



© Halfpoint -Adobe Stock

MITARBEITERINFORMATION: MOBILES ARBEITEN



PRIVACYXPERTS

INHALT

1. Mobiles Arbeiten: Das müssen Sie beachten!

Arbeiten von Unterwegs

Im Homeoffice sicher arbeiten

2. Datenschutz und Office 365: So klappts mobil!

Outlook in Office 365. Was muss ich beachten?

Sharepoint und OneDrive

3. Frequently Asked Questions

MOBILES ARBEITEN: DAS MÜSSEN SIE BEACHTEN!

Durch die zunehmende Vernetzung wird die Welt immer kleiner und auch das Arbeiten von unterwegs wird durch mobile Geräte und Internetanschluss immer flexibler. Das Bewusstsein dafür, dass außerhalb der Unternehmensmauern die gleichen Regelungen für den Umgang mit schutzwürdigen Informationen wie am Arbeitsplatz gelten, ist nicht immer vorhanden.

Arbeiten von Unterwegs: Diese Aspekte sollten Sie beachten

Mobile Geräte

Sie sind Ihr ständiger Begleiter und dürfen erst recht unterwegs nicht fehlen: Smartphone, Notebook, USB-Stick & Co. Diese Geräte haben eines gemeinsam: Sie enthalten eine Vielzahl an schutzwürdigen Informationen. Überprüfen Sie regelmäßig, ob Ihre Geräte nach dem neuesten Stand der Technik verschlüsselt sind, um auch bei Verlust der Geräte den Zugriff Unbefugter zu verhindern. Außerdem: Erkundigen Sie sich immer vor der Reise oder Arbeit von unterwegs, ob in Ihrem Hotel ein Safe vorhanden ist, den Sie vor Ort für Ihre Geräte nutzen können. Achten Sie dabei auch darauf, dass ein Safe nicht nur existiert, sondern dass er auch Sicherheitsstandards erfüllt und groß genug ist, um z.B. Ihren Laptop darin zu verstauen.

Sichtschutz und Telefonie

Unterwegs, zum Beispiel im Zug, bleibt es kaum aus, dass Ihnen jemand mal unbemerkt einen Blick über die Schulter wirft. Hat der Blick freie Bahn, dann können schutzbedürftige Informationen unbefugten Personen zur Kenntnis gelangen. Unerwünschte Blicke können Sie ver-

hindern, indem Sie eine Sichtschutzfolie verwenden. Diese wird z.B. auf dem Bildschirm Ihres Notebooks oder Smartphones angebracht und macht ein Mitlesen von der Seite unmöglich.

So schützen Sie effektiv Informationen vor unbefugten Dritten.

Beim Telefonieren unterwegs gilt: Achten Sie auf eine vor Mithörern geschützte, sichere Umgebung. Das heißt: Suchen Sie immer einen Ort abseits der Menschenmengen auf, wenn Sie telefonieren möchten. Wenn jemand Sie anruft, während Sie sich an einem für vertrauliche Gespräche ungeeigneten Ort befinden, teilen Sie dem Anrufer mit, dass Sie sich gleich zurückmelden, und suchen Sie einen sicheren Ort zum Telefonieren auf.

Passwörter und WLAN

Passwörter sind wie der Schlüssel zu Ihrem Zuhause: Erfüllt er bestimmte Sicherheitsstandards nicht, ist es für Einbrecher ein Leichtes, sich Zugang zu Ihren vier Wänden zu verschaffen. Genauso ist es mit Ihren Passwörtern. Passwort ist nicht gleich Passwort: IT-Sicherheitsexperten vertreten mittlerweile die Meinung, dass es weniger auf die Komplexität als auf die Länge des Passwortes ankommt: 12 Zeichen sind empfehlenswert. Jedes weitere Zeichen erhöht die Sicherheit. Genauso wichtig wie die Gestaltung des Passwortes ist, dass Sie Ihr Passwort niemals weitergeben – auch nicht an Personen, denen Sie absolutes Vertrauen schenken. Ein Schaden, der durch ein weitergegebenes Passwort entsteht, fällt grundsätzlich auf Sie zurück.

