Sicheres Arbeiten von unterwegs

↗ Leitfaden zum Umgang mit mobilen Medien für Unternehmen

↗ Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e.V.

Schirmherrschaft:

Bundesministerium des Innern

Deutschland sicher im Netz

Vorwort

Neue Geräte wie Smartphones und Tablet-PCs haben im letzten Jahrzehnt die Organisation von beruflichen und privaten Aktivitäten maßgeblich verändert. Vielfältige Kommunikationskanäle lassen die Entfernungen zwischen zwei Orten gefühlt schrumpfen. Dies ist auch für mittelständische Unternehmen ein Vorteil – sei es der Eventveranstalter, der seinen Mitarbeitern in letzter Minute noch eilige Informationen liefert, oder der Tischler, der sich per Mail, SMS oder Anruf mit seinen Monteuren im Außendienst über Fenstermaße austauscht.

Die Geräte erlauben nicht nur den Zugriff auf Daten im Gerät selbst, sondern vor allem auch auf Daten im Internet bzw. in der Cloud. Wenn es sich anbietet, nutzt man private Geräte für den Beruf und berufliche Geräte für das Privatleben. Dies stellt für Unternehmer auch eine Herausforderung in Sachen Sicherheit dar. Die privaten Daten der Mitarbeiter sollen unangetastet bleiben, aber die Sicherheitsfunktionen zu den Anforderungen des Unternehmens passen. Sicherheitsrichtlinien und -lösungen sind wichtig, da bei einem Diebstahl (selbst bei kleinen Unternehmen) der Wert der verlorenen Daten höher sein kann als der des Geräts.

Deutschland sicher im Netz e.V. (DsiN) setzt sich dafür ein, mittelständische Unternehmen für IT-Sicherheit zu sensibilisieren. Daher unterstützen DsiN und DATEV eG mit diesem gemeinsamen Leitfaden Unternehmen dabei, passende organisatorische Maßnahmen zu ergreifen. Nutzen Sie die vorliegende Broschüre, um Ihre Mitarbeiter im Umgang mit mobilen Geräten zu stärken und Ihr Unternehmen vor Datenverlusten zu schützen.

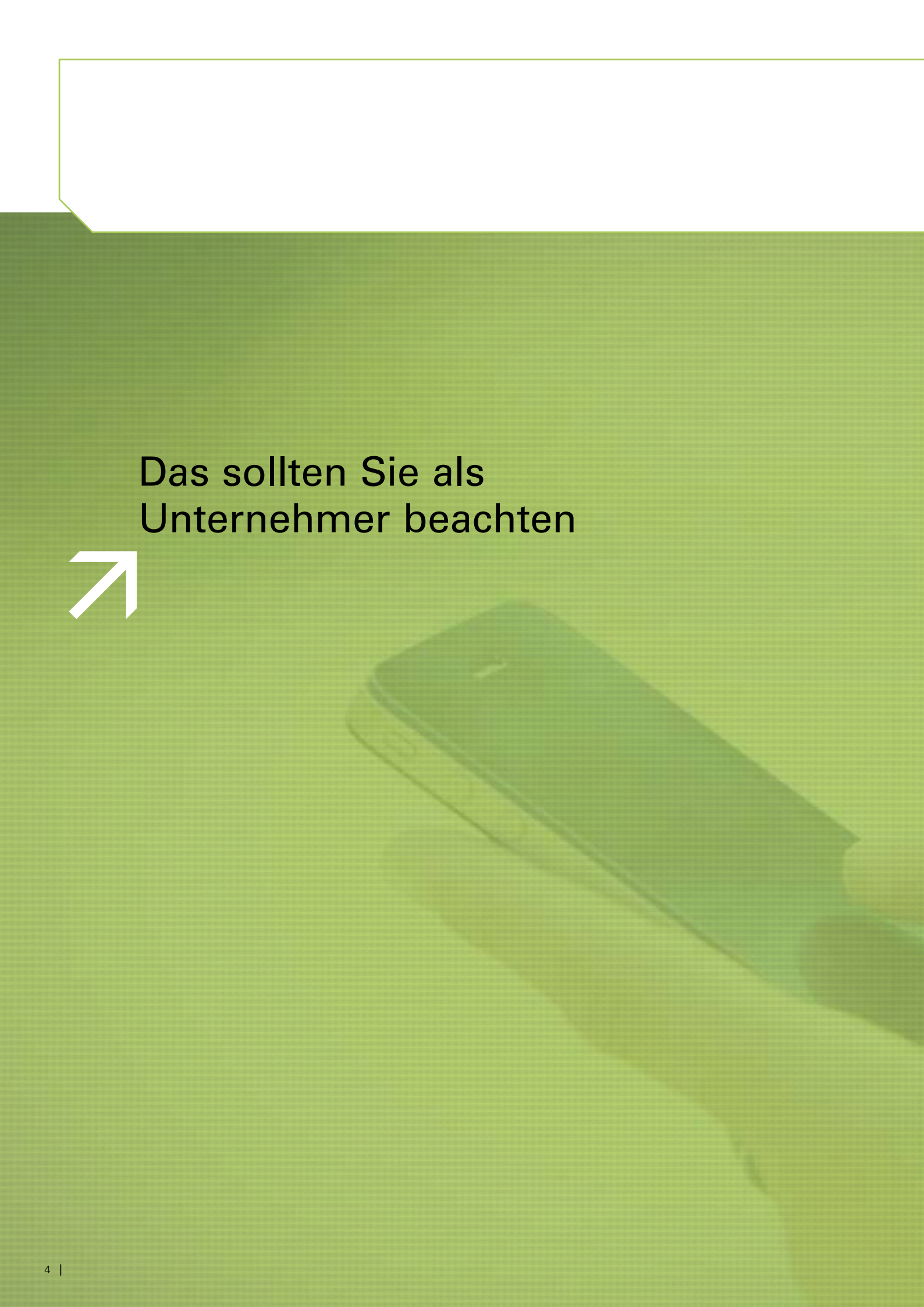
Dr. Christian P. Illek
Vorstandsvorsitzender Deutschland sicher im Netz e.V.

