esatus AG
Enforcing Information Security

WPA2 geKRACKt –
Status, Gegenmaßnahmen, Perspektiven

Eine als „KRACK" bezeichnete Sicherheitslücke in dem weit verbreiteten WLAN Sicherheitsstandard WPA2 erlaubt es einem Angreifer, unter gewissen Umständen die Kommunikation zwischen einem Endgerät – Smartphone, Notebook, Webcam, TV, etc. – und einem Access Point abzufangen, zu entschlüsseln und im schlimmsten Fall zu manipulieren. Dieses Whitepaper liefert eine Übersicht über die gefundene Sicherheitslücke und mögliche Angriffsszenarien, beschreibt wer und welche Geräte betroffen sind und zeigt auf, welche Gegenmaßnahmen kurzfristig umgesetzt werden können, bis einzelne Hersteller Updates für ihre Software und Geräte liefern.

Begriffe: KRACK – Key Reinstallation Attack | WPA2 – Wi-Fi Protected Access 2 | WLAN – Wireless Local Area Network | VPN – Virtual Private Network

WPA2 und der KRACK

Der Sicherheitsstandard WPA2 gilt seit vielen Jahren als ungebrochen und konnte diversen Sicherheitsüberprüfungen standhalten. Dies ist jetzt Vergangenheit: Kürzlich wurden kritische Schwachstellen durch den Sicherheitsforscher Mathy Vanhoef von der Katholieke Universiteit Leuven (KU Leuven) in zahlreichen Implementierungen des Standards identifiziert. Getauft wurde der Angriff „KRACK" – ein Akronym für „**K**ey **R**einstallation **A**tta**ck**".

Die Lücken erlauben es, je nach verwendetem Gerät und softwaretechnischer Implementierung, die Kommunikation zwischen Client und Access Point mitzuschneiden oder zu manipulieren. Der Angriff beruht auf einem Fehler in der Aushandlung von Session Keys während des 4-Wege-Handshakes. Hierbei kann durch erneutes Senden des dritten Schrittes der Client dazu gebracht werden, die bereits ausgehandelten Session Keys zu überschreiben. Durch Ausnutzung der Sicherheitslücken ist es **nicht** möglich an den verwendeten WLAN Schlüssel zu gelangen. Einzelheiten über die Lücke können Vanhoefs informativer Webseite https://www.krackattacks.com und dem zugrundeliegenden Paper entnommen werden.

Wer und was ist betroffen?

Theoretisch sind alle WLAN-fähigen Geräte betroffen, da die gefundene Lücke in der clientseitigen Implementierung, d. h. in der Software des Endgerätes, liegt. In der Praxis muss jeder Hersteller überprüfen, ob die eigene Implementierung des WLAN-Standards für den Angriff anfällig ist und im Anschluss Patches, d. h. Softwareaktualisierungen für die entsprechenden Module des Betriebssystems, bereitstellen.

Für einen erfolgreichen Angriff sind drei Voraussetzungen unabdingbar:

1. Die Implementierung des WLAN-Standards muss anfällig für die gefundene Sicherheitslücke sein.
2. Es muss eine aktive WLAN-Verbindung zwischen einem Client und einem Access Point bestehen.
3. Der Angreifer muss sich in Funkreichweite zum Client und Access Point befinden.

Ist das WLAN am Client ausgeschaltet oder besteht keine Verbindung zu einem Access Point, so ist das Gerät nicht anfällig für den Angriff.

Angriffe sind sowohl gegen WPA (WPA1) als auch WPA2 erfolgreich. Hierbei hängt der Erfolg eines Angriffs nicht davon ab, ob ein Preshared Key (PSK) oder die im Enterprise-Umfeld verbreitete Variante mit RADIUS-Authentifizierung zum Einsatz kommt. Weiterhin sind alle kryptographischen Verfahren, d. h. WPA-TKIP, AES-CCMP und GCMP, in unterschiedlichem Ausmaß von dem Angriffsvektor betroffen.

Besonders gefährdet sind laut Vanhoef Geräte mit Android-Betriebssystem ab Version 6.0 und diverse Linux-Distributionen, da diese meist als WLAN-Client-Software auf „wpa_supplicant" Version 2.4 und höher setzen. In Version 2.4 ist ein erfolgreicher Angriff besonders einfach zu bewerkstelligen und erlaubt einem Angreifer weitreichende Manipulationsmöglichkeiten.

Die Implementierungen in Windows und Apples iOS sind ebenfalls, wenn auch unterschiedlich stark, anfällig für den Angriff. Von diesen und weiteren Herstellern wurden als Reaktion auf die Veröffentlichung bereits Updates öffentlich verfügbar gemacht.

