Stellungnahme

Bund-Länder Projektgruppe „Smartphonesperre“ – Fragenkatalog vom 21. August 2014
03. September 2014

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. Mehr als drei Viertel der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils knapp 10 Prozent kommen aus sonstigen Ländern der EU und den USA, 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Albrechtstraße 10
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 & 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

Im Nachgang zu einem ersten Gespräch des Bremer Innensenators Herrn Mäurer mit den deutschen Mobilfunkanbietern am 18. August 2014[1] ging dem BITKOM mit Brief vom 21. August die Bitte um Beantwortung verschiedener Fragen zum Thema „Smartphonesperre“ zu. Zur Unterstützung der zum Thema gegründeten Bund-Länder Projektgruppe wurde um Beantwortung der Fragen bis 03. September gebeten. Die durch den BITKOM-Arbeitskreis Mobilkommunikation abgestimmten Antworten finden Sie untenstehend.

Für die folgenden Ausführungen ist darauf hinzuweisen, dass wir stets unterschiedliche Geräteklassen zu betrachten haben. Auf Mobiltelefonen (M) kann nur mit unverhältnismäßig hohem Aufwand Software aufgespielt werden was für den Endnutzer nicht zumutbar ist. Smartphones (S) bieten generell die Möglichkeit, Software-Applikationen auf einfache Weise (zumeist aus einem frei zugänglichen Portal) zu beziehen und für den Nutzer zugänglich zu machen. Beide Geräteklassen besitzen stets eine IMEI-Adresse (nebst anderen Adressierungs- bzw. Kennungstypen, z.B. Seriennummer, WLAN MAC-Adresse, Bluetooth MAC-Adresse). Die Geräteklasse der Tablets bietet durchgängig die Möglichkeit, Applikationen zu installieren, ist aber abhängig von der Verfügbarkeit eines Mobilfunkmoduls (TM) mit einer IMEI-Adresse versehen. Tablets, die nur mit WLAN-Schnittstelle versehen sind, haben keine IMEI-Adresse (TW). Generell ist festzustellen, dass im hochpreisigen Tablet-Segment der Anteil der Geräte mit Mobilfunkmodul überwiegt. Im Niedrigpreissegment verhält es sich umgekehrt.

Aus Sicht des BITKOM stellt sich aktuell die Frage, von welcher Situation in Bezug auf Diebstahl von mobilen Endgeräten ausgegangen werden muss. Wie

[1] Das dazu vorbereitete BITKOM-Positionspapier „Sperrung von Mobiltelefonen“ finden Sie unter http://www.bitkom.org/de/themen/54882_80245.aspx

hoch sind die absoluten Fallzahlen? Werden mehrheitlich Geräte in Benutzung oder auf dem Transportweg (z.B. zum Händler) gestohlen? Ist der Diebstahl dieser Geräte ein explizites Tatmotiv oder ein Kollateralschaden bei z.B. Handtaschendiebstählen? Antworten zu diesen Fragen erleichtern die Auswahl gezielter und wirksamer Maßnahmen.
Im Jahr 2013 wurden insgesamt mehr als 38.000.000[2] Mobiltelefone, Smartphones und Tablets in Deutschland verkauft. In der Annahme, dass die Sachfahndungsliste 300.000 vermisste Geräte aus 2013 zählt, läge die Diebstahlquote pro Jahr bei klar unter 1%.
Die Angemessenheit von angestrebten Maßnahmen sollte unter dieser Prämisse betrachtet werden.

[2] nach EITO/IDC

Welche aktuellen Leistungspakete im Zusammenhang mit Diebstahlschutz bzw. der generellen Verhinderung der Nachnutzung von entwendeten mobilen Endgeräten werden von den einzelnen Mobilfunkbetreibern angeboten?
Welche Erfahrungen wurden gemacht
Worauf fußen die verschiedenen Lösungen (z.B. Whitelist, iTunes, andere Software)?
Welche Möglichkeiten der Umgehung gibt es schon?

