Special Innovation

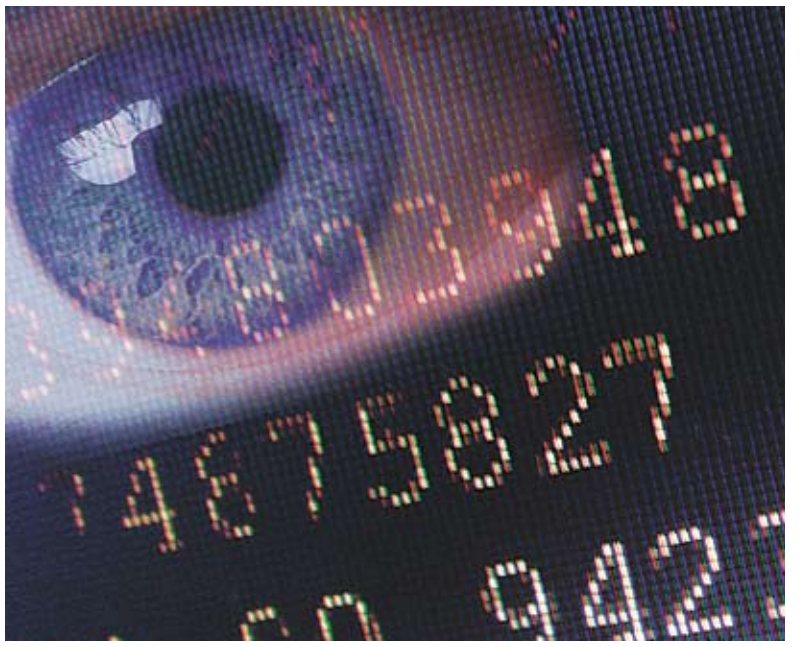
Diskrete Geschäfte im Tunnel

Datensicherheit wird zu einer zentralen und enorm aufwändigen Unternehmensaufgabe.

„Über 39 Mio. IT-Arbeitsstunden gehen jedes Jahr durch eine zu geringe Verfügbarkeit der IT-Systeme verloren“, warnt Dir. Wilfried Pruschak, Geschäftsführer der Raiffeisen Informatik GmbH. Ausfallzeiten bedeuten Umsatzverluste und Einbußen in der Kundenzufriedenheit. Die jederzeitige Verfügbarkeit der IT-Infrastruktur für unternehmenskritische Prozesse ist daher nicht nur aus geschäftlichen Notwendigkeiten erforderlich, sondern auch eine Frage des Ansehens.“

Laut einer Studie von Cumulus Research entstanden 2003 europaweit aufgrund von Systemausfällen über fünf Mrd. Euro an Verlusten, die sich aus 39 Mio. IT-Arbeitsstunden und 3,5 Mrd. Euro durch nicht verfügbare IT-Infrastruktur zusammensetzen. „Die Zeit, die Unternehmen mit wertvollen und teuren Mitarbeiterressourcen für die ständige Verfügbarkeit ihrer IT-Systeme aufwenden, stellt eine enorme Belastung an Unternehmensressourcen dar. In fünf Jahren werden bis zu vier Prozent des Umsatzes dafür ausgeben werden müssen – mehr als die Deckungsbeiträge in vielen Branchen“, so Pruschak. Betroffen sind Firmen aller Größenklassen. Nahezu alle kleinen Unternehmen haben inzwischen Internetanbindung und E-Mail. Rund 30 Prozent aller unternehmenskritischen Prozesse nutzen heute das Internet als Trägermedium. Sicherheitsmaßnahmen werden aber oft aus Unkenntnis links liegen gelassen.

Vielen Unternehmen wird die Bedeutung von eigener IT-Security erst bewusst, wenn es zu spät ist. Der Schaden, der allein durch Computerviren entsteht, beträgt in Österreich derzeit jährlich etwa 50 Mio. Euro, und seine Eintrittswahrscheinlichkeit ist deutlich größer als die eines Wasserschadens. Allerdings sind Viren wesentlich gefährlicher und können im Extremfall den Verlust unternehmens- oder projektrelevanter Daten bedeuten. Risikofaktor Nummer eins im Sicherheitsbereich sind aber nicht die Viren und Angreifer von außen, sondern das Chaos von innen: nachlässige Mitarbeiter und Unwissenheit in Sicherheitsfragen. Das beginnt beim leichtfertigen Gebrauch von Passwörtern und endet dort, wo Computernutzer auf so genannte Phishing-Attacken, das kriminelle Ausspähen von Passwörtern, hereinfallen – derzeit eine der aktuellsten Bedrohungen. *bra*



Ausfallsicherheit der IT-Infrastruktur und Schutz der Daten unternehmenskritischer Prozesse wird zu einer vorrangigen Aufgabe der Unternehmen. Foto: Bilderbox.com

Wilfried Pruschak: „In ein paar Jahren wird man bei kritischen Unternehmensprozessen wieder die IT aus der Steckdose beziehen, wie vor 30 Jahren, als die ersten Großrechner eingeführt wurden“, erklärt der Geschäftsführer der Raiffeisen Informatik.

Zentrale Datenhaltung ist der Weg der Zukunft

Ernst Brandstetter

economy: ***In den vergangenen Jahren haben Sicherheitsbedrohungen im Bereich der Informationstechnologie massiv zugenommen. Was ist der Grund dafür?***

Wilfried Pruschak: Tauscht man über das Internet kritische Daten aus, muss man auf eine Ebene mit höherer Sicherheit wechseln. Bei Raiffeisen haben wir hunderttausende Kunden im Internet-Banking. Daher muss in Sicherheit investiert werden, zum Beispiel, indem man Datentunnels baut und die übermittelten Daten auch ver- und entschlüsselt. Eine andere Möglichkeit sind Signaturen.

