ITDSC UG
Data-Security-Consulting
www.itdsc.de

Informationen zum Thema Datenschutz

Liebe Leserin, lieber Leser,

warum nur dieser Aufwand?

Das fragen sich viele, wenn es um den Datenschutz geht.
Es ist deshalb wichtig, zu verstehen, warum die Datenschutz-Maßnahmen notwendig sind.
So erfahren Sie zum Beispiel in dieser Ausgabe, weshalb Sie noch mehr für die Sicherheit Ihres Smartphones und für den Datenschutz bei Filesharing tun sollten.

Ich wünsche Ihnen viel Spass beim Lesen.

Detlef Riese
Datenschutzbeauftragter

Ist Ihr Smartphone sicher genug?

Smartphones sind für viele zum täglichen Begleiter geworden. Trotzdem wird die Sicherheit bei Smartphones weiterhin vernachlässigt. Das kann gefährliche Folgen haben. Denn Smartphones dienen zunehmend als Identitätsnachweis.

Ohne Smartphone geht es für viele nicht mehr

„Die Faszination für Smartphones ist so groß wie nie“, so Markus Haas, Präsidiumsmitglied im Digitalverband Bitkom. „Sie informieren und unterhalten uns, steigern unsere Produktivität und unterstützen uns in vielen Lebenslagen. Smartphones stehen für Innovation und Wachstum.“

Dies bestätigt eine Bitkom-Umfrage: Für nahezu alle Nutzerinnen und Nutzer (96 Prozent) sind Smartphones eine große Erleichterung im Alltag. Neun von zehn (90 Prozent) können sich ein Leben ohne Smartphone nicht mehr vorstellen.

Umso wichtiger ist es, für die notwendige Datensicherheit bei den Smartphones zu sorgen.

Smartphones werden immer noch schlechter als PCs geschützt

Obwohl es gerade die smarten Funktionen zusätzlich zum Telefonieren sind, die die Smartphones so beliebt machen, denken immer noch viele Nutzerinnen und Nutzer, sie hätten ein „Handy“ dabei, also ein Mobiltelefon. Doch bekanntlich sind Smartphones mehr Computer als Telefon.

Trotzdem werden Computer wie PCs und Notebooks anders und besser abgesichert als Smartphones, wie aktuelle Umfragen belegen.

Mit 96 Prozent haben fast alle Smartphone-Nutzer eine Bildschirmsperre eingestellt, neun von zehn (90 Prozent) haben einen SIM-Karten-Schutz aktiv. Dabei sperrt sich das Handy, sobald die SIM-Karte entfernt wird. Aber nur etwa jeder Zweite (55 Prozent) erstellt auch regelmäßig Backups seiner Smartphone-Daten. Virenschutzprogramme haben 43 Prozent installiert. Jeder Sechste (16 Prozent) deckt seine Smartphone-Kamera ab.

Wie ist es bei Ihnen? Schützen auch Sie Ihren „täglichen Begleiter“ Smartphone schlechter als den PC?

Bedeutung des Smartphones steigt und damit die Risiken

Bereits 13 Prozent nutzen einen Passwort-Safe, um Passwörter auf dem Smartphone zentral zu verwalten. Das ist nur ein Beispiel dafür, dass Smartphones zunehmend als Sicherheitswerkzeuge genutzt werden. Smartphones sind auch die häufigste Basis für den zweiten Faktor bei Online-Banking und Online-Shopping, zum Beispiel über den Fingerabdruck-Sensor.

Denkt man dann noch an mobiles Bezahlen per Smartphone, an digitale Impfzertifikate und Pläne für digitale Ausweise, die auf dem Smartphone gespeichert werden, ist schnell klar, dass Smartphones zu einem immer größeren Sicherheitsrisiko werden, wenn der Smartphone-Schutz nicht stimmt.

Denken Sie an die Smartphone-Sicherheit, im Privatleben und im Beruf

Gleich ob Sie Ihr Smartphone nur privat oder auch beruflich nutzen: Überprüfen Sie umgehend, ob Sie diesen Schutz bereits aktiv haben:

- regelmäßig Smartphone-Betriebssysteme wie Android oder iOS aktualisieren
- regelmäßig Updates für Apps installieren
- Bildschirmsperre nutzen
- in aller Regel bereits verfügbare Verschlüsselung für die Daten auf dem Smartphone nutzen
- keine Apps außerhalb der App-Stores installieren
- Verbindungen über WLAN und Bluetooth nach Nutzung abschalten
- an Diebstahl- und Verlustrisiko denken
- eine professionelle Sicherheits-App installieren

Schützen Sie Ihren „täglichen Begleiter“, um die Vorteile eines Smartphones ohne die damit verbundenen Datenrisiken nutzen zu können!

So wird Filesharing nicht zum Risikoaustausch

In Zeiten von Homeoffice und mobiler Arbeit müssen auch größere Dateien mit anderen Nutzenden ausgetauscht werden. Datenaustausch über Filesharing-Dienste ist deshalb beliebt, leider aber nicht automatisch sicher. Denken Sie an zusätzliche Schutzmaßnahmen.

Das Problem der großen Dateien

Von zu Hause aus zu arbeiten, ist seit Ausbruch der Corona-Pandemie zur neuen Normalität in der Arbeitswelt geworden. Auch in Zukunft werden dezentrale und hybride Arbeitsformen weiter an Bedeutung gewinnen, versichern Marktforscher. Doch was bedeutet das für Ihren Arbeitsalltag?

