Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

Einsatz mobiler Endgeräte – 10 Tipps für eine sichere Nutzung

ROLAND HALLAU

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

Smartphones, Tablets u. a. mobile Endgeräte sind leistungsstarke Mini-Computer und 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, sodass diese nunmehr auch in Produktionsumgebungen eingesetzt werden, um z. B. Prozesse zu steuern oder zu visualisieren. Mit Blick auf die IT-Sicherheit bieten diese Vorzüge aber auch potenzielle Nachteile. Aufgrund der Leistungsfähigkeit der Geräte sind die Bedrohungen mit denen eines Arbeitsplatzrechners vergleichbar, jedoch ist die Gefahr des kompletten Verlustes durch den mobilen Einsatz der Geräte natürlich höher.

In diesem Nachgelesen erfahren Sie:

- wie Sie mit Apps auf mobilen Endgeräten umgehen sollten,
- wie Sie Ihr mobiles Endgerät vor unbefugten Zugriffen schützen können,
- wie Sie Ihre Daten schützen können,
- wie Sie Ihr mobiles Endgerät vor Schadsoftware schützen können und
- wie Sie auf den Verlust Ihres Smartphones oder Tablet reagieren können.

Impressum

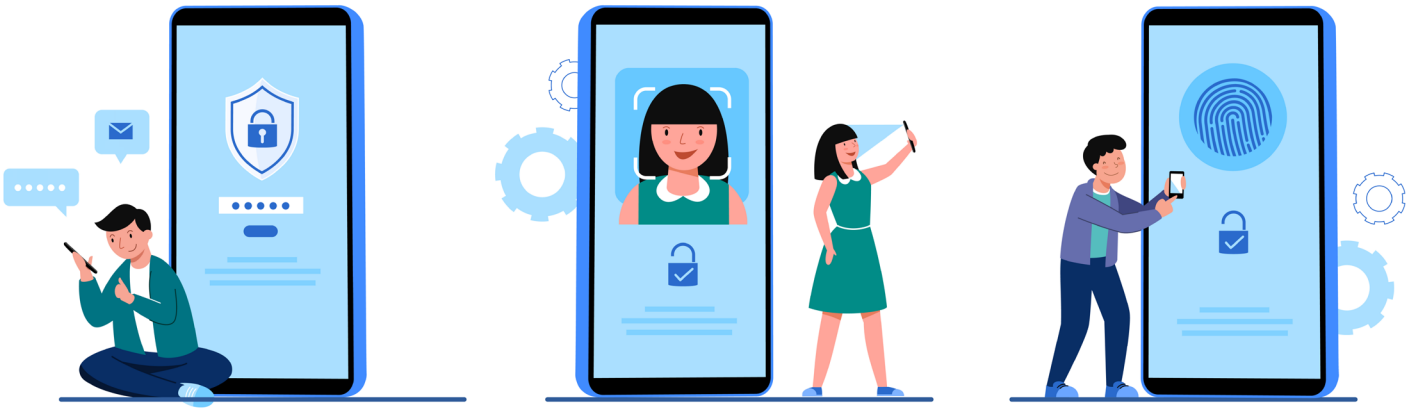
HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Bianca Eichler

GESTALTUNG UND PRODUKTION
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL rawpixel.com - Freepik.com

VERÖFFENTLICHUNG Januar 2025



Vorsorglichen Schutzmaßnahmen können unbefugte Zugriffe auf persönliche Daten abwehren © jcomp - Freepik.com

Einsatz mobiler Endgeräte – 10 Tipps für eine sichere Nutzung

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.

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

Wie sollten Sie mit Apps auf den mobilen Endgeräten umgehen?

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 Nutzenden ist dann schwer möglich. Apps können darüber hinaus auch Viren oder Trojaner enthalten, die Ihre Daten ausspähen oder schädigen können.

TIPP 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 sollte im Internet nach Bewertungen bzw. Testberichten gesucht werden. In einem Unternehmen sollten die Auswahl und Installation von Apps durch Verantwortliche klar geregelt und umgesetzt werden.

Apps bieten großes Gefahrenpotenzial für private Daten © Freepik - Freepik.com

Wie können Sie Ihr mobiles Endgerät vor unbefugten Zugriffen schützen?

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 wie ein Fingerabdruck empfehlenswert, 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.

TIPP 2: KONFIGURATION MIT FOKUS AUF IT-SICHERHEIT

Mobile Endgeräte für geschäftliche Zwecke sollten 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 Mitarbeitenden entsprechende Regeln definiert werden.

TIPP 3: GUTES PASSWORT ODER NUTZUNG BIOMETRISCHER FUNKTIONEN

Wird beim Zugangsschutz ein Passwort verwendet, muss in jedem Fall ein sicheres Passwort verwendet werden. Je länger und je kryptischer das Passwort, desto sicherer ist es. Hier empfiehlt sich ein guter Mix aus kleinen und großen Buchstaben, Ziffern und Sonderzeichen. Weitere Tipps und Informationen können Sie in unserem Beitrag zu Authentifizierung: Schutz durch sichere Passwörter und erweiterte Sicherheitsmaßnahmen nachlesen.

