

Antifurto auto e smart meter a rischio cyber attacchi perché connessi con il 2G

In un'epoca dominata dalla velocità e dall'innovazione tecnologica, il **2G**, la prima generazione di reti cellulari digitali, potrebbe sembrare un lontano ricordo. Eppure, questa tecnologia, nonostante la sua età, rappresenta ancora oggi una minaccia significativa per la nostra sicurezza online.

Il 2G è una **tecnologia obsoleta e intrinsecamente vulnerabile**. I cybercriminali sfruttano il protocollo utilizzando dispositivi relativamente economici e facili da reperire, noti come "False Base Station" o "Stingray", che simulano una torre cellulare, inducendo smartphone e altri device a connettersi ad essi. Una volta stabilita la connessione, i malintenzionati possono intercettare le comunicazioni, compresi SMS e dati sensibili, e perpetrare una vasta gamma di attacchi, dal phishing alle frodi finanziarie.

I rischi del 2G senza crittografia

Lo ricorda anche **Google**, che ha pubblicato un post in cui spiega perché sarebbe meglio disattivare la connettività 2G. Gli esperti hanno evidenziato come sia ormai facile e poco costoso procurarsi sul mercato delle false stazioni base 4G o 5G, **comunemente chiamate FBS o Stingray**. Queste sono in grado di **simulare una rete cellulare legittima**, ingannando così i dispositivi mobili a connettersi ad essi.

Una volta stabilita la connessione, l'obiettivo primario delle FBS è quello di limitare la comunicazione alla sola rete 2G,

sfruttando la vulnerabilità di questo protocollo, **privo di crittografia**. Grazie alle loro dimensioni ridotte, i dispositivi sono facilmente trasportabili e spesso nascosti in zaini dai cybercriminali. Questi i rischi concreti:

- **SMS Blaster**: la tecnica permette di inviare messaggi ingannevoli, bypassando i filtri anti-spam degli operatori.
- **Intercettazione di dati**: i cybercriminali possono intercettare le comunicazioni e rubare informazioni personali e finanziarie.
- **Frodi**: le informazioni rubate possono essere utilizzate per effettuare acquisti non autorizzati o per sottrarre denaro dai conti bancari.

La soluzione più efficace per mitigare le problematiche è **disattivare completamente la connettività 2G**, a partire da quella sugli smartphone. **Android 12 e versioni successive** offrono questa possibilità. Sebbene le indicazioni precise possano variare a seconda del modello di smartphone, è generalmente possibile trovare l'opzione nelle **impostazioni della rete mobile**.

Come mai il 2G persiste

Nonostante i rischi, il 2G continua a essere utilizzato in molti settori, come **l'automazione industriale**, la **logistica** e **l'IoT**. Ma non solo: il protocollo viene usato anche come rete di backup del traffico voce, nel caso in cui le reti più recenti non funzionassero, per i contatori elettrici o del gas e gli antifurto delle auto. Anche le **SIM Machine to Machine** (M2M) fanno uso del 2G.

Tuttavia, la maggior parte dei dispositivi IoT sta gradualmente migrando verso tecnologie più moderne e sicure come il 4G e il 5G. In Italia, il 2G sarà definitivamente dismesso solo nel 2029. Un rapporto di Ericsson ha sottolineato che a oggi "il 2G e il 3G abilitano ancora la

maggior parte delle applicazioni IoT", circa il 60%. **Entro il 2025** le connessioni IoT aumenteranno velocemente grazie al 4G, al 5G e al **Narrowband-IoT** (NB-IoT); ma il 13% resterà ancorato al 2G e al 3G.

Leggi le altre notizie sull'home page di Key4biz

<https://www.key4biz.it/antifurto-auto-e-smart-meter-a-rischio-cyber-attacchi-perche-connessi-con-il-2g/501212/>