Deloitte.

Deloitte Cyber Security Report 2021

Home Office als Risikofaktor für Österreichs Unternehmen

Eine Studie von Deloitte Österreich in Kooperation mit SORA

MAKING AN IMPACT THAT MATTERS since 1845

Impressum

Herausgegeben von Deloitte Services Wirtschaftsprüfungs GmbH
Autoren: Alexander Ruzicka und Andreas Niederbacher
unter redaktioneller Mitarbeit von Armin Nowshad, Gina Grassmann und Tamara Spiegel
Grafik und Layout: Claudia Hussovits

Vorwort

Mit März 2020 hat sich die Arbeitssituation für die meisten Österreicherinnen und Österreicher durch die Corona-Pandemie von heute auf morgen nachhaltig verändert: Der Arbeitsalltag wurde zum Großteil ins Home Office verlagert. Auch heute arbeiten viele noch zumindest teilweise von zu Hause aus. Durch diesen neuen Arbeitsmodus haben sich im vergangenen Jahr vielerorts neue Sicherheitslücken im Bereich Cyber Security offenbart: Denn im Home Office haben die Unternehmen weniger Kontrolle über die Sicherheit ihrer Informationen und Daten, die Mitarbeiterinnen und Mitarbeiter wiederum sind sich mancher Risiken nicht bewusst.

Seit 2019 erheben wir gemeinsam mit SORA den Status quo österreichischer Unternehmen beim Thema Cyber Security. Während in den Vorjahren die Entscheidungsträgerinnen und Entscheidungsträger österreichischer Unternehmen befragt wurden, werden in diesem Jahr aus gegebenem Anlass die Mitarbeiterinnen und Mitarbeiter und deren Situation betrachtet: Wie ist ihre Arbeitssituation im Home Office? Wie steht es um ihre Cyber-Security-Awareness in den eigenen vier Wänden? Und gibt es ausreichend Unterstützung seitens der Unternehmen bei dieser Thematik?

Auf den nächsten Seiten finden Sie die Antworten auf diese und viele weitere Fragen.

Wir wünschen eine spannende Lektüre!