Ebenfalls wichtig: Auch wenn bei lahmem und ruckeligem Reiseinternet wenig so verlockend wirkt wie ein WLAN-Hotspot in der Bahn oder am Flughafen: Nutzen Sie für Ihre Datenübertragung immer einen soge-

nannten VPN-Tunnel (Virtual Private Network). Dann sind Sie und Ihre Daten auf der sicheren Seite.

Im Homeoffice sicher arbeiten

Umgang mit Arbeitsmitteln

Achten Sie darauf, dass zur Verfügung gestellte Arbeitsmittel wie Notebook, Tablet oder Smartphone tatsächlich nur für Arbeitsangelegenheiten genutzt und nicht an Dritte weitergegeben werden. Außerdem müssen die Geräte regelmäßig mit Sicherheitsupdates oder Programmaktualisierungen versorgt werden, z. B. durch einen Anschluss an das Firmennetzwerk. Wichtig: Bei Unregelmäßigkeiten unverzüglich die IT-Abteilung aufsuchen!



Verwenden Sie für die Arbeit im Homeoffice ausschließlich die vom Unternehmen zur Verfügung gestellten Datenübertragungsverfahren (z. B. VPN-Einwahl). Vorhandene Schutzmechanismen wie Firewall, Virenschutz und WLAN-Verschlüsselung sollten stets aktuell gehalten und auf keinen Fall deaktiviert werden.

Schutz vor Zugriff durch Unbefugte

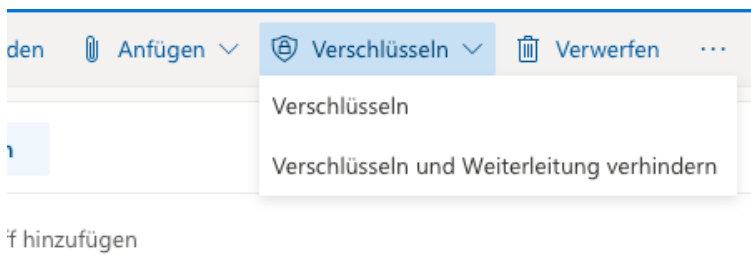
Arbeitsmittel und schützenswerte Informationen müssen Sie so aufbewahren und schützen, dass Unbefugte keinen Zugriff darauf haben und Kenntnis davon erhalten können.

DATENSCHUTZ UND OFFICE 365: SO KLAPPTS MOBIL!

Microsoft verfolgt seit einigen Jahren eine weitreichende Cloudstrategie. Insbesondere das Produkt Office 365 hat Microsoft den Weg in viele Unternehmen geebnet. Für Sie als Nutzer gilt es jedoch, einige grundlegende Anforderungen zum Schutz der Daten zu beachten.

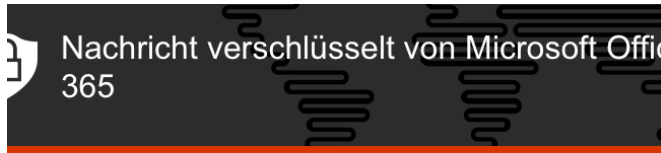
Outlook in Office 365. Was muss ich beachten?

Outlook unterscheidet sich in der Online- Variante kaum von der lokal installierten Office-Version. Allerdings bietet die Office- 365-Variante ab der Lizenz E5 die Möglichkeit, E-Mails sicher zu verschlüsseln, und das auch mit Partnern außerhalb des Unternehmens. Die Partner müssen noch nicht einmal Office 365 nutzen. Das ist ein enormer Mehrwert für den Datenschutz und die Datensicherheit. Wenn Sie bei einer neuen E-Mail die Option „Verschlüsseln“ im Menüband auswählen können, steht Ihnen diese Funktion zur Verfügung.



Wählen Sie „Verschlüsseln“, wird die E-Mail inklusive Anhang sicher verschlüsselt. Der Empfänger erhält eine E-Mail mit einem Link auf die verschlüsselte E-Mail. Der Empfänger muss sich nun authentifizieren.

In diesem Fall entweder mit einem Google Account oder einem temporären Account. Wird der temporäre Account gewählt, erhält der Empfänger eine E-Mail mit einem Zifferncode, den er in das Anmeldefenster eingeben muss. Dann steht ihm die Nachricht zur Verfügung.



Geben Sie den Code ein, den wir Ihnen gerade unter andreas.hessel@gmail.com gesendet haben.

A light gray rectangular input field with a thin blue border. Inside the field, the text "Code eingeben" is written in a light gray font. To the right of the text is a small black icon of a speech bubble with three dots inside. To the right of the input field is a solid black square button.

☐ Diesem Computer für die nächsten 12 Stunden vertrauen

Sharepoint und OneDrive. Was muss ich beim Teilen von Dateien beachten?

Das Teilen von Dateien in Sharepoint oder OneDrive ist ein sehr effektives Mittel, um anderen Personen schnell Informationen zur Verfügung zu stellen. Doch gilt es, einige Regeln zu beachten, denn sonst sind die Informationen auch schnell in den falschen Händen oder stehen schlimmstenfalls für jedermann frei im Internet zur Verfügung. Wenn Ihnen Ihr Administrator erlaubt hat, Daten auch außerhalb Ihres Unternehmens zu teilen, sollten Sie nachfolgende Regeln beachten. Wenn Sie eine Datei teilen möchten, bekommen Sie zunächst folgendes Fenster angezeigt:

Link senden

...

×



Von Ihnen angegebene Personen können bearbeiten

>



Andreas.hessel@gmail.com

×

Weiteres hinzufügen



Andreas.hessel@gmail.com ist außerhalb Ihrer Organisation.

Nachricht hinzufügen (optional)

Senden



Link kopieren



Outlook

Prüfen Sie zunächst die Option „Von Ihnen angegebene Personen können bearbeiten“ im Detail. Klicken Sie hierzu auf die entsprechende Schaltfläche:

Linkeinstellungen

×

Bei wem soll dieser Link funktionieren? [Weitere Informationen](#)



Jeder mit dem Link



Personen bei Datenschutz...onssicherheit mit dem Link



Personen mit Zugriff



Bestimmte Personen

✓

Weitere Einstellungen

☒

Bearbeitung zulassen

☐

Download blockieren



Übernehmen

Abbrechen

Das müssen Sie konkret zu den Optionen wissen: Haben Sie die entsprechende Option ausgewählt, können Sie das Fenster mit der Schaltfläche „Übernehmen“ schließen und im folgenden Fenster entweder direkt mit der Schaltfläche „Senden“ den Link verschicken oder über die Schaltfläche „Link kopieren“ lediglich kopieren.

Fazit

Office 365 stellt eine Vielzahl von Services bereit, die insbesondere die Zusammenarbeit und den Datenaustausch erleichtern. Prüfen Sie immer, welche Rechte Sie den Empfängern einräumen und ob der Zugriff auf die Daten überhaupt erforderlich ist. Nicht jeder benötigt nämlich alle Daten. Dann sind Sie auch mit Office 365 auf der sicheren Seite.

Checkliste: Teilen und Bearbeiten im Sharepoint

Option	Auswirkung	Empfehlung
Jeder mit dem Link	Jeder, der den Link erhält, kann die Datei bearbeiten. Wird die E-Mail ab-gefangen oder an andere Personen weitergeleitet, haben Sie keinerlei Kontrolle mehr.	nicht empfehlenswert
Personen im jeweiligen Unternehmen (Beispiel Personen bei Datenschutz und Informationssicherheit)	Nur wer in Ihrem Unternehmen registriert ist, kann die Datei abrufen	empfehlenswert, wenn interne Informationen im Unternehmen verteilt werden sollen; nicht empfehlenswert im Unternehmen, wenn es sich um personenbezogene Daten handelt
Personen mit Zugriff	nur Personen, die von Ihnen oder in der Regel bereits von einem Administrator Zugriff auf die Datei erhalten haben (z. B. Teams oder Abteilungen)	empfehlenswert
Bestimmte Personen	alle Personen, die Sie per E-Mail-Adresse eingetragen haben	empfehlenswert, unkritisch, wenn der Personenkreis fest definiert wurde
Weitere Optionen		
Download blockieren	Der Empfänger kann die Datei nicht downloaden	empfehlenswert bei sensiblen Daten, über die lediglich informiert werden soll
Bearbeitung zulassen	Der Empfänger des Links kann die Datei herunterladen und damit in seinen Einflussbereich bringen. Sie haben keine Kontrolle mehr.	empfehlenswert, wenn es sich um eine Datenübermittlung handelt nicht empfehlenswert bei Informationen zu sensiblen Vorgängen

FREQUENTLY ASKED QUESTIONS

Wie sollten Notebook, Datenträger und Unterlagen unterwegs aufbewahrt werden?

Wenn Sie unterwegs sind, sollten Sie Notebook, Datenträger und Unterlagen nach Möglichkeit immer so aufbewahren, dass sie den Blicken Unberechtigter entzogen sind. Das bedeutet etwa, dass ein Notebook während der Fahrt im Auto nur im Kofferraum transportiert wird. Bei Tagungen und Besprechungen kann es sinnvoll sein, dass Sie Ihr Notebook mittels eines sogenannten Kabelschlosses an einem Tisch oder Heizkörper sichern. So machen Sie es potenziellen Dieben schwer und brauchen sich um Ihr Gerät in der Regel keine Sorgen machen, wenn Sie den Raum kurz für eine Kaffeepause verlassen.



Inwiefern sollte das Minimalprinzip zur Anwendung kommen?

Auf Geschäftsreise brauchen Sie in der Regel nie Ihre komplette Büroausstattung. Nehmen Sie daher nur diejenigen Gerätschaften, Speichermedien und Unterlagen mit, die Sie für Ihre Arbeit unbedingt benötigen. Wenn Sie weniger bei sich haben, erleichtern Sie dadurch nicht nur das entsprechende Gepäck. Was Sie nicht dabei haben, kann weder gestohlen werden noch abhandenkommen.

Weshalb sollten Datenträger und Daten verschlüsselt werden?

Werden Datenträger und Daten verschlüsselt, machen Sie es Unbefugten ziemlich schwer, auf diese zuzugreifen. Möglichkeiten zur Verschlüsselung gibt es zahlreiche, etwa durch Anlegen eines verschlüsselten Dateiarchivs (sogenannte ZIP-Datei) oder durch die Nutzung von Verschlüsselungssoftware oder hardwareverschlüsselten Speichermedien. Der entscheidende Vorteil: Kommt es zu einem Diebstahl, beschränkt sich der Schaden in erster Linie auf den Materialwert der gestohlenen Sache. Weil man dank Verschlüsselung nicht auf die Daten zugreifen kann, besteht in aller Regel kein Risiko für Datenschutz und Vertraulichkeit.

Welche technischen Schutzmechanismen sind von besonderer Bedeutung?

