# 9 Risiken beim Datentransfer

## *Wie können Unternehmen sich und Ihre Mitarbeiter schützen?*

**Datenverlust, Virenbefall, Erpresser-Software – ein Albtraum für jedes Unternehmen! Doch welche Risiken lauern tatsächlich beim digitalen Datentransfer, und wie kann man sich davor schützen?**

Die meisten Unternehmen sind heutzutage auf digitale Datenübertragung angewiesen. Dabei setzen allerdings viele Angestellte auf unsichere und von der Geschäftsleitung nicht autorisierte Methoden wie Mail oder cloudbasierte Filesharing-Angebote ohne besondere Zertifizierung.

Welche Risiken der Datentransfer im Internet für Unternehmen und Angestellte konkret bergen kann, haben wir hier für Sie zusammengetragen:

- **Datenverlust/Datendiebstahl**
  Daten „zu verlieren“, ist eines der häufigsten Probleme bei der Verwendung unsicherer Übertragungsmethoden im Internet. Das umfasst sowohl
  - den Verlust vertraulicher Informationen als auch
  - den unbefugten Zugriff Dritter auf sensible Daten.

  Laut der aktuellen Studie Global Data Protection Index kostet jeder Datenverlust deutsche Unternehmen im Schnitt eine halbe Million Euro. Als Ursachen kommen verlorene Passwörter, aber auch Bedienfehler oder fahrlässige Handlungen von Seiten des Dienstbetreibers in Frage.

- **Beschädigte Daten**
  Manchmal werden Daten durch fehlerhafte Datenträger, Übertragungsprotokolle oder Schnittstellen beschädigt und müssen aufwendig repariert oder wiederhergestellt werden – falls das noch möglich ist. Laut einer aktuellen Kroll-Studie gehören beschädigte Daten zu den Hauptursachen für Datenverlust in deutschen Unternehmen.

- **Schadsoftware**
  Der Begriff Schadsoftware umfasst sowohl Viren als auch andere Schadprogramme wie Würmer, Trojaner, Spyware und Erpresser-Software. Die Folgen können von unerwünschten Werbeeinblendungen über Spionage und Datendiebstahl bis hin zu Erpressungsversuchen reichen – letztere sind einer KPMG-Umfrage zufolge besonders häufig.
  Von den Mitarbeitern kann man selbstverständlich nicht erwarten, mit allen Formen von Malware vertraut zu sein; hier müssen Unternehmen entsprechende Schutzmaßnahmen treffen.

- **Spam**
  Die meisten Formen von Spam sind nervig, aber harmlos. Laut des aktuellen Cisco Cybersecurity Report 2017 machen Spam-Mails immerhin 65 Prozent des täglichen Mail-Aufkommens in Unternehmen aus – allerdings werden die Methoden der Spammer immer raffinierter, so dass es zunehmend schwieriger wird, Spam zuverlässig als solchen zu erkennen.
  Immerhin: Schadcode enthalten nur rund 8 Prozent aller Spam-Mails.

- **Phishing/Identitätsdiebstahl**
  Spam-Mails sind oft getarnte Phishing-Versuche. Beim Phishing wird versucht, mit Hilfe gefälschter Mails, Webseiten und Kurznachrichten Informationen über Unternehmen und ihre Angestellten herauszufinden. Dazu gehören beispielsweise Zugangsdaten zu Online-Diensten, aber auch Kreditkarten- und andere Zahlungsinformationen, mit deren Hilfe dann beispielsweise unautorisierte Transaktionen getätigt werden. Sogar in den Verbindungsdaten können Cyberkriminelle Anknüpfungspunkte finden, die ihnen helfen, arglose Opfer zu täuschen. Diese Form des Datenmissbrauchs bezeichnet man auch als Identitätsdiebstahl.

- **Hacker-Angriffe**
  Obwohl hinter Schadsoftware und Phishing-Mails oft ebenfalls Hacker stecken, können Unternehmen auch ganz gezielt Opfer eines Hacker-Angriffs werden. Das können DDoS-Attacken sein, bei denen „nur" die Server eines Unternehmens lahmgelegt werden, aber auch Versuche, auf vertrauliche Daten und Informationen zuzugreifen. Hacker können Sicherheitslücken in Übertragungsprotokollen oder unsicheren, öffentlichen Cloud-Diensten nutzen, um sich unbefugten Zugang zu fremden Rechnersystemen zu verschaffen. Vor allem der Mittelstand rückt in Deutschland zunehmend stärker ins Visier von Cyberkriminellen, wie eine aktuelle PwC-Studie zeigt.

- **Incompliance**
  Für den Umgang mit bestimmten Daten gibt es gesetzliche Vorschriften, die es zu beachten gilt. Das betrifft beispielsweise die Erhebung, Speicherung und Übertragung personenbezogener Daten – dazu gehören auch Kundendaten. Der Verstoß gegen diese Vorschriften kann mittlerweile empfindliche Strafen nach sich ziehen. Und ab dem 25. Mai 2018 wird es noch strenger: Dann tritt die EU-Datenschutz-Grundverordnung in Kraft. Mit ihr werden zahlreiche neue Informations- und Dokumentationspflichten für Unternehmen eingeführt. Bei Verstößen sieht die Datenschutz-Grundverordnungen Strafzahlungen bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens vor.

