Stealth Phones

Bedeuten Sicherheit.

"Mit welchem Mobiltelefon kann ich mich vor verschiedenen Angriffen schützen?" Um diese Frage zu beantworten, ist es essenziell zu wissen, vor wem Sie sich schützen müssen. Suchen Sie Schutz vor neugierigen Blicken, z. B. eines Geschäftspartners, Hackern oder vor professionellen Institutionen wie Spionagefirmen, skrupellosen Unternehmen oder missbräuchlichen Regierungen? Die Auswertung der Antwort und die Analyse der jeweiligen "sicheren Mobiltelefone" erfordert jedoch viel Zeit und muss durch erfahrene Experten durchgeführt werden.

Anbieter und Entwickler "sicherer Mobiltelefone" nutzen das geringe Verständnis der Endverbraucher in diesem komplexen Thema zu Ihrem eigenen Vorteil, indem sie Sicherheit suggerieren, ohne zu erwähnen, welcher Instanz ihr Schutz gilt. **Endverbraucher laufen Gefahr, ein "sicheres Mobiltelefon" zu verwenden, das in keiner Weise den notwendigen Anforderungen entspricht.**

Die Telekommunikationsüberwachung wird ein immer grösseres Problem.

"Welche Absicht steckt hinter einer individuellen Telekommunikationsüberwachung?" Das Abhören und Überwachen von Bürgern ist eine äusserst ernste Angelegenheit. Die Fähigkeit in die Privatsphäre einzudringen ist eine enorme Macht, mit der eine Person überwacht, in Verlegenheit gebracht, kontrolliert, beschämt oder sogar ruiniert werden kann. Unser Recht auf Privatsphäre schützt uns, damit wir nicht wegen unserer Überzeugung, unserer Religion oder unseres Lebensstils verfolgt werden. Da die Technologie des Abhörens so entscheidend ist, unterliegt sie fast seit ihrer Erfindung sorgfältig ausgearbeiteten und rechtlichen Kontrollen. Die Missachtung dieser Kontrollen und das Abhören ohne richterlichen Beschluss ist in jedem Land eine Straftat, die mit erheblichen Gefängnisstrafen geahndet wird. Doch all dies wird ignoriert und das Abhören von Bürgern ohne richterliche Anordnung ist selbst in demokratischen Ländern zur täglichen Routine geworden. Die Unterscheidung zwischen legaler und illegaler Überwachung ist heutzutage nicht mehr möglich, da immer mehr private Einrichtungen Zugang zu Überwachungs- und Abhörsystemen haben und bereits ein Augenblick der Korruption ausreicht, um die erlangten Informationen zu ihrem eigenen Vorteil zu verwenden. Unsere Privatsphäre wird angegriffen, ohne dass wir es merken.

> Ein "sicheres Handy" muss den Benutzer unter allen Umständen schützen, alle Gefahren gleichbehandeln und darf nicht zwischen legaler und illegaler Telekommunikationsüberwachung unterscheiden.

