Praxisleitfaden

SICHERES ARBEITEN IM HOME OFFICE

Praxisleitfaden: Sicheres Arbeiten im Home Office

Version 2021

Inhalt

1. Einleitung

In allen Bereichen, in denen produktives Arbeiten auch von einem anderen Ort als dem Firmenstandort möglich ist, wird seit geraumer Zeit (und nicht erst seit Beginn der COVID19-Pandemie) der Ruf nach mobilen und flexiblen Arbeitsplätzen zunehmend lauter. Neu sind die Begriffe Home- bzw. Mobile-Office folglich nicht. Durch flächendeckende Home-Office-Regelungen aufgrund der Corona-Eindämmungsmaßnahmen wurde jedoch vielen Unternehmern klar, dass mobiles Arbeiten auch für einen größeren Mitarbeiterkreis Vorteile bietet.
Die Gründe sind vielfältig, es herrscht jedoch im Allgemeinen Einigkeit darüber, dass die gewonnene Flexibilität nachhaltig auch über die Pandemie hinaus fortbestehen wird. Der etwas schleppende, aber sicher kommende, Ausbau leistungsfähiger digitaler Infrastruktur ebnet den Weg - Tendenzen wie Klimapolitik, urbane Mietpreise sowie Mangel an ortsansässigem qualifiziertem und bezahlbarem Personal zeigen der Wirtschaft Perspektiven und Potentiale auf, welche zuvor außer Acht gelassen wurden.
Im zurückliegenden Jahr wurden vielerorts hastig Konzepte gezimmert, die die Arbeit aus dem Home-Office ermöglichen sollten. Spätestens jetzt ist es aber an der Zeit, einen Schritt zurückzutreten und zu prüfen, wie es denn um die Sicherheit der geschaffenen Situation steht. Da die Arbeit aus dem heimischen Umfeld heraus kein vorübergehendes Phänomen bleiben wird lohnt sich also ein genauerer Blick.

Immer häufiger werden Unternehmen über Wochen und Monate lahmgelegt, indem Schadsoftware Zugriff auf interne Systeme erlangt, sich dort fest einnistet, wichtige Daten ausleitet und lokal verschlüsselt. Eine Rückkehr zum Normalbetrieb ist erst durch Zahlung von Lösegeld möglich, Garantien gibt es keine, Wiederholungen sind nicht ausgeschlossen. Jüngste Beispiele hierfür sind die Angriffe auf die irische Gesundheitsbehörde HSE oder auf die IT der Betreibergesellschaft der „Colonial Pipeline“. Letzterer stoppte weitgehend die Ölversorgung der amerikanischen Ostküste und sorgte für entsprechende Turbulenzen. Ideales Einfallstor für solche und andere Angriffe auf die Unternehmens-IT kann das in der Regel weniger gut abgesicherte Home-Office sein.

Folgende Fragen sollten also bzgl. des mobilen Arbeitens gestellt (und beantwortet) werden:

- Welche simplen Maßnahmen sind umgesetzt und werden gelebt?
- Wo kann mit überschaubarem Aufwand weiter optimiert werden?
- Wo bestehen hohe Risiken, denen begegnet werden muss?
- Wo wurden ergriffene Maßnahmen, z.B. zur Einhaltung der DSGVO, geschwächt?
- Wo entgleitet die Kontrolle über die Daten, wo über die Richtlinien und Prozesse?

