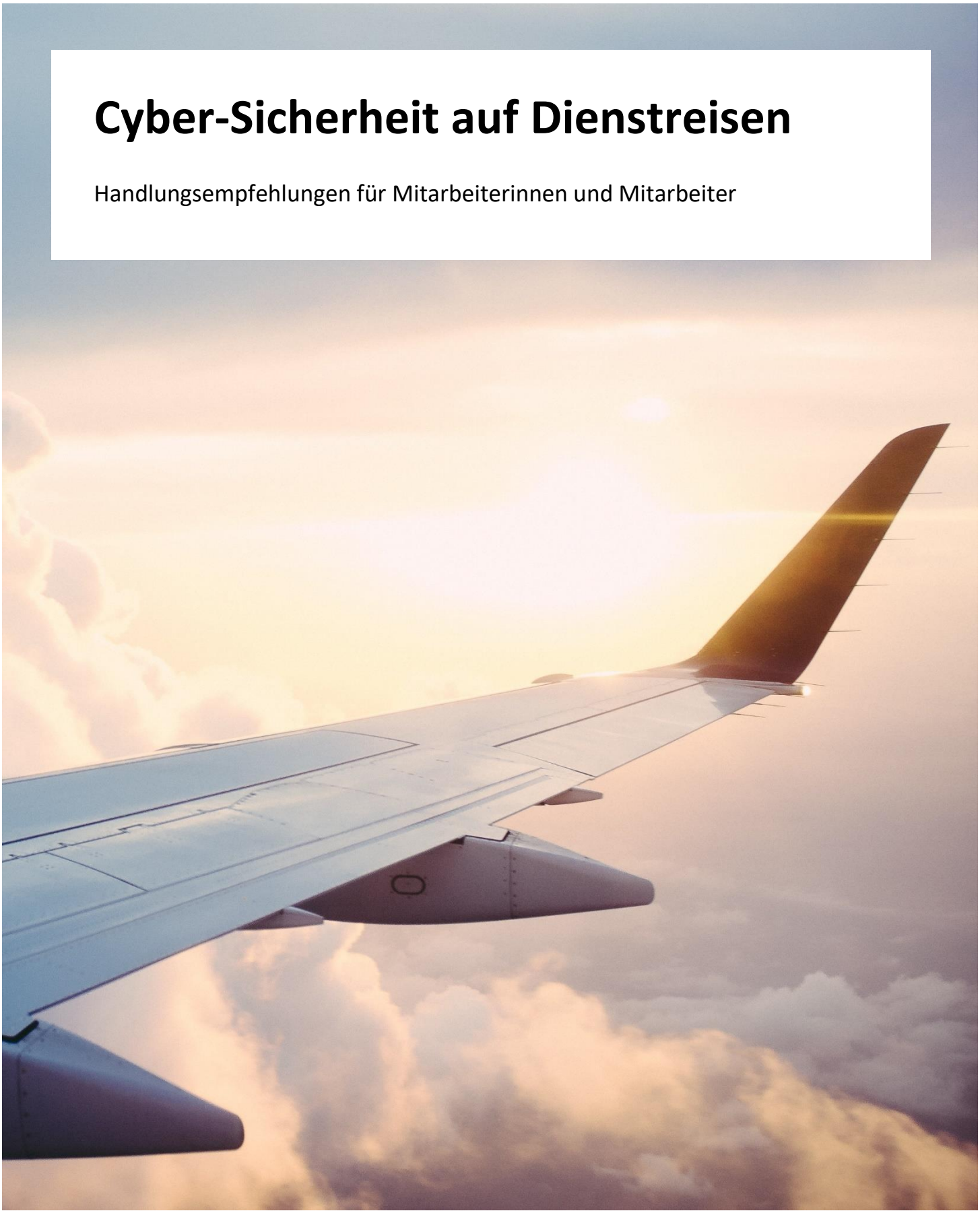
Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Cyber-Sicherheit auf Dienstreisen

Handlungsempfehlungen für Mitarbeiterinnen und Mitarbeiter



Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Herrengasse 7, 1010 Wien
bvt.gv.at
Autor: Cyber Security Center - Bereich Prävention
Druck: Digitalprintcenter des BMI

Überarbeitete Neuauflage
Wien, Juli 2020

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an csc@bvt.gv.at.

Cyber Security .BVT
Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Vorwort


Philipp Blauensteiner

Postindustrielle Gesellschaften und hochentwickelte Staaten nutzen mehr denn je den Cyber-Raum für ihre technische, wirtschaftliche, soziale, kulturelle, wissenschaftliche und politische Entwicklung. Öffentliche und private Einrichtungen, die der Daseinsvorsorge der Bevölkerung dienen, sind dabei zunehmend von einer funktionierenden Informations- und Kommunikationstechnik (IKT) abhängig. Ein nachhaltiger Schutz vor Bedrohungen aus dem Cyber-Raum kann jedoch nicht von einer einzelnen Entität sichergestellt werden. IKT-Abteilungen, das Management, aber auch die Mitarbeiterinnen und Mitarbeiter in allen Bereichen sind gleichsam die Säulen, auf denen die Sicherheit ruht. Gemeinsamer Erfolg ist dabei nur möglich, wenn im Falle eines Angriffs alle Säulen Bestand haben. Oder, anders formuliert, Cyber-Sicherheit ist niemals nur die Aufgabe anderer.

Gerade auf Dienstreisen ist jeder und jede Einzelne gefordert, einen eigenen Betrag zur Cyber-Sicherheit zu leisten. Das vorliegende Dokument versucht, eine Bewusstseinsbildung (Awareness) bei denjenigen Mitarbeiterinnen und Mitarbeitern zu erreichen, die im Rahmen ihrer Tätigkeit Dienstreisen unternehmen. Ziel ist, durch entsprechendes Wissen über mögliche Angriffsszenarien und Kenntnis über häufig genutzte Angriffsvektoren, eine nachhaltige Veränderung im Umgang mit diesen Gefahren zu bewirken. Zu diesem Zweck werden grundlegende Verhaltensweisen und vielfältige Handlungsempfehlungen zu allen Aspekten von Cyber-Sicherheit auf Dienstreisen dargestellt.

Das vorliegende Dokument wurde vom Cyber Security Center im Bundesministerium für Inneres erstellt. Die Anregung zur Erstellung erfolgte vom Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK). Der IKDOK ist ein staatliches Gremium, das primär auf Basis des Netz- und Informationssicherheitsgesetzes (NISG) agiert. Dem Gremium gehören staatliche Akteure aus dem Bundeskanzleramt, dem BMI, dem BMLV sowie dem BMEIA an.

