Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

[redacted]

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-0
FAX +49 (0) 228 99 9582-5400

Referat-B21@bsi.bund.de
https://www.bsi.bund.de

Betreff: Auskunft nach dem IFG

Bezug: Ihr Antrag vom 18.07.2015
Aktenzeichen: B21-010 03 05/001
Datum: 12.08.2015

Anlage: 1

Sehr gee[redacted]

auf Ihre Anfrage vom 18.07.2015 auf Informationszugang nach dem Informationsfreiheitsgesetz des Bundes (IFG) ergeht folgender

Bescheid:

Ihrem o.g. Antrag wird stattgegeben. Das von Ihnen angeforderte Merkblatt liegt diesem Schreiben als Anlage bei.

Rechtsbehelfsbelehrung:

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Widerspruch erhoben werden.

Bundesamt
für Sicherheit in der
Informationstechnik

Ich hoffe, dass ich Ihnen bei Ihrem Anliegen weiterhelfen konnte.

Mit freundlichen Grüßen

im Auftrag

[redacted]

Informiert bleiben

Merkblatt für den Umgang mit mobiler Informationstechnik, vorrangig in Ländern mit besonderem Sicherheitsrisiko

Vorbemerkungen

Das Merkblatt

- dient der persönlichen Sensibilisierung für reale Sicherheitsrisiken und
- sollte rechtzeitig vor Antritt der Reise aufmerksam gelesen werden.

Unter dem Begriff „mobile Informationstechnik" werden hier neben Notebook, Tablet, PDA, Handy und Smartphone auch Speichermedien wie USB-Sticks, Wechselfestplatten und CDs bzw. DVDs verstanden. Grundsätzlich müssen die Standards der IT-Sicherheit nach BSI-Grundschutz (www.bsi.bund.de) umgesetzt sein.

Insbesondere in Ländern mit besonderem Sicherheitsrisiko (siehe jeweils aktuelle BMI-Staatenliste) müssen Sie mit nachrichtendienstlichen Angriffen rechnen, wobei die mobile Informationstechnik besonderen Gefährdungen ausgesetzt ist.

Informieren Sie sich bei der Planung der Reise umfassend über Einschränkungen und Verbote des Gastlandes hinsichtlich des Umgangs mit mobiler IT (z.B. Handyverbot, Fotografierverbot) und befolgen Sie diese sehr gewissenhaft.

Wenn Sie beabsichtigen, ein Kryptogerät oder Produkte zur Verschlüsselung von Dateien, Festplatten, USB-Sticks, etc. mitzuführen, informieren Sie sich unbedingt über die diesbezüglichen gesetzlichen Bestimmungen im Gastland.

Die Risikosituation:

- Mobile Informationstechnik wird, sobald sie sich in ein Mobilfunknetz eingebucht hat, integraler Bestandteil der Kommunikationsinfrastruktur des Gastlandes und ist dann nahezu vollständig durch den Netzbetreiber kontrollierbar. Diese Tatsache kann auch aktiv für die nachrichtendienstliche Informationsbeschaffung genutzt werden.
- Eine nachhaltige und dauerhafte Manipulation der Geräte ist nicht auszuschließen, Risiken bei der Nutzung bestehen auch weiterhin nach Abschluss der Reise.
- Telekommunikationsinhalte können mitgehört oder -gelesen werden. Dies gilt sowohl für Festnetze als auch für Mobilfunknetze.
- Rechnen Sie auch damit, dass die kryptierte Kommunikation im Gastland möglicherweise unterbunden wird, um Sie zur Nutzung ungeschützter Verbindungen zu verleiten.
- Die zur Nutzung von Mobilfunknetzen erforderliche SIM-Karte verschafft dem

Mobilfunk-Netzbetreiber, von dem Sie die Karte erworben haben, einen direkten technischen Zugriff auf Ihr mobiles Gerät. Somit bestehen Möglichkeiten, den Funktionsumfang nahezu beliebig zu verändern oder zu erweitern. Dies geschieht drahtlos („over the air") und ist prinzipiell auch ohne Ihr Wissen und Zutun möglich.
Mögliche Schadfunktionen nach einer derartigen Veränderung sind:

- Mithören von Mobil-Telefonaten, Mitlesen von SMS, E-Mails bzw. des gesamten Datenverkehrs.
- Auslesen und Verändern aller gespeicherten Daten.
- Mithören von Gesprächen in der Umgebung.