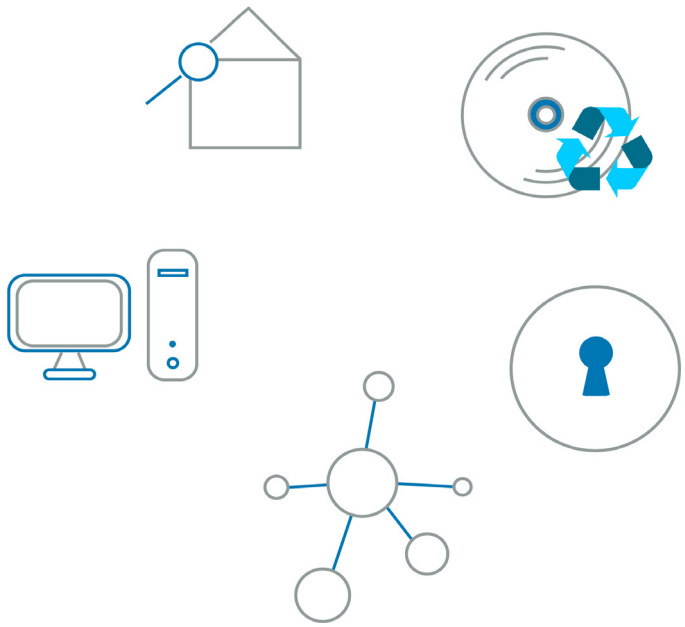
Ziel muss es sein, das Sicherheitsniveau am Standort des Unternehmens in die Wohnungen der Mitarbeiter auszuweiten, denn zwangsläufig verlieren alle Maßnahmen zur IT- und Informationssicherheit ihre Wirksamkeit, wenn der Arbeitsraum auf unkontrollierbare Bereiche ausweicht.

2. Konkrete Maßnahmen zur Steigerung der Informationssicherheit im Home Office

Zunächst betrachten wir die üblichen etablierten Maßnahmen zur Informationssicherheit, wie sie die Unternehmen aus Eigeninteresse und aufgrund externer Anforderungen auf angemessenem Niveau einsetzen.

Die üblichen Maßnahmen, beginnend beim physikalischen Schutz und dem geregelten Zutritt zu Systemen und Dokumenten, erstrecken sich über:

- die sichere Entsorgung oder Vernichtung von Datenträgern und Schriftstücken.
- technische Maßnahmen die Server, Arbeitsplatzrechner und Unternehmensnetze absichern.
- sowie die Registrierung und Aufzeichnung von Auffälligkeiten, Alarmierung und ggf. die Einleitung von Gegenmaßnahmen.



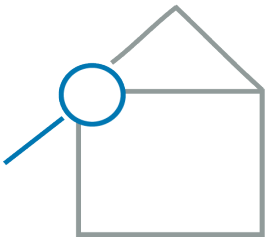
Vieles davon ist im Home Office nicht ohne weiteres gegeben oder umsetzbar. Die Verantwortung hierzu darf nicht alleine dem Mitarbeiter überlassen werden.

Welche Maßnahmen im Einzelfall nötig oder ausreichend sind, hängt wesentlich mit der individuellen Situation zusammen:

- Wie sensibel sind die jeweils verarbeiteten Daten?
- Welche Zugriffsmöglichkeiten benötigt und besitzt der jeweilige Mitarbeiter im Home Office?
- Welches Risiko geht davon aus?

Viele der möglichen Maßnahmen sind ohne großen Aufwand umzusetzen, Versäumnisse hier jedoch schon fahrlässig zu nennen – hinsichtlich der geforderten technischen organisatorischen Maßnahmen zum Datenschutz besteht auch die strafbewehrte Pflicht einer Festlegung und Durchsetzung solcher Vorkehrungen.

2.1 Zutrittsschutz/ Zugriffsschutz/Physikalische Sicherheit

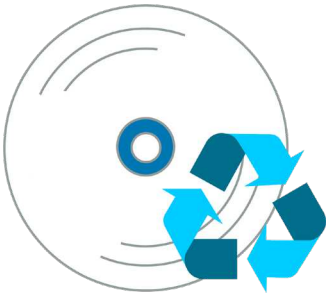


Kaum ein Privathaushalt wird über ein System zur Zutrittskontrolle verfügen, wie es in Geschäftsräumen heute Standard ist. Auch Einbruchsmelde- bzw. Alarmanlagen sind meist nicht vorhanden. Besucher, Handwerker, eventuell Putzhilfen, Bekannte und Bekannte von Bekannten bewegen sich oft unkontrolliert in den Räumen.

