OUCH!

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

Entsorgung Ihres Mobilgeräts

Übersicht

Mobile Geräte, wie Smartphones, intelligente Uhren und Tablets, entwickeln sich mit erstaunlicher Geschwindigkeit. Infolgedessen ersetzen einige Menschen ihre mobilen Geräte im Jahrestakt. Leider merken die Menschen oft nicht, wie viele persönliche Daten sich auf diesen Geräten befinden. Nachfolgend erfahren Sie, was sich auf Ihrem mobilen Gerät befinden kann und wie Sie es sicher löschen können, bevor Sie es entsorgen. Wenn Ihr mobiles Gerät von Ihrem Arbeitgeber zur Verfügung gestellt wurde oder betriebliche Daten darauf gespeichert sind, erkundigen Sie sich bitte zuerst bei Ihrem Vorgesetzten über die ordnungsgemäßen Sicherungs- und Entsorgungsverfahren.

Ihre Daten

Mobile Geräte speichern mehr sensible Daten, als viele Menschen glauben. Oft weitaus mehr als Ihr Computer.

⚠

- **Wo Sie wohnen, arbeiten und Orte die Sie besuchen**
- **Die Kontaktdaten aller Personen in Ihrem Adressbuch, einschließlich Ihrer Familie, Freunde und Kollegen**
- **Anrufverlauf einschließlich eingehender, ausgehender und verpasster Anrufe, sowie Benachrichtigungen vom Anrufbeantworter**
- **Nachrichten- oder Chatverläufe in Spielen, Social Media und sogar verschlüsselten Instant-Messaging-Diensten, wie Threema oder Signal**
- **Webbrowser-Verlauf, Suchverlauf, Cookies und zwischengespeicherte Seiten**
- **Persönliche Fotos, Videos und Audioaufnahmen**
- **Gespeicherte Passwörter und Zugangsdaten Ihrer Konten, wie z.B. Ihrer Bank, Social Media oder E-Mail Dienste.**
- **Gesundheitsdaten, einschließlich Ihres Alters, Ihrer Herzfrequenz, Ihres Trainingsverlaufs oder Ihres Blutdrucks.**

Sicheres Löschen Ihres Geräts

Unabhängig davon, wie Sie Ihr mobiles Gerät entsorgen (z.B. spenden, gegen ein neues austauschen, an ein anderes Familienmitglied weitergeben, weiterverkaufen oder sogar wegwerfen), müssen Sie sicher sein, dass Sie zuerst alle Ihre sensiblen Daten löschen. Einfaches Löschen von Daten reicht nicht aus, Sie müssen alle Daten auf Ihrem Gerät sicher löschen. Der einfachste Weg dies zu tun, ist das Zurücksetzen des Geräts auf den Werkszustand. Die Funktion zum Zurücksetzen ist von Gerät zu Gerät unterschiedlich; im Folgenden sind die Schritte für die beiden häufigsten Geräte aufgeführt. Noch sichererer ist es, wenn Sie die Daten auf Ihrem Gerät verschlüsseln, bevor Sie es zurücksetzen. Auf den meisten mobilen Geräten gelingt das ganz leicht durch das Aktivieren der Bildschirmsperre (was Sie hoffentlich bereits getan haben). Zu guter Letzt empfehlen wir Ihnen dringend Ihre Daten zu sichern, bevor Sie Ihr Gerät zurücksetzen.

- **Apple iOS Geräte: Einstellungen | Allgemein | Zurücksetzen | Alle Inhalte und Einstellungen löschen**
- **Android-Geräte: Einstellungen | Sichern und zurücksetzen | Auf Werkszustand zurücksetzen**

SIM Karten & externe Speicherkarten

Zusätzlich zu den Daten auf Ihrem Gerät müssen Sie auch Gedanken über die Daten auf Ihrer SIM-Karte (Subscriber Identity Module) machen. Ihr mobiles Gerät nutzt die SIM-Karte um eine Mobilfunk- oder Datenverbindung herzustellen. Wenn Sie Ihr Gerät löschen, enthält die SIM-Karte immer noch sensible und persönliche Daten. Wenn Sie Ihre Telefonnummer beim Wechsel auf ein neues Gerät behalten wollen, sprechen Sie mit Ihrem Telefonanbieter über die Übertragung Ihrer SIM-Karte. Wenn dies nicht möglich ist, behalten Sie Ihre alte SIM-Karte und zerstören Sie sie physisch. Damit können Sie verhindern, dass jemand anderes sie wiederverwendet, um sich als Sie auszugeben und Zugang zu Ihren Daten oder Benutzerkonten zu erhalten. Zudem verwenden einige Android-Mobilgeräte eine oder mehrere austauschbare SD-Karten (externe Speicherkarten) für zusätzlichen Speicherplatz. Entfernen Sie diese externen Speicherkarten vor der Entsorgung Ihres mobilen Geräts. Diese Karten können oft in neuen mobilen Geräten wiederverwendet werden oder, mit Hilfe eines USB-Adapters, auf Ihrem Computer verwendet werden. Wenn die Wiederverwendung Ihrer SD-Karte nicht möglich ist, dann empfehlen wir Ihnen, diese ebenfalls physisch zu vernichten.

Wenn Sie sich bei der Ausführung der oben beschriebenen Schritte nicht sicher sind, oder wenn die Schritte für das Zurücksetzen Ihres Geräts nicht wie beschrieben sind, dann bringen Sie Ihr mobiles Gerät zu dem Geschäft zurück in dem Sie es gekauft haben und holen Sie Hilfe von einem geschulten Techniker. Bevor Sie ein Gerät entsorgen, denken Sie bitte darüber nach, es gegebenenfalls zu spenden. Es gibt viele gemeinnützige Organisationen die gebrauchte Geräte annehmen und viele Mobilfunkanbieter haben in ihren Filialen Wertstofftonnen bereitgestellt.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT Sicherheit spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gastredakteur

Christopher Crowley *(@CCrowMontance) ist ein unabhängiger Berater im Bereich Washington DC mit Schwerpunkt auf Sicherheitsoperationen. Er twittert und bloggt gelegentlich. Halten Sie Ausschau nach seinem bevorstehenden Buch über Security Operations Centers. Er ist Senior Instructor am SANS Institute.*

Referenzen

SANS Kurs: Pen Testing Mobile Devices: https://sans.org/sec575

SANS Kurs: Advanced Smartphone Forensics: https://sans.org/for585

BSI für Bürger:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/BasisschutzGeraet/EinrichtungMobileGeraete/EinrichtungMobileGeraete_node.html