

## Sicherheit bei mobilen Endgeräten

### Smartphones und Tablets im Alltag

Mobile Endgeräte haben sowohl im privaten als auch im geschäftlichen Umfeld eine enorme Verbreitung erreicht. Immer mehr Beschäftigte nutzen ein geschäftliches oder auch ein privates Gerät, um auf E-Mails, Software und Daten ihrer Firma zuzugreifen. Die hohe Mobilität und Kommunikationsfähigkeit der Geräte sind geschätzte Eigenschaften, so dass diese nunmehr auch in Produktionsumgebungen eingesetzt werden, um beispielsweise Prozesse zu steuern oder zu visualisieren. Diese Vorzüge sind aber auch potenzielle Nachteile in Bezug auf die IT-Sicherheit. In diesen mobilen Endgeräten steckt ein leistungsfähiger Minicomputer. Deshalb gelten prinzipiell ähnliche Gefährdungen wie bei Arbeitsplatzrechnern, wobei auf Grund des mobilen Einsatzes der Geräte die Gefahr des kompletten Verlustes natürlich höher ist.

### Sicherheitsrisiko

Sensible Unternehmensdaten sind auf mobilen Geräten einem besonders hohen Risiko ausgesetzt. Häufig gehen Geräte verloren, werden gestohlen oder sind über falsch konfigurierte und unsichere Verbindungen angreifbar. So können die Zugänge zu Bank- und E-Mail-Konten, zu Produktionsanlagen, zu geschäftlichen Daten und sozialen Netzwerken schnell in falsche Hände gelangen.

### Vorsorge

Vorsorgliche Schutzmaßnahmen sind daher unerlässlich für die Nutzung der Geräte. Das gilt insbesondere, wenn private Geräte auch geschäftlich genutzt werden.

## 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](http://www.mittelstand-digital.de)

### Impressum

**Text und Redaktion:**  
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](mailto: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:** Denys Prykhodov, Maksim Kabakou, ekostov, zapp2photo – Fotolia.com

Magdeburg, Januar 2019



Betrieb 4.0  
machen!



## Mobile Endgeräte sicher nutzen

### 10 Goldene Regeln aus der Praxis

[www.mittelstand-digital.de](http://www.mittelstand-digital.de)

Mittelstand-Digital

Gefördert durch:  
  
aufgrund eines Beschlusses  
des Deutschen Bundestages

## 10 Goldene Regeln, die wirklich helfen

### Smartphones und Tablets ja, aber sicher!

Die 10 Goldenen Regeln sollen Ihnen helfen, die Mobilität dieser Geräte zu nutzen und dabei sicher im Unternehmen einzusetzen. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Anregungen rund um das Thema Datensicherung und Datensicherheit finden Sie unter

[www.betrieb-machen.de](http://www.betrieb-machen.de)





## Wie sollten Sie mit Apps auf den mobilen Endgeräten umgehen?

### Apps

Erst durch die Nutzung zusätzlicher Anwendungen (Apps) – kleiner, aus dem Internet ladbarer Programme – werden Smartphones und Tablets zu Alleskönnern. Doch Vorsicht: Zahlreiche Apps geben persönliche Daten z. B. aus dem Adressbuch über das Internet weiter, wenn bei der Installation die Einstellungen nicht richtig gewählt wurden. Eine Kontrolle durch den Nutzer ist dann schwer möglich. Apps können darüber hinaus auch Viren oder Trojaner enthalten, die Ihre Daten ausspähen oder schädigen können.

- + Regel 1: Apps nur aus sicheren Quellen laden**  
Vor einer Installation muss also gut überlegt werden, ob eine App tatsächlich notwendig ist und ob diese aus einer vertrauenswürdigen Quelle stammt. Dazu kann im Internet nach Bewertungen bzw. Testberichten gesucht werden.

## Wie können Sie Ihre Daten auf mobilen Endgeräten schützen?

### Zugriffskontrolle

Smartphones und Tablets gehen schnell verloren oder sind zeitweise unbeaufsichtigt. Aus diesen Gründen ist ein funktionierender Zugangsschutz mittels einer PIN, eines Passwortes oder einer biometrischen Lösung z. B. Fingerabdruck sinnvoll, um einen unbefugten Zugriff auf das Gerät bzw. auf die Daten, E-Mails, Adressen usw. zu verhindern. Es sollte jeweils eine PIN für die SIM-Karte, für das Gerät selbst und z. B. für eine Datensynchronisation vergeben werden. Eingeschaltete Bluetooth- und WLAN-Verbindungen sind ebenso mögliche Einfallstüren für einen unbefugten Zugriff.

- + Regel 2: Konfiguration**  
Mobile Endgeräte für geschäftliche Zwecke sollten deshalb von einem fachlich kompetenten Verantwortlichen, z. B. dem Administrator, für den sicheren Zugriff auf die E-Mails oder virtuelle Netzwerke (VPN) eingerichtet werden. Im Unternehmen sollten für die Nutzung privater Geräte gemeinsam mit den Mitarbeitern entsprechende Regeln definiert werden.