Die Mobilfunknetzbetreiber bieten unterschiedliche, ggf. nur einzelne der im Folgenden genannten Leistungspakete an, die vor Diebstahl, der Nutzung eines entwendeten Endgeräts oder einem monetären Schaden durch einen Diebstahl schützen sollen. Dazu gehören:

Ortung des Endgeräts bzw. der SIM (S, TM, TW)
Es besteht die Möglichkeit, Endgeräte über entsprechende Apps zu orten. Diese Apps werden sowohl direkt von den Endgeräteherstellern als auch von Drittanbietern angeboten. Zur Lokalisierung werden die Standortdienste des Endgerätes genutzt: GPS Daten, bekannte WLANs oder, sofern vorhanden, Netzstandort der SIM. Es besteht darüber hinaus die Möglichkeit der Ortung durch die Lokalisierung des Endgeräts anhand der Positionskoordinaten der Mobilfunkzelle, in die das Endgerät eingebucht ist. In einem Webinterface wird dem Kunden nach entsprechender Authentifizierung auf expliziten Lokalisierungswunsch hin der Standort seiner eigenen SIM innerhalb eines relevanten Radius um die Funkzelle herum angezeigt. Der Kunde kann die Lokalisierung des Endgerätes alternativ via SMS (nur bei S und TM) auslösen.

Sperrung bestimmter Gesprächsarten (z.B. Sonderrufnummern, Auslandstelefonate) (M, S)
Auf Kundenwunsch können bestimmte Vorwahlbereiche oder gegebenenfalls Nummerngassen für die Nutzung gesperrt werden. Anhand der IMSI werden die jeweiligen Berechtigungen im Netz gespeichert. Die Limitierung ist nur durch den Austausch der SIM-Karte zu umgehen.

Sperrung der SIM-Karte (M, S, TM)
Das Endgerät kann beim Mobilfunknetzbetreiber als gestohlen gemeldet werden und die im Gerät befindliche SIM-Karte wird zur Nutzung gesperrt. Die über die IMSI registrierte SIM-Karte kann durch den Kunden selbst über ein Web-Interface oder telefonisch zur weiteren Nutzung im Mobilfunknetz gesperrt werden. Die Maßnahme lässt sich von Dritten nicht umgehen. Die Wiederherstellung der Mobilfunkverbindung ist durch den Austausch der SIM-Karte möglich.

Sperrung anhand der IMEI-Adresse (M, S, TM)
Vodafone bietet als einziger Mobilfunknetzbetreiber in Deutschland die Sperrung eines Endgeräts für die Nutzung von Mobilfunkservices an. Die IMEI wird in der Blacklist des EIR des Mobilfunknetzes eingetragen – bei bestimmten Aktionen zwischen dem Endgerät und dem Mobilfunknetz erfolgt ein IMEI-Check im EIR, so dass bei einem Positiv-Check das Endgerät vom Netz abgewiesen wird.
Eine Schwäche dieser Lösung entsteht aus der Tatsache, dass gleiche IMEIs für verschiedene Endgeräte mehrfach vergeben sind, so dass in Folge eines validen Sperrantrages eines Kunden ggf. mehrere Endgeräte anderer Kunden

unrechtmäßig vom Netz abgewiesen werden. Im Beschwerdefall muss durch den Netzbetreiber die IMEI aus der Blacklist ausgetragen werden, so dass auch das entwendete Gerät im Netz wieder verwendet werden kann.
Eine weitere Schwäche ist die einfache Manipulierbarkeit der IMEI in den Endgeräten. Im Internet finden sich zu Dutzenden Anweisungen und Videos zur Manipulation der IMEI. Einfache Suchbegriffe, wie „IMEI ändern“ führen bereits zum Ziel, so dass auch technisch nicht-versierte Personen die IMEI gestohlener Endgeräte innerhalb weniger Minuten ändern können. Selbst nach einem Gelegenheitsdelikt hat der Täter damit eine schnelle und einfache Möglichkeit, das Diebesgut für sich nutzbar zu machen. Technisches Wissen, organisierte kriminelle Strukturen sind nicht notwendig. Ein Eintrag der originären IMEI (egal ob nationales oder europäisch-einheitliches EIR) in die Blacklist des EIR nach Antrag des bestohlenen Kunden ist damit ineffektiv. Das manipulierte Gerät kann uneingeschränkt in den Netzen verwendet werden.
IMEI-basierte Analysen bei Vodafone haben beispielsweise ergeben, dass betrügerisch entwendete Endgeräte im deutschen Vodafone-Netz in der Regel nicht verwendet werden. Analoges Vorgehen wird bei gestohlenen Geräten vermutet. Vodafone geht davon aus, dass entweder die IMEIs vor dem Weiterverkauf manipuliert oder ein grenzüberschreitender Austausch der Geräte erfolgt. Auch in diesem Fall würde eine Eintragung in EIR nicht effektiv sein, insbesondere, wenn nur eine nationale EIR Lösung angestrebt wird und keine mindestens EU-einheitliche Lösung. Wenn man dennoch die IMEI eines bestimmten Kunden sperren würde, wären möglicherweise allein in Deutschland hunderte von Kunden gleichzeitig betroffen, deren Endgeräte ohne für sie erkennbaren Grund nicht mehr nutzbar wären. Betroffen wären übrigens nicht nur eigene Kunden, sondern – wenn der Austausch der IMEI-Daten über das zentrale EIR-Register (CEIR) in Dublin genutzt wird -, auch Kunden ggf. aller anderen Netzbetreiber mit EIR-Sperrmöglichkeit. Der Kundenservice der Netzbetreiber könnte in solchen Fällen zunächst keine Abhilfe schaffen, da systemseitig das gestohlene Endgerät vom nicht gestohlenen Endgerät mit derselben IMEI nicht unterscheidbar wäre. Derart betroffene Kunden wären hochgradig verärgert. Besondere Sorge bereiten daher den Mobilfunkprovidern die Haftungsfragen auf Grund ungerechtfertigter Sperren.

