Management Summary

Das vorliegende Dokument soll als Checkliste dienen, um Homeoffice Nutzer aus Sicherheitssicht vor Schaden zu schützen. Die Empfehlungen können und müssen je nach Bedarf und tatsächlich gegebener Situation angepasst oder erweitert werden.

Die im nachfolgenden aufgeführten Themenkomplexe basieren auf Erfahrungen aus unterschiedlichen Kundenprojekten – unterschiedlicher Industrien.

Die in diesem Dokument bereitgestellten Informationen von Operatis Business Technology Consulting wurden mit großer Sorgfalt zusammengestellt. Es wird keine Gewähr auf Vollständigkeit und Umsetzbarkeit der zur Verfügung gestellten Informationen übernommen. Ebenfalls übernimmt Operatis Business Technology Consulting keine Haftung für eventuelle Folgen, wie Folgen aus Nutzung von Informationen, dem Vertrauen auf Informationen oder Folgen aus Aktionen, die aufgrund von Informationen basierend auf dem vorliegenden Dokument -als auch Informationen auf der Internetseite von Operatis Business Technology Consulting unternommen oder entstanden sind.

Die dargestellten Punkte sprechen unterschiedliche Sichtweisen, so den Betreiber einer Remote Verbindung, die IT Abteilung als auch den Nutzer im Home Office an.

Home Office Anwender / Verantwortlichkeit

Checks:

- 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

- Passwörter- und deren Verwendung
  - Stichwort Brute-Force-Attacke
  - Passwörter sollten nicht dem „Duden“ entnommen werden
  - Lange Passwörter nutzen und einer eigenständigen Bildungsregel folgen
    - Siehe: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html
  - Für jedes System, Systemzugang, Austauschplattform eigenständiges Passwort nutzen
  - Passwörter in Passwort Safes pro Eisatzzweck und System ablegen, so dass nur ein Hauptpasswort eingeprägt werden muss
    - Mögliche Passwort Safes: KeePass – Open Source; 1Password, PasswordSafe, Kaspersky PasswordSafe (Beispiel oder andere Hersteller Angebote)
    - Aktuelle Software einsetzten

Home Office Anwender / Verantwortlichkeit (Fortsetzung)

- Aktualisierung der Windows Client Umgebung ständig überprüfen, wie Sicherheitsupdates von Herstellern
- Remote Access für zentrale Sicherheitschecks einrichten

Remote IT-Organisation

Zielgruppen:

- **Home Office Infrastruktur**
- **Security Policy**

Checks:

- Systemzugänge mittels 2FA – Zwei-Faktor Authentifizierung sichern
  - Nutzung zwei unterschiedlicher Medien zu Benutzer Authentifizierung, neben der Passworteingabe 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 Mediakanäle
  - 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 http 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
- 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 nutzen
  - 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

Operatis Business Technology Consulting

Fürther Straße 6 ● 63607 Wächtersbach ● Mail: info@operatis-consulting.de ● Internet: www.operatis-consulting.de

Remote IT-Organisation (Fortsetzung)

- 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 Bespiel Windows (Bitlocker) oder MacOS (FileVault)
- Kontinuierliche Datensicherung der mobilen Devices
  - Sicherung der gesamte Festplatte und Bootsector 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 Mobilen Endgeräte Software Firewalls installieren / installiert haben um die Kommunikation zusätzlich zu Router Firewalls abzusichern
  - Einsatz von Virenscanner 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
  - Dokumente 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

Operatis Business Technology Consulting
Fürther Straße 6 ● 63607 Wächtersbach ● Mail: info@operatis-consulting.de ● Internet: www.operatis-consulting.de