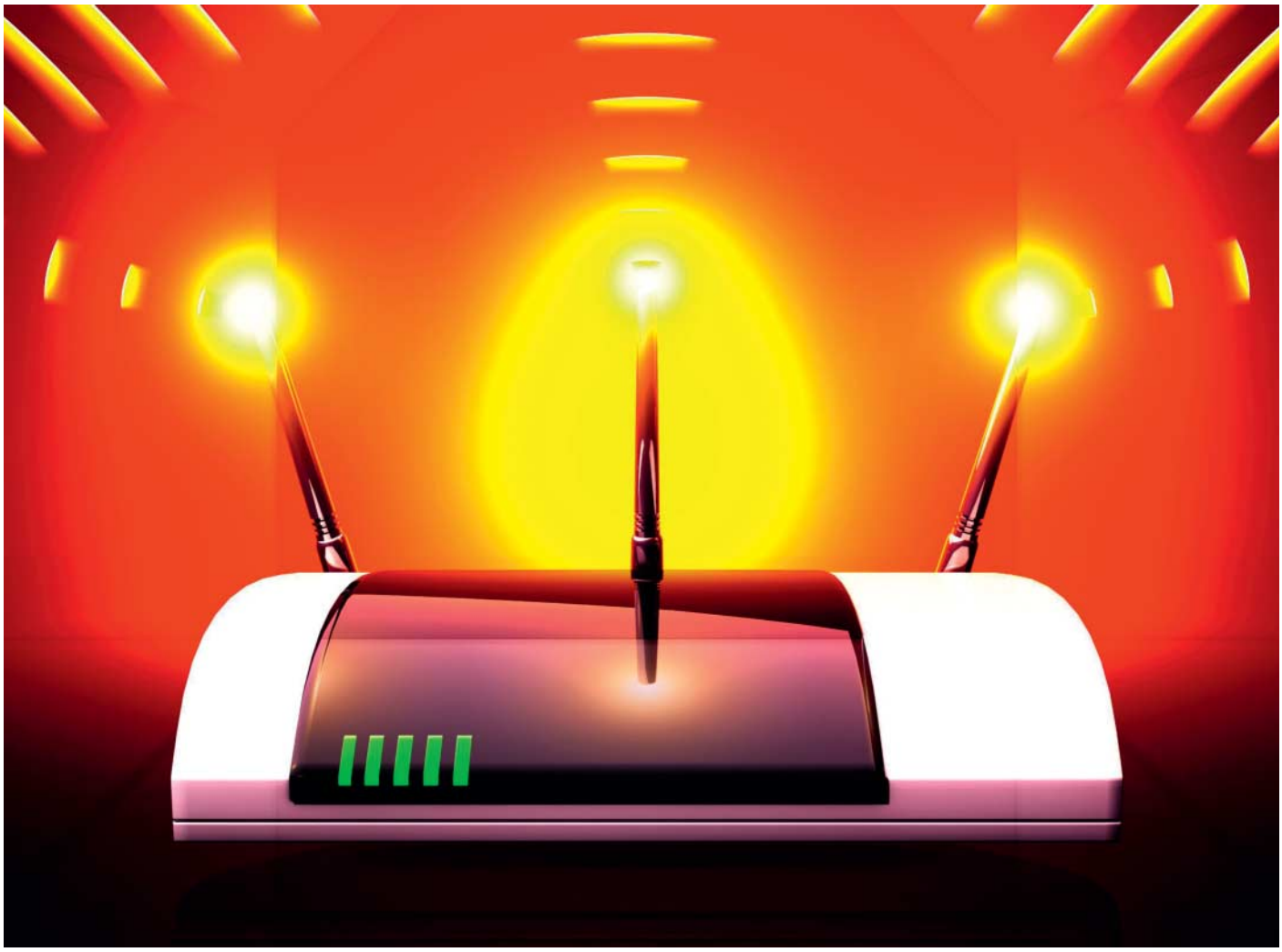

WLAN ist angeKRACKt

WPA2-Lücke KRACK analysiert und eingeschätzt

Der KRACK-Angriff ist fatal, weil er im Grunde alle Geräte mit WLAN-Chip betrifft. Dabei sollte man aber nicht den Kopf verlieren: Eine Attacke ist nicht ohne Weiteres möglich, zudem sind viele Inhalte im Internet zusätzlich geschützt.

