

DATENSICHERHEIT. Viele Unternehmen investieren in computergesteuerte Maschinen und Software für die Produktionsplanung – die Abhängigkeit von digitalen Daten wächst. Allerdings wird das Thema Datensicherheit oft vernachlässigt.

Ein Backup für alle Fälle

Neben Viren können auch Elementarereignisse zu Datenverlusten führen. Ein externes Backup stellt in solchen Fällen die Wiederherstellung sicher.



Bild: Robby Schenk, fotolla.com

In vielen Schreinerbetrieben, egal ob gross oder klein, ist die Auftragsabwicklung mittels EDV-Systemen kaum mehr wegzudenken. Sämtliche Daten werden mittels ERP- und PPS-Programmen erfasst und gespeichert. Produktionszeichnungen erstellt der Planer mittels CAD, die Präsenzzeiten erfassen die Mitarbeiter ebenfalls elektronisch. Hinzu kommen Dateien von computergesteuerten Maschinen, E-Mails und sonstigen Dokumenten.

Ein Verlust dieser essentiellen Daten kann weitreichende Folgen für das Unternehmen haben: Je nach Arbeitsvorrat und Abhängigkeit von EDV-Systemen muss die Produktion nach einigen Tagen reduziert oder sogar eingestellt werden, da keine Produktionsdaten mehr zur Verfügung stehen. Man wäre vielleicht nicht einmal in der Lage, seine Kunden anzurufen, da man keinen Zugriff auf die Adressdaten hat. Un-

tersuchungen in Grossbritannien haben gezeigt, dass 70% der Unternehmen, bei denen es zu einem katastrophalen Datenverlust kam, innerhalb von 18 Monaten aufgeben mussten. Dies klingt dramatisch und mag so nicht auf die Schweiz zutreffen, aber es zeigt, wie schwerwiegend die Auswirkungen sein können. «Insbesondere in kleineren Betrieben wird das Thema Datensicherheit leider oft vernachlässigt», berichtet Max Klaus, stellvertretender Leiter der Melde- und Analysestelle Informationssicherung des Bundes (Melani).

Häufigste Ursache: Hardwarefehler

Das grösste Risiko für einen Datenverlust geht nicht etwa von kriminellen Handlungen mit Malware (Viren, Würmer, Trojaner, Spyware) aus, sondern von Hardwarefehlern. «Computer und Server sind oft über Jahre in Betrieb und man geht fälschlicher-

weise davon aus, dass sie ohne Weiteres funktionieren», berichtet Adi Stierli, System-Engineer bei der Swissvault AG. Das Unternehmen hat sich auf die Datensicherung, insbesondere von KMU, spezialisiert. In den Rechnergehäusen sammelt sich mit der Zeit Staub an und auch die Komponenten haben keine unbegrenzte Lebensdauer. Eine entsprechende Kontrolle und Reinigung durch einen Spezialisten trägt demnach einiges zur Systemsicherheit bei. An zweiter Stelle steht der Faktor Mensch. Viele EDV-Probleme sind auf Anwenderfehler zurückzuführen. Aus Unwissenheit oder Unachtsamkeit werden Dateien gelöscht oder Einstellungen geändert. Aber auch die Software selbst kann Fehler verursachen. Auf den Computern befinden sich immer mehr Programme und Treiber, die untereinander Konflikte verursachen, was zu einem Systemfehler führen kann.

Virenschutz unabdingbar

Gezielte Hackerangriffe, wie sie bei grossen Konzernen passiert sind, kommen bei Schreinerereien kaum vor. Dies bestätigt eine 2006 veröffentlichte Umfragestudie zur Informationssicherheit in Schweizer Unternehmen der ETH Zürich. Die Studie hält fest, dass Firmen mit mehr als 250 Mitarbeitern einem erhöhten Risiko für Hackerangriffe ausgesetzt sind. 72% der befragten Unternehmen aus allen Branchen, Landesteilen und Grössen Kategorien gaben jedoch an, dass im Jahr 2005 irgend eine Form von Kriminalität zu einem Vorfall in der Informationsinfrastruktur geführt hat.