Alexander Ruzicka &
Andreas Niederbacher

Alexander Ruzicka
Partner | Risk Advisory

Andreas Niederbacher
Senior Manager | Risk Advisory

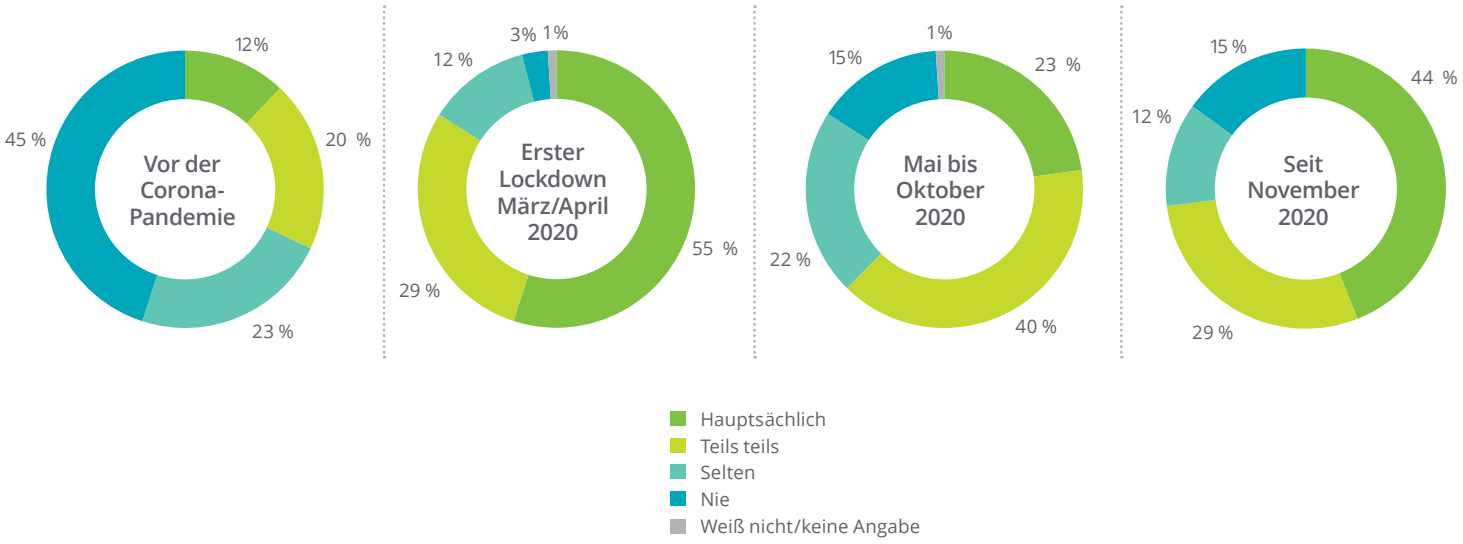
Home Office in der Corona-Pandemie

Durch COVID-19 mussten viele Unternehmen ihren Betrieb zum Teil ins Home Office verlagern. Das zeigt auch die Studie: Im Zeitverlauf wird deutlich, dass die Home-Office-Nutzung vor allem in den Lockdown-Phasen stark zugenommen hat.

Für die vorliegende Studie wurden insgesamt 500 unselbständig Beschäftigte telefonisch befragt, die seit Beginn der Corona-Pandemie zumindest fallweise im Home Office am PC oder Laptop tätig waren.

Während vor der Corona-Pandemie noch knapp die Hälfte (45 %) nie von zu Hause aus gearbeitet hat, befand sich während des ersten Lockdowns im März und April 2020 plötzlich mit 84 % die überwiegende Mehrheit der Befragten hauptsächlich oder teilweise im Home Office. Seit den weiteren Verschärfungen im November geben das immerhin noch 73 % an.

Home-Office-Nutzung im Zeitverlauf

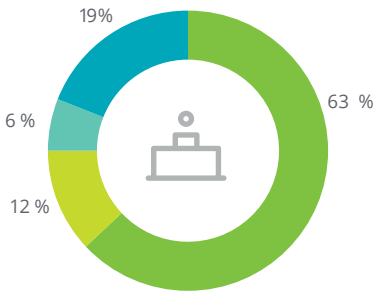


Arbeitssituation im Home Office

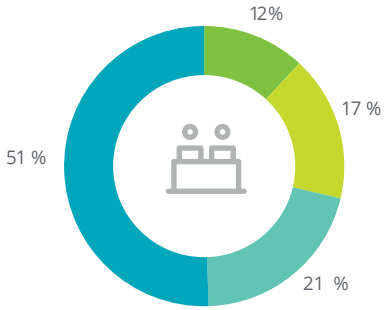
Den täglichen Home-Office-Arbeitsalltag bestreiten die Befragten mit einem (78 %) oder sogar mehreren (22 %) Laptops oder Stand-PCs. Nicht allen steht jedoch ein dezidierter Arbeitstisch zur Verfügung: Ein Viertel (25 %) kann nur selten oder sogar nie an einem Schreibtisch arbeiten, der nicht auch für andere Zwecke genutzt wird.

Mit 84 % lebt der Großteil der Studienteilnehmerinnen und -teilnehmer außerdem zumindest mit einer anderen Person im selben Haushalt. Dementsprechend müssen sich 29 % ihren Arbeitsplatz im Home Office immer oder oft mit anderen Haushaltsmitgliedern teilen. 60 % der Befragten verfügen jedoch über einen eigenen Raum, in dem sie größtenteils ungestört arbeiten können.

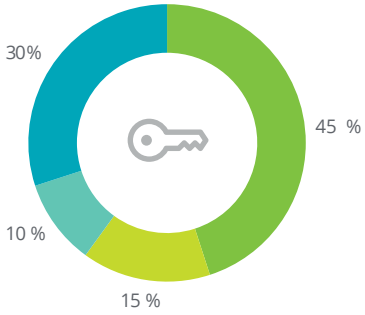
Ich habe einen Schreibtisch zur Verfügung, der nicht für andere Zwecke benötigt wird (z.B. als Esstisch).