- **Ruf- und Imageschäden**
  Abgesehen von den direkten wirtschaftlichen Schäden und rechtlichen Konsequenzen, die ein Datenverlust, Hacker-Angriffe oder Schadsoftware anrichten können, müssen betroffene Unternehmen einen Imageverlust in Kauf nehmen; im schlimmsten Fall verlieren sie dadurch Partner und Kunden. Eine derart beschädigte Reputation wieder herzustellen, erfordert viel Aufwand. Schon Investment-Guru Warren Buffet sagte: „Es dauert 20 Jahre, sich einen guten Ruf aufzubauen – und fünf Minuten, ihn wieder zu zerstören."

- **Verstoß gegen interne Richtlinien**
  Dieser Punkt betrifft speziell Angestellte, die – oft unwissentlich – unsichere Übertragungsmethoden anwenden. In einer Tenable-Umfrage gaben 65 Prozent aller befragten Unternehmen an, dass die Nutzung von Schatten-IT – also unautorisierter Geräte oder Anwendungen – in den vergangenen zwölf Monaten zu einem Angriff auf Unternehmensdaten geführt hat. Bei 39 Prozent der Befragten wurden in der Folge sogar Daten entwendet.

Die Risiken sind also beträchtlich: Unsichere Datenübertragung kann nicht nur für die Unternehmen, sondern auch für Angestellte, Partner und Kunden unangenehme Folgen haben. Die wirtschaftlichen Schäden sind zum Teil verheerend.

Um sich und ihre Mitarbeiter effizient zu schützen, müssen Unternehmen auf Lösungen setzen, die eine sichere und möglichst gesetzeskonforme Datenübertragung gewährleisten. Eine geeignete

Übertragungsmethode sollte mindestens die folgenden Kriterien erfüllen:

- ✓ **Verschlüsselte Übertragung:** Die Dateien müssen während der Übertragung vor Fremdzugriffen geschützt sein.

- ✓ **Verschlüsselte Speicherung:** Die Daten müssen verschlüsselt auf dem Server gespeichert werden. Sie müssen vor unbefugtem Auslesen geschützt sein.

- ✓ **Geschützte Metadaten:** Die Metadaten (Verbindungsdaten) müssen durch technische Maßnahmen so unkenntlich gemacht werden, dass sich daraus keine Rückschlüsse darüber ableiten lassen, wer wann mit wem wie viele Daten ausgetauscht hat.

- ✓ **Geeigneter Speicherort:** Mindestens ebenso wichtig wie die Verschlüsselung sind Standort und Beschaffenheit des Servers. Dritte dürfen keine Möglichkeit haben, Daten auszulesen, zu löschen, zu missbrauchen oder zu beschädigen.

- ✓ **Betreibersicherheit:** Um einen Datenverlust oder -missbrauch vollends auszuschließen, darf auch der Betreiber eines Dienstes bzw. des Rechenzentrums keine Möglichkeit haben, auf Daten oder Metadaten zuzugreifen.

Unternehmen sollten zusätzlich ihre Mitarbeiter entsprechend schulen, damit sie wissen, wie ein sicherer und verantwortungsvoller Umgang mit vertraulichen Daten aussieht. Das erfordert aber auch, dass die Unternehmen Tools anbieten, die sich genauso leicht und verbraucherfreundlich verwenden lassen wie die privat genutzten, aber leider oft unsicheren Dienste: Nur so kann sich eine sichere Übertragungsmethode wirklich durchsetzen – andernfalls greifen Mitarbeiter auf die unsicheren, aber bequemeren Methoden zur Datenübertragung zurück.

Mit der Wahl eines geeigneten Anbieters kann sich ein Unternehmen übrigens nicht nur wirkungsvoll gegen Hacker, Datenverlust und Schadsoftware schützen. Es sichert sich auch rechtlich ab: Ein Unternehmen, dass sich für einen Cloud-Anbieter entscheidet, der mit in der zum Schutzbedarf der eigenen Daten passenden Schutzklasse nach dem Trusted Cloud Datenschutzprofil (TCDP) zertifiziert ist, entspricht automatisch seinen gesetzlichen Kontrollpflichten. Die datenschutzrechtlichen Anforderungen des Bundesdatenschutzgesetzes wurden bei der Entwicklung dieses Zertifikats ebenso berücksichtigt wie die Anforderungen der EU-Datenschutz-Grundverordnung.

**Weiterführende Links:**

- Schutzbedarfs-Rechner für Unternehmen – welcher Cloud-Dienst ist der richtige?
- Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)
- Wie bleibt ein Geheimnis in der Cloud gewahrt?
- So täuschend echt sind Phishing-Mails

**Quellen:**
https://germany.emc.com/microsites/emc-global-data-protection-index/index.htm
https://www.krollontrack.de/unternehmen/pressemitteilung/datenverlust-index/
https://home.kpmg.com/de/de/home/themen/2017/04/ecrime-studie.html
http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464170
https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf
https://www.datenschutz-grundverordnung.eu/
http://www.tenable.com/press-releases/rise-in-shadow-it-linked-to-more-cyberattacks-in-germany-than-in-the-uk-according-to