Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: METHODIK

Checkliste für Mitarbeiter

IT-Sicherheit im Home-Office

Die folgenden Ausführungen sollten Mitarbeiter beim Wechsel ins Home-Office sorgfältig überprüfen. Durch die Berücksichtigung der jeweiligen Punkte kann das IT-Sicherheitsniveau und somit der Schutz von Unternehmensdaten signifikant verbessert werden.

- ☐ **Falls noch nicht vorhanden: Bitten Sie Ihren Arbeitgeber um die Bereitstellung der notwendigen IT-Ausstattung für zu Hause.**
  Hierzu zählen neben PC und Smartphone auch Zubehör, wie USB-Sticks und Netzteile.

- ☐ **Benutzen Sie sichere Passwörter.**
  Je länger desto besser – zwölf Zeichen sind ein guter Schutz. Verwenden Sie nicht das gleiche Passwort für mehrere Konten.
  Weiterführende Informationen finden Sie hier:
  https://www.bsi.bund.de/Passwoerter

- ☐ **Übertragen Sie die erarbeiteten Daten regelmäßig auf das zentrale Firmensystem.**
  Sollten Sie keinen Firmen-PC haben, werden die auf privaten Endgeräten verarbeiteten Daten nicht durch die Sicherheitsmechanismen Ihres Unternehmens geschützt. Ein regelmäßiger Transfer der Daten ist daher unbedingt zu empfehlen. Reden Sie mit Ihrem Administrator, wie diese Übertragung sicher realisiert werden kann.

- ☐ **Schützen Sie Ihre Technik mit regelmäßigen Updates.**
  Aktualisieren Sie Virenscanner und installierte Anwendungen. Wenn Sie dazu Fragen haben, können Sie bei der IT-Abteilung Ihres Unternehmens nachfragen.

- ☐ **Schützen Sie Ihren WLAN-Router vor unerlaubtem Zugriff.**
  Sofern Sie das Passwort noch nie geändert haben: Stellen Sie sicher, dass es sich hierbei nicht um Standard-Zugangsdaten handelt, die von Angreifern z.B. in der Bedienungsanleitung auf der Herstellerwebseite recherchiert werden können. Aufgrund des besonders hohen Schutzbedarfs eines WLANs sollte das Passwort mindestens 18 Zeichen lang sein.

- ☐ **Im Home-Office ist das kurze „Türangel-Gespräch“ nicht möglich.**
  Zum schnellen Austausch werden u.a. Messenger sowie Telefon- oder Videokonferenz-Systeme benutzt. Verwenden Sie nur Dienste, die Ihr Arbeitgeber autorisiert hat.

- ☐ **Die Zahl der Phishing-Mails mit Corona-Betreff hat stark zugenommen.**
  Liegt Ihnen eine Liste mit Kontaktpersonen vor, bei denen Sie sich im Zweifelsfall wegen einer Mail rückversichern und den Absender verifizieren können? Wünscht sich Ihr Chef eine kurzfristige Kontoänderung, die Sie sich nicht erklären können? Hacker wenden diese Methode des CEO-Frauds an, um Gelder aus Unternehmen abzuziehen. Hier kann eine kurze Rückfrage an der richtigen Stelle großen Schaden abwehren.

- ☐ **Hängen Sie sich Zuhause die IT-Notfallkarte hin, sodass Sie auch hier schnell reagieren können.**
  Kommt Ihnen Ihre Firmentechnik abhanden, sollten Sie ebenfalls die IT-Notfallnummer/IT-Support Ihres Unternehmens anrufen. Download der Karte:
  https://www.allianz-fuer-cybersicherheit.de/ACS/IT-Notfallkarte

- ☐ **Stellen Sie sicher, dass nur Sie Zugriff auf die Firmen-IT haben.**
  Auch zu Hause können immer wieder Situationen entstehen, in denen Unbefugte Zugriff auf Ihre IT erhalten oder Daten einsehen können – zum Beispiel dann, wenn sich Handwerker in Ihrer Wohnung aufhalten oder wenn Sie mit dem Laptop auf dem Balkon arbeiten. Ergreifen Sie in diesen Situationen entsprechende Maßnahmen, die Zugriffe und Einblicke verhindern.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.