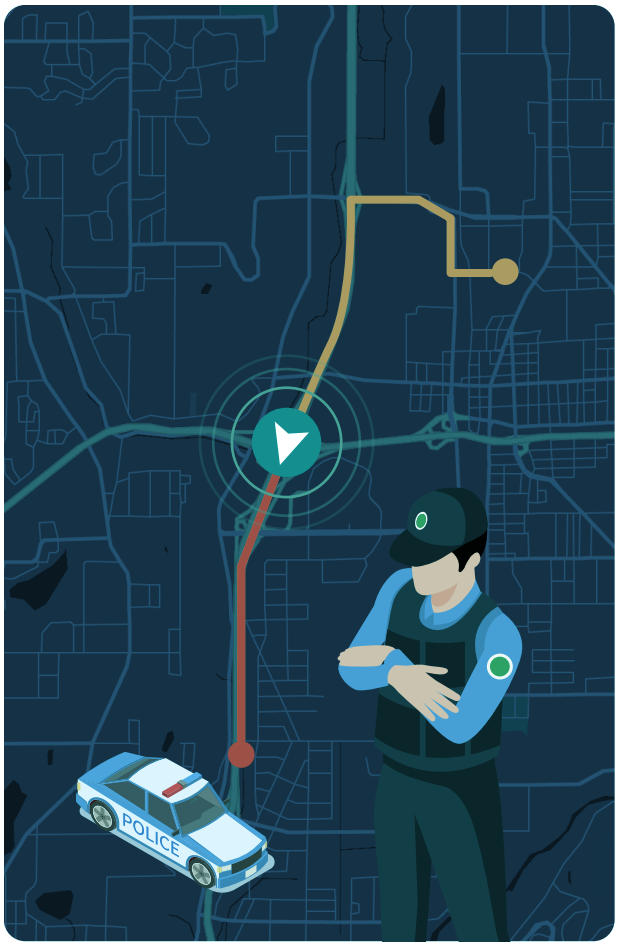
"Unterschied in der Technologie" Die legale und illegale Telekommunikationsüberwachung unterscheiden sich technologisch nicht. Legale Überwachungsmassnahmen müssen durch eine autorisierte Person genehmigt werden, damit die Ergebnisse offizielle vor Gericht verwertbar sind. Illegale Massnahmen nutzen die gleichen Überwachungs- und Abhörtechnologien, bedürfen jedoch keiner Genehmigung oder Kontrolle durch eine übergeordnete Stelle, da die Ergebnisse nicht zur offiziellen Verwendung vor Gericht erhoben werden. **Illegal gewonnene Ergebnisse dienen als Grundlage für die Genehmigung einer legalen Überwachung, deren neu gewonnene Ergebnisse vor Gericht Bestand haben.**

"Die Identität des Ziels entspricht der Identität des Mobiltelefons" Ein Mobiltelefon ist eigentlich ein Ortungsgerät, mit dem man Anrufe tätigen, Nachrichten schreiben und das Internet nutzen kann. Ein Handy identifiziert sich gegenüber dem Netz mit zwei 15-stelligen Seriennummern, anhand derer ein Handy weltweit eindeutig identifiziert werden kann.

Die IMEI
Eindeutige Telefonregistrierungsnummer.

Die IMSI
Eindeutige SIM-Registrierungsnummer.

Sobald ein Telefon eingeschaltet wird, **verbindet es sich automatisch mit dem Mobilfunkturm mit dem stärksten Signal**, auch ohne eingelegte SIM-Karte! Unabhängig von Marke, Betriebssystem, Preis oder Netztechnologie (2G, 3G, 4G oder 5G). Dieser Vorgang wiederholt sich periodisch. Damit soll verhindert werden, dass ein Mobiltelefon versehentlich vom Netz getrennt wird. Diese grundlegende Funktion des Verbindungsaufbaus erfüllt jedoch noch einen weiteren Zweck: die Ortung eines Zieltelefons. Private und staatliche Einrichtungen können den Verbindungsaufbau missbrauchen, um den Standort des Nutzers zu jedem beliebigen Zeitpunkt zu ermitteln. Jede Verbindung wird von den Mobilfunkbetreibern auf der Grundlage der Identität des Mobiltelefons und der Identität des Mobilfunkturms gespeichert. Rückwirkend können diese Datensätze von den Behörden angefordert werden oder direkt vom Mobilfunkturm heruntergeladen werden, wie dies in den USA der Fall ist (sog. Tower-Dump-Verfahren). Da dieser Vorgang periodisch wiederholt wird, lässt sich durch die Standortkontrolle der Mobilfunktürme ein nahezu lückenloses Bewegungsprofil des Handynutzers erstellen.