Gegenmaßnahmen

Um möglichen Angriffen kurzfristig entgegenzuwirken gibt es mehrere Sofortmaßnahmen, die der Anwender in Eigenverantwortung praktizieren kann. Diese sind solange erforderlich, bis die einzelnen Hersteller Aktualisierungen für ihre Software und Geräte bereitstellen.

Auf sichere Verbindungen achten! In erster Linie ist darauf zu achten, dass nur noch sichere Verbindungen benutzt werden, wenn das WLAN genutzt wird. Wichtig ist, dass beim Surfen alle Verbindungen mittels „https“ gesichert sind. Selbst wenn ein Angreifer die Kommunikation durch Ausnutzung der Sicherheitslücke mitlesen kann, ist er nicht in der Lage die gesicherte https-Verbindung zu entschlüsseln. Treten jedoch Zertifikatsprobleme auf oder wird die Verbindung plötzlich nicht mehr über https geleitet, sollte man sofort das WLAN deaktivieren und einen anderen Kommunikationsweg nutzen, da dies Hinweise auf einen möglichen Angriff sind.

Zusätzliche Verschlüsselung verwenden! Eine weit sicherere Gegenmaßnahme, die sowohl im geschäftlichen als auch privaten Bereich genutzt werden kann und definitiv sollte, ist die zusätzliche Verschlüsselung der Verbindung mittels VPN. Virtual Private Networks (VPN) verschlüsseln die gesamte Kommunikation zwischen einem Endgerät und einer vertrauenswürdigen Gegenstelle, welche die Verbindungen ins Internet weiterleitet. Selbst wenn die Verbindung über WLAN durch einen Angreifer mitgehört werden kann, so ist eine Entschlüsselung oder Manipulation der gesicherten VPN-Verbindung nur schwer möglich. Im geschäftlichen Umfeld setzen bereits viele Unternehmen auf VPN. Dieser Technologie sollte im Zuge der gefundenen Sicherheitslücke nochmals mehr Aufmerksamkeit gewidmet werden, sodass alle Mitarbeiter die Möglichkeit einer sicheren betrieblichen Kommunikation erhalten und ihr Bewusstsein dafür geschärft wird. Auch im privaten Umfeld hat VPN immer stärker Einzug gehalten. Zahlreiche Hersteller von Routern, die meist einen Access Point integriert haben, bieten bereits einfache Konfigurationsmöglichkeiten über die grafische Benutzeroberfläche an, um auch im heimischen Netzwerk sowie von unterwegs VPN einsetzen zu können. Wichtig hierbei ist darauf zu achten, nur vertrauenswürdige, d. h. vom Routerhersteller empfohlene oder bereitgestellte, VPN-Software bzw. -Apps einzusetzen.

WLAN-Kommunikation vermeiden! Eine andere, oft weniger praktikable Lösung ist, verstärkt auf andere Kommunikationswege als WLAN zu setzen. Bei Smartphones könnte hierbei verstärkt auf Mobilfunk zurückgegriffen werden und bei Notebooks auf eine kabelgebundene Anbindung.

Perspektiven

Trotz der genannten kurzfristigen Gegenmaßnahmen ist es unerlässlich Updates vom Hersteller einzuspielen, sobald sie verfügbar sind, oder von der automatischen Updatefunktion Gebrauch zu machen. Besonderes Augenmerk sollte auf Geräte gelegt werden, die dauerhaft über WLAN verbunden sind und solche, die selten oder gar keine Updates erhalten. Starkes Gefährdungspotential haben eingebettete Systeme und IoT-Geräte, da solche in vielen Fällen gar keine oder mit deutlicher Verspätung Updates erhalten und somit unter Umständen dauerhaft anfällig für den Angriff bleiben. Hier sollte der Hersteller kontaktiert werden, um Informationen über die Anfälligkeit der Geräte zu erfragen und mögliche Updates schnell zu erhalten.

Fazit

Der WPA2 Sicherheitsstandard ist nach wie vor sicher und wurde nicht gebrochen. Die gefundenen Sicherheitslücken liegen einzig in der jeweiligen clientseitigen Implementierung des Standards. Eine Aktualisierung des Access Points kann einen Angriff nicht abwenden. Die genannten Gegenmaßnahmen bieten einen kurzfristigen Schutz, entlasten jedoch nicht die Hersteller von ihrer Verantwortung, für ihre Software und Geräte Updates zu liefern.