FRAGEN UND ANTWORTEN

Datensicherheit und Schutz vor Datenverlust

Auch für kleinere Unternehmen spielt die Sicherheit der Geschäftsdaten eine große Rolle. Wenn Sie nicht mehr darauf zugreifen können, steht im schlimmsten Fall der Betrieb still! Hackerangriffe, Viren oder schlicht die kaputte Festplatte: Es gibt viele Fragen zur Sicherheit von Daten. Beim Lexware Unternehmertag Datensicherheit stand **Experte Thomas Schirmer** Ihnen daher Rede und Antwort!

Hier können Sie direkt zum jeweiligen Themenbereich springen:

Allgemeine Fragen zur Arbeit mit Daten

Was sind die wichtigsten Aspekte beim Thema Datensicherheit, die jeder Unternehmer auf dem Schirm haben sollte?

Antwort: Das ist ein sehr weites Feld: Virenschutz, Update-Sicherheit, Datensicherung, Zugriffsschutz, Zugangsschutz und vor allem aber auch die Beachtung der nicht-digitalen Umgebung. Die besten digitalen Sicherheitsmaßnahmen nützen nichts, wenn z. B. vertrauliche oder personenbezogene Informationen im Altpapier landen.

Im Tagesgeschäft habe ich eigentlich keine Zeit, um mich großartig um die Sicherheit der Daten auf meinem Betriebs-PC zu kümmern. Wie kann ich denn meine Daten schützen, ohne zu viel Zeit reinstecken zu müssen?

Antwort: Das ist eine gute Frage! Versuchen Sie, möglichst viele Vorgänge zu automatisieren: z. B. automatische Updates für Virenschutz- und Anwendungsprogramme sowie das Betriebssystem oder eine automatische Zuwachsdatensicherung.

Lohnt es sich, für meine Mitarbeiter einen Benutzerzugang mit eingeschränkten Rechten einzurichten?

Antwort: Auf einem Windows-Rechner auf jeden Fall. Man könnte das sogar verallgemeinern und jedem Nutzer empfehlen, grundsätzlich mit eingeschränkten Rechten zu arbeiten.

Der Sicherheitsaspekt dabei ist, dass ein Nutzer mit eingeschränkten Rechten keine Änderungen der Systemeinstellungen vornehmen und auch keine Programme installieren kann. Wenn ein Schadprogramm unbemerkt über das Internet auf den Rechner gelangt, kann es auch nur mit eingeschränkten Rechten arbeiten und z. B. keine weiteren Programme installieren. Die alltägliche Arbeit am PC ist aber auch mit eingeschränkten Rechten möglich.

Wenn Sie zusätzlich ein Administrator-Konto einrichten, kann man bei Bedarf für die Installation von Programmen oder für die Änderung von Systemeinstellung die Administratorrechte nur für diesen Zweck einsetzen und dann automatisch in den eingeschränkten Modus zurückwechseln. Bei allen Aktionen, die zusätzliche Rechte erfordern, erscheint ein entsprechendes Abfragefenster.

Daten speichern und wiederherstellen

Was sind gängige Fehler bei der Datensicherung und wie kann ich sie vermeiden?

Antwort: Da gibt es einige Fehler, die Sie relativ leicht vermeiden können:

- Daten werden nicht häufig genug gesichert (mindestens einmal am Tag), sodass bei einem Systemausfall zu viele Daten verloren gehen.
- Es wird nur ein Datensatz gespeichert.
- Daten werden nur online bei einem Cloudanbieter gespeichert.
- Daten werden nur vor Ort gespeichert
- Externe Sicherungsmedien (z. B. externe Festplatten) verbleiben am Gerät und sind daher ebenso Malware-gefährdet wie die PCs selbst
- Die Wiederherstellung (Restore) der Daten wird nicht geübt und lässt sich daher nicht zeitnah oder im schlimmsten Fall gar nicht durchführen.

Abhilfe schafft eine automatische schrittweise Zuwachsdatensicherung (d. h. die Daten sollten einmal komplett gespeichert werden, dann nur noch Daten, die hinzukommen oder geändert werden), z. B. mit Time Machine (macOS) oder Windows-Backup. Auch die 3-2-1 Faustregel hilft hier weiter: 3 Sicherungssätze, 2 unterschiedliche Medien (z. B. externe Festplatte, USB-Stick, beschreibbare DVD) und 1 externer Speicherort (Cloudsystem, Banktresor).

Mein Tipp:

Setzen Sie ein NAS-System (Network Attached Storage) mit mehreren Festplatten ein, die als RAID-System arbeiten, das für Ausfallsicherheit sorgt. Zum Lieferumfang gehört normalerweise auch ein maßgeschneidertes Programm zur Datensicherung. Proben Sie immer mal wieder den Ernstfall.

Ich speichere meine Daten regelmäßig (ein bis zweimal in der Woche) auf einer externen Festplatte. Reicht das?

Antwort: Das kommt ganz auf die Daten an. Zu empfehlen ist eine automatische Datensicherung, die in kurzen Abständen (z. B. stündlich) vorgenommen wird. Das lässt sich recht einfach direkt mit der Backup-Funktion von Windows oder macOS realisieren. Sie sichern die Daten Ihres Rechners erst komplett und dann nur noch die Daten, die neu hinzukommen oder verändert werden.

Wie teuer ist es, wenn ich die Daten auf meiner Festplatte wiederherstellen lassen muss?

Antwort: Das lässt sich nicht pauschal beantworten. Wenn die Festplatte einen mechanischen Schaden hat oder gar verformt ist, kann die Wiederherstellung, wenn sie überhaupt möglich ist, durchaus mehrere Tausend Euro kosten. Liegt „nur“ ein Softwareproblem vor, können u. U. sogar kostenlos erhältliche Wiederherstellungsprogramme wie „PC Inspector File Recovery“ helfen. Datenrettungsunternehmen wie Convar oder Ontrack arbeiten mit Kostenvoranschlägen.

Weitere Informationen zur Datenwiederherstellung finden Sie auf der Lexware Themenseite Datenrettung.

Ich habe noch einige Daten auf USB-Sticks und zum Teil auf CD-ROMs. Ist das sicher genug?

Antwort: Nein, zumindest nicht auf Dauer. Alle Datenträger haben eine begrenzte Haltbarkeit, auch nicht-mechanische Datenträger wie USB-Sticks und CDs/DVDs. Sie sollten die Daten sicherheitshalber mindestens alle 5 Jahre auf neue Datenträger übertragen und dann vielleicht auch gleich auf CDs/DVDs verzichten, da immer weniger PCs und Notebooks mit einem CD/DVD-Laufwerk ausgestattet werden.

Wenn ich die Daten nicht lokal speichern will: Worauf muss ich achten, wenn ich meine Daten bei einem Cloudanbieter speichern will?

Antwort: Darauf, dass die Daten verschlüsselt übertragen und gespeichert werden, damit ausgeschlossen ist, dass die Daten während der Übertragung abgegriffen werden können und dass weder der Cloudanbieter selbst noch Hacker Zugriff auf die Daten bekommen können.

Werden personenbezogene und/oder steuerrelevante Daten gespeichert, muss auch der Standort des Cloudservers beachtet werden. Dieser muss dann innerhalb der EU liegen. Kostenpflichtige Cloudspeicher großer Anbieter wie Amazon, Telekom, Microsoft garantieren dies, es gibt aber auch viele andere Anbieter mit Sitz in Deutschland oder der Schweiz wie z. B. Strato oder Tresorit.

Grundsätzlich gilt: Sensible betriebliche Daten nicht auf den großen kostenlosen Cloudsystemen von Google (Google Drive), Microsoft (One Drive) oder Dropbox sichern!

Weiterführende Informationen zum Thema Datensicherung erhalten Sie auf der Lexware Themenseite Datenverlust.

Schutz vor Viren, Trojanern und Co.

Wie kann ich mich am besten vor Viren schützen? Reicht der Windows-Defender dazu aus?

Antwort: Grundsätzlich reicht der Windows Defender aus. Die Virenschutzlösungen spezialisierter Hersteller wie Avira, Kaspersky oder McAfee bieten allerdings zusätzliche Schutzfunktionen. Zum Beispiel gegen Ransomware. Zudem haben sie einen eigenen Support, an den Sie sich direkt wenden können.

Für ein paar meiner Mitarbeiter ist das Internet „Neuland“. Was kann ich tun, um sie vor Spam, Phishing etc. zu schützen?

Antwort: Grundschutz einrichten (aktuelles Betriebssystem, aktuelles Virenschutzprogramm, Einsatz der Schutzmechanismen von Windows/macOS, Spamfilter aktivieren etc.), immer wieder über Gefahren aufklären und insbesondere für Phishing-Angriffe sensibilisieren. Es gibt z. B. Online-Trainings zum Erkennen von Phishing-Mails (etwa sosafe.de).

Reicht es aus den PC mit einem Kennwort vor „Fremden“ zu schützen, wenn eine Firewall vorhanden ist?

Antwort: Wenn Ihr Rechner grundgeschützt ist (Virenschutz, Firewall, aktuelle Software) reicht der Zugriffsschutz per Kennwort aus, um den PC vor einem direkten Fremdzugriff zu schützen.

Man liest ja in letzter Zeit viel von solchen Hacker-Angriffen. Kleine Unternehmen brauchen sich da aber ja bestimmt keine Sorgen zu machen, oder?

Antwort: Egal, ob klein oder groß, die Bedrohungslage ist die gleiche. Das Problem ist, dass sich Schadprogramme mittlerweile im Internet in Baukastensystemen „zusammenklicken“ und über Spamverteiler auf die Reise schicken lassen. Man braucht also keinen Sachverstand mehr, um zum Hacker zu werden. Und treffen kann es tatsächlich jeden Rechner, der mit dem Internet verbunden ist.

Weitere Informationen zum Schutz Ihrer Daten vor Viren, Trojanern und Co. erhalten Sie auf der Lexware Themenseite Datenmissbrauch.

Sicherheit im Internet

Ich habe ein kleines Café und wir wollen unseren Kunden in Zukunft W-Lan anbieten. Dürfen wir das einfach so?

Antwort: Ein klares Ja! Das dürfen Sie einfach so, weil Sie nicht mehr dafür haften müssen, was Ihre Kunden im Internet treiben. Es gibt keine „Störerhaftung“ mehr. Allerdings sollte der WLAN-Zugang geregelt und sauber von Ihrem eigenen Internetzugang getrennt erfolgen. Würden Sie Ihren eigenen WLAN-Zugang einfach Ihren Gästen zur Verfügung stellen (was rechtlich sogar OK wäre), könnten diese darüber schlimmstenfalls auf Ihren PC oder Ihr lokales Netzwerk zugreifen.

Unternehmen wie die Telekom oder Hotsplots bieten „Kunden-WLAN-Lösungen“ an, die nicht nur für Sie und Ihre Kunden datensicher sind, sondern auch vor dem WLAN-Zugriff über eine Willkommens-Seite über alle rechtlichen Aspekte informieren und Ihren Gästen eine Einverständniserklärung abverlangen, die DSGVO-konform ist.

Ganz rechtsfrei sind öffentliche WLAN-Zugänge aber nicht. Würde es wiederholt zu Rechtsverletzungen kommen, weil Ihre Gäste illegal downloaden, könnten die Rechteinhaber auf Unterlassung klagen. Das Risiko ist aber durch den Wegfall der Störerhaftung jedoch sehr gering.

Ich bekomme immer diese Cookie-Hinweise. Sind Cookies gefährlich?

Antwort: Grundsätzlich sind Cookies an sich nicht gefährlich.

Es handelt sich dabei um kleine Textdateien, in denen Informationen zum Aufruf einer Internetseite gespeichert werden, die bei einem erneuten Aufruf der Seite wieder abgerufen werden können. Anhand eines Cookies erkennt z. B. ein Online-Shop-System, dass Sie dieses schon einmal benutzt haben und erspart es Ihnen, dass Sie Ihre Adressdaten erneut eingeben müssen.

Cookies können also der Benutzerfreundlichkeit diesen. Andererseits handelt es sich dabei schon um persönliche Daten, schließlich geben die vielen Cookies, die auf Ihrem Rechner gespeichert sind, Auskunft über Ihr Nutzerverhalten. Cookies können ausgelesen und zur Erstellung eines Nutzerprofils verwendet werden. Sie sollten daher Cookies nicht grundsätzlich, sondern nur gezielt zulassen. Sie finden in allen gängigen Browsern dazu eine entsprechende Einstellungsmöglichkeit. Beachten müssen Sie dabei aber auch, dass Sie einige Internetseiten vielleicht nur noch eingeschränkt nutzen können, wenn Sie keine Cookies zulassen.

Kann ich mich auf die digitalen Zertifikate von Websites verlassen?

Antwort: Es gibt keine 100-prozentige Sicherheit! Auch digitale Zertifikate können gefälscht sein. Andererseits aber bieten digitale Zertifikate ein sehr hohes Maß an Sicherheit und werden ständig auf ihre Gültigkeit überprüft. Sollte Ihnen allerdings Ihr Browser beim Aufruf einer Internetseite mitteilen, dass das digitale Zertifikat abgelaufen ist oder es Probleme damit gibt, sollten Sie diesen Hinweis ernst nehmen und prüfen, ob Sie die Seite wirklich aufrufen müssen.

Hardware und Schutz vor äußeren Einflüssen

Kann ich schon beim Rechner-Kauf auf Datensicherheit achten? Gibt es Unterschiede zwischen den Herstellern?

Antwort: Datensicherheit kann man leider nicht als solche kaufen. Unterschiede zwischen den Hardware-Herstellern gibt es allerdings schon zu beobachten. Grundsätzlich gilt: Finger weg von absoluten Schnäppchenangeboten! Nicht immer, aber häufig kommen die günstigen Preise dadurch zustande, dass tatsächlich minderwertige Bauteile wie Festplatten oder Arbeitsspeicher verwendet werden, die entweder B-Ware namhafter Hersteller oder gleich No-Name-Ware sind.

Für den betrieblichen Einsatz sollten Markengeräte angeschafft werden, die zusätzlich ausdrücklich noch als Business-Geräte verkauft werden. Die Unterschiede zu den „normalen" Consumer-Geräten liegen dabei nicht in der Hardware, die durchaus baugleich sein kann, sondern in den Garantie- und Kundendienstleistungen wie vor-Ort-Austausch-Service und Telefon-Support. Bei einigen Herstellern und Händlern können diese Zusatzleistungen auch zu hinzugebucht werden.

Das soll heißen: Datensicherheit hat auch mit der Zuverlässigkeit der Geräte zu tun und die ist bei Markenherstellern größer.

Ganz allgemein: Was kann ich tun, damit meine Unternehmensdaten zum Beispiel vor einem Wasserschaden geschützt sind?

Antwort: Aktuelle Datensicherung auf externen Datenträgern, die vor Ort sicher verwahrt werden (bestenfalls in einem Tresor) und zusätzlich „außer Haus", also z. B. auf einem Cloudspeicher.

Mein Chef sieht nicht ein, wieso wir ein extra Backup der Buchhaltungsdaten brauchen. Sie sind ja auf unserem ganz neuen PC gespeichert. Wie kann ich ihn trotzdem davon überzeugen?

Antwort: Gegen äußere Einwirkungen und Hardware-Fehler ist leider auch ein neuer PC nicht immun. Die besten Argumente für die Datensicherung sind immer Systemausfälle, egal wie sie verursacht werden (Wasserschaden, Brand, Hackerangriff). Das macht auch gleich die Notwendigkeit einer nicht-lokalen Datensicherung deutlich.

Datenschutz und Datensicherheit

Woher weiß ich, welche Daten ich an wen weitergeben darf?

Antwort: Grundsätzlich problematisch sind personenbezogene Daten. Speichern und z. B. an Dritte übermitteln dürfen private Stellen oder Sie als Mitarbeiter („verantwortliche Stelle") personenbezogene Daten nur in drei Fällen:

1. Wenn der Betroffene schriftlich eingewilligt hat,
2. wenn es eine Rechtsvorschrift gibt
3. oder wenn die neue DSGVO dies erlaubt.

Sonst ist dies verboten. Wenn z. B. ein Unternehmen Mitarbeiter-, Kunden- oder Lieferantendaten führt, der Arzt Patientendaten oder ein geschäftsmäßig tätiger Verein eine Mitgliedsdatei anlegt, müssen bestimmte Voraussetzungen für die Datenverarbeitung vorliegen.

Das Speichern personenbezogener Daten ist nur zulässig

- im Rahmen der Zweckbestimmung eines Vertrages

- ODER im Rahmen eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen, z. B. bei einer Anfrage bzw. Bewerbung
- ODER soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden
- ODER wenn Daten aus allgemein zugänglichen Quellen entnommen werden, z. B. Telefonbuch
- ODER natürlich dann, wenn der Betroffene schriftlich (!) eingewilligt hat.

Wir (Lohnsteuerbüro mit 10 Angestellten) haben mit unserem Datenschutzbeauftragen verbindliche Datenschutzrichtlinien erstellt. Wie kann ich sicherstellen, dass sich auch wirklich alle daran halten?

Antwort: Formal durch eine entsprechende Betriebsvereinbarung. Ansonsten aber durch ständige Thematisierung und Sensibilisierung der Mitarbeiter, damit ein „Datenschutzbewusstsein“ entsteht. Dabei gilt immer, dass nicht Zwang, sondern Motivation und Transparenz zielführend sind.