Sicheres Arbeiten von unterwegs

Leitfaden zum Umgang mit mobilen Medien für Unternehmen

Leitfaden: Das sollten Sie als Unternehmer beachten

Das sollten Sie als Unternehmer beachten



Leitfaden

Mobiles Arbeiten hat verschiedene Facetten, wie Zugriff auf die Unternehmensdaten über Tablet-PC oder Notebook, das Bearbeiten der Mails unterwegs auf dem Smartphone, Recherchen im Internet oder die Nutzung von Apps. Diese Möglichkeiten verändern die Beziehung zu Ihren Kunden – aber auch die Strukturen in Ihrem Unternehmen. Egal, welche Alternativen des mobilen Arbeitens Sie in Ihrer Praxis einführen oder nutzen – Sie greifen über das Internet meistens auf sensible Daten zu. Deshalb ist der sichere Zugriff auf die Unternehmensdaten und der verantwortungsvolle Umgang mit den Geräten unabdingbare Voraussetzung für deren Einsatz. Die folgende Struktur unterstützt Sie dabei, sich im Vorfeld gezielt mit den richtigen Fragen zu beschäftigen und zeigt Ihnen, wie Sie Ihre Mitarbeiter aufklären sollten. Diese Checkliste ersetzt jedoch keine umfassende Beratung zu Sicherheitsthemen.

1 Einsatzmöglichkeiten

Legen Sie im Vorfeld Ihre Mobilstrategie fest. So können Sie die Anforderungen strukturieren.

Das Angebot an mobilen Geräten ist vielfältig. Für Ihre Wahl sind unterschiedlichste Faktoren entscheidend:

- Was will ich machen?
- Wie sicherheitssensibel sind die Daten, auf die ich zugreifen möchte?
- Wie lässt sich das Gerät adäquat absichern?
- Wie lässt sich das Gerät in die vorhandene IT-Struktur einbinden?
- Welche persönlichen Präferenzen gibt es?

Der folgende, kurze Exkurs zu Chancen und Möglichkeiten der einzelnen Geräte hilft Ihnen bei der Entscheidungsfindung.

1.1 Zugriff auf E-Mail, Kalender und Kontakte

Wenn Sie, beziehungsweise Ihre Mitarbeiter, unterwegs in den Informationsfluss des Unternehmens eingebunden sein wollen, ist ein Smartphone die richtige Wahl. So können Sie E-Mails austauschen und auf Kalender und Kontakte in Outlook zugreifen. Sie können Ihre Management-Aufgaben wahrnehmen und die Steuerung des Unternehmens per Mail auch in Abwesenheit weiterführen.

