

Checkliste für Unternehmen

# HOME OFFICE

Infrastruktur,  
Zugang und Policy

[www.g4c-ev.org](http://www.g4c-ev.org)

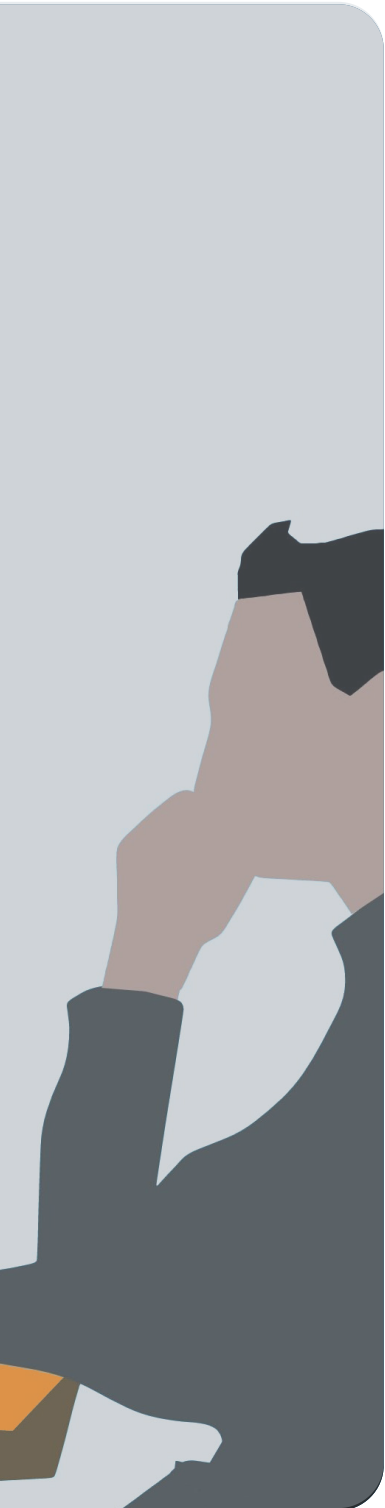
Unsere  
Kooperationspartner



Bundeskriminalamt



Bundesamt  
für Sicherheit in der  
Informationstechnik



## Vorwort

Das Dokument soll als Checkliste dienen, um Homeoffice Nutzer aus Sicherheitssicht vor Schaden zu schützen. Die Empfehlungen können je nach Bedarf angepasst oder erweitert werden und stammen aus Best Practices von Beratungsprojekten unterschiedlicher Industriekunden.

Es wird keine Gewähr übernommen auf Vollständigkeit und Umsetzbarkeit, da Sicherheitsaspekte von Unternehmen zu Unternehmen sehr unterschiedlich sein können. Die Punkte betreffen den Remote Betreiber/IT Abteilung und den Nutzer im Home Office.

# Home Office Anwender

## Private Netzwerkstrukturen

- **Standard Passwörter auf WLAN Access Point ändern**
- **Standard Passwörter von Routern ändern**
- **Sicheren WPA2 Standard als WLAN Verschlüsselung nutzen**
- **MAC Adressen Filter nutzen**
- **Verbreitung im gesamten Netzwerk**

## Passwörter und deren Verwendung

- **Stichwort Brute-Force-Attacke**
- **Passwörter sollten nicht dem „Duden“ entnommen werden**
- **Lange Passwörter nutzen und einer eigenständigen Bildungsregel folgen<sup>1</sup>**
- **Für jedes System, Systemzugang, Austauschplattform eigenständiges Passwort nutzen**

- **Passwörter in Passwort Safes pro Einsatzzweck und System ablegen, so dass nur ein Hauptpasswort eingepägt werden muss**

- » Mögliche Passwort Safes: s. Box
- » Aktuelle Software einsetzen
- » Aktualisierung der Windows Client Umgebung ständig überprüfen, wie Sicherheitsupdates von Herstellern
- » Remote Access für zentrale Sicherheitschecks einrichten.

