Handel mit Computern und Bürosystemen - Wien

Datensicherheit für KundInnen und Firmen

Wie sicher sind Ihre Daten?

Fälschlicherweise wird im Alltag gerne der Begriff Datenschutz als Synonym für Datensicherheit verwendet. Von Datensicherheit ist aber nur dann die Rede, wenn man den technischen Schutz der Daten und die damit verknüpften Maßnahmen meint. Datenschutz umschreibt, wie der Name schon sagt, den Schutz personenbezogener Daten.

Grundlagen der Sicherung

Bei der Datensicherung wird mindestens eine Kopie einer Datei auf einem separaten Speichermedium abgespeichert. Wichtig ist, dass es sich hierbei um einen externen Datenspeicher handelt. Wie beispielsweise einem USB-Stick, eine externe Festplatte oder einen Clouddienst.

1. Spiegelung/RAID-Systeme

Bei der Spiegelung wird ein Datensatz auf zwei verschiedenen und voneinander unabhängigen Festplatten abgespeichert. Die beiden Festplatten sollten voneinander räumlich getrennt aufbewahrt werden. So gehen beim Ausfall eines der beiden Medien keine Informationen verloren

2. Zeitliche Sicherungen im Verlauf

Bei Windows 10 gibt es die Funktion „Dateiversionsverlauf". Dabei entstehen im Hintergrund automatisch Absicherungen eines Files. Mit dieser Funktion kann eine gelöschte, verlorene oder fehlerhafte Datei wiederhergestellt werden, indem man die Vorgängerversion abruft.
Ebenso kann die Rücksicherung von gelöschten Daten über eine inkrementelle Sicherung erfolgen.

3. Notfallsicherungen für Katastrophe

Um eine Notfallsicherung auch nach Brand, Vandalismus, Wasserschäden, etc. zu haben, müssen die Datenträger der Backups räumlich von den Rechnern getrennt sein. Nur so bleiben sie bei einem etwaigen Schadensfall unbeschädigt.

Neue Speichermedien sind günstiger geworden

Heutzutage kostet eine externe Festplatte nicht mehr eine Unmenge an Geld wie anno dazumal. Wir FachhändlerInnen können Festplatten mit entsprechender Speicherkapazität kompetent verkaufen und auch gleich die Hinweise für ordnungsgemäße Sicherungen geben.

Backupstrategie

Jedes Unternehmen sollte sich Gedanken zu einer Backupstrategie machen.
Um sensible Daten zu sichern, sollte es drei Kopien der Dateien geben. Bei einer Kopie könnte es nämlich passieren, dass aus einem unerfindlichen Grund die Datei nicht lesbar und somit defekt ist.
Ein weiterer Grund ist, dass die Kopie aufgrund äußerer Einflüsse beschädigt wird (Brand, Wasserschaden, etc.)

Strategien für private KundInnen - Das Motto hierbei lautet: 3-2-1:

- 3 Speicherungen
- 2 davon befinden sich an unterschiedlichen Orten
- 1 von ihnen befindet sich nicht zuhause

Hierbei benötigt man entweder eine externe Festplatte, einen Cloud-Service oder zwei Festplatten, wobei sich eine davon außer Haus befindet.

Wie sorgen Firmen vor?

Firmen sollten diverse Maßnahmen setzen, um deren Daten zu sichern.
Zum einen sollten Mitarbeiter und Mitarbeiterinnen eingeschult und mit eingebunden werden. Denn nur so können sie sensibilisiert werden.
Ein Virenschutz und eine Firewall sind ebenfalls in Betracht zu ziehen, um vor etwaigen „Angriffen" geschützt zu sein. Die Verschlüsselung der Daten ist zu beachten, damit nur berechtigte Personen Zugriff auf die jeweiligen Daten haben.

Cloudlösungen

Wenn man eine kleine bis mittlere Menge an Daten besitzt, kann eine Online-Datensicherung durchaus in Betracht gezogen werden. Der Vorteil hierbei ist, dass die dort abgespeicherten Daten nicht mit dem Original verknüpft sind.
Aus dem Datensicherheitsaspekt sind Cloud-Dienste sinnvoll, denn die Absicherung der räumlich getrennten Daten erweist sich als durchaus praktisch und sinnvoll.

Aber Achtung, wenn es um den Datenschutz geht. Denn hier sind Cloudlösungen mit Vorsicht zu genießen. Wichtig ist vorerst, dass der Standort sich in Europa befindet und nicht so wie viele Anbieter in den USA. Weiters gibt es noch ein Zertifikat (BDSG). Wenn dieses vorhanden ist, dann entspricht der Anbieter den DSGVO-Normen. Zahlreiche Anbieter aus Österreich bieten professionelle Services für Unternehmen.

Die wichtigsten Sicherheitsaspekte noch einmal kurz zusammengefasst:

1. Die regelmäßige Sicherung der Daten
2. Das zusätzliche Abspeichern auf externen Speichermedien
3. Die Verschlüsselung der gespeicherten Daten
4. Die Nutzung einer Software, die automatisch im Hintergrund arbeitet
5. Die regelmäßige Überprüfung zur Vergewisserung, dass die Daten funktionsfähig sind

› Certified Data & Security Expert Betriebe Wien