Schützen Sie Ihre digitalen und physischen Informationen

Daten werden weithin als das neue Öl angesehen. Ihre Online-Systeme und -Aufzeichnungen, in denen sich häufig vertrauliche Daten befinden, sind daher in den Augen von Datendieben, die alles daran setzen, in diese einzudringen, Goldgruben (oder Ölfelder).

Tatsächlich werden täglich Tausende von Online-Systemen kompromittiert und allein im letzten Jahr berichteten 39 % der Geschäfte in Europa, dass sie Opfer eines Cyberangriffs wurden[1]. Doch die Zahl der in diesem Jahr gemeldeten Datenschutzverletzungen übersteigt bereits die Gesamtzahl für das Jahr 2020.

Als Antwort darauf müssen Geschäfte ihre Mitarbeiter mit dem Wissen und den Werkzeugen ausstatten, um Ihre vertraulichen Informationen zu schützen. Unsere wichtigen Tipps zum Datenschutz helfen Ihnen dabei.

[1] Source: Statista

01

Einrichten eines Risikomanagement-Regimes

Ein Risikomanagement-Regime ermöglicht es Geschäften, Bedrohungen zu erkennen und zu verstehen – und hilft Ihnen dann, diese Risiken zu beseitigen oder zu verringern, indem Sie die Technologie, Systeme und Informationen in Ihrem Unternehmen sichern.

02

Sichern Sie Ihre Netzwerke

Zu den wichtigsten Cybersicherheitsgrundlagen gehören Firewall- und Antivirenprogramme. Vergewissern Sie sich, dass die E-Mails seriös sind und klicken Sie nicht auf die Links: Rechtschreibfehler, schlechte Grammatik, merkwürdige Formulierungen und dringende Geldaufforderungen sind ein Warnsignal.

03

Sichere Passwörter verwenden

Sichere Passwörter bestehen aus mindestens acht Zeichen und enthalten eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen. Bewahren Sie Passwörter an einem sicheren Ort auf, verwenden Sie nicht dasselbe für mehrere Konten und ändern Sie es alle drei Monate.

Wir schützen das, was wirklich zählt.

Shred-it®
Ein Unternehmen von Stericycle®

04

Weniger auf sozialen Medien teilen

Kriminelle können mit nur wenigen Datenpunkten an Ihre vertraulichen Informationen gelangen. Je weniger Sie also preisgeben, desto besser! Wenn Sie z. B. den Namen Ihres Haustiers veröffentlichen, könnten Sie die Antworten auf eine häufig gestellte Sicherheitsfrage preisgeben.

05

Mitarbeiterschulung und -bewusstsein

Erstellen Sie Sicherheitsrichtlinien und bieten Sie Schulungen zur Cybersicherheit an. Die Mitarbeiter müssen wissen, wie sie fragwürdige E-Mails oder Links erkennen können, und sollten darauf achten, welche Websites sie besuchen und welche Apps sie herunterladen. Ermutigen Sie Ihre Mitarbeiter, alle Cyberangriffe zu melden.

06

Nutzen Sie Festplattenvernichtungsdienste

Horten Sie keine Computer und digitalen Daten. Halten Sie digitale Daten archiviert sowie auf dem neuesten Stand und löschen Sie die Dateien regelmäßig. Sobald Ihr altes Gerät hinfällig ist, lassen Sie alte oder ungenutzte Computerfestplatten sicher vernichten.

07

Schützen Sie Smartphones und andere Geräte

Handys und andere Geräte können Ihr schwaches Glied sein. Lassen Sie sie nie unbeaufsichtigt und schalten Sie den Passwortschutz ein. Halten Sie Ihre Apps und Betriebssysteme auf dem neuesten Stand und achten Sie darauf, verlorene oder gestohlene Geräte zu verfolgen, zu sperren und zu löschen.

08

Vergessen Sie nicht die Dokumente und physischen Bedrohungen!

Auch alte Dokumente stellen ein erhebliches Risiko dar, wenn sie nicht sicher behandelt, aufbewahrt und vernichtet werden. Eine Clean-Desk-Richtlinie kann die Sicherheit unterstützen, während eine Shred-it-All-Richtlinie dazu beiträgt, menschliches Versagen, das häufig für Datenverletzungen verantwortlich ist, zu reduzieren.

Wir schützen das, was wirklich zählt.

Shred-it®

Ein Unternehmen von Stericycle®