Einfach mal ausschalten:
Warum Smartphone-Detox unsere Geräte schützen kann

24/7 im Einsatz – ohne Gemurre. Wir muten unseren Mobilgeräten ganz schön viel zu. Sie aber regelmäßig komplett herunterzufahren, kommt Hard- und Software zugute. Außerdem eine gute Gelegenheit, unnötigen (App-) Ballast abzuwerfen, findet Paul Ducklin von Sophos.

Regelmäßiges Ausmisten beruhigt die Nerven und man behält den Überblick. So wie wir Hausrat, Dokumente und Bekanntschaften kritisch unter die Lupe nehmen, sollten wir auch unsere technischen Geräte detoxen.

Der australische Premierminister Anthony Albanese riet seinen Landsleuten kürzlich, ihre Handys jede Nacht für fünf Minuten auszuschalten – und zwar für die Cybersicherheit. Die britische Tageszeitung The Guardian, die das Zitat veröffentlichte, mutmaßt, dass diese Angaben darauf abzielen, „jede Spyware zu stoppen, die möglicherweise bereits auf dem Gerät im Hintergrund läuft."

„Da ist etwas dran", so Paul Ducklin von Sophos. „Denn Infektionen mit Schadsoftware lassen sich generell in zwei Kategorien einteilen: 'Ständige Bedrohungen' und der ‚Rest'. Ständig bezieht sich hierbei auf kriminelle Software, die die Anwendung, die sie gestartet hat, überlebt. Sie übersteht auch aktuelle Login-Sessions (wenn man am Laptop ist) und sogar einen komplett Abschalt- und Neustart-Prozess. Nicht-dauerhafte Bedrohungen überleben weder App-Neustarts noch einen System-Reboot. Und ein Herunterfahren des Geräts schließt generell alle Anwendungen und beendet das operative System. Es stoppt damit jegliche Schad- oder Spionagesoftware, die im Hintergrund aktiv war. In dieser Hinsicht ist ein regelmäßiger Neustart für das Handy durchaus sinnvoll und fügt dem gerät auch keinen Schaden zu."

Reboot schützt vor Schadsoftware – manchmal

Das Problem ist, dass die meiste Malware, insbesondere aufwändig entwickelte, verborgene und mobile Spyware, heutzutage zur Kategorie der dauerhaften Bedrohung gehört. Ein Beispiel: das letzte Sicherheitsupdate von Apple zur Eliminierung einer Spionagesoftware für iPhones, iPads und Macs beinhaltete Patches für zwei Zero-Day-Code-Ausführungs-Schwachstellen: eine im WebKit (Apples tiefverankerter Browser-Software) und eine im Kernel des Betriebssystems.

Typ 1: Schadsoftware via Browser

Wenn Angreifer die Ausführung von unautorisiertem Code nur im Browser des Opfers ausführen können, dann ist es sehr wahrscheinlich, dass
a) die Schadsoftware sich nicht von dem Browser-Prozess lösen kann und
b) damit auch nicht in der Lage ist, Zugang oder Manipulationen an irgendwelchen anderen Teilen des Geräts vornehmen zu können.

Die Schadsoftware ist hier limitiert auf die laufende Browser-Sitzung. Ein Neustart des Handys würde das Gerät damit praktischerweise entseuchen.

Typ 2: Schadsoftware via System-Schwachstelle

„Wenn aber der unautorisierte Code, den die Angreifer innerhalb des Browsers über den Zero-Day-Webkit-Fehler starten, daraufhin den anderen Zero-Day-Bug im Kernel auslöst, dann hat der Handy-Nutzer ein Problem", so Ducklin. „Cyberkriminelle können die nicht-permanente Schadsoftware im Browser nutzen, um den Kernel selbst zu

kompromittieren und erhalten damit die Kontrolle über das gesamte Gerät. Damit können sie den unautorisierten Code im Kernel verwenden, um eine dauerhafte Schadsoftware-Infektion zu implantieren, die sich automatisch startet, auch wenn das Telefon aus ist. Genau das ist der Grund, warum Angreifer diesen Weg ausgewählt haben, denn das gewissenhaft tägliche Neustarten des Handys wiegt das Opfer in falscher Sicherheit."