## Mögliche Passwort Safes

- KeePass – Open Source
- 1Password
- PasswordSafe
- Kaspersky PasswordSafe
- andere Hersteller/Angebote

<sup>1</sup> <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html>



## Trickbetrügereien und Social Engineering mit dem Aufhänger Corona bzw. COVID19

- » Lassen Sie sich von allgemeinen Mails, Nachrichten etc. mit Corona bzw. COVID19 Bezug nicht verunsichern
- » Prüfen Sie bitte immer sorgfältig, von wem eine Nachricht oder Mail mit Corona bzw. COVID19 Bezug stammt
- » Versuchen Sie ggf. den Sachverhalt unabhängig zu überprüfen (z.B. Websuche mit Schlüsselwörtern der Nachricht)
- » Öffnen Sie bei "Corona-Mails" Ihnen unbekannter Absender keine Anhänge und leiten Sie solche Mails auch nicht unbedacht weiter
- » Lassen Sie Vorsicht walten und denken Sie genau nach, bevor Sie sich davon zu irgendwelchen Handlungen (z.B. Öffnen von Mail-Anhängen, Installation von Software, Weiterleiten an Freunde oder Kollegen etc.) verleiten lassen
- » Seien Sie selbst bei "Corona"-Mails oder -Nachrichten Ihnen bekannt erscheinender Absender vorsichtig und fragen Sie ggf. z.B. telefonisch nach, bevor sie z.B. Anhänge öffnen oder Software installieren

# Remote IT Organisation: Home Office Infrastruktur, Zugang und Policy

## ■ Systemzugänge mittels 2FA – Zwei-Faktor Authentifizierung sichern

- » Nutzung zwei unterschiedlicher Medien zu Benutzer Authentifizierung, neben der Password-eingabe wird ein zweiter Faktor, z.B. einmaliger Code, per SMS oder App dem Benutzer mitgeteilt, mit dem er sich am System final anmeldet

## ■ Sichere Kommunikation

- » Keine Nutzung von „öffentlichen“ Chat oder Social Medikanälen
- » Nutzung von Werkzeugen zur sicheren Kommunikation wie Microsoft Teams, Skype, verschlüsselte E-Mails
- » Messenger Nutzung wie z.B. Threema
- » E-Mail Programme bzw. Server bieten in aller Regel einen über https Verbindung erreichbaren WebClient an, über diesen können Home Office Benutzer Ihre geschäftlichen Mails weiterhin bearbeiten, ohne eine Weiterleitung auf nicht sichere Maildienste außerhalb des jeweiligen Unternehmens
- » Nutzung von VPN zwischen Home Office Arbeitsplatz und Unternehmen bereitstellen

## ■ Schutz der VPN-Server vor DDoS

- » Möglichst automatisierten Schutz der VPN-Server vor DDoS-Angriffen gewährleisten, da die VPN-Server für Home Office Mitarbeiter als Gateway zum internen Netzwerk eines Unternehmens fungieren
- » Wird ein VPN-Server durch DDoS angegriffen, werden dadurch alle Remote - Mitarbeiter daran gehindert, ihre Arbeit zu erledigen, was ein Unternehmen effektiv lahmlegen würde



### ■ **Bereitgestellte Sicherheitsupdates in Systeme und Komponenten einspielen, gilt für**

- » Netzwerkkomponenten
- » Betriebssystem
- » Anwendungen wie Office, Mail, Zusatz Software

### ■ **Daten Austausch**

- » Keine Daten in öffentlichen Speichern ablegen
- » Nutzung von USB Sticks, die Verschlüsselung ermöglichen
- » Daten bei Transport verschlüsseln, z.B. mittels Zip oder WinRar Datei packen und mit Passwort sichern
- » Daten für Home Office Mitarbeiter über sicheren Kommunikationsweg – VPN – und Dateistrukturen auf Dateiserver im Unternehmen bereitstellen

