MOBILFUNK

Datenfischen im Regierungsbezirk

Sicherheitsmängel bei Bluetooth-Handys: Per Funk lassen sich Gespräche mithören oder Rufnummern auslesen – der Nutzer merkt von dem Lauschangriff nichts.

Die privaten Handy-Nummern von Politikern, Personenschützern und Polizei-Einsatzleitern gehören zum gutgehüteten Herrschaftswissen der Republik – eigentlich. Doch um sie in Erfahrung zu bringen, reichen ein bisschen Geduld und etwas technisches Können.

Um das zu beweisen, unternahm „Dagobert“ vor zwei Wochen in der Hauptstadt ein kleines Experiment. Er war zur Hackerkonferenz „ph-neutral“ nach Berlin gereist. Seinen bürgerlichen Namen möchte der Informatiker und Sicherheitsberater lieber nicht in der Zeitung lesen.

Sein Versuchsaufbau war denkbar einfach: Er mietete sich ein Fahrrad und radelte durch das Regierungsviertel, drehte eine Runde um Reichstag und Paul-Löbe-Haus. Wenn irgendwo eine schwarze Limousine vorfuhr, blieb er in einigen Metern Abstand stehen und durchsuchte die Taschen der vorbeieilenden Bodyguards und Politiker nach Telefonnummern – allerdings nicht physisch.

Das Durchfilzen nach Daten übernahm ein kleiner Rechner in seinem Rucksack, ohne dass die Durchsuchten etwas davon bemerkten. Jeweils etwa 15 Sekunden reichten dafür aus.

Nach einer halben Stunde war der Test beendet. Die Ausbeute: die kompletten Telefonnummernverzeichnisse von drei Handys, dazu die Informationen, wer angerufen hat, wer angerufen wurde. Mit dabei waren die Durchwahlnummern von Kontakten bei Polizei, Bundesgrenzschutz, Kanzleramt und Verfassungsschutz. Wahrscheinlich handelte es sich um die Handys von Bodyguards. Ein Politiker-Handy war anscheinend nicht dabei. Aber das wäre wohl nur eine Frage der Zeit gewesen.

Das Problem ist Datenschützern bekannt: Einige moderne Handys verfügen über eine Sicherheitslücke, den sogenannten Bluebug. Der Name bezieht sich auf den Funkstandard „Bluetooth“.

Normalerweise wird der Handy-Nutzer gewarnt, wenn ein unautorisiertes Bluetooth-Gerät versucht, auf das eigene Mobiltelefon zuzugreifen. Doch einige Modelle lassen sich austricksen: Unbemerkt vom Besitzer lassen sich Adressen auslesen oder verändern. Sogar Gespräche können gestartet oder mitgehört werden.

Bisher war für derartige Lauschangriffe ein Notebook erforderlich. Mittlerweile reicht schon ein anderes Bluetooth-Handy. Und per Richtantenne lassen sich Handys sogar aus fast zwei Kilometer Entfernung manipulieren.

Nicht nur in der Berliner Luft schwirren Daten umher, die nicht in unbefugte Hände gehören. Ein Test in den britischen Houses of Parliament führte zu ähnlichen Ergebnissen. Seitdem gilt eine neue Verordnung: Bluetooth-Handys müssen im Parlamentsgebäude ausgeschaltet bleiben.

Eine blauäugige Regelung; denn in der mobilfunkvernetzten Welt reicht es nicht aus, Handy-Sicherheit an einem bestimmten Ort zu garantieren – im Zweifel lauern die Datensauger eben vor der Tür.

Bei modernen Handys sind sehr viele sensible Daten zu holen: Wer häufig telefoniert, hat leicht 500 Nummern in seinem Speicher; dazu kommen oft SMS, E-Mails, Fotos, PIN-Codes für Bankautomaten, Office-Dokumente. Selten wurden derart sensible Datensätze so leichtfertig in der Hosentasche herumgetragen wie heute – ein Alptraum für Datenschützer.

Der eigentliche Skandal der Bluetooth-Attacken liegt jedoch bei der schlafmützigen Industrie: Schon vor über einem Jahr hat „Dagobert“ die Handy-Hersteller auf die Lücke hingewiesen – und geholfen, diese zu schließen. Seitdem bieten die Firmen zwar Software-Updates für ihre Handys an; doch nur wenige Kunden haben überhaupt mitbekommen, dass ihre Geräte ein schweres Sicherheitsproblem haben.

Dabei sei es eigentlich recht einfach, sich zu schützen, so der Experte: „Schalten Sie so oft es geht die Bluetooth-Funktion aus. Oder kaufen Sie einfach ein altes Handy – ohne Bluetooth.“

HILMAR SCHMUNDT

Handy-Attacke

Wie das Abhören über Bluetooth funktioniert