Philipp Blauensteiner
Leiter des Cyber Security Centers

Inhalt

1 Vor der Dienstreise

„Wer vorsieht, ist Herr des Tags.“ (Johann Wolfgang von Goethe)

„Manche planen, um nicht zu versagen. Andere versagen, weil sie nicht planen.“ (Peter E. Schuhmacher)

Um ein ausreichendes Maß an Cyber-Sicherheit auch im Verlauf von Dienstreisen sicherstellen zu können, ist es erforderlich, bereits vor Reiseantritt einige Überlegungen anzustellen und eine Reihe von vorbereitenden Maßnahmen zu setzen.

1.1 Geräteauswahl

Elektronische Geräte sind im Zuge von Dienstreisen hinsichtlich der Sicherstellung von Cyber-Sicherheit erhöhten Risiken ausgesetzt. Dies betrifft grundsätzlich alle elektronischen Geräte. Besonders gefährdet sind Notebooks, Tablet-Computer, Mobiltelefone, Datenträger wie externe Festplatten und USB-Speichersticks, E-Book-Reader, Fotoapparate, MP3-Player und Smartwatches, die sensible Informationen bzw. Daten enthalten.

Größtmögliche Cyber-Sicherheit kann dadurch erreicht werden, dass man Geräte und Datenträger mit sensiblen Inhalten erst gar nicht auf die Reise mitnimmt. Es ist daher sinnvoll, bereits vor Reiseantritt zu überlegen, welche Daten (und daraus abgeleitet, welche Gegenstände) für die erfolgreiche Durchführung der Reise unbedingt erforderlich sind. Nur diese sollten mitgenommen werden. Das schließt die Überlegung mit ein, ob man bestimmte „smarte“ Geräte des Alltags während der Dienstreise überhaupt benötigt (z. B. Smartwatch).

Eine sinnvolle Option könnte auch sein, statt der eigenen Geräte dedizierte Dienstreisegeräte zu verwenden (z. B. Dienstreisetelefon), die von Haus aus auf die minimal erforderliche Funktionalität reduziert sind. Bei Verlust oder Diebstahl kommt so im Wesentlichen nur der Materialwert zum Tragen.

Inwieweit der Einsatz dedizierter Dienstreisegeräte mit den Zielsetzungen der Dienstreise in Einklang zu bringen ist, muss im Einzelfall bewertet werden.

Wir empfehlen:

- Nehmen Sie nur die elektronischen Geräte und Datenträger auf Dienstreisen mit, die Sie für eine erfolgreiche Durchführung der Reise unbedingt benötigen.
- Überlegen Sie, ob Sie bestimmte „smarte“ Geräte des Alltags (z. B. Smartwatch) während der Dienstreise überhaupt benötigen.
- Prüfen Sie im Einzelfall, ob für die Zielsetzung der Dienstreise die Mitnahme von dedizierten Dienstreisegeräten ausreichend ist.

1.2 Gerätesicherheit

Die Sicherheit, sowohl von dienstlichen wie auch privaten Daten, die in mobilen Endgeräten oder Cloud-Services gespeichert und verarbeitet werden, ist im Wesentlichen durch drei Faktoren bestimmt, nämlich der Vertraulichkeit, der Integrität und der Verfügbarkeit dieser Daten sowie der Dienste und Netzwerke, die benutzt werden. In diesem Sinne erscheint es sinnvoll, die mitgeführten Geräte schon vor Reiseantritt in Bezug auf Cyber-Sicherheit bestmöglich zu konfigurieren.

Wir empfehlen:

- Machen Sie sich mit den Sicherheitsfunktionen aller Ihrer elektronischen Geräte bereits vor Reiseantritt vertraut.
- Aktivieren Sie die Vollverschlüsselung aller elektronischen Geräte und Datenträger, bei denen diese Funktionalität möglich ist (z. B. Bitlocker bei Microsoft Windows, File-Vault bei MacOS).
- Wählen Sie eine geeignete Bildschirmsperre (z. B. Passphrase) und aktivieren Sie diese.
- Deaktivieren Sie die WLAN- und die Bluetooth-Schnittstelle immer dann, wenn sie nicht benötigt wird.
- Deaktivieren Sie, soweit dies möglich ist, das automatische Verbinden mit bereits bekannten oder mit unverschlüsselten WLAN-Zugangspunkten.

- Entfernen Sie alle gegebenenfalls im Browser oder in einer Anwendung gespeicherten Passwörter (z. B. für VPN-Verbindungen oder E-Mail-Postfächer).

Kennwortsicherheit

Kennwortsicherheit ist ein zentrales Thema im Zusammenhang mit Cyber-Sicherheit. Kennwörter sind nach wie vor die mit Abstand häufigste Authentifizierungsmethode und damit von großer Bedeutung. Insbesondere auf Dienstreisen muss sichergestellt sein, dass alle mitgeführten elektronischen Geräte mit einem geeigneten Kennwort abgesichert sind.

Grundsätzlich gilt, dass die Sicherheit eines Kennworts mit steigender Länge und Komplexität zunimmt (sofern der Benutzer noch in der Lage ist, sich das entsprechende Kennwort zu merken). Kennwörter in sensiblen Bereichen sollten derzeit eine Mindestlänge von 12 Stellen bei ausreichend hoher Komplexität (d. h. Klein- und Großbuchstaben, Ziffern, Sonderzeichen) aufweisen.

Es dürfen keinesfalls Kennwörter verwendet werden, die als schwach bzw. unsicher eingestuft werden. Dazu zählen insbesondere Kennwörter mit mangelnder Kennwortlänge oder -komplexität, Kennwörter, die in „Listen“ jedweder Art enthalten sind (z. B. Wörterbücher, Kennwortlisten aus dem Internet), Kennwörter mit sprechenden Schemata und vor allem Kennwörter, die im Vorfeld recherchiert werden könnten (z. B. Namen von Partnern, Kindern oder Haustieren, Kosenamen, Geburtsdaten oder Auto- bzw. Telefonnummern).

Für viele Menschen ist es trotz der Verwendung von Merktechniken wie Schlüsselsätzen sehr schwierig, sich für unterschiedliche Accounts mehrere individuelle Kennwörter zu merken. Eine Möglichkeit, diesem Problem entgegen zu wirken, kann die Verwendung von Programmen zur Kennwortverwaltung (Password Safes) sein. In diesem Fall ist die Sicherheit des verwendeten Master-Kennworts für die Sicherheit aller eingegebenen Accounts relevant. Das Master-Kennwort muss daher besonders gewissenhaft gewählt werden. Bei Dienstreisen sollte darauf geachtet werden, dass im Password Safe nur die während der Reise unbedingt benötigten Zugangsdaten gespeichert sind.

