Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages
Fachhochschule Gelsenkirchen
Mitglied im:
Netzwerk Elektronischer Geschäftsverkehr

Mit Notebook und Handy sicher in den Urlaub

Geschäftliche E-Mails und Telefonate direkt von der Hotel-Terrasse aus, oder einfach nur Fotos von Land und Leuten an die Daheimgebliebenen schicken: Auch im Urlaub gewinnt die Kommunikation via Notebook und Handy für immer mehr Menschen an Bedeutung. Doch Vorsicht: Auch Kriminelle haben in den schönsten Tagen des Jahres Hochsaison. Trotz aller Vorfreude sollten Sicherheitsbedenken deshalb nicht leichtfertig beiseite geschoben werden. Wer sich gut vorbereitet und einige Grundregeln beachtet, kann in den schönsten Wochen des Jahres folgenlos entspannen.

Treffen Sie bereits vor der Abreise notwendige Sicherheitsvorkehrungen!

Bringen Sie Ihr Notebook kurz vor Reisebeginn auf den neuesten Stand. Installieren Sie dazu alle verfügbaren Sicherheitsupdates für Ihr Betriebssystem und sämtliche Anwendungsprogramme (z.B. Mozilla Firefox). Auch das Antivirenschutzprogramm sollte aktuell sein und Ihre Festplatte vor Reisebeginn auf Schadsoftware untersucht werden. Richten Sie Passwörter für alle Benutzerkonten Ihres Notebooks ein, um Unbefugten den Zugriff auf Ihre Daten zu erschweren. Zusätzlich empfiehlt es sich für sensible Daten eine lokale Verschlüsselung einzurichten. Bevor Sie Ihr Notebook mit auf Reisen nehmen, sollten Sie für den Fall eines Diebstahls oder Defekts zumindest die sensiblen und wichtigen Daten sichern. Dazu eignen sich externe Speichermedien wie DVDs, USB-Sticks oder externe Festplatten. Müssen Sie mit Ihrem Notebook über ein fremdes WLAN auf Ihr Unternehmensnetzwerk zugreifen, sollte die Kommunikation immer verschlüsselt (zum Beispiel über ein so genanntes VPN) ablaufen. Sprechen Sie dazu am besten mit Ihrem IT-Berater.

Vorsicht an fremden Rechnern!

Wenn Sie statt Ihres eigenen Rechners einen öffentlichen PC benutzen (zum Beispiel im Internetcafé), ist besondere Vorsicht geboten. Denn in punkto Sicherheit sind viele Rechner noch immer schlecht gepflegt. Informieren Sie sich deshalb vorab beim Betreiber über die jeweiligen Sicherheitsstandards. Besonders wichtig: eine Firewall, ein aktuelles Virenschutzprogramm und regelmäßige Updates für sämtliche installierte Software und das Betriebssystem. Sicherheitskritische Anwendungen (z.B. Online-Banking), sollten Sie keinesfalls an einem öffentlichen PC benutzen. Zu groß ist die Gefahr, dass Kriminelle mittels Spionagesoftware, so genannte Spyware, an Ihre Zugangsdaten gelangen. Vernichten Sie nach der Benutzung Ihre digitalen Spuren: Löschen Sie die temporären Dateien des Browsers, die Browserhistorie und die Cookies. Im Internet Explorer finden Sie die Möglichkeit in der Navigationsleiste unter: Extras → Internetoptionen → Allgemein. Beim Mozilla Firefox hingegen unter: Extras → Neueste Chronik löschen.

Verwenden Sie Hotspots mit Vorsicht!

Wer sich entschieden hat, sein Notebook oder Smartphone mit in den Urlaub zu nehmen, kann mittlerweile an vielen Orten - wie Flughäfen, Restaurants aber auch im Hotel - auf öffentliche Netzwerke, sogenannte „Hotspots“, zurückgreifen. Gerade hier ist Vorsicht geboten, denn bei einigen dieser Netzwerke kommt keine oder nur eine schwache Verschlüsselung zum Einsatz. Für Hacker ist es dann ein Leichtes, die von Ihnen übermittelten Daten abzufangen (z.B. E-Mails, Benutzerdaten) und für Ihre Zwecke zu missbrauchen. Wenn Sie sich mit einem HotSpot verbinden, achten Sie darauf, dass die angebotene Verschlüsselung des Funknetzwerkes mindestens WPA, besser WPA II entspricht. Überprüfen Sie, ob sich Ihr Virenschutz und Ihre Personal Firewall auf dem neuestem Stand befinden. In öffentlichen Netzwerken ist es empfehlenswert, sich nicht als Benutzer mit Administratorrechten anzumelden, um Kriminellen im Falle eines erfolgreichen Angriffs nicht sämtliche Rechte einzuräumen. Legen Sie stattdessen lieber einen Nutzeraccount mit deutlich eingeschränkten Rechten an, den Sie dann für das Surfen über öffentliche Netze benutzen können.

Schützen Sie Ihr Handy!

Wenn Sie ein Handy mit drahtlosen Schnittstellen wie Bluetooth, WLAN oder Infrarot besitzen, sollten Sie die Übertragungsfunktionen bei Nichtgebrauch deaktivieren. Das trägt dazu bei, dass im Falle einer Sicherheitslücke Ihres Mobiltelefons niemand unbemerkt gefährliche Inhalte, wie Viren oder Würmer, auf Ihr Mobilfunktelefon übertragen kann. Verlieren Sie Ihr Handy oder wird es sogar geklaut, ist das sehr ärgerlich. Der eigentliche Wert des Mobiltelefons gerät dabei jedoch schnell in den Hintergrund, wenn nicht mehr auf Telefonnummern und Kalendereinträge zurückgegriffen werden kann. Deshalb empfiehlt es sich vor der Abreise eine Datensicherung Ihrer Telefon- und Kalendereinträge zu erstellen, damit diese bei Verlust des Gerätes wieder herstellbar sind. Bei den meisten Mobiltelefonen liegt die dafür notwendige Software der Verpackung bei. Notieren Sie sich zudem die Seriennummer Ihres Handys. Diese können Sie mit der Tastenkombination *#06# abfragen. Im Falle eines Diebstahls ist sie für eine Anzeige hilfreich, wenn das Gerät später wiedergefunden wird.

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: Robert Taylor - Fotolia.com

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 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 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