Oberhessische Presse 28.03.13

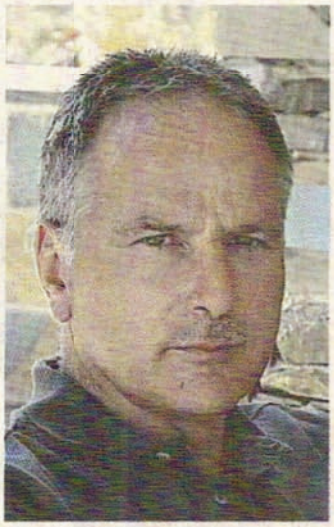
Sorglose Smartphone-Nutzer riskieren Sicherheitsproblem

Informatiker: Hochschulrechenzentrum warnt meist vergeblich

Viele Smartphone-Besitzer ignorieren Sicherheitsempfehlungen für den drahtlosen Internetzugang und nehmen dadurch Risiken in Kauf. Dies ist das Ergebnis einer Studie des Informatikers Professor Bernd Freisleben.

Marburg. Der Informatiker Professor Bernd Freisleben von der Philipps-Universität hat in einer Studie untersucht, wie sicherheitsbewusst sich Smartphone-Nutzer verhalten. Dies teilte die Marburger Uni-Pressesstelle mit. Das Fazit des Informatikers: „Durch die Verkettung von Einstellungsfehlern und unsicheren Konfigurationen setzt sich ein Großteil der Benutzer selbst unnötigen Gefahren aus", warnt Freisleben.

Lokale Funknetze (WLAN) ermöglichen eine Nutzung des Internets durch mobile Geräte wie Smartphones, Mobiltelefone und Tablets, die mit dem Betriebssystem „Android" ausgestattet sind. „Ziel der Umfrage war es, zu ermitteln, wie viele der Android-Benutzer im Uni-WLAN sich bei der Konfiguration ihres Netzzugangs an die sicheren Vorgaben des Marburger Hochschulrechenzentrums halten", erläutert Freisleben. Der Marburger Hochschullehrer ist auf mobile Internetanwendungen spezialisiert und deckte erst vor Kurzem auf, dass die Nachlässigkeit der Entwickler von Smartphone-Anwendungen, so genannter Apps, das Ausspähen von Nutzerdaten ermöglicht. An der aktuellen Umfrage nahmen 390 Android-Benutzer teil. „Nur die Installation eines passenden Zertifikats und die Einstellung verlässlicher Authentifizierungsmethoden garantieren einen sicheren Zugriff auf das WLAN-Netz", erläutert Freisleben. Das Hochschulrechenzentrum (HRZ) der Philipps-Universität empfiehlt, ein geeignetes Sicherheitszertifikat auf einem Android-Gerät zu installieren. Das Ergebnis der Studie: Lediglich zwischen 12 und 24 Prozent der Nutzer installieren das Sicherheitszertifikat, das vom HRZ zur Verfügung gestellt wird. „Nur durch dessen Verwendung ist wirksam zu verhindern, dass eine Verbindung mit betrügerischen Netzen aufgebaut wird", betont Dr. Martin Pauly vom HRZ. „Gleichzeitig ist damit die Verschlüsselung nach heutigem Kenntnisstand sicher." Gelingt ein Angriff gegen das Smartphone, weil dieser erste Schritt zu einer unsicheren Konfiguration geführt hat, so kann der Angreifer die Kommunikation mitlesen und verfälschen. somit ist er auch in der Lage, das im zweiten Schritt zu prüfende, besonders kritische Benutzer-Passwort abzuhören. „Damit erlauben sie potenziell unsichere Verbindungen", erklärt Freisleben. Auch im zweiten Schritt wählen bis zu zwei Drittel aller Benutzer eine wenig sichere oder keine spezielle Einstellung. Das alarmierende Fazit der Wissenschaftler: Über 80 Prozent der Android-Benutzer halten sich nicht an die vorgeschlagene Konfiguration des HRZ. Das Hochschulrechenzentrum stellt auf seiner Internetseite Anleitungen zur empfohlenen Konfiguration des WLAN-Zugangs für eine Vielzahl von Betriebssystemen zur Verfügung (http://www.uni-marburg.de/hrz/internet/wlan/anleitungen). Zuletzt hatte Freislebens Arbeitsgruppe Schlampereien bei den Sicherheitsvorkehrungen hunderter Smartphone-Applikationen aufgedeckt (die OP berichtete). Die Sicherheitslücken der Apps ermöglichten den Forschern, Kontodaten sowie Codes für E-Mail- und Social-Media-Dienste abzufangen. 40 bis 185 Millionen Android-Nutzer könnten von unberechtigten Zugriffen bedroht sein, mutmaßen die IT-Experten.



Der Informatiker Professor Bernd Freisleben. Privatfoto

MMA2