Datensicherung IT-Richtlinie BSI:

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinen IT-Grundschutz-Katalogen generelle Richtlinien erarbeitet, die Unternehmen beim Aufbau einer sicheren IT-Umgebung unterstützen sollen. Dabei liegt der forcierte Schwerpunkt auf pauschalisierten Gefahren, die anhand der Vorgaben auch von Laien identifiziert und ggf. mit Hilfe von Fachleuten behoben werden können. Dadurch soll es auch fachfremden Unternehmen ermöglicht werden, bei vergleichsweise geringem Aufwand einen hinreichenden IT-Grundschutz zu entwickeln. Natürlich deckt dieser Basisschutz nicht alle Eventualitäten ab und ist für Firmen mit extrem hohen Sicherheitsbedarf selbstverständlich allein nicht ausreichend.

Datensicherung ist ein wichtiger Bestandteil des IT-Grundschutzes.

Datensicherung ist für Unternehmen überlebenswichtig

Oft ist den Verantwortlichen in den Unternehmen überhaupt nicht klar, welche Anforderungen an die Sicherheit bestehen. Neben anderen Bereichen betrifft dies vor allem das Thema Datensicherung, das für gewerbliche IT-Systeme (auch aus fiskalrechtlichen Gründen) verpflichtend ist. Um die Gefahren eines möglichen Datenverlusts besser einschätzen zu können, empfiehlt das BSI allen Betrieben, einige grundsätzliche Fragen zu klären.

Gibt es eine Backupstrategie?

Es ist bei der Komplexität heutiger IT-Systeme nicht mehr ausreichend, nur bestimmte Daten auf irgendwelche Datenträger zu sichern. Vielmehr muss gewährleistet sein, dass eine regelmäßige und vor allem umfassende Datensicherung durchgeführt wird, um im Notfall eine Wiederherstellung aller wichtigen Komponenten zu gewährleisten. Hierfür empfiehlt es sich, eine Backupstrategie zu entwickeln, die festlegen sollte, welche Daten in welchem zeitlichen Rhythmus zu sichern sind. Auch der Speicherort spielt dabei eine Rolle, beispielsweise kann man die physische Sicherung auch in entsprechend zertifizierte Cloud-Systeme auslagern.

Ist festgelegt, welche Daten wie lange gesichert werden?

Nicht alle Daten sind gleich wichtig. So wie im normalen Papierbüro auch, können manche Daten nach einer gewissen Zeit entsorgt werden, während andere längere Zeit als Nachweis behalten werden müssen bzw. sollten. Da dies bei manchen Firmen zu extrem großen Datensammlungen führen kann, sollte festgelegt sein, wann Daten wieder gelöscht werden können (falls überhaupt). Besondere Aufmerksamkeit sollte außerdem personenbezogene Kundendaten gelten, für deren Löschung zum Teil datenschutzrechtliche Bestimmungen maßgeblich sein können.

Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?

Nur wenige Unternehmen sind heute noch rein auf Desktop-Systeme ausgerichtet. Mitarbeiter im Außendienst oder in bestimmten Unternehmensbereichen (z.B. Lager) greifen häufig auf mobile Geräte und tragbare Computer zu, die nicht immer aktuell vernetzt sein müssen. Bei der Datensicherung dürfen diese Geräte nicht vergessen werden. Eine regelmäßige Synchronisierung ist dringend zu empfehlen, um keine wichtigen Vorgänge zu verlieren.

Werden die Sicherungsbänder regelmäßig kontrolliert?

In vielen Unternehmen wird das Backup noch immer auf Sicherungsbändern durchgeführt. Unabhängig vom Speichermedium (Bänder, Festplatten, optische Datenträger etc.) sollte eine regelmäßige Überprüfung stattfinden, ob die Medien noch einwandfrei funktionieren. Denn das beste Backup hilft nichts, wenn die Datenträger sich nicht mehr lesen lassen. Hilfreich kann dabei auch eine redundante Auslegung sein, also die Anfertigung weiterer Kopien auf andere Medien oder geeignete Cloud-Speicher.

Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

Damit man die Backups auch später noch zu jeder Zeit nachvollziehen kann, sollten sämtliche Sicherungs- und Rücksicherungsverfahren ausreichend dokumentiert werden. Dies dient nicht nur einer besseren Organisationsstruktur der Backupstrategie, sondern auch dem Nachweis über die kohärente Durchführung von Datensicherungsmaßnahmen. Dies kann bei Versicherungsfällen oder auch bei unklaren Fragen durch Finanz- und andere Aufsichtsbehörden von Vorteil sein. Nicht zuletzt erleichtert eine gute Dokumentation auch die Behebung von eventuellen technischen Problemen.

Warum braucht es eine Datensicherung?

Jederzeit kann es passieren: Ein Crash auf der Festplatte und nichts existiert mehr von dem, was vorher da war. Für den Fall, dass dies geschieht, sollten Sie entsprechende Schutzmaßnahmen präventiv einleiten. Die wichtigste Schutzmaßnahme ist das Anlegen einer Datensicherung. Dies ist definitiv **essentiell**: Eine richtige Datensicherung umfasst mehr als nur das Kopieren der Dateien. Was nützt Ihnen z.B. ein Backup für den seltenen Fall, dass Ihr Geschäft oder Arbeitsplatz Opfer eines Brandes wird und ihre Backup-Harddisk in der Schublade Ihres Schreibtisches ebenfalls verbrannt ist: Es besteht zwar eine nur geringe Wahrscheinlichkeit mit dafür aber umso höherem Schaden!

Warum ist Datensicherung essentiell?

Wenn Sie sich nicht schützen und kein Backup erstellen, müssen Sie mit einem Totalverlust rechnen. Datenrettungsfirmen, welche die unbeschädigten Daten noch von der Platte retten könnten, werden die meisten Personen nicht beauftragen, da eine Datenrettung schnell **Tausende von Euro** kosten kann. Selbst dann ist nicht garantiert, dass alle Daten wiederhergestellt werden können. Machen Sie heute den ersten Schritt, und schützen Sie sich vor einem potentiellen Datenverlust. Als wichtigste Maßnahme gilt, regelmäßig Datensicherungen durchzuführen.