- + Regel 3: Gutes Passwort**  
Wird beim Zugangsschutz ein Passwort verwendet, muss in jedem Fall ein sicheres Passwort verwendet werden. Je länger und je kryptischer das Passwort (guter Mix aus kleinen und großen Buchstaben, Ziffern, Sonderzeichen), desto sicherer ist es. Siehe auch den Flyer: „**Sichere Passwörter**“

- + Regel 4: Schnittstellen Bluetooth und WLAN**  
Bluetooth- und WLAN-Verbindungen immer erst dann einschalten, wenn sie tatsächlich benötigt werden. Das dient nicht nur der allgemeinen Sicherheit, sondern schont auch den Akku. Sollte die Bluetooth-Verbindung z. B. für Freisprecheinrichtungen oft benötigt werden, kann der Modus „unsichtbar“ gewählt werden.

### Datenverschlüsselung

Werden separate Speicherkarten für eine zusätzliche Datenspeicherung eingesetzt, ist es sinnvoll, diese Daten verschlüsselt zu speichern, wie z. B. mit der App EDS Lite von sovworks ([www.sovworks.com](http://www.sovworks.com)) für Android-Geräte. So verschlüsselte Ordner sind mit dem Format von TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org)) kompatibel. Unbefugten wird so der Zugriff auf die Daten verwehrt oder zumindest erschwert.

- + Regel 5: Verschlüsselung aktivieren**  
Viele Geräte erlauben mit integrierten Funktionen eine entsprechende Einstellung die Verschlüsselung aller Nutzungsdaten.
- + Regel 6: Software-Lösung**  
Bietet ein Smartphone oder ein Tablet selbst die Einstellung der Verschlüsselung nicht, kann die Verschlüsselung über eine zusätzliche Software erfolgen.

- + Regel 7: Security Services**  
Beim Einsatz betrieblicher Geräte fragen Sie Ihren Netzbetreiber, ob ein Angebot über Security Services für E-Mail und Netzzugriff wahrgenommen werden kann.

### Schutz vor Viren und Trojanern

Sowohl durch die E-Mail-Kommunikation als auch durch den Aufruf von Internetseiten besteht wie bei PCs und Notebooks die Gefahr, dass ein Smartphone oder ein Tablet durch Schadware befallen wird.

- + Regel 8: Schutzsoftware**  
Zur Abwehr dieser Gefahren sollte immer ein entsprechendes Schutzprogramm installiert und dann aktuell gehalten werden. Empfehlenswert sind auch hier Testberichte oder der Rat von Experten. Einen guten Überblick sowie zahlreiche Testberichte findet man auf den Seiten der AV-Test GmbH ([www.av-test.org](http://www.av-test.org)).

- + Regel 9: Aktualität**  
In diesem Zusammenhang muss ebenfalls darauf geachtet werden, dass die jeweils zur Verfügung stehenden Updates für die auf den Geräten installierte Software eingespielt werden. Diese Aktualisierungen bringen nicht nur Verbesserungen an der Software, sondern schließen bekannt gewordene Sicherheitslücken.

### Verlust des Smartphones oder Tablets



In Bezug auf Datenverlust bzw. -missbrauch gibt es auch dann Lösungsansätze, wenn ein mobiles Gerät vermisst wird. Die erste vorbeugende Maßnahme ist, das Gerät mit einem guten Zugangsschutz zu sichern, welches das Display nach kurzer Zeit einer Inaktivität verriegelt.

Die Freischaltung durch Passwort oder biometrische Informationen lässt sich zwar mit einem Hardware-Reset umgehen, aber die Daten werden dabei ebenfalls gelöscht. Außerdem muss danach die eingeseetzte SIM-Karte durch eine PIN wieder aktiviert werden. Diese sollte nur dem Besitzer bekannt sein.

- + Regel 10: Fernzugriff**  
Sicherheitstools bieten die Möglichkeit, dass der rechtmäßige Besitzer aus der Ferne Daten kopiert, löscht oder den Standort des Smartphones oder Tablets ausfindig macht. Die meisten Anbieter mobiler Endgeräte und fast alle Sicherheitspakete bieten solche Funktionen an. Voraussetzung ist natürlich die Freischaltung bzw. Installation vor einem Verlust des Gerätes. Die Nutzer eines Apple-Gerätes müssen dazu unter [www.icloud.com](http://www.icloud.com) die Option entsprechend einrichten. Besitzer von Geräten mit einem anderen Betriebssystem nutzen ein vergleichbares Sicherheitspaket. Dabei gibt es für Android-Geräte mit dem Tool „Plan B“ von Lookout (<https://www.lookout.com/de>) sogar eine Lösung, die selbst nach einem Verlust auf das Gerät aus der Ferne installiert werden kann, um dann die erwähnten Funktionen zu nutzen.

Smartphones sind leistungsfähige Minicomputer mit einem ähnlich hohen Gefährdungspotential wie Notebooks und PCs.



Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter: [www.betrieb-machen.de](http://www.betrieb-machen.de)