Setzen Sie in diesem Fall eine Sicherheitslösung ein, um auf die Daten im Unternehmensnetz sicher zugreifen zu können. Diese schützt Ihre E-Mails, Ihre Kalendereinträge sowie Ihre Kontakte vor dem unbefugten Mitlesen auf dem Server und während der Übertragung zu Ihrem Smartphone.

1.2 Zugriff auf Firmendaten

Möchten Sie unterwegs auf umfangreichere Daten in Ihrem Unternehmen zugreifen, so benötigen Sie ein Gerät mit einem etwas größeren Bildschirm als ein Smartphone. Tablet-PCs eignen sich nicht nur hervorragend für Präsentationen. Sie sind auch für andere Tätigkeiten eine Alternative zum Notebook, weil Sie weniger Peripherie benötigen: Der Akku hält mehrere Tage und das Ladegerät ist deutlich kleiner. Bei Bedarf kann eine Tastatur oder Maus angeschlossen werden. Wenn Sie also unterwegs kurz den Bearbeitungsstand eines Kunden oder einen Vertrag anschauen wollen, ist ein Tablet-PC die richtige Wahl. So profitieren Sie von minimalem Gepäck bei maximalem Zugriff. Kundenfragen können Sie beispielsweise unkompliziert und präzise von unterwegs beantworten – ganz ohne Rückfragen in der Firma.

Planen Sie umfangreichere und komplexere Anwendungen von unterwegs zu nutzen, sollten Sie auf ein Notebook umsteigen. Damit können Sie sich auch in das Unternehmensnetz einwählen und mit aktuellen Daten arbeiten. Das Notebook ist die richtige Wahl, wenn Sie unterwegs oder im Home Office arbeiten möchten, als wären Sie in der Firma.

Sorgen Sie dabei in jedem Fall mit entsprechenden Sicherheitslösungen vor, um auf Daten im Unternehmensnetz auch von unterwegs sicher zugreifen zu können. Sie schützen die Firmendaten vor dem unbefugten Mitlesen auf dem Server und während der Übertragung zu Ihrem Smartphone.

1.3 Zugriff über das Home-Office

Arbeiten Sie außerhalb des Unternehmens meistens an einem festen Ort, zum Beispiel zu Hause, ist ein Notebook mit größerem Bildschirm und Tastatur besser geeignet als ein Tablet-PC – und lässt sich zudem unterwegs nutzen. Alternativ können Sie einen Desktop-PC einsetzen. So arbeiten Sie auch von außerhalb immer in Ihrer bekannten Umgebung und es stehen Ihnen alle Daten und Anwendungen in gewohntem Komfort und Umfang zur Verfügung.

1.4 Zugriff auf Nachrichten, Tools und Recherchen

Falls es Ihr vorrangiges Ziel ist, unterwegs an aktuelle Informationen aus dem Internet zu gelangen, ist ein Smartphone ausreichend. So haben Sie Nachrichten oder Verkehrsmeldungen immer im Blick. Durch die Nutzung von entsprechenden Apps bestimmen Sie selbst, welche Informationen Sie erhalten.

2 Auswirkungen

Mobiles Arbeiten beeinflusst Ihre Arbeitsorganisation und die Beziehung zu Ihren Kunden und Mitarbeitern. Gehen Sie mit diesen Auswirkungen konstruktiv um: Nicht für jeden Mitarbeiter bedeuten diese Möglichkeiten eine willkommene Veränderung. Auch nicht alle Ihrer Kunden werden die Vorteile schätzen. Im Gegenzug können Sie diejenigen, die dem Thema offen und positiv gegenüberstehen, wirklich begeistern. Denn die flexiblen Arbeitsweisen machen Sie zu einem attraktiven Arbeitgeber.

Gehen Sie das Thema konstruktiv an, indem Sie auch Bedenken Ihrer Mitarbeiter und Geschäftspartner einbeziehen. Von den Vorteilen profitieren Sie am meisten, wenn Sie organisatorische Regelungen treffen.

Treffen Sie ausreichende Regelungen zur Erreichbarkeit für die Abwesenheitszeiten, damit diese Art der Arbeitsorganisation nicht zu einer Belastung wird. So können Sie zur Mitarbeiterzufriedenheit und Kundenbindung positiv beitragen.