Bereitstellung von Sicherheitsapplikationen (S, TM, TW)
Applikationen, die die Ortung, Fernlöschung oder die Sperrung des Endgeräts aus der Ferne ermöglichen, werden durch den Mobilfunkprovider direkt angeboten. Der Kunde muss die Applikationen selbst auf dem Endgerät einrichten. Die Löschung durch einen Dieb ist grundsätzlich möglich, sofern auf dem Endgerät keine Displaysperre eingerichtet ist und das Gerät nicht zuvor vom Nutzer via Internet oder SMS gesperrt wurde.

Handyversicherung (M, S, TM, TW)
Dies ist eine Versicherung, die unter anderem im Falle des Diebstahls den Wert des Endgeräts ersetzt. Beispielsweise die Deutsche Telekom hat zur Zeit rund 300.000 Kunden, die eine solche Versicherung abgeschlossen haben. Die gemeldete Diebstahlquote unter diesen Kunden liegt bei ca. 1%. Eine Handyversicherung ist zwar kein originärer Diebstahlschutz, aber eine mögliche Lösung des eigentlichen Kundenproblems durch Begrenzung des finanziellen Schadens. Die Sperre eines bereits gestohlenen Endgerätes hilft dem rechtmäßigen Besitzer letztlich nicht.

Welche Möglichkeiten sehen die Provider, um der negativen Entwicklung der Phänomene Diebstahl/Raub/Betrug im Zusammenhang mit mobilen Endgeräten (Mobiltelefone/Smartphones/Tablets) entgegenwirken zu können?

Es gibt verschiedene weitere Maßnahmenoptionen, um dem Diebstahl von mobilen Endgeräten entgegenzuwirken.

Bereitstellung von Schutzapplikation durch Endgeräte- oder Betriebssystemhersteller (S, TM, TW)
Die Funktionalität zum Lokalisieren und Sperren des Endgeräts ist direkt bei Auslieferung bereits implementiert. Mitunter basiert die Lösung darauf, dass das Gerät periodisch bei einer anbieterspezifischen Stelle prüft, ob ein Diebstahl bzw. eine Sperrung des jeweiligen Geräts vorliegt. Dabei erfolgt die Identifizierung durch Accountinformationen in Verbindung mit einer hardwarebezogenen ID. Diese Prüfung erfolgt über jegliche Internetverbindung (z.B. über jedes Mobilfunknetz oder jedes zugängliche WLAN). Dies stellt eine effektive Kontrolle sicher, da jedes Smartphone/Tablet früher oder später mit dem Internet verbunden wird, um effektiv genutzt werden zu können. Wird ein Gerät als gestohlen gemeldet, wird dem Endgerät ein Sperrsignal gesandt.
Der Kunde muss, wenn er die Schutzapplikation nutzen möchte, den Dienst aktivieren oder sich dafür registrieren. Es ist aber schon aus Datenschutzgründen unerlässlich, dem Kunden auch die Möglichkeit einzuräumen, den Dienst nicht zu aktivieren bzw. nachträglich den Dienst deaktivieren zu können. Die anfallenden Informationen werden entsprechend den Datenschutzbedingungen des jeweilig anbietenden Unternehmens verarbeitet. Bei Sperrung ist das Gerät auch nach einem Hard-Reset nicht für den Dieb nutzbar.
Durch Überschreiben des EPROMs, welches den Datensatz für die Betriebssysteminstallation trägt, ist allerdings unter hohem Aufwand die Möglichkeit gegeben das Gerät wieder nutzbarzumachen. Für den Diebstahl etwa auf dem Transportweg zum Händler ist allerdings auch dieser Mechanismus wirkungslos.