Ich teile mir meinen Arbeitsplatz mit anderen Haushaltsmitgliedern.



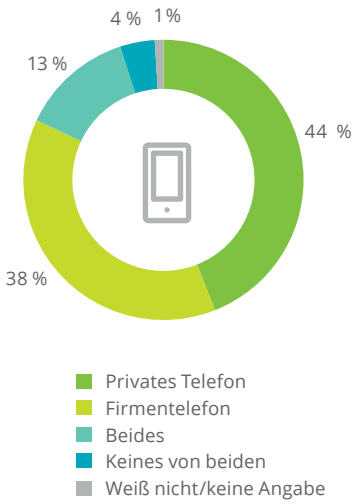
Ich habe einen eigenen Raum für das Home Office, in dem ich ungestört arbeiten kann.



Ausstattung und Netzwerkzugang

Obwohl sich die Arbeit für viele Österreicherinnen und Österreicher zunehmend ins Home Office verlagert hat, fehlt es laut Umfrage in vielen Fällen noch an entsprechender Hardware-Ausstattung durch den Arbeitgeber. So verwenden etwa 44 % der befragten Arbeitnehmerinnen und Arbeitnehmer für die Tätigkeit im Home Office ihr privates Telefon. Nur 38 % nutzen ausschließlich ein Firmentelefon für berufliche Gespräche.

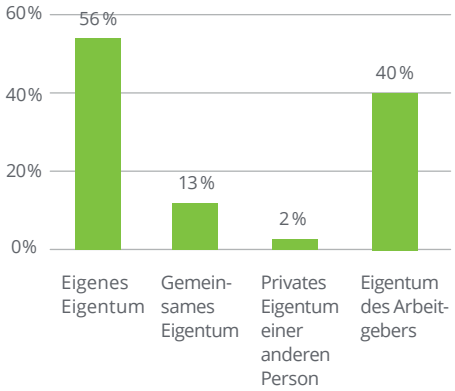
Verwenden Sie für berufliche Telefongespräche im Home Office ein privates Telefon oder wird Ihnen ein Firmengerät zur Verfügung gestellt?



Ähnlich fällt das Ergebnis bei der Frage nach den genutzten PCs aus: Während 40 % der Befragten ein Firmengerät zur Verfügung gestellt wird, arbeiten 56 % mit einem eigenen, privaten Gerät und 13 % verwenden gemeinsam genutzte, private Geräte wie den Familiencomputer. 2 % mussten sich für die Arbeit im Home Office sogar einen PC von anderen Personen ausleihen.

Dadurch besteht das Risiko, dass Unternehmen die Endgeräte nicht ausreichend sichern können. Gar nicht oder nur schlecht gewartete Geräte können leichter von Schadprogrammen angegriffen werden. Zudem besteht die Gefahr, dass auf dem Familiencomputer schnell auch Firmengeheimnisse eingesehen werden können.

