63341

13/ 2021

OKTOBER

Führung & Management AKTUELL

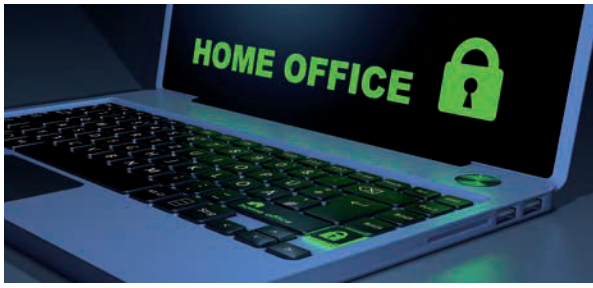
Mitarbeiterführung · Motivation · Selbst- und Zeitmanagement

INHALT

BESSER ENTSCHEIDEN

Datensicherheit im Homeoffice

Beim Thema Homeoffice geht es um Vertrauen. Vertrauen, dass Mitarbeiter zu Hause ebenso engagiert arbeiten wie im Büro. Vertrauen, dass Kollegen konzentriert bleiben und produktive Entscheidungen sogar am Küchentisch funktionieren. Was viele Unternehmen beim mobilen Arbeiten übersehen: die Datensicherheit.



Als zu Beginn der Pandemie Tausende Arbeitsplätze kurzfristig ins Homeoffice verlagert wurden, war fehlender Datenschutz kein Argument. Priorität hatte die Gesundheit der Mitarbeiter und dass der Betrieb irgendwie weitergeht. Doch jetzt, ein Jahr später, gilt diese Ausrede für mangelnde Datensicherheit nicht mehr.

HINWEIS

Unternehmen stehen jetzt in der Rechenschaftspflicht. Inzwischen ist die Datenschutz-Grundverordnung (DSGVO) kein Papiertiger mehr, sondern hat Zähne bekommen. Für Unternehmer bedeutet das: Die Umsetzung muss zur Chefsache werden. Früher musste die Aufsichtsbehörde Betrieben nachweisen, dass sie Datenschutz nicht umsetzen. Ähnlich wie bei einer Betriebsprüfung des Finanzamts.

Es kann richtig teuer werden!

Heute ist es genau andersherum: Auf Nachfrage müssen Firmen belegen, dass sie die DSGVO einhalten. Ein Brief der Behörde reicht aus, um die DSGVO-Konformität auf den Prüfstand zu stellen. In diesem wird der Verantwortliche aufgefordert, in einer Frist von zwei bis vier Wochen bestimmte Papiere nachzuweisen – z. B. das Verzeichnis von Verarbeitungstätigkeiten, die Dokumentation über technische und organisatorische Maßnahmen oder eine Beschreibung darüber, wie Unternehmen im Falle von Datenschutzpannen vorgehen. Wer all das nicht vorzeigen kann, dem droht Bußgeld (bis zu 20.000.000 € bzw. 4 % vom Jahresumsatz).

Die DSGVO und das BDSG (Bundesdatenschutzgesetz) sehen vor, dass Unternehmen einen Datenschutzbeauftragten benennen. Seine Aufgabe ist es, datenschutzfreundliche Lösungen zu empfehlen und Verantwortliche zu unterstützen, alle Anforderungen DSGVO-konform umzusetzen. Unternehmen mit weniger als 20 Mitarbeitern müssen niemanden beauftragen – sie können es freiwillig. Ohne Beauftragten steht der Inhaber selbst in der Pflicht, sich um die Maßnahmen zu kümmern.