### ■ **Client Computer Nutzung**

- » Bereitstellung eigener Unternehmenshardware wie Notebook oder Mobiltelefon für Home Office Benutzer
- » Nutzung von Remote Desktop Verbindungen/ Windows Terminal Server über gesicherte Verbindung – wie VPN und/oder Webzugang mit SSL Verschlüsselung
- » Verschlüsselung der Client Hardware wie zum Beispiel Windows (Bitlocker) oder MacOS (FileVault)

### ■ **Kontinuierliche Datensicherung der mobilen Devices**

- » Sicherung der gesamten Festplatte und Boot-sector mittels Festplatten Image, z.B. Acronis True Image
- » Sicherung der realen Daten nach jedem Änderungsvorgang, vollständiges Backup wöchentlich, inkrementell täglich auf externe Festplatte, NAS Network Attached Storage (NAS)

### ■ **Client Software Firewalls einsetzen**

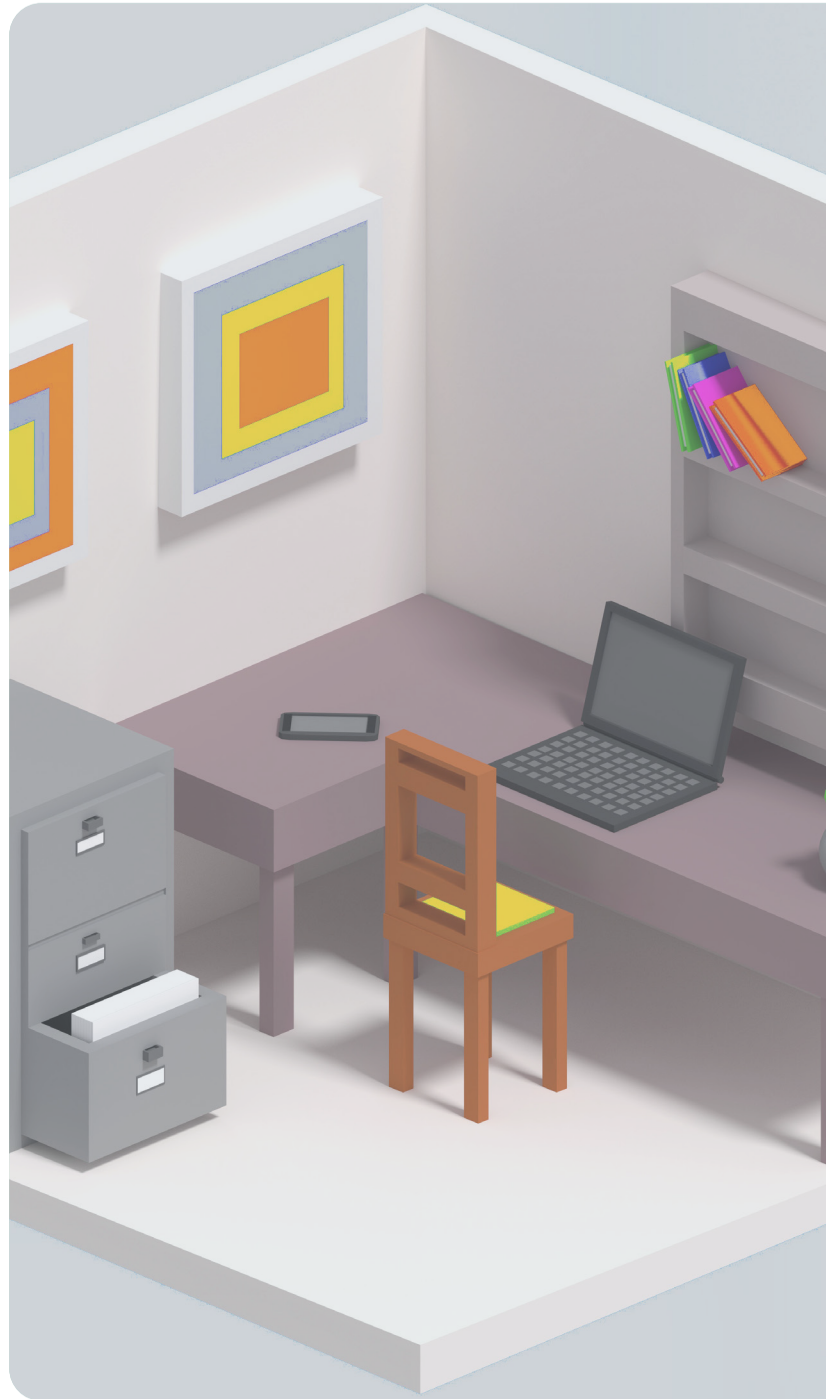
- » Home Office Benutzer sollten auf ihren Mobilien Endgeräte Software Firewalls installieren /installiert haben um die Kommunikation zusätzlich zu Router Firewalls abzusichern
- » Einsatz von Virens Scanner zwingend erforderlich und permanent updaten

