Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Fachhochschule Gelsenkirchen

Mitglied im:

Netzwerk Elektronischer Geschäftsverkehr

Sicherheit bei mobilen Geräten

Die Zeiten in denen das Handy nur zum Telefonieren und SMS-Schreiben verwendet wurde sind vorbei. Moderne Smartphones bieten neben den klassischen PDA-Funktionen wie Adressbuch und Kalender heutzutage auch die Möglichkeit von unterwegs bequem auf E-Mails und das Internet zuzugreifen oder via Navigationssoftware schnell und einfach zum neuen Kunden zu finden. Mit zahlreichen Zusatzprogrammen, die meist kostenfrei im Internet heruntergeladen werden können, lässt sich der Funktionsumfang nahezu beliebig erweitern. Viele Möglichkeiten also – auch für Kriminelle!

Achten Sie auf einen angemessenen Basisschutz!

Auch bei den Smartphones wird Schadsoftware (Viren, Würmer und Trojaner) zu einer immer größeren Bedrohung. Daher sollte jedes internetfähige Handy mit einem Basisschutz ausgestattet sein, um die Sicherheit des Geräts und der darauf gespeicherten Daten zu gewährleisten. Ihr Smartphone sollte stets über ein aktuelles Virenschutzprogramm und eine Personal Firewall verfügen. Halten Sie die Firewall und das Anti-Virenprogramm aber auch das Betriebssystem Ihres Smartphones und sämtliche installierte Software mit Sicherheitsupdates immer auf dem neuesten Stand, um Sicherheitslücken zu schließen. Lassen Sie Ihr Handy nie unbeaufsichtigt und verleihen Sie es nicht. In nur wenigen Minuten könnte ein Angreifer Schadsoftware darauf installieren, die unbemerkt im Hintergrund abläuft.

Nutzen Sie die Sicherheitseinstellungen Ihres Smartphones!

Schalten Sie die vom Werk integrierten Sicherheitseinstellungen für das Smartphone nicht aus! Gerade wenn Sie Ihr Handy verlieren oder es Ihnen gestohlen wird, kann die Kennwortabfrage (beim Einschalten und bei der Wiederbenutzung) Ihre Daten zumindest eine Zeit lang vor dem Zugriff durch Dritte schützen. Einige Smartphones bieten für solche Fälle zudem die Möglichkeit, persönliche Daten auch aus der Ferne zu löschen oder übernehmen dies selbstständig, wenn das Passwort mehrfach falsch eingegeben wurde. Auch automatische Software-Updates sollten keinesfalls deaktiviert werden, da Sie beim Erscheinen von Sicherheitsupdates garantieren, dass diese auch unmittelbar eingespielt werden.

Aktivieren Sie drahtlose Schnittstellen nur bei Bedarf!

Mit drahtlosen Schnittstellen können Daten schnell und bequem zwischen verschiedenen Geräten übertragen werden. WLAN, Bluetooth und Infrarot sind aber auch ein zusätzliches Einfallstor für Kriminelle und können zum Beispiel dazu missbraucht werden, um unerwünschte Programme auf Ihrem Telefon zu installieren oder unbemerkt Daten auszulesen. Schalten Sie drahtlose Schnittstellen nur ein, wenn Sie sie auch tatsächlich benötigen. Achten Sie außerdem darauf, dass Ihre WLAN-Verbindung, ausreichend verschlüsselt ist. Heute (Stand Dezember 2010) sollte ausschließlich der Verschlüsselungsstandard WPA oder besser WPA-2 verwendet werden. Ältere Verschlüsselungsstandards wie WEP sind unsicher und können schnell entschlüsselt werden. Nutzen Sie Bluetooth, sollten Sie darauf achten, dass Sie Ihre Benutzerkennung nicht permanent senden. Andernfalls könnte ein potentieller Angreifer sich mit Ihrem Gerät verbinden und Ihre Daten auslesen, sobald Sie dies quittieren. Das kann schnell ungewollt oder unwissend passieren. Darüber hinaus sollte Ihre Benutzerkennung nicht Ihrem Gerätenamen entsprechen. Ansonsten kann sich einem Angreifer helfen, gezielt Sicherheitslücken zu dem Typ Ihres Mobiltelefons zu nutzen.