Eine Authentifizierung, also der Nachweis der eigenen Identität gegenüber einem beliebigen System, kann grundsätzlich auf drei verschiedenen Faktoren beruhen: Etwas, das ich

weiß (z. B. Kennwort), etwas, das ich habe (z. B. Keycard) oder etwas, das ich bin (z. B. Fingerabdruck). Die Mehrfaktor-Authentifizierung, also die zwingende Verwendung von zwei oder mehr Faktoren für einen einzelnen Anmeldevorgang, erhöht die Sicherheit des Authentifizierungsvorgangs erheblich und sollte daher überall dort genutzt werden, wo sie zur Verfügung steht.

Alle Arbeiten an einem System sollten, insbesondere auf Dienstreisen, immer nur mit den für die jeweilige Aufgabe unbedingt erforderlichen Berechtigungen durchgeführt werden. Dies ist insbesondere für hochprivilegierte Accounts (z. B. Administratoren) von großer Bedeutung. Es sollte daher sichergestellt werden, dass der während der Dienstreise verwendete Account nur mit dem minimal erforderlichen Set an Berechtigungen ausgestattet ist.

Wir empfehlen:

- Stellen Sie sicher, dass alle elektronischen Geräte, die auf die Dienstreise mitgenommen werden, über ein starkes Kennwort verfügen.
- Überlegen Sie, ob Sie alle während der Dienstreise zu benutzenden Kennwörter kennen oder gegebenenfalls einen ausreichend abgesicherten Password-Safe mitführen.
- Aktivieren Sie, wo immer das möglich ist, Mehrfaktor-Authentifizierung.
- Stellen Sie sicher, dass während der Dienstreise verwendete Accounts nur über das jeweils erforderliche Minimum an Berechtigungen verfügen.

Sicherheits-Updates

Programmierfehler in Softwareprodukten können von findigen Hackern für Angriffe auf das zugrundeliegende System ausgenutzt werden. Ein simpler Programmfehler kann zu einer Sicherheitslücke werden. Softwarehersteller versuchen (mit unterschiedlichem Engagement), Programmfehler und Sicherheitslücken zu korrigieren und durch die Verteilung von Sicherheits-Updates zu entschärfen.

Der einzige Schutz vor Gefahren durch Sicherheitslücken ist, diese so weit wie möglich aus dem System zu entfernen. Dies kann aus Benutzersicht nur durch das gewissenhafte, zeitnahe Einspielen aller verfügbaren Sicherheits-Updates erfolgen.

Darüber hinaus ist zu beachten, dass Softwarehersteller nur für einen begrenzten Zeitraum Ressourcen zur Verbesserung von Sicherheitslücken zur Verfügung stellen. Sicherheitslücken, die nach diesem Zeitraum entdeckt werden, bleiben bestehen und stellen von da an ein permanentes Risiko dar. In vernetzten Systemen sollte daher grundsätzlich keine Software eingesetzt werden, die vom Hersteller nicht mehr mit Sicherheits-Updates versorgt wird (Out-of-Support-Phase).

Wir empfehlen:

- Stellen Sie vor Reiseantritt sicher, dass sich alle mitgeführten Systeme am jeweils letztverfügbaren Softwarestand befinden.
- Setzen Sie grundsätzlich (und insbesondere während Dienstreisen) keine Software ein, die vom Hersteller nicht mehr mit Sicherheits-Updates versorgt wird.

1.3 Zubehör

Elektronische Geräte benötigen in der Regel eine Reihe von Zubehörteilen – zumindest ein Ladegerät. Vor Reiseantritt sollten unbedingt Überlegungen angestellt werden, welches Zubehör zu einer uneingeschränkten Nutzung der Geräte erforderlich ist. Es muss sichergestellt werden, dass diese Gegenstände vollständig und funktionstüchtig vorhanden sind.

Zu diesen Gegenständen zählen unter anderem:

- USB-Schnittstellenadapter (z. B. USB-RJ45, USB-VGA),
- externe Kommunikationsgeräte (z. B. 3G/4G-Modem, WLAN-Stick),
- Videoadapter (z. B. miniDP-HDMI, HDMI-VGA),
- Ladegräte und Netzteile.

Weitere Zubehörteile, die nicht vergessen werden sollten sind Display-Blickschutzfolien, Verbindungskabel (z. B. Mobiltelefon-Notebook) oder Kensington-Schlösser.

Hintergrund dieser Überlegung ist, dass erforderliche Geräte, die nicht mitgenommen wurden, in der Regel vor Ort ausgeliehen werden müssen. Bei einer Reihe von Zubehörteilen (vor allem USB-Geräte und externe Kommunikationsgeräte) besteht die Möglichkeit einer

Manipulation der fremden Gegenstände durch Dritte. Auf diese Art kann eine Kompromittierung des eigenen Gerätes durchgeführt werden.

Wir empfehlen:

- Überprüfen Sie vor Reiseantritt, ob alle für die Nutzung elektronischer Geräte erforderlichen Zubehörteile vollständig vorhanden und funktionstüchtig sind.
- Stellen Sie sicher, dass alle diese Gegenstände mitgenommen werden.

1.4 Verfügbarkeit von Daten und benötigten Diensten

In manchen Ländern wird aus (sicherheits-)politischen oder wirtschaftlichen Interessen der freie Zugang zum Internet bzw. zu bestimmten Diensten im Internet eingeschränkt oder vollständig unterbunden. Daher kann es vorkommen, dass während einer Dienstreise keine Verbindung zum Internet aufgebaut werden kann, eine VPN-Verbindung nicht zustande kommt oder der Zugriff auf bestimmte Seiten oder Daten (z. B. in einem Cloud-Dienst) nicht möglich ist.

Es erscheint daher sinnvoll, sich entsprechend auf solche Szenarien vorzubereiten. Der Erfolg einer Dienstreise sollte nicht vom Vorhandensein dieser Elemente abhängig sein.

Wir empfehlen:

- Planen Sie ein, dass Sie während der Dienstreise gegebenenfalls ohne Verbindung ins Internet arbeiten müssen.
- Stellen Sie sicher, dass alle benötigten Daten auf Ihren mitgeführten Geräten sicher verfügbar sind.
- Sollten sich benötigte Daten normalerweise ausschließlich in einem Cloud-Speicher befinden, kopieren Sie diese auf Ihr elektronisches Gerät und überprüfen Sie vor Reiseantritt, ob diese dann tatsächlich auch im Offline-Betrieb zur Verfügung stehen.

1.5 Entfernung nicht benötigter Daten

Wie bereits ausgeführt, sollte sichergestellt werden, dass ausschließlich diejenigen Geräte und Datenträger auf eine Dienstreise mitgenommen werden, die für die Reise unbedingt erforderlich sind. Ist festgelegt, welche Gegenstände mitgenommen werden, empfiehlt es sich, alle Daten, die nicht während der Reise benötigt werden, von diesen Gegenständen zu entfernen, um so den Schaden bei Verlust oder Diebstahl zu minimieren. Stellen Sie zuvor sicher, dass die zu entfernenden Daten an einem anderen Ort sicher gespeichert sind.

