Positionspapier

Sperrung von Mobiltelefonen
28. Juli 2014

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.100 Unternehmen, davon über 1.300 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Johannes Weicksel
Referent
Telekommunikations-
technologien und
intelligente Mobilität
Tel.: +49.30.27576-250
Fax: +49.30.27576-51-250
j.weicksel@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Einleitung

Auf der Frühjahrskonferenz der Landesinnenminister Mitte Juni 2014 in Bonn wurde über eine Sperrung der Nutzung von Mobiltelefonen in Mobilfunknetzen anhand der IMEI-Adresse diskutiert. Die Innenministerkonferenz stellte die erhebliche Bedeutung von Raub-, Diebstahls- und Betrugstaten im Zusammenhang mit dem Erlangen von hochwertigen Handys/Smartphones und Tablet-Computern fest. Sie hält es für erforderlich, diese Straftaten und die damit verbundenen erheblichen Folgen für die Opfer deutlich zu reduzieren. Sie beauftragte den AK II mit der Prüfung, welche Möglichkeiten zur Verhinderung der Nachnutzung von Handys/Smartphones/Tablet-Computern - etwa durch die Sperrung der IMEI-Nummern abhanden gekommener Geräte - bestehen und welche technischen, organisatorischen und rechtlichen Voraussetzungen erforderlich wären, um dieses Ziel zu erreichen. Der AK II, solle zur Herbstsitzung 2014 (geplant am 11 und 12. Dezember 2014) dazu berichten.

Sperrung gestohlener Mobiltelefone

BITKOM begrüßt grundsätzlich das Vorhaben den Diebstahl von Telekommunikationsendgeräten zu reduzieren. Durch den Aufbau von „Equipment Identity Register“ können Mobilfunknetzbetreiber bei Diebstahl oder Missbrauch ein durch die IMEI identifiziertes Endgerät von der Nutzung Ihres Mobilfunknetzes ausschließen. Diese Lösung bewertet BTKOM jedoch aufgrund zahlreicher technischer Unzulänglichkeiten als nur bedingt geeignet. Alternativ ist die Sperrung von Smartphones oder Tablets durch spezielle Softwarelösungen möglich. Folgende Eigenschaften sind dabei zu beachten:

IMEI-Sperrung

Fehlende Eindeutigkeit bei der IMEI-Zuordnung
Die Zuordnung einer IMEI zu einem individuellen Endgerät ist nicht immer möglich. In der Vergangenheit sind immer wieder Fälle bekannt geworden, in denen dieselbe IMEI für mehrere Endgeräte vergeben wurde. Dies geschieht von Seiten der Gerätehersteller und kann daher von Mobilfunkanbietern nicht beeinflusst werden. Da eine technische Differenzierung nicht möglich ist, wären in einem solchen Fall bei einer Sperrung alle Geräte mit derselben IMEI betroffen. Dies ist keine verbraucherfreundliche Lösung, zumal Betroffenen nicht einmal klar ist, warum ihr Endgerät keine Mobilfunkverbindung mehr bekommt. Hier stellt sich zudem die Haftungsfrage bei ungerechtfertigten Sperren.

Einfache Manipulierbarkeit der IMEI
Bei vielen gängigen Endgeräten ist die IMEI relativ leicht mit entsprechender Software manipulierbar und kann selbst nach einer erfolgten Sperrung durch einfach zugängliche Tools abgeändert werden. Ein solches Telefon ist wieder uneingeschränkt nutzbar.

Geringe Reichweite einer solchen Lösung
Zudem ist eine Sperrung nur innerhalb des Netzes möglich, dessen Betreiber ein sogenanntes „Equipment Identity Register“ führt. Alternativ wäre auch ein zentrales „Equipment Identity Register“ für alle Netzbetreiber eines Landes möglich. Kriminellen wäre es aber selbst dann ein Leichtes, gestohlene Ware im Ausland weiter zu veräußern. Dort wäre eine uneingeschränkte Nutzung möglich.
Eine effektive Sperrung der IMEI wäre also nur dann möglich, wenn alle Netze einer Region den Status der Endgeräte in einem zentralen „Equipment Identity Register“ abfragen. Hier wäre eine zumindest europäische Lösung erforderlich. Durch eine Europaweite Sperrung einer IMEI würde es jedoch auch häufiger zu Kollateralschäden in Folge mehrfacher Zuweisung der identischen IMEI kommen.

Fehlender Kundennutzen
Ohne einen effektiven Abschreckungseffekt durch starken Wertverlust des Handys für den Dieb entsteht dem Kunden kein Nutzen. Das Gerät bleibt verschwunden. Bei der heutigen Verbreitung von Smartphones wirkt zudem vielfach der Verlust von und/ oder Zugang Dritter zu auf dem Handy gespeicherten Daten zu größeren Problemen. Selbst eine erfolgreiche IMEI-Sperrung kann hier nicht helfen.
Zudem gibt es auf dem Markt zahlreiche Ortungsfunktionen, die eine Lokalisation und Fernsteuerung eines Endgerätes auch nach dessen Verlust möglich machen, solange das Gerät über Konnektivität verfügt. In Folge der IMEI-Sperrung wäre eine Erreichbarkeit des Endgerätes für diese Ortungsfunktionen nicht mehr möglich.

Software-Sperrung

Alternativ zur Sperrung über IMEI haben Hersteller von Smartphones bereits vereinzelt Lösungen entwickelt, um ein Endgerät bei Diebstahl aus der Ferne sperren zu können oder zur Benutzung unbrauchbar zu machen. Im April diesen

Jahres einigten sich die große Smartphone-Hersteller auf ein gemeinsames System („Smartphone Anti-Theft Voluntary Commitment“, http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment). Dabei wird eine Sperrfunktion über eine individuelle PIN integriert. Zum einen ist hierbei eine eindeutige Zuordnung zu einem Endgerät möglich. Zum anderen lässt sich ein einmal gesperrtes Handy nicht einfach durch das Zurücksetzen auf Werkseinstellungen reaktivieren. Damit sinkt der Weiterverkaufswert im Falle eines Diebstahls deutlich. Zudem lassen sich gelöschte Daten nach den Plänen der Anbieter durch Nutzung von Backup-Systemen auch wiederherstellen. Dies ist für Kunden relevant, die ihr Endgerät irrtümlich gesperrt haben oder es nach einem Diebstahl wiedererlangen.

Schlussfolgerung

Für den Erfolg der Sperrung anhand der IMEI-Informationen wäre ein durchgängiges „Equipment Identity Register“ über alle Mobilfunknetze einer Region notwendig. Damit würde ein vereinheitlichtes Vorgehen der Sperrung der Mobilfunkfunktion für alle Nutzer von Mobiltelefonen realisiert.
Herstellerspezifische Softwarelösungen bewirken einen höheren Grad an Sicherheit, sind jedoch vom Nutzer eines Smartphones selbst einzurichten.