07.05.2026

SMS-Blaster: Neue Betrugsmasche erreicht die Schweiz

In der Schweiz etabliert sich derzeit eine neue und besonders raffinierte Form von Cyberbetrug: der Einsatz sogenannter SMS-Blaster. Diese Technologie erlaubt es Kriminellen, Smartphones in ihrer unmittelbaren Umgebung gezielt mit betrügerischen SMS-Nachrichten zu erreichen – ohne dass sie Telefonnummern kennen oder auf das reguläre Mobilfunknetz angewiesen sind.

Technisch handelt es sich bei einem SMS-Blaster um eine Art Mobilfunkantenne. Das Gerät sendet ein starkes Signal aus, mit dem es Smartphones im Umkreis von mehreren hundert Metern dazu bringt, sich automatisch zu verbinden. In diesem Moment werden die Geräte kurzfristig auf das veraltete 2G-Netz umgestellt. Genau dort liegt die Schwachstelle: Über eine bekannte Sicherheitslücke können die Angreifer SMS-Nachrichten direkt auf die verbundenen Geräte übertragen, ohne dass diese durch Filter der Mobilfunkanbieter überprüft werden.

Die versendeten SMS-Nachrichten wirken dabei oft täuschend echt. Sie geben sich beispielsweise als Mitteilungen von Behörden, Banken oder Paketdiensten aus und enthalten meist einen Link zu einer gefälschten Webseite. Ziel ist es, die Empfängerinnen und Empfänger zur Eingabe sensibler Daten zu bewegen – etwa Kreditkarteninformationen oder Zugangsdaten zum E-Banking. Besonders perfide ist, dass die Inhalte situativ angepasst werden können. So kann etwa in einer Gegend mit vielen parkierenden Fahrzeugen gezielt eine angebliche Parkbusse verschickt werden.

Besonders kritisch ist, dass diese Angriffe nicht über klassische Kommunikationskanäle laufen. Während herkömmliche Phishing-SMS zunehmend durch Filtersysteme erkannt werden, umgehen SMS-Blaster diese Schutzmechanismen vollständig. Gleichzeitig erlaubt die Technik ein sehr flexibles Vorgehen: Die Täter können sich mobil bewegen, ihre Angriffe lokal ausrichten und beliebig oft wiederholen. Da viele Smartphones weiterhin 2G unterstützen, sind auch moderne Geräte potenziell betroffen.

Wichtig ist dabei die Abgrenzung zu internetbasierten Kommunikationsdiensten: Diese Angriffsmethode betrifft ausschliesslich SMS, da sie direkt auf der Mobilfunkinfrastruktur aufsetzt. Dienste wie WhatsApp, Signal oder Telegram sind davon nicht betroffen.

Schutzmassnahmen

Um sich vor dieser Betrugsmasche zu schützen, sollten Sie folgende Punkte beachten:

- Keine Links in unerwarteten oder verdächtigen SMS-Nachrichten anklicken.
- Webseiten von Banken, Behörden oder Dienstleistern immer manuell im Browser eingeben bzw. deren offizielle App verwenden.
- Keine sensiblen Daten wie Kreditkarten- oder Login-Informationen über SMS-Links eingeben.
- Wenn möglich, die 2G-Funktion auf dem Smartphone deaktivieren.
  - Android: Auf vielen Geräten kann die Nutzung von 2G in den Einstellungen deaktiviert werden, in der Regel unter «Netzwerk & Internet».

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

  - iPhone: Eine direkte Deaktivierung von 2G ist nicht vorgesehen. Als Alternative kann der sogenannte Blockierungsmodus unter «Datenschutz & Sicherheit» aktiviert werden. Dieser unterbindet Verbindungen zu 2G-Netzen, kann jedoch auch die Funktionalität des Geräts einschränken.
- Verdächtige SMS-Nachrichten konsequent löschen und melden (z. B. auf www.antiphishing.ch (https://www.antiphishing.ch)).
- Im Zweifelsfall direkt über die offizielle Telefonnummer bei der angeblichen Absenderorganisation nachfragen.

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik