5 Empfehlungen für KMU mit Homeoffice

Im Homeoffice wird die sichere, organisierte und kontrollierte Firmenumgebung verlassen. Dieser Umstand erfordert spezielle technische, organisatorische und personenbezogene Massnahmen, um die Sicherheit der Firmendaten zu gewährleisten.

In einem Homeoffice kann nicht die gleiche Infrastruktursicherheit gewährleistet werden wie in den Firmenräumlichkeiten. Der Arbeitsplatz ist möglicherweise auch für Familienmitglieder oder Besucher zugänglich, Familienmitglieder arbeiten eventuell am gleichen Gerät, welches auch für die Arbeit bestimmt ist und im Zuge einer möglichen BYOD (Bring your own Device) Strategie gelangen Firmendaten auf die privaten Geräte der Mitarbeitenden.

Was muss ich nun als Unternehmen vorkehren, um mit dieser speziellen Situation umzugehen und die Sicherheit zu gewährleisten? Die nachfolgenden fünf Empfehlungen richten sich an Unternehmen, mit Mitarbeitenden im Homeoffice.

Empfehlungen für die Mitarbeitenden selbst finden Sie in unserem Artikel «5 Empfehlungen für Mitarbeitende im Homeoffice» (https://www.ebas.ch/5-empfehlungen-fuer-mitarbeiter-im-homeoffice/) .

1. Homeoffice Richtlinie

Eine Regelung wie Mitarbeitende sich im Homeoffice um die Vertraulichkeit, Integrität und Verfügbarkeit der Firmeninformationen zu kümmern haben bildet die Grundlage und ist unerlässlich. Empfehlenswert ist es, dies in einer Homeoffice-Richtlinie festzuhalten und den Mitarbeitenden zu kommunizieren. In einer solchen Richtlinie sollten mindestens folgende Punkte geregelt werden:

- Generelle Themen, wie Arbeitszeitregelung, Reaktionszeiten, Arbeitsmittel, Sicherheitsmassnahmen, Datensicherung, Datenschutz, Datenkommunikation, Meldewege, Zutrittsrecht zum Homeoffice, Transport von Informationen und Geräte, Autorisierungen.
- Verhalten und Vorgehen im Krisenfall: Sind viele Mitarbeitende im Homeoffice und die üblichen Kommunikationswege versagen oder sind eingeschränkt, kann es zu massivem Arbeitsausfall und somit zu einer sehr eingeschränkten Krisenbewältigung führen.

Für eine erfolgreiche Umsetzung dieser Richtlinie ist es unerlässlich, entsprechende Sensibilisierungen, Schulungen und Kontrollen durchzuführen.

2. Handhabung der Homeoffice-Infrastruktur und der Verbindung ins Firmennetzwerk

Für die Infrastruktur im Homeoffice sind angemessene Sicherheitsmassnahmen vorzuschreiben. Dies beinhaltet insbesondere den Umgang mit Updates, Virenschutz, Firewall, Betriebssysteme mit Benutzertrennung, Verschlüsselung etc. Die Firma soll durch IT-Support und den Sicherheitsbeauftragten die Homeoffice-Mitarbeitende in der Absicherung von solchen Geräten unterstützen und beraten. Hierzu ist unbedingt zu beachten, dass die Verbindung zwischen den Geräten im Homeoffice und dem Unternehmensnetzwerk speziell geschützt ist, z.B. über ein VPN

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

mittels 2-Faktor-Authentifizierung oder verschlüsselter Remote-Desktop-Verbindung.

3. Akten- und Datenträgertransport

Zwangsläufig werden Dokumente, Datenträger und IT-Geräte von der Firma zum Homeoffice transportiert. Dabei können diese Daten und Geräte verloren gehen, von unbefugten Dritten entwendet, gelesen und/oder manipuliert werden. So kann es zu Verlust der Vertraulichkeit, Integrität und Verfügbarkeit kommen. Hierzu sind folgende Punkte zu beachten:

- Firmengeräte, Datenträger und Dokumente sind möglichst auf direktem Wege von der Firma ins Homeoffice zu bringen.
- Werden sehr sensible (z.B. vertrauliche oder gar streng vertrauliche Dokumente, Datenträger oder Firmengeräte) ins Homeoffice transportiert, muss die vorgesetzte Person darüber in Kenntnis gesetzt, die Person dafür autorisiert und der Vorgang dokumentiert werden. Diese sensiblen Dokumente sollten idealerweise in einem verschliessbaren Behälter (z.B. Aktenkoffer) transportiert und aufbewahrt werden.

4. Zugang zu Firmeninformationen durch Dritte

Werden im Homeoffice schützenswerte Informationen bearbeitet oder aufbewahrt, sind diese auch in den privaten Räumen entsprechend zu schützen. Betreten Dritte diese Räume unbeaufsichtigt, kann der Schutz der Informationen gefährdet sein. Hierzu sind mindestens folgende Punkte zu beachten:

- Der Arbeitsplatz im Homeoffice sollte sich in einem eigenen Raum befinden, welcher ausschliesslich der beruflichen Tätigkeit dient und insbesondere abschliessbar ist.
- Vertrauliche Dokumente, Datenträger und Firmengeräte müssen im Homeoffice in einem verschliessbaren Bereich (z.B. Schrank, Schreibtisch) verstaut werden, sobald nicht mehr daran gearbeitet wird.

5. Entsorgung von Datenträgern und Dokumenten

Fehlt im Homeoffice eine geeignete Entsorgungsmöglichkeit für Dokumente und Datenträger, können Firmeninformationen via Hausmüll oder normaler Altpapiersammlung schnell in falsche Hände geraten. Hierzu sind folgende Punkte zu beachten:

- Datenträger und Firmengeräte werden generell nur von der IT der Firma entsorgt, damit diese sicher gelöscht und nicht mehr wiederhergestellt werden können.
- Papier-Dokumente müssen auch im Homeoffice entsprechend ihrer Vertraulichkeit korrekt entsorgt werden. Je nach Aufgabegebiet und Bedarf ist es sinnvoll den entsprechenden Mitarbeitenden einen Schreder zur Verfügung zu stellen.

Das Homeoffice (früher auch Telearbeit genannt) ist eine Form der Flexibilisierung von Arbeit in räumlicher und meist auch zeitlicher Hinsicht. Der Arbeitsauftrag wird dabei meist im privaten Umfeld (Zuhause) erfüllt. Unter dem Begriff Mobile Arbeit (engl. Remote Work) wird der Arbeitsauftrag ohne festen Arbeitsplatz erfüllt. In diesem Artikel werden die beiden Definitionen unter dem Begriff Homeoffice zusammengeführt.

Copyright © 2024 – Alle Rechte vorbehalten. Hochschule Luzern – Informatik