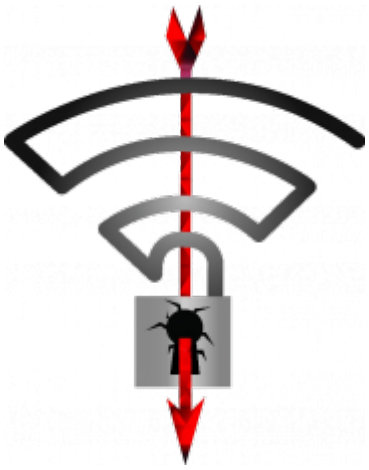
Ist WLAN jetzt unnutzbar? Brauchen wir jetzt wieder überall LAN-Kabel?



Seit Mitte Oktober geht durch die IT-Medien eine neue Attacke auf den derzeit gültigen und überall genutzten WLAN-Standard WPA2. Dabei ist es unerheblich, ob es sich um die Betriebssysteme Linux, Windows, Android oder iOS handelt. KRACK ist dabei die Abkürzung für „Key Reinstallation AttaCK“ und ist eine Angriffsmethode auf WLAN-Verbindungen, die ein IT Spezialist aus Belgien entwickelt hat.

Die technischen Details

Kurz erklärt geht es darum, dass WPA2 zum Verschlüsseln der Daten einen XOR-Algorithmus verwendet. Dieser ist 100% sicher, solange der Verschlüsselungsschlüssel niemals doppelt verwendet wird. Genau hier setzt KRACK an. Indem es einige WLAN-Pakete blockiert, wird ein WLAN-Client gezwungen, vermeintlich verloren gegangene Pakete nochmals zu senden. Hierbei nutzt er den gleichen Schlüssel! Damit ist die XOR-Verschlüsselung nutzlos und auch weitere Pakete können mit geringem Aufwand entschlüsselt werden.

Wer die vollen technischen Details wissen möchte - diese sind hier zu finden:

https://papers.mathyvanhoef.com/ccs2017.pdf

Patchen der Geräte

Prinzipiell kann man nun davon ausgehen, dass WLAN-Verbindungen komplett unsicher sind - zumindest bis alle Geräte gepatcht sind. Größtes Problem hierbei: Viele Hersteller von Geräten wie Routern oder Access Points werden wahrscheinlich keine Updates veröffentlichen! Glücklicherweise kann das Problem einfach gefixt werden und es muss kein komplett neuer Standard entwickelt werden.

Welche Netzwerke sind unsicher?

Jeglicher Netzwerkverkehr, der nicht nochmal extra verschlüsselt wird, ist nun mitlesbar. Dabei reicht es, dass der Angreifer sich in Reichweite des Funknetzwerkes befindet. Man muss also davon ausgehen, dass ein Angreifer mit einer entsprechenden Antenne das WLAN auch außerhalb des Firmengeländes empfangen kann.

Sicher ist heute sowieso schon verschlüsselter Netzwerkverkehr. So z.B. alle verschlüsselten Verbindungen über https - welche dank TLS Verschlüsselung weiterhin sicher sind.

Gleichzeitig bieten sich für einen Angreifer, der einmal im Firmennetzwerk ist, erhebliche Möglichkeiten, Sicherheitslücken auszunutzen und Kennwörter abzufangen. Es ist quasi unmöglich sicherzustellen, dass bestimmte Passwörter (z.B. Netzwerkfreigaben unter Windows, Anmeldevorgänge über RDP, Datentransfer über FTP etc.) nie über ein WLAN transferiert werden. Notfalls sollten VPNs genutzt werden.

Weiteres Vorgehen

Das weitere Vorgehen ist nun abhängig von der persönlichen Gefährdungssituation und muss individuell eingeschätzt werden. Tendenziell sollte man aber WLANs, bei denen nicht alle Geräte mit einem Sicherheitsupdate versorgt worden sind, als unsicher ansehen. Die Hersteller geben detaillierte Informationen, welche Geräte potenziell betroffen sind, unter welchen Konfigurationen und ab wann das Problem gepatcht wurde. Mittlerweile sind die meisten Betriebssysteme schon gepatcht.

Kunden, die unsere WLAN-Produkte der Firma Ruckus verwenden, sind nur anfällig, wenn der Modus Mesh, Point-to-point oder Point-to-multipoint verwendet wird. Wenn Sie einen Datenbankserver unter RHEL oder SLES verwenden, ist dieser normalerweise nicht anfällig, da Datenbankserver kein WLAN verwenden.

Mehr Informationen zur Attacke auf der Website von Mathy Vanhoef:

https://www.krackattacks.com/