CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

CSBW-Factsheet: Cybersecurity-Wissen kompakt

HOMEOFFICE

Personen im Homeoffice sind ein leichtes Angriffsziel. Tipps zu Ihrem Schutz!

Die Arbeit im Homeoffice führt zu mehr Verantwortung der einzelnen Beschäftigten bei der IT-Sicherheit. Denn technische und organisatorische Maßnahmen, die innerhalb einer Institution zentral geregelt sind, müssen aktiv auf das Arbeitsumfeld zuhause übertragen werden.

Die Gefahren im Homeoffice:

Im Homeoffice sind Ihre Daten und sensible Informationen anderen Gefahren ausgesetzt als in geschützten Büroräumen.

Während einer Video-Konferenz, ob im Haus oder im Garten, können andere Personen Ihre Gespräche mithören und so an vertrauliche Informationen gelangen.

Ebenso kann ein nicht ausreichend abgesichertes Heim-Netzwerk angegriffen und somit Zugang zu vertraulichen Informationen erlangt werden.

Sorgen Sie daher an Ihrem Heimarbeitsplatz stets für ausreichende Schutzmaßnahmen.

Was ist ein VPN und was kann es?

- VPN steht für **V**irtual **P**rivate **N**etwork, also ein virtuelles privates Netzwerk.
- Es ermöglicht den geschützten **Zugriff von außerhalb** auf ein bestehendes Netzwerk. Sie können beispielsweise von zu Hause auf Ihre betrieblichen Ordner und Anwendungen zugreifen.
- Dabei wird der **Datenverkehr verschlüsselt** und zugleich die eigene Online-Identität verschleiert.
- Es schützt die Datenübertragung zwischen dem von Ihnen genutzten PC und dem Server Ihres Arbeitsgebers zuverlässig.
- Achten Sie auf die regelmäßige Aktualisierung der Software.

Quellen:
[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/home-office_node.html
[2] https://blog.academy.fraunhofer.de/blogbeitraege/llcs-zuhause-ist-man-co-sicherheitsbeauftragter/#1

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

Handlungsempfehlungen:

Sichere Internetverbindung

- Aktivieren Sie immer Ihre **VPN-Verbindung**, wenn Sie außerhalb Ihres Büros auf geschäftliche Daten zugreifen oder mit dem Internet verbunden sind.[1]

Nutzung privater Hardware

- Nutzen Sie möglichst keine private Hardware, da diese nicht den gleichen strengen Sicherheitsanforderungen wie betriebliche Hardware unterliegt.
- Falls nicht vermeidbar, klären Sie mit Ihrer IT-Abteilung, inwiefern Sie private Hardware verwenden dürfen.

Umgang mit geschäftlichen Dokumenten und Arbeitsmaterialien

- Lassen Sie keine geschäftlichen Dokumente an Ihrem Schreibtisch zurück, wenn Sie Ihren Arbeitsplatz verlassen. Bewahren Sie Dokumente während Ihrer Abwesenheit verschlossen auf.
- **Entsorgen** Sie dienstliche Dokumente und Datenträger niemals über den Hausmüll. Durch unsachgemäße Entsorgung können Angreifende wichtige Informationen gewinnen.
- Geben Sie Datenträger zur sicheren Vernichtung an Ihre IT-Abteilung zurück und machen Sie Dokumente vor der Entsorgung mit einem Aktenvernichter unkenntlich.

Arbeitsumfeld [2]

- Richten Sie sich möglichst einen klar definierten Arbeitsplatz ein. Vermeiden Sie die Arbeit auf dem Balkon oder im Garten.
- Achten Sie darauf, dass Unbefugte keine Gespräche mithören bzw. auf Ihren Bildschirm schauen können.
- **Sperren** Sie immer Ihren PC beim Verlassen des Arbeitsplatzes.

CSBW – Abteilung 1: Prävention – Stand 03.2023
Kontakt: schulungen@cybersicherheit.bwl.de