Datensicherheit: Ihre Daten - Ihr Unternehmen - Ihr Kapital

Von Eric Drissler - ED Computer & Design e.K.

Die meisten Immobilienunternehmen setzen heutzutage, bei der täglichen Arbeit, auf die Unterstützung der Informationstechnologie. Hierdurch ergeben sich Zeitvorteile und natürlich die Möglichkeit die Daten weiterzuverarbeiten. Die moderne Technik birgt aber auch Gefahren: Was passiert wenn Daten verloren gehen? Was wenn die Systeme nicht laufen? Oder was passiert wenn Daten gestohlen werden? Für diese Fälle müssen geeignete Vorsorgekonzepte erstellt und umgesetzt werden.

Einen Datenverlust verhindert man durch Redundanzen und Datensicherungen. Gängige Serversysteme werden mit RAID-Systemen (redundant array of independent disks, deutsch: redundante Anordnung unabhängiger Festplatten) betrieben. Dies bedeutet, je nach RAID-Level, dass die Daten in einer Maschine auf zwei oder n-Festplatten gespiegelt werden.

Während diese Sicherheitslösung langsam zum Standard solcher Rechner wird, wird das Thema Datensicherung (Backup) mehrfach vernachlässigt. Häufig kämpfen IT-Dienstleister mit der Kundeneinstellung: „Keiner braucht Backups - aber alle brauchen Restores“.

Das notwendige Sicherungskonzept hängt dabei von den vorhandenen Gegebenheiten und Anforderungen ab. Denkbar sind: Sicherungen auf Festplatten, Streamer, CDs oder DVDs. Dabei spielt die Datenmenge und die gewünschte Zugriffszeit auf die gesicherten Daten die entscheidende Rolle. Auch über den Aufbewahrungsort sollten man sich Gedanken machen. Der Rollcontainer ist vielleicht nicht gerade der sicherste Ort in Bezug auf Einbruch, Diebstahl oder gar einen Brand. Viele Unternehmen setzen auf Offsite-Backups, wie der Name erkennen lässt Offsite = außerhalb des Standorts, bzw. Online-Backups. Ein Klon der Daten wird hierbei in einem Hochsicherheitsrechenzentrum abgelegt.

Aber nicht nur das Spiegeln und Sichern ist notwendig, sondern auch eine regelmäßige Kontrolle. Waren die Sicherungen erfolgreich und können die Daten

wiederhergestellt werden? Im Rahmen Ihres Sicherungskonzeptes sollte ein für diesen Prozess verantwortlicher Mitarbeiter benannt werden. Auch der Zugang zu den Serversystemen und Datensicherungen muss geregelt sein - immerhin ist eine Kopie einer Vollsicherung der einfachste Weg zu Ihren Daten.

Auch für den täglichen Zugriff auf die IT-Systeme sollte es Berechtigungen geben. Nicht allzu selten werden die Daten auf lokalen Rechnern, anstelle des gesicherten Serverlaufwerks, abgelegt. Des Weiteren dienen USB-Sticks, Wechseldatenträger und Brenner als unbemerktes Datentransportmittel.

Gerade die rechtlich vorgeschriebene E-Mail-Archivierung ist vielen nicht bekannt. Hierbei müssen Themen wie: Revisionssicherheit, Auffindbarkeit und Verfügbarkeit besonders beachtet werden. Durch diese Vorgaben reicht eine einfache Kopie eines E-Mail-Postfachs meist nicht aus, da nicht jede ein- und ausgehende Mail revisionssicher abgelegt wird. Geeigneten Lösungen werden vor Empfang und Versand in den E-Mailverkehr zwischengeschaltet und sorgen für die notwendige Rechtssicherheit. Selbstverständlich müssen Unternehmen über eine Regelung bezüglich der privaten E-Mail-Nutzung verfügen.

Im Rahmen Ihres Konzeptes sollten auch Sie Ihre externen Dienstleister im Auge behalten und zum Beispiel überprüfen, ob deren Mitarbeiter gemäß BDSG verpflichtet sind.

Vorsicht bei unbekannten E-Mail-Anhängen

Vorsicht, Seuchengefahr! Öffnen Sie auch nur einen falschen E-Mail-Anhang, ist Ihr PC schon infiziert. Nicht alles, was reinkommt, ist auch vertrauenswürdig. Manipulierte Dateien erreichen das Innere des Rechners dabei nämlich nicht nur via USB-Stick, CD, DVD oder durchs Surfen im Internet. Ein häufiger Weg, wie Ihr Rechner mit verseuchten Dateien infiziert wird, ist der leichtfertige Umgang mit E-Mail-Anhängen. Je nach Dateiendung können Sie schon im Vorfeld erkennen, ob eine Datei im Mail-Anhang eine Gefahr darstellt oder eher nicht. So sind EXE-Dateien ausführbare Programm-Dateien, die sofort nach einem Doppelklick ihr schadhaftes Werk beginnen können. Txt-Dateien sind reine Textdateien, die erst einmal ungefährlich sind.

Checkliste zum Schutz

- Installieren Sie einen guten Virenscanner, der die Nachrichten in Ihrem E-Mail-Programm überwachen kann und aktualisieren Sie ihn regelmäßig.
- Melden Sie sich nicht mit Administratorrechten an Ihrem Computer an, sondern nutzen Sie ein Profil mit eingeschränkten Rechten.
- Führen Sie keine angehängten Dateien direkt aus dem Mail-Programm heraus aus. Ein Schädling könnte sich hinter einer doppelten Dateiendung verstecken oder mittels spezieller Tools so präpariert sein, dass er harmlos erscheint. Nicht vertrauenswürdige Mail-Anhänge, die Sie interessieren, speichern Sie am besten in einen separaten Ordner und lassen diesen erneut durch Anti-Viren- und Anti-Spionage-Programme durchleuchten, bevor Sie eine Datei öffnen.
- Besondere Vorsicht ist geboten, wenn Dateien mit Endungen wie .exe, .com, .vbs, .bat, .sys, .reg im Anhang sind. Sie lauern nur auf einen Doppelklick. Diese ausführbaren Dateien starten nämlich unmittelbar und können sofort schadhaften Code auf Ihrem System verbreiten.
- Eine weitere Gefahr sind getarnte Exe-Dateien, wie zum Beispiel sample.jpg.exe. Wird die letzte Dateiendung im E-Mail-Programm nicht angezeigt, ist Sample.jpg nur als Bild-Datei zu erkennen. Achten Sie darauf, dass in den Voreinstellungen nicht Dateinamenerweiterungen bei bekannten Dateitypen ausblenden ausgewählt ist.
- So genannte „Spionageprogramme“ („Spyware“) sind oft in Gratis-Software eingebaut, die als E-Mail-Anhang angeboten wird. Lassen Sie Anti-Spyware-Programme nach den Datenschnüfflern suchen und sperren Sie die Spionagesoftware aus.

Prinzipiell gilt: Vertrauen Sie keinen E-Mail-Anhängen von unbekannten Absendern.

Auch durch Versprechungen im Text, der Anhang enthält tolle Programme oder flotte Video-Clips, sollten Sie sich nicht verleiten lassen. „Dateianhang nicht öffnen“ lautet hier die Devise.