

Sicherheitstipps für Ihr Notebook

Immer mehr Menschen packen bei Dienstreisen Ihr Notebook mit ein. Das ist praktisch und ermöglicht auch während der Reise für viele einen fast uneingeschränkten Arbeitsalltag! So können E-Mails in Echtzeit abgerufen, Präsentationen überarbeitet oder Berichte gegengelesen werden. Viele der auf dem Notebook gespeicherten Daten sind jedoch zumeist sensibel und dürfen keinesfalls an die Öffentlichkeit gelangen. Doch sind die Daten ausreichend vor dem Zugriff durch Dritte geschützt? Immer häufiger kommt es zum Diebstahl von Daten oder dem ganzen Gerät. Mit diesen Tipps aus dem Netzwerk Elektronischer Geschäftsverkehr schützen Sie Ihr Notebook vor Risiken.



► Erstellen Sie ein Systemkennwort!

Richten Sie als erste Hürde einen Benutzeraccount mit Systemkennwort ein, um Unbefugten den Zugang zu Ihren Daten zu erschweren (Die Einstellungen dazu finden Sie in der Regel unter: Start » Systemsteuerung » Benutzerkonten). Wählen Sie dafür ein „starkes Passwort“ (sinnfrei zusammengesetzt, mindestens 10 Zeichen, darunter Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen). Ausführliche Informationen zur richtigen Passwortwahl erhalten Sie in unserem bereits veröffentlichten IT-Sicherheitstipp „So erstellen Sie ein sicheres Passwort“ [www.ec-net.de]. Sperren Sie das Gerät mit der Tastenkombination „Windows-Taste + L“, wenn Sie es einen Moment unbeaufsichtigt lassen.



► **Ergänzen Sie den Passwortschutz!**

Einige Hersteller bieten bereits Notebooks mit einem integrierten Fingerabdruck-Scanner und solche Geräte auch zum nachträglichen Einbau an.

Nur wenn der gescannte Fingerabdruck mit dem zuvor gespeichertem Abdruck übereinstimmt, fährt das Betriebssystem hoch oder lädt den Benutzeraccount. Auch ein sogenannter USB-Token erhöht den Schutz. Dieser ist wie ein kleiner USB-Stick und enthält eine individuelle Passwortdatei. Erst mit der Eingabe eines zusätzlichen Passworts des Benutzers wird der Systemzugriff ermöglicht. Diese Verfahren sind jedoch nur dann wirksam, wenn jemand versucht über Ihr installiertes Betriebssystem auf Ihre Inhalte zuzugreifen. Wird die Festplatte nach einem Diebstahl Ihres Notebooks ausgebaut und in einem anderen System montiert, sind zumeist sämtliche Informationen ohne die Eingabe des Passworts oder den Fingerabdruck zugänglich.

► **Verschlüsseln Sie Ihre sensiblen Daten!**

Einen wirklich verlässlichen Schutz Ihrer auf dem Notebook gespeicherten Daten erreichen Sie mit einer sogenannten lokalen Verschlüsselung. Dabei werden bestimmte Bereiche oder sogar die gesamte Festplatte des Notebooks mittels eines Passworts oder einer Schlüsseldatei (z.B. auf einem USB-Stick) verschlüsselt. Im Falle eines Diebstahls kann der Dieb ohne Kenntnis des Passworts nichts mit den gestohlenen Daten anfangen. Die in Windows integrierten Verschlüsselungsprogramme weisen einige Schwächen in der Kompatibilität bei Festplatten auf. Kostenlose Programme wie „True Crypt“ [<http://www.truecrypt.org>] oder „Disk Cryptor“ [<http://diskcryptor.net>] sind benutzerfreundlicher und verwenden zur Verschlüsselung den als derzeit sehr sicher geltenden Verschlüsselungsstandard AES. Dieser wird in den USA sogar für staatliche Dokumente mit höchster Geheimhaltungsstufe verwendet.

► **Halten Sie Ihre Sicherheitsprogramme auf dem neuesten Stand!**

Achten Sie darauf, Ihr Notebook auch vor digitalen Bedrohungen (Viren, Würmern und Trojanern) zu schützen. Ein Virenschutzprogramm und eine Personal Firewall sind neben dem regelmäßigen Einspielen von so genannten Sicherheitsupdates (sowohl bei Anwendungsprogrammen als auch beim Betriebssystem) die Sicherheitsgrundlagen für jeden Computer.

► **Machen Sie regelmäßig Sicherungskopien!**

Lassen Sie Ihr Notebook nie in einem öffentlichen Raum unbeaufsichtigt stehen. Verschießen Sie Ihr Büro beim Verlassen immer, so dass Dritten der Zugang zu Ihren Dokumenten und Daten verwehrt bleibt.

Wird Ihr Notebook trotz Einhaltung aller Schutzmaßnahmen doch geklaut, sind Ihre sensiblen Daten bei einer lokalen Verschlüsselung für Kriminelle wertlos. Ärgern werden Sie sich vermutlich trotzdem. Denn wichtige Dokumente und Informationen sind Ihnen jetzt nicht mehr zugänglich. Abhilfe schaffen regelmäßige Sicherungskopien des gesamten Systems. Externe Festplatten eignen sich aufgrund ihrer großen Speicherkapazität optimal für Datensicherungen. Je häufiger Sie ein Backup durchführen, desto nützlicher wird es Ihnen im Schadensfall sein. Natürlich müssen Notebook und Speichermedium getrennt voneinander aufbewahrt werden. Andernfalls fehlen Ihnen bei einem Diebstahl oder Brand unter Umständen sowohl die Originaldaten als auch die Sicherungskopien.

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>

<http://www.internet-sicherheit.de>

<https://www.it-sicherheit.de/topthema/notebooks/>

<http://www.internet-sicherheit.de/institut/buch-sicher-im->

<internet/videos/screenvideos/video/11/>

<https://www.it-sicherheit.de>

Bildquelle: Sashkin – 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>