Von Dennis Schirrmacher und Jürgen Schmidt

Mitte Oktober versetzten zwei Forscher der belgischen Universität Leuven zunächst die Security-Gemeinde und danach fast die ganze Welt in einen Schockzustand. Mathy Vanhoef und Frank Piessens demonstrierten, dass die eigentlich als sehr sicher erachtete Funknetz-Verschlüsselung WPA2 keineswegs unangreifbar ist.

Sie demonstrierten, dass sie in WLANs eigentlich gesichert übertragene Daten mitlesen können. Das kann zum Diebstahl von wichtigen Daten und sogar zur Übernahme von Verbindungen zwischen zwei Geräten – etwa einem Browser und einem Web-Server – führen. Das WLAN-Passwort können sie dabei jedoch nicht knacken. Genauso wenig können Angreifer einen Router via KRACK übernehmen.

Das Prekäre an dem KRACK, kurz für „Key Reinstallation AttaCK“, getauften Angriff ist, dass er nicht auf einem einfachen Programmierfehler eines Herstellers beruht, sondern auf einem grundsätzlichen Problem des WPA2-Standards. Das betrifft sowohl den Einsatz in Heim- als auch in Firmennetzen inklusive AES-CCMP, WPA-TPKIP und GCMP.

Betroffen: alles, was funkt

So sind denn auch nicht nur einzelne Geräte-Typen anfällig, sondern nahezu alles, was WLAN einsetzt, vom Smartphone über IoT-Geräte bis hin zu Notebooks und Routern. Wie stark sich die Probleme konkret auswirken – sprich: wie viel Gefahr davon ausgeht, hängt davon ab, wie eng sich der Hersteller der WLAN-Treiber an die WPA2-Spezifikation gehalten hat.

AVM nimmt für sich in Anspruch, in ihren Routern wie der Fritzbox die angreifbaren Teile des Protokolls gar nicht umzusetzen. Microsoft und Apple bescheinigen die Forscher, dass diese sich bei Windows und iOS gewisse Freiheiten herausgenommen haben, die dazu führen, dass Windows-PCs und iOS-Geräte nur sehr eingeschränkt angreifbar sind.

Den sprichwörtlichen Vogel abgeschossen haben die Entwickler des WPA-Supplicant-Treibers, der bei Linux und somit auch auf vielen Android-Geräten zum Einsatz kommt. Dem wiesen die Forscher nach, dass die Geräte als Folge ihres Key-Reinstallation-Angriffs mit einem Schlüssel mit dem Wert 0 arbeiten – also praktisch unverschlüsselte Daten über den Äther schicken. Rund 41 Prozent aller Android-Geräte sind den Sicherheitsforschern zufolge für diese „besonders verheerende Variante“ ihres Angriffs anfällig.

Schlimm, aber …

Das alles klingt zunächst sehr dramatisch. Der erste Schock legt sich bei genauerer Betrachtung zumindest ein wenig. Denn letztlich reduziert KRACK die Sicherheit nur auf die eines offenen Funknetzes an öffentlichen Hotspots. Außerdem müssen sich die Angreifer in Funkreichweite, also in unmittelbarer Nähe des abzuhörenden WLAN befinden, was das massenhafte Ausnutzen der Schwachstelle bei Heimanwendern eher unwahrscheinlich macht. Gefährdet sind vor allem Firmennetze, bei denen man sich ohnehin Gedanken über gezielte Angriffe etwa zur Industrie-Spionage machen muss.

Bei wirklich wichtigen Dingen wie dem Online-Banking oder Login-Vorgängen spielt die WLAN-Verschlüsselung ohnehin keine tragende Rolle. Die gehen nämlich davon aus, dass man dem benutzten Netz nicht vertrauen kann und sichern Daten deshalb mit Transportverschlüsselung. Dieses TLS äußert sich dann zum Beispiel als grünes Schloss im Browser und https-Vorsatz in der Web-Adresse. Alternativ kann man auch eine VPN-Verbindung einsetzen, um sich vor KRACK zu schützen. TLS und auch Ende-zu-Ende-Verschlüsselung wie sie etwa WhatsApp, Signal, Threema und PGP umsetzen, sind von KRACK nicht betroffen und bieten ausreichenden Schutz. Außerdem versichert die Wi-Fi Alliance, dass es bislang keine Beweise für ein Ausnutzen der Schwachstellen gibt.

Erste Patches verfügbar

Trotzdem darf man das Sicherheitsproblem nicht verharmlosen. Die betroffenen Geräte sollten schnellstmöglich mit Updates versorgt werden. Damit man wirklich sicher ist, muss man Clients und Router aktualisieren. Mittlerweile sind schon viele Sicherheits-Updates erschienen. Etwa Microsoft hat Windows bereits vor Bekanntwerden von Details zu KRACK am Patchday im Oktober abgesichert. Auch viele Linux-Distributionen wie Ubuntu sind mittlerweile mit einer reparierten WPA-Supplicant-Version ausgestattet. Apple hat bereits Fixes in diverse iOS-Beta-Versionen integriert; die Versionen für alle sollen folgen. Google hat die Sicherheits-Updates bisher nur angekündigt. Auch Router-Hersteller wie D-Link wollen erst noch liefern. Unter ct.de/y2wb finden Sie eine aktuelle Liste mit einer Übersicht zu Hersteller-Updates und Stellungnahmen.

Wer sich darüber hinaus schützen will, hat nur wenig Möglichkeiten. Das Wichtigste ist, verstärkt auf die ohnehin empfehlenswerte TLS-Verschlüsselung, also bei Web-Seiten auf das „https“ in der Adressleiste, zu achten. Noch mehr Schutz bieten Applikationen wie WhatsApp, Signal, Threema oder PGP, die auf Ende-zu-Ende-Verschlüsselung setzen. Die Verschlüsselung des WLAN von WPA2 auf WPA oder sogar WEP zu wechseln ist keine Option. WEP gilt schon lange als geknackt. Unter WPA gilt die KRACK-Attacke als noch verheerender und Angreifer sollen in diesem Fall sogar Daten manipulieren und so etwa Schadcode in den Datenverkehr einschmuggeln können. Wer es ganz ernst nimmt mit der Sicherheit, folgt der Empfehlung des BSI und verzichtet darauf, Dinge wie Online-Banking und -Shopping im WLAN zu machen. Die Sicherheitsbehörde empfiehlt, dafür wieder ein Netzwerkkabel in sein Notebook zu stecken. Das erscheint uns jedoch angesichts der Tatsache, dass es bisher keine realen KRACK-Angriffe gibt und sich diese nicht auf die TLS-Verschlüsselung auswirken, etwas übertrieben. *(des@ct.de)* c't

Weitere Infos zu KRACK und Updates:
ct.de/y2wb

So funktioniert der KRACK-Angriff

Die WPA2-Verschlüsselung beruht auf einer sehr einfachen logischen Operation auf Bit-Ebene namens XOR. Das ist ein striktes „Entweder-oder“. Es ergibt 1 (wahr), wenn genau eines der beiden Bits 1 ist (also bei 0x1 oder 1x0), sonst ergibt es 0 (0x0 und 1x1).

XOR hat aber eine bekannte Schwäche: Wer zwei verschlüsselte Botschaften mitlesen kann, die mit dem gleichen Schlüssel XOR-chiffriert wurden, kann daraus in aller Regel recht einfach Klartext errechnen. Man darf also bei XOR die Schlüssel immer nur ein einziges Mal verwenden.

Das wussten natürlich auch die Architekten von WPA2. Sie haben deshalb dafür gesorgt, dass die eingesetzten Schlüssel aus einer sogenannten Nonce abgeleitet werden. Das steht für „Number used ONCE“. In der Praxis besagt der Standard, dass WPA2-Clients die Nonce ständig hochzählen und somit sicherstellen, dass nie zweimal die gleiche Nonce zum Einsatz kommt. WPA2 hat die XOR-Klippe scheinbar umschifft.

Diese Rechnung wurde jedoch ohne die trickreichen Forscher aus Belgien gemacht. Deren Angriff beruht darauf, dass die WLAN-Geräte ihre Nonces austauschen müssen, damit beide den gleichen Schlüssel verwenden. Dieser Austausch ist natürlich gesichert und lässt sich auch nicht knacken. Aber der Angreifer kann in den Nonce-Austausch im Funknetz eingreifen und dafür sorgen, dass Teile davon nicht beim Empfänger ankommen.

Konkret fangen die KRACKer beispielsweise eine letzte Empfangsbestätigung des WLAN-Clients ab, bevor sie den WLAN-Router erreicht. Der WLAN-Client bekommt davon nichts mit und verschlüsselt bereits munter Daten. Nach dem Verstreichen einer bestimmten Frist schickt der Router das scheinbar verloren gegangene Paket erneut – und diesmal lassen es die Angreifer durch. Der Client merkt, dass er voreilig war und macht einen Reset – und führt die namensgebende Key Reinstallation durch. In der Folge verschlüsselt der Client Daten mit der gleichen Nonce wie beim ersten Mal: Die Angreifer haben gewonnen.