CHECKLISTE HOME OFFICE

AUF WAS MAN ACHTEN MUSS

ZIELSETZUNG

Sensibilisierung der Home-Office Nutzer und deren Informatik

MITARBEITER

- Stellen Sie sicher, dass alle für den Fernzugriff verwendeten Geräte auf dem neuesten Stand sind (Patches), sowie ein aktueller Virenscanner installiert ist. Gilt grundsätzlich für alle Anwendungs-programme.
- Stellen Sie sicher dass Ihr lokaler Benutzeraccount passwortgeschützt ist und dieses Passwort bei den Angehörigen nicht bekannt ist.
- Erstellen Sie ein für Ihren Account ein starkes Passwort und nehmen Sie für jeden Dienst ein separates Passwort. Verzichten Sie auf «Sequenzen» in Passwörtern zu (z.B. Passwort1, Passwort2 usw.).
- Der Arbeitsplatz sollte so gewählt werden, dass von aussen keine Einblicke möglich sind. Dies gilt natürlich auch für den Ton.
- Wählen Sie den Platz an dem Sie Home-Office machen gut aus. Er sollte ruhig und separiert sein.
- Achten Sie darauf, dass Ihr Hintergrund keine privaten oder datenschutzrelevanten Daten oder Hinweise zeigt.
- In Videokonferenzen zeigt man gerne auf Dokumente, dazu schaltet man oft seinen Bildschirm frei. Achten Sie darauf, dass auch Ihr Desktop aufgeräumt ist und keine privaten Elemente zeigt.
- Schalten Sie alle privaten Programme aus, die Meldungen via popUp zeigen.
- Erstellen Sie Regeln mit Ihren Mitbewohnern, wie Sie sich verhalten sollen, wenn sie Home-Office machen.
- Wenn Ihnen Ihre Firma kein Notebook zur Verfügung stellt und Sie ihr persönliches Gerät fürs Homeoffice nutzen müssen, dieses aber nicht die neusten Sicherheitsrichtlinien erfüllt, gehen Sie keine Kompromisse ein! Melden Sie diese Umstände der Firma.
- Privaten und dienstlichen Rechner trennen. Falls nur ein Gerät verfügbar ist, achten Sie darauf, dass ein dienstliches und ein privates Profil (getrennte Log-ins) eingerichtet wird.
- WLAN mit Passwort sichern. Ein anderes Passwort als für den Rechner verwenden. Das WLAN so benennen, dass kein Rückschluss auf Sie möglich ist.

- Im Router WLAN-Verschlüsselung aktivieren.
- Bei seltsamen Betreffzeilen E-Mail erst gar nicht öffnen, sondern löschen und gelöschte E-Mail aus dem "Papierkorb" entfernen. Falls das Mail schon geöffnet wurde und verdächtig erscheint, nicht etwaige Anhänge öffnen. Die erste Firewall ist der gesunde Menschenverstand.

INFORMATIK

- Prüfen Sie die Logdaten Ihrer Geräte mit Fernzugriff laufend auf Anomalien (z.B. ausländische IP-Adressen, wenn die meisten Mitarbeitenden in der Schweiz tätig sind; IP-Adressen aus TOR Netzwerken; VPN oder generell Netzwerke von Hosting Providern
- Erzwingen Sie ein Tunneling für alle Geräte, um die sichere Kommunikation zu gewährleisten und Verbindungen ins Internet sichtbar zu machen.
- Planen Sie die Bereitschaft für forensische Analysen, insbesondere, wenn Sie Mitarbeitenden erlauben, mit ihren privaten Geräten auf das Unternehmensnetzwerk zuzugreifen.
- Die Aktualisierung der für den Fernzugriff verwendeten Geräte muss ohne physischen Präsenz im Unternehmen möglich sein.
- Stellen Sie sicher, dass von zuhause aus arbeitendem Personal keine Verbindung zwischen privatem und Unternehmensnetzwerk herstellen kann.

GESCHÄFTSLEITUNG

- Sensibilisieren Sie die Mitarbeitenden bezüglich Gefahren von Home-Office und kommunizieren Sie Kontaktinformationen für den Fall, dass die Mitarbeitenden etwas Verdächtiges feststellen.