Bluetooth absichern

Die Funktechnik Bluetooth ist zwar komfortabel, aber alles andere als sicher. Schützen Sie Ihre Bluetooth-Verbindungen – auch gegen die neue «KNOB»-Sicherheitslücke. ● **VON GABY SALVISBERG**

Unter Bluetooth versteht man eine für kurze Distanzen vorgesehene Funktechnologie. Am häufigsten kommt sie beim Verbinden von Kopfhörern oder Lautsprechern mit dem Smartphone zum Einsatz. Es gibt aber auch Bluetooth-Mäuse, -Eingabestifte, -Tastaturen und -Game-Controller, die sich mit dem PC oder einer Spielkonsole verbinden lassen. Inzwischen ebenso im Trend sind Smart-Home-Geräte («Internet of Things», IoT), die untereinander und mit den Steuergeräten via Bluetooth kommunizieren.

Funktechnologien aller Art sind für Angreifer verlockend. Gerade an Orten, an denen sich viele Personen mit Bluetooth-Geräten aufhalten, möchte ein Bösewicht vielleicht mal ein paar Daten abfangen oder den Geräten Schädlinge einverleiben.

Zum Glück ist Bluetooth aber relativ sicher. Es weist eine vergleichsweise geringe Funkreichweite auf. Das bedeutet, dass sich der Angreifer in unmittelbarer Nähe seiner potenziellen Opfer befinden muss. Ausserdem besteht die grösste Gefahr für Bluetooth-Verbindungen jeweils nur sehr kurz, nämlich im empfindlichen Moment des Pairings – meistens jedenfalls.

Was bedeutet Pairing?

Gäbe es kein Pairing, könnte jedes Handy auf jeden Kopfhörer in der Umgebung seinen Sound abspielen und das Mikrofon von jedem erreichbaren Headset abhorchen. Das Pairing sorgt jedoch dafür, dass Sie genau Ihr Headset, Ihren Kopfhörer mit genau Ihrem Smartphone verbinden, ohne sich durch andere Geräte stören zu lassen und ohne andere zu tangieren. Am Beispiel des Smartphones und eines Kopfhörers verläuft das so: Sie schalten Bluetooth auf Ihrem Smartphone ein und aktivieren die Suche. Damit sucht das Smartphone eine kurze Zeit die Umgebung nach «paarungswilligen» Bluetooth-Geräten ab. Damit der Kopfhörer sich «pairen» lässt und vom suchenden Smartphone entdeckt wird, drücken Sie am Kopfhörer eine bestimmte Taste; manchmal muss man diese ein paar Sekunden lang betätigen. Das Smartphone listet die gefundenen Geräte auf – inklusive Ihres Kopfhörers. Sobald Sie diesen auswählen, vereinbaren die beiden Geräte untereinander einen sicheren, geheimen Langzeitschlüssel, mit dem sie die Daten in Zukunft für die Kommunikation verschlüsseln werden. Ab jetzt sind Kopfhörer und Smartphone aufeinander eingeschworen und der Pairing-Vorgang ist abgeschlossen. Ab diesem Zeitpunkt kann die Bluetooth-Verbindung als relativ sicher betrachtet werden.

Sicherheitstipps

Achten Sie darauf, dass Sie neue Bluetooth-Geräte nur in sicheren Umgebungen mit Ihrem Smartphone oder Computer pairen. Angenommen, man drückt Ihnen an einer Computermesse einen Bluetooth-Kopfhörer zum Testen in die Hand, warten Sie vielleicht besser mit dem Pairing, bis Sie die grosse Masse der Computerfreaks und Möchtegern-Hacker hinter sich gelassen haben. Verzichten Sie besonders während des Pairing-Vorgangs aufs Annehmen irgendwelcher sonstiger Dateien oder Verbindungen.

Verwenden Sie irgendeine Art von Zugangssperre zu Ihrem Bluetooth-fähigen Notebook oder Smartphone, also eine PIN oder ein Passwort. Wenn Sie ein Bluetooth-Peripheriegerät entsorgen, verlieren oder es gestohlen wurde, entfernen Sie es umgehend aus der Liste der bekannten Geräte auf Ihrem Notebook oder Smartphone. Rufen Sie hierfür *Einstellungen/Bluetooth* auf. Tippen oder klicken Sie das abhandengekommene Gerät an und entfernen Sie es.

