

DSGVO: besser als ihr Ruf

Die Datenschutzgrundverordnung kann für Betriebe und ihre Kunden sehr vorteilhaft sein – wenn man sie *richtig* einsetzt.

WIEN. Seit Ende Mai 2018 sind Unternehmen (und Behörden) in Österreich verpflichtet, die EU-Datenschutzgrundverordnung zu realisieren und dadurch die Daten ihrer Kunden vor jeglichem Missbrauch zu schützen.

Bevor die Umsetzung der DSGVO bindend wurde, waren viele Firmen verunsichert, wie sie diese Vorgaben in der täglichen operativen Arbeit erfüllen könnten. Mittlerweile hat sich die Aufregung gelegt, denn die DSGVO war mehr als notwendig, damit umfassend für IT-Sicherheit und Datenschutz gesorgt wird. Unternehmen profitieren davon, wenn sie Synergieeffekte nutzen und sich gleichzeitig auch auf die eigene Datensicherheit fokussieren – denn dann lohnt sich der Aufwand in allen Fällen.

Unterschätzte Gefahren

Gefahren für Kundendaten lauern an vielen Ecken: intern oft durch nicht ausreichend geschulte Mitarbeiter oder durch Angriffe von außen.

„Cyberkriminalität ist eine negative Begleiterscheinung der Digitalisierung“, weiß Datenschutzexperte Vincenz Leichtfried. „Wer die DSGVO nicht nur juristisch, sondern vor allem auch *technisch* umsetzt, kann sich in hohem Maße vor Angriffen von außen schützen! Datenschutz ist gleich IT-Sicherheit



© Hannes Fuß

ist gleich Unternehmensstabilität.“

Denn wer die Verordnung tatsächlich praktisch umsetzt, erhöht die Datensicherheit im

Unternehmen und schützt es gleichzeitig vor Betriebsausfällen. „In einem ersten Schritt müssen die Firmen ermitteln, welche Datenanwendungen bei ihnen tatsächlich vorhanden sind“, betont Leichtfried die Wichtigkeit einer *ganzheitlichen* Risikoevaluierung des Betriebes.

Es geht dabei um folgende Fragen:

- Wie lange dürfte ein Betriebsausfall dauern, bevor Umsatzentgang und Reputationsverlust drohen?
- Wie aktuell müssen Backups sein? Sollte es zu einem Datenverlust kommen, müssen Sicherheitskopien vorhan-

den sein, die einerseits die entsprechenden aktuellen Informationen beinhalten und auch jene Daten, die vor dem Datenschutzvorfall gespeichert wurden.

- Wie hoch ist die Abhängigkeit von Dienstleistern und Schlüsselpersonen? Was passiert, wenn Dienstleister ausfallen oder Mitarbeiter nicht erreichbar sind? Es muss klar sein, wofür welche Kenntnisse und Fähigkeiten benötigt werden, um im Anlassfall rasch reagieren zu können.

Experten-Rat einholen

Bei all diesen Themen gibt es Parallelen zwischen den DSGVO-Vorgaben und dem spezifischen Eigeninteresse des jeweiligen Unternehmens.

Studien zeigen, dass Unternehmen wie auch Privatpersonen inzwischen viel sensibler sind als noch vor zwei Jahren. Ein wichtiges Instrument zur Schaffung von mehr Sicherheit ist dabei ein durchdachtes *Berechtigungsmanagement*: Nicht jeder Mitarbeiter muss auf alles Zugriff haben.

Darüber hinaus ist das Passwortmanagement entscheidend. Wenn für mehrere Anwendungen das gleiche Passwort verwendet wird, kann ein einzelner Leak enorme Folgen haben.

„Eine weitere Gefahr ist fehlendes Bewusstsein darüber, wo Daten *tatsächlich* liegen und wie diese Speicherorte abgesichert sind“, empfiehlt Leichtfried, auch wenn man davon überzeugt ist, alles für die IT-Security und für den Datenschutz zu tun, einen Notfallplan. „Legen Sie fest, wie der Schaden schnell behoben werden kann. Dazu gehört, dass bekannt ist, wie die Schlüsselpersonen erreichbar sind und wie das IT-Security-Problem möglichst eingegrenzt werden kann.“ (pj)

Rat und Tat

11.000 Helfer

Unternehmen ohne eigene IT-Abteilung sollten externe Experten zuziehen – allein in Wien gibt es 11.000 IT-Dienstleister.

Wer sichergehen möchte, dass die EU-DSGVO richtig umgesetzt wird und darüber hinaus für IT-Sicherheit und damit für Betriebsstabilität sorgen will, ist bei diesen Experten bestens aufgehoben.

Keine Angst

Die europäischen Datenschutzbehörden waren bei der Anwendung der neuen Strafbestimmungen 2018 noch überaus zurückhaltend: In Österreich wurden nur vier Verwarnungen und drei Geldstrafen aufgrund von datenschutzrechtlichen Verstößen ausgesprochen.