Homeoffice und IT-Sicherheit

Homeoffice und mobiles Arbeiten sind nicht zuletzt durch die Folgen der Corona-Pandemie allgegenwärtig. Viele Unternehmen traf die plötzliche Arbeit von zu Hause völlig unvorbereitet und es wurden ad hoc Maßnahmen umgesetzt. Themen wie Informations- und Datensicherheit kamen dabei oft zu kurz. Somit sind die wichtigen IT-Sicherheitsschutzziele, z. B. nach dem VIVA-Prinzip (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität), oftmals nicht mehr gesamtheitlich erfüllt. Die Bedeutung von Vertraulichkeit bzw. Authentizität von Daten ist zwar vielen bewusst, wird jedoch beispielsweise aufgrund der Nutzung von „unsicheren" Tools für Webkonferenzen oder durch den Abfluss sensibler Daten über unverschlüsselte Kommunikationskanäle nicht immer gewährleistet. Die Themen Integrität und insbesondere die Verfügbarkeit der Daten sind weitere entscheidende Ziele für ein erfolgreiches, effizientes und sicheres Arbeiten von zu Hause aus.

Was ist unter Homeoffice zu verstehen?

Homeoffice (oder auch Heimarbeit) ist jede Form von Telearbeit, die von zu Hause aus durchgeführt wird. Telearbeit bezeichnet wiederum alle Tätigkeiten der Mitarbeiter eines Unternehmens, welche außerhalb der betrieblichen Arbeitsstätte mit der Nutzung von Telekommunikationseinrichtungen durchgeführt werden. Eine weitere Form der Telearbeit ist das mobile Arbeiten, welches örtlich und zeitlich variierend bzw. unterwegs ausgeübt wird. In der Regel sind Homeoffice-Arbeitsplätze nicht nur temporär, sondern längerfristig eingerichtet. Dadurch ergeben sich zu den beiden Formen der Telearbeit zwar Schnittmengen aber auch Besonderheiten (z. B. rechtlicher Natur). Somit können zwar Tipps aus diesem Flyer auch auf das mobile Arbeiten übertragen werden, sind aber vornehmlich für das Homeoffice zu betrachten. Weitere Informationen zur Telearbeit können Sie auf den Seiten des Mittelstand 4.0-Kompetenzzentrum Chemnitz unter **https://betrieb-machen.de/ng-telearbeit** finden.

Mittelstand 4.0-Kompetenzzentrum Chemnitz

Als Mittelstand 4.0-Kompetenzzentrum Chemnitz unterstützen wir Sie als kleines und mittelständisches Unternehmen! Wir zeigen Ihnen die technologischen und wirtschaftlichen Potenziale der Digitalisierung, Vernetzung und Anwendung von Industrie 4.0 und begleiten Sie auf dem herausfordernden Weg in eine digitale Zukunft. Mit der Expertise und Erfahrung unserer Partner wollen wir das Thema Industrie 4.0 für Sie als Unternehmen greifbar machen, Ihre Führungskräfte und Mitarbeiter qualifizieren und die Umsetzung der Digitalisierung bei Ihnen vor Ort unterstützen. Unsere Angebote umfassen ein umfangreiches Leistungsportfolio – von der Sensibilisierung über den Kompetenzaufbau bis hin zur Umsetzung im Unternehmen. Die Leistungsbereiche bauen aufeinander auf und werden vor Ort in den Unternehmen, in den Testumgebungen der Partner und auf unserer Onlineplattform angeboten. Im Rahmen unserer kostenfreien und praxisnahen Angebote können Sie sich intensiv mit diesen Themen beschäftigen.

Dabei bearbeiten wir folgende Themenfelder:

- **Menschen machen's! –** Der Mensch in der digitalen Arbeitswelt.
- **Alles Unternehmen! –** Das Unternehmen für morgen aufstellen.
- **Leistung bringen! –** Den Prozess digital verbessern.
- **Produkte gestalten! –** Das Produkt für den Nutzer machen.
- **Recht behalten! –** Recht, Sicherheit & Schutz beim digitalen Miteinander.
- **Sicher bleiben! –** Digitalisieren und vernetzen, aber sicher.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter:
www.mittelstand-digital.de

Impressum

Text und Redaktion:
Andreas Neuenfels, Mike Wäsche, Roland Hallau,
Mittelstand 4.0-Kompetenzzentrum Chemnitz

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9, 39108 Magdeburg
Tel.: +49 391 74435-24 • Fax: +49 391 74435-11
E-Mail: rhallau@tti-md.de
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich
Amtsgericht Stendal, HRB 104429
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

Grafische Konzeption und Gestaltung:
toolboxx-media UG (haftungsbeschränkt)

Druckerei: KOCH-DRUCK

Bildnachweis: Marina Andrejchenko, adam121 – stock.adobe.com

Magdeburg, Februar 2021

Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

IT-Sicherheit im Homeoffice

10 Goldene Regeln aus der Praxis

www.mittelstand-digital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

10 Goldene Regeln zur sicheren Arbeit im Homeoffice

Die 10 Goldenen Regeln sollen Ihnen helfen, die Informations- und Datensicherheit für das Arbeiten Ihrer Mitarbeiter im Homeoffice zu gewährleisten. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet und basieren zudem auf Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik.[1]

Weiterführende Informationen und Anregungen rund um die Themen IT-Sicherheit und Digitalisierung finden Sie unter

www.mittelstand-digital.de.