Gerade unterwegs ist es wichtig, dass Sie vorhandene Schutzmechanismen nutzen. Deaktivieren Sie auf keinen Fall die Firewall Ihres Notebooks und schalten Sie nie die Überwachungsfunktion des Virenscanners aus. Firewall und automatische Virenerkennung sind gerade dann von Bedeutung, wenn Sie Ihren Computer mit dem Internet verbinden, etwa um E-Mails abzurufen. Sie sind aber genauso wichtig, wenn Sie Daten und Dateien von Geschäftspartnern oder Kunden erhalten, die

sich auf USB-Sticks oder CDs befinden. Personenbezogene Daten auf einem mobilen Datenträger sollten immer besonders gegen unberechtigten Zugriff geschützt werden. Verschlüsselung der Daten oder des ganzen Datenträgers ist ein adäquates Mittel. Übrigens: Machen Sie es Hackern so schwer wie möglich. Wenn Sie keine Drahtlosverbindung benötigen, sollten Sie die entsprechende Funktion an Ihrem Notebook oder Ihrem Smartphone abschalten.

Was ist beim Arbeiten in Zug, Flugzeug oder im Hotel zu beachten?

Bedenken Sie immer, dass Ihr Umfeld unter Umständen sehr neugierig ist und wissen will, was Sie machen. Wählen Sie nach Möglichkeit Ihren Sitzplatz so, dass Ihnen niemand über die Schulter schauen kann. Auch sogenannte Sichtschutzfolien für Notebookbildschirme, Smartphones und Smartpads sind eine datenschutzfreundliche Hilfe. Sie sorgen für eine andere Lichtbrechung, sodass Ihre Sitznachbarn nicht erkennen können, was auf Ihrem Bildschirm zu sehen ist.

Warum sollte nicht jedes verfügbare WLAN für eine Verbindung ins Internet genutzt werden?

Wenn Sie Ihr Notebook mit einem WLAN verbinden wollen, sollten Sie immer solchen WLAN-Hotspots den Vorzug geben, die von renommierten Diensteanbietern bereitgestellt werden. Bei anderen Diensteanbietern oder sogenannten wilden WLAN-Hotspots können Sie sich nie sicher sein, welche Interessen der Anbieter tatsächlich verfolgt, vielleicht wartet er – wie die Spinne im Netz – auf fette Beute. Alternativ können Sie auch Datenübertragungsdienste von Mobilfunkanbietern nutzen. Doch auch hier gilt: Wie beim WLAN ist eine Datenübertragung nur dann sicher, wenn sie verschlüsselt erfolgt. Nutzen Sie daher zur Verfügung stehende VPN-Lösungen. Die IT-Abteilung berät Sie gerne.

Was ist zu tun, wenn Computer, Datenträger oder Unterlagen gestohlen werden oder verloren gehen?

Kommt es hierzu, müssen Sie unverzüglich das Unternehmen verständigen. Informieren Sie einerseits Ihren Vorgesetzten und andererseits die IT-Abteilung. Sind personenbezogene Daten oder vertrauliche Informationen betroffen, sollten Sie zusätzlich den Datenschutzbeauftragten informieren. Diese Stellen werden die Situation bewerten und geeignete Maßnahmen in die Wege leiten. Wichtig: Wird Ihnen etwas gestohlen, sollten Sie unbedingt Strafanzeige bei der örtlichen Polizei stellen und sich die Erstattung einer Anzeige bestätigen lassen.



PrivacyXperts

ein Unternehmensbereich der

VNR Verlag für die Deutsche Wirtschaft AG

Theodor-Heuss-Straße 2-4; D-53095 Bonn

Vorstand: Richard Rentrop

Telefon: 0228 - 9 55 01 50 (Kundendienst)

Telefax: 0228 - 3 69 64 80

E-Mail: kundendienst@privacyxperts.de

Internet: <https://www.privacyxperts.de>

Redaktionell Verantwortlicher:

Thomas Steiner, Theodor-Heuss-Straße 2-4, D-53177 Bonn

Autor: Andreas Würtz, Andreas Hessel, Sebastian Tausch

Satz: Anna Gels, Bonn

© 2020 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest,
Manchester, Warschau