Weitere Tipps zum Handy-Detox:
Die folgenden Sicherheitstipps sind leider nicht ganz so einfach wie das oben beschriebene „Aus und wieder An", verdienen aber trotzdem eine Chance:

- Weg mit Apps, die nicht mehr gebraucht werden. Deinstallieren Sie überflüssige Anwendungen vollständig und löschen Sie alle damit verbundenen Daten. Sollten Sie die App vermissen, können Sie sie ja wieder nachinstallieren. Leider haben viele mobile Geräte vorinstallierte Software, die nicht entfernen werden kann, sogenannte Bloatware. Einiges lässt sich aber zumindest abstellen, so verhindert der Nutzer, dass sie nicht automatisch im Hintergrund laufen.

- Loggen Sie sich explizit von Anwendungen aus, wenn sie nicht mehr in Gebrauch sind. Ein unbeliebter Rat, weil es bedeutet, dass man eine App wie zum Beispiel Zoom oder Outlook, nicht einfach wieder öffnen und in das Meeting oder die Diskussionsgruppe zurückschalten kann. Und: das Login mit Passwort und 2FA über die fummelige Handy-Tastatur kann lästig sein. Aber der beste Weg, seine Daten nicht aus Versehen preiszugeben, geht über die eigene Autorisierung.
  Der Neustart des Gerätes bedeutet übrigens nicht gleichzeitig den Neustart des Anmeldestatus' von Apps. Das Handy geht normalerweise mit den üblich genutzten Anwendungen in Betrieb, die sich automatisch bei ihren jeweiligen Online-Konten neu anmelden, es sei denn, Sie haben sich zuvor absichtlich abgemeldet. Leider setzen verschiedene Apps (und verschiedene Betriebssystemoptionen) ihre Abmeldevorgänge auf unterschiedliche Weise um, so dass Sie möglicherweise etwas herumprobieren müssen, um herauszufinden, wie sie sich wo ausloggen müssen.

- Befassen Sie sich mit Privatsphäre-Einstellungen all Ihrer Anwendungen und Dienste. Einige Funktionen lassen sich direkt über das Betriebssystem des Handys festlegen, andere in den Apps selbst und wieder andere nur über ein Online-Portal. Etwas mühsam, aber es lohnt sich.

- Lernen Sie, wie man die Browser-Historie löscht und wenden Sie diesen Vorgang regelmäßig an. Mit dem Neustart des Gerätes werden diese Daten eben nicht automatisch gelöscht.

- Schalten Sie so viele Funktionen wie möglich auf dem gesperrten Bildschirm aus. Am besten lasen Sie nur Notruf und die Entsperrung zu. Denn jede Anwendung, die auf dem gesperrten Bildschirm auftaucht, schwächt die eigene Cybersicherheit – schließlich kann sie jeder mitlesen.

- Setzen Sie den längsten Sperrcode und die kürzeste Sperrzeit, die Sie noch tolerieren können. Oder nutzen Sie Identifizierungsmethoden wie Gesichtserkennung. Und: gewöhnen Sie sich gern an, Ihr Handy zu sperren, sobald Sie es ablegen.

- „Be aware of what you share" – Seien Sie vorsichtig mit dem, was Sie teilen. Der aktuelle Standort ist gerade für die Navigation nicht wichtig? Dann bitte ausschalten. Surfen ist gerade unnötig, zum Beispiel im Kino? Dann Wi-Fi ausmachen. Ebenso verhält es sich mit Bluetooth.

- Setzen Sie einen PIN-Code auf Ihrer SIM-Karte. Eine physische SIM-Karte ist der Chiffrierschlüssel für Anrufe, Textnachrichten, und vielleicht auch einige 2FA Sicherheitscodes oder Konto-Zurücksetzung. Bei Diebstahl des Geräts muss man dem Kriminellen seine Daten ja nicht auf dem Silbertablett servieren.

Und was ist mit dem Laptop?
Es gibt keinen Grund, warum nur das Handy ein Fresh-Up bekommen sollte. Auch Laptops profitieren vom regelmäßigen Neustart. Der Schlafmodus auf modernen Geräten ist zwar ziemlich praktisch, aber angesichts des schnellen Hochfahrens aktueller Modelle, lieber einmal ganz aus und wieder an. Auch hier bitte immer mal wieder den Browser-Verlauf inklusive Cookies etc. bereinigen.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de