- Manche Institutionen verlangen, dass mobile IT-Geräte von Besuchern an der Pforte abzugeben sind. Damit sind diese Geräte einem besonderen Manipulationsrisiko ausgesetzt. Lehnen Sie also entsprechende Bitten möglichst ab.
- Sobald Ihr mobiles Endgerät in ein Mobilfunknetz eingebucht ist, kann Ihr momentaner Standort leicht festgestellt werden. Berücksichtigen Sie dies in Ihrem Verhalten.

Empfehlung von IT-Sicherheitsmaßnahmen, die erkannte Risiken reduzieren

Vor Antritt der Reise:

- Reduzieren Sie die Mitnahme von mobilen IT-Geräten auf das absolut notwendige Maß.
- Wenn die Mitnahme eines mobilen IT-Gerätes unumgänglich ist, sollte dies nur nach sicherer Löschung aller nicht erforderlicher Daten zum Einsatz kommen.
- Es sollten nur Daten gespeichert sein, auf die Sie während der Reise nicht verzichten können.
- Auf den Geräten sollte möglichst eine Speicher- bzw. Festplattenverschlüsselung installiert sein; beachten Sie dabei jedoch die Vorschriften des Gastlandes.
- Deaktivieren Sie alle drahtlosen Schnittstellen von mobilen Geräten, die nicht zwingend benötigt werden (z.B. Bluetooth und Infrarot).
- Nutzen Sie immer eine SIM-Karte eines deutschen Netzbetreibers.
- Es empfiehlt sich, für die Reise ein preiswertes Handy zu erstehen, welches anschließend entsorgt oder für unkritische Anwendungen genutzt werden kann.

Während der Reise:

- Lassen Sie Ihre mobilen IT-Geräte niemals aus den Augen.

- Keine unbeaufsichtigte Ablage von mobilen IT-Geräten, auch nicht im Hotelzimmer oder im Hotelsafe.
- Vermeiden Sie Situationen, bei denen Sie Ihre mobilen IT-Geräte abgeben müssen. Ist dies unvermeidlich oder kommen Sie überraschend in eine solche Situation, schalten Sie die Geräte auf jeden Fall aus. Sie müssen dann dennoch mit einer dauerhaften Manipulation Ihrer Geräte rechnen.
- Verwenden Sie stets Bildschirmschoner mit Passwort-Abfrage.
- Verzichten Sie möglichst auf den Komfort drahtloser Schnittstellen von mobilen Geräten (z.B. Infrarot, Bluetooth).
- Erwerben Sie keine SIM Karte im Gastland.
- Vergewissern Sie sich, dass stets die vierstellige PIN zum Schutz der SIM-Karte aktiviert ist.
- Je weniger Sie die elektronische Kommunikation nutzen, desto besser.
- Kommunizieren Sie keinesfalls sicherheitskritische Informationen über ungeschützte Kanäle. Üben und praktizieren Sie im Alltag Sprechdisziplin.
- Kommunizieren Sie als Verschlusssache eingestufte Informationen ausschließlich über vom BSI zugelassene Kryptogeräte.
- Nutzen Sie nur eigene Kommunikationsmittel.
- Beachten Sie alle Einschränkungen und Verbote des Gastlandes konsequent und nachhaltig.

Nach Abschluss der Reise:

- Mobile Informationstechnik sollte von Grund auf neu installiert werden.
- Nach Rückkehr sollte die SIM-Karte möglichst nicht mehr benutzt werden.
- Sie sollten ein mitgeführtes mobiles IT-Gerät nicht mehr für sicherheitskritische Zwecke nutzen.

Bieten Sie durch Ihr Verhalten den örtlichen Sicherheitskräften keinen Anlass zur Beschlagnahme Ihrer IT-Geräte. Ein besonders umsichtiges und risikobewusstes Verhalten vor, während und nach der Reise ist unbedingt erforderlich - Risiken können dadurch erheblich reduziert werden.

Kontakt

Sollten Sie Beratungsbedarf haben, steht Ihnen das Beratungsreferat des BSI gerne zur Verfügung:

E-Mail: Sicherheitsberatung@bsi.bund.de
Web: https://www.bsi.bund.de/Sicherheitsberatung
Telefon: 0228 99 9582 - 333