Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Ihre Informationen
- Löschen des Endgerätes
- SIM / Externe Speicherkarten

Entsorgung von mobilen Endgeräten

Überblick

Die Technologie mobiler Endgeräte, wie Smartphones und Tablets, entwickelt sich in einem erstaunlich hohen Tempo. Als Folge dieser rasanten Entwicklung ersetzen wir unsere mobilen Endgeräte im Schnitt alle 18 Monate. Leider entsorgen zu viele Menschen ihre älteren mobilen Geräte ohne sich Gedanken zu machen, wie viele persönliche Daten sich darauf angesammelt haben. In diesem Newsletter werden wir darauf eingehen, welche Arten von persönlichen Daten sich auf Ihrem mobilen Gerät befinden und wie Sie diese vor der Entsorgung, dem Verkauf oder dem Zurückgeben an den Provider sicher entfernen. Wenn Ihnen das Mobilgerät von Ihrem Arbeitgeber zur Verfügung gestellt wurde oder irgendwelche betrieblichen Daten darauf gespeichert sind, sollten Sie Ihren Vorgesetzten bzgl. des richtigen Backup- und Entsorgungsverfahrens kontaktieren, bevor Sie die folgenden Schritte befolgen.

Gast Autor

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) arbeitet als Berater in der Umgebung von Washington, DC. Er ist leitender Ausbilder für den Kurs Mobile Device Security and Ethical Hacking (SEC575) und Autor des Kurses Incident Response Team Management (MGT535) des SANS Institute.

Ihre persönlichen Daten

Auf mobilen Endgeräten sind weit mehr sensible Daten gespeichert als Sie vielleicht glauben, wahrscheinlich sogar mehr als auf Computern. Darunter fällt zum Beispiel:

- wo Sie leben und arbeiten und welche Orte Sie häufig besuchen
- die Kontaktinformationen für jede Person in Ihrem Adressbuch, einschließlich Familie, Freunden und Arbeitskollegen
- Anrufprotokoll einschließlich eingehender, ausgehender und verpasster Anrufe
- Text- und Sprachnachrichten
- Chat-Sitzungen innerhalb von Anwendungen, wie z.B. Spielen und Sozialen Medien
- Standortbezogene Daten, basierend auf GPS-Koordinaten oder Funkzellenverlauf
- Verlauf besuchter Webseiten, Cookies und zwischengespeicherter Webseiten
- Persönliche Fotos, Videos, Audioaufzeichnungen und E-Mails
- Gespeicherte Passwörter und Zugriff auf persönliche Konten (Online-Banking oder E-Mail)
- Zugriff auf Fotos, Dateien oder Informationen die in der Cloud gespeichert sind
- gesundheitsbezogene Informationen, einschließlich Gewicht, Herzfrequenz, Blutdruck oder Ernährungsplan

Entsorgung von mobilen Endgeräten

Löschen des Endgerätes

Wie Sie sehen, kann sich eine enorme Menge an sensiblen Daten auf Ihrem mobilen Gerät befinden. Unabhängig davon wie Sie sich von Ihrem mobilen Gerät trennen, ob Sie es spenden, einem anderen Familienmitglied geben, weiterverkaufen oder sogar komplett entsorgen, müssen Sie sicher sein, dass Sie zuerst alle Ihre sensiblen Informationen löschen. Darüber hinaus sollten sie zusätzlich all Ihre Informationen löschen, wenn Sie Ihr mobiles Endgerät zurückgeben oder gegen ein Neues eintauschen. Wenn Sie dies nicht tun, kann jeder, der am Ende Ihr mobiles Endgerät in den Händen hält, mit überschaubarem Aufwand auf Ihre persönlichen Informationen zugreifen. Bevor Sie jedoch Ihre Daten löschen, sollten Sie eine Sicherung aller Ihrer Daten, einschließlich Fotos, Videos und sonstiger Informationen, durchführen. Sobald Sie Ihr Gerät löschen, werden Sie nicht mehr in der Lage sein, die Daten, die auf dem Gerät gespeichert waren, wiederherzustellen.

Achten Sie bei der Entsorgung Ihres mobilen Endgeräts darauf, dies auf seine Werkseinstellungen zurückzusetzen und entfernen Sie die SIM-oder SD-Karten sofern Ihr Gerät diese enthält.

Nachdem Sie Ihre Daten gesichert haben, können Sie das Gerät sicher löschen. Ein einfaches Löschen von Dateien, Fotos oder Daten ist nicht genug. Daten, die gelöscht wurden lassen sich leicht mit kostenlosen Tools im Internet wiederherstellen. Sie wollen aber alle Daten auf dem Gerät verlässlich löschen, dies nennt sich auch „wiping“. Mit dieser Methode überschreiben sie die Daten mit zufälligen oder vordefinierten Werten, so dass diese nicht wiederhergestellt werden können. Der einfachste Weg, dies zu tun ist die Funktion “Factory-Reset” des Geräts zu verwenden. Dadurch wird es auf den Zustand zurückgesetzt, der vor der ersten Benutzung nach Auslieferung existierte. Das Zurücksetzen auf die Werkseinstellungen stellt meist die einfachste Methode zum Entfernen von Daten von mobilen Endgeräten dar. Diese Funktion variiert zwischen den verschiedenen Geräten. Im Folgenden sind die Schritte für die drei gängigsten Geräte aufgelistet.

- Apple (iOS) Gerät: Einstellungen | Allgemein | Zurücksetzen | Inhalte & Einstellungen löschen
- Android-Geräte: Einstellungen | Nutzer | Sichern & zurücksetzen
- Windows Phones: Einstellungen | Info | Handy zurücksetzen

Wenn Sie noch Fragen bzgl. des Zurücksetzens Ihres mobilen Endgerätes auf den Werkszustand haben, sehen Sie in der Bedienungsanleitung oder auf der Website des Herstellers nach. Denken Sie daran, ein einfaches Löschen Ihrer persönlichen Daten ist nicht genug, da diese leicht wiederhergestellt werden können.

SIM / Externe Speicherkarten

Zusätzlich zu den auf dem Gerät selbst gespeicherten Daten müssen Sie auch bedenken, wie Sie mit Ihrer SIM-Karte (Subscriber Identity Module) umgehen. Eine SIM-Karte wird vom mobilen Endgerät genutzt, um ein mobile Telefon- oder Datenverbindung

Entsorgung von mobilen Endgeräten

herzustellen. Wenn Sie Ihr Gerät auf Werkseinstellung zurücksetzen bleiben die Daten auf der SIM-Karte, und somit die darauf befindlichen persönlichen Informationen, erhalten. Wenn Sie Ihre Telefonnummer auch mit dem neuen Gerät benutzen wollen, sprechen Sie mit dem Verkäufer bzgl. der Vorgehensweise. Wenn dies nicht möglich ist, da Ihr neues Telefon z.B. eine andere SIM-Karten-Größe verwendet, behalten Sie Ihre alte SIM-Karte und zerstören Sie diese (z.B. durch Zerschneiden mit einer Schere) um auszuschließen, dass jemand anderes diese weiter verwenden kann.

Einige mobile Endgeräte nutzen eine zusätzliche SD (Secure Digital) Karte, um zusätzlichen Speicherplatz bereitzustellen. Diese Speicherkarten enthalten oft Bilder, Smartphone-Anwendungen und andere sensible Daten. Vergessen Sie daher nicht, externe Speicherkarten aus Ihrem mobilen Endgerät vor der Entsorgung zu entfernen (bei einigen Geräten ist die SD-Karte im Batteriefach des Geräts versteckt, möglicherweise unter dem Akku). Diese Karten können oft in neuen mobilen Geräten wiederverwendet werden oder als externer Speicher an Ihrem Computer mit einem USB-Adapter verwendet werden. Falls eine Wiederverwendung der SD-Karte nicht möglich ist, verfahren Sie genauso wie mit Ihrer alten SIM-Karte und zerstören Sie diese physisch.

Falls Sie vor der Ausführung eines der im Newsletter beschriebenen Schritte Bedenken haben, sprechen Sie mit einem Fachmann, am besten in dem Geschäft, in dem Sie Ihr mobiles Endgerät gekauft haben. Bevor Sie Ihr Gerät entsorgen, bedenken Sie bitte, dass dies auch gespendet werden kann. Es gibt viele ausgezeichnete gemeinnützige Organisationen, die gebrauchte mobile Endgeräte gerne entgegennehmen.

Weiterführende Informationen

BSI für Bürger: Sicheres Löschen von Daten:
https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/RichtigLoeschen/richtigloeschen_node.html
OUCH! Archiv - Sicherung und Wiederherstellung Ihrer Daten:
http://www.securingthehuman.org/ouch/2013#september2013

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

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

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis