Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Fachhochschule Gelsenkirchen

Mitglied im:

Netzwerk Elektronischer Geschäftsverkehr

Sicherer Umgang mit Wechseldatenträgern

Im digitalen Zeitalter sind Wechseldatenträger für Unternehmen und Privatpersonen unverzichtbar geworden. Sie bieten trotz geringer Größe ein Fassungsvermögen, das sich längst im Gigabyte-Bereich bewegt und eignen sich deshalb ideal für Datensicherungen und zum Transport von Daten. Doch die mobilen Datenträger haben nicht nur Vorteile. Schnell sind CD, DVD, USB-Stick und Co. verloren oder geraten durch Diebstahl in die Hände von Kriminellen. Auch ihren Ruf als Virenschleudern tragen externe Speichermedien nicht zu unrecht. Was es zu beachten gibt, um Ihre Daten und Ihr System vor potentiellen Gefahren zu schützen, erfahren Sie in diesem Sicherheitstipp.

Verschlüsseln Sie sensible Informationen!

Wegen Ihres großen Fassungsvermögens sind USB-Sticks beliebt um Daten zu speichern und zu transportieren. Aufgrund der geringen Ausmaße ist aber auch die Gefahr des Liegenlassens oder des Diebstahls besonders groß. Kommt Ihnen der Stick abhanden, geraten die sensiblen Informationen unter Umständen in die falschen Hände und können missbraucht werden. Um in so einem Fall der unautorisierten Nutzung Ihrer Daten vorzubeugen, empfiehlt es sich, USB-Sticks komplett zu verschlüsseln. Einerseits gibt es USB-Sticks die bereits von Werk aus mit speziellen Bauteilen ausgestattet sind, um alle gespeicherten Inhalte zu verschlüsseln. Andererseits können alle gespeicherten und hinzukommenden Daten eines USB-Sticks auch mit spezieller Software automatisch verschlüsselt werden. Bei beiden Varianten muss der Nutzer dem Stick im Vorfeld ein sicheres Passwort zuordnen. Dieses gibt er jedes Mal ein, wenn er den USB-Stick mit dem Computer verbindet, um die Entschlüsselung beim Lesen bzw. Verschlüsselung beim Schreiben zu ermöglichen.

Neben einer Vielzahl von kommerziellen Angeboten, gibt es zu diesem Zweck auch kostenfreie Software wie zum Beispiel TrueCrypt [1]. Achten Sie bei der Verschlüsselung darauf, ein sicheres Passwort zu verwenden. Details dazu finden Sie in dem bereits veröffentlichten IT-Sicherheitstipp „Wie erstelle ich ein sicheres Passwort?“.

▸ Halten Sie die Sicherheitssoftware auf dem neuesten Stand!

Häufig nutzen Kriminelle portable Speichermedien, um Schadsoftware wie Viren, Würmer und Trojaner zu verbreiten. Sie infizieren zum Beispiel einen USB-Stick mit einem Schädling, der genau auf ein neu entdecktes Sicherheitsleck abzielt und bringen diesen in Umlauf. Wird dieser infizierte USB-Stick nun mit einem Computer verbunden, nistet sich das Schadprogramm unbemerkt ein. Handelt es sich um einen Unternehmens-PC kann der Schädling sich über das gesamte Unternehmensnetzwerk ausbreiten. Um diesem Szenario vorzubeugen, müssen Sie einige Dinge beachten: Arbeiten Sie, wenn nicht zwingend notwendig, mit eingeschränkten Benutzerrechten. Gelangt Schadsoftware auf Ihren Rechner, kann diese auch nur mit eingeschränkten Benutzerrechten ausgeführt werden. Schließen Sie nur vertrauenswürdige Wechselmedien an Ihren PC an und geben Sie Ihre eigenen Benutzerrechte niemals preis. Untersuchen Sie Speichermedien regelmäßig mit einem Antivirenprogramm. Weil Hacker tagtäglich neue Malware entwickeln, muss Ihr Virenscanner regelmäßig aktualisiert werden, damit er effektiv arbeitet. Halten Sie auch das Betriebsystem und sämtliche installierte Software mit Sicherheitsupdates immer auf dem neuesten Stand. So schließen Sie schnell neu entdeckte Sicherheitslücken und verkleinern damit die Angriffsfläche.

▸ Melden Sie Wechseldatenträger vor dem Herausnehmen ab!

Alle Wechseldatenträger sollten vor dem Entfernen immer vom System abgemeldet werden, insbesondere dann, wenn der Schreibvorgang noch aktiv ist und den Zwischenspeicher gerade leert. Unter Umständen kann es sonst zu Datenverlust kommen. Wechseldatenträger trennen Sie sicher, indem sie in der Taskleiste auf den Menüpunkt „Hardware sicher entfernen“ klicken. Dieser ist bei Windows durch ein grünes Pfeilsymbol gekennzeichnet. Nur so haben Sie die Gewissheit, dass sämtliche übertragenen Daten vollständig und korrekt gespeichert werden.

▸ Speichern Sie nur Kopien!

Um bei Verlust oder Defekt des Wechseldatenträgers nicht das Nachsehen zu haben, sollten Sie immer nur Kopien von Dateien darauf speichern. Halten Sie zur Sicherheit die Originale auf Ihrem PC oder anderen externen Speichermedien vor.

Achten Sie auf die richtige Lagerung Ihrer Speichermedien!

Vermeiden Sie bei CDs und DVDs eine feuchte Lagerung, starke Temperaturunterschiede sowie eine direkte Sonneneinstrahlung. Benutzen Sie zum Beschriften Etiketten oder spezielle Marker. Andernfalls kann durch Kratzer oder Lösungsmittel die Reflexionsschicht so beeinträchtigt werden, dass die Daten nicht mehr lesbar sind. Vermeiden Sie es magnetische Speichermedien, wie Ihre externe Festplatte, in der Nähe von anderen magnetischen Komponenten (z.B. Lautsprechern) aufzubewahren. Bei unzureichender Abschirmung können die gespeicherten Daten sonst verloren gehen. Bewahren Sie alle Wechselmedien stets an einem sicheren Ort getrennt von den Originaldaten auf. Bