Ihre IT, das unbekannte Wesen?

Veraltete Systeme laden Hacker und Kriminelle zu Angriffen ein. Es ist daher ratsam, Systeme immer auf dem aktuellsten Stand zu halten und Sicherheitslücken mittels Updates, Virenscanner, Firewalls und Ähnlichem zu schließen. Dabei sollten auch mobile Geräte, die sich täglich im Einsatz befinden, nicht vergessen werden.

Eine regelmäßige Mitarbeiterschulung für einen sorgsamen Umgang mit E-Mails, deren Anhängen, Datenträgern und Programmen sollte fest in den Arbeitsprozess eingeplant werden. Risiken hängen nicht von der Größe des Unternehmens ab, sondern von deren Einstellung zur IT-Sicherheit. Meist wird das Sicherheitsrisiko durch unangemessene Kosteneinsparungen enorm erhöht. Weiterhin fehlt oftmals die Informationssicherheits-Strategie, da dieser ein zu niedriger Stellenwert zugeordnet wird. Kontrollen finden so gut wie gar nicht statt und verstärken damit das Risiko um ein Vielfaches, Opfer eines Verstoßes oder Angriffs zu werden – ob über das Internet oder über die Mitarbeiter. Die alleinige Einrichtung einer Firewall heißt nicht, dass das System damit vollständig geschützt ist. Sensible Daten sollten von offenen Netzen abgeschirmt werden. Diese Sicherheitsmaßnahmen werden immer wieder sträflich vernachlässigt. Sichere Passwörter sind der Beginn der Datensicherheit im Unternehmen. Jedoch gilt es auch, die Benutzer von IT-Systemen zu sensibilisieren, sodass diese keine Interna – unbeabsichtigt oder nicht – an Unbefugte weitergeben. Von Seiten des Unternehmens können hierzu Schulungen abgehalten werden, die mitunter auch den korrekten Umgang mit Wechseldatenträgern und der Informationsweitergabe, zum Beispiel via Internet oder Social-Media-Kanälen, behandeln. Solche Sicherheitsmaßnahmen müssen fest in den Workflow integriert werden, um dauerhaft Gefahren vorzubeugen. Auch kann ein fehlender Schutz vor Diebstahl und Elementarschäden zu sehr negativen Auswirkungen führen.

Notwendige Schritte für die IT-Sicherheit im Unternehmen

Das IT-System sollte auf dem aktuellen Stand gehalten werden, um eine größere Hürde für Angreifer darzustellen. Updates des Herstellers sind hierfür ebenfalls essenziell, wobei nicht nur Software, sondern auch Hardware betrachtet werden muss. Kritische Sicherheitslücken entstehen meist, wenn Updates nicht zügig installiert werden und der Virenscanner nicht up to date ist. Mobile Geräte benötigen ebenfalls Virenscanner und regelmäßige Aktualisierungen. Ein besonderes Augenmerk gilt der Datensicherung, um wichtige Daten im Fall eines Verlustes möglichst kostengünstig und einfach wiederherzustellen. Hierbei sollten die Backups regelmäßig (beispielsweise täglich) geprüft und von Zeit zu Zeit auch sogenannte „Restore-Tests“ vorgenommen werden, denn nur so ist gewährleistet, dass die gesicherten Daten im schlimmsten Fall wiederherstellbar sind. Zudem ist bei der Sicherung der Daten auch die räumliche Trennung ein wichtiges Kriterium, denn so sind Backups auch im Katastrophenfall noch verfügbar. Ebenfalls empfehlenswert ist die Verschlüsselung sensibler Daten, nicht nur in Backups, sondern auch auf Netzlaufwerken und den mobilen Geräten. Auf diese Weise kann einem Datenverlust effizient vorgebeugt werden. Fakt ist, dass mangelhafte IT-Administration zu massiven Folgeschäden führt, die ein Unternehmen in den Ruin treiben können.

Es ist also unumgänglich, die IT-Sicherheit kontinuierlich zu auditieren und anzupassen. Die IT-Sicherheit im Unternehmen steigt und fällt mit dem verantwortungsvollen Umgang der Daten durch die Mitarbeiter.

Stefan Lew
Geschäftsführer der
„Bits & Bytes“ GmbH

Fotos: Oleksii, Daniel Berkmann - stock.adobe.com