2.1 Auswirkungen auf die Organisation des Unternehmens

Mobiles Arbeiten erhöht die Flexibilität Ihrer Mitarbeiter. So können berufliche Termine mit privaten Verpflichtungen besser in Einklang gebracht werden. Sie als Führungskraft können mit Ihren Mitarbeitern auch aus der Ferne kommunizieren.

Die Auswirkungen:

- Mitarbeiter bzw. Sie sind nicht immer persönlich erreichbar. Besprechungen müssen deshalb im Voraus organisiert werden.
- Immer erreichbar zu sein, kann auch Druck auslösen. Legen Sie Regelungen fest, zu welchen Zeiten Sie bzw. Ihre Mitarbeiter bei Außenterminen erreichbar sein sollen. Die Möglichkeit, beinahe immer und überall arbeiten zu können, darf nicht bedeuten, dass man das auch muss.
- Im Gegenzug können Sie auf Fachkräfte zurückgreifen, die sonst aus familiären Gründen ihre Berufstätigkeit einschränken müssten.

2.2 Auswirkungen auf die Mitarbeiterführung

Wenn Sie auch unterwegs für Ihre Mitarbeiter erreichbar und dadurch ins Firmengeschehen stets eingebunden sind, können Sie Ihre Management-Aufgaben besser wahrnehmen. Durch den Zugriff auf Unternehmensdaten stehen Sie Ihren Mitarbeitern für qualifizierte Antworten zur Verfügung und sind in der Lage, sie auch bei Abwesenheit fachlich zu unterstützen.

Termine lassen sich durch den Zugriff auf Ihren Kalender sofort und verbindlich vereinbaren. Das erhöht Ihre Zuverlässigkeit, gibt Ihren Mitarbeitern mehr Handlungssicherheit und bedeutet für Ihre Kunden eine zügige Bearbeitung. Permanente Erreichbarkeit kann allerdings auch Druck erzeugen. Treffen Sie deshalb Regelungen, wie unter Punkt 2.1 beschrieben.

2.3 Auswirkungen auf die Kundenbeziehung

Mit dieser Arbeitsweise können Sie gerade innovative Kunden begeistern: Die Verwendung von Smartphones oder Tablet-PCs gehört auch in Geschäftsbeziehungen zum Image. Zusätzlichen Imagegewinn erzielen Sie durch die Absicherung der Geräte mit einer entsprechenden Lösung.

Neben der Außenwirkung zählen natürlich die Sachargumente: Über die einfache Erreichbarkeit hinaus können Sie unabhängig vom Ort auf relevante Daten zugreifen und Ihre Kunden auf dieser Basis detailliert beraten. So wird in der Konsequenz auch die Entscheidungsfindung beschleunigt.

Beispiel: Sie sind unterwegs und Sie erreicht die dringende Anfrage eines Kunden. Um eine fundierte Antwort geben zu können, müssen Sie auf Unterlagen zugreifen, wie zum Beispiel auf den Bearbeitungsstatus eines Vorganges. Anschließend können Sie die Anfrage mit Ihrem Kunden telefonisch besprechen oder ihm eine E-Mail schicken.

3 Sicherheit

Treffen Sie ausreichende Maßnahmen zum Schutz der Geräte, der Verbindung zum Unternehmensnetz und der Daten. Klären Sie Ihre Mitarbeiter regelmäßig auf.

Die Sicherheitsvorkehrungen decken zwei Bereiche ab: zum einen den Schutz des Gerätes als materielles Gut gegen Diebstahl und zum anderen den Schutz der Unternehmensdaten, auf die Sie Zugriff haben. Ein Hackerangriff auf das Gerät erfolgt meist remote (also rechnerfern), ohne dass der Angreifer physischen Zugang zu dem Gerät hat. Um Risiken auszuschließen, geben Sie im gesamten Unternehmen einheitliche Regelungen für den Umgang mit dem Gerät vor. Setzen Sie ein zentrales Device Management[1] ein, welches auch für die Sicherheit sorgt.

[1] Zentrales Device Management steht für die zentrale Konfiguration und Verwaltung von PDAs, Smartphones und Tablet-Computern per Mobilfunk. Eine automatisierte, zentrale Installation und Konfiguration der Programme, Zertifikate und Einstellungen sorgen für den effizienten und sicheren Einsatz der mobilen Geräte.