TIPP 4: SCHNITTSTELLEN BLUETOOTH UND WLAN

Bluetooth- und WLAN-Verbindungen sollten immer erst dann eingeschaltet werden, wenn Sie diese tatsächlich benötigen. 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.

Wie können Sie Ihre Daten auf mobilen Endgeräten schützen?

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) für Android-Geräte. So verschlüsselte Ordner sind mit dem Format von VeraCrypt (www.veracrypt.de) kompatibel. Unbefugten wird so der Zugriff auf die Daten verwehrt.

TIPP 5: VERSCHLÜSSELUNG AKTIVIEREN

Viele Geräte erlauben mit integrierten Funktionen eine entsprechende Einstellung zur Verschlüsselung von Nutzungsdaten.

TIPP 6: EINSATZ VON TOOLS ZUR VERSCHLÜSSELUNG

Bietet ein Smartphone oder ein Tablet selbst die Einstellung der Verschlüsselung nicht, kann die Verschlüsselung über eine zusätzliche Software erfolgen.

Auch bei Tablets empfiehlt sich ein Passwortschutz © rawpixel.com - Freepik.com

TIPP 9: AKTUALITÄT

In diesem Zusammenhang muss ebenfalls darauf geachtet werden, dass die jeweils zur Verfügung stehenden Updates sowohl für die auf den Geräten installierte Software als auch für das jeweilige Betriebssystem eingespielt werden. Diese Aktualisierungen bringen nicht nur Verbesserungen der Software, sondern schließen zumeist bekannt gewordene Sicherheitslücken.

TIPP 7: NUTZUNG ZUSÄTZLICHER DIENSTE

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

Wie können Sie sich vor Schadsoftware (Malware) schützen?

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.

TIPP 8: EINSATZ VON SCHUTZSOFTWARE

Zur Abwehr der Gefahr durch Malware sollte immer ein entsprechendes Schutzprogramm installiert und dann aktuell gehalten werden. Empfehlenswert sind auch hier Testberichte oder der Rat von Sachverständigen. Einen guten Überblick sowie zahlreiche Testberichte findet man auf den Seiten der AV-Test GmbH (www.av-test.org).

Wie können Sie auf den Verlust des Smartphones oder Tablets reagieren?

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 eingesetzte SIM-Karte durch eine PIN wieder aktiviert werden. Diese sollte nur dem Besitzer bekannt sein.

TIPP 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 die Freischaltung bzw. Installation vor dem Verlust des Gerätes. Wenn Sie ein Apple-Gerät besitzen, können Sie unter www.icloud.com die Option entsprechend einrichten. Bei anderen Betriebssystemen können Sie ein vergleichbares Sicherheitspaket verwenden.

Links mit weiterführenden Inhalten

HINWEISE UND VERGLEICH VON ZUGRIFFSSCHUTZ

- Smartphone und Tablet effektiv schützen:
  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html

- Sichere Nutzung von Smartphones und Tablets:
  https://www.vis.bayern.de/digitale_welt/weg_ins_netz/mobilesinternet_checkliste.htm

- Handy sicher entsperren – Die besten Methoden für sichere Display-Sperre und zuverlässigen Zugriffsschutz beim Smartphone: https://www.datenwache.de/handy-sicher-entsperren-displaysperre-zugriffsschutz/

- Handysicherheit – Die ultimative Checkliste:
  https://www.sparhandy.de/info/ratgeber/handy-sicherheit?srsltid=AfmBOopzwqRax0mj09O0nE9VkEp5XA9B-fpONwuZ7FujJz9Ica3pum9Jz

PASSWÖRTER

- Authentifizierung – Schutz durch sichere Passwörter und erweiterte Sicherheitsmaßnahmen:
  https://digitalzentrum-chemnitz.de/wissen/authentifizierung-schutz-durch-sichere-passwoerter-und-erweiterte-sicherheitsmassnahmen/

VERSCHLÜSSELUNG

- Verschlüsselung auf mobilen Geräten:
  https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/Verschluesselung-auf-mobilen-Geraeten/verschluesselung-auf-mobilen-geraeten_node.html

MOBILE GERÄTE ORTEN

- Handy verloren oder gestohlen – Sperren lassen, Anzeige erstatten:
  https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/handy-verloren-oder-gestohlen-sperren-lassen-anzeige-erstatten-13870

- Handys und verlorene Geräte orten per App – Die besten Tools und Anwendungen:
  https://www.netzwelt.de/sicherheit/handy-spionage/downloads/verlorene-geraete-orten.html

- Handy weg? Das ist jetzt zu tun:
  https://www.zdf.de/nachrichten/ratgeber/handy-verloren-was-tun-100.html

- Smartphone verloren – das können Sie tun:
  https://www.connect.de/ratgeber/handy-verloren-smartphone-orten-daten-loeschen-sim-sperren-tipps-2489281.html

Autoren

ROLAND HALLAU Roland Hallau ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er als Fachkoordinator im Bereich IT-Sicherheit tätig.
roland.hallau@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?
Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages