Leitfaden
zur Erstellung einer betriebsinternen
Telefonanweisung (Mobilfunk)

Die moderne Mobilfunktechnik beinhaltet auch ein immenses Gefährdungspotential im Bereich der illegalen Ausspähung von Unternehmen und Behörden. In diesem Zusammenhang wird auf die umfassenderen Hintergrundinformationen für die Erstellung einer betriebsinternen Telefonanweisung (Moblifunk) auf dem Geheimschutzserver (www.bmwi-sicherheitsforum.de - Bibliothek) verwiesen.

Nachfolgend soll nur auf die Schutzmaßnahmen gegen die bekannten Gefährdungen eingegangen werden, die in zwei Bereiche aufgeteilt wurden. Die allgemeinen Schutzmaßnahmen, die jeder Mobilfunkteilnehmer zum Schutz seiner Privatsphäre oder auch von firmenvertraulichen Angelegenheiten beachten sollte und die verbindlichen Regelungen für den Schutz von Verschlusssachen.

A: Allgemeine Schutzmaßnahmen

1. Allgemeines

Grundsätzlich gilt, dass Art und Umfang der Schutzmaßnahmen abhängig sind von der Gefährdungslage. Welche Maßnahmen im Einzelfall umgesetzt werden, liegt in der Verantwortung des Einzelnen.
Da aber oft auch leichtfertig mit der Abhörgefahr im Telekommunikationsbereich umgegangen wird, sollten Sicherheitsverantwortliche prüfen, inwieweit die bisherigen Maßnahmen zur Aufklärung ihrer Mitarbeiter über Gefährdungen im Telekommunikationssektor ausreichen.
Für den VS-Bereich müssen jedoch höhere Schutzmaßnahmen ergriffen werden.

2. Schutz vor Abhören von Telefonaten

Ein wirksamer Schutz gegen das Abhören von Telefonaten ist die interoperable, netzübergreifende Ende-zu-Ende-Verschlüsselung. Solange eine solche Verschlüsselung nicht realisiert ist, kann jede Verbindung, ob im Festnetz oder im Mobilfunknetz, potenziell abgehört werden.
Folgende Maßnahmen werden zur Verringerung der Gefährdung empfohlen:

- Grundsätzlich sollten ohne besondere Schutzmaßnahmen keine Telefongespräche mit sensiblem Inhalt geführt werden.
- Es sollten Geräte verwendet werden, die eine fehlende Verschlüsselung auf dem Display anzeigen.
- Im Bedarfsfall ist geschlossenen Benutzergruppen die Verwendung von speziellen kryptierenden Mobiltelefonen anzuraten. Für behördliche Benutzerkreise sei an dieser Stelle auf Kryptomobiltelefone mit VS-Zulassung hingewiesen.
- Einzelverbindungsnachweise sollten auf unbekannte Rufnummern hin überprüft werden.
- Ferner sollte geprüft werden, ob alle Gesprächsgebühren dem Teilnehmer in Rechnung gestellt wurden; fehlende Gebühren für bestimmte Verbindungen können auf Abhören hindeuten.

3. Schutz vor Abhören von Raumgesprächen

Schutz vor Abhören von Raumgesprächen mittels handelsüblicher Mobiltelefone

Das Abhören von Raumgesprächen mittels Mobiltelefonen kann nur dann sicher ausgeschlossen werden, wenn das Einbringen von Mobiltelefonen in den zu schützenden Raum verhindert wird.

Auf dem Markt sind passive Warngeräte (GSM-Mobiltelefon-Detektoren) verfügbar, die Mobiltelefone, die sich im Sendebetrieb befinden oder neu in Sendebetrieb gehen, melden. Der Wirkungsbereich der Geräte kann so eingestellt werden, dass er auf den zu überwachenden Bereich beschränkt ist. Es wird empfohlen, solche Warngeräte zu installieren und diese bei Gesprächen mit sensitivem oder vertraulichem Inhalt zu aktivieren.

Es gibt aktive Mobiltelefon-Detektoren, die alle in Reichweite befindlichen Mobiltelefone auffordern, in den Sendebetrieb zu gehen. Diese können wegen der fehlenden Betriebserlaubnis für Deutschland nicht empfohlen werden. Auch für Störsender, die in einem räumlich abgegrenzten Bereich den Funkbetrieb derart stören, dass dort kein Mobilfunkempfang möglich ist, gibt es in Deutschland keine Betriebsgenehmigung.

Schutz vor Abhören von Raumgesprächen mittels manipulierter Mobiltelefone

Zusätzlich ist zu beachten, dass das Ausschalten des Mobiltelefons als Schutz nicht ausreicht, da bei manipulierten Mobiltelefonen ein unbemerkter Übergang in den Sendebetrieb nicht mit hinreichender Sicherheit ausgeschlossen werden kann.

Das Risiko einer Manipulation kann vermindert werden, wenn der Kauf von Mobiltelefonen bei vertrauenswürdigen Stellen erfolgt, damit nicht schon beim Erwerb mit einer Manipulation gerechnet werden muss. Bei der Beschaffung größerer Stückzahlen sollte der Auftrag auf mehrere Anbieter aufgeteilt werden. Bei Manipulationsverdacht sollte das betroffene Mobiltelefon aus dem Verkehr gezogen werden.
Hardware-Manipulationen können sicher mit Röntgenprüfverfahren oder auch per Sichtprüfung nach Zerlegen des Gerätes erkannt werden. Derzeit existiert kein Prüfwerkzeug, mit dem die Software von Mobiltelefonen auf Manipulationen hin überprüft werden kann.

4. Schutz vor missbräuchlicher Datenweitergabe über GSM-Endgeräte

Schutz vor unberechtigter Datenweitergabe

Einen absoluten Schutz gegen Innentäter gibt es nicht. Daher ist es ratsam, die Mitnahme von Mobiltelefonen in sensitive Bereiche zu untersagen; die Umsetzung dieses Verbotes sollte überprüft werden.

Schutz vor ungewollter Datenweitergabe

Da Fälle von manipulierten Card-Phones nicht auszuschließen sind, sollten in PCs, auf denen sensitive Daten verarbeitet werden beziehungsweise die mit einem Rechner-Netzwerk verbunden sind**,** keine Mobilfunkkarten zugelassen werden.

Schutz vor SIM-Kartenmissbrauch

Das Mobiltelefon und die SIM-Karte sollten stets sicher aufbewahrt werden. Die persönliche Geheimzahl PIN sollte aktiviert bleiben und darf keinesfalls zusammen mit der zum Mobiltelefon gehörigen SIM-Karte aufbewahrt werden.
Bei Verlust der SIM-Karte sollte sofort beim Netzbetreiber eine Kartensperre veranlasst werden, um einen eventuellen Missbrauch - und damit auch einen persönlichen Schaden - abzuwehren.
Es ist empfehlenswert, Einzelverbindungsnachweise regelmäßig auf unerklärliche Gebühren und Zielrufnummern zu prüfen.

Schutz vor Erstellen von Bewegungsprofilen

Wird die Erstellung von Bewegungsprofilen als Gefährdung angesehen, dann sollten - falls umsetzbar - die Mobiltelefone und auch die SIM-Karten häufiger unter den Mitarbeitern getauscht werden. So wird eine Zuordnung der Geräte und Karten zu einem bestimmten Nutzer zumindest erschwert. Soll der Aufenthaltsort zu bestimmten Zeiten unentdeckt bleiben, hilft nur ein Ausschalten des Mobiltelefons. Um ganz sicher zu sein, sollte auch der Akku entfernt werden.

Schutz vor Rufnummernermittlung

Einen gewissen Schutz gegen die Zuordnung von Rufnummern zu bestimmten Personen gewährt der Austausch von Mobiltelefonen und SIM-Karten. Damit ist keine dauerhafte Zuordnung zwischen Benutzer und Rufnummer beziehungsweise Gerät und Nutzer möglich. Die Zuordnung zum Beispiel zu einer Firma bleibt aber bestehen. Weitere Möglichkeiten sind die Nichtveröffentlichung der Rufnummern im öffentlichen Telefonbuch und die Nichtveröffentlichung der Rufnummern im internen Telefonbuch.

5. Schutzmaßnahmen für die Nutzung zusätzlicher Dienste

Kurznachrichten-Dienste

Da es keine Möglichkeit gibt, den Empfang von SMS zu unterbinden, kann an dieser Stelle nur die Empfehlung ausgesprochen werden, die eigene Rufnummer nur vertrauenswürdigen Personen mitzuteilen.

M-Commerce und M-Payment sowie Virenproblematik

Hier gelten die allgemeinen Schutzmaßnahmen bei Nutzung des Internets und des Homebankings.

B: Regelungen für den Schutz von Verschlusssachen

Folgende Regelungen sind in einer betriebsinternen VS-Anweisung zu regeln

1. Die Nutzung von Phone-Cards für VS-zugelassene Notebooks bedarf der Genehmigung des BMWi. Voraussetzung der Genehmigung wäre in jedem Fall eine Verschlüsselung der Informationen nach vom BMWi zugelassenen Verfahren zwischen Sender und Empfänger.

2. Das Führen von Telefongesprächen, übermitteln von SMS, MMS oder anderer Daten mit VS-eingestuften Inhalten bedarf der Genehmigung des BMWi. Voraussetzung der Genehmigung wäre in jedem Fall eine Verschlüsselung der Informationen nach vom BMWi zugelassenen Verfahren zwischen Sender und Empfänger.

3. Das Einbringen von Handys in VS-Sperrzonen oder VS-Registraturen ist grundsätzlich untersagt. Ausnahmen sind in der jeweiligen Sperrzonenanweisung festzulegen, die der Einwilligung des BMWi bedarf. Die Einhaltung der Maßnahme ist vom SiBe durch Verwendung eines passiven Warngerätes (GSM-Mobiltelefon-Detektoren) regelmäßig zu überwachen. Zuwiderhandlungen stellen die Ermächtigung zum Zugang zu VS in Frage und sollten auch arbeitsrechtlich geahndet werden.

4. Zu Besprechungen von Mitarbeitern in Kontrollzonen oder Arbeitsräumen mit VS-eingestuften Inhalten dürfen keine Handys mitgenommen werden. Das Personal ist entsprechend zu belehren und zu verpflichten. Die Einhaltung ist ebenfalls zu kontrollieren (siehe vorstehende Nummer 3).

5. Zu Besprechungen mit größerem Personenkreis und externen Teilnehmern über VS-eingestufte Inhalte gilt ebenfalls das Verbot zur Einbringung von Handys in den Besprechungsraum. In der Besprechungseinladung und bei Empfang der Teilnehmer muss hierauf hingewiesen werden.

   Es empfiehlt sich eine Belehrungsanweisung für die Teilnehmer an der Besprechung zu erstellen.

   Es muss eine Aufbewahrungsmöglichkeit für mitgeführte Handys außerhalb des Besprechungsraumes vorgesehen (Sekretariat, Schließfächer usw.) und die Einhaltung der Maßnahme durch Verwendung eines passiven Warngerätes (GSM-Mobiltelefon-Detektoren) überwacht werden. Bei festgestellten Verstößen ist sofort der SiBe einzuschalten.
   Sind vorgesehene Teilnehmer nicht bereit, auf die Mitnahme ihres Handys zu verzichten, sind sie von der Besprechung auszuschließen. Der SiBe und das BMWi sind hierüber zu unterrichten.

6. Die vorstehend zu 2. bis 5. genannten Regelungen gelten insbesondere für Fotohandys, die u.U. auch bereits von der VS-Fotografieranweisung oder des betrieblichen Fotografierverbotes erfasst werden. Im Jahr 2003 wurden weltweit 55 Millionen Fotohandys verkauft. Diese Zahl ist gleich groß wie die der weltweit verkauften analogen oder digitalen Fotoapparate. Wegen der Möglichkeiten, die diese Technik mit sich bringt, verbieten viele Unternehmen weltweit aus Angst vor Industriespionage das Einbringen solcher Handys auf das Unternehmensgelände.
   Wegen der zusätzlichen besonderen Gefährdung durch solche Fotohandys ist deren Einbringung zu allen VS-Arbeitsplätzen grundsätzlich untersagt.