Installieren Sie Programme nur aus sicherer Quelle!

Generell gilt: Das Installieren sogenannter Apps kann unter Sicherheitsaspekten grundsätzlich problematisch sein, denn sie können Sicherheitsfunktionen deaktivieren oder Daten erfassen, die für die spezielle Anwendung nicht notwendig sind. Überlegen Sie sich im Vorfeld gut, ob Sie eine Applikation wirklich brauchen und installieren Sie lieber zu wenige als zu viele Programme. Achten Sie insbesondere darauf, Apps nur aus vertrauenswürdiger Quelle zu installieren. Wenn Sie sich unsicher sind, können Sie über eine Suchmaschine Erfahrungsberichte anderer Nutzer und deren Beurteilung heranziehen.

Verschlüsseln Sie sensible Daten!

Gerade wenn das Smartphone nicht nur privat, sondern auch geschäftlich genutzt wird, müssen besondere Vorkehrungen getroffen werden, um sensible Daten im Falle eines Verlusts oder Diebstahls zu schützen. Kontaktdaten von Geschäftspartnern, Korrespondenz per E-Mail und SMS oder gar Passwörter zum Unternehmensnetzwerk

sollten daher stets mittels einer speziellen Verschlüsselungssoftware verschlüsselt abgespeichert werden. Mit einer Verschlüsselung sind Ihre Daten vor fremdem Zugriff geschützt. Jeder, der versucht sich ohne Kenntnis des Passworts Zugang zu verschaffen, findet nur unbrauchbaren Datenmüll, selbst wenn er die Speicherkarte herausnimmt. Wichtig hierbei ist, dass Sie ein starkes Passwort definieren. Ein starkes Passwort ist auf den ersten Blick sinnfrei zusammengesetzt, steht in keinem Wörterbuch und besteht aus mindestens zehn Zeichen. Ideal ist eine Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Weitere Informationen finden Sie in dem vom Netzwerk Elektronischer Geschäftsverkehr erschienenen IT-Sicherheitstipp „Wie erstelle ich ein sicheres Passwort?“.

- **Machen Sie regelmäßig Sicherungskopien!**

Haben Sie durch Verlust oder Diebstahl keinen Zugriff mehr auf Ihre gespeicherten Daten, ist dies häufig schwerwiegender als der materielle Schaden. Abhilfe schafft eine regelmäßige Synchronisation der auf dem Smartphone gespeicherten Daten mit Ihrem PC. Einige Anbieter stellen solch eine Backup-Software mittlerweile kostenfrei zum Download im Internet bereit. Je häufiger Sie das „Sicherheitsarchiv“ auf Ihrem Computer auf den aktuellen Stand bringen, desto hilfreicher wird es Ihnen sein, wenn sie es einmal tatsächlich brauchen.

Autoren:
Dipl.-Inform.(FH) Sebastian Spooren
Dustin Pawlitzek
Prof. Dr. (TU NN) Norbert Pohlmann

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit – if(is)

Weiterführende Informationen:
http://www.ec-net.de
https://www.it-sicherheit.de
http://www.bsi.bund.de

Bildquelle: Ivelin Ivanov - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr
Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 29 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 als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk" etabliert. Das Netzwerk ist das einzige bundesweite Angebot seiner Art und verzeichnet jährlich rund 30.000 Besucher in Beratungen und Veranstaltungen. Es stellt 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.

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)
Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Sichere E-Geschäftsprozesse in KMU und Handwerk
Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk" des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.ec-net.de/sicherheit