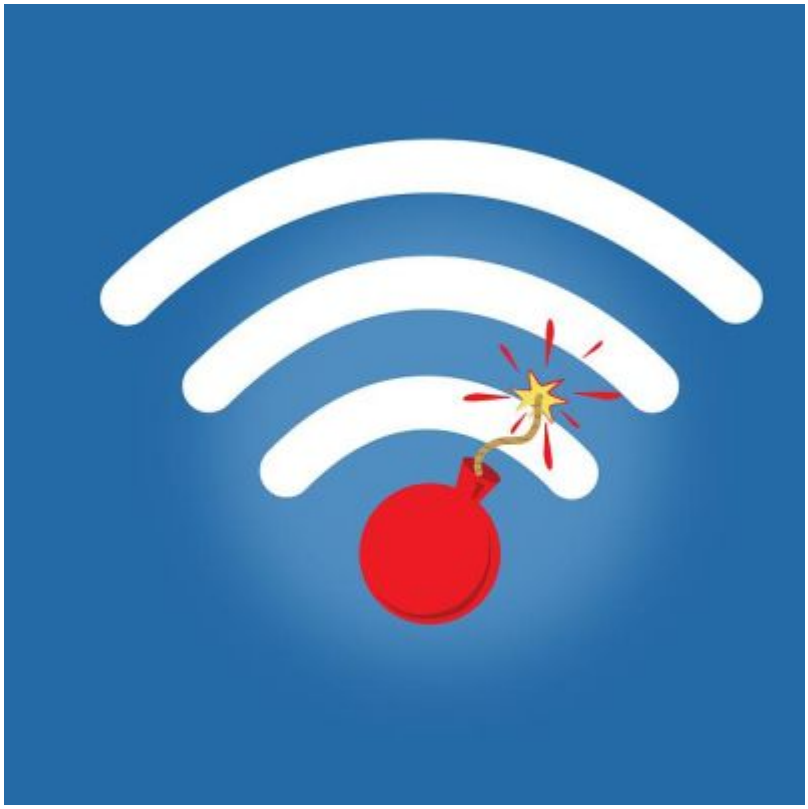
Krack Attacke oder die Wlan-Sicherheitslücke

24.10.2017, 10:26 | IT, New Media & Software

Pressemitteilung von: *Mahr EDV*



In der letzten Woche sorgte das Schlagwort von der „Krack Attacke“ für einige Irritationen unter jenen, die mit der IT-Sicherheit vor allem von Unternehmen beschäftigt sind. Auch in vielen Unternehmen selbst löste die Meldung, dass eine Schwäche im WPA2-Standard alle Wlan-fähigen Geräte betreffe, und es Cyber-Kriminellen so ermöglichen würde, zuverlässig verschlüsselt geglaubte Daten mitzulesen, beträchtliche Verunsicherungen aus.

Inzwischen mehren sich zwar die Stimmen, die das alles für nur halb so wild erklären – „Krack klingt schlimmer, als es ist“, titelt etwa Zeit-Online am 16.10.2017 –, doch sollte man sich über akuten Handlungsbedarf, wie Fabian Mahr, Geschäftsführer des IT-Dienstleisters Mahr EDV

https://www.mahr-edv.de

sagt, nicht hinwegtäuschen: „Dass sich die mit Krack verbundenen Probleme erfreulicher Weise lösen lassen, heißt nicht, dass sie nicht ernst zu nehmen wären.“

Krack Attacke

Übereinstimmenden Medienberichten zufolge haben Forscher Sicherheitsschwächen im Verschlüsselungsprotokoll WPA2 entdeckt. Lange Zeit galt WPA2 bei Verwendung eines langen und komplizierten Passwortes im Unterschied zu seinen Vorläufern WEP und WPA als absolut sicher. Mittels eines Hacks, den sie „Krack“ nennen, was für key reinstallation attacks steht, haben die Forscher der KU Leuven jedoch vergangene Woche einen grundsätzlichen „Systemfehler“ im Verschlüsselungsprotokoll WPA2 bloßgelegt.

Folgen der WPA2-Sicherheitslücke

Der Fehler macht es potentiellen Angreifern in Reichweite des Netzwerkes möglich, Daten auf jeden Fall mitzulesen und unter Umständen – je nach den Einstellungen des Netzwerkes – sogar zu manipulieren. Theoretisch ist damit jede Wlan-Verbindung samt der angeschlossenen Geräte (Router, Desktop-Rechner, Notebooks, Smartphones etc.) gefährdet.

Gegenmaßnahmen

Wie die Wi-Fi Alliance informiert,

https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-security-update

werden die Hersteller der gängigen Betriebssysteme zeitnah mit der Veröffentlichung entsprechender Updates reagieren. Diese beinhalten sogenannte Patches, mittels derer sich die Wlan-Sicherheitslücke schließen lässt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät daher,

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/WPA2Verschuesselung_16102017.html

„WLAN-Netzwerke bis zur Verfügbarkeit von Sicherheits-Updates nicht für Online-Transaktionen wie Online Banking und Online Shopping oder zur Übertragung anderer sensitiver Daten zu nutzen."

Wichtige Tipps für Unternehmen

Gerade Unternehmen, die den Transfer relevanter Daten über Wlan-Verbindungen organisieren, mahnt Mahr EDV zu äußerster Sorgfalt. Nicht nur wären die gesamte IT-Architektur in Hinblick auf Krack zu überprüfen und die passenden Updates, sobald verfügbar, zu installieren sowie sich anschließend über den Erfolg der Maßnahmen zu vergewissern. Ist es üblich, dass sich Mitarbeiter mit betrieblichen als auch privaten mobilen Endgeräten ins Firmen-Wlan-Netz einwählen, so sollte sichergestellt werden, dass auch diese ausnahmslos den entsprechenden Updates unterzogen werden.

Portrait

Das IT Systemhaus Mahr EDV sorgt seit 18 Jahren mit umfassenden IT-Dienstleistungen dafür, dass kleine und mittelständische Unternehmen vorrangig in Berlin, Potsdam, Düsseldorf und Umgebung störungsfrei arbeiten und sich auf ihre Kerngeschäfte konzentrieren können. Zuverlässig stellen wir rund um die Uhr an 365 Tagen im Jahr eine Regelreaktionszeit von weniger als zwei Stunden sicher.

News-ID: 976041 • Views: 463 (Stand: 02.07.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/976041/Krack-Attacke-oder-die-Wlan-Sicherheitsluecke.html