Im Folgenden werden einige mögliche Fälle beschrieben. Lassen Sie sich umfassend zu IT-Sicherheit in Ihrem Unternehmen beraten. Ein Online-Sicherheitscheck vermittelt Ihnen einen schnellen Überblick zu Ihrer IT-Sicherheitslage.
Den Check finden Sie unter **www.sicher-im-netz.de/sicherheitscheck.**

3.1 Sicherheitsfalle „Apps"

Die Auswahl an möglicher Software, welche auf Smartphone oder Tablets installiert werden kann – sogenannte Apps – ist riesig. Leider gibt es einen sehr hohen Anteil an Apps, die nicht nur Vorteile bieten: Spyware und Programme, die deutlich mehr können, als sie vorgeben, sind für den Benutzer nicht erkennbar. Diese Apps agieren zusätzlich zu ihrem vorgegebenen Zweck im Hintergrund und richten Schaden an, indem sie ohne Ihre Zustimmung aus dem Gerät Informationen auslesen und unbefugten Dritten weiterschicken.

Geräte von manchen Herstellern sind weitgehend geschützt, weil diese Hersteller nur signierte und geprüfte Apps zulassen. Allerdings empfinden viele Benutzer das als einen Nachteil. Um auch Apps außerhalb des geprüften App-Stores auf einem Gerät zu installieren, muss das Gerät für beliebige Programme freigeschaltet werden: Diese Freischaltung bezeichnet man als Jailbreak.

Mit dem Jailbreak gewinnt man zwar viel Freiheit – dafür werden die Sicherheitshürden aber aufgehoben. Es ermöglicht den Zugriff auf die Daten trotz Sperrcode. Kennwörter, Zugangsdaten und andere gespeicherten Daten können problemlos ausgelesen werden – es muss nicht einmal der Sperrcode geknackt werden. Sie merken es unter Umständen nicht einmal.

3.2 Sicherheitsfalle „Diebstahl"

Mobile Geräte sind nicht nur praktisch, sondern auch beliebt und klein. Damit können sie einfach entwendet oder liegen gelassen werden. Beim Diebstahl steht nicht nur der materielle Wert der Hardware im Vordergrund, sondern auch der Kontrollverlust über sensible Daten. Besonders kritisch ist es, wenn Sie Daten auf dem Gerät gespeichert haben. Werden die mobilen Geräte durch ein zentrales Device Management verwaltet, so besteht je nach Anbieter die Möglichkeit, hier einzugreifen. So kann bei Bedarf eine Fernlöschung und Zugriffssperrung veranlasst werden.

Unsere Empfehlung: Greifen Sie bei Bedarf gesichert auf die Daten im Unternehmen zu, statt diese auf dem Gerät zu speichern. So minimieren Sie das Risiko des Datendiebstahls.

Durch Jailbreak (s. Punkt 3.1) kann der Passwortschutz umgangen werden. Das bedeutet, der Zugriff auf Ihre Firmendaten kann unbefugten Dritten gelingen, sofern Sie nicht anderweitige Sicherheitsmaßnahmen ergreifen.

3.3 Sicherheitsfalle „Einbindung ins Unternehmensnetz"

Smartphones & Co. sind ähnlich zu behandeln wie Notebooks, DVDs oder USB-Sticks: Es muss zunächst eine Virenprüfung erfolgen, bevor sie in die Systeme im Unternehmen eingebunden werden, Daten vom oder an das Gerät überspielt werden.

Viele Unternehmen erlauben ihren Mitarbeitern die geschäftliche Nutzung eines eigenen Tablets bzw. Smartphones. Die Vorteile sind vielfältig, die Risiken allerdings auch. Deshalb muss die IT sicherheitstechnisch angepasst werden. Am besten lassen Sie sich von Ihrem betreuenden Techniker beraten.

Immer mehr Menschen – darunter sicher auch Ihre Mitarbeiter – nutzen ein Smartphone. Die Forderung, von dieser Flexibilität ebenso im Beruf zu profitieren, wird stärker. Doch das eigene Gerät auch beruflich zu nutzen bietet nicht nur Vorteile: Was passiert zum Beispiel, wenn das Gerät beim Familientreffen im Restaurant liegen bleibt? Sind Unternehmensinformationen (Kontakte, E-Mails, Gesprächsnotizen) auf dem Gerät? Für solche Fälle müssen umfassende Regelungen vereinbart und regelmäßig geübt werden.

3.4 Zugangskontrolle

Aus Sicherheitsgründen ist es zu empfehlen, auf dem Smartphone oder Tablet-PC keine vertraulichen Daten zu speichern. Es ist auch nicht zwingend notwendig, denn der Zugriff auf die aktuellen und vollständigen Unternehmensdaten ist jederzeit möglich. Abzusichern ist nicht nur der Zugangsweg in das Unternehmensnetz, sondern auch der Zugriff auf die Daten. Bitte beachten Sie dabei:

- Eine einfache Zugangskontrolle mit Benutzernamen und Passwort ist leicht zu umgehen.
- Es gibt – wie bei Notebooks – Hardware-Komponenten zur Absicherung, der Aufwand für die Handhabung ist jedoch nicht angemessen.
- Die wirksame Zugangskontrolle muss auch praktikabel sein.

3.5 Sicherheits-Updates

Auch beim Einsatz moderner Smartphones und Tablets spielen Updates für Apps und das Betriebssystem eine wichtige Rolle.

Die Hersteller gehen sehr unterschiedlich mit der Sicherheit der Geräte um. Nicht alle halten das Betriebssystem zeitnah auf dem aktuellen Stand. Das ist problematisch, weil mit den Sicherheits-Updates die Lücken gleich mitgeliefert werden: Über spezielle Tools lassen sich die Unterschiede zwischen Original und gepatchter Version analysieren. So kann schädliche Software, sogenannte „Malware", zielgerichtet programmiert werden.

Viele Hardware-Anbieter scheuen nach Angaben von Experten den Aufwand, ein bereits ausgeliefertes System nachträglich auf die neuere Version des Basissystems zu aktualisieren. Es lohnt sich also, bereits vor der Anschaffung zu klären, wie schnell der jeweilige Hersteller dir bekannten Lücken durch Updates behebt.

Auch für die Apps sind die jeweiligen Hersteller verantwortlich. Treten Sicherheitslücken auf, zeigt sich die Qualität des Anbieters an der Geschwindigkeit, mit der Schwachstellen behoben werden.

3.6 Einbindung in fremde Netzwerke

Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht. Vermeiden Sie es, sensible Anwendungen wie Online-Banking in nicht vertrauenswürdigen Umgebungen durchzuführen. Bei einigen sozialen Netzwerken oder auch Online-Händlern wird die Verbindung nur über die aktuelle Session abgesichert. Hört ein Angreifer die Verbindung ab, so kann er beim sogenannten Session-Hijacking die Sitzung des Nutzers übernehmen.

Deaktivieren Sie grundsätzlich alle drahtlosen Schnittstellen (z. B. WLAN oder Bluetooth), wenn diese nicht benötigt werden. Nehmen Sie das Pairing von externen Komponenten, die über eine Bluetooth-Schnittstelle verfügen, nur in gesicherter Umgebung vor.

4 Sensibilisierung der Mitarbeiter

Die Sicherheit der mobilen Geräte hängt auch davon ab, wie der Benutzer damit umgeht. Der Schutz der Unternehmensdaten ist für jeden Unternehmer existenziell. Deshalb: Sensibilisieren Sie Ihre Mitarbeiter für die Gefahren.

Die Freiheit, außerhalb des Unternehmens auf Firmendaten zuzugreifen, erhöht die Flexibilität und trägt zur Zufriedenheit Ihrer Mitarbeiter und Ihrer Kunden bei. Sicherlich ist gerade für Ihre innovativen Mitarbeiter die berufliche Nutzung der privaten Geräte ein Motivationsfaktor. Treffen Sie Sicherheitsvorkehrungen, stellen Sie verbindliche Regelungen auf und informieren Sie umfassend und regelmäßig Ihre Mitarbeiter.

Weitere Informationen:
Wie bewege ich mich sicher im mobilen Netz?:
http://www.bsi-fuer-buerger.de/Handy

Mobile Sicherheit:
https://www.bsi.bund.de | Themen | Mobile Security

Herausgeber:
Deutschland sicher im Netz e. V.
Albrechtstraße 10 a
10117 Berlin
info@sicher-im-netz.de
www.sicher-im-netz.de

2015-04-01