Rückwirkend werden nur die Verbindungsdetails wie Datum, Uhrzeit, Dauer, Richtung, Telefonnummern, IMEI's und IMSI's und Standorte aller beteiligten Handys aufgezeichnet. Es ist nicht möglich, den Inhalt von Sprachanrufen, SMS und Daten im Nachhinein zu analysieren, ohne dass zuvor eine richterliche Anordnung vorliegt. Alle Kommunikationsinhalte werden in Echtzeit ausgewertet oder falls ein Überwachungsbefehl vorliegt während der Dauer des Überwachungsprozesses (1 Tag bis 6 Monate). Dies ist auf direkter Ebene des Mobilfunkkernnetzes unter Ausnutzung bekannter SS7-Schwachstellen oder mithilfe explizit für die Telekommunikationsüberwachung entwickelter, mobil einsetzbarer Überwachungs- und Abhörsystemen möglich.

> Ein "sicheres Mobiltelefon" muss in der Lage sein, seine Identität durch Änderung von IMEI und IMSI zu wechseln, und muss über Funktionen zur Erkennung von Abhörversuchen verfügen. Das alleinige Vertrauen in die Verschlüsselung eines Mobiltelefons ist kein Garant für Sicherheit.

Mobiltelefone, die nur verschlüsselt sind, bieten keinen Schutz gegen das Abhören von Anrufen/SMS, Überwachung und Standortverfolgung durch Hacker, die Laborgeräte wie modifizierte Femtozellen, SDR-Geräte, Standortsimulatoren, Netzprüfgeräte und USRP-Geräte verwenden. Unerfahrene Hacker können nur die Luftschnittstelle ausspionieren und einige Daten wie IMEI, IMSI, Telefonnummern, den relativen Standort und - manchmal - SMS-Inhalte sammeln, aber keine Telefongespräche abhören. Erfahrene Hacker mit der entsprechenden Hardware können dasselbe wie Strafverfolgungsbehörden tun: Telefongespräche, SMS, Datenverkehr (einschliesslich Konto-Login-Informationen, Chat-Inhalte, Messenger-Inhalte usw.) abfangen und den Standort mit einer Genauigkeit von bis zu 3 Metern verfolgen.

Ein Cryptophone ist nicht so sicher, wie man denkt. Ein Mobilfunkbetreiber oder die Einrichtung, die einen GSM-Interceptor betreibt, kann wichtige Informationen wie z. B.: Kontaktpersonen, genaue Standorte und das Kommunikationsverhalten über den Benutzer herausfinden. Die aufgezählten Informationen können (und werden) verwendet, um letztendlich Ihre Geheimnisse herauszufinden, die dann vor Gericht als Beweismittel gegen Sie gewertet werden.

Abhörerkennung als Sicherheitsvorteil

Wir setzen mobile Sicherheit oft mit physischer Sicherheit gleich. Ein Unternehmen stellt einen Wachmann ein und postiert ihn an der Eingangstür seines Gebäudes. Der Wachmann steht auf seinem Posten. Er kontrolliert die Ausweise und sorgt für die Sicherheit am Eingang. Da er an der Eingangstür steht, ist er nicht in der Lage, alle Bereiche des Unternehmens zu überwachen. Wenn jemand einfach über den Zaun springt und eindringt, kann er nicht erkennen, dass ein Sicherheitsrisiko vorliegt. Das Gleiche gilt für den Einsatz einer Verschlüsselungslösung (Software oder Hardware): Sie werden nie wissen, wann Ihr Handy abgehört wird. Sie werden also nie wissen, **wann Sie wirklich in Gefahr sind**. Darüber hinaus kann jedermann (selbst ein Kind oder ein Durchschnittsbürger), der im Besitz eines einfachen und billigen Jammers ist, jedes sichere Mobiltelefon aus der Ferne durch Störung des Downlink-Kanals oder, wie es die Strafverfolgungsbehörden tun, durch Störung nur des Datenkanals ausser Betrieb setzen. Dies zwingt den Telefonbenutzer dazu, sein sicheres Telefon wie ein normales Mobiltelefon zu benutzen, normale Telefonanrufe zu tätigen und zu empfangen und normale SMS zu senden und zu empfangen, die unter diesen Umständen leicht abgefangen werden können.

> “ Ein "sicheres Mobiltelefon" muss Abhörversuche von Anrufen/SMS erkennen und den Nutzer in Echtzeit über die Überwachungsmassnahme informieren. Erst die Warnung in Echtzeit ermöglicht es dem Nutzer, die Sicherheit seines Lebens zu gewährleisten und sein Verhalten an die neuen Gefahren anzupassen.

