Der monatliche Security Awareness Newsletter für Jedermann

Absicherung Ihrer Mobilen Geräte

Überblick

Ihre mobilen Geräte sind ein faszinierender und einfacher Weg, mit Freunden, Geschäften oder Ihrer Bank zu kommunizieren, Filme anzusehen, Spiele zu spielen oder eine Vielzahl andere Dinge zu tun. Weil die Geräte in Ihrem Leben eine so wichtige Rolle einnehmen, wollen wir Ihnen im Folgenden einige Tipps geben um Sie und Ihre Geräte bestmöglich zu sichern.

Absicherung Ihrer Geräte

Es überrascht Sie vielleicht zu erfahren, dass das größte Risiko für Ihre mobilen Geräte nicht Hacker, sondern sehr wahrscheinlich Sie selbst sind. Es ist viel wahrscheinlicher, dass Sie ein Gerät verlieren oder vergessen, als dass es jemand hackt. Die wichtigste Maßnahme ist daher die Aktivierung der automatischen Bildschirmsperre. Jedes Mal, wenn Sie Ihr Gerät nutzen möchten, müssen Sie von nun an den Bildschirm entsperren, z.B. mit einem starken Passcode oder mit Ihrem Fingerabdruck. Dies stellt sicher, dass niemand auf das Gerät zugreifen kann, wenn Sie es verlieren oder es gestohlen wird. Hier sind weitere Schritte die der Absicherung Ihrer Geräte dienen:

Aktualisierung

Aktivieren Sie das automatische Aktualisieren Ihrer Geräte, so dass darauf immer die neueste Version des Betriebssystems und der Apps laufen. Angreifer suchen ständig nach Schwachstellen in Software, und Hersteller veröffentlichen Aktualisierungen und Korrekturen, um solche Lücken zu schließen. Durch die Nutzung der aktuellsten Versionen machen Sie es Angreifern deutlich schwerer, die Geräte zu hacken.

Verfolgen

Installieren oder Aktivieren Sie Softwarefunktionen um die Geräte über das Internet verfolgen zu können. Sollte Ihr Gerät verloren gehen oder gestohlen werden, können Sie so jederzeit seinen Standort herausfinden und im schlimmsten Fall eine Fernlöschung durchführen, um all Ihre Daten vom Gerät zu löschen.

Vertrauenswürdige Apps

Laden Sie nur Apps die Sie brauchen, und nur aus vertrauenswürdigen Quellen. Für iPads oder iPhones bedeutet das die Nutzung des Apple App Store. Für Android laden Sie Apps über Google Play und für Amazon Tablets nutzen Sie den Amazon App Store. Vielleicht wären Sie in der Lage, Apps auch aus anderen Quellen zu laden, diese sind aber meist nicht sicherheitsüberprüft und viel wahrscheinlicher infiziert. Bevor Sie eine

App herunterladen sollten Sie zudem sicherstellen, dass sie möglichst viele positive Bewertungen hat und vom Hersteller regelmäßig aktualisiert wird. Lassen Sie die Finger von brandneuen Apps mit wenigen Kritiken oder solchen ohne Aktualisierungen. Wenn Sie eine App länger nicht mehr nutzen, löschen Sie sie vollständig von Ihrem Gerät.

Datenschutzeinstellungen

Wenn Sie eine neue App installieren, überprüfen Sie die Datenschutzeinstellungen und Zugriffsberechtigungen. Braucht die gerade heruntergeladene App beispielsweise wirklich Zugriff auf die Daten all Ihrer Freunde und Kontakte? Sie sollten auch den Zugriff auf den aktuellen Standort generell verbieten und nur für diejenigen Apps zulassen, bei denen Sie das für sinnvoll halten. Wenn Sie sich mit den von einer App angeforderten Zugriffsrechten nicht wohl fühlen, suchen Sie sich einfach eine andere App die Ihre Bedürfnisse erfüllt. Prüfen Sie zudem immer wieder einmal die Berechtigungen um sicherzugehen, dass sich nichts geändert hat.

Backups

Sichern Sie immer Ihre Daten. Auf mobilen Geräten wird ein großer Teil davon oft automatisch in die Cloud gesichert, wie z.B. Ihre Fotos oder Nachrichten. Backups sichern jedoch auch Ihre Einstellungen, Apps und sonstigen Geräteinformationen und machen es so deutlich leichter, nach Verlust oder bei Wechsel auf ein neues Gerät, alles wiederherzustellen.

Beruflich

Bei beruflicher Nutzung sollten Sie besonders umsichtig sein und niemals Bilder oder Videos anfertigen, die möglicherweise schützenswerte Daten enthalten, wie z.B. Fotos von Whiteboards oder Computerbildschirmen.

Ihre mobilen Geräte sind mächtige Werkzeuge. Das Befolgen dieser einfachen Schritte trägt viel dazu bei, Sie und Ihre Geräte abzusichern.

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-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Weiterführende Informationen

Starke Passwörter:	https://www.sans.org/u/A3E
Datensicherung und Wiederherstellung:	https://www.sans.org/u/A3z
Sichere Entsorgung Ihres Mobilgeräts:	https://www.sans.org/u/A3u
Sichere Nutzung mobiler Apps:	https://www.sans.org/u/A3p
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License

Redaktionsleitung: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley