Datenschutz: Homeoffice, Telearbeit und Co

Während ich diese Zeilen verfasse, sind wir noch mitten in der unsäglichen Coronakrise und erliegen zeitweise dem Informations-Overload. Ist denn die „neue Normalität" schon eingetreten oder ist wieder alles „normal", also wie früher? Beim Thema Datenschutz ist leider nichts mehr so wie früher! Wenn zu den bereits bekannten „Datensammlern" noch weitere „große Brüder" das Spielfeld betreten, sollten wir genau beobachten, was mit unseren und vor allem mit den uns anvertrauten Daten passiert …

Wenn wir von „Datenschutz" reden, sollten wir zuerst einmal definieren, was genau es zu schützen gilt und wo die Gefahren liegen. Da wäre zuerst der Schutz der **Infrastruktur** inklusive Hardware:

Schließanlagen, Büroschlüssel, elektronische Schlösser (Smartlock)
Workstations, PC, Mac
interne und externe Server
Router und Firewall
Alarmanlagen und Überwachungskameras
alle mobilen Geräte (Mobiltelefone, Tablets)
Wearables, Smartwatch etc.

Dann die **logische Ordnung der Daten** auf den verschiedenen Datenspeichern:

in einfachen Ordnerstrukturen, Mailkonten oder in Datenbanken
in geschlossenen integrierten Systemen (CMS etc.)
in extern gehosteten Cloudsystemen

Letztendlich die **Daten** selber:

Zugangsdaten zu den Systemen, Mailkonten, Cloudsystemen
unsere eigenen Daten
externe Daten von Kunden, Lieferanten, Subfirmen, Behörden etc.
die temporär zur Verfügung gestellten Daten für Auftrags-Datenverarbeitung

Frei nach Murphys Gesetz „Was schiefgehen kann, wird schiefgehen" sollten wir auch die Gefahrenfelder bzw. die „Feinde", die an unsere Daten wollen, analysieren. Es ist keine Schwarzmalerei, sondern eine nüchterne Betrachtung, um aufzuzeigen, wo man eventuell noch Raum für Verbesserung hat.

Auch hier möchte ich zwischen organisatorischen Unterlassungen wie

der **eigene Leichtsinn** („Wird schon passen")

das „**keine Zeit**“-Syndrom („Was soll ich noch alles machen“ ...)
fehlendes **Datensicherheitskonzept** (Zutrittsberechtigung)
kein **Berechtigungskonzept** (Datenzugriff)
keine oder zu alte **Datensicherung**
nicht versperrbares **Büro** bzw. **Serverraum**
Passwörter sind zu einfach und werden selten geändert
Festplatten sind nicht verschlüsselt
Übertragung von wichtigen **Dokumenten** erfolgt nicht verschlüsselt
keine oder zu einfache **PIN-Codes** bei Mobilgeräten
IP-Kameras der **Videoüberwachung** sind nicht geschützt
Phishing E-Mail & SMS
vor **Installation von APPs** die Datenschutzbestimmungen nicht zu lesen
und technisch notwendigen Maßnahmen, die nicht ergriffen wurden, unterscheiden:

Fehlen von oben erwähnten technischen Komponenten wie Alarmsystem, Firewall, Videoüberwachung etc.
zu alte Betriebssysteme (Wartung vom Hersteller eingestellt) und Anwendungsprogramme (Win7, Office Mac 2011 etc.)
falsche Einstellungen am Router (Firewall aktivieren)
kein Tresor für wichtige Unterlagen und Festplatten
keine Datensicherung in die Cloud
Die DSGVO sieht vor, dass die Maßnahmen dem „aktuellen Stand der Technik“ entsprechen müssen. Weiter in Art. 32: „Die für Datenschutz verantwortliche Person hat dafür zu sorgen, dass geeignete technische und organisatorische Maßnahmen festgelegt werden, die sicherstellen, dass die Datensicherheit bei der Verarbeitung von personenbezogenen Daten gewährleistet ist.“ Es muss nicht die allerneueste Generation des iMac am Tisch stehen (wäre nett – ist aber auch ein Budgetthema), aber die Kombination aus technisch einwandfreier Hardware und gut gewarteter Software (sprich Herstellersupport) verbunden mit Aufmerksamkeit bringt uns schon auf die sichere Seite.

Telearbeit

Noch ein paar Worte zur Telearbeit, die in den letzten Wochen für viele von der Not zur Tugend wurde. Viele von uns arbeiten ja schon jahrelang im Homeoffice und haben deshalb Erfahrung damit. Aber dennoch gilt, dass auch bei der Telearbeit alle notwendigen Datenschutzmaßnahmen zu ergreifen sind. Sollten Sie Ihren PC mit anderen Familienangehörigen teilen müssen, empfehle ich folgende Maßnahmen:

Router bzw. WLAN **konfigurieren** (Firewall, Passwortschutz, eventuell Gastzugang)
für jeden Benutzer des Gerätes ein **eigenes Userkonto** anlegen
Berechtigungen für Programme und Ordner vergeben
strikte **Trennung** zwischen **Privat- und Firmendaten**
eigene **externe Festplatten** für die Kids
Datensicherung durchführen
Passwörter geschützt aufbewahren
Videokonferenzsysteme mit Bedacht auswählen (Datenschutzproblem „Zoom“)
wenn möglich Zugriff auf Firmenrechner mit VPN
Datenschutz-Richtlinien der Firma beachten sowie
den **Zugang vor Dritten schützen** („Lass mich mal kurz meine E-Mails checken“ …)
Bei allen Vorschriften, guten Tipps und Empfehlungen bitte ich Sie wie immer: Hören Sie auf den Hausverstand! Glauben Sie nicht alles, was Sie in Foren und Chats lesen und gehen Sie mit Bedacht ans Werk, denn die Daten sind immer noch ein schützenswertes Gut. Unsere Aufgabe als Unternehmer ist es, die eigenen und die uns anvertrauten Daten nach besten Möglichkeiten zu schützen, um Missbrauch zu verhindern. Ich hoffe und wünsche uns allen, dass wir gut und gesund durch diese Krise kommen und uns das zweite Halbjahr 2020 wieder spannende und ertragreiche Projekte bringt.

Weitere Informationen:

Link-Empfehlungen zum Thema:

It-safe – Informationen der Bundessparte Information und Consulting

Datenschutz – Zukunftsfragen und aktuelle Judikatur

DSGVO – Begriffsbestimmungen

Sichere freie Software für Gruppenkommunikation

Foto: iStock.com/Geber86