Auch beim Grenzübertritt (Details siehe Folgekapitel) erscheint es empfehlenswert, nur ein Minimum an sensiblen Daten auf mitgeführten Geräten oder Datenträgern zu transportieren.

Bei der Löschung ist zu beachten, dass Daten, die mit einem gängigen Betriebssystem (z. B. Microsoft Windows) gelöscht werden, in der Regel bis auf Weiteres trotzdem noch immer auf dem Datenträger enthalten sind, auch wenn das Betriebssystem beim Leeren des Papierkorbs davor warnt, dass diese Daten nun unwiderruflich verloren seien. Solange der betreffende Speicherplatz nicht mit einer anderen Datei überschrieben wurde, können solcherart gelöschte Daten mit geeigneten Anwendungen leicht wieder rekonstruiert werden.

Es ist daher im Interesse der Datensicherheit darauf zu achten, dass der Löschvorgang wirklich unwiderruflich durchgeführt wird. Dies kann mit Hilfe geeigneter Programme bewerkstelligt werden.

Wir empfehlen:

- Entfernen Sie alle nicht benötigten Daten von den Geräten und Datenträgern, die Sie während der Dienstreise mitführen. Stellen Sie zuvor sicher, dass die zu entfernenden Daten an einem anderen Ort sicher gespeichert sind.
- Stellen Sie sicher, dass die solcherart gelöschten Daten mit Hilfe geeigneter Programme wirklich unwiderruflich vom jeweiligen Datenträger entfernt wurden.

1.6 Bereinigung elektronischer Geräte und sozialer Medien

In bestimmten Regionen der Erde sind Freiheitsrechte erheblich eingeschränkt. Dienstreisen in solche Länder stellen daher eine besondere Herausforderung für die Cyber-Sicherheit von mitgeführten Geräten und Datenträgern dar. Es erscheint sinnvoll, in Abhängigkeit von den rechtlichen Rahmenbedingungen im Reiseland, bestimmte Vorkehrungen zu treffen, um den Erfolg der Dienstreise nicht durch diesbezügliche Schwierigkeiten zu gefährden.

Insbesondere sollte darauf geachtet werden, ob auf mitgeführten Geräten oder Datenträgern Inhalte gespeichert sind, die rechtlichen Vorschriften des Reiselandes widersprechen. Solche Inhalte sollten unbedingt vor Reiseantritt entfernt werden. Besonders in diesem Bereich ist auf eine unwiderrufliche Löschung der Daten zu achten. Beispiele für mögliches Konfrontationspotenzial sind etwa im Reiseland verbotene Schriften und Bücher, die beispielsweise am E-Reader gespeichert sind. Auch die Mitnahme von pornografischem oder homoerotischem Datenmaterial kann zu ernsthaften Konsequenzen führen.

In der privaten Nutzung sozialer Medien sollte darauf geachtet werden, ob aktuelle, aber auch ältere Postings den politischen, religiösen oder weltanschaulichen Vorschriften oder Einstellungen des Reiselandes zuwiderlaufen oder diese kritisieren. Es erscheint sinnvoll, auch bei den sozialen Medien vor Reiseantritt eine Bereinigung durchzuführen und Postings, die potenziell zu Schwierigkeiten führen könnten, zu entfernen. Eine Entfernung der Postings vor Reiseantritt ist keine Gewähr dafür, dass die Behörden des Reiselandes nicht Kenntnis darüber erlangen können.

Wir empfehlen:

- Entfernen Sie vor Reiseantritt (unwiderruflich) alle Daten von mitgeführten Geräten aller Art, die den Vorschriften des Reiselandes widersprechen.
- Entfernen Sie vor Reiseantritt (so gut dies für Sie möglich ist) alle Postings auf sozialen Medien, die politischen, religiösen oder weltanschaulichen Vorschriften oder Einstellungen des Reiselandes zuwiderlaufen.

1.7 Herstellung von Sicherheitskopien

Daten auf mitgeführten Geräten und Datenträgern sind während einer Dienstreise hinsichtlich der physischen Sicherheit, der Möglichkeit von Verlust oder Diebstahl sowie auch hinsichtlich der Gefahr einer Infektion mit Schadsoftware einem erhöhten Risiko ausgesetzt.

Um sich vor einem vollständigen Verlust wertvoller Daten im Falle von Verlust oder Diebstahl bzw. nach einer möglichen Infektion mit Schadsoftware zu schützen, ist es erforderlich, unmittelbar vor Reiseantritt eine Sicherheitskopie (Back-up) aller mitgeführten Daten vorzunehmen. Dabei ist zu bedenken, dass es sich dabei nicht ausschließlich um einzelne Dateien (z. B. Word-Dokumente) handelt, sondern, dass auch andere Daten, wie beispielsweise lokal am Gerät eingerichtete E-Mail-Postfächer und dergleichen gesichert werden sollten.

Stellen Sie vor Reiseantritt sicher, dass die Sicherheitskopie ordnungsgemäß und vollständig durchgeführt wurde und dass eine Wiederherstellung gegebenenfalls problemlos möglich ist. Fehlerhafte Back-ups führen im Bedarfsfall unter Umständen zu einem vollständigen Datenverlust.

Verwahren Sie die Sicherheitskopie an einem sicheren Ort und stellen Sie sicher, dass sich die gesicherten Daten nicht im direkten permanenten Zugriff eines anderen Systems befinden. Nehmen Sie die Sicherungsmedien keinesfalls auf die Dienstreise mit.

Wir empfehlen:

- Stellen Sie vor Reiseantritt Sicherheitskopien aller mitgeführten Daten her.
- Überprüfen Sie, ob die Sicherheitskopien ordnungsgemäß durchgeführt wurden und ob gegebenenfalls eine Wiederherstellung problemlos möglich ist.
- Verwahren Sie die Sicherheitskopien an einem sicheren Ort und nehmen Sie diese keinesfalls auf die Dienstreise mit.

1.8 Persönliche und soziale Kontakte

Vielen Menschen ist es ein Anliegen, Details über das eigene Leben im privaten Bereich persönlich oder über soziale Medien zu kommunizieren. Im Zusammenhang mit Dienstreisen erscheint es ratsam, jede über den engsten Familienkreis hinausgehende, private Kommunikation über Tatsache, Dauer und Inhalt der Abwesenheit zu vermeiden.

Im Hinblick auf soziale Medien darf nicht vergessen werden, dass eine bekannt gegebene Information einer Veröffentlichung gleichkommt und auch jeder potenzielle Angreifer zielgerichtet darauf zugreifen kann. Detailinformationen zu etwaigen Dienstreisen können einem Angreifer bei der Vorbereitung und Durchführung von Social-Engineering-Angriffen helfen.