Binden Sie Angreifern nicht auf die Nase, welchen Gerätetyp Sie haben und wie Ihr eigener Name lautet. Schlecht wäre also zum Beispiel «Hanna Musters LG K10». Benennen Sie Ihr Gerät für Bluetooth-Zwecke in etwas Unverfängliches um, das Sie wiedererkennen, aber das Fremden möglichst keinen Aufschluss über Gerätetyp und Inhaber gibt. Öffnen Sie hierfür die *Einstellungen*-App, gehen Sie zu etwas wie *Verbundene Geräte/Verbindungseinstellungen/Bluetooth*. Tippen Sie auf *Gerätename*, um den Namen zu bearbeiten, **Bild 1**.

Foto: Shutterstock/Media Whalestock

Taufen Sie es vielleicht `Mein Handy`, `Fon mit Bluetooth` oder `Flunderphone`.

Schalten Sie Bluetooth aus, während Sie es nicht brauchen. Auch wenn ein untätiges Bluetooth heute nicht mehr viel Saft braucht, dürfte das dennoch eine positive Nebenwirkung auf Ihren Akku-Ladestand haben.

Für nur gelegentliche Bluetooth-Nutzung bietet sich ein schnell erreichbarer *Ein-/Aus*-Schaltknopf an. Bei vielen Android-Geräten können Sie mit einem Wisch von oben nach unten die *Schnellzugriffe* öffnen. Die lassen sich meist über einen Tipper auf etwas wie ein *Bleistift*-Symbol anpassen, **Bild 2 A**.

So können Sie die häufig benötigten Icons einmal länger antippen und auf die vorderen Plätze ziehen. Gönnen Sie auch *Bluetooth* **B** einen solchen Logenplatz, damit Sie das in Zukunft schnell zur Hand haben.

Es gibt allerdings auch in Bluetooth immer wieder Sicherheitslücken. Manche Angriffe haben «nur» zur Folge, dass die Verbindung zu bereits gepairten Geräten unterbricht. Damit kann ein Angreifer bewirken, dass Sie es neu verbinden oder gar neu pairen müssen. Es ist in diesem Fall das Ziel des Angreifers, den heiklen Pairing-Vorgang zu provozieren, um sich möglicherweise in die Kommunikation der beiden Geräte einzuklinken. Seien Sie also skeptisch, wenn ein gepairtes, von Ihnen oft genutztes Gerät plötzlich wieder ein Pairing verlangt.

Und natürlich: Updates. Installieren Sie nicht nur Betriebssystem- und Treiber-Updates für Ihren PC und Ihr Smartphone. Auch die Bluetooth-Geräte selbst lassen sich mittels Firmware-Updates aktualisieren. Suchen Sie auf der Herstellerwebseite Ihres Bluetooth-Gadgets nach Downloads zu Ihrem Gerät. Oftmals finden Sie einen Firmware-Installer, der Ihre Hardware auf den neusten Stand bringt. Das ist besonders jetzt sehr ratsam, da es eine wichtige Sicherheitslücke zu schliessen gibt: jene gegen die KNOB-Attacke.

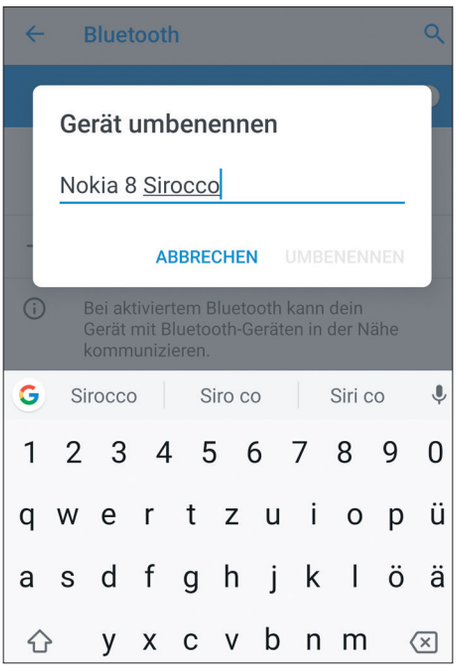

Bild 1: Taufen Sie Ihr Gerät so, dass es nichts über sich oder den Besitzer verrät

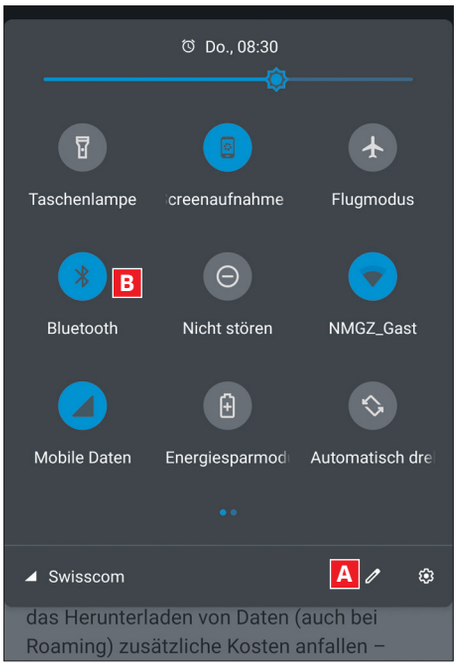

Bild 2: Legen Sie das Icon zum Einschalten von Bluetooth auf einen der vorderen Plätze