Wem gehören die Geräte (PC, Laptop), die Sie im Home Office verwenden?*

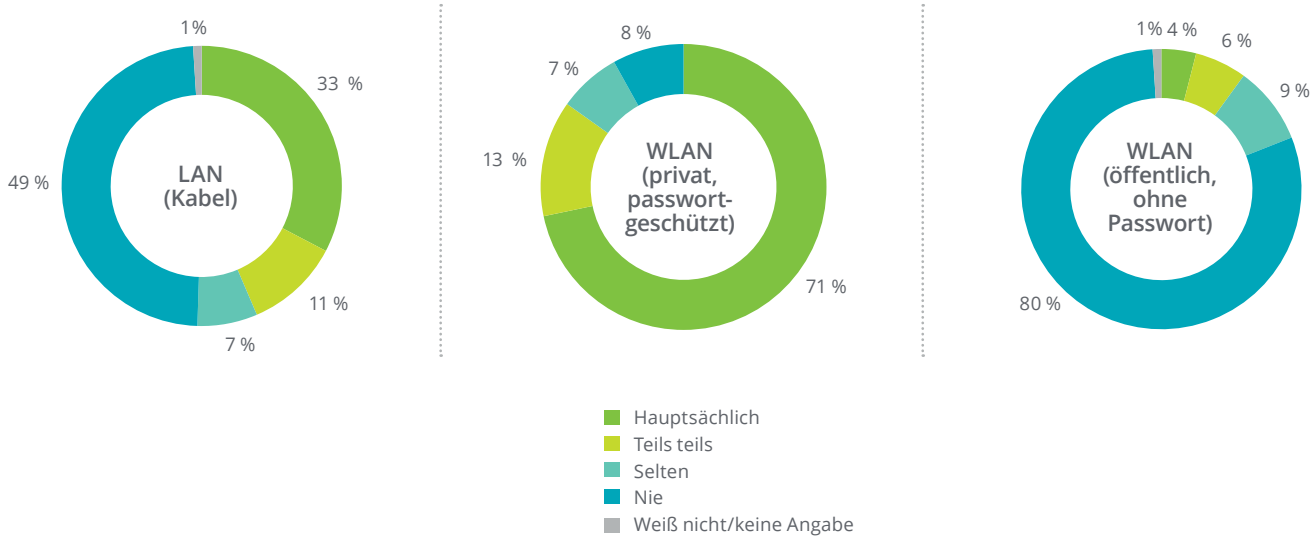


* Mehrfachantworten möglich

Für den Netzwerkzugang verwendet nur ein Drittel (33 %) hauptsächlich eine LAN-Verbindung. Ein privates, passwortgeschütztes W-LAN ist im Home Office deutlich verbreiteter und wird von 71 % großteils verwendet. Immerhin ein Fünftel (19 %) verwendet bisweilen aber auch ein öffentliches W-LAN ohne Passwort.

Die Nutzung von öffentlichen W-LAN-Verbindungen birgt einige Risiken: Da keine Authentifizierung notwendig ist, können sich Angreifer zwischen Gerät und Wireless-Access-Point schalten und somit Zugriff auf sensible Informationen wie vertrauliche E-Mails, Zugangsdaten und Kreditkarteninformationen verschaffen. Die Verbreitung von Malware ist für Cyberkriminelle in einem öffentlichen W-LAN ebenfalls leichter als bei einer privaten und passwortgeschützten Verbindung.

Netzwerknutzung im Home Office



Um von einem externen Standort auf das Firmennetz zugreifen zu können, nutzt knapp die Hälfte (49 %) der befragten Arbeitnehmerinnen und Arbeitnehmer eine VPN-Verbindung. Bei Beschäftigten in Großunternehmen ist dieser Anteil deutlich höher (63 %) als bei jenen in Kleinst- (34 %) und Kleinunternehmen (33 %). Ein Drittel (35 %) der Befragten gibt außerdem an, sich über eine Remote-Desktop-Verbindung Fernzugriff zu verschaffen.

Jeweils vier von zehn Befragten nutzen im Home Office eine firmeneigene Cloud über Firmenserver (44 %) oder externe Cloud-Dienste wie Dropbox, GoogleDrive, OneDrive und iCloud (40 %). Die Nutzung letzterer ist besonders dann gefährlich, wenn die Dienste vor der Verwendung keinem Sicherheits- und Datenschutzcheck durch das Unternehmen unterzogen wurden. Dadurch kann es unter anderem zu datenschutzrechtlichen Verstößen sowie zu fehlenden Service-Level-Agreements kommen. Sensible Unternehmensinformationen sind dadurch ebenfalls gefährdet.