Daher sollte eine entsprechende Regelung zum Home-Office die Verpflichtung des Mitarbeiters enthalten, seine Arbeitsgeräte und Unterlagen vor fremden Zugriff zu schützen.

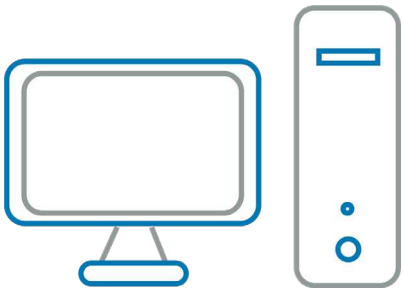
Rechner, Dokumente und Datenträger sind nicht offen zugänglich und einsehbar aufzubewahren, bei Nichtgebrauch nach Möglichkeit wegzusperren. Idealerweise findet Home-Office ohnehin in einem separaten, abschließbaren Raum statt. Da dies sicher nicht überall zu realisieren ist, ist die Umsetzung und Durchsetzung der „kleineren Maßnahmen" umso wichtiger.

2.2 Sichere Entsorgung von Datenträgern



Ausdrucke und Datenträger (z.B. CDs oder Flash-Speichermedien wie USB-Sticks) dürfen auch im Home-Office nicht ohne weiteres in den Müll wandern. Lassen sich Papierdokumente und teils auch CDs mit handelsüblichen Shreddern zu Hause leicht und sicher vernichten, so gestaltet sich dies bei Datenträger wie USB-Sticks oder Speicherkarten deutlich schwieriger.
Diese sind entweder durch die physikalische Zerstörung durch entsprechend spezialisierte Unternehmen oder durch Verwerfen eines gesetzten kryptographischen Schüssels wirklich sicher unlesbar zu machen. So oder so: der Hausmüll ist keine Option und die Entsorgung sollte durch die Unternehmens-IT organisiert und umgesetzt werden.

2.3 Der Computer



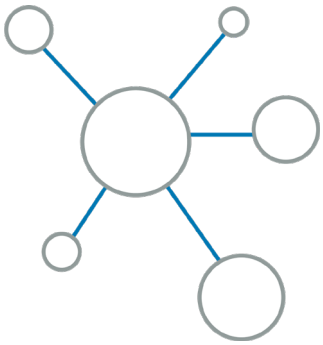
Als das Werkzeug, welches Home-Office erst sinnvoll möglich macht, kommt diesem Arbeitsgerät eine zentrale Bedeutung zu. Auch im Home-Office muss das Unternehmen die Kontrolle über den Rechner behalten. Eine Nutzung des Privat-PCs oder gar des „Familien-PCs" kommt daher nicht in Frage. Niemand kann die Verantwortung dafür übernehmen, welche Sicherheitslücken solch ein System aufweist, welche Würmer, Trojaner, Keylogger oder sonstige Malware dort ihr Unwesen treiben.

Es liegt in der Verantwortung des Arbeitgebers dafür Sorge zu tragen, dass die Systeme, über die vertrauliche Geschäftsdaten fließen, sauber bleiben. Das kann

nur über ein zentral bereitgestelltes Firmengerät erfolgen, welches in der Verantwortung und Wartung der Unternehmens-IT bleibt.
Diese stellt sicher und überwacht, dass stets aktuelle Patches und Updates installiert werden, dass ausschließlich freigegebene Software eingesetzt wird und dass ein wirkungsvoller Schutz vor Schadsoftware auf dem System installiert ist.
Wichtige Systemmeldungen, wie z.B. eben solche Virenfunde oder fehlgeschlagene Aktualisierungen, dürfen nicht unbeachtet bleiben. Damit das System sich nicht unter dem Radar der Unternehmens-IT bewegen kann, muss es weiterhin stark in die diesbezüglichen Mechanismen der Unternehmens-IT eingebunden bleiben. Genannt seien Systeme zur Software- und Updateverteilung, zentrale Management-Systeme zur Verwaltung der Anti-Malware-Software, falls vorhanden auch zentrale Log- bzw. SIEM-Systeme. Voraussetzung dafür ist die Einbindung des Systems in das Unternehmensnetzwerk (siehe 2.5).

