BM.I
BUNDESMINISTERIUM FÜR INNERES

SICHERHEITSINFORMATION

FÜR EIGENTÜMER/BETREIBER KRITISCHER INFRASTRUKTUREINRICHTUNGEN IN ÖSTERREICH

INHALTSVERZEICHNIS

VORWORT 1

1. EINLEITUNG 2
2. MOTIVATION 3
3. ALLGEMEINE VERHALTENS-EMPFEHLUNGEN 3
4. KOMMUNIKATIONSEINRICHTUNGEN 4
   - 4.1 Festnetztelefon und Mobiltelefon 4
5. SICHERE NUTZUNG VON COMPUTERN UND SMARTPHONES 4
   - 5.1 Internet 6
   - 5.2 E-Mail 7
6. SICHERHEIT IM HÄUSLICHEN BEREICH 8
7. SICHERHEIT ZWISCHEN WOHNUNG UND ARBEITSPLATZ 9
   - 7.1 Eigener Pkw oder Dienstkraftfahrzeug 9
   - 7.2 Taxi und Mietwagen 10
   - 7.3 Öffentliche Verkehrsmittel 10
8. SICHERHEIT AM ARBEITSPLATZ 11
9. AUSLANDSREISEN 11
10. VERDÄCHTIGE POSTSENDUNGEN 13
    - 10.1 Erkennungsmerkmale und Überprüfungskriterien 13
    - 10.2 Merkmale sprengstoffverdächtiger Briefsendungen 13
    - 10.3 Merkmale verdächtiger Paketsendungen 14
    - Verhaltensmaßnahmen 14
11. HINWEISE ZUR VORBEUGUNG VON SPRENGSTOFF- UND BRANDANSCHLÄGEN 15
12. GEFÄHRLICHE DROHUNGEN, BOMBENDROHUNGEN, SABOTAGEAKTE 16
    - Verhalten bei Drohanrufen 16
    - Verhalten bei Bombendrohungen 16
    - Verhalten bei Sabotageakten 17
13. SCHUTZ VOR SPIONAGE/AUSSPÄHUNG IM IN- UND AUSLAND 17
    - Allgemeine Maßnahmen 17
14. EMPFEHLUNGEN IM FALLE EINER TELEFONISCHEN BENACHRICHTIGUNG ÜBER DIE ENTFÜHRUNG EINES/R ANGEHÖRIGEN 18
    - Allgemeine Hinweise für Familienangehörige 19

VORWORT

Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) beobachtet und setzt bei sicherheitsgefährdenden Bedrohungslagen die dafür notwendigen Maßnahmen. Ein wichtiges Aufgabengebiet des BVT ist in diesem Zusammenhang der Schutz kritischer Infrastruktur. Dabei ist es dem BVT ein Anliegen, nicht nur Präventivmaßnahmen und adäquate Hilfestellung anzubieten, sondern Ihnen auch in allen sicherheitsrelevanten Fragen als Ansprechpartner zur Verfügung zu stehen.

Um Schutzmaßnahmen maßgeschneidert umsetzen zu können, sind wir als staatliche Institution auf eine vertrauensvolle Kooperation mit Ihnen als Betreiber/in beziehungsweise Verantwortliche/r einer kritischen Infrastruktureinrichtung angewiesen. Angriffe können nie vollkommen ausgeschlossen werden; in Österreich werden aber beispielhafte Vorkehrungen getroffen, um Gefährdungen abzuwehren.

Da kritische Infrastruktureinrichtungen und Unternehmen unterschiedlichster Branchen von wesentlicher Bedeutung für die Aufrechterhaltung des wirtschaftlichen und sozialen Wohlergehens der Bevölkerung sind, stellen sie für verschiedenste Tätergruppen auch verlockende Ziele dar. Als Eigentümer/in, Betreiber/in oder Verantwortliche/r von kritischen Infrastrukturen sorgen Sie zwar selbst für die Aufrechterhaltung ihrer Geschäftsfähigkeit und den Schutz Ihrer Anlagen und Einrichtungen; das BVT steht Ihnen aber jederzeit beratend zur Seite. Neben technischen Maßnahmen bedarf es auch Ihrer Sensibilisierung für die Wahrnehmung möglicher Gefahren. In diesem Sinn hoffen wir, Ihnen mit dieser Broschüre Bedrohungsarten und Handlungsempfehlungen näherbringen zu können und damit bei den Sicherheitsvorkehrungen eine Hilfestellung zu bieten.

Mag. Peter GRIDLING
Direktor BVT

Die in dieser Broschüre angeführten Empfehlungen erheben nicht den Anspruch auf Vollständigkeit und sollen nur über mögliche Gefährdungslagen informieren. Es handelt sich dabei um eine demonstrative Aufzählung. Dieser Ratgeber wurde erstellt, um die Bedeutung, die Tragweite sowie die praktischen Konsequenzen der behandelten Themen zu erläutern. Der vorliegende Leitfaden zielt demgemäß darauf ab, Sie in Ihrem Sicherheitsdenken zu unterstützen und zu sensibilisieren.

1. EINLEITUNG

Im Sinne der EU-Richtlinie 2008/114/EG ist eine „kritische Infrastruktur" eine Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten.[1]

Kritische Infrastruktureinrichtungen können sowohl durch Naturkatastrophen, Unfälle und Nachlässigkeit als auch durch Anschläge, Sabotage, Manipulierung von EDV-Einrichtungen, mutwilliges Verhalten und sonstige strafbare Handlungen in ihrem Betrieb gestört, beschädigt oder vernichtet werden und damit ein enormes Schadensausmaß erreichen.

In diesem Zusammenhang und in Anbetracht Ihrer Stellung als Eigentümer/in bzw. Betreiber/in von kritischen Infrastruktureinrichtungen, sind Sie möglicherweise mit einem erhöhten Gefährdungspotenzial konfrontiert. Das BVT und alle mit dieser Aufgabe betrauten Dienststellen sind bemüht, Präventionsmaßnahmen zu setzen und mit Kompetenz und Effektivität bei eventuellen Bedrohungslagen einen umfassenden Schutz zu bieten.