Welche Vorkehrungen sind zu treffen?

Regel 1: Definieren Sie den Einsatz von Homeoffice

Zunächst sollten Sie sich als Verantwortlicher oder Geschäftsführer im Unternehmen darüber klar werden, wofür und in welchem Rahmen Homeoffice eingesetzt werden soll. Typische Fragestellungen sind dabei, wie lange und wann Mitarbeiter im Homeoffice verbringen sollen bzw. können, ob es sich um einen dauerhaften Arbeitsplatz fernab der Betriebsstätte handelt oder ein Mittel zur Gestaltung von flexiblem Arbeiten darstellen soll.

Regel 2: Leiten Sie Regelungen für Ihr Unternehmen ab

In Abhängigkeit der ersten Regel sollten Sie Regelungen, Befugnisse und Verantwortlichkeiten für Ihre Mitarbeiter aufstellen. Dies umfasst Informationen darüber, mit welchen Daten gearbeitet werden darf, welche Hard- bzw. Software zu benutzen ist, welche Datenschutzbestimmungen gelten und wie zu kommunizieren ist. Diese Regelungen ergeben sich auch aus den weiteren aufgeführten Punkten in diesem Flyer.

Regel 3: Schaffen Sie die technischen Voraussetzungen

Zur Sicherstellung der Arbeitsfähigkeit Ihrer Mitarbeiter außerhalb des Unternehmen müssen alle wesentlichen technischen Voraussetzungen geschaffen werden. Hierzu gehört u. a. mitarbeiter- und unternehmensseitig ein hinreichend schneller Internetzugang mit ausreichenden Up- und Download-Kapazitäten. Weiterhin sollten Sie beachten, dass genügend Lizenzen und mobile Endgeräte vorhanden sind, welche vom Unternehmen auszugeben und zu konfigurieren sind. Von der Benutzung privater Endgeräte ist aufgrund von datenschutzrechtlichen Aspekten nach Möglichkeit abzusehen! Zudem sollten Sie sicherstellen, dass Arbeitsschutzmaßnahmen ebenfalls im Homeoffice umgesetzt werden sollten.

Regel 4: Holen Sie sich Unterstützung

Die Einführung von Homeoffice, insbesondere wenn keine oder nur wenig Erfahrungen im Unternehmen vorhanden sind, ist sehr komplex und facettenreich. Dies alles zu überblicken und alle technischen sowie rechtlichen Fallstricke zu beachten, ist sehr schwierig. Daher sollten Sie sich Unterstützung von Experten holen, die Sie z. B. bei den Mittelstand 4.0-Kompetenzzentren (**www.mittelstand-digital.de**) oder am freien Markt finden. Zudem sollten Sie bundesweite Fördermöglichkeiten wie „go-digital", „digital-jetzt!" oder weitere Programme auf Landesebene in Betracht ziehen.

Wie sieht ein sicheres Homeoffice aus?

Regel 5: Zugriffs- und Zugangsschutz

Es sollten Maßnahmen ergriffen werden, die den Zugang und den Zugriff auf Daten und Geräte auch im eigenen Haushalt erschweren. Abschließbare Schränke und Rollcontainer sind hierbei naheliegende Maßnahmen, genauso wie der Einsatz von Sichtschutzfolien für Bildschirme oder das Sperren von Arbeitsoberflächen, wenn der Raum verlassen wird.

Regel 6: Verschlüsselte Kommunikation und Remote-Zugriff

Eine sichere Kommunikation ist essentiell für das Homeoffice. Sind Zugriffe auf betriebsinterne Ressourcen (Daten und Systeme) erforderlich, sollte ein abgesichertes Virtuelles Privates Netzwerk (VPN) genutzt werden. Hiermit werden Manipulationen bzw. das Abgreifen von Daten durch Dritte deutlich erschwert. Weiterhin sollten auch Telefonate nicht auf privaten Telefonen durchgeführt und E-Mails nur über die dienstlichen Accounts versendet werden. Die Nutzung des Internets, von Messenger-Diensten und Videokonferenztools sollte den IT-Sicherheitsanforderungen des Unternehmens entsprechen. Der Einsatz von verschlüsselten Transferprotokollen wie HTTPS oder die Kommunikation zwischen befugten Personen sollte obligatorisch sein.