Die KNOB-Attacke

Letztes Jahr wurde eine als «KNOB» (Key Negotiation of Bluetooth, Kennnummer: CVE-2019-9506) bezeichnete Sicherheitslücke in Bluetooth entdeckt. Beim Pairing erzeugen die beiden verbundenen Geräte einen sicheren Langzeitschlüssel. Zusätzlich verhandeln sie bei jeder Verbindungsaufnahme (etwa nach dem Einschalten der Geräte) einen Sitzungsschlüssel, der aus diesem Langzeitschlüssel abgeleitet wird. Leider liess sich dieser Sitzungsschlüssel in enorm vielen Geräten auf die Länge von lediglich einem Byte drücken. Das beschränkt die Anzahl möglicher Schlüssel auf läppische 256, die im Nu mittels «Brute Force» durchprobiert und herausgefunden sind. Die Hersteller wurden durch die Entdecker der Lücke letztes Jahr informiert. Im Sommer 2019 haben die meisten Betriebssystemhersteller ein Update veröffentlicht, weshalb ab dem Zeitpunkt auch öffentlich über die Lücke informiert werden durfte. Apple hat im Juli entsprechende Updates ausgeliefert und Microsofts Sicherheits-Patch gegen KNOB erschien im August 2019, siehe Link **support.microsoft.com/kb/4514157**.

Bloss: Dieser stopft die Lücke nicht wirklich! Er hat in Windows lediglich eine Einstellungsmöglichkeit eingebaut, um eine minimale Länge von 7 Byte für den Session Key zu erzwingen. Die Einstellung ist jedoch inaktiv. Begründung: Erstens seien spezielle Geräte und eine relativ kurze Distanz für den Angriff nötig. Zweitens müsse der Angreifer die anvisierten Geräte abschirmen, damit er beispielsweise Schadcode übermitteln könne. Ausserdem gibt es laut Microsoft eine Reihe von Geräten, die mit dieser Mindestlänge des Session Keys nicht klarkommen. Und die Lücke werde derzeit gar nicht aktiv ausgenützt. Wer mag, kann die Einstellung in der Windows-Registry dennoch von Hand aktivieren. Klicken Sie hierfür auf *Start*, tippen Sie `cmd` ein, klicken Sie mit rechts auf die *Eingabeaufforderung* und wählen Sie *Als Administrator ausführen*. Tippen Sie nun die Zeile aus der Box unten ein. Starten Sie danach den Computer neu. Es wäre möglich, dass manche Ihrer Bluetooth-Geräte nicht mehr funktionieren. In diesem Fall machen Sie die Änderung wieder rückgängig.

Suchen Sie beim Hersteller eines betroffenen Geräts nach der Kennnummer `CVE-2019-9506`. Vielleicht gibt es ja ein Treiber- oder Firmware-Update, mit dem Sie es absichern können.

Bei Android-Geräten müssen Sie betreffs KNOB-Lücke auf zügige Updates hoffen. Wer die Sicherheits-Updates vom 5. August 2019 erhalten hat, dürfte auf der sicheren Seite sein. Öffnen Sie die *Einstellungen*-App Ihres Smartphones, gehen Sie zu etwas wie *System/Erweitert/Systemupdate*. Versuchen Sie auch einmal mit *Auf Updates prüfen*, **Bild 3**. Auch wenn das Update noch auf sich warten lässt: Solange die Lücke nicht aktiv ausgenützt wird, brauchen Sie auf Bluetooth nicht zu verzichten. ●

Bild 3: Dieses Android-Gerät hat sogar schon die Oktober-Updates an Bord

Registry-Eintrag gegen KNOB-Attacke

AKTIVIEREN (ALLES AUF 1 ZEILE SCHREIBEN)

```
reg add HKLM\System\CurrentControlSet\Policies\Hardware\Bluetooth /v
EnableMinimumEncryptionKeySize /t REG_DWORD /f /d 1
```

DEAKTIVIEREN (ALLES AUF 1 ZEILE SCHREIBEN)

```
reg add HKLM\System\CurrentControlSet\Policies\Hardware\Bluetooth /v
EnableMinimumEncryptionKeySize /t REG_DWORD /f /d 0
```