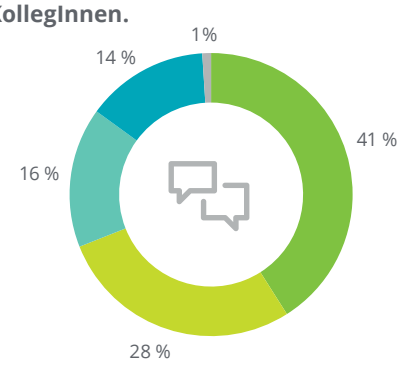
Informationssicherheit im Home Office

Im Umgang mit arbeitsbezogenen Informationen im Haushalt offenbart sich ein beunruhigendes Bild: Ganze 30 % der Befragten räumen ihre Arbeitsunterlagen selten oder gar nie weg, bevor haushaltsfremde Personen wie Besucherinnen und Besucher oder die Reinigungskraft das Zuhause betreten, 18 % tun dies immerhin manchmal. Bei 19 % können haushaltsfremde Personen sogar häufig bis manchmal bei Telefonaten oder Videokonferenzen zuhören bzw. -sehen. Bei über der Hälfte (54 %) können Personen aus dem gleichen Haushalt mithören.

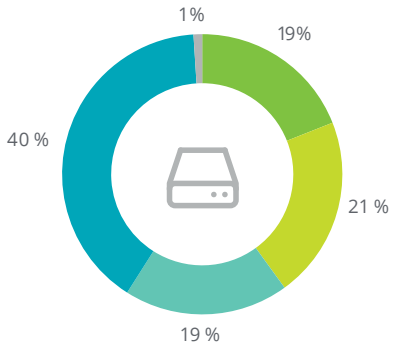
Messaging-Dienste wie WhatsApp oder Telegram werden von über zwei Drittel der Befragten (69 %) häufig oder zumindest manchmal für den beruflichen Austausch mit Kolleginnen und Kollegen verwendet. Hier verbergen sich grundsätzlich ähnliche Risiken wie bei der Nutzung externer Cloud-Dienste: Sensible Unternehmensinformationen werden bei der Verwendung von Messaging-Diensten nicht geschützt und es kann zu Verstößen gegen die EU-Datenschutz-Grundverordnung kommen. Zudem steigt die Gefahr von Malware-Angriffen. Es ist auch zu bedenken, dass Metadaten, die über Messaging-Dienste geteilt wurden, von Dritten analysiert und missbräuchlich verwendet werden können.

Auch mobile Datenträger wie USB-Sticks und externe Festplatten werden von 40 % häufig oder manchmal für den Transport von Arbeitsunterlagen aus dem Büro verwendet. Unterschiede lassen sich hier aber je nach Unternehmensgröße erkennen: In Großunternehmen werden solche mobilen Datenträger nur von 25 % häufig oder manchmal genutzt, in Kleinunternehmen sind das mit 53 % deutlich mehr.

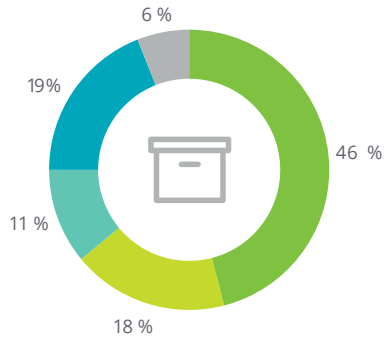
Ich nutze Messaging-Dienste (z.B. WhatsApp, Telegram) für den beruflichen Austausch mit KollegInnen.



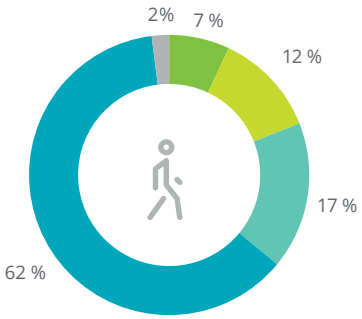
Ich verwende mobile Datenträger (z.B. USB-Stick, externe Festplatte) für Arbeitsunterlagen aus dem Büro.



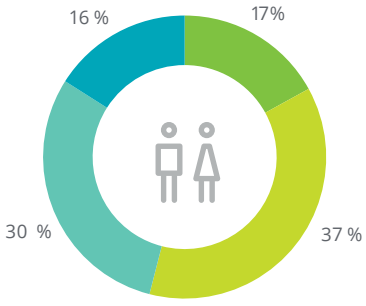
Bevor haushaltsfremde Personen (z.B. BesucherInnen, Reinigungskraft) kommen, räume ich alle Arbeitsunterlagen weg.