Selbstverständlich sein sollte der Schutz des Rechners durch die aktivierte automatische Sperre bei Nichtbenutzung und ein starkes Benutzerpasswort, idealerweise ergänzt um einen zweiten Faktor wie biometrische Daten oder ein Token.
Ebenfalls unabdingbar und einfach umsetzbar ist die Verschlüsselung der Datenträger des Rechners und etwaiger mobiler Datenträger. Dies verhindert wirkungsvoll, dass Daten bei Diebstahl oder Verlust durch Fremde ausgelesen werden können. Fehlt diese Verschlüsselung und sind auf dem Rechner personenbezogene Daten gespeichert (z.B E-Mails), so stellt jeder Verlust einen meldepflichtigen Datenschutzvorfall mit entsprechenden Folgen dar.

2.4 Das Netzwerk



Zum Home-Office-Alltag gehört, dass vom heimischen Arbeitsplatz aus auf das Internet und insbesondere auf im Unternehmen stehende Systeme und Daten zugegriffen werden muss. In der Regel soll hierfür die in den Haushalten schon vorhandene Technik genutzt werden. Dies kann meist auch mit angemessener Sicherheit erfolgen, sofern einige wichtige Punkte beachtet werden.

Problematisch ist grundsätzlich, dass das Netzwerk in Privathaushalten in den meisten Fällen kein sicherer Ort ist. Gefahren drohen unter anderem durch den Einsatz veralteter und unsicherer Standards, durch nicht gewartete Router mit entsprechenden Sicherheitslücken, diverse unkontrollierbare Fremdsysteme der Mitbewohner oder Familienmitglieder sowie deren Bekannte im heimischen WLAN.

Oft wird das WLAN-Passwort bereitwillig herausgegeben, geändert wird es nie bis selten.

Zunehmend zur Bedrohung werden auch die zahlreichen IoT-Geräte, von Heizungssteuerung über „intelligente" Küchengeräte, vernetzte Unterhaltungselektronik bis hin zum witzigen China-Gadget, an dessen Inbetriebnahme man sich kaum mehr erinnern kann. Problematisch sind all diese Geräte, da sie nicht regelmäßig gewartet werden und oftmals direkt oder indirekt aus dem Internet zugreifbar (und damit angreifbar) sind. Stellen im Unternehmen entsprechende Richtlinien und Prozesse sicher, dass keine unsicheren Geräte im Unternehmensnetzwerk geduldet sind, so ist dies im Heimnetzwerk kaum realisierbar. Wer prüft schon, ob für die Firmware des Kühlschranks wichtige Sicherheitsupdates zu installiere sind oder ob für die Videoüberwachung des Vorgartens überhaupt noch solche entwickelt und bei Bedarf bereitgestellt werden?

Schwierig ist diese Situation in zweierlei Hinsicht: Zum einen kann ein Angreifer über das unsichere Gerät versuchen, Zugriff auf das interne Netzwerk zu gewinnen, zum andern sind solche Systeme aber auch willkommener Rückzugsort und Basislager für Angreifer, die bereits Zugriff auf das Netzwerk gewonnen hatten. Bevor eine Schadsoftware vom Laptop des Mitbewohners entfernt wurde, kann diese beispielsweise eine Sicherheitslücke des Webservers der Kaffeemaschine genutzt haben, um sich dort einzunisten. Ein eventueller Angreifer hat von dort dann auch später Zugriff, um jederzeit neue Schwachstellen zu suchen, neue Angriffe vorzubereiten und durchzuführen.

Kurzum: Das heimische Netzwerk ist nicht sicher. Dementsprechend wichtig ist es, die für die Home-Office-Tätigkeit genutzten Systeme von den Gefahren des Heimnetzwerks zu separieren. Dies erfolgt zum einen über die Nutzung einer restriktiv konfigurierten lokalen Firewall-Software, zum einen über „Netzwerkseparierung". Wie im Unternehmen die Netze der Produktion von denen der Verwaltung oder der Entwicklung getrennt sind, so sollte eine solche Trennung auch für den Netzbereich des Home-Office von den übrigen Bereichen im Heim-Netzwerk erfolgen.

