

# Informationen brauchen Kontrolle

Unternehmenskritische Daten und Dokumente gehören durch umfassende Maßnahmen geschützt.

**Sonja Gerstl**

Das Thema Informationssicherheit hat in den letzten Jahren in allen Branchen und Bereichen an Bedeutung gewonnen.

Die virtuelle Vernetzung und der stets wachsende Zugang zu neuen Informationsquellen prägen unser Kommunikations- und Informationsverhalten. Da an unsere Informationen Werte gebunden sind, die einen wesentlichen Faktor für den Erfolg und die Entwicklung eines Unternehmens darstellen, muss der Zugang zu unternehmenskritischen Informationen entsprechend kontrolliert und gesichert sein. Informationssicherheit nimmt einen immer wichtigeren Stellenwert ein.

Ursula Freiseisen-Pfneiszl, Unternehmenssprecherin von Raiffeisen Informatik: „Raiffeisen Informatik setzt sich zum Ziel, die Informationssicherheit des Unternehmens und seiner Kunden zu gewährleisten und zukunftsweisend auszubauen. Vertraulichkeit, Integrität und Verfügbarkeit sind unverzicht-

bare Grundwerte unserer Services und Produkte.

Durch gezielten Einsatz von Wissen und Technologie schaffen wir Vorsprung für uns und unsere Kunden.“ Die Raiffeisen-Informatik-Informationssicher-

sicherheitsstrategie wird auf Basis umfangreicher Recherchen, Marktforschungsdaten sowie Weiterbildungsmaßnahmen und dem technologischen Fortschritt entsprechend kontinuierlich weiterentwickelt. Re-

gelmäßige Audits stellen sicher, ob umgesetzte Maßnahmen die Sicherheitsziele auch adäquat unterstützen. Dabei wird die Wirksamkeit wie auch die Wirtschaftlichkeit überprüft. „Die Diskussion über die Aus-

lagerung der Informationstechnologie wird immer mehr als strategische und wichtige Management-Entscheidung gesehen. Waren Outsourcing-Projekte bisher vorwiegend aus Kostengründen motiviert, geht der Trend nun dazu, IT-Prozesse aus Gründen technologischer Herausforderungen hinsichtlich Sicherheit, Innovation und Beherrschbarkeit an professionelle Partner zu übergeben“, so Freiseisen-Pfneiszl.

Es bedarf nämlich in der Tat eines profunden Wissens um Thema Security und Informationssicherheit, um apotenziellen Gefahren effektiv entgegenwirken zu können. Sich hausintern einen solchen Profi zu leisten, ist mitunter sehr kostspielig.

Hier kann Outsourcing die Lösung sein. Die Vergabe der Unternehmens-IT an einen professionellen IT-Dienstleister ermöglicht Firmen, stets die aktuellsten Sicherheitsvorkehrungen eingesetzt zu haben, ohne hier erheblichen Mehraufwand leisten zu müssen.

[www.raiffeiseninformatik.at](http://www.raiffeiseninformatik.at)



Die Zusammenarbeit mit einem professionellen Rechenzentrum ermöglicht Unternehmen Zugang zu technischer Expertise, Prozessverbesserung und neuesten Technologien. Foto: Raiffeisen Informatik

## Vor Diebstahl und Missbrauch schützen

Videüberwachung, Brandschutz und Bewegungsmelder sorgen für die physische Sicherheit von IT-Systemen.

Kaum ein Unternehmen kann mehr von sich behaupten, unabhängig von Informationstechnologie (IT) seinem Business nachzukommen. Fällt die IT aus, besteht meist keine Alternative mehr, die Geschäfte fortzuführen. IT hat sich zur kritischen Komponente, zum Rückgrat der Unternehmen entwickelt, das aus eben diesem Grund auch entsprechend zu schützen ist. Eine wichtige Rolle spielt dabei unter anderem die physische Sicherheit der IT-Systeme und der gespeicherten Daten. Denn schließlich nützt die beste IT-Infrastruktur nichts, wenn diese nicht entsprechend den Geschäftsanforderungen ausgelegt und abgesichert ist.

### Umfassende Maßnahmen

„Nur Außenhaut- und Zutrittsschutz sind bei Weitem zu wenig! Bei Raiffeisen Informatik wird die physische Sicher-

heit gesamthaft betrachtet, und es werden bestehende Umfeldbedingungen mitberücksichtigt. Die physische Sicherheit ist für uns eine Selbstverständlichkeit und für unsere Kunden selbstverständlich auch ein wichtiges Entscheidungskriterium, wenn sie uns den Betrieb ihrer IT anvertrauen. Wir setzen umfassende Maßnahmen und treffen Vorkehrungen. Diese reichen von Videüberwachung, Bewegungsmeldern, Brandfrüherkennung, Brandschutz, Zutritts- und Zugriffsschutz, Datenspiegelung an mehreren Standorten, sichere Datenträgerentsorgung, Zutrittskontrollen bis hin zum Vier- oder Mehr-Augenprinzip in hochsensiblen Bereichen“, erläutert Michael Ausmann, Chief Security Officer von Raiffeisen Informatik, die umfassende Strategie.

Neben redundanter Energieversorgung, unterbrechungs-



Zum Schutz der Unternehmens-IT sind umfassende Sicherheitsvorkehrungen notwendig. Foto: Photos.com

freier Stromversorgung und Notstromaggregaten werden die einzelnen Gebäude des Un-

ternehmens basierend auf Sicherheitszonen- und Zutrittskonzepten darüber hinaus je

Zone mit unterschiedlichen Sicherheitsvorkehrungen abgesichert. Alle Vorkehrungen dienen dazu, die IT-Systeme und Daten der Kunden vor Verlust, Diebstahl und Missbrauch zu schützen.

### Professionelle Arbeit

Ausmann bekräftigt: „Es erfordert einen sehr hohen Zeitaufwand und intensive Beschäftigung mit dem Thema Security und Informationssicherheit, um den stets wachsenden Herausforderungen und den neuen Angriffen sinnvoll und effektiv entgegenwirken zu können. Das ist eine echte Herausforderung für Sicherheitsexperten und muss daher von solchen gemacht werden. Raiffeisen Informatik verfügt über eine fast 40-jährige Erfahrung im Umgang mit hochsensiblen Daten und im sicheren IT-Betrieb.“ sog

[www.raiffeiseninformatik.at](http://www.raiffeiseninformatik.at)