### ■ **Personal Firewall**

- » Grundsätzlich gilt: was ich nicht im Unternehmens Büro öffnen würde, auch nicht im Home Office öffnen
- » „lieber einmal mehr nachfragen“ als einmal zu wenig, vor allem Nutzung eines anderen Kommunikationskanals
- » Kopf und Verstand einschalten

## ■ **Physischer Schutz**

- » Es sollten gleiche Anforderungen an den Home Office Arbeitsplatz gestellt werden wie auch an den tatsächlichen Unternehmens Arbeitsplatz
- » Zutritt zum möglichen Home Office Arbeitsplatz sollte nur Befugten möglich sein
- » Nicht einsehbar durch Fenster: Sichtschutzfolie, Vorhang, etc.
- » Geschlossene Fenster unter Windows Anwendungen
- » Sowohl vertrauliche als auch nicht-vertrauliche Dokumente sollten nicht „wahllos“ herumliegen und gesichert aufbewahrt werden
- » Genutzte Hardware wie PC, Notebook, Mobiltelefon, Tablet, sollten bei nicht Verwendung gesperrt werden





German Competence Centre  
against Cyber Crime e. V.



BECKER BÜTTNER HELD

Die Rechtsanwaltskanzlei Becker, Büttner,  
Held ist Kooperationspartner von G4C e.V.

Als gemeinnütziger Verein hat sich das German Competence Centre against Cybercrime (G4C) zum Ziel gesetzt, präventiv, ermittelnd und reaktiv gegen Angriffe im Cyberraum vorzugehen. G4C fungiert so als Know-how-Träger, Frühwarnsystem und Initiator eines regelmäßigen Austauschs über Bedrohungen aus dem Netz. Operative Kooperationspartner sind das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Darüber hinaus besteht auch international ein Informationsaustausch mit relevanten Stellen zur Bekämpfung von Cyberangriffen.

Die Arbeit des Vereins basiert auf vier Säulen: G4C baut sukzessive eine aktuelle Datenplattform neben dem direkten persönlichen Austausch als Frühwarnsystem aus, übernimmt Datenausleitungen für das BKA und andere Ermittlungsbehörden, und engagiert sich in der Aus- und Fortbildung sowie bei Zuverlässigkeitsüberprüfungen zur Kompetenzstärkung von Cybersicherheitsbeauftragten.

Gründer und Initialmitglieder von G4C sind Banken und Versicherungen; der Verein weitet seine Kompetenz jedoch konsequent auf weitere Branchen aus.

---

Alle Inhalte dieser Broschüre, insbesondere Texte, Bilder und Grafiken, sind urheberrechtlich geschützt. Die Verbreitung und Verwertung ist gestattet, solange diese nicht-kommerziell erfolgt. Die Vervielfältigung und Bearbeitung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung von G4C. Die Verwendung von Auszügen aus der Broschüre ist nur mit Quellenangabe gestattet.

## KONTAKT

Eintrag im Vereinsregister  
Wiesbaden VR 6806

[www.g4c-ev.org](http://www.g4c-ev.org)

Stand: Juni 2020

German Competence Centre  
against Cyber Crime e. V. (G4C e. V.)

Borsigstraße 36  
65205 Wiesbaden

Telefon: +49 6122 178 4800

Fax: +49 6122 178 4803

E-Mail: [info@g4c-ev.org](mailto:info@g4c-ev.org)