Exkurs: **Verifizierung und Authentifizierung von Mitarbeitern**

Ein großes Problem, wenn man sich nicht physisch gegenübersteht, ist die Prüfung der Identität eines Kommunikationspartners – die sogenannte Authentifizierung. Es kann z. B. bei einem Telefonat schwierig sein, sein Gegenüber eindeutig zu identifizieren. Social-Engineering bzw. Phishing-Attacken bedienen sich sehr oft dieser Schwachstelle (z. B. „CEO-Fraud"). Deshalb sollten in einem Unternehmen Abläufe und Maßnahmen definiert sein, welche die Verifizierung (oder Falsifizierung) der vorgegebenen Identität des Gegenübers ermöglichen:

- Zwei-Faktor- bzw. Multi-Faktor-Authentifizierungen
- verschlüsselte E-Mails mit öffentlichen und privaten Schlüsseln bzw. Zertifikaten
- benutzerbezogene VPN-Zugänge (ggf. auch mit Zwei-Faktor-Authentifizierung)
- Identity- und Access-Management-Systeme zur Unterstützung und Verwaltung

Regel 7: Datensicherung

Auch im Homeoffice sollten Sie darauf achten, dass die Mitarbeiter Ihre Daten regelmäßig und konform der unternehmenseigenen Backup-Strategie sichern. Dies ist wichtig, da z. B. bei mobilen Endgeräten Schäden durch Stürze und Transporte entstehen können, Diebstähle häufiger auftreten oder Daten verloren gehen. Hierbei sollten Sie auf technische (softwaregestützte) Routinen zurückgreifen, welche die Daten beispielsweise über die eingerichteten VPN-Kanäle oder Cloud-Dienste speichern.[2]

Regel 8: Umgang mit Unterlagen und vertraulichen Informationen

Es kommt häufig vor, dass auch papiergebundene Unterlagen oder Datenträger mit an den Homeoffice-Arbeitsplatz genommen werden müssen. Diese sollten sowohl beim Transport als auch vor Ort geschützt werden (Verschlüsselung oder Verschluss). Hierbei ist Regel 5 zu beachten, insbesondere wenn es sich um personenbezogene Daten und unternehmenskritische Informationen handelt. Ein wichtiger Punkt ist die Entsorgung von Dokumenten und Datenträgern, welche nicht über den Hausmüll geschehen sollte, da diese die Vertraulichkeit verletzt. Idealerweise sollten Dokumente und Datenträger zur Zerstörung oder Archievierung wieder in die Betriebsstätte gelangen.

Wie nehme ich meine Mitarbeiter mit?

Regel 9: Haben Sie Vertrauen gegenüber Ihren Mitarbeitern

Die besten Regeln, Richtlinien und technischen Ausstattungen schützen nicht vor dem alles entscheidenden Faktor Mensch. Sie sollten die Verfahrensweisen im Homeoffice eng mit Ihren Mitarbeitern abstimmen und aufstellen, da nur so Schwierigkeiten vor Ort und Fehler vermieden werden können. Zudem können Sie auch Unverständnis gegenüber Regelungen und Prozessen vorbeugen, da die Mitarbeiter wissen, wie diese entstanden sind. Ferner sollten Regeln so aufgebaut werden, dass diese nicht zu kleinteilig sind, da sonst schnell Frust erzeugt werden kann bzw. die Mitarbeiter sich eingeengt fühlen. Abwehrreaktionen und das bewusste Umgehen von Regelungen können die Folge sein. Dies würde die IT-Sicherheit nachhaltig negativ beeinflussen.

Regel 10: Laufende Sensibilisierung für Gefahren

Schulen bzw. trainieren Sie regelmäßig Ihre Mitarbeiter, um Wissen zu vermitteln und über aktuelle Gefahrenlagen (z. B. Phishing und Spear-Phishing) aufmerksam zu machen. Nutzen Sie dafür auch Angebote der Mittelstand 4.0-Kompetenzzentren oder des Bundesamtes für Sicherheit in der Informationstechnik. Ermutigen Sie Ihre Mitarbeiter auch zur Meldung von Schadensereignissen und Sicherheitsvorfällen (z. B. Verlust oder Diebstahl von Dokumenten).

Literatur, Standards und Normen zu IT-Sicherheit im Homeoffice

1)Bundesamt für Sicherheit in der Informationstechnik (BSI) www.bsi.de

- Aktueller Hinweis: Tipps für sicheres mobiles Arbeiten
- IT-Grundschutz-Kompendium OPS.1.2.4 Telearbeit
- IT-Grundschutz-Kompendium INF.8 Häuslicher Arbeitsplatz
- Empfehlungen zum sicheren mobilen Arbeiten im Homeoffice

2) Mittelstand 4.0-Kompetenzzentrum Chemnitz www.betrieb-machen.de

- Nachgelesen: Was tun bei einem Sicherheitsvorfall?
- Nachgelesen: IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen
- Nachgelesen: Wie sichere ich meine Daten?
- Nachgelesen: Telearbeit kompakt: Grundlagen, Vorteile, Nachteile
- Nachgelesen: Business-Guide: Datenschutz in Videokonferenzen
- Der rechtliche Rahmen von Arbeit 4.0

Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter: **www.betrieb-machen.de**