[1] Siehe „EU-RICHTLINIE 2008/114/EG DES RATES vom 8. Dezember 2008" über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern.

Dieser Leitfaden soll Ihnen, Ihren Angehörigen und engsten Mitarbeitenden mögliche Bedrohungsarten und Handlungsempfehlungen näherbringen. Er soll eine Hilfestellung bei den Sicherheitsvorkehrungen bieten, Ihnen mögliche Gefährdungslagen veranschaulichen und Ihre Präventionskenntnisse vertiefen.

2. MOTIVATION

Eigentümer/innen bzw. Betreiber/innen von kritischen Infrastruktureinrichtungen können Angriffsziele sein. Die Motive und Hintergründe der Täter sind vielfältig.

Die Hauptmotive potenzieller Angreifer reichen von Wirtschaftsspionage über Extremismus bis zu persönlicher Frustration. Die Vorgangsweisen reichen von Drohhandlungen, über Cyber-Angriffe, Sabotage, Ausspähung, Entführung und Geiselnahmen bis hin zu Anschlägen.

3. ALLGEMEINE VERHALTENSEMPFEHLUNGEN

- Eine rege Kommunikation mit den für Ihre Sicherheit eingesetzten Mitarbeitenden erleichtert deren Arbeit.
- Hinweise aus Ihrem persönlichen Umfeld, wie z. B. Familie, Mitarbeiterstab und Freundeskreis, über mögliche Bedrohungen sollten ernst genommen werden.
- Teilen Sie verdächtige Wahrnehmungen unverzüglich der Polizei und Ihrer/Ihrem Sicherheitsbeauftragten mit.
- Vermeiden Sie bei Veröffentlichungen oder in Publikationen Adressen- und Telefonangaben.
- Achten Sie darauf, dass Ihr Gepäck bzw. Ihre persönlichen Gebrauchsgegenstände nicht von fremden Personen transportiert werden.

- Ersuchen Sie Ihre Angehörigen und Ihr Personal, sich im Sinne dieser Sicherheitsempfehlungen zu verhalten.
- Vereinbaren Sie für den Fall einer Entführung mit Ihren Angehörigen und engsten Mitarbeitenden unverwechselbare Erkennungszeichen bzw. Codewörter.

4. KOMMUNIKATIONSEINRICHTUNGEN

4.1 Festnetztelefon und Mobiltelefon

- Beantragen Sie eine Geheimnummer mit Nichteintragung in Telefonverzeichnissen und ohne Auskunftserteilung.
- Verzichten Sie auf die Nennung Ihres Namens bei der Gesprächsannahme.
- Führen Sie keine Telefonate zu sensiblen Themen.
- Schützen Sie Ihre Mobiltelefone und Smartphones mittels PIN vor unrechtmäßiger Nutzung (inkl. PIN-geschützter Tastatursperre).
- Informieren Sie sich über die technischen Gegebenheiten bzw. Manipulationsmöglichkeiten von Smartphones.
- In diesem Zusammenhang wird ein restriktiver und vorsichtiger Umgang bei Downloads, bei der Nutzung von Apps und Social Media angeraten.

5. SICHERE NUTZUNG VON COMPUTERN UND SMARTPHONES

Zum Bereich der Informations- und Kommunikationstechnologie (IKT) ist vorab auszuführen, dass die Täter meist über keine persönlichen Kontakte zum Angriffsopfer verfügen. In vielen Fällen fällt daher oftmals die persönliche Hemmschwelle und in Folge auch das eigene Unrechtsbewusstsein weg.

Häufig wird Cyber-Kriminalität auch genutzt, um Schwächen bzw. Angreifbarkeiten des Systems darzustellen bzw. aufzuzeigen. Deshalb ist es grundsätzlich notwendig, bei der Benutzung der Informations- und Kommunikationstechnologie (IKT), die Sicherheitssoftware immer aktuell zu halten.

- Generell ist anzuraten, keine fremden Geräte (PC, Notebook, Tablet-PC, Smartphone) zu benutzen. Es besteht die Gefahr des Ausspähens persönlicher (Zugangs-)Daten.
- Verwenden Sie mit eigenen dienstlichen Geräten keine fremden Datenträger (USB-Stick, CD, DVD, externe Festplatten) oder sonstige fremde Geräte wie Maus, Scanner, Drucker, W-LAN-Stick, Bluetooth-Stick oder Ähnliches. Dies gilt insbesondere für Werbegeschenke und „Präsentationsunterlagen", da die Gefahr des Einschleusens von Schadsoftware besteht.
- Nutzen Sie unterschiedliche Geräte für berufliche und private Verwendung.
- Vermeiden Sie es, die eigenen IT-Geräte fremden Personen zu überlassen, auch nicht Kolleginnen und Kollegen.
- Es empfiehlt sich, eigene Datenträger niemals anderen zu überlassen und nicht an fremde Geräte anzuschließen bzw. mit fremden Geräten zu verwenden.
- Zum Datentransfer nur einmal beschreibbare bzw. schreibgeschützte Datenträger verwenden (CD oder DVD).
- Wenn möglich alle Datenträger vollständig verschlüsseln (entweder Festplatten bzw. USB-Stick mit integrierter Verschlüsselung verwenden oder z. B. mit Bitlocker oder Truecrypt im Nachhinein verschlüsseln). Ist dies nicht möglich, dann zumindest jene Dateien verschlüsseln, die persönliche oder sonstige sensible Informationen beinhalten.
- Schützen Sie jeden Computer durch Benutzerkennung und Passwort vor unberechtigtem Zugriff. Verwenden Sie zusätzlich einen sich automatisch aktivierenden, passwortgeschützten Bildschirmschoner.
- Ein Passwort sollte mindestens acht Stellen lang sein und aus einer Kombination von Buchstaben (Groß- und Kleinschreibung), Ziffern und Zeichen bestehen.
- Benutzen Sie niemals gleiche Passwörter für unterschiedliche Systeme. Je sensibler die verarbeiteten Informationen eines Systems sind, desto komplexer sollte das Passwort sein.
- Geben Sie unter keinen Umständen jemals irgendjemanden Ihr Passwort.