Stealth Phones für mobile Sicherheit, es gibt keinen Ersatz. Der Rest des Marktes geht den Weg der Text- und Sprachverschlüsselung, die dem Benutzer nur ein falsches Gefühl von Sicherheit vermittelt. XCell Stealth Phones gehen den Weg, der direkt zum Kern des Problems führt, indem sie die gleichen Netzwerkschwachstellen ausnutzen, die für die Benutzer-Identifizierung, Lokalisierung, Sprach- und Datenüberwachung verantwortlich sind.

"Abhörerkennung" Stealth Phones sind in der Lage, alle Arten des Abhörens von Anrufen, SMS und Daten zu erkennen und dem Benutzer in Echtzeit zu signalisieren:

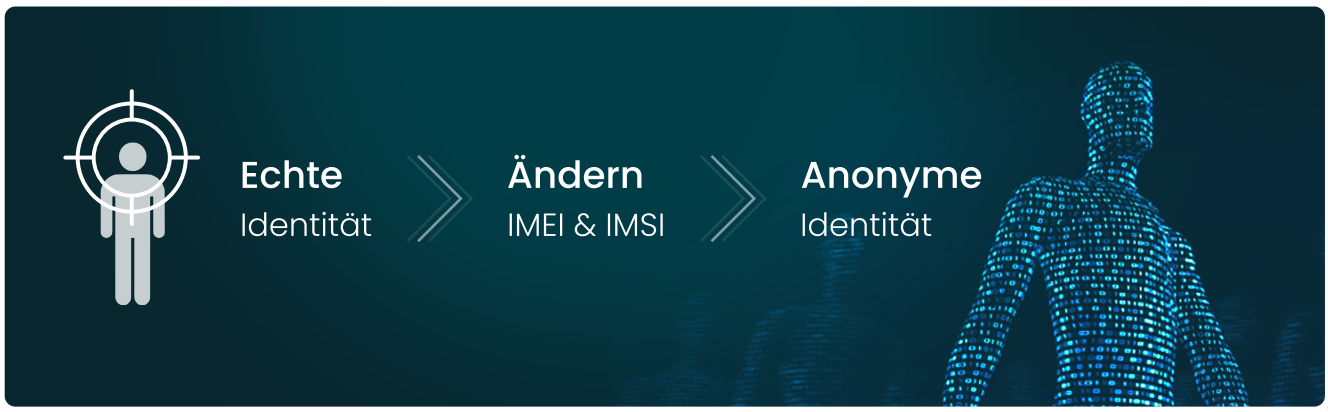
- ✓ IMSI Catcher.
- ✓ Active GSM Interceptoren.
- ✓ Semi Active GSM Interceptoren.
- ✓ Passive GSM Interceptoren.
- ✓ SS7-Mittel (mithilfe des Netzbetreibers, auch Lawful Interception genannt).

Stealth Phones erkennt auch, wenn das andere Mobiltelefon, das am Anruf beteiligt ist, abgehört wird.

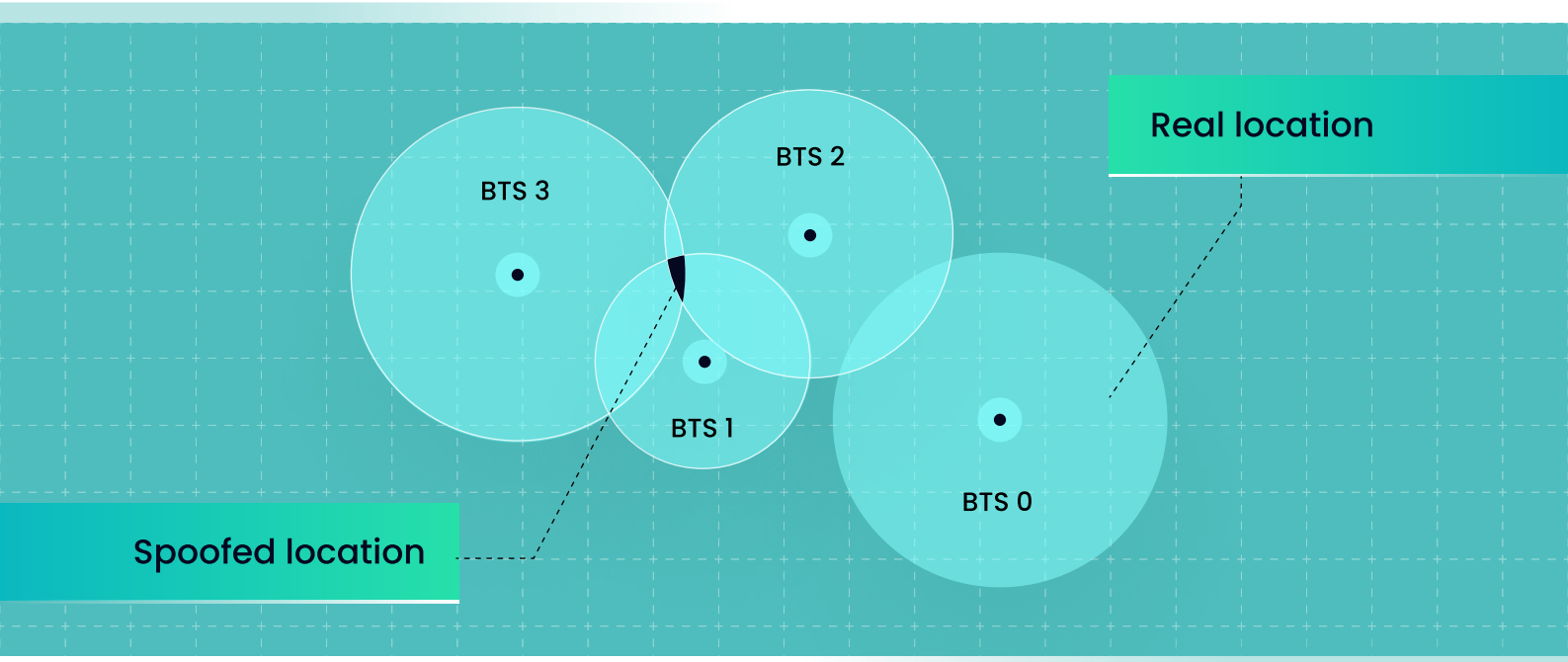
"Benutzer-Identifizierung" Einige Stealth Phones sind mit einer automatischen IMEI- und IMSI-Change Funktion ausgestattet, die Ihr Mobiltelefon in eine intelligente Spionageabwehrwaffe verwandelt. Die gleichzeitige Änderung von IMEI und IMSI verhindert die Überwachung von Standort, Anrufen, SMS und Daten. Die Tatsache, dass alle Ihre Telefonkennungen geändert wurden (die zuvor in der Zielauswahlliste eines GSM-Interceptors oder eines Mobilfunkbetreibers registriert waren), bedeutet, dass der Betreiber nicht mehr weiss, wer überwacht werden muss. Das Überwachungsorgan muss zusätzliche Anstrengungen unternehmen, um Ihre neuen Telefon-Kennungen zu erhalten und zu registrieren.

Wenn die IMSI nicht lokal auf dem Telefon geändert wird (wie es nur bei XCell Stealth Phones der Fall ist), ohne eine Internetverbindung zu benutzen und von Servern unterstützt wird, die der Benutzer nicht überprüfen und denen er nicht vertrauen kann, sondern über eine Internetverbindung durch den SIM-Hersteller, wie es einige russische und polnische Firmen tun, löst dies das Problem nicht, da ein IMSI-Catcher oder ein GSM-Interceptor mit Jamming-Funktionen solche IMSI-ändernden SIM-Karten einfach deaktivieren kann. Heutzutage ist dies eine gängige Praxis unter den Betreibern von GSM-Interceptoren.