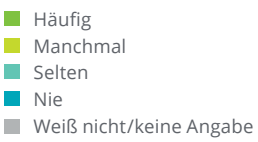


Haushaltsfremde Personen (z.B. BesucherInnen, Reinigungskraft) können bei Telefonaten oder Videokonferenzen zuhören bzw. -sehen.



Im gleichen Haushalt lebende Personen können bei Telefonaten oder Videokonferenzen zuhören bzw. -sehen.



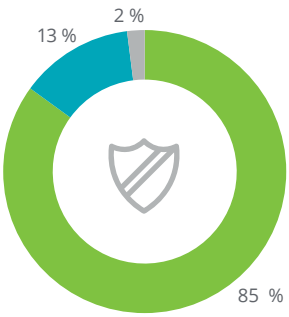


Die für das Home Office verwendeten Laptops bzw. PCs werden in 37 % der Fälle auch von anderen Personen mitverwendet – für private oder berufliche Zwecke. Neben der Aufklärung der Mitarbeiterinnen und Mitarbeiter, welche Risiken damit einhergehen, sollten Unternehmen hier klare Regeln festlegen: Nach der Nutzung der Geräte sollten beispielsweise alle Daten gelöscht oder über den eigenen Account gesichert werden. Zudem empfiehlt sich eine Verschlüsselung der Daten, denn bei einem Datenverlust würde ansonsten eine verpflichtende Meldung an die Datenschutzbehörde erfolgen müssen.

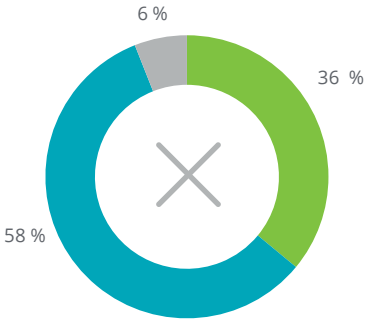
13 % der Befragten haben außerdem keinen passwortgeschützten Sperrbildschirm bei ihrem PC oder Laptop eingestellt, 36 % speichern Daten im Home Office tendenziell häufiger auf der lokalen Festplatte als im Büro. Aufgrund der lokalen Speicherung besteht das Risiko, sensible Daten zu verlieren. Mit diesem Problem setzten sich die Unternehmen zwar schon seit einigen Jahren auseinander, die schlechten Datenverbindungen im Home Office führen allerdings dazu, dass alte Gewohnheiten wieder aufgenommen und sensible Daten häufiger lokal abgespeichert werden.

Bei knapp einem Drittel (31 %) der Befragten finden sich Sprachassistenten wie Alexa, Cortana oder Siri im Haushalt – diese können das Risiko für Cyber-Angriffe steigern. In Büroräumlichkeiten wäre das Dulden eines solchen Sicherheitsrisikos direkt im Arbeitsumfeld nicht denkbar.

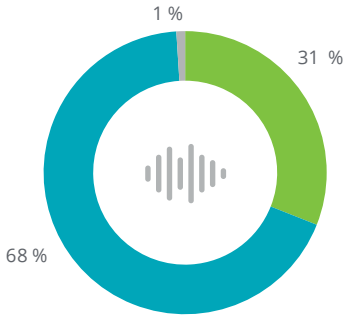
Der PC oder Laptop, den ich hauptsächlich verwende, hat einen passwortgeschützten Sperrbildschirm.

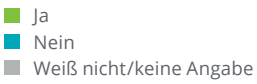


Ich speichere Daten im Home Office tendenziell häufiger auf der lokalen Festplatte als im Büro.



Gibt es in Ihrem Haushalt einen Sprachassistenten (z.B. Alexa, Cortana oder Siri)?

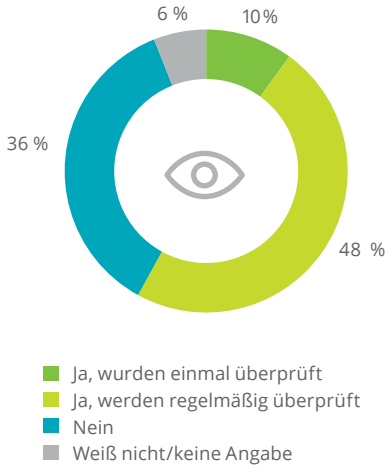




Sicherheitsmaßnahmen seitens der Unternehmen

Die Umfrage zeigt: Einige Unternehmen haben wichtige Sicherheitsvorkehrungen verabsäumt. Während etwa die Arbeitsgeräte bei knapp der Hälfte der Befragten (48 %) regelmäßig auf Software-Updates und Virenschutz überprüft werden, hat eine solche Prüfung bei einem besorgniserregend hohen Anteil von 36 % gar nicht stattgefunden.

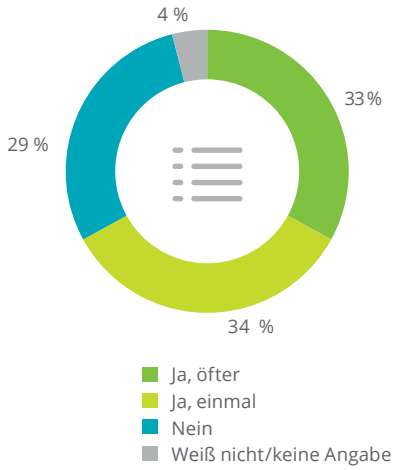
Wurde bzw. wird Ihr Laptop/PC von Ihrem Arbeitgeber auf Software-Updates, Virenschutz etc. überprüft?



Auch in puncto Aufklärung herrscht Aufholbedarf. Zwar wurden insgesamt zwei Drittel der Arbeitnehmerinnen und Arbeitnehmer von ihrem Arbeitgeber öfter (33 %) oder zumindest einmal (34 %) über Informationssicherheit und Datenschutz im Home Office aufgeklärt. Weitere 29 % geben allerdings an, nie darüber informiert worden zu sein. Wenn aufgeklärt wurde, so fand das in 63 % der Fälle per E-Mail statt. Effektivere Maßnahmen wie Schulungen (36 %) und E-Learnings (34 %) wurden selten angeboten.

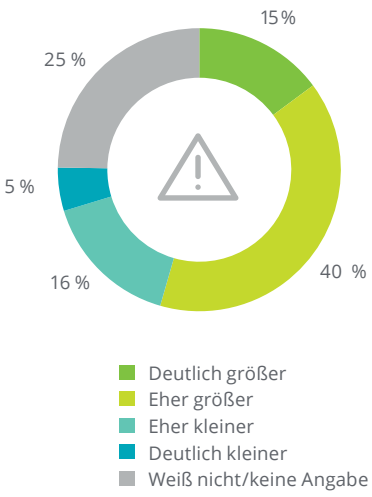
Unterschiede lassen sich auch hier bei der Unternehmensgröße erkennen: Angestellte von Großunternehmen wurden häufiger (76 %) über Informationssicherheit und Datenschutz informiert als solche von Kleinunternehmen (66 %) oder mittleren Betrieben (65 %).

Wurden Sie von Ihrem Arbeitgeber über die Informationssicherheit und Datenschutz im Home Office aufgeklärt?



Dementsprechend kommt es häufig zu Wissenslücken und Fehleinschätzungen beim Thema Cyber Security im Home Office: Ein Fünftel (21 %) der Befragten glaubt, dass die Cyber-Risiken zu Hause eher oder deutlich geringer sind als bei der Arbeit im Büro, ein Viertel (25 %) traut sich hier keine Einschätzung zu oder gibt keine Antwort.

Wie schätzen Sie die Bedrohung durch Cyber-Risiken, der Sie im Home Office ausgesetzt sind, im Vergleich zur Arbeit im Büro ein?