Umgesetzt werden kann dies aufwendig und konsequent, in dem ein eigener Internet-Zugang mit eigener, vom Unternehmen gewarteter Router-Hardware, ggf. einer Firewall, genutzt wird. Notwendige Kosten und Aufwand hierfür sind vom Risiko bzw. Schutzniveau der zu Hause verarbeiteten Daten und den Zugriffsmöglichkeiten des Mitarbeiters im Unternehmens abhängig. Ist das Risiko überschaubar, so ist der zweite Zugang nicht unbedingt erforderlich. Stattdessen kann über die Nutzung der Optionen aktueller Standard-Hardware ein gutes Sicherheitsniveau hergestellt werden.

Eine erste, zentrale Überlegung ist, ob überhaupt das WLAN genutzt werden muss. Das Funknetzwerk bietet viele Vorteile.

Generell ist WLAN nicht auf die eigenen vier Wände begrenzt, Angriffe aus der Nachbarschaft sind also möglich. Je nach verwendetem Standard ist WLAN auch nur bedingt sicher - es spricht also einiges für die Verwendung eines kabelgebundenen Netzwerks, sofern die baulichen Gegebenheiten dies zulassen. Neben der besseren Sicherheit ist die tatsächliche Performance in der Regel höher als die des WLANs, die Störanfälligkeit geringer.

Nutzt man also den vermeintlich veralteten kabelgebundenen Anschluss, so kann die Separierung vom Heimnetzwerk oft einfach erfolgen: Nicht nur teure Firewall-Hardware erlaubt die Nutzung einzelner Netzwerk-Ports als isolierte Zone. In vielen Varianten der weitverbreitete „Fritz-Box“ z.B. lässt sich ein Port als „Gast-Zugang“ nutzen, welcher isoliert von den übrigen Geräten im Netzwerk und dem WLAN betrieben wird. Der Name muss also nicht Programm sein, das „Gäste-Netz“ lässt sich also ebenso gut als sauberes, isoliertes Home-Office-Netz nutzen. Bietet der vorhandene Router eine solche Option nicht, so kann mit einem „managed-“ oder „smart“-Switch die Funktion eines isolierten Ports nachgebildet werden.

Auch für das WLAN bieten viele Router-Hersteller die Option, einen „Gast-Zugang“ getrennt vom übrigen WLAN bereitzustellen. Ist dieser nicht schon für „Gäste“ im Einsatz, dann kann er analog zur kabelgebundenen Lösung für ein isoliertes Büro-WLAN genutzt werden. Ist der „Gast-Zugang“ schon in Benutzung, dann kann die kabelgebundene Lösung aus dem vorhergehenden Abschnitt über einen eigenen Access-Point um ein weiteres, isoliertes WLAN erweitert werden.
Bei der Nutzung von WLAN muss ein sicheres WLAN-Passwort verwendet werden (mindestes 30 Zeichen, inkl. Groß-, Kleinbuchstaben, Ziffern, und internationale Sonderzeichen).

Grundsätzlich ist die WLAN-Kommunikation verschlüsselt. Die veralteten und seit langem unsicheren Standards „WPA“ oder gar „WEP“ dürfen jedoch keinesfalls mehr verwendet werden, ideal ist das aktuelle WPA3. Um 2018 gab es Möglichkeiten, die Sicherheit von WPA2 auszuhebeln. Durch Patchen auf Betriebssystemseite konnte dies aber wieder eingefangen werden. Aktuell ist der Einsatz von WPA2 daher unbedenklich.

2.5 Der Zugang zum Unternehmen

Die Ausführlichkeit, in der im letzten Kapitel die Sicherheit des Netzwerks im Home-Office betrachtet wurde, liegt darin begründet, dass letztendlich ja ein Zugriff vom Home-Office auf das Unternehmensnetzwerk erfolgen muss. Durch diese Verbindung ist die Sicherheit des Home-Office-Netzes also auch relevant für die Sicherheit des Unternehmensnetzwerks.

Die Anbindung ans Unternehmensnetzwerk soll idealerweise dafür sorgen, dass der Mitarbeiter im Home-Office mit den Unternehmensressourcen und -Daten weitgehend so arbeiten kann, als wäre er vor Ort. Dabei soll sichergestellt werden, dass weiterhin nur Berechtigte auf diese Ressourcen zugreifen und die Vertraulichkeit erhalten bleibt.
Diese Funktion wird über ein „VPN" (Virtual Private Network") bereitgestellt. Eine Technik, die auch weithin genutzt wird, um Unternehmensstandorte über das öffentliche Internet hinweg sicher miteinander zu verbinden.

Im Falle des Mitarbeiters im Home-Office werden in der Regel jedoch nicht die Standorte (also ganze Rechnernetze auf beiden Seiten der Verbindung) miteinander verbunden. Lediglich der Heim-Arbeitsplatzrechner erhält Zugang. Im Normalfall erfolgt dies über eine Client-Software, die einen VPN-Tunnel aufbaut, denjenigen Datenverkehr ermittelt, der sich auf ein Ziel im Unternehmen bezieht, diesen verschlüsselt und auf den Weg durch das öffentliche Internet schickt, an dessen Ende die Unternehmensfirewall steht. Diese nimmt den Verkehr entgegen, entschlüsselt den Inhalt und speist den Verkehr ins Unternehmensnetzwerk ein. Umgekehrt verfahren wird mit der Antwort des angesprochenen Systems. Auf diesem Weg wird das private Unternehmensnetzwerk völlig anwendungstransparent „virtuell" bis zum Arbeitsplatz im Home-Office erweitert.

Viele VPN-Lösungen bieten gleich mehrere Optionen, um vom externen Nutzer potentiell eingebrachte Risiken zu minimieren. So können Richtlinien hinterlegt werden, die automatisiert geprüft werden, wenn ein System Zugang anfordert. Erfüllt ein System im Home-Office diese Voraussetzungen nicht, so wird der Zugang verweigert.

Zu den geprüften Kriterien gehören z.B.:

- Betriebssystemversion und Patch-Level,
- Antivirus-Software und Pattern-Aktualität,
- keine Malware-Funde,
- keine gravierenden Vulnerabilitäten,
- Firewall-Einstellungen und weitere mehr.

Auch die Identität des Benutzers wird geprüft, ggf. auch über einen zweiten Faktor und unter Einbindung bestehender Authentifizierungssysteme im Unternehmen. Außerdem ist es möglich (und i.d.R. auch sinnvoll), den direkten Zugriff vom Home-Office auf das öffentliche Internet zu unterbinden. Der Zugriff auf das öffentliche Netz erfolgt stattdessen über das bestehende VPN und damit über den Unternehmens-Internetzugang. Dort implementierte Maßnahmen zum sicheren Internetzugriff (Webfilter, AV-Proxy, …) greifen damit vollumfänglich auch für jeden Mitarbeiter im Home-Office.

Über das VPN können alle Netzwerkprotokolle sicher wie vor Ort genutzt werden, es gibt keine technisch bedingten Einschränkungen. Allenfalls Latenz und Netzwerkperformance können bei der Nutzung mancher Anwendung zu Nachteilen gegenüber der Nutzung vor Ort führen. Das Ausmaß der Einschränkung ist stark abhängig von der Art der Anwendung, der Geschwindigkeit des Netzzugangs am Heimarbeitsplatz, der Entfernung zum Unternehmen und der zur Verfügung stehenden Bandbreite auf Unternehmensseite. Besonders Anfällig für solch nachteilige Auswirkungen sind datenbankgestützte Client-Server-Anwendungen wie z.B. viele ERP-Systeme. Da der Arbeitsplatz-Client direkt zahlreiche Abfragen auf dem Serversystem initiiert und es zum Austausch sehr vieler, meist kleiner Datenpakete kommt, wirkt sich die Latenz besonders nachteilig aus. Abhilfe schafft hier, die Interaktion mit dem Server „in der Nähe" des Anwendungsservers stattfinden zu lassen. Dies bringt uns zu Terminalserver- oder VDI-Lösungen (Virtual Desktop Infrastruktur). Beiden Ansätzen ist gemein, dass die aus dem Home-Office genutzten Anwendungen an zentraler Stelle im Unternehmen betrieben werden. Lediglich Anzeige und Ausgabe wird zum Home-Office-Rechner geleitet, welcher wiederum Eingaben entgegennimmt und diese zum zentralen System weiterleitet.

Der Arbeitsplatzrechner im Home-Office wird zum simplen Terminal, welches kaum lokal installierte Software und Daten vorhalten muss. Die Wartung und Kontrolle der Systeme durch das Unternehmen wird simpler, Risiken werden minimiert. Umgekehrt bringt eine solche Lösung wiederum anwendungsspezifische Nachteile, z.B. bei der Bild- oder Videobearbeitung, mit sich.

3. Fazit

Mit Sicherheit wird das Thema Home Office auch nach der aktuellen Pandemie seine Bedeutung behalten und diese weiter ausweiten. Das Unternehmen muss sich damit neuen Risiken stellen und Maßnahmen ergreifen, um die Kontrolle über die Sicherheit der Home-Office-Rechner zu behalten und sich gegenüber neuen Gefahren aus dem dortigen Netzwerkumfeld zu wappnen. Die technischen Möglichkeiten sind gegeben. Welche davon in welchem Umfang eingesetzt werden sollen ist, wie so oft, eine Abwägung von individuellem Risiko und erforderlichem Aufwand, die im Unternehmenskontext vorgenommen werden muss. Entscheidet sich das Unternehmen dafür, dem Mitarbeiter die Absicherung des Home-Offices in Teilen selbst aufzubürden, so muss dies eine bewusste Entscheidung sein. Dem Kollegen im Home-Office müssen die Risiken und Verantwortlichkeiten bewusst gemacht werden. Gleichzeitig erhält er aber die notwendige technische und organisatorische Unterstützung , die erforderlich ist, um das angestrebte Sicherheitsniveau zu erreichen und zu erhalten.

4. Checkliste Sicheres Home Office

- Daten und Dokumente auch im Home-Office vor fremdem Zugriff schützen
- Sichere Entsorgung: Shredder für Dokumente bereitstellen; zentrale, sichere Entsorgung von Datenträger ermöglichen
- Ausschließlicher Einsatz eines vom Unternehmen gestellten und gemanagten Laptops/Computers
- Einsatz einer lokale Firewall und von Virenscannern
- Einbindung in zentrale Update-, Patch- und Softwareverteilung sowie zentrale Monitoring- und Alarmierungsmechanismen
- Isolierung im Heimnetzwerk sicherstellen (eigenes Netzwerksegment, z.B. Umdeutung des "Gast-Zugangs")
- Kabelgebundenen Zugang gegenüber WLAN bevorzugen
- Bei WLAN-Einsatz aktueller Standards (WPA2/WPA3)
- Gesicherter Unternehmenszugang über VPN, Absicherung über zweiten Faktor
- Automatische Prüfung festgelegter Zugangskriterien (in Bezug auf Sicherheit des Clients)
- Geregelter Internet-Breakout zentral über Unternehmens-Firewall
- Ggf. Einsatz von Terminalservern oder VDI

Praxisleitfaden

Sicheres Arbeiten im Home Office

Continum AG

Bismarckallee 7b–d
79098 Freiburg

Tel.: +49 (0)761 217111-0
Fax: +49 (0)761 217111-99

www.continum.net

Technik
E-Mail: technik@continum.net
Tel.: +49 (0)761 217111-77

Vertrieb
E-Mail: vertrieb@continum.net
Tel.: +49 (0)761 217111-0