Stellungnahme

Bund-Länder Projektgruppe „Smartphonesperre“ – Fragenkatalog vom 19. Dezember 2014
21. Januar 2015

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. 76 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 10 Prozent kommen aus Europa, 9 Prozent aus den USA und 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
Telekommunikationstechnologien 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

Die Bund-Länder Projektgruppe „Smartphonesperre“ wurde im Auftrag der Innenministerkonferenz ins Leben gerufen um Vorschläge zur Reduzierung der Diebstahlszahlen von Smartphones und Tablets auszuarbeiten. BITKOM begrüßt diese Aktivitäten und versucht die BLPG entsprechend zu unterstützen.[1] Im Nachgang zur Teilnahme an der Sitzung der Bund-Länder Projektgruppe „Smartphonesperre“ am 10.Dezember 2014 in Stuttgart ging dem BITKOM mit Schreiben vom 19. Dezember die Bitte um Beantwortung eines zweiten Fragenkatalogs zum Thema zu. Im Weiteren finden Sie die in Kapitel 4. des Schreibens formulierten Fragestellungen sowie entsprechende Antworten.

4.1.1. IMEI-Mehrfachvergabe und IMEI-Sperre

Vorab: Die IMEI ist wird im Herstellungsprozess auf einem Endgerät verankert und ist mit der Hardware verbunden. Diese Identifikationszahl ist unabhängig von Nutzer und SIM-Karte. Daher ist sie auch weiterhin gültig, wenn die SIM-Karte ausgetauscht wird. Augenscheinlich ist es grundsätzlich möglich, die IMEI-Adresse mit Hilfe von Software zu fälschen. Für aktuelle Endgeräte ist dies in der Regel nur dannder Fall, wenn sich der Nutzer zunächst Zugriff auf die Grundeinstellungen des Betriebssystems verschafft hat (bekannt als jailbreak oder root-Zugriff).

- Welche Möglichkeiten bestehen Ihrer Ansicht nach, die Mehrfachvergabe von IMEI Nummern auszuschließen?

[1] siehe dazu auch das Positionspapier vom 28.07.2014 (http://www.bitkom.org/de/themen/54882_80245.aspx) sowie die Stellungnahme zur Beantwortung des ersten Fragenkatalogs der BLPG vom 03.09.2014 (http://www.bitkom.org/de/themen/54882_80372.aspx)

Herstellerseitig wäre sicherzustellen, dass die Grenzen der IMEI-Variationen so ausgenutzt werden, dass eine Doppelvergabe einer IMEI mind. innerhalb von 10 Jahren ausgeschlossen werden kann.
Die Implementierung im Endgerät müsste auf einem nicht wieder beschreibbaren Chip erfolgen, um Dopplungen durch Änderung der IMEI Nummer auszuschließen.

- Welche Maßnahmen unternehmen Sie, eine Mehrfachvergabe zu verhindern?
Ein Hersteller nutzt einen fest vergebenen IMEI-Bereich, der nur ihm zugeordnet ist. Dies schließt Doppelungen aus. Hersteller-interne Prozesse sichern die eineindeutige Zuordnung zum Endgerät.

- Wird dem IMEI-Sperr-Verfahren eine Chance auf Realisierung eingeräumt?
Technisch ist die Realisierung einer EIR (Equipment Identity Register Datenbank) mit einer Blacklist-Systematik auf unterschiedlichen Ebenen (national, europäisch, international) theoretisch möglich. Aufgrund der bekannten Schwächen (IMEI-Mehrfachvergabe, Manipulation/ Änderung der IMEI) und der Herausforderung, qualitativ gleichwertige und zuverlässige Prozesse bei allen Beteiligten hinsichtlich Prüfung auf Rechtmäßigkeit der Sperr- und Entsperraufträge von Personen zu etablieren, räumen wir der Realisierung einer praxistauglichen Umsetzung keine Chance ein. Es existiert kein zuverlässiges Verfahren – bspw. analog zur Kfz-Zulassung –, mit dem eine Person den rechtmäßigen Besitz eines Endgerätes nachweisen kann – als Basis zur Prüfung der Rechtmäßigkeit des Sperr-/ Entsperrauftrages. Die Person kann bestenfalls eine Rechnung des Herstellers/Providers oder Händlers als Erwerbsnachweis vorlegen, allerdings kann ein Sperrauftrag auch dann schon unzulässig sein, falls die Person das Gerät nach dem ursprünglichen Kauf an einen Dritten zur Nutzung durch (beleglosen) Weiterverkauf oder Schenkung weitergegeben hat.
Die Probleme, die sich bereits mit den national erhobenen Daten ergeben, gelten umso mehr für die Daten, die von ausländischen Datenbanken übernommen werden müssen, da der internationale Datenaustausch essentiell für das Funktionieren des EIR-Ansatzes ist.
Ohne umfassenden internationalen Austausch wäre die IMEI-Sperre nur jeweils im eigenen Land gültig. Entwendete Endgeräte würden im Falle einer nur lokal funktionierenden Lösung (z.B. nur in Deutschland) dann eben in anderen Regionen weiterverwertet.
Aufgrund dieser Tatsache ergeben sich mehrere problematische Szenarien der IMEI-Sperre – Beispiele:
  - Person A verkauft sein eigenes Gerät auf dem Flohmarkt/ einer Online-Plattform an Person B. Person A lässt basierend auf dem ursprünglichen Kaufvertrag die IMEI sperren.
  - Person B kauft beleglos (z.B. auf dem Flohmarkt, Verkaufsplattformen im Internet oder von Bekannten) ein Endgerät. Sollte es ihm gestohlen werden, wäre Person B nicht in der Lage, den rechtmäßigen Besitz nachzuweisen und könnte somit keinen Sperrauftrag stellen.
  - Person B kennt die IMEI des Endgeräts von Person A. Person B ändert die IMEI seines Endgeräts auf die IMEI von A und lässt diese IMEI dann sperren („Beweis“ der Rechtmäßigkeit ggf. über Nutzungsprofil beim Netzbetreiber).
  - Person A kann wegen einer systemseitigen IMEI-Sperre auf Basis einer aus dem Ausland importierten IMEI sein rechtmäßig erworbe-

nes und in seinem Besitz befindliches Endgerät von einem Tag auf den anderen nicht mehr nutzen. Er erhält zudem weder vor noch nach Einrichtung der Sperre eine diesbezügliche Information. Auch sein Mobilfunknetzbetreiber könnte hier nicht weiterhelfen. Im Gegenteil: Der Mobilfunknetzbetreiber muss sich ggf. mit Haftungsfragen auf Grund einer möglicherweise ungerechtfertigten Sperre auseinandersetzen.

- Gibt es bei den Endgeräteherstellern Überlegungen, die IMEI manipulationssicher in einem Microcontroller/Speicher zu hinterlegen oder anderweitig besser zu sichern?

Dieses ist bereits heute bei einigen Herstellern gängige Praxis.
Die GSM Association definiert auch entsprechende Richtlinien[2].

- Wie hoch wird der Aufwand für eine europäische Datenbank für entwendete bzw. verlorene Endgeräte eingeschätzt (keine Schutzfunktion Kill-Switch). Beispiel wäre die CEIR in Großbritannien.

Der Aufwand setzt sich mind. aus den folgenden Teilen zusammen:

(a) Aufwand zur Etablierung eines EU-Standards/ -Richtlinie
(b) Aufwand zur technischen Implementierung der zentralen EU Datenbank
(c) Aufwand zur technischen Implementierung der EIR-Datenbank bei den TK-Providern (die DBs müssen synchronisiert/ gespiegelt sein, um die Zuverlässigkeit und geforderte Schnelligkeit der Zugriffe beim Verbindungsaufbau, Handover, Zellwechsel etc. im Mobilfunk des Providers zu erreichen)
(d) Aufwand zur technischen Implementierung der netzseitigen Funktionalitäten zur Überprüfung der IMEI bei jedem Verbindungsaufbau
(e) Aufwand zur Erhöhung der Signalisierungskapazitäten wegen der Erhöhung des Signalisierungsaufkommens (zwecks o.a. Überprüfung)
(f) Aufwand zur Definition und Implementierung der rechtssicheren Prozesse zur Umsetzung von Sperr- und Entsperraufträgen von Nutzern.
(g) Aufwand zum technischen Betrieb und Maintenance der zentralen EU Datenbank
(h) Aufwand zum technischen Betrieb und Maintenance der EIR Datenbanken bei den TK-Providern
(i) Aufwand zum Betrieb der Sperr- und Entsperrprozesse und der Regelung von Clearingfällen
(j) Aufwand zur Information der Nutzer über dieses Verfahren (einmalige und dauerhafte Aufwände)

Eine realistische Abschätzung dieser Aufwände ist basierend auf den derzeitigen Informationen nicht möglich, dazu müsste mind. ein High-Level Konzept, besser noch ein Detailkonzept entwickelt werden, was Ausgangspunkt der Aufwandsschätzung sein könnte.
Allein zu Punkt (c) ist eine partielle Aussage möglich, die Erneuerung der Hard- und Software einer existenten, operativen EIR-Datenbank bei einem TK-Provider kostet zwischen 3 und 4 Millionen Euro. Der tatsächliche Aufwand der Implementierung einer neuen IMEI-Sperre– also ne-

[2] siehe dazu http://www.gsma.com/newsroom/wp-content/uploads/2012/03/omtptrustedenvironmentomtptr0v12.pdf sowie http://www.gsma.com/publicpolicy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf

ben der Anschaffung der Hard- und Software zusätzlich die technische Implementierung im Mobilfunknetz (Entwicklung, Test, Roll-Out) – dürfte sich auf ein Vielfaches davon belaufen.

- Gibt es Bedenken, gegen eine von einer deutschen Behörde administrierten CEIR, bei der die Geschädigten Ihre Gerätekennungen hinterlegen können?

Die zuvor bereits in der Antwort zu „Wird dem IMEI-Sperr-Verfahren eine Chance auf Realisierung eingeräumt“ beschriebenen Bedenken zur Sicherstellung der Rechtmäßigkeit eines Anliegens bestehen auch hier: Ist der Sperrantrag rechtmäßig? Wie wird sichergestellt, dass die Behörde eine rechtmäßige Entsperrung zulässt?

4.1.2. Kill-Switch

Vorab: Der Kill-Switch Begriff schließt verschiedene Funktionalitäten zum Schutz eines Endgeräts ein. Er fußt auf der von der CTIA publizierten freiwilligen Selbsterklärung[3] vom April 2014. Der Begriff „Option-Out“ im Zusammenhang mit der Bereitstellung der Kill-Switch Funktionen bezeichnet die Möglichkeit, die im Initialisierungsprozess des Geräts angebotene und vorab ausgewählte Aktivierung der entsprechenden Funktionen optional zu deaktivieren.

- Welche Ziele verfolgen die externen Experten zur Reduzierung der Fallzahlen?

In erster Linie steht der Schutz personenbezogener und vertraulicher Daten durch Verhinderung des Zugangs im Fokus der derzeitigen Lösungen. Die indirekte abschreckende Wirkung für potentielle Straftäter durch verhinderte Nachnutzung wird als Sekundärziel unterstützt.

- Wie lautet der aktuelle Sachstand zur Ausstattung mobiler Endgeräte mit einer Kill-Switch-Funktion?

Aktuelle Geräte werden mit Funktionen zum Wiederauffinden, Sperren und ggf. Löschen ausgestattet. Betriebssystem-spezifische Lösungen wie bei Apple oder Google sind für die meisten der jeweiligen ab 2010 ausgelieferten Geräte nutzbar. Werden die Sperren eingerichtet, können diese nur noch mit einem jeweils definierten Passwort aufgehoben werden. Damit macht es die Geräte für Dritte nutzlos.

- Wie lautet möglicherweise der kleinster gemeinsame nationale/internationale Nenner der Kill-Switch-Funktionalität?

Die freiwillige Abgabe einer Erklärung, entsprechende Funktionalitäten für die Nutzer verfügbar zu machen, erscheint als möglicher Vorschlag, der weitreichenden Konsens hervorrufen wird. Die in dieser Erklärung geoforderten Inhalte dürfen allerdings nicht über andere in der Welt gültige Erklärungen hinausgehen.

- Gibt es Bedenken gegenüber einer Option-Out-Lösung und welche Voraussetzungen müssen hierfür gegeben sein?

Der Initialisierungsprozess des Endgeräts würde sich verlängern, was zur Kundenunzufriedenheit beitragen würde. Eine spezielle Modifikation, die rein für Deutschland zu implementieren wäre, würde dazu führen, dass Endgeräte eher im Ausland gekauft würden, um einer vermeintli-

[3] siehe dazu http://www.ctia.org/policy-initiatives/voluntary-guidelines/smartphone-anti-theft-voluntary-commitment

chen Bevormundung zu entgehen. Weiterhin müssten Datenbanken auf eine solche Lösung hin erweitert werden, was Investitionen und steigende Betriebskosten mit sich bringt.

- Wäre eine Option-Out-Lösung mit einer Grundfunktionalität „Fernsperre“ denkbar?

Die Option-Out Implementierung einer Aktivierungsfunktion steht erst einmal nicht im direkten Zusammenhang mit den angebotenen Funktionalitäten. „Fernsperre“ könnte als eine dieser Funktionalitäten dann auch aktiviert werden.

- Wird die Kill-Switch-Funktionalität durch die Endgeräte- und/oder Betriebssystemhersteller gewährleistet?

Die Betriebssystemhersteller bieten Grundfunktionalitäten an, die es den Endgeräteherstellern ermöglichen, eine eigene Lösung darauf aufbauend zu entwickeln und den Nutzern die Möglichkeit geben, Sicherungsfunktionen des Betriebssystems direkt zu nutzen.

- Welche Zusatzfunktionalitäten müssen durch Drittanbieter geliefert werden?

Teilweise bieten die Hersteller eine derartige Lösung an. Wird vom Kunden, z.B. als Teil einer Firmenlösung, eine andere Implementierung gewünscht, so kann diese als App durch Drittanbieter realisiert werden.

- Gibt es die Möglichkeit einer nachträglichen Aktivierung der Kill-Switch-Funktion durch den Geschädigten?

Aktuell implementierte Sicherheitssysteme sind nicht im Falle eines Diebstahls (over the air) aktivierbar. Dies würde zu vielen Missbrauchsmöglichkeiten führen, da der physische Besitz des Geräts dann nicht mehr erforderlich ist, um Sperren zu ermöglichen.Solange der Nutzer im Besitz des Gerätes ist kann eine Aktivierung jederzeit nachgeholt werden. Dies verhindert auch einen Missbrauch z.B. nach dem Veräußern des Smartphones, siehe hierzu auch den Punkt IMEI-Sperre.

- Gibt es Überlegungen, die geografische Ortung via Mobilfunk oder IP-Adresszuordnung zu präzisieren?

Nein, dazu besteht keine Notwendigkeit. Die derzeitigen im Mobilfunknetzen angewandten Verfahren orientieren sich an dem technisch Notwendigen zum Betrieb der TK-Netze und zur Erfüllung der Notrufanforderungen. Ortungsfunktionalitäten zur Lokalisierung eines Geräts durch den Nutzer beziehen weiterhin Satelliten-gestützte Technologien wie GPS, GLONASS oder Beidou oder auch WLAN zur Ortung mit ein. Dies sorgt außerhalb von Gebäuden für metergenaue Ortung.

- Bedarf es zusätzlicher Regelungen im Telemedien- (TMG) oder Telekommunikationsgesetz (TKG)?

Wir bevorzugen eine freiwillige Selbstverpflichtung vergleichbar zur CTIA-Initiative.

- Bedarf es für eine Option-Out-Lösung einer rechtlichen Regelung „Verpflichtung Dritter“, um der Industrie einen Rechtfertigungsgrund gegenüber den Kunden zu geben?

o Welche Akteure müssen eingebunden werden?

BITKOM sieht eine Option-Out-Lösung, wie eingangs beschrieben, als relevante Informationsmaßnahme um den Nutzer auf Schutzmechanismen hinzuweisen. Die Verhinderung der Nachnutzung ist ein wirksames Mittel zur Abschreckung, wenn es mit entsprechenden Informationskampagnen hinterlegt ist. Die Nutzer und auch indirekt mögliche Diebe aufzuklären halten wir für effektiver, als rein technische Maßnahmen in der Anwendung zu erzwingen.
Beispiele für erfolgreiche Informationskampagnen sind im Vereinten Königreich oder den Niederlanden zu finden. Auch Österreich möchte mit einer solchen Kampagne in Kooperation mit den Mobilfunkunternehmen die Aufmerksamkeit für das Thema erhöhen.

- Welche Möglichkeiten gibt es, bereits im Bestand vorhandene mobile Endgeräte mit einer Kill-Switch-Funktion nachträglich auszustatten und welche Voraussetzungen müssen hierfür vorliegen?

Betriebssystem- und/oder Firmwareupdates ermöglichen, Geräte nachträglich mit den genannten Schutzmechanismen nachzurüsten. Für eine große Anzahl der in den letzten vier Jahren verkauften Geräte, die noch keine solchen Schutzfunktionen haben, wäre dies möglich. Weiterhin sind Software-Lösungen von Drittanbietern verfügbar, die es ermöglichen, entsprechende Funktionen auf Smartphones und Tablets zu nutzen.

- Welche Firmen sind dem „Smartphone Anti-Theft Voluntary Commitment“ beigetreten? -

Apple Inc.
Asurion
AT&T
Google Inc.
HTC America, Inc.
Huawei Device USA
LG Electronics MobileComm USA, Inc.
Motorola Mobility LLC
Microsoft Corporation
Nokia, Inc.
Samsung Telecommunications America, L.P.
Sprint Corporation
T-Mobile USA
U.S. Cellular
Verizon Wireless
ZTE USA, Inc.

- Welche Auswirkungen sind aufgrund der Entwicklungen in den USA für den europäischen Markt zu erwarten?

Es ist zu erwarten, dass die für den USA-Markt entwickelten Funktionalitäten auch auf dem europäischen Markt angeboten werden, da die Mehrheit der Endgerätehersteller Produktmerkmale für den gesamten Weltmarkt entwickelt und alle Geräte entsprechend ausstattet.

4.1.3. Weitere Möglichkeiten

- Wie bewerten Sie eine Passwortabfrage vor dem Bootloader?

- Wäre diese Option eine Alternative zur IMEI-Sperre und auch zum Kill-Switch Verfahren?
- Was spricht dagegen?

Das wäre keine Alternative, sondern ein anderer Ansatz, um den Diebstahl von mobilen Endgeräten unattraktiver zu gestalten. Zusammen mit einem Gerätepasswort, welches den Zugang zum Gerät im aktivierten Zustand erfolgreich verhindert, böte die Passwortabfrage vor dem Bootloader möglicherweise einen Schutz gegen eine Weiternutzung des Endgerätes durch Dritte.
Aus unserer Sicht ist die Option einer Passwort-Abfrage vor dem Bootloader nicht sinnvoll. Ein Passwort festzulegen, das die Gerätenutzung gänzlich unmöglich macht und gleichzeitig, falls es verloren geht, nicht umgangen oder zurückgesetzt werden kann (auch nicht durch berechtigte Personen) würde einer deutlich größeren Zahl an Endnutzern schaden, als es anderen hilft. Die Erfahrung in Service-Centern mit selten genutzten Passworten (z.B. der PUK bei SIM-Karten) zeigt, dass, auch wenn Kunden darauf hingewiesen werden, diese sicher zu verwahren, sie im Bedarfsfall sehr häufig nicht (mehr) zur Verfügung stehen und der Betroffene auf Hilfe durch eine jeweilige Hotline bzw. Kundenbetreuung angewiesen ist. Die Wahrscheinlichkeit, einen solchen Code künftig nicht mehr aufzufinden, wird dadurch erhöht, dass Bedienungsanleitungen immer häufiger online abgerufen werden und die abgedruckten Versionen immer seltener dauerhaft verwahrt werden. Auch der Weiterverkauf von Smartphones und Tablets wird für Privatpersonen schwieriger, da potentielle Käufer nicht sicher sein können, ob nun für ein angebotenes Gerät ein Bootloader-Passwort benötigt wird bzw. ob das korrekte weitergegeben wurde.

Zudem besteht die Gefahr, dass das Gefährdungspotential steigt, wenn nicht mehr „nur“ das Smartphone entwendet wird, sondern der Geschädigte zusätzlich zur Herausgabe des Bootloader-Passworts gezwungen wird.

Weiterhin sind wir der Meinung, dass der Implementierungsaufwand sowie die Bevormundung der Nutzer nicht dadurch zu rechtfertigen ist, dass ein Dieb das gestohlene Gerät nicht weiter verwenden kann – der Schaden für den Nutzer (im günstigen Fall der Aufwand der Wiederbeschaffung) entsteht dennoch.

- Welche weiteren Optionen halten Sie für geeignet, die Nachnutzung der durch Straftatenerlangten mobilen Endgeräte zu verhindern?
  Siehe hierzu die Inhalte der ersten Stellungnahme „Bund-Länder Projektgruppe „Smartphonesperre“ –Fragenkatalog vom 21. August 2014“ vom 03. September 2014[4].

4.2. Recht

- Liegen Ihnen bereits rechtliche Stellungnahmen zum IMEI- und/oder Kill-Switch-Verfahren vor, die der BLPG zur Verfügung gestellt werden können?

[4] zu finden unter http://www.bitkom.org/de/themen/54882_80372.aspx

Entsprechende Stellungnahmen liegen dem BITKOM nicht vor.

Fazit

BITKOM begrüßt die Aktivitäten der Innenministerkonferenz zur Reduzierung des Diebstahls von Smartphones und Tablets und der damit einhergehenden Förderung des Gemeinwohls. Die Zunahme der Zahl von Handys und Mobiltelefonen auf der INPOL Sachfahndungsliste Stehl-/Raubgut von 2012 auf 2013 um 70380 Stück regt zum Nachdenken an; gerade mit Bezug auf den monetären körperlich/seelischen Schaden den Opfer eines solchen Delikts erleiden.

Demgegenüber stehen ca. 38 Millionen im Jahr 2013 in Deutschland verkaufte Handys, Smartphones und Tablets. Jegliche Maßnahmen, die der Erhöhung der Raub- und Diebstahlzahlen entgegenwirken sollen, müssen daher auf ihre Verhältnismäßigkeit im Gesamtkontext geprüft werden.

Das IMEI-Sperrverfahren sehen wir aufgrund der hohen Implementierungskosten sowie der geringen Wirksamkeit als nicht geeignet für diese Zwecke an.
Die Implementierung eines Bootloader-Passworts würde sich deutlich negativ auf die Nutzerfreundlichkeit eines Endgeräts auswirken und erscheint uns daher nicht als geeignet.
Die Nutzung des Kill-Switch-Verfahrens im Sinne der kalifornischen Gesetzgebung bietet aufgrund der komfortablen Handhabung und der Verbreitung über alle führenden Endgerätehersteller hinweg die größten Chancen, eine Reduzierung von Diebstahlzahlen herbeizuführen. Die bereits bestehenden oder kurzfristig im Markt zu erwartenden Angebote der Endgerätehersteller bieten die Möglichkeit, sowohl persönliche Daten auf einem entwendeten Gerät unbrauchbar zu machen als auch in Verbindung mit entsprechenden Informationskampagnen für eine abschreckende Wirkung bei Kriminellen zu sorgen.
Gerne stehen verschiedene Endgerätehersteller der Bund-Länder Arbeitsgruppe zur Verfügung um die jeweilige Implementierung der Kill-Switch Funktionalitäten zu präsentieren und näher zu erläutern.