Verbraucherinformationen publizieren (M, S, TM, TW)
Die Sensibilisierung der Endnutzer stellt eine Möglichkeit der Vorbeugung dar. Mit dem verstärkten Hinweis auf die Attraktivität von Endgeräten als Diebesgut würden Nutzer besser auf Ihre Habe aufpassen.
Auch Hinweise auf bereits implementierte Mechanismen zur Verhinderung von Diebstählen (z.B. SIM-Sperrung, Datenlöschung auf dem Endgerät, Erstattung einer Anzeige) und Anleitungen wie diese konkret zu nutzen sind, würde das Problembewusstsein erhöhen. Dies müsste als konzertierte Initiative von Polizei, Endgeräteherstellern und Netzbetreibern geschehen.

Geräte-PIN / Entsperrbildschirm
Die Nutzung einer Geräte-PIN oder eines Entsperrbildschirms stellt bereits eine Erhöhung der Sicherheit dar. Die PIN oder ein festgelegtes Muster muss nach dem Ausschalten des Bildschirms oder einer längeren Phase der Inaktivität eingegeben werden. Auf diese Weise hat ein Dieb nur noch geringe Chancen, auf die Daten, die auf dem Smartphone gespeichert sind, zuzugreifen. Allerdings ist nicht ausgeschlossen, dass der Dieb mit einem zusätzlichen Aufwand bzw. Expertenwissen das Gerät initialisiert und dann für sich in Betrieb nimmt.

Juristische Maßnahmen

Eine weitere Möglichkeit, Diebstahlsdelikte im Zusammenhang mit Mobiltelefonen, Smartphones und Tablets zu reduzieren, liegt darin, geeignete juristische Maßnahmen zu ergreifen. Denkbar wäre, das Strafmaß für ebensolche Delikte zu erhöhen oder eine öffentlichkeitswirksame Ächtung zu forcieren.

Gibt es providerübergreifende weitere Möglichkeiten des Diebstahlschutzes?

Eine providerübergreifende Möglichkeit, gestohlene Geräte zu sperren bzw. zu deaktivieren, ist dringend geboten, um den Diebstahl von mobilen Geräten entscheidend einzudämmen. Dabei ist anzuraten, die Gerätehersteller für eine effektive und effiziente Lösung einzubinden, da selbst ein weltweit aufzubauendes EIR letztlich keinen effektiven Nutzen in der Diebstahlprävention erwirken könnte. Die Lösung des Problems alleine durch eine Kooperation aller Mobilfunknetzbetreiber erscheint dabei nur schwer umsetzbar. Gestohlene Geräte könnten stets in Länder "exportiert" werden, in denen eine Kooperation der dort ansässigen Provider nicht gegeben ist oder aufgrund von anderen wirtschaftlichen Interessen Einzelner, nicht richtig gelebt wird.
Der US-amerikanische Bundesstaat Kalifornien ist das Diebstahlproblem angegangen, indem er Hardwarehersteller verpflichtet hat, einen technischen Diebstahlschutz zwingend in allen neuen zum Verkauf stehenden Endgeräten ab Juli 2015 einzubauen. Anders als in den Vereinigten Staaten werden in Deutschland viele Endgeräte nicht direkt über die Telekommunikationsanbieter, sondern „vertragsfrei“ im Handel, auf Flohmärkten oder anderweitig verkauft. Als Folge werden mobile Endgeräte des Öfteren auch von Provider zu Provider „transferiert“. Schon aus diesem Grund ist eine flächendeckende Lösung geboten, die möglichst auch unabhängig von den Providern funktionieren sollte, da ansonsten allein schon bei einem Providerwechsel ein nicht unerheblicher Aufwand für das Gerätemanagement entsteht.
Für einen flächendeckenden Diebstahlschutz ist es wichtig, dass die jeweiligen Geräte providerunabhängig identifizierbar sind. Es bietet sich beispielsweise an, hierfür eine hardwarebezogene ID der Geräte zu verwenden, da diese oftmals entweder in nicht-schreibbaren Bereichen des ROMs oder auf speziellen Chips in der Gerätehardware gespeichert sind. Dies schließt für die jeweiligen Endgeräte eine nachträgliche Verfälschung effektiv aus bzw. erschwert diese erheblich. Auch ist die Hardware-ID der Geräte in der Regel nicht mit personenbezogenen Daten verknüpft, was aus Datenschutzgesichtspunkten dringend geboten erscheint.
Aber auch bei einer solchen Lösung wäre zu berücksichtigen, dass unabdingbar für den Erfolg eines solchen Verfahrens insbesondere hardwarebezogene ID und die notwendige Software verlässlich im Endgerät gespeichert sein müssen, dass die Verifikation der Legitimität höchst problematisch ist, dass Kunden für die Sperrung notwendige Passwörter im Falle des Falles (z.B. im Ausland) nicht zur Verfügung haben oder aber, dass sie ein einfaches Passwort wählen, das ein Dritter erraten kann, so dass ein Angreifer die Geräte des Kunden sperren könnte.