- Notieren Sie niemals Ihr Passwort direkt neben dem Computer auf einen Zettel.
- Für die normale Verwendung Ihres Gerätes empfiehlt es sich, einen Benutzer-Account mit minimalen Rechten (Gast-Account) zu verwenden. Der Administratoren-Account sollte nur zum Installieren von Software verwendet werden.
- In Geräten, die nicht ausreichend sicherheitstechnisch abgesichert werden können, sollen keine Firmendaten oder sensible private Daten gespeichert werden (z. B. Mail- und Telefonkontakte bzw. E-Mails und Terminkalender).

5.1 Internet

- Bei einem Internetauftritt sollte mit Daten sensibel umgegangen werden. Achten Sie darauf, dass keine persönlichen Informationen, wie z. B. Privatadressen, auf Webseiten veröffentlicht werden.
- Sensibilisieren Sie Ihre Angehörigen, sich in diesem Sinne zu verhalten. Denn der vorsichtige Umgang mit persönlichen Angaben beugt einem allzu leichten Ausspähen Ihres privaten Lebensbereichs vor.
- Software sollte immer von seriösen Firmen in Originalverpackung gekauft werden. Downloads über das Internet, Programmkopien von Bekannten etc. sollten auf keinen Fall installiert werden.
- Virenschutzprogramme und andere Software sind regelmäßig auf Sicherheits-Updates zu überprüfen und zu aktualisieren (automatische Aktualisierung einstellen).
- Die Nutzung von Netzwerkverbindungen (Kabel, W-LAN oder Bluetooth) soll immer nur mittels aktivierter Firewall erfolgen. Bei drahtlosen Netzwerkverbindungen ist immer das stärkste angebotene Verschlüsselungsverfahren zu verwenden (z. B. WPA2 statt WPA oder WEP).
- Schließen Sie nach jedem Internetzugriff die W-LAN-, UMTS- oder GPRS-Funktion Ihres Notebooks, Tablets oder Smartphones.
- Verwenden Sie niemals öffentliche W-LAN oder W-LAN-Verbindungen, die von Hotels, Veranstaltern und Firmen angeboten werden.
- Benutzen Sie für den Internetzugang außerhalb Ihres Büros oder Ihrer Wohnung nur die Datenverbindung (GPRS, EDGE, UMTS, HSPA, LTE etc.) Ihres privaten bzw. beruflichen Mobiltelefon-Providers. Dabei nach Möglichkeit immer sichere Verfahren (https, sftp, SVPN) bzw. verschlüsselten Datenaustausch einsetzen.

- Speichern Sie keine sensiblen bzw. persönlichen Daten auf Ihnen nicht bekannten bzw. Ihnen nicht vertrauenswürdig erscheinenden Webseiten.
- Öffnen Sie Webseiten nach Möglichkeit nicht durch das Anklicken von Links, sondern nach vorheriger Plausibilitätsprüfung durch die Eingabe der URL in der Adresszeile. Vermeiden Sie das Aufrufen von nicht vertrauenswürdigen Webseiten.
- Verwenden Sie einen vom Betriebssystem unabhängigen Internetbrowser, wie z. B. Firefox, und aktivieren Sie die eingebauten Sicherheitsvorkehrungen. Informieren Sie sich im Internet zum Thema „Sichere Nutzung des Internets".

5.2 E-Mail

Gehen Sie mit Drohungen per E-Mail sensibel um. Die genaue Dokumentation der E-Mails hilft bei der Ausforschung der Täter.

- Öffnen Sie keine E-Mails oder Anhänge von unbekannten Absendern.
- Geben Sie Ihre E-Mail-Adresse nur an Personen Ihres Vertrauens weiter.
- Verwenden Sie gegebenenfalls einen Nickname in Ihrer E-Mail-Anschrift.
- Löschen Sie keine Droh-Mails, sondern sichern Sie diese und verständigen Sie umgehend die Polizei.
- Vermeiden Sie den Austausch von Firmendaten oder sensibler privater Daten außerhalb Ihres beruflichen E-Mailsystems bzw. persönlichen privaten E-Mailproviders.
- Unterlassen Sie Terminvereinbarungen mittels Internetkalender bzw. Online-Terminplaner, wie z. B. Google-Kalender oder Doodle.
- Verwenden Sie Ihre persönliche E-Mailadresse beruflich sowie privat nur im dafür vorgesehenen Mailverkehr und in keinem Fall für die Nutzung anderer Internetdienste, wie z. B. Newsletter, Online-Shops oder Social-Media-Dienste wie Facebook, Google, YouTube, Twitter etc. Verwenden Sie dazu Alias-Adressen.
- Halten Sie den Empfängerkreis beim Versenden von E-Mails so klein wie möglich, wobei Adressaten, die unterschiedlichen Empfängerkreisen angehören, als BCC (Blind Carbon Copy) angegeben werden sollten.
- Entfernen Sie beim Weiterleiten von E-Mails alle Adressaten aus dem E-Mail-Verlauf.

- Nutzen Sie zur Kommunikation mit Smartphones und Computer keine Online-Messenger-Systeme, wie ICQ, Windows Live Messenger, Skype, WhatsApp, Facebook Messenger, iMessage etc.

Sollten die erwähnten Begriffe und Hinweise für Sie unverständlich sein, lassen Sie sich durch Fachpersonal im Umgang mit Computer und dessen Zubehör sowie dem Internet und seinen Diensten schulen.

Detaillierte Informationen für den IT-Sicherheitsbereich finden Sie im Österreichischen Informationssicherheitshandbuch.[2]

6. SICHERHEIT IM HÄUSLICHEN BEREICH

- Sofern im häuslichen Bereich noch keine Maßnahmen getroffen wurden, nehmen Sie die kostenlose kriminalpolizeiliche Beratung[3] in Anspruch.
- Beziehen Sie alle Zugangs- und Einstiegsmöglichkeiten am Haus oder in der Wohnung in Ihre Gebäudeschutzmaßnahmen ein.
- Im Falle tatsächlicher Bedrohungssituationen empfiehlt es sich, die Außentüren und Fenster ständig verschlossen zu halten.
- Öffnen Sie keinem Unbekannten, ohne die Türsicherung aktiviert zu haben
- (z. B. Überwachungskamera, Sperrkette, Kastenschloss mit Sperrbügel).
- Achten Sie auf Ihre Wohnungsschlüssel; bei Verlust oder sonstigem ungeklärten Verbleib wird ein Auswechseln der Schließanlage empfohlen. Versehen Sie den Schlüsselbund nicht mit Ihrer Adresse.
- Geben Sie auf Personen und Fahrzeuge Acht, die sich ohne ersichtlichen Grund in der Nähe Ihres Wohnbereichs aufhalten.

[2] Bundeskanzleramt Österreich, Österreichisches Informationssicherheitshandbuch, Version 3.1.5, Stand: 10.11.2013, https://www.sicherheitshandbuch.gv.at/

[3] Kriminalpolizeiliches Beratungszentrum, 1070 Wien, Andreasgasse 4, +43-1-31310-44938, Montag bis Freitag: 10 bis 18 Uhr, jeden 1. Samstag im Monat 10 bis 16 Uhr.

- Vereinbaren Sie mit Handwerkern feste Termine, prüfen Sie die Identität durch telefonische Rückfragen und lassen Sie Arbeiten nur unter Aufsicht durchführen.
- Bieten Sie potenziellen Tätern keinen Einblick in Ihren Wohnbereich und erschweren Sie das Ausspähen Ihrer Lebensgewohnheiten. Greifen Sie auf Sichtschutz (Gardinen, Rollläden, Jalousien etc.) zurück.
- Verzichten Sie möglichst auf Türnamensschilder, auch an Postkästen.
- Sie können bei der Meldebehörde eine Meldeauskunftssperre beantragen.
- Nehmen Sie grundsätzlich keine Geschenk- oder unbestellte Warensendungen von Unbekannten an der Tür entgegen.
- Sorgen Sie für eine gute Außenbeleuchtung und für Alarmvorrichtungen.
- Prüfen Sie nach längerer Abwesenheit Haus bzw. Wohnung auf Beschädigungen oder sonstige Veränderungen. Es empfiehlt sich im Falle einer längeren Abwesenheit, eine Sicherheitsfirma mit der Bestreifung des Objekts zu beauftragen.
- Lassen Sie Ihren Briefkasten bei Abwesenheit entleeren. Vor der Tür abgelegte Zeitungen und Werbematerialien sollten ebenfalls entfernt werden.
- Legen Sie sich Fluchtrouten zurecht, eventuell in Absprache mit dem oder der Sicherheitsbeauftragten.
- Benützen Sie für Ihren Pkw eine Garage.

7. SICHERHEIT ZWISCHEN WOHNUNG UND ARBEITSPLATZ

7.1 Eigener Pkw oder Dienstkraftfahrzeug

- Im Gefährdungsfall empfiehlt es sich, die Fahrtstrecken und die Abfahrtszeiten so häufig wie möglich zu variieren, dabei sollten auch größere Umwege in Kauf genommen werden. Wenn möglich, wechseln Sie das Fahrzeug.
- Fahren Sie möglichst nicht ohne Begleitung.
- Überprüfen Sie vor der Abfahrt die Umgebung oder lassen Sie diese beobachten.

- Vorsicht bei außergewöhnlichen Zwangshalten, es könnte beispielsweise eine gestellte Unfallsituation vorliegen.
- Achten Sie auf Verfolgerfahrzeuge. Bei Verdacht fahren Sie einen sicheren Ort an (Polizeidienststelle, belebter Platz).
- Aktivieren Sie die Zentralverriegelung bzw. versperren Sie die Fahrzeugtüren.
- Sehen Sie Kommunikationsmittel im Fahrzeug vor (Mobiltelefon, Funk, Alarmierungsgerät).
- Informieren Sie vertraute Personen über Reiseziel und Aufenthaltsort, Ankunfts- und Abfahrtszeiten und ersuchen Sie sie, die Informationen vertraulich zu behandeln.
- Bei längeren Fahrten verständigen Sie vertraute Personen über das Eintreffen am Zielort. Setzen Sie Maßnahmen fest für den Fall, dass diese Information ausbleibt.
- Lassen Sie keine wichtigen Unterlagen oder technische Geräte wie Laptop, Handy etc. im Fahrzeug.

7.2 Taxi und Mietwagen

- Verwenden Sie ausschließlich bekannte Taxiunternehmen oder Mietwagenfirmen.
- Verwenden Sie nur telefonisch vorbestellte Taxis oder solche von gekennzeichneten Abstellplätzen.
- Nehmen Sie auf der Rückbank Platz und legen Sie wichtige Unterlagen neben sich.

7.3 Öffentliche Verkehrsmittel

- Lassen Sie wichtige Dinge nicht liegen bzw. nicht unbeaufsichtigt.
- Nehmen Sie Ihren Sitzplatz so ein, dass Sie über eine gute Übersicht haben mit Blick zur Tür.