Das viel größere Risiko: Sie werden gehackt

Die Gefahr für Pannen und Hackerangriffe ist bei Telearbeitsplätzen besonders groß. Chef und Team rätseln

Die richtige Mentalität

Liebe Leserinnen, liebe Leser,

zur Mentalität einer Führungskraft gehört es, die Mitarbeiter nicht allein zu lassen. Auch dann nicht, wenn sie außer Sichtweite im Homeoffice arbeiten. Und im Gegenzug sollten die Mitarbeiter ein Gespür für die Sicherheitsrisiken im Homeoffice entwickeln. Auch das eine Frage der Mentalität, inwieweit man ein Verständnis für die eigene Verantwortung entwickelt und dann dementsprechend handelt. Bei zwei weiteren Artikeln steht das Thema Mentalität noch stärker im Fokus der Empfehlungen: beim Thema Serviceorientierung (Seite 7) und ebenfalls beim Thema Diversität (Seite 5). Denn bei Letzterem geht es um Toleranz, Neugier und Verständnis, und das ist eine pure Frage der Mentalität, die Sie aber gezielt entwickeln und fördern müssen.

Ihr

Gerhard Tinnefeldt

Gerhard Tinnefeldt ist Wirtschaftspsychologe und arbeitet als Karrierecoach sowie als Berater und Trainer im Bereich Führung, Kommunikation und Personalauswahl.

LOGIN: IHRE MEDIATHEK!

www.fum-gwi.de

Benutzername:
fum
Passwort Oktober:
kompetenz21

DIREKTER KONTAKT:

redaktion-management@weka.de

dabei fast immer über dieselben Themen: Dürfen Mitarbeiter mit dem Privatlaptop arbeiten? Unter welchen Umständen können Kollegen das Diensthandy für private Zwecke nutzen? Wie funktioniert ein sicheres Webmeeting? Schon zu einer einfachen Frage spuckt das Internet viele konträre Ergebnisse aus. Sogar Datenschutzbehörden widersprechen sich. Um Kapitän und Mannschaft Sicherheit zu geben, im Folgenden die wichtigsten Infos im Überblick:

Die fünf wichtigsten Säulen für den Datenschutz

1. Hardware & Telefon
Um Datenschutz im Homeoffice zu optimieren, sollten Arbeitgeber sowohl Hardware als auch Smartphone stellen und für die Mitarbeiter einrichten. Das sorgt nicht nur für optimale Kompatibilität, sondern legt die Basis für hochwertigen Schutz. Nur in Ausnahmefällen wie spontanen Quarantänephasen oder Ähnliches sollten private Endgeräte zum Einsatz kommen.

2. Software & Tunnel
Um sich vor Hackern zu schützen, müssen Unternehmer die Software im Blick haben. Hier geht es z. B. um einen VPN-Tunnel ins Büro. Zur sicheren IT gehören auch Firewalls und Anti-Viren-Programme. Auf jedem Rechner müssen entsprechende Anwendungen installiert sein. Bei typischen Büroverarbeitungen reichen die Windows-Angebote im Regelfall aus. Doch alle Schutzmaßnahmen helfen nicht, wenn Systeme veraltet sind. Spielen Sie also Updates und Patches zeitnah ein. Wichtig ist auch, alte Systeme zu deinstallieren. Gerade bei diesen Softwareleichen besteht erhöhte Gefahr, dass Hacker durchkommen.

3. Passwörter & Blickschutz
Wer mobil arbeitet, muss aufpassen, dass vertrauliche Telefonate nicht mitgehört werden – ob am Küchentisch, auf der Parkbank oder im Zug. Die Diskretion der Daten und Gespräche muss gewährt bleiben. Zudem sollten Laptop, Smartphone sowie Festplatte mit Passwörtern geschützt sein. Auch Programme brauchen Kennwortschutz.

4. E-Mails & Phishing-Schutz
Die meisten Hackerangriffe gelingen aufgrund geöffneter E-Mail-Anhänge. Führungskräfte sollten Sorge tragen, dass Mitarbeiter mit elektronischer Post sensibel umgehen. Per Mail übermittelte Text-, Bild- oder Datendateien dürfen nicht ohne Prüfung des Absenders und Echtheit geöffnet werden. So können gefährliche Schadprogramme Schwachstellen von Software oder Betriebssystem ausnutzen und Viren oder Trojaner ins System gelangen.

