

Sicherheitswarnung

Sicherheit von Mobiltelefonen nach GSM-Standard

1 Sachstand

Die mobile Kommunikation auf der Basis des GSM-Standards unterliegt zahlreichen Sicherheitsrisiken. Das BSI beobachtet und analysiert neue Risiken und empfiehlt Sicherheitsmaßnahmen zur Reduzierung der Gefährdungen. Die Risiken betreffen neben der Sprachkommunikation auch alle Formen der Datenkommunikation (SMS, MMS, E-Mail etc.). Angriffspotential bieten neben den Endgeräten und ihren Betriebssystemen insbesondere die Funkschnittstellen.

Eine aktuelle Beratungsbroschüre zur IT-Sicherheit öffentlicher Mobilfunknetze sowie der zugehörigen Funkschnittstellen (GSM, GPRS, UMTS etc.) finden Sie unter:
<http://www.bsi.de/literat/doc/oefms/oefmobil.pdf>

Informationen zur IT-Sicherheit lokaler Funkschnittstellen (WLAN, Bluetooth etc.) finden Sie unter: <http://www.bsi.de/literat/doc/drahtkom/drahtkom.pdf>

Eine Broschüre zur Sicherheit mobiler Endgeräte finden Sie unter:
http://www.bsi.de/literat/doc/mobile/mobile_endgeraete.pdf

2 Gefährdungen

2.1 Gefährdungen an der Funkschnittstelle zwischen Endgerät und Mobilfunknetzen

Die GSM-Sicherheitsmechanismen bieten keinen verlässlichen Schutz der über die Luftschnittstelle übertragenen Informationen.

In GSM-Netzen muss sich das mobile Endgerät gegenüber dem Mobilfunknetz authentisieren, eine Authentisierung des Mobilfunknetzes gegenüber dem Endgerät erfolgt nicht. Diese Schwachstelle ermöglicht „Man-in-the-Middle“-Angriffe unter Verwendung sogenannter mobil einsetzbarer IMSI-Catcher, bei denen dann die GSM-Verschlüsselung deaktiviert werden kann. Hierdurch sind Vertraulichkeit und Integrität der über die GSM-Funkschnittstelle übertragenen Daten gefährdet.

Da für die Mobilkommunikation nach UMTS-Standard ein Wechsel zur Kommunikation über GSM-Infrastruktur möglich ist, stellt die Verwendung von UMTS-Endgeräten keinen hinreichenden Schutz vor solchen Angriffen auf die Luftschnittstelle dar.

Zudem gibt es dokumentierte Angriffsmethoden gegen die nach GSM-Standard eingesetzten Kryptoalgorithmen, mit denen sich passiv abgehörte Mobilfunkverbindungen entschlüsseln lassen.

Unter Einsatz entsprechender Geräte ist es einem Angreifer somit beispielsweise möglich, Gespräche abzuhören und SMS- oder E-Mail-Daten mitzulesen.

Neben dem Schutz der Vertraulichkeit gesprochener oder schriftlicher Informationen, sind personenbezogene und personenbeziehbare Daten gefährdet. Aufenthaltsorte eines Mobilfunkteilnehmers lassen sich innerhalb gewisser Grenzen bestimmen und somit Bewegungsprofile erstellen.

2.2 Gefährdungen auf Endgeräteseite

Wenn die Sicherheitsmechanismen in den Endgeräten und deren Betriebssystemen unzureichend sind, können Hardware- oder Software-Manipulationen, z. B. über die Geräte- oder SD-Karten-Schnittstellen, nicht ausgeschlossen werden. Bei erfolgreichem Angriff ist es dem Angreifer möglich, das Endgerät fernzusteuern sowie auf Kommunikationsdaten und Speicherinhalte zuzugreifen oder das Endgerät zum Abhören von Raumgesprächen zu missbrauchen.

Bei unzureichender Absicherung lokaler Funkschnittstellen wie Bluetooth oder WLAN bieten sich einem Angreifer Möglichkeiten, das Endgerät per Software zu manipulieren oder die über diese Funkschnittstellen kommunizierten Daten abzufangen.

2.3 Weitere Gefährdungen

Die sich aus der allgemeinen Nutzung des Internets resultierenden Probleme der IT-Sicherheit werden zunehmend auch bei Nutzung von mobilen Endgeräten festgestellt. Mangelnde Sensibilität der Nutzer und unsichere Konfigurationen der Geräte sind hierbei ebenso als Quellen für Gefährdungen der Informationssicherheit zu nennen.

Durch Vernetzung mobiler Endgeräte mit der behörden- bzw. firmeninternen Infrastruktur („Hausnetz“) ergibt sich ein weiteres Potenzial an Risiken. Vermeintlich lokale - auf die Endgeräte fixierte - Risiken werden bei nicht sicherer Konfiguration oder bei unsachgemäßer Nutzung zur globalen Gefährdung, die sich nicht nur auf das Hausnetz sondern auch auf das Behördennetz insgesamt auswirken kann.

2.4 Fazit

Das BSI hält handelsübliche GSM-Mobiltelefone für nicht hinreichend manipulationssicher. Das BSI betrachtet die GSM-Luftschnittstelle als nicht hinreichend abhörsicher, lokale Funkschnittstellen bieten vielfältige Möglichkeiten für Angriffe.

3 Sicherheitsmaßnahmen

Das BSI empfiehlt:

- ➔ den Umgang mit mobilen Telefonen in einer Sicherheitspolicy zu regeln, die Policy ist den Nutzern vor Gebrauch mobiler Telefone bekannt zu geben
- ➔ regelmäßige Schulungen der Nutzer, um diese über neue Risiken und Sicher-

heitsmaßnahmen zu informieren und für den sachgerechten Umgang mit mobiler IT zu sensibilisieren

- die gemischte Nutzung (dienstliche und private Nutzung) dienstlich zu verwendender mobiler Endgeräte zu untersagen
- sensitive Inhalte ausschließlich über hinreichend abgesicherte Endgeräte und Infrastrukturen auszutauschen
- insbesondere bei der Übertragung von Verschlusssachen grundsätzlich nur für den entsprechenden Geheimhaltungsgrad zugelassene Geräte („Krypto-Handys“) zu verwenden

Beim Einsatz mobiler Endgeräte im Ausland sind die im „Merkblatt für den Umgang mit mobiler Informationstechnik, vorrangig in Ländern mit besonderem Sicherheitsrisiko“ (07/2008) formulierten Hinweise und Empfehlungen zu beachten.

4 Bewertung

Die Kommunikation mit GSM-Mobiltelefonen ist ohne hinreichende Sicherheitsmaßnahmen als unsicher anzusehen.

Aufgrund der anhaltenden Aktualität und der Präsenz des Themas in den Medien weist das BSI erneut auf Sicherheitsrisiken hin, die beim Einsatz mobiler Kommunikationsmittel vorhanden sind. Die Sicherheitswarnung dient dem Ziel einer fachlichen und sachlichen Aufklärung.

5 Kontakt

Sollten Sie grundsätzlichen Beratungsbedarf zum Schutz Ihrer Systeme haben, steht Ihnen das Beratungsreferat des BSI gerne zur Verfügung:

E-Mail: sicherheitsberatung@bsi.bund.de

Web: <http://www.bsi.bund.de/sicherheitsberatung/>

Telefon: 0228 99 9582-333