Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

# Merkblatt zu „Cyber-Sicherheit im Home Office“

## Cyber-Sicherheit am Arbeitsgerät

### Physische Sicherheit

- Stellen Sie in den Zeiten aktiven Arbeitens sicher, dass Ihr Arbeitsplatz weder von Dritten eingesehen werden kann (Blickschutz), noch, dass dienstliche Kommunikation von Dritten mitgehört werden kann (Mitbewohnerinnen oder Mitbewohner, offene Fenster, Sprachassistenten).
- Stellen Sie in inaktiven Zeiten eine gesicherte Verwahrung aller Arbeitsgeräte sicher.
- Sorgen Sie beim vorübergehenden Verlassen des Heimarbeitsplatzes für eine geeignete Sperre Ihrer Arbeitsgeräte.

### Festplatten-Verschlüsselung

- Stellen Sie sicher, dass alle Datenträger, mit denen Sie einen gesicherten Bereich verlassen, stets verschlüsselt sind.
- Bedenken Sie, dass dies nicht nur Notebooks, sondern beispielsweise auch externe Festplatten und USB-Speichersticks betrifft.

### Sicherheits-Updates

- Spielen Sie alle für Ihre Arbeitsgeräte verfügbaren Sicherheits-Updates gewissenhaft und zeitnah ein.
- Werden Sie nach einem Sicherheits-Update von Ihrem System zu einem Neustart aufgefordert, sollten Sie diesen möglichst zeitnah durchführen.
- Deaktivieren Sie auf keinen Fall Funktionalitäten zum automatisierten Einspielen von Sicherheits-Updates.
- Setzen Sie keine Software ein, die vom Hersteller nicht mehr mit Updates oder Patches versorgt wird.

### Absicherung des Arbeitsgerätes

- Sichern Sie Ihr Arbeitsgerät mit Antivirensoftware und Firewall ab und deaktivieren Sie diese Programme keinesfalls.
- Halten Sie Ihre Antivirensoftware stets auf dem aktuellen Stand.

## Verbindung mit dem Firmenstandort

### Einrichtung einer sicheren Verbindung

- Greifen Sie ausschließlich über ein kryptographisch abgesichertes Virtual Private Network (VPN) auf das Unternehmensnetzwerk zu.
- Befolgen Sie alle Sicherheitsrichtlinien und Policies Ihres Unternehmens und führen Sie keinesfalls eigenmächtig Konfigurationsänderungen am VPN durch.
- Verwenden Sie ausschließlich die von Ihrem Unternehmen zur Verfügung gestellte Software.

### Mehrfaktor-Authentifizierung

- Wenn Ihnen bei der Nutzung eines Dienstes die Möglichkeit einer Mehrfaktor-Authentifizierung zur Verfügung gestellt wird, sollten Sie diese auf jeden Fall verwenden.

### E-Mail Verschlüsselung

- Unverschlüsselte E-Mails sind kein adäquates Medium, um vertrauliche Informationen über das öffentliche Internet auszutauschen.
- Befolgen Sie im Zusammenhang mit dem Versenden von E-Mails alle Richtlinien und Policies Ihres Unternehmens.

### Datenspeicherung

- Speichern Sie alle Daten nach Möglichkeit ausschließlich auf Servern im Unternehmensnetzwerk und greifen Sie über den Kommunikationskanal auf diese zu.
- Speichern Sie Daten nur im Ausnahmefall auf Ihrem lokalen Arbeitsgerät. Erstellen Sie in diesem Fall regelmäßig Sicherheitskopien der Daten und verwahren Sie diese an einem sicheren Ort.

## Sicheres Verhalten

### Exklusive Nutzung des Arbeitsgerätes

- Trennen Sie strikt zwischen dienstlichen und privaten Aufgaben und verwenden Sie nach Möglichkeit die Arbeitsgeräte des Home Office nicht für private Aktivitäten.
- Weichen Sie für die private Internetnutzung nach Möglichkeit auf alternative Geräte aus.
- Stellen Sie sicher, dass die Arbeitsgeräte auch in Ihrer Abwesenheit nicht durch Dritte (z. B. Familienmitglieder) benutzt werden können.

### Kennwortsicherheit

- Verwenden Sie stets starke Kennwörter, die Sie sich jedoch noch merken können.
- Ist es erforderlich, Zugangsdaten niederzuschreiben, verwahren Sie diese Unterlagen stets an einem sicheren Ort (z. B. Safe).
- Geben Sie Ihre persönlichen Zugangsdaten ausnahmslos an niemanden weiter.

### Social Engineering

- Befolgen Sie niemals Anweisungen eines unbekannten Anrufers bzw. geben Sie niemals vertrauliche Daten (z. B. Zugangsdaten) an unbekannte Anrufer weiter.
- Wenn Sie im Zusammenhang mit der Home Office-Nutzung an unerwarteter Stelle bzw. zu einem unerwarteten Zeitpunkt zur Eingabe von Zugangsdaten aufgefordert werden, sollten Sie dies vor einer etwaigen Eingabe mit Ihrem Unternehmen verifizieren.
- Führen Sie keine eigenmächtigen Softwareinstallationen (z. B. Fernwartungssoftware) oder Konfigurationsänderungen an den Kommunikationskanälen zum Unternehmen durch, außer es handelt sich um einen zuvor verifizierten Auftrag eines berechtigten Unternehmensvertreters.

### Phishing & Co

- Behandeln Sie unerwartete E-Mails oder E-Mails von unbekannten Absendern mit einem gesunden Maß an Skepsis.
- Machen Sie sich bewusst, dass Absenderadressen von E-Mails vergleichsweise leicht gefälscht werden können und keinesfalls wirklich vom angegebenen Absender stammen müssen.
- Öffnen Sie keine fragwürdigen E-Mail Attachments und klicken Sie niemals auf Hyperlinks in E-Mails.

### Nutzung von USB-Speichersticks

- Schließen Sie keine unbekannten USB-Geräte (insbesondere USB-Speichersticks) an Ihr Arbeitsgerät an.