Sicherheitslücke in WPA2

Bedroht „Hole 196" die WLAN-Security?

WPA2 gilt als sichere Verschlüsselung des Funkverkehrs für WLANs. Für Aufregung in Fachkreisen sorgte darum im Sommer 2010 die Nachricht, WPA2 sei geknackt. Was ist dran an der Ankündigung, die unter dem Schlagwort „Hole 196" die Runde macht? Lesen Sie dazu die Einschätzung der IT-Security-Experten Christoph Bott und Sebastian Schreiber.

Ursächlich für das jüngst bekannt gewordene Angriffsszenario ist eine Eigenschaft des WLAN-Designs, die auf Seite 196 (daher der Name) des IEEE-802.11-2007-Standards beschrieben ist und sich nun als Schwäche erweist. Praktisch bedeutet dies, dass ein bereits am WLAN angemeldeter Nutzer durch Einsatz eines einfachen Programmcodes den Datenverkehr eines fremden Clients (z. B. des Laptops oder WLAN-Handys eines anderen Nutzers) über den Access-Point und dann das eigene System umleiten kann. Er kann dabei eine Umchiffrierung der Nutzdaten durch den Accesspoint bewirken, sodass diese mit dem eigenen Sitzungsschlüssel dechiffriert und infolgedessen von ihm eingesehen und/oder manipuliert werden können. Konsequenz: Zur WLAN-Nutzung autorisierte Personen (Mitarbeiter im Unternehmen, Gäste mit Zugang) können außer auf ihren eigenen Datenverkehr auch unbefugten Zugriff auf den sonstigen Datenverkehr im WLAN erlangen.

Die Frage nach der Auswirkung des im Juli dieses Jahres veröffentlichten Hole 196 wird in Expertenkreisen kontrovers diskutiert.

Schreiber: „Sicherheit bestimmt sich immer aus der Gesamtheit aller Maßnahmen."

Festzuhalten ist, dass Horrormeldungen wie „WPA2 ist geknackt" nur Teilwahrheiten propagieren und ein stark verzerrtes Bild des tatsächlichen Ausmaßes der entdeckten Schwachstelle erzeugen.

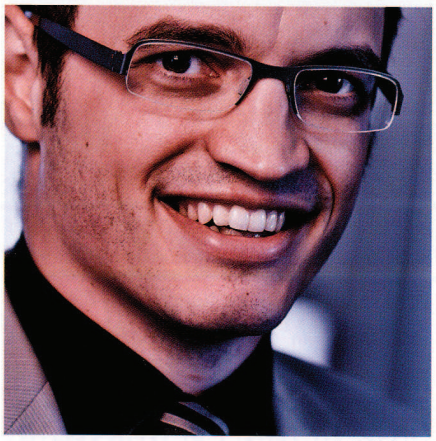
Nur Angriffe von innen möglich

Betrachtet man allgemein die Sicherheit von Netzwerken, so rücken drei wesentliche Schutzziele in den Mittelpunkt: die Zugangskontrolle (Autorisierung) legitimer Nutzer sowie die Integrität und die Vertraulichkeit der übermittelten Daten. Hole 196 gefährdet hierbei lediglich die beiden letztgenannten Aspekte: Ein unbefugter Zugriff auf WPA2-geschützte WLANs wird durch diese Schwachstelle nicht ermöglicht. Richtig jedoch ist, dass legitimierte Benutzer eines WPA2-WLAN durch Ausnutzung dieser Schwachstelle unter Umständen die beiden anderen Schutzziele, also Vertraulichkeit und Integrität der von anderen Benutzern übermittelten Daten angreifen können.

Die Bewertung hängt nun vom Blickwinkel ab: Unter den Entwicklern des WPA2-Standards dürfte allein die Tatsache, dass ein Designfehler zu einer Reduzierung des angestrebten Sicherheitsniveaus führt, für Kopfschmerzen sorgen. Der Endanwender lernt jetzt, dass unter Umständen Sicherheitsmerkmale verloren gehen, die in einer simplifizierten Betrachtung noch nie als solche wahrgenommen wurden. Und für den Netzwerkadministrator wird klar, dass nun auch im WLAN Angriffe möglich sind, die in ähnlicher Form im drahtgebundenen Bereich seit Jahren eine Bedrohung darstellen.

Sicherheitsniveau sinkt, aber nur graduell

Faktisch sinkt das Sicherheitsniveau von



Bott: „Sensible Nutzdaten sollten zusätzlich auf Anwendungsebene verschlüsselt werden."

WPA2-WLANs durch Hole 196 in etwa auf das eines klassischen Ethernets, wobei allerdings Hole-196-basierte Angriffe im Gegensatz zu vergleichbaren Angriffen im Ethernet nicht mehr ohne Weiteres detektierbar sind. Auf der anderen Seite ermöglichen die meisten WLAN-Komponenten professioneller Netzwerkausrüster die Einschaltung zusätzlicher Schutzmaßnahmen (z. B. Verhinderung von Client-zu-Client-Kommunikation), die der durch Hole 196 bedingten Problematik entgegenwirken.

Zusammenfassend stellt Hole 196 für WLAN-Einsatzszenarien mit normalem Schutzbedarf keine ernstzunehmende Gefahr dar, solange sensible Nutzdaten zusätzlich auf Anwendungsebene verschlüsselt übermittelt werden (z. B. mittels SSL). Diese – in der Praxis oft nicht beachtete – Empfehlung gilt jedoch sowieso und uneingeschränkt auch im drahtgebundenen Netzwerk. Der Einsatz von WPA2 in hochsensiblen Bereichen wird bedingt durch Hole 196 allerdings deutlich infrage zu stellen sein.

Autoren: Christoph Bott und Sebastian Schreiber, SySS GmbH, www.syss.de