Wie könnten aus Sicht der Provider und des BITKOM die Gerätehersteller und die Softwareanbieter (Betriebssysteme und Sicherheitsapplikationen) in den gestarteten Prozess einbezogen werden?

Da sich bei der Einführung einer Diebstahlschutzlösung auch technische Fragen stellen, sehen wir es als extrem wichtig an, Hardwarehersteller als auch Softwarehersteller einzubinden, da ohne diese beiden Parteien und nur durch die Telekommunikationsanbieter alleine keine praktikable Lösung realisierbar erscheint.
Auch wenn eine zentrale Stelle (vgl. den zentralen Sperr-Notruf 116 116) zur Annahme von Sperranfragen geeignet scheint und dem Interesse der Konsumenten entsprechen könnte, stellt sich dennoch die Frage, auf welche Weise nachgewiesen werden kann, ob der Konsument eine Berechtigung der Sperrung des von ihm benannten Endgerätes besitzt. Eine solche Lösung könnte die Komplexität bei möglichen Providerwechseln reduzieren und böte für den Konsumenten immer einen klaren Ansprechpartner bei Fragen rund um die Sperrung seines Gerätes.

Mit Bezug auf die CTIA-Initiative sollten die dort genannten und am deutschen Markt vertretenen Hersteller durch den Bremer Innensenat eingeladen werden um aufzuzeigen, ob die für den US-Markt ab Juni 2015 zu implementierenden Funktionen auch Standardfunktionen der Geräte auf dem deutschen Markt werden können und falls ja, ab wann. Die Hersteller könnten gegebenenfalls eine CTIA-ähnliche Selbstverpflichtung unterschreiben. Ab dem Zeitpunkt der Verfügbarkeit einer nationalen Lösung sollte eine weitere Sensibilisierungsmaßnahme initiiert und gesteuert werden. Eine Möglichkeit dazu wäre, einen Hinweis auf diese Endgeräte-Funktion im Initialisierungsprozess des Endgeräts anzuzeigen und somit den Nutzer bei der Inbetriebnahme des Geräts über die Möglichkeit des Schutzes zu informieren.

Fazit
In dieser Stellungnahme wurden viele Maßnahmen kurz umrissen. Für die Prüfung auf Tauglichkeit muss eine klarere Definition der Ziele abgeleitet von aktuellen Diebstahlstatistiken erfolgen. Die möglichen Maßnahmen dazu müssen sowohl technisch wie u.a. auch datenschutzrechtlich genauer betrachtet werden. Auch die Prüfung nicht-technischer Maßnahmen wie die Erhöhung des Strafmaßes für solche Delikte muss mit einbezogen werden. Es müssen aber auch mögliche negative Auswirkungen von einzelnen Maßnahmen betrachtet werden: Besteht nicht die Gefahr, dass ein Dieb mit eher üblen Methoden seinem Opfer mögliche Sicherheitskennungen (z.B. bei einem iPhone die Apple-ID + Passwort), die eigentlich dem Diebstahlschutz dienen sollen, abpresst?