Davon unabhängig sollte bedacht werden, dass jede diesbezügliche Information – vor oder auch während einer Reise – auch im privaten Bereich ein erhebliches Risiko darstellt. So werden immer wieder vermeintlich harmlose Postings über geplante oder gerade im Gange befindliche Reisen bzw. Abwesenheiten von Kriminellen genutzt, um geeignete Zeitpunkte für Wohnungs- bzw. Eigenheimeinbrüche festzulegen.

Diese Empfehlungen erstrecken sich auch auf etwaige Taxifahrten (z. B. zum Flughafen). Oft werden Taxilenkern gedankenlos detaillierte Informationen zu Dauer und Ziel von Reisen mitgeteilt. Die Abholung unmittelbar vor dem Eigenheim ergänzt diese Informationen noch um die genaue Anschrift. In der Vergangenheit wurden bereits mehrfach solche Daten von schwarzen Schafen unter den Taxilenkern an professionelle Einbrecherbanden weitergegeben.

Wir empfehlen:

- Vermeiden Sie jede über den engsten Familienkreis hinausgehende private Kommunikation über Tatsache, Dauer und Inhalt von Dienstreisen (oder sonstigen Abwesenheiten).
- Vermeiden Sie vor oder während Abwesenheiten eine Veröffentlichung diesbezüglicher Informationen auf sozialen Medien.
- Vermeiden Sie gedankenlose Informationsweitergabe an Taxilenker und lassen Sie sich gegebenenfalls nicht unmittelbar von Ihrer Anschrift (sondern z. B. von der nächsten Straßenecke) abholen.

Abwesenheitsassistent

Obwohl die Nutzung des E-Mail-Abwesenheitsassistenten zweifelsfrei eine Reihe von Vorteilen bietet, erscheint es trotzdem empfehlenswert, die darin enthaltenen Informationen sorgsam zu überlegen. Die Verwendung (vor allem des externen) Abwesenheitsassistenten stellt die darin enthaltenen Daten de facto jedermann zur Verfügung, was einer Veröffentlichung gleichkommt.

Alleine die Tatsache, dass eine Abwesenheitsnachricht ausgesandt wird, ist für einen Angreifer von erheblichem Wert. Ein potenzieller Angreifer, der die Struktur der E-Mail-Adressen einer Organisation noch nicht kennt, kann diese durch wiederholtes Senden von E-Mail-Adressvariationen vergleichsweise einfach herausfinden. Doch auch wenn die Struktur bekannt ist, kann ein aktivierter Abwesenheitsassistent dazu benutzt werden, zu bestätigen, dass die verwendete E-Mail-Adresse wirklich gültig ist.

Gleichzeitig stellen viele der normalerweise in Abwesenheitsassistenten bekannt gegebenen Daten für einen Angreifer wertvolle Informationen dar, die für die Vorbereitung und Durchführung von Social-Engineering-Angriffen genutzt werden können. In vielen dieser Nachrichten sind Informationen wie Grund der Abwesenheit, Dauer der Abwesenheit, Dienstreiseziel, Name und Kontaktdaten des Vorgesetzten, der Vertretung oder des Sekretariats, gegebenenfalls Zuordnung von Aufgaben zu Personen im Unternehmen („bei Fragen zum Thema x rufen Sie bitte y“) und vieles mehr enthalten.

Wir empfehlen daher grundsätzlich, entweder auf die Nutzung (zumindest des externen) Abwesenheitsassistenten generell zu verzichten oder die Menge der enthaltenen Informationen möglichst zu beschränken. Etwaige diesbezügliche Maßnahmen müssen natürlich stets im Einklang mit eventuell bestehenden firmeninternen Richtlinien stehen.

Wir empfehlen:

- Verzichten Sie nach Möglichkeit generell auf den Einsatz (zumindest des externen) Abwesenheitsassistenten.
- Überlegen Sie, welche der beabsichtigten Inhalte des Abwesenheitsassistenten einem potenziellen Angreifer Vorteile verschaffen würden und verzichten Sie zumindest auf die Bekanntgabe dieser Informationen.

2 Während der Dienstreise

„Vorsicht ist einfach, Reue vielfach.“ (unbekannt)

„Incustoditum captat ovile lupus. (Der Wolf trachtet nach einem unbewachten Schafstall.)“ (Ovid)

2.1 Rechtliche Lage beim Grenzübertritt

Der Grenzübertritt ist, insbesondere auf Flughäfen, in Bezug auf Cyber-Sicherheit eine besonders heikle Phase jeder Reise. Dementsprechend sollte dem Grenzübertritt großes Augenmerk gewidmet werden. Die rechtlichen Rahmenbedingungen hinsichtlich der Kontrolle von elektronischen Geräten und Datenträgern sind weltweit stark unterschiedlich und mitunter vergleichsweise recht undurchsichtig. Werden auf einer Dienstreise sensible Daten mitgeführt, so ist es notwendig, bereits vor dem Erreichen der Grenzkontrollstelle zwei grundlegende Überlegungen anzustellen.

Was sind die genauen rechtlichen Rahmenbedingungen im Reiseland in Bezug auf die Kontrolle von elektronischen Geräten und Datenträgern?

Ohne genaue Kenntnis der rechtlichen Rahmenbedingungen im Reiseland besteht die große Gefahr, dass sich Reisende im Zuge des Grenzübertritts bei einer Konfrontation mit den Organen unüberlegt verhalten oder auf vermeintlichen Rechten beharren, die sie im jeweiligen Land möglicherweise gar nicht haben. Dies kann zu sehr unangenehmen Konsequenzen führen. Es ist daher dringend anzuraten, die genauen rechtlichen Rahmenbedingungen in Bezug auf die Kontrolle von elektronischen Geräten und Datenträgern vorab zu recherchieren und sich entsprechend vorzubereiten.

Es ist den Behörden der meisten Länder gesetzlich explizit erlaubt, elektronische Geräte und Datenträger beim Grenzübertritt einer Kontrolle zu unterziehen. Ob sich diese rechtliche Möglichkeit jedoch lediglich auf eine rein oberflächliche Kontrolle beschränkt oder aber eine tiefgehende Untersuchung zulässig ist, ist je nach Land unterschiedlich geregelt. Oft sind für weitergehende Untersuchungen auch bestimmte Rahmenbedingungen oder Verdachtsmomente zwingend erforderlich.

Ebenfalls unterschiedlich wird die Mitwirkungspflicht der Reisenden gehandhabt. So dürfen in einigen Jurisdiktionen Reisende verpflichtet werden, ihre Zugangsdaten bekannt zu geben (oder selbst einzugeben). In anderen Reiseländern ist dies wiederum nicht zulässig, dafür dürfen Reisende dort unter Umständen gezwungen werden, das Gerät durch eine biometrische Authentifizierung (Fingerabdruck, Gesichtserkennung) zu entsperren.