8. SICHERHEIT AM ARBEITSPLATZ

- Veranlassen Sie eine lückenlose Zutrittskontrolle im gesamten Büro- bzw. Geschäftsbereich.
- Es empfiehlt sich, Besucher nur eintreten zu lassen, wenn deren Identität eindeutig feststeht.
- Lassen Sie eventuell die Gegensprechanlage zu Ihrem Vorzimmer eingeschaltet, damit Sie zu Ihrem Sekretariat Kontakt halten können.
- Besucher innerhalb Ihres Geschäftsbereichs sollten begleitet werden.
- Ihr Arbeitszimmer sollte nur durch das Sekretariat zu erreichen sein.
- Essenszeiten und Restaurants sollten variieren.
- Veranlassen Sie die ausreichende Sicherung des Büro- bzw. Geschäftsbereichs durch bauliche und organisatorische Schutzmaßnahmen sowie die Installation von Notrufmöglichkeiten. Nehmen Sie auch hier die Fachberatung von Spezialisten in Anspruch.
- Empfohlen wird eine umfassende Außensicherung des Firmengeländes.

9. AUSLANDSREISEN

In vielen Ländern außerhalb Europas gibt es Sicherheitsrisiken. Es wird ein erhöhtes Gefahrenbewusstsein bei Reisen in Risikogebiete empfohlen, um Schwachstellen zu erkennen und sich entsprechend zu verhalten.

- Informieren Sie sich vor Antritt einer Reise über das jeweilige Land und die damit verbundenen Sicherheitsrisiken. Ein nützliches Portal ist die Länderinformation des Bundesministerium für Europa, Integration und Äußeres (BMEIA): www.bmeia.gv.at
- Halten Sie Notrufnummern (BMEIA-Notrufnummer +43-1-901154411) sowie Telefonnummern der österreichischen Vertretung (eventuell auch Kontaktinformationen zu EU-Mitgliedstaatenvertretungen) im jeweiligen Land bereit.
- Sollten Sie verschuldet oder unverschuldet mit Behörden des Reiselandes in Schwierigkeiten geraten, verständigen Sie sofort die nächste diplomatische oder konsularische Vertretung der Republik Österreich.

- Beachten Sie die landestypischen Höflichkeits- und Verhaltensregeln.
- Achten Sie auf die Gültigkeit von Reisepass und Visum und machen Sie Kopien von mitgeführten Originaldokumenten, die Sie getrennt von den Originalen verwahren sollten.
- Halten Sie Telefonnummern für das Sperren von Kreditkarten und Mobiltelefonen bereit.
- Programmieren Sie die ICE-Nummer (In Case of Emergency) auf Ihrem Mobiltelefon.
- Verstauen Sie vertrauliche Dokumente in Ihrem Handgepäck.
- Das Packen der Koffer sollte immer persönlich erfolgen.
- Verwenden Sie bekannte Reiseagenturen und sichere Fluglinien.
- Beschriften Sie Ihr Gepäck mit Geschäftsadresse und Telefonnummer.
- Lassen Sie Ihr Gepäck nicht unbeaufsichtigt.
- Nehmen Sie kein Gepäck anderer Personen entgegen.
- Überprüfen sie den Inhalt von Gastgeschenken.
- Prüfen Sie im Hotelzimmer die Sicherheit der Eingangstüren und Fenster und machen Sie sich mit den Fluchtwegen vertraut.
- Beachten Sie Flucht- und Evakuierungspläne.
- Empfangen Sie unbekannte Besucher nicht im Hotelzimmer.
- Benützen Sie Zimmer- bzw. Hotelsafes für Wertgegenstände und Dokumente.
- Veranlassen Sie, dass zugestellte Dokumente oder sonstige Gegenstände grundsätzlich an der Rezeption zur Selbstabholung hinterlegt werden sollen.

10. VERDÄCHTIGE POSTSENDUNGEN

10. 1 Erkennungsmerkmale und Überprüfungskriterien

Nachstehende Auffälligkeiten können Ihnen helfen, verdächtige Briefe und Pakete zu identifizieren:

- Unerwartete bzw. unaufgeforderte Zusendungen aus dem In- und Ausland.
- Unübliche Sendungen in Bezug auf den Absender.
- Überfrankierung mit Briefmarken.
- Besondere schriftliche Hinweise auf der Sendung, wie „persönlich", „privat", „zu eigenen Handen", „vertraulich", „geheim", „nur durch den Empfänger zu öffnen", „Eilsendung", „dringend", die dazu dienen, dass eine bestimmte Person erreicht wird.
- Auffällig fehlerhafte Absenderangaben oder offensichtliche Verwendung von Fantasienamen als Absender.

10.2 Merkmale sprengstoffverdächtiger Briefsendungen

- Briefsendungen können starr und fest wirken, der Inhalt des Briefes kann sich jedoch elastisch bis knetbar oder als Luftpolster anfühlen.
- Sie weisen zumeist ein ungewöhnlich hohes Gewicht im Verhältnis zur Größe auf. Die Gewichtsverteilung kann unregelmäßig sein.
- Präsenz von metallischen Materialien im Inneren, fühlbare Unebenheiten und Verstärkungen.
- Verdächtige Geräusche (Rasseln, Rieseln), Gerüche oder Dämpfe (z. B. Mandel oder Vanille) sowie „Ausschwitzen" (Fettflecke am Kuvert).
- Austreten einer pulverförmigen Substanz aus einer beschädigten Sendung oder Sichtbarwerden von Materialien, die Fensterkitt oder Plastilin ähnlich sind.

- Verpackungen, bei denen das Ende der Verschnürung oder ein mit Klebefolie abgedeckter Faden ins Innere der Sendung führt.
- Eine beim Öffnen der äußeren Verpackung zum Vorschein kommende sorgfältige innere Verpackung, die eines der oberen Kriterien erfüllt.

10.3 Merkmale verdächtiger Paketsendungen

- Ungewöhnlich hohes Gewicht.
- Übermäßig feste, äußere Verpackung bzw. massive Verklebung bzw. Verschnürung.