Höhere Sicherheit kostet bis zu vier Prozent des Umsatzes. Rentiert sich das?

Darüber gibt es keine Diskussion. Viele Prozesse sind ohne umfangreiche IT nicht zu bewältigen. Wir bei Raiffeisen wickeln täglich etwa 2,5 Mio. Transaktionen im Zusammenhang mit der österreichischen Lkw-Maut ab.

Steckbrief

Dir. Wilfried Pruschak, Geschäftsführer der Raiffeisen Informatik GmbH. Als drittgrößter IT-Services-Anbieter Österreichs serviciert das Unternehmen 10.000 Clients und verwaltet über 2.000 Server.

Was kann man gegen Angriffe von außen unternehmen?

Wir versuchen, die Hürden für Angreifer möglichst hoch zu machen. Manches kann man technisch bekämpfen, aber bei der aktuellsten Bedrohung, den Phishing-Attacken, gibt es dagegen kaum technische Mittel. Hier kann vor allem eine gewisse Bewusstseinsbildung hilfreich sein.

Das zweite Hauptthema ist Ausfallssicherheit.

Die Ansprüche wachsen exponentiell. In alten Zentralrechner-Systemen konnte man die Verfügbarkeit zu 100 Prozent steuern. Heute sehen wir uns mit vielfältigen Systemen von Großrechnern, gekoppelt mit Serversystemen, Routern und diversen selbstständigen Netzwerken, konfrontiert. Alle diese Stufen haben eigene Ausfallwahrscheinlichkeiten. Wenn man die multipliziert, fällt man von 99,9 Prozent Verfügbarkeit sehr rasch auf 95 Prozent zurück.

Welche Trends ergeben sich daraus?

Die zentrale Datenhaltung ist der Weg der Zukunft. Wir betreiben beispielsweise heute 20.000 Clients, was einen enormen Aufwand im Softwareversand und in der Datenhaltung nach sich zieht, wenn man es nicht zentral macht. In ein paar Jahren wird man bei kritischen Prozessen daher wieder IT aus der Steckdose beziehen, wie vor 30 Jahren.

Was bedeutet das für Unternehmen?

Die Wirtschaft wäre gut beraten, sich häufiger die Frage zu stellen, ob eine IT-Auslagerung nicht besser wäre, als alles semiprofessionell selbst zu machen. Die IT-Infrastruktur im eigenen Haus zu belassen, beruht meist auf Überlegungen, die den tatsächlichen Betriebsaufwand und die versteckten Kosten nicht berücksichtigen. Ich glaube, externe IT wird zum Normalfall werden. Es kommt ja auch niemand auf den Gedanken, selbst Strom zu produzieren.

Was bringt Outsourcing?

Die Auslagerung der gesamten IT kann die IT-Prozesse eines Unternehmens verbessern und hat einen unmittelbaren, positiven Effekt auf die Hochverfügbarkeit der Systeme. Unternehmen können durch Fremdvergabe von nicht zur Kernleistungserstellung zählenden Aufgaben ihre Ressourcen gezielt auf das Kerngeschäft richten und Investitionen in Randbereiche vermeiden.

info

Die 10 Gebote der IT-Sicherheit

- **Verantwortlichkeiten – Sicherheit ist Chefsache.** Geben und leben Sie eine Sicherheitsstrategie vor! Das reduziert die Risiken und ist die Ausgangslage für angepasste Maßnahmen, um den Geschäftsbetrieb aufrechtzuerhalten.

- **Datensicherung.** Beugen Sie möglichen Datenverlusten vor (irrtümliches Löschen, Viren, mechanische Defekte), indem Sie angemessene Datensicherungsmaßnahmen (Back-up) vorsehen! Bewahren Sie die Sicherungsmedien an einem anderen Standort auf.

- **Schutz vor Computerviren.** Ein System ohne Virenschutz auf dem neuesten Stand zu betreiben, ist heutzutage nicht mehr verantwortbar.

- **Sichere Verbindung.** Bei unzureichendem Schutz der internen IT-Infrastruktur (Clients, Server, Netzwerk) können Daten von außen manipuliert werden. Treffen Sie angemessene Sicherheitsvorkehrungen.

- **Software aktuell halten.** Fehler in der Software können von Angreifern, Viren oder Würmern ausgenützt werden, um sich Zutritt zu Systemen zu verschaffen. Setzen Sie rechtzeitig geprüfte und getestete Software-Patches, die von den Software-Herstellern angeboten werden, ein!

- **Umgang mit Passwörtern.** Geben Sie nie ein Passwort weiter, und schreiben Sie dieses auch nie auf! Zur Sicherstellung dieses Zugriffsschutzes setzen Sie adäquate Passwortregelungen ein.

- **Zutrittsregelungen.** Definieren Sie die unterschiedlichen Sicherheitszonen, und bauen Sie darauf die Schlüsselverwaltung auf. Generell darf ein Zutritt zum Unternehmen nur über den Empfang möglich sein.

- **Benutzerrichtlinien.** Legen Sie in einfach formulierten Benutzeranweisungen die Rahmenbedingungen für die Nutzung der zur Verfügung gestellten Infrastruktur fest.

- **Sensibilisierung der Mitarbeiter.** Schärfen Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter durch gezielte Schulungen!

- **Ordnung und Informationssicherheit.** Schaffen Sie Regeln für die Ablage von Informationen. Das gilt sowohl für die Papier- als auch für die elektronische Ablage. Sensible und vertrauliche Informationen müssen besonders geschützt werden.