Notiz: Wenn Sie nur die IMSI (SIM-Karte) oder nur die IMEI geändert haben, erhalten Sie keinen Mehrwert, und Ihre Anrufe werden weiterhin abgehört, als hätten Sie nichts geändert, da ein Zusammenhang zwischen unverändertem und geändertem IMEI- und IMSI-Wert erkannt werden kann.



"Ortung" Einige Stealth Phones sind mit einer "Real Location Spoofing"-Funktion ausgestattet. Dabei handelt es sich um eine echte GSM-Standortmanipulation, die auf der Manipulation von Mobilfunkmasten basiert und ein gefälschtes Triangulationsergebnis liefert. Die GSM-Triangulation wird von allen Ortungssystemen verwendet. Die GPS-Ortung ist davon nicht betroffen. Denn alle Mobiltelefone müssen geortet werden, auch jene ohne GPS-Funktion, die sogenannten Dumb Phones. Einige "sichere Mobiltelefone" bieten lediglich eine Lösung für die GPS-Ortung über eine Datenverbindung an, bei der es sich nur um eine GPS-Fälschung durch eine auf dem Telefon installierte Anwendung (VPN) handelt, die einen gefälschten GPS-Standort erzeugt, der für den Benutzer des Telefons und andere installierte Anwendungen sichtbar ist und hauptsächlich zu Scherz- und Unterhaltungszwecken verwendet wird. Die GPS-Fälschung eignet sich nicht zur professionellen Standortverfolgung. Sobald der GSM-Standort ermittelt wurde, kann das Ortungssystem problemlos eine GPS-Position berechnen. Ein Ortungssystem wird niemals direkt GPS-Daten aus dem Handy auslesen! Dies kann nur mithilfe einer sogenannten Spionagesoftware geschehen, die auf dem Zieltelefon installiert werden muss. Der Nutzer eines Stealth Phone kann wählen, mit welchem Mobilfunkturm das Telefon verbunden ist. Auf diese Weise liefert jede Triangulationstechnik, die zur Bestimmung des Standorts verwendet wird, falsche Ergebnisse und damit einen falschen Standort. Da ein Telefon die Cell-ID sendet, mit der es verbunden ist, werden die manipulierten Verbindungsdaten auch vom Mobilfunkbetreiber gespeichert. Die Entfernung zwischen dem tatsächlichen Standort des Nutzers und dem Standort des verbundenen Mobilfunkturms beträgt zwischen 1 und 10 km. Falls diese Datensätze später von den Behörden angefordert werden, führen alle Standortdaten zu falschen Ergebnissen und damit zu einem unbrauchbaren Bewegungsprofil. Gleiches gilt, wenn die Standortverfolgung in Echtzeit durch einen GSM-Interceptor erfolgt.



> XCell Stealth Phones verfügen über patentierte Technologien und ein Sicherheitsniveau, das derzeit von keinem anderen Mobiltelefon erreicht wird.

Für Ihre garantiert sichere Kommunikation bieten Ihnen die XCell Stealth Phones den höchstmöglichen Schutz vor den Risiken des Abhörens und Verfolgens von Mobiltelefonen. Stealth Phones schützen Gespräche vor der Überwachung durch Mobilfunkbetreiber, Spionagefirmen, geschickte Hacker und missbräuchliche Regierungen und garantieren, dass Ihre Anrufe, SMS und Daten 100 % vertraulich bleiben und nicht von Dritten oder IMSI-Catchern abgefangen werden können.

Stealth Phones sind die perfekte Wahl für jeden, der die Notwendigkeit einer vollständig sicheren Kommunikation erkannt hat.

Kontakt

Wenn Sie Interesse an unseren Lösungen und Demos haben, vereinbaren Sie gerne einen Termin mit uns. Wir freuen uns, mehr über Ihre anstehenden Herausforderungen zu erfahren und stellen Ihnen unsere Lösungen gern im Detail vor – in der aktuellen Lage auch in einer Online-Session.

+41 76 452 99 93

info@anti-interception.com

www.anti-interception.com

ECN GmbH
Ettenhauserstrasse 50
8620 Wetzikon ZH, Schweiz