Verhaltensmaßnahmen

Ein sensibler Umgang mit konventionellen und elektronischen Drohschreiben durch potenzielle Opfer bzw. durch Ihre Mitarbeitenden kann frühzeitige Hinweise auf eine mögliche Eskalation liefern. Ein dokumentierter Korrespondenzverlauf, die Aufbewahrung der Postsendung(en) und das „Nicht berühren" können sinnvoll für die weiteren polizeilichen Ermittlungen sein.

- Postsendungen haben bereits einen langen Weg überstanden (Aufgeben, Abstempeln, Transporte). Es besteht im Allgemeinen bei sorgfältigem Umgang (nicht knicken, brechen oder sonst beschädigen) meist kein Grund zur Panik.
- Betrachten Sie unerwartete Sendungen kritisch. Bestehen Zweifel, nehmen Sie mit dem Absender Kontakt auf.
- Legen Sie verdächtige Sendungen sofort vorsichtig an einem gesicherten Ort ab (eventuell abgeschirmt durch Mauer oder Wandvorsprünge) und verlassen Sie den Raum.
- Die Sendung sollte keiner Feuchtigkeit (Kurzschlussgefahr!) und keiner großen Kälte oder Hitze (Sonneneinstrahlung oder Heizung) ausgesetzt werden.
- Brief- oder Paketsendung nicht knicken, falten oder lochen. Vermeiden Sie mechanische Belastungen wie Stöße oder Schläge.

- Verändern Sie die verdächtig erscheinende Brief- oder Paketsendung nicht durch Beschriften oder anderweitige Umgestaltung.
- Verständigen Sie die örtlich zuständige Sicherheitsdienststelle und allenfalls den zuständigen Sicherheitsbeauftragten.
- Unterbinden Sie den Zutritt Unbeteiligter und bewahren Sie Ruhe.
- Notieren Sie Namen des Überbringers und die Uhrzeit der verdächtigen Brief- oder Paketsendung.
- Sie erleichtern die Arbeit der Polizei, wenn Sie verhindern, dass Personen aus Ihrem Umfeld zusätzliche Spuren (z. B. Fingerabdrücke) auf die Postsendung setzen. Dokumentieren Sie, wer die Sendung berührt hat.
- Ist der bedenkliche Brief bereits geöffnet, berühren Sie ihn nicht mehr und geben Sie ihn an keine anderen Personen weiter.
- Bedenken Sie, dass neben Sprengstoffen auch chemische und biologische Mittel verwendet werden können.

11. HINWEISE ZUR VORBEUGUNG VON SPRENGSTOFF- UND BRANDANSCHLÄGEN

- Vielfältige Manipulationsmöglichkeiten bieten Kraftfahrzeuge. Ihr Pkw sollte ausnahmslos in geschützten Bereichen verschlossen abgestellt werden.
- Es wird empfohlen, den Pkw mit einer Alarmanlage und einem GPS-Tracking-System auszustatten.
- Vorsicht bei „stehen gelassenen“ oder „vergessenen“ Gegenständen, die keiner Person zugeordnet werden können, wie Aktentaschen, Kleidungsstücke und Ähnliches. Diese könnten Spreng- oder Brandvorrichtungen enthalten.
- Halten Sie Brandbekämpfungsmittel im Wohn- und Arbeitsbereich bereit. Alle Angehörigen bzw. Mitarbeitenden sollten sich mit der Bedienungsanleitung vertraut machen.
- Kommt ihnen ein Gegenstand verdächtig vor, berühren Sie ihn nicht und sorgen Sie dafür, dass auch andere Personen dies nicht tun. Verlassen Sie den Fundort und verständigen Sie sofort die Polizei und Ihre/n Sicherheitsbeauftragte/n.

12. GEFÄHRLICHE DROHUNGEN, BOMBENDROHUNGEN, SABOTAGEAKTE

Verhalten bei Drohanrufen

- Verwenden Sie als Hilfsmittel stets das zur Verfügung gestellte Formular (siehe Anhang).
- Im Falle eines Drohanrufes schalten Sie das Aufnahmegerät bzw. den Lautsprecher ein und geben Sie ein vereinbartes Zeichen an Anwesende.
- Versuchen Sie mit dem Anrufer ins Gespräch zu kommen, indem Sie offene Fragen stellen. Dabei können im Formular enthaltene Fragen verwendet werden.
- Versuchen Sie nach Möglichkeit während des Gesprächs, jedoch unbedingt unmittelbar danach, Notizen zu den im Formular angeführten Punkten zu tätigen.
- Für die Sicherheitsbehörden sind in Bezug auf eine eventuelle Strafverfolgung die verwendete Sprache, der Dialekt, die Sprechart sowie Eigenarten im Sprechverlauf (Lispeln, Stottern, auffällige Wortwiederholungen) sehr wichtig.
- Außerdem sollte auf Hintergrundgeräusche geachtet werden (z. B. Baulärm, Verkehrslärm, Kirchenglocken, Vogelgezwitscher etc.).

Verhalten bei Bombendrohungen

- Erfragen Sie bei einer telefonischen Bombendrohung den beabsichtigten Explosionszeitpunkt: Um welche Uhrzeit soll die Bombe explodieren?
- Verständigen Sie unverzüglich die Polizei.
- Veranlassen Sie die sofortige Räumung des gefährdeten Objekts.
- Nehmen Sie persönliche Gegenstände, wie Taschen und Dokumente, mit.
- Halten Sie sich für die Polizei zur Verfügung.
- Die Anwesenheit eines ortskundigen Bediensteten (Hausmeister, Portier, Sicherheitsbeauftragter) sollte für weiterführende polizeiliche Erhebungen gewährleistet sein.

Verhalten bei Sabotageakten

- Sobald Sie Kenntnis über Sabotage bzw. Sabotageversuche erlangen, verständigen Sie umgehend die nächste Sicherheitsdienststelle und Ihre/n Sicherheitsbeauftragte/n.

