WLAN/WPA2-Lücke

Vor kurzem wurde von zwei belgischen Forschern ein Problem mit der **WLAN-Verschlüsselung WPA2** bekannt gemacht. Sie haben sicherlich in den Medien bereits darüber erfahren.

In diesem Zusammenhang möchte ich Ihnen *im ersten Teil* ein paar Fakten zu dem Problem zusammenstellen und Ihnen Handlungsempfehlungen geben.
Im zweiten Teil finden sich weitergehende technische Hintergründe und Vorgehensweisen für bestimmte Konstellationen.

Was ist bei WLAN das Problem?

- **WPA2** ist die Verschlüsselungstechnik für alle heute eingesetzten WLANs.
  Die Verschlüsselung kann gebrochen und der Datenverkehr abgehört werden.

- ***Das WLAN-Passwort kann dadurch nicht gebrochen werden. Das Passwort ist weiterhin sicher.***

- Das Problem ist im **WLAN-Standard** enthalten und betrifft **alle Geräte**.

- Das Problem kann durch einen Software-Update behoben werden, manche Systeme und Geräte *sind bereits repariert*.

- Damit Angriffe nicht mehr möglich sind, müssen **das Endgerät und zusätzlich der WLAN-Accespoint** mit einem Update versorgt werden.

Was bedeutet das für den Anwender?

Sie können in einem verschlüsselten WLAN nicht mehr auf Vertraulichkeit oder auf Schutz gegenüber Angriffen vertrauen. Auch ein verschlüsseltes WLAN ist nicht besser als ein öffentlicher Hotspot ohne Verschlüsselung.

Wie verhalte ich mich im Privatbereich?

Im privaten Umfeld wird es wahrscheinlich größere Probleme geben, sofern Sie zuhause auf eine umfangreiche WLAN-Nutzung setzen. Die Anwendungen und die spezifischen Probleme sind sehr vielfältig, daher hier nur kurz ein paar Hinweise:

- Das Surfen im Internet, Online-Banking und Einkaufen bei den meisten Shops ist unproblematisch, sofern die Verbindungen mit **https://** abgesichert sind.
  Das gilt auch für Tablets und Smartphones.

- Viele im Privatbereich eingesetzte Geräte werden erst spät oder niemals einen Software-Update erhalten. Das gilt besonders für viele Billig-Tablets und Smartphones.
  Bitte beobachten Sie hier die Herstellerankündigungen.
  Achtung: Linux-basierte Endgeräte und Android-Geräte sind besonders gefährdet.

- **WLAN-Router im Heim-Umfeld** sind **kritisch**, wenn sie Client-Funktionen nutzen, z.B. wenn **WLAN-Repeater-Funktionen** eingeschaltet sind. Schalten Sie diese Funktionen aus, bis Sie einen Sicherheits-Update verfügbar haben.

- Besonders problematisch sind **WLAN-fähige Kleingeräte** (Internet of Things, IoT).
  Dazu gehören insbesondere WLAN-gesteuerte Lampen, Heizungsanlagen und Thermostate, Staubsauger, Fernsehapparate sowie Schließsysteme und Alarmanlagen.
  Diese Geräte sollten Sie vorsichtshalber außer Betrieb nehmen, bis Sie Ihren Haushalt vollständig mit Sicherheitsupdates versorgt haben.

Sofern Sie mit dem Betrieb von WLANs betraut oder allgemein technisch interessiert sind, finden Sie im Folgenden ein paar technische Details über das Problem und weitere Hinweise.

Was ist das genaue Problem?

WLAN mit WPA2-Verschlüsselung nutzt für jedes Endgerät einen eigenen Schlüssel zur Verschlüsselung. Dieser *Sitzungs-Schlüssel* wird zu Beginn in einem *Handshake-Verfahren* zwischen WLAN-Accesspoint und Endgerät ausgetauscht. Die Schwachstelle basiert darauf, dass durch Manipulation von Handshake-Daten (Fälschen der Pakete durch einen Angreifer) der ausgewählte Sitzungsschlüssel **beim Client** *mehrfach neu installiert* wird und damit Schutzmechanismen gegen eine Entschlüsselungsattacke (Nonce, Replay Counter) zurückgesetzt werden.

Linux-Systeme sowie Android (ab Version 6) können durch die Attacke dazu gebracht werden, einen „NULL"-Key zu nutzen, was die Entschlüsselung von Datenpaketen zusätzlich vereinfacht.

Die Angriffe richten sich gegen verwundbare Client-Geräte, WLAN-Access-Points sind nicht Ziel dieser Attacken. Gerade im IoT-Umfeld gibt es jedoch besondere Geräte, die AP-Funktionen und Client-Funktionen kombinieren. Auch wenn diese als WLAN-AP betrieben werden, können sie über aktivierte Client-Funktionen angegriffen werden.

Die Angriffe können nur während eines Handshakes durchgeführt werden. Bei ständig aktiven WLAN-Sitzungen wird i.d.R. stündlich ein Handshake für den Austausch des Sitzungsschlüssels durchgeführt. Zu diesen Momenten kann der Angriff durchgeführt werden.

Für Broadcom-Chips in WLAN-APs gibt e seine besondere Form der Attacke, diese können zu einem vorzeitigen Austausch des Sitzungsschlüssels und dem dazugehörigen Handshake gezwungen werden. Der Angriff ist daher zu beliebigen Zeitpunkten durchführbar.

Gibt es weitere Informationen?

Über die üblichen Kanäle erhalten Sie Informationen zu der aktuellen Gefahr und zu Angriffsmöglichkeiten oder verfügbare Patches. Insbesondere das US CERT liefert Informationen über betroffenen Systeme und aktuelle Patch-Stände.
Bitte verfolgen Sie Updates der Seite **https://www.kb.cert.org/vuls/id/228519.**

Genauere Informationen finden Sie auf der Webseite der Forscher **https://www.krackattacks.com/.**
Bei Interesse empfehle ich die Lektüre des wissenschaftlichen Papiers
https://papers.mathyvanhoef.com/ccs2017.pdf.

Für die Angriffe gibt es bisher kein automatisiertes Werkzeug. Es ist aber damit zu rechnen, dass innerhalb weniger Wochen ein auch für Nicht-Fachleute nutzbares Werkzeug zur Verfügung steht. Die Gefahr ist also real.