5. Richtlinien für Webmeetings
Mittlerweile gehören Videocalls zum festen Repertoire in der Fernarbeit. Bevor Unternehmen sich für einen Anbieter entscheiden, stellt sich die Frage nach dem Einsatzzweck. Führen Sie große Veranstaltungen mit mehreren Hundert Teilnehmern durch? Oder brauchen Sie die Videocalls eher für vertrauliche 1:1-Coaching-Gespräche? Liegt der Fokus auf Status-quo-Meetings oder kreativen Workshops? Egal, für welches Werkzeug Betriebe sich entscheiden: Auch hier brauchen Mitarbeiter Orientierung für den Umgang. Klare Richtlinien regeln z. B., ab wann ein Webmeeting Passwortschutz braucht oder wie das Team die Chat-Funktion nutzen darf. Auch ein Online-Knigge mit Verhaltens-, Kleidungs- und Kommunikationsregeln gibt Sicherheit.

EXPERTEN-TIPP

Unternehmen sollten genau regeln, unter welchen Umständen ein Mitarbeiter seinen eigenen Laptop fürs Geschäft nutzen darf. Der Fachbegriff für die betriebliche Nutzung privater Hardware lautet: BYOD – Bring Your Own Device.

EXPERTEN-TIPP

Für Kennworte sind acht bis zwölf Sonderzeichen („x4p2$o9?q2Sd“) empfehlenswert oder ein kurzer Satz über 20 Zeichen („Ichesseseitjahrengerne Sushi!“). Ist das Passwort lang genug und steht nicht auf einem Notizzettel, muss es auch nicht mehr in kurzen Abständen geändert werden. Um den Bildschirm von Blicken abzuschirmen, eignen sich Blickschutzfolien.

EXPERTEN-TIPP

Um Mitarbeiter zu sensibilisieren, helfen Phishing-Simulationen. Dabei werden fingierte Spam-E-Mails an alle Mitarbeiter gesandt. Wer die Mail öffnet, gelangt auf eine Lernseite.

Panne? Frag den Datenschutzprofi

Kommt es trotz aller Vorsicht zu einer Datenlücke, heißt es: Ruhe bewahren – und den Verantwortlichen informieren. Innerhalb von 72 Stunden muss er entscheiden: Handelt es sich um einen meldepflichtigen Vorfall oder nicht? Worst Case wäre, wenn die Aufsicht von der Panne erst durch einen Betroffenen erfährt. Egal, wer den Verteiler transparent gemacht oder aus Versehen persönliche Daten weitergegeben hat – verantwortlich bleibt immer der Inhaber, Geschäftsführer oder Vorstand. Trotzdem tragen Beschäftigte im Homeoffice höhere Verantwortung: Wer als Mitarbeiter vorsätzlich oder grob fahrlässig handelt, wird ebenfalls dafür geradestehen müssen.

HINWEIS

Unternehmen sollten Datenschutz nicht als Problem, sondern als Hilfsmittel verstehen. Schließlich geht es um die Privatsphäre der Mitarbeiter sowie um den Schutz von Firmengeheimnissen. Beides ist beim mobilen Arbeiten besonders gefährdet. Nur wenn die Daten im mobilen Büro ebenso geschützt sind wie innerhalb des Firmengebäudes, ist Homeoffice ein sicheres Zukunftsmodell.

INTERNET-TIPP

Wer sein Team zuverlässig ins Thema einweisen will, steht bei folgender Onlineschulung auf der sicheren Seite: Datenschutz im Homeoffice. Innerhalb von 20 Minuten erhalten die Teilnehmer alle relevanten Infos zum Thema und nach erfolgreichem Abschlusstest ein Zertifikat. ■

Autor: Achim Barth versteht sich als digitaler Aufklärer, der die Tricks der Datenräuber kennt, aber eben auch die Wege, wie man sich im Netz schützen kann.