Auch die technischen Mittel, die den Behörden des Reiselandes zur Durchsetzung ihrer rechtlichen Möglichkeiten zur Verfügung stehen, sind durchaus unterschiedlich geregelt. Während in manchen Jurisdiktionen Organe über vergleichsweise eingeschränkte Mittel verfügen, ist es in anderen Reiseländern zulässig, dass Behörden, zumindest bei bestimmten Verdachtslagen, auf technische Zwangsmaßnahmen (Hacking) zurückgreifen dürfen – dies gegebenenfalls auch ohne das Beisein der Reisenden.

Wie weit ist man bereit zu gehen, um die mitgeführten sensiblen Daten einem möglichen Zugriff der Behörden des Reiselandes zu entziehen?

Sofern man sensible Daten mit sich führen muss, ist es also einerseits entscheidend, die rechtlichen Rahmenbedingungen zu möglichen Kontrollrechten der Behörden zu kennen, aber andererseits auch sehr empfehlenswert, bereits vor dem Erreichen der Grenzkontrollstelle das eigene Verhalten zu planen. Anderenfalls kann es dazu kommen, dass man in der Stresssituation der Grenzkontrolle unüberlegte Handlungen setzt, was je nach Reiseland erhebliche Konsequenzen nach sich ziehen kann.

So werden die rechtlichen Konsequenzen bei einer Verweigerung der Aushändigung oder Mitwirkung sehr unterschiedlich gehandhabt. Während es sich dabei in manchen Ländern um eine strafbare Handlung per se handeln kann, ist dies in anderen Ländern zwar nicht strafbar, kann aber zu anderen, teils sehr unangenehmen Konsequenzen führen. Diese reichen von längeren Anhaltungen, über eine Beschlagnahme der fraglichen Geräte, bis hin zu einer generellen Verweigerung der Einreise.

Wir empfehlen:

- Recherchieren Sie bereits vor Reiseantritt die genauen rechtlichen Rahmenbedingungen im Reiseland in Bezug auf die Kontrolle elektronischer Geräte und Datenträger beim Grenzübertritt.

- Wägen Sie bereits vor einer möglichen Konfrontation genau ab, wie weit Sie zu gehen bereit sind, um mitgeführte sensible Daten einem möglichen Zugriff der Behörden des Reiselandes zu entziehen.
- Verlieren Sie die möglichen Konsequenzen Ihres Handelns niemals aus den Augen.

2.2 Verhalten beim Grenzübertritt

Generell sollte nie vergessen werden, dass die Behörden des Reiselandes den Reisenden in den seltensten Fällen feindselig gegenüberstehen, sondern lediglich ihrer Arbeit nachgehen. Oft ist eine etwaige Konfrontation vielmehr auf das Verhalten der Reisenden zurückzuführen. Es ist daher dringend anzuraten, nach Möglichkeit mit den Organen zu kooperieren und diese korrekt und freundlich zu behandeln. Eine Konfrontation sollte immer nur der letztmögliche Ausweg sein, wenn dies zum Schutz von sensiblen Daten unbedingt erforderlich erscheint.

Es wird dringend angeraten, bei einer Konfrontation mit den Behörden des Ziellandes, vor allem auch im Zuge eines Grenzübertritts, niemals zu lügen. In der Stresssituation des Grenzübertritts ist die Versuchung vergleichsweise groß, zum Schutz sensibler Daten zu lügen. Diese Lügen können von „Ich führe keine externen Datenträger mit mir“ bis zu „Ich besitze kein Facebook-Profil“ reichen. Oft zeigt sich in der Praxis, dass die Konsequenzen für einen überführten Lügner wesentlich unangenehmer sind, als für eine Verweigerung der Aushändigung oder Mitwirkung.

Sofern man sich zum Schutz der sensiblen Daten (unter Bedachtnahme aller daraus entstehenden Konsequenzen) entscheidet, eine Mitwirkung zu verweigern (z. B. keine Bekanntgabe des Kennwortes), gibt es einige Möglichkeiten, technische Zwangsmaßnahmen (Hacking) der Behörden maßgeblich zu erschweren oder zu verhindern. Dazu zählen unter anderem:

- das vollständige Ausschalten aller elektronischen Geräte (kein Stand-by)
- das rechtzeitige Aktivieren einer Datenträger-Vollverschlüsselung
- die Deaktivierung aller biometrischen Entsperrmöglichkeiten, da in manchen Ländern entsprechende Zwangsmaßnahmen zulässig sind.
- die Nutzung von Mehrfaktor-Authentifizierungsmöglichkeiten.

Entscheidend ist, dass diese Maßnahmen bereits vor Erreichen der Grenzkontrollstelle gesetzt wurden.

Wir empfehlen:

- Kooperieren Sie nach Möglichkeit stets mit den Organen des Reiselandes.
- Lügen Sie niemals.
- Nutzen Sie, sofern dies unabdingbar ist, alle technischen Möglichkeiten, technische Zwangsmaßnahmen (Hacking) durch die Behörden maßgeblich zu erschweren oder zu verhindern.

2.3 Nutzung fremder Geräte (und umgekehrt)

Gerade während Dienstreisen kann es mitunter zu Situationen kommen, in denen man sich gezwungen sieht, auf fremden Geräten zu arbeiten. Solche Situationen sollten allerdings nach Möglichkeit vermieden werden.

Jedes Gerät, über das man keine vollständige Kontrolle hat, birgt ein erhebliches Risiko für den Benutzer. Zum einen weiß man als temporärer Nutzer nicht, über welches Sicherheitsniveau das Gerät verfügt (z. B. Sicherheits-Updatestand, Antiviren-Software, Firewallkonfiguration), zum anderen kann nie sichergestellt werden, dass nicht im Verborgenen bösartige Software (z. B. Spionagesoftware, Schadsoftware) auf dem Gerät aktiv ist. Sollte es in einer bestimmten Situation unumgänglich sein, auf einem fremden Gerät zu arbeiten, sollten zumindest niemals Daten auf dem Gerät gespeichert werden.

Werden insbesondere auf einem fremden Gerät (wobei dies gleichermaßen für jedes Gerät gilt) Webdienste genutzt, die eine Anmeldung erfordern, so muss unbedingt darauf geachtet werden, dass nach erledigter Arbeit ein korrekter Abmeldevorgang durchgeführt wird. Das bloße Schließen des Browserfensters (ohne Abmeldung) erlaubt es Angreifern unter Umständen, die Sitzung wiederaufzunehmen und in Ihrem Namen Aktionen durchzuführen.

Eine weitere Gefahrenquelle stellt in diesem Zusammenhang die Nutzung fremder (Netzwerk-)Drucker dar. In der Regel werden die zu druckenden Daten im System zwischengespeichert und können auch nach dem erfolgten Druckvorgang im System verbleiben (z. B. für eine Druckwiederholungs-Funktion).