Ob Sie selbst im Büro, im Homeoffice oder unterwegs sind – es ist nur eine Frage der Zeit, dass Sie eine große Datei verschicken müssen. Sei es die neue Kundenpräsentation, das hochauflösende Foto vom neuen Messestand oder die Demo-Version einer Software, die ein Kollege beim Kunden vorstellen soll.

Wie aber überträgt man große Dateien? Als E-Mail-Anhang? Nicht nur die oftmals fehlende E-Mail-Verschlüsselung kann hier ein Problem sein. Große Dateien sind nicht wirklich als E-Mail-Anhang geeignet, entsprechend warnen viele E-Mail-Programme bereits beim Versuch.

Filesharing ist zunehmend beliebt

Anstatt die großen Dateien direkt per E-Mail zu verschicken, reicht es bei Filesharing-Diensten, einen Link als E-Mail zu versenden. Zuvor lädt man die Dateien in ein Filesharing-Verzeichnis und erzeugt den Link, den der Empfänger erhalten soll.

Das klingt einfach. Ist es auch, aber leider ist es nicht automatisch sicher, die Dateien über einen Filesharing-Dienst auszutauschen.

Das beginnt bereits damit, dass Sie sich fragen sollten, wohin Sie eigentlich die Dateien übertragen, damit sie in dem Austauschverzeichnis liegen. Meist steckt ein Cloud-Dienst dahinter, oftmals betrieben von einem Anbieter jenseits EU. So stellt sich bei personenbezogenen Daten die Frage, ob die Übertragung an den Filesharing-Dienst denn zulässig ist oder nicht.

Unklarer Speicherort, unsicherer Versand von Links

Neben der Frage, wohin Sie eigentlich die Dateien, die Sie austauschen möchten, übertragen, sollten Sie bei Filesharing auf die Datensicherheit achten.

Erscheint der Datenaustausch sehr komfortabel, ist er leider meist nicht sicher genug. Generiert der Dienst zum Beispiel einen Link, den Sie auf Knopfdruck an eine E-Mail-Adresse Ihrer Wahl versenden können, erzeugt das eine einfache E-Mail, die jeder Empfänger öffnen und bei der jeder auf den Link klicken kann. Ein Fehler in der E-Mail-Adresse führt dann dazu, dass womöglich unbefugte Dritte die Datei herunterladen können.

Besser ist es, wenn der Link allein nicht ausreicht, sondern ein Einmal-Passwort erzeugt wird, das der Empfänger benötigt und das auf einen anderen Weg an den Empfänger übertragen wird. Ein Passwort, das in der gleichen E-Mail steht wie der Link ist, bringt dagegen nichts.

Prüfen Sie also genau, welche Sicherheitsfunktionen der Filesharing-Dienst, den Sie nutzen möchten, anbietet. Verwenden Sie beruflich nur den Filesharing-Dienst, der im Unternehmen zugelassen ist.

Denken Sie auch an die Risiken, wenn Sie selbst einen Link erhalten, um über Filesharing eine größere Datei herunterladen zu können. Ist es wirklich der angegebene Absender? Was verbirgt sich tatsächlich hinter dem Link? Ist die Datei womöglich verseucht?

Sie sehen: Filesharing-Dienste vereinfachen zwar den Datenaustausch. Sie liefern aber nicht automatisch Sicherheit mit. Daher können mit dem Datenaustausch leicht zu übersehende Risiken verbunden sein.

Wissen Sie, was zu sicherem Filesharing gehört? Machen Sie den Test!

Frage: Dateien aus Filesharing-Diensten sind immer virenfrei. Stimmt das?

1. Nein. Gelangt Malware in das Austauschverzeichnis, könnte sich die Malware auch hinter dem generierten Link verbergen, der per E-Mail verteilt wird.
2. Ja, Filesharing ist immer mit einem Malware-Schutz verknüpft, der melden würde, wenn es sich um Schadsoftware handelt.

Lösung: Die Antwort 1. ist richtig. Sie können nicht davon ausgehen, dass die Dateien, die in einem Austauschverzeichnis liegen, auf Malware hin untersucht wurden. Prüfen Sie also selbst, ob die Dateien verseucht sind, bevor Sie diese übertragen. Als Empfänger eines Links sollten Sie diesen mit einem Link-Scanner überprüfen, bevor Sie die Datei herunterladen.

Frage: Die Datei, zu der der Link führt, liegt auf dem Computer des Absenders. Ist das so?

1. Ja, der Filesharing-Dienst stellt nur die Verbindung zwischen den Rechnern her.
2. Nein, die Datei wird zuvor auf der Filesharing-Plattform abgelegt, also dort zwischengespeichert.

Lösung: Die Antwort 2. ist richtig. Bei Filesharing geht es nicht um die Verknüpfung von Computern, sondern um die Übertragung von Dateien. Anstatt eine Datei direkt zu verschicken, lädt man sie bei Filesharing auf eine Plattform. Von dort lädt sie der Empfänger dann herunter. Deshalb wird die Datei an einen Dritten, den Filesharing-Betreiber, übertragen und von ihm gespeichert. Entsprechend muss bei dem Betreiber geklärt sein, ob der Datenschutz angemessen ist.

Impressum

Detlef Riese (ITDSC UG)
Datenschutzbeauftragter
Anschrift:
ITDSC UG • Bethanienstrasse 8 • 03172 Guben
Telefon: 03561 5595574 • E-Mail: d.riese@itdsc.de