13. SCHUTZ VOR SPIONAGE/AUSSPÄHUNG IM IN- UND AUSLAND

Jedes Unternehmen, unabhängig von seiner Branchenzugehörigkeit, kann Opfer von Wirtschafts- und Industriespionage werden. Der Schutz eines Unternehmens beschränkt sich nicht ausschließlich auf den Gebäudeschutz und etwaige IT-Sicherheit, sondern erstreckt sich auch auf die Schulung und Sensibilisierung der Mitarbeitenden über den Umgang mit Daten und Unterlagen. Wenngleich elektronische Angriffe aufgrund des technischen Fortschritts zunehmen, so zeigen die Fälle der jüngeren Vergangenheit, dass der Mensch als Akteur im Vordergrund steht. Zumeist sind es aktive oder ehemalige Mitarbeitende, Geschäftspartner oder betriebsfremde Personen.

Spionagefälle in der Wirtschaft werden häufig nicht angezeigt, da betroffene Unternehmen durch Bekanntwerden eines Spionagefalls einen Imageschaden befürchten. Unabhängig von einem konkreten Verdachtsfall empfiehlt sich die Kontaktaufnahme mit der BVT-Kontaktstelle Wirtschafts- und Industriespionage, WIS@bvt.gv.at. Weitere Kontaktdaten finden sie im Anhang.

Allgemeine Maßnahmen

- Sensibilisieren Sie Ihre Mitarbeitenden und Ihre nächsten Angehörigen auf diese Gefährdungsmöglichkeit.
- Lassen Sie die technische Datensicherheit regelmäßig überprüfen.
- Achten Sie auf einen vorsichtigen Umgang mit vertraulichen Unterlagen.

- Seien Sie achtsam mit sensiblen Informationen im Gespräch mit Dritten und ziehen Sie, falls möglich, eine Vertrauensperson bei.
- Ein vorsichtiger Umgang mit „zufälligen Bekanntschaften" im In- und Ausland wird empfohlen.
- Verzichten Sie bei Auslandsaufenthalten im Zweifel auf Übertragung sensibler Daten per Mail oder Handy.
- Lassen Sie sich weder zu Gefälligkeiten verleiten, die Ihnen nachteilig ausgelegt werden könnten, noch zu negativen Äußerungen über das Reiseland.
- Geben Sie Handynummer und E-Mailadresse bei Verdachtsmomenten nicht an Unbekannte weiter.
- Nehmen Sie keine wichtigen Daten (auf Laptop, Tablet-PC, Datenstick, Smartphone etc.) mit. Wenn dies nicht vermeidbar ist, schützen bzw. verschlüsseln Sie diese Daten und führen Sie diese immer bei sich.
- Setzen Sie bei längeren Auslandsaufenthalten nach Möglichkeit bei Ankunft und Abreise die österreichische Botschaft in Kenntnis.
- Bedenken Sie, dass bei Auslandsreisen in sensible Gebiete Taxifahrer, Hotelpersonal, Reiseführer etc. beauftragt sein können, Reisende zu überwachen. Verhalten Sie sich daher unauffällig.
- Vermeintliches oder tatsächliches Fehlverhalten, wie z. B. Devisenvergehen, Verstöße gegen Zollbestimmungen, Ordnungswidrigkeiten oder sexuelle Aktivitäten, werden manchmal als Vorwand genommen, um Reisende zu erpressen.
- Schalten Sie bei Auftreten von Verdachtsmomenten im In- oder Ausland sofort die österreichischen Sicherheitsbehörden ein.

14. EMPFEHLUNGEN IM FALLE EINER TELEFONISCHEN BENACHRICHTIGUNG ÜBER DIE ENTFÜHRUNG EINES/R ANGEHÖRIGEN

- Telefongespräche sollten wenn möglich von weiteren Personen mitgehört und aufgenommen werden. Machen Sie zum Anruf Notizen.
- Wiederholen Sie die Anweisungen der Entführer in Ruhe, um Zeit zu gewinnen.
- Machen Sie dem Anrufer klar, dass man den Ernst der Lage erkannt hat und bereit ist, für die Freilassung der entführten Person alles im Sinne des Tatplanes zu erfüllen.

- Verlangen Sie Beweise für die Identität und die Situation der entführten Person.
- Verlängern Sie Gespräche mit dem Ziel, möglichst viele Informationen zu erlangen.
- Beachten, merken und notieren Sie Persönlichkeitsmerkmale (Stimme, Dialekt u. a.) des Anrufers sowie Hintergrundgeräusche. Nehmen Sie das Telefongespräch nach Möglichkeit auf.
- Vereinbaren Sie den nächsten Kontakt bzw. den nächsten Anruf.
- Stellen Sie so überzeugend wie möglich die Schwierigkeiten einer raschen Erfüllung der Forderungen dar.
- Informieren Sie unverzüglich Ihre/n Sicherheitsbeauftragt/n sowie die Polizei und besprechen Sie das weitere Verhalten.

Allgemeine Hinweise für Familienangehörige

- Informieren Sie Ihre Angehörigen stets über Aufenthaltsort und Rückkehrzeit.
- Wirken Sie auf Ihre Angehörigen ein, sich im Sinne dieser Sicherheitsempfehlungen zu verhalten.
- Wecken Sie bei Kindern Verständnis und Einsicht für bestimmte Sicherheitsvorkehrungen.
- Lassen Sie Kinder nicht ohne Aufsicht. Mindestens ein Elternteil muss wissen, wo sich die Kinder aufhalten und mit wem sie zusammen sind.
- Geben Sie dem Aufsichtspersonal von Schulen, Kindergärten, Sportvereinen etc. die Personen bekannt, die zur Abholung des Kindes/der Kinder berechtigt sind.

Empfehlung: Beratende Gespräche über das Verhalten bei einer Entführung können durch Spezialisten wie Polizei oder private Sicherheitsfirmen erfolgen.

Der Leitfaden wurde sorgfältig erstellt, dennoch wird vom BVT keine Haftung für die Vollständigkeit der Ratschläge und Empfehlungen übernommen.

