Daten, Daten, Daten: So schützen Sie Ihr wichtigstes Gut

DATA SECURITY: Warum es sich lohnt, mehr in die digitale Sicherheit im Betrieb zu investieren

Sowohl ein umfassender Datenschutz als auch die Datensicherheit sind heutzutage in der medialen Welt von enormer Relevanz – zum einen für jeden, der Daten von sich preisgibt, zum anderen aber auch für Unternehmen, die mit Daten arbeiten. Zu Letzteren gehören mittlerweile wohl fast alle, für sie gehören Daten mit zu den wertvollsten Ressourcen im Betrieb – Grund genug, mehr für ihren Schutz zu unternehmen.

Zunächst gilt es jedoch zwischen den einzelnen Begriffen zu unterscheiden: Der Begriff Datensicherheit umschreibt den generellen Schutz von Daten, unabhängig davon, ob diese einen Personenbezug haben oder nicht. Dabei geht es bei dem Thema Datensicherheit nicht um die Frage, ob Daten überhaupt erhoben und verarbeitet werden dürfen. Vielmehr geht es um die Frage, welche Maßnahmen ergriffen werden müssen, um den Schutz der Daten zu gewährleisten und damit schließlich die bestmögliche Datensicherheit zu erreichen. Dieser angestrebte Zustand kann durch eine Vielzahl an Maßnahmen erreicht werden.

Mindestens ein Backup täglich zu erstellen, hilft häufig, einem gänzlichen Datenverlust vorzubeugen.

Datensicherheit: Vernachlässigtes Thema

Und welches Ziel verfolgt die Datensicherheit? Datensicherheit hat das primäre Ziel, Daten jeglicher Art gegen Manipulation, Verlust, Klau und andere Bedrohungen zu sichern. Im Kontext des Datenschutzes im Unternehmen ist so die Datensicherheit durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen zu gewährleisten. Datenschutz und Datensicherheit gehen somit Hand in Hand. Denn der Zustand der Datensicherheit lässt sich nicht ohne die Maßnahmen des Datenschutzes erreichen. Umgekehrt ist eine hinreichende Datensicherheit die Voraussetzung für effektive Datenschutzmaßnahmen.

Unsere Daten sind uns heilig. Das hat man mit dem Inkrafttreten der DSGVO nochmal deutlich zu spüren bekommen. Datensicherheit ist somit gerade für Unternehmen zu einem großen Thema geworden. Doch bisher setzen sich gerade kleinere Unternehmen noch viel zu wenig mit dem Thema auseinander. Denn oftmals setzen Unternehmen einfach zu großes Vertrauen in die Technik und verfügen selbst über zu wenig Wissen über die Wichtigkeit der Datensicherheit. Doch mit dem Thema Datensicherheit sollte nicht leichtfertig umgegangen werden. Bei Nichteinhaltung der Vorschriften drohen hohe Bußgelder und Sanktionen.

Daten regelmäßig sichern

Neben den personenbezogenen Daten, mit denen entsprechend umgegangen werden muss, zählen natürlich auch andere Daten eine Rolle. Gehen Unternehmen nicht sorgfältig mit diesen um, kann im schlimmsten Fall sogar eine existenzielle Bedrohung bedeuten. Vor diesem Hintergrund sollten Unternehmen ihre Daten regelmäßig sichern. Es wird empfohlen, jegliche Daten mindestens einmal täglich zu sichern. Ein tägliches Backup erfüllt zudem die Anforderungen an eine gesetzeskonforme Archivierung der Daten.

Oftmals übersehen wir kleine und dennoch wichtige Details, die die Datensicherheit betreffen. Denn die Gefahren von Sicherheitslücken lauern meist im ganz normalen Arbeitsalltag und drohen gar nicht von außen. Zum Beispiel durch USB-Sticks: Gerade die kleinen Helfer können schnell mal verloren gehen und auch schnell unbemerkt und unbewusst einen Schaden durch das ungeschützte Einstecken in das interne Firmennetz verursachen.

Firewall und Co. sind Pflicht

Ein zweites Beispiel sind Endgeräte: Gerade bei der Nutzung von Laptops treten können durch eine fehlende Verschlüsselung, lokal gespeicherte Informationen oder unzureichend gesicherte VPN-Zugänge Probleme auftreten.

Um das Risiko von Viren jeglicher Art zu verringern, empfiehlt sich der verpflichtende Einsatz von Firewall, Virenscannern, Spamfiltern usw. Diese wenigen Beispiele zeigen, dass Datensicherheit bereits im ganz normalen Arbeitsalltag beginnen. Um diese Gefahrenpunkte vorzubeugen oder zumindest abzuschwächen, bietet sich eine schlüssige Compliance-Strategie an.

Diese bewertet die Punkte entsprechend und sieht dafür bewährte Verfahrensweisen vor, etwa die Erstellung und Umsetzung geeigneter, unternehmensweiter Benutzerrichtlinien für den Umgang mit Technologien mit Gefährdungspotential, regelmäßige Schulungen und Sensibilisierungen von Mitarbeitern, sowie eine fortlaufende Unterrichtung der Geschäftsführung und Mitarbeiter über neue Bedrohungsszenarien aufgrund technischer Weiterentwicklungen.