Inwiefern ist es derzeitig notwendig für ein Unternehmen aufgrund der DSGVO eine Verschlüsselung der Mails anzuwenden. Sprich: Müssen Unternehmen z. B. S/MIME verwenden um DSGVO-konform zu arbeiten? Oder reicht die normale SSL-Verschlüsselung aus (die natürlich nicht die Mail direkt verschlüsselt)?

Antwort: Die DSGVO verlangt zwar die Verschlüsselung vertraulicher E-Mails, über das Verfahren ist aber noch nicht entschieden. Nach meinem Kenntnisstand reicht die SSL-Verschlüsselung derzeit noch aus.

Archivierung und GoBD

Guten Tag, ich speichere zu jeder Buchung immer die dazugehörige Rechnung eingescannt, bzw. wenn sie mir bereits als PDF vorliegt, auch direkt. Das sollte doch auch revisionssicher sein, oder?

Antwort: Streng genommen nicht. Die Revisionssicherheit erfordert unveränderbare Inhalte und eine unveränderbare Protokollierung der Speichervorgänge. Das scheint mir bei Ihrem Verfahren nicht unbedingt gegeben zu sein, da auch PDFs nachträglich verändert werden können.

Guten Tag, ich habe eine Frage zur Datensicherheit bei der digitalen Lohnabrechnung: Welches Dateiformat können Sie empfehlen? Genügt eine Speicherung als PDF? Außerdem: Beim Versand der Lohnabrechnung sollte man ja auch auf die Verschlüsselung achten, ist eine End-to-End-Verschlüsselung notwendig? Wenn ja, welches System können Sie empfehlen?

Antwort: Rechtlich ist der Versand der Lohnabrechnung als PDF in Ordnung, da PDF auch als „Papierform“ gilt. Statt einer End-to-End-Verschlüsselung, wie sie z. B. recht kompliziert mit PGP und S/Mime realisiert werden kann, würde ich den Versand passwortgeschützter und verschlüsselter ZIP-Dateien empfehlen, die z. B. mit dem kostenlosen Programm 7-ZIP angelegt werden können.

Gibt es eine Vorschrift wie lange man Datensicherungen speichern sollte? Also auf was für einen Stand man Dateien auf einen Server immer zurückspielen können muss?

Antwort: Im Gegensatz zur regelrechten Archivierung, für die gesetzliche Vorschriften gelten, gibt es für die Datensicherung keine Vorschrift. Erfahrungsgemäß sollten aber mindestens die letzten beiden Wochen gesichert sein.

Sind die Daten, die in Lexware Programmen gespeichert werden, revisionssicher?

Antwort: Die Lexware Programme bieten Ihnen die Möglichkeit, Ihre Daten gegen Verlust zu sichern. Dabei liegt der Fokus darauf, dass diese Daten im Ernstfall möglichst einfach wiederhergestellt werden können. Für den Fall, dass Sie Ihre Daten auch revisionssicher archivieren möchten, gibt es den Service Lexware archivierung. Bei dieser Lösung handelt es sich um eine Archivierungssoftware, die speziell dazu entwickelt wurde, wichtige Dokumente wie Belege und Rechnungen entsprechend der Vorgaben der GoBD zu archivieren. Ihr Lexware Programm lässt sich ganz einfach mit Lexware archivierung verknüpfen.

Datensicherheit „offline“

Wenn wir jetzt mal den Blick vom Computer nehmen: Reicht dann ein normaler Schredder, der Papier klein macht, aus oder muss man sich hier jetzt auch ein High-End-Gerät zulegen? Man hört derzeit überall so viel „Unsinn“, das kann man gar nicht alles glauben.

Antwort: Das stimmt. Also: Auch für Papier-Schredder gibt es Sicherheitsklassen, die die Größe der Schnipsel betreffen. Nachlesen kann man das z. B. sehr gut in den äußerst empfehlenswerten Veröffentlichungen des BSI (Bundesamt für die Sicherheit in der Informationsverarbeitung: www.bsi.de). Für den normalen Bürobetrieb sollte aber ein einfacher Papier-Schredder bereits ausreichend sein. Anders ist dies natürlich bei hochvertraulichen und wirklich sicherheitskritischen Informationen. Das sind z. B. Kennwörter, Zugangsdaten, u. U. Forschungsergebnisse.

Ein grundsätzliches Problem beim Thema Datensicherheit ist, dass alle Beteiligten zu sehr auf digitale Lösungen fixiert sind: Man sorgt für einzelne Lösungen, verliert aber schnell den Gesamtüberblick!