NOTRUF- UND NOTFALLNUMMERN IN ÖSTERREICH

- Feuerwehr: 122
- Polizei: 133
- Euro-Notruf: 112
- Rettung: 144
- BVT-Journal: +43-1-53126-4100
- Notruf für Gehörlose (SMS-Dienst): 0800-133-133; gehoerlosennotruf@polizei.gv.at

KONTAKT- UND MELDESTELLEN

- SKI-Kontaktstelle im BVT: SKI@bvt.gv.at
- WIS-Kontaktstelle im BVT: WIS@bvt.gv.at
- BMI-Plattform zum Schutz von Unternehmen vor Wirtschafts- und Industriespionage: www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis/start.aspx
- Cybercrime Competence Center (C4): against_cybercrime@bmi.gv.at
- GovCERT – Computer Emergency Response Team: reports@govcert.gv.at

PORTALE

- CIWIN: https://ciwin.europa.eu
- IKT-Sicherheitsportal: www.onlinesicherheit.gv.at

HANDBÜCHER

- Österreichische Strategie für Cyber-Sicherheit: www.bka.gv.at
- Österreichisches Informationssicherheitshandbuch: www.sicherheitshandbuch.gv.at
- Broschüre „Sicherheit in öffentlichen Gebäuden“: www.bmi.gv.at
- „BVT-Sicherheitsinformation für Eigentümer/Betreiber kritischer Infrastruktureinrichtungen in Österreich“: www.bmi.gv.at
- Wirtschafts- und Industriespionage, Handbuch „Know-how-Schutz für die österreichische Wirtschaft“: www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis/start.aspx

IMPRESSUM

Medieninhaber:
Bundesministerium für Inneres,
Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung (BVT)

Redaktion:
BVT in Kooperation mit
LV Wien und LV OÖ, BMI, EKO Cobra,
BMI-IT-Sicherheitsbeauftragter

Layout und Fotos:
BMI I/8 - Protokoll und Veranstaltungsmanagement

Druck:
BMI/Digital Print Center

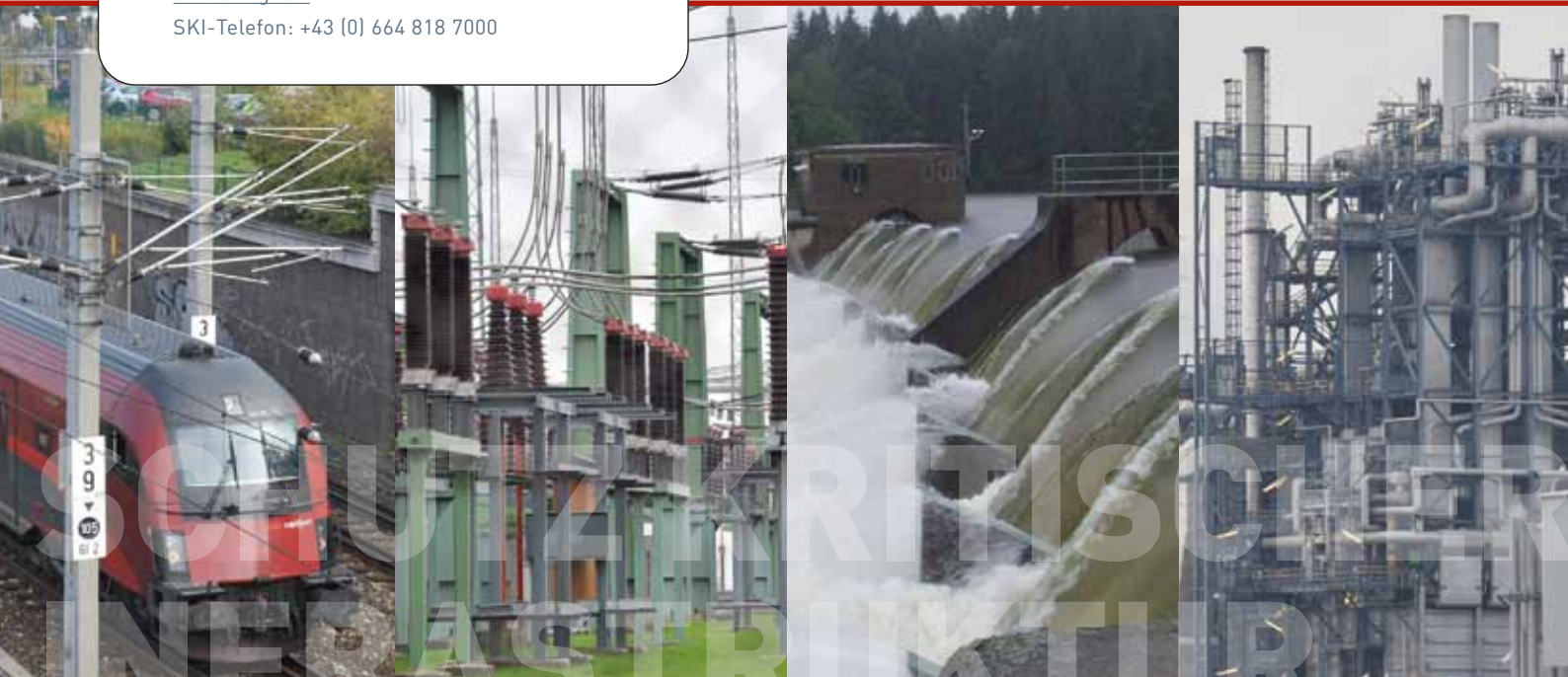
alle:
1014 Wien, Herrengasse 7
Postfach 100
Telefon: +43-1-53126-0
info@bmi.gv.at
www.bmi.gv.at

.BVT
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

ZENTRALE KONTAKT- UND MELDESTELLE

im Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

- Bietet Unterstützung, Beratung, Schulung oder weitere Informationen zum Thema
- Meldestelle für sicherheitsrelevante Vorfälle

SKI@bvt.gv.at

SKI-Telefon: +43 (0) 664 818 7000