Methode und Sample

Zielpopulation:
Unselbständig Beschäftigte
(seit Beginn der Corona-Pandemie
im Home Office tätig)

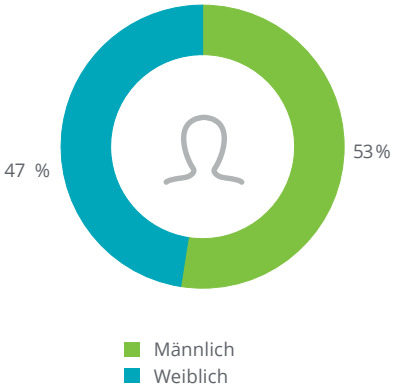
Erhebungsmethode:
300 telefonisch (CATI) +
200 web-basiert (CAWI)

Befragungszeitraum:
26. Jänner – 9. Februar 2021

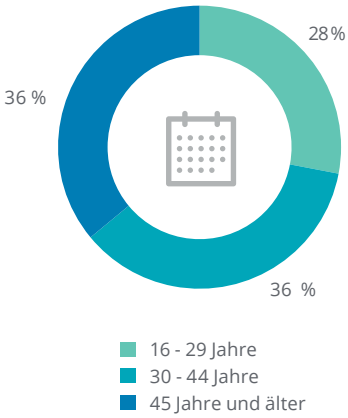
Stichprobe:
500 Arbeitnehmerinnen und Arbeitnehmer aus ganz Österreich, die seit Beginn der Corona-Pandemie zumindest fallweise im Home Office gearbeitet haben

Hinweis: Geringfügige Abweichungen von Sollwerten (z.B. 99 % oder 101 % statt 100 %) sind auf Rundungseffekte zurückzuführen.

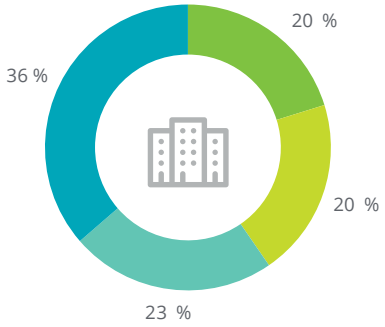
Geschlecht



Alter



Unternehmensgröße



Fazit

Die vorliegende Studie gibt einen spannenden Einblick in die Wohn- und Arbeitszimmer der Arbeitnehmerinnen und Arbeitnehmer: Das Arbeiten über ein öffentliches W-LAN ohne Passwort, die Verwendung von Messaging-Diensten und externen Cloud-Anbietern sowie der geteilte Arbeitsplatz im Home Office stellen eine große Gefahr für sensible Unternehmensdaten dar. Die Umfrageergebnisse zeigen jedoch, dass die heimischen Unternehmen derzeit viele dieser Risiken gar nicht oder noch zu wenig aufgreifen.

Denn obwohl zahlreiche Mitarbeiterinnen und Mitarbeiter bereits seit über einem Jahr hauptsächlich von zuhause aus arbeiten, haben viele Informationssicherheits-Management-Systeme den Arbeitsmodus Home Office noch nicht strukturiert in ihr Risiko-Assessment aufgenommen. Es empfiehlt sich daher dringend eine Risikoanalyse und eine entsprechende Ableitung konkreter Maßnahmen wie Datenverschlüsselungen, die Ausgabe von Headsets und anderen firmeneigenen Geräten sowie Vorgaben für sichere Netzwerkverbindungen.

Natürlich können Unternehmen im privaten Umfeld der Mitarbeiterinnen und Mitarbeiter keine Kontrollen durchführen, wie dies am Arbeitsplatz beispielsweise durch eine Clean-Desk-Policy möglich wäre. Trotzdem ist es zu empfehlen, klare Regeln für den sicheren Umgang mit arbeitsbezogenen Daten und Informationen im Home Office festzulegen und zu kommunizieren. Arbeitnehmerinnen und Arbeitnehmer müssen verstärkt für das Thema Cyber Security im Home Office sensibilisiert werden – denn deren Awareness ist und bleibt neben technischen Maßnahmen das zentrale Instrument im Kampf gegen Cyber-Angriffe und Datenlecks.

Kontakt

Alexander Ruzicka
Partner | Risk Advisory
+43 1 537 00-7950
aruzicka@deloitte.at

Andreas Niederbacher
Senior Manager | Risk Advisory
+43 732 675 290-250
aniederbacher@deloitte.at

Deloitte.