Fast 70% der betroffenen Unternehmungen wurden Opfer von Viren, Würmern und Trojanern. Solche Malware fängt man sich aber nicht nur auf dubiosen Websites ein. «Auch seriöse Seiten und E-Mails können damit infiziert sein», hält Max Klaus fest. Ein umfassender Schutz durch Virens Scanner und Firewall ist also heute unverzichtbar. Hier gibt es etliche kostenlose Programme, die man sich gratis vom Internet herunterladen kann. «Einige dieser Lösungen bieten durchaus einen guten Schutz», weiss Adi Stierli. Am besten bewähren sich nach wie vor Produkte von namhaften Herstellern wie Kaspersky, McAfee, Norman oder Symantec. Diese Schutzsysteme müssen aber immer auf dem aktuellsten Stand sein, sprich die Updates müssen regelmässig durchgeführt werden. Die meisten Programme führen dies automatisch durch, sobald ein Update zur Verfügung steht. Dies aber nur, solange eine gültige Software-Lizenz vorhanden ist. Dasselbe gilt auch für alle anderen Programme und Betriebssysteme. «Oft ist dem Softwarehersteller die Sicherheitslücke oder der Softwarefehler bekannt und er stellt ein entsprechendes Update zur Verfügung», erzählt Adi Stierli. Erstaunlich hoch liegt der konventionelle Diebstahl von Datenträgern, zum Beispiel durch Entwenden eines Laptops: Annähernd 10% der Unternehmen berichteten von solchen Vorfällen. Damit keine unberechtigten Personen auf den Datenträger zugreifen können, empfiehlt sich der Schutz durch ein Passwort, das Ziffern, Gross- und Kleinbuchstaben enthält.

Veraltete Sicherungsmethoden

Alle diese Sicherheitsmassnahmen können eine Panne im EDV-System jedoch nicht vollständig ausschliessen. In so einem Fall

zahlt sich eine Datensicherung – das sogenannte Backup – aus. Im Idealfall enthält es alle wichtigen Daten und ist innert kürzester Zeit verfügbar. Nach wie vor weit verbreitet ist die Sicherung mittels CD, DVD oder Magnetbändern. Sie entsprechen jedoch nicht mehr dem Stand der Technik und weisen entscheidende Nachteile auf: Solche Speichermedien müssen täglich von einem Mitarbeiter ausgetauscht und zum Beispiel in ein Bankschliessfach gebracht werden, was einen erheblichen Zeitaufwand bedeutet. Ausserdem stossen die Kapazitäten dieser Speichermedien angesichts der heutigen Datenmengen an ihre Grenzen.

Etwas zeitgemässer ist die Datenübermittlung mit einem Backup-Programm auf eine externe Festplatte. Aber auch hier ist Aufbewahrung des Datenträgers an einem externen, sicheren Ort einer der entscheidenden Faktoren: «Die Sicherung hilft reichlich wenig, wenn sie sich zum Beispiel im selben Gebäude wie der Server oder Computer befindet und die Liegenschaft durch ein Feuer oder Hochwasser zerstört wird», begründet Adi Stierli.

Sicherung überprüfen

Ein zeitgemässes Backup muss also vollautomatisch durchgeführt werden können und sich an einem sicheren Ort befinden. Darauf spezialisierte Unternehmen wie die Swissvault AG bieten Standardpakete und individuelle Lösungen für Privat- und Geschäftskunden an. Ein von Swissvault entwickeltes Backup-Programm übermittelt in festgelegten Intervallen die Daten verschlüsselt über das Internet in eines der beiden Rechenzentren, die sich in zwei verschiedenen Bunkern der Schweizer Armee befinden. Dabei werden nur bei der ersten Sicherung alle Daten übermittelt. Nachher gleicht das Programm nur noch die Daten ab, bei denen eine Veränderung stattgefunden hat, was die Übertragungszeiten auf ein Minimum reduziert. «Unser System kontrolliert zudem, ob das Backup tatsächlich durchgeführt wurde. Ist dies nicht der Fall, erhält der Kunde von uns eine Nachricht», ergänzt Stierli.

Zur Datensicherung gehört also auch eine regelmässige Kontrolle, ob das Backup gemacht wurde und ob es funktioniert – egal, ob die Daten auf einem Band gespeichert werden oder in einem externen Rechenzentrum. «Der Datenträger könnte zum Bei-

spiel beschädigt sein, was insbesondere bei den Bändern oft vorkommt. Oder die Leute wissen schlicht nicht, wie man die Daten mit Hilfe des Backups wiederherstellt», weiss Adi Stierli. PH

Die Swissvault AG bietet den SZ-Lesern und Leserinnen ein kostenloses Testangebot für die Datensicherungs-Software «Swissvault Solo» an. Der Link für die Anmeldung befindet sich auf der Website www.schreinerzeitung.ch unter «Zusatzinformationen».

- www.swissvault.ch
- www.melani.admin.ch
- www.swissecURITYday.ch

MERKPUNKTE DATENSICHERHEIT

1. Sichern

Regelmässige Datensicherung auf externe Medien. Kontrollieren, ob die Daten tatsächlich gespeichert wurden.

2. Schützen

Virenschutzprogramm installieren und so einstellen, dass es sich automatisch und regelmässig aktualisiert.

3. Überwachen

Datenverkehr mit Firewall überwachen. Das Programm warnt den Benutzer vor verdächtigen oder unerlaubten Aktivitäten.

4. Vorbeugen

Programme und Betriebssystem regelmässig updaten. Hardware überprüfen und warten lassen.

5. Aufpassen

Verantwortungsvoll mit Daten umgehen und den Computer mit einem sicheren Passwort schützen.