
# Im Home Office an der langen Leine? Besser nicht!

Wir haben Ihnen im vorangegangen Artikel bereits einige Gefahren vorgestellt, die das Home Office für Ihre IT-Sicherheit darstellt. Ein wichtiger Faktor zum Schutz Ihres Netzwerks – und da sind sich die Experten einig – ist es, Ihre Mitarbeiter auf eine sensible Internetnutzung hinzuweisen. So ließen sich laut „Bundeslagebild Cybercrime 2019“ des BKA bereits viele Gefahren vermeiden. Welche Regeln und Hinweise Sie Ihren Mitarbeitern geben sollten, lesen Sie hier.

## Auf Cybercrime sensibilisieren

Manche Arbeitnehmer werden im Home Office abgelenkt und fallen so schneller auf  Cyber-Attacken herein. Schulen Sie Ihre Mitarbeiter und kommunizieren Sie regelmäßig, worauf geachtet werden sollte und was die neuesten Angriffsstrategien der Cyberkriminellen sind.

## WLAN-Netzwerke und private IT-Geräte

Weisen Sie Ihre Mitarbeiter darauf hin, regelmäßige Router-Updates durchzuführen und unbedingt ein neues, nicht standardmäßig vergebenes WLAN-Passwort zu definieren. Es bietet sich zudem an, Ihren Mitarbeitern zu Routern zu raten, die ein sicheres Verschlüsselungsverfahren nutzen. Legen Sie ebenso fest, dass Ihre Mitarbeiter keine privaten IT-Geräte wie Laufwerke oder USB-Sticks mit ihren Firmen-PCs verwenden und auch keine Verbindung zu Cloud-Diensten herstellen, die sie privat nutzen.

## Vorsicht vor der Einsicht durch Dritte

Das Home Office ist nicht das Büro. Da Mitarbeiter häufig am Küchentisch oder im Schlafzimmer arbeiten, kann nicht ausgeschlossen werden, dass Dritte Einsicht in datenschutzrelevante Inhalte bekommen.

## Betriebsübliche Arbeitszeiten einhalten

Auch im Home Office gelten die normalen Arbeitszeiten. Bitten Sie Ihre Mitarbeiter, diese weitestgehend einzuhalten, denn damit wird einerseits die Zusammenarbeit leichter, andererseits können so die üblichen Geschäftszeiten eingehalten werden.

## Unterstützung gefällig?

Wir helfen Ihnen gern dabei, den Arbeitsplatz Ihrer Mitarbeiter im Home Office sicher zu gestalten. Selbstverständlich sind wir auch für Sie da, wenn Ihr Unternehmen bereits Opfer einer Cyberattacke geworden ist. Merken Sie sich jedoch: Vorsicht ist besser als Nachsicht. Warten Sie nicht, sondern kommunizieren Sie unsere Tipps schnellstmöglich an Ihre Mitarbeiter.