Wir empfehlen:

- Vermeiden Sie nach Möglichkeit generell die Verwendung von fremden Geräten.
- Vermeiden Sie nach Möglichkeit insbesondere die Übermittlung sensibler Daten, die Nutzung von VPN-Verbindungen, das Abfragen von E-Mail-Postfächern oder die Nutzung von Online-Banking-Diensten und dergleichen mittels fremder Geräte.
- Vermeiden Sie nach Möglichkeit das Drucken über fremde Drucker, insbesondere über Netzwerk-Drucker.

Dieselben Überlegungen sollten auch in umgekehrter Richtung angestellt werden. Genauso wenig, wie man fremde Geräte nutzen sollte, sollte stets vermieden werden, eigene Geräte, eigene Datenträger (z. B. USB-Speichersticks) oder eigene Zubehörteile an Dritte zu verborgen oder es diesen Personen zu ermöglichen, auf bzw. mit diesen Geräten zu arbeiten, da in solchen Fällen eine bewusste oder unbewusste Kompromittierung bzw. eine Infektion mit Schadsoftware niemals ausgeschlossen werden kann.

Wir empfehlen:

- Gewähren Sie zu keinem Zeitpunkt Dritten Zugriff auf Ihre Geräte, Ihre Datenträger (z. B. USB-Speichersticks) oder Ihre Zubehörteile.
- Vermeiden Sie es, Ihre externen Datenträger an fremde Systeme anzuschließen.
- Vermeiden Sie, wenn möglich, die Installation von speziellen Apps des Veranstalters.

2.4 Schutz von Daten während der Dienstreise

Zu Gewährleistung von Vertraulichkeit und Integrität ist es notwendig, stets die Kontrolle über die eigenen Geräte zu bewahren. Vertraulichkeit und Integrität können einerseits bei gespeicherten Daten (also direkt am Gerät) verletzt bzw. kompromittiert werden, andererseits besteht die Möglichkeit, dass Daten beim Transport über eine Kabel- oder kabellose

Verbindung (drahtloses Netzwerk, Bluetooth, NFC) kompromittiert werden. In beiden Fällen sollten entsprechende Vorsichtmaßnahmen unbedingt eingehalten werden.

Ein weiteres immer wieder auftretendes Problem ist die gesicherte Verwahrung von elektronischen Geräten und Datenträgern. Grundsätzlich erscheint es empfehlenswert, entsprechende Gegenstände immer bei sich zu führen. Ist dies aufgrund einer individuellen Situation nicht möglich, müssen besondere Vorsichtsmaßnahmen getroffen werden.

Insbesondere empfiehlt es sich, Geräte, die im Zuge der Dienstreise beispielsweise beim Sicherheitsdienst hinterlegt werden müssen, speziell dafür vorzubereiten. In jedem Fall sollte die Hinterlegung in einer versiegelbaren Tasche erfolgen. Diese schützt Ihr Gerät zwar nicht vor Kompromittierung, stellt aber sicher, dass Sie dies im Anlassfall zumindest bemerken und entsprechend reagieren können. Ebenfalls von Vorteil ist, wenn das Material dieser Tasche elektromagnetische Strahlung blockieren kann und somit ein Auslesen von Gerätedaten durch Funkwellen verhindert wird („Faraday-Bag“).

Verwahrung von elektronischen Geräten und Datenträgern

Die erste Gruppe von Empfehlungen behandelt die Verwahrung von elektronischen Geräten und Datenträgern während einer Dienstreise.

Wir empfehlen:

- Lassen Sie Ihre elektronischen Geräte und Datenträger zu keinem Zeitpunkt unbeaufsichtigt.
- Lassen Sie Ihre elektronischen Geräte nicht im Hotelzimmer zurück.
- Müssen Sie Ihre elektronischen Geräte aufgrund äußerer Zwänge doch im Hotel zurücklassen, nutzen Sie dafür jedenfalls einen (Hotel-)Safe. Beachten Sie dabei, dass auch ein solcher keinen wirklichen Schutz bietet und vermeiden Sie daher derartige Situationen, wenn dies irgendwie möglich ist.
- Vermeiden Sie in jedem Fall das Hinterlegen von elektronischen Geräten an Garderoben.
- Sollten Sie gezwungen sein, Ihr Gerät beim Betreten eines Gebäudes oder vor einer Besprechung (Sicherheitsdienst) abgeben zu müssen, verwenden Sie unbedingt spezielle, versiegelbare und/oder elektrisch abgeschirmte Taschen.

Schutz der Vertraulichkeit und Integrität von gespeicherten Daten

Die zweite Gruppe von Empfehlungen beinhaltet alle Handlungsempfehlungen, die dem Schutz der Vertraulichkeit und Integrität von gespeicherten Daten dienen.

Wir empfehlen:

- Führen Sie tragbare elektronische Geräte nach Möglichkeit stets mit sich.
- Ist dies aufgrund der jeweiligen Situation nicht möglich, verwenden Sie Ihr Kensington-Schloss und schalten Sie das unbeaufsichtigte Gerät vollständig aus. Bloßes Aktivieren der Bildschirmsperre oder des Ruhezustands bieten keinen ausreichenden Schutz.
- Vermeiden Sie das „ungeschützte“ Aufladen ihrer elektronischen Geräte über angebotene USB-Steckdosen. Sollte dies unbedingt erforderlich sein, nutzen Sie unbedingt sogenannte „USB-Kondome“ (Zwischenstecker zur Unterbrechung der Datenverbindung bei gleichzeitiger Aufrechterhaltung der Stromversorgung).
- Lassen Sie keine, auch nicht defekte Datenträger (z. B. USB-Speichersticks, externe Festplatten) im Reiseland zurück.
- Verwenden Sie für alle Gegenstände, die über NFC/RFID-Bausteine verfügen (z. B. Kreditkarten, Bankkarten, Reisepässe) nach Möglichkeit geeignete NFC/RFID-Schutzhüllen, die ein unbefugtes Auslesen der Informationen verhindern.

Schutz der Vertraulichkeit und Integrität von Daten in Bewegung

Die letzte Gruppe von Empfehlungen beinhaltet alle Handlungsempfehlungen, die dem Schutz von Daten in Bewegung (Transport, Übermittlung) dienen.

Wir empfehlen:

- Berücksichtigen Sie, dass Sie sich und Ihre Daten bei der Nutzung von fremden WLAN-Zugangspunkten einem erhöhten Risiko aussetzen.
- Vermeiden Sie daher nach Möglichkeit generell die Nutzung von fremden WLAN-Zugangspunkten, insbesondere in Hotels, Restaurants, Veranstaltungsorten, öffentlichen Bereichen (z. B. Flughäfen, Bahnhöfen), Verkehrsmitteln (z. B. Flugzeug, Bahn, Taxi).
- Trennen Sie Ihre elektronischen Geräte immer sofort von fremden WLAN-Zugangspunkten, wenn Sie die Verbindung nicht mehr benötigen.

Erscheint eine Nutzung eines fremden WLAN-Zugangspunkten ausnahmsweise unumgänglich, nutzen Sie alle Formen von Verschlüsselung, die Ihnen in der gegebenen Situation möglich sind.

Wir empfehlen:

- Nutzen Sie VPN-Verbindungen bei der Kommunikation mit Ihrer Organisation.
- Nutzen Sie verschlüsselte Verbindungen auch für die Abfrage von privaten E-Mail-Postfächern (bei dienstlichen Postfächern sollte dies ohnehin von der IKT entsprechend eingerichtet sein).
- Nutzen Sie verschlüsselte https://-Verbindung beim Surfen im Internet. Dies ist insbesondere dann unbedingt erforderlich, wenn Sie persönliche Daten auf einer Webseite eingeben (z. B. Zugangsdaten, Zahlungsdaten, personenbezogene Daten).
- Sollten Sie in solchen Situationen Zertifikatswarnungen irgendeiner Art erhalten, sollten Sie aus Sicherheitsgründen die Kommunikation abbrechen.

2.5 Nutzung sozialer Medien

Wie bereits bei den Handlungsempfehlungen für die Zeit vor einem Reiseantritt erwähnt, sind in bestimmten Regionen der Erde Freiheitsrechte noch (oder wieder) erheblich eingeschränkt oder haben religiöse Einflüsse unmittelbaren Einfluss auf diese. In diesem Zusammenhang ist es oftmals gelebte Praxis, dass der Zugang zu sozialen Netzwerken behördlich überwacht wird und explizite und implizite Äußerungen, die lokalen Vorschriften zuwiderlaufen, unter Umständen streng sanktioniert werden.

Es erscheint daher empfehlenswert, auf die Nutzung von sozialen Medien während einer Dienstreise generell zu verzichten. Damit kann einerseits das Risiko eines bewussten oder unbewussten Fehlverhaltens während der Nutzung vermieden werden, andererseits können die in sozialen Medien geteilten Informationen auch im Sinne einer nachrichtendienstlichen Bearbeitung nicht gegen Sie oder Ihre Organisation verwendet werden.

Wir empfehlen:

- Vermeiden Sie während einer Dienstreise generell die Nutzung sozialer Medien.
- Tätigen Sie auf sozialen Medien aber jedenfalls keinerlei Äußerungen, die geeignet erscheinen, die Vorschriften, Weltanschauungen oder politischen Aktivitäten im Reiseland zu hinterfragen, zu kritisieren oder verächtlich zu machen.

2.6 Internet-of-Things (IoT) und Sprachassistenten

Ein vergleichsweise junger Bereich der Informationstechnologie ist das sogenannte Internet-of-Things (IoT). Dabei werden Gebrauchsgegenstände des täglichen Lebens (z. B. Fernsehgeräte, Webcams, Babyphones, Haushaltsgeräte) oder des industriellen Einsatzes (z. B. Industriekontrollanlagen, Steuersysteme) mit digitaler Logik und Zugang zum Internet ausgerüstet. Im Wissen, dass die Grenzen hier fließend sind, kann vereinfacht auch definiert werden, dass das IoT alle vernetzten, elektronischen Geräte umfasst, auch wenn diese nicht unbedingt sofort als solche zu erkennen sind. Auch die immer verbreiteter eingesetzten smarten Sprachassistenten (z. B. Amazon Echo, vulgo Alexa) zählen zu dieser Gruppe.

Es kann davon ausgegangen werden, dass vergleichbare Technologien auch im Reiseland eingesetzt werden. Ein Problem bei IoT-Geräten ist unter anderem, dass deren Aktivitäten für einen nicht informierten Gast in manchen Fällen nur schwer feststellbar sind. Das Risiko, das von solchen Gegenständen, insbesondere von Sprachassistenten ausgeht, wird kontroversiell diskutiert, die Möglichkeit von Spionageaktivitäten ist jedoch keinesfalls auszuschließen.

Wir empfehlen:

- Vermeiden Sie vertrauliche Gespräche oder Tätigkeiten in Gegenwart von IoT-Geräten, die ein Risiko für die Vertraulichkeit darstellen können.
- Haben Sie die Vermutung, dass IoT-Geräte am Veranstaltungsort bzw. im Besprechungsraum vorhanden sind, sprechen Sie den Veranstalter bzw. Gastgeber gezielt darauf an.
- Nehmen Sie keine eigenen IoT-Geräte (z. B. Smartwatch, Sprachassistent) auf Dienstreisen mit.

3 Nach der Dienstreise

„Finis coronat opus. (Das Ende krönt das Werk.)“ (Ovid)

„Manch' bitteres Ende verdirbt selbst dem Teufel den Geschmack.“
(Martin Gerhard Reisenberg)

Auch nach Abschluss einer Dienstreise sollten noch einige Vorsichtsmaßnahmen gesetzt werden, um eine nachhaltige Cyber-Sicherheit sicherzustellen.

Es empfiehlt sich, alle während der Dienstreise verwendeten Zugangsdaten zu ändern. Dies umfasst neben naheliegenden Bereichen (z. B. Notebook, Cloud-Dienst, E-Mail-Postfach) aber auch andere Bereiche. Dazu zählen beispielsweise Streaming-Dienste (z. B. Netflix, AmazonPrimeVideo), die möglicherweise an einem smarten Fernseher im Hotelzimmer genutzt wurden.

Spezielle elektronische Geräte, die während der Dienstreise verwendet wurden (z. B. dedizierte Dienstreisegeräte), sollten – sofern dies im Einklang mit vorhandenen Policies der Firma oder Behörde steht – den zuständigen Kolleginnen und Kollegen zurückgegeben werden, ohne, dass das Gerät zuvor rückgesetzt wurde. Dies ermöglicht es der zuständigen Stelle, das Gerät einer forensischen Untersuchung zuzuführen, um eventuelle Manipulationen zu erkennen und zukünftige Reisende zu warnen bzw. entsprechende Maßnahmen zu setzen.

Wir empfehlen:

- Ändern Sie nach Abschluss der Dienstreise alle während der Abwesenheit verwendeten Zugangsdaten.
- Vermeiden Sie es, dedizierte Dienstreisegeräte vor der Rückgabe an die verantwortliche Stelle zurückzusetzen.
- Kommunizieren Sie alle eventuell getätigten Wahrnehmungen und Verdachtsmomente im Zusammenhang mit Cyber-Sicherheit an die verantwortlichen Kolleginnen und Kollegen.

Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Cyber Security Center – Bereich Prävention
Herrengasse 7, 1010 Wien
csc@bvt.gv.at
bvt.gv.at