Smartphones: mobil, flexibel und unsicher?

Smartphones erobern die Unternehmen. Immer mehr Beschäftigte nutzen ihr geschäftliches, aber auch privates Smartphone, um auf E-Mails, Software und Datenbanken ihrer Firma zuzugreifen. Die hohe Mobilität und Kommunikationsfähigkeit der Geräte sind geschätzte Eigenschaften – können jedoch auch gravierende Nachteile haben.

Smartphones sind schließlich mehr als nur ein Mobiltelefon: In ihnen steckt ein höchst leistungsfähiger Minicomputer. Deshalb gelten prinzipiell ähnliche Gefährdungen aber auch Vorbeugemaßnahmen wie z.B. bei Notebooks oder PCs.

Hohes Sicherheitsrisiko

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

Vorsorgen schützt

Vorsorgliche Schutzmaßnahmen sind daher unerlässlich für die Nutzung der Geräte. Insbesondere wenn Sie private Smartphones geschäftlich nutzen, sollten Sie betont achtsam sein.

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteiischer Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Netzwerk Elektronischer Geschäftsverkehr

www.ec-net.de

Praxistipps

Aus der Praxis für die Praxis

Smartphones sicher nutzen

10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Netzwerk Elektronischer Geschäftsverkehr

TeleTrusT

TeleTrusT Deutschland e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische“ rund um das Thema Informationssicherheit.

TeleTrusT ist mit mehr als 100 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.

TeleTrusT
Pioneers in IT security.

Impressum

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business-Lösungen.

Herausgeber:
TeleTrusT Deutschland e.V., Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:
Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:
Karl-Heinz Kottenhahn

Druck:
Buersche Druckerei Neufang KG

Bildnachweis:
Scanrail/fotolia.de, Inga F/fotolia.de, pressmaster/fotolia.de

Stand: 04/2011

10 Tipps, die wirklich helfen

Smartphones sicher im Unternehmen einsetzen

10 grundlegende Praxistipps helfen Ihnen, die Mobilität von Smartphones zu nutzen und die Geräte dabei sicher im Unternehmen einzusetzen.

Die Tipps stammen alle aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema Datensicherung und Datensicherheit finden Sie unter www.ec-net.de.

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

Wie sollten Sie mit Apps auf Ihrem Smartphone umgehen?

Apps

Erst durch die Nutzung zusätzlicher Anwendungen (Apps) – kleiner, herunterladbarer Programme – werden Smartphones zu Alleskönnern. Doch Vorsicht: Zahlreiche Apps geben persönliche Daten z.B. aus dem Adressbuch des Smartphones über das Internet weiter – ohne den Nutzer zu fragen. Eine Kontrolle durch den Nutzer ist dann nicht mehr möglich. Apps können auch Viren oder Trojaner enthalten, die Ihre Daten ausspähen oder schädigen können.

Tipp 1: Apps nur aus sicheren Quellen
Überlegen Sie sich vor dem Installieren, ob Sie die Apps auch wirklich benötigen. Auf jeden Fall sollten Sie Apps nur aus vertrauenswürdigen Quellen beziehen. Vergleichen Sie Testberichte z.B. im Internet und achten Sie ggf. auf Zertifikate oder Vergleichbares.

Wie können Sie Ihre Daten auf dem Smartphone schützen?

Zugriffskontrolle

Smartphones gehen schnell verloren oder bleiben unbeaufsichtigt im Büro liegen. Umso wichtiger ist ein funktionierender Zugangsschutz (PIN und/oder Passwort), um einen unbefugten Zugriff auf Ihre Daten, Mails, Adressen oder Telefonnummern zu verhindern. Vergeben Sie je eine PIN für die SIM-Karte, für das Gerät selber und z.B. für das Synchronisieren. In eingeschaltetem Zustand sind auch Bluetooth und WLAN mögliche Einfallstüren für Unbefugte. Verschlüsseln Sie die eingelegten Speicherkarten, falls darauf sensible Daten gespeichert sind.

Tipp 2: Konfiguration
Alle betrieblichen Smartphones sollten von einem Verantwortlichen (z.B. dem Administrator oder einem externen Experten) für den sicheren Zugriff auf E-Mail oder virtuelle Netzwerke (VPNs) konfiguriert werden. Definieren Sie Regeln für die Nutzung privater Smartphones und sprechen Sie diese mit den Mitarbeitern ab. Am Besten verwenden Sie ein separates Smartphone nur für die geschäftliche Nutzung.

Tipp 3: Gutes Passwort
Wählen Sie ein sicheres Passwort. Je länger und je kryptischer das Passwort (auch Sonderzeichen verwenden!), desto sicherer. Denn: kurze und einfach zu erratende Passwörter können erschreckend leicht ausgehebelt werden.

Tipp 4: Schnittstellen: Bluetooth und WLAN
Schalten Sie die Funktion erst dann ein, wenn Sie sie wirklich benötigen. Das dient der Sicherheit und schont den Akku. Falls Sie Bluetooth oft benötigen, z.B. für Freisprecheinrichtungen, schalten Sie auf den Modus „unsichtbar“.

Datenverschlüsselung

Verschlüsseln Sie Ihre persönlichen Daten, auch die, die sich auf der eingelegten Speicherkarte befinden. Für Unbefugte wird es dadurch wesentlich schwieriger, auf Ihre Daten zuzugreifen.

Tipp 5: Verschlüsselung aktivieren
Die umfassende Verschlüsselung aller Nutzerdaten können Sie bei einigen Geräten einstellen.

Tipp 6: Security Services
Beim Einsatz betrieblicher Smartphones sollten Sie den Netzbetreiber fragen, ob er Security Services für E-Mail bzw. Netzzugriff anbietet.

Tipp 7: Stand-alone-Software
Falls Sie ein privates Smartphone nutzen, das Datenverschlüsselung nicht unterstützt, verwenden Sie eine zusätzliche Software-Lösung.

Schutz vor Viren und Trojanern

Ähnlich wie PCs und Notebooks werden auch Smartphones immer häufiger mit Viren und Trojanern angegriffen, die Ihre Daten gefährden.

Tipp 8: Schutzsoftware
Zur Abwehr von Schadsoftware sollten Sie ein Schutzprogramm installieren und immer aktuell halten. Hier sollten Sie zumindest Testberichte oder besser einen Experten zu Rate ziehen.

Tipp 9: Aktualisierung
Installieren Sie die von den Herstellern bereitgestellten aktuellen Software-Updates, da diese auch zwischenzeitlich entdeckte oder neu entstandene Sicherheitslücken schließen.

Was tun, wenn Sie Ihr Smartphone verlieren?

Datenlöschung

Wurde Ihr Smartphone gestohlen oder haben Sie es verloren – auch dann gibt es oft eine Sicherheitslösung: Die gespeicherten Daten lassen sich auch aus der Ferne löschen, z.B. durch Server-Synchronisierung oder die dreimalige falsche Eingabe des Passworts.

Tipp 10: Fernlöschung
Nutzen Sie ggf. eine Lösung (Software/Service), mit deren Hilfe verlorengegangene oder gestohlene Endgeräte aufgespürt und bei Bedarf außer Betrieb gesetzt werden können. Lassen Sie sich hierbei unbedingt von einem Fachmann beraten.