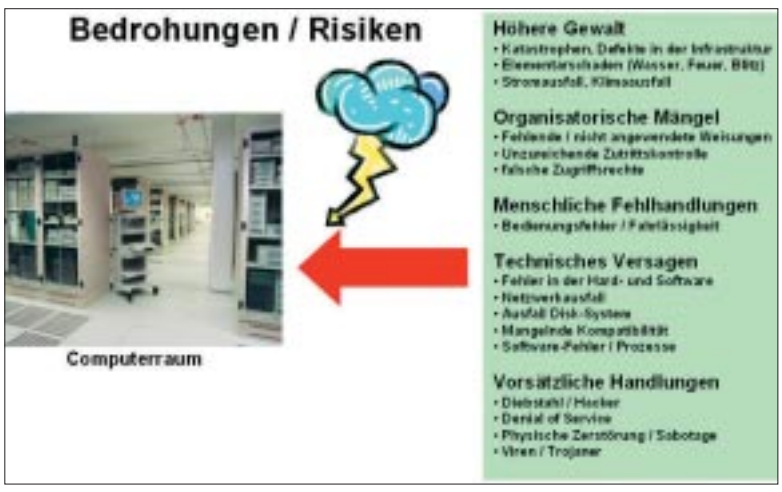


Geschäftsprozesse und deren Anhängigkeiten.

Verantwortung des Managements

Praktisch jedes unternehmerische Ziel, von der Kostensenkung bis hin zur Geschäftsprozessoptimierung, hängt von der Effizienz, der Effektivität sowie von der Sicherheit und Zuverlässigkeit des Informatikeinsatzes ab. Zur Informationssicherheit gehört der ganzheitliche Schutz von Informationen. Informationssicherheit ist daher eine strategische und nicht ausschliesslich eine technische Frage. Informationssicherheit kann nur wirkungsvoll und nachhaltig umgesetzt werden, wenn sie ein fester Bestandteil der Unternehmenspolitik ist und das IT-Sicherheitsmanagement organisatorisch im Unternehmen eingebunden wird.

Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die anschliessende Auswahl der geeigneten Massnahmen zur Informationssicherheit sind Führungsaufgaben, die sich nur eingeschränkt delegieren lassen. Damit die Informationssicherheit erfolgreich umgesetzt werden kann, ist die volle Unterstützung des Managements nötig. Die Verantwortung für die Informationssicherheit liegt beim Management, welches die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren muss.



Verschiedene Bedrohungen und Risiken sind denkbar.

Dabei gelten die folgenden Grundregeln:

► Die *Initiative* für Informationssicherheit geht *vom Management* aus.

► Die *Verantwortung* für Informationssicherheit *liegt beim Management* und kann nicht delegiert werden.

► Der Prozess wird *vom Management kontrolliert.*

► Nur wenn sich das *Management um Informationssicherheit bemüht,* wird die Aufgabe auch wahrgenommen.

► Die Umsetzung muss *wirtschaftlich* sein. IT-Sicherheit darf nicht mehr kosten als die damit erreichte Risikominderung.

► Die IT-Sicherheit muss in sinnvoller Relation zum Schutzbedarf stehen *(Angemessenheit).*

► Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen *(Praktikabilität).* Sie müssen nachweisbar Bedrohungen abwehren und Risiken mindern *(Wirksamkeit).*

► IT-Sicherheit darf nicht «behindern» und muss von allen als Notwendigkeit verstanden werden *(Akzeptanz).*

Datensicherung, Schutz vor Computerviren, eine sichere Anbindung an das Internet, eine sichere Remote-Zugang-Lösung, Software aktualisieren, Zutritts- und Zugriffsregeln definieren, Weisungen erlassen, die Mitarbeiter sensibilisieren und ausbilden, ein Risiko-Management aktiv betreiben und einen den Bedürfnissen gerechten physischen Schutz erstellen sind wichtige Massnahmen für die Führung eines Unternehmens.

Die Einhaltung dieser *Grundregeln* der Informationssicherheit ist die Pflicht eines Unternehmens und muss von der Geschäftsleitung im Rahmen ihrer Sorgfaltspflicht überprüft werden. Es geht darum, sich auf das Wesentliche zu konzentrieren und aus Gründen des Aufwands gewisse Abstriche zu machen. Viele Massnahmen können ohne grossen finanziellen Aufwand realisiert werden, nur durch das Nutzen vorhandener Funktionen in den bestehenden Systemen.

Unternehmenserfolg ist massgebend von Know-how, Kompetenz und Information abhängig. Diese müssen geschützt und gesichert werden. Deshalb ist die Sicherheit von Informationen regelmässig zu prüfen, um sie auch in Zeiten des Wandels anzupassen und auf einem hohen Niveau zu halten.

Längst kein Fremdwort mehr dürfte für die meisten mittelständischen Unternehmen der Begriff Basel II sein. Viele Firmen sind sich darüber im Klaren, dass künftig bei der Kreditvergabe die damit verbundenen Risiken viel genauer unter die Lupe genommen werden. Dabei hängt es entscheidend von der Ratingnote ab, ob und zu welchen Konditionen ein Unternehmen Fremdkapital erhält. In dieses Rating fliessen eine Reihe unterschiedlicher Faktoren ein – nicht nur betriebswirtschaftliche Kennzahlen.

Einen wichtigen Punkt lassen Firmenchefs von KMU oft aus den Augen: die Absicherung gegen operationelle Risiken und damit den Schutz der IT-Infrastruktur vor den bereits genannten vielfältigen Gefahren. Je mehr der Geschäftsbetrieb auf die IT-Infrastruktur angewiesen ist, desto stärker hängt die Bonität und somit die Kreditentscheidung von einem effektiven IT-Sicherheitsmanagement ab. Umgekehrt: Wer bei der IT-Sicherheit spart, muss auch ein schlechteres Rating beziehungsweise höhere Zinssätze fürchten.

«Sicherheitshandbuch für die Praxis»

Das «Sicherheitshandbuch für die Praxis» hebt sich von anderen Publikationen zum Thema ab, indem es sich explizit an kleine bis mittlere Unternehmen und Verwaltungen richtet. Denn diese sind genauso auf die Verfügbarkeit und Verlässlichkeit ihrer Informations- und Kommunikationssysteme angewiesen wie grosse Firmen, haben aber nicht die gleichen Ressourcen zur Verfügung und auch meist nicht das entsprechende Fachpersonal.

Das Handbuch führt den Leser kompetent und verständlich in die komplexe Materie ein und erörtert die verschiedenen Problemkreise. Es zeigt mögliche Bedrohungen und Gefahren auf, gibt praktische Hinweise und unterbreitet konkrete Lösungsvorschläge. Checklisten und Musterdokumente erleichtern zudem die Umsetzung der vorgeschlagenen Sicherheitsmassnahmen und ebnen den Weg zu angemessener Informations- und IT-Sicherheit.

«Das Sicherheitshandbuch befasst sich in verdienstvoller Weise sehr umfassend mit sämtlichen Aspekten der Datensicherheit und kann mit Fug und Recht diesbezüglich als wichtiges Standardwerk bezeichnet werden», kommentiert Hanspeter Thür, Eidgenössischer Datenschutzbeauftragter.

Das Buch richtet sich an IT-Betreuer, Datenschutz- und Sicherheitsbeauftragte in KMU und in kleinen bis mittelgrossen Verwaltungen sowie an Berater und Dienstanbieter im Bereich IT- und Informationssicherheit.

Die Diplom-Elektroingenieure Martin Sibler, Carlos Rieder und Peter Infanger reichten im Sommer 2000 die erste Version als gemeinsame Diplomarbeit beim IWI (Institut für Wirtschaftsinformatik) der Hochschule für Wirtschaft Luzern als Abschluss des Nachdiplomstudiums Informatiksicherheit NDS-INS ein. Carlos Rieder und Rolf Brunner (isec AG, Luzern) entwickelten danach das Buch kontinuierlich weiter. Im Rahmen einer Diplomarbeit des NDS-INS wurde im Frühling 2002 das Sicherheitshandbuch für die Praxis von Urs Achermann, im Sommer 2003 von Daniel Wüthrich und im Herbst 2004 von Wolfgang Sidler überarbeitet und erweitert.

**Wolfgang Sidler ist Security Consultant Manager Europe bei Zurich Financial Services, Executive Master of Information Security (EMIS) und Mitautor des Sicherheitshandbuches für die Praxis.*

Auszug aus den Themenbereichen

Management: IT-Sicherheitspolitik, Sensibilisierung des Managements, Sicherheitsorganisation, Informationssicherheitsprozess, Qualitätsmanagement, Personalwesen, Risiko-Management, Integrales Konzept, Wirtschaftlichkeit, Periodische Kontrollen und Revision.

Recht: Datenschutz, Urheberrecht und Lizenzen, Informatikverträge, Outsourcing, Vertrsaulichkeitsvereinbarungen mit Externen, Aufzeichnungs- und Archivierungspflichten, Haftung im Internet, strafrechtliche Aspekte, Computer Forensics, Überwachung von Online-Diensten am Arbeitsplatz und Versicherungen.

Organisation: Schulung und Sensibilisierung, Clear Desk, Schlüsselverwaltung, Entsorgen von Dokumenten, Richtlinien für Benutzer, Notfallvorsorge und BCP, Passwort-Richtlinien, Zugriffsschutz, Sicherheit im IT-Projektmanagement, Unterhalt und Reparatur.

Technik: Verschlüsselung, USV, Datensicherung, Virenschutz, Firewall, Remote Access, Umgang mit Online-Diensten (E-Mail, Internet), Wireless LAN, PDAs, physische Sicherheit, Datenbank- und Applikations-Sicherheit, Einsatz von Notebooks.

Bezugsquelle

Buchtitel	Sicherheitshandbuch für die Praxis
Herausgeber	Prof. Carlos Rieder
Informationen	www.sihb.ch
Auflage	Version 4.0
Umfang	A4-Ordner mit 337 Seiten inkl. CD
Verlag	Verlag Gisler, Altdorf
ISBN-Nr.	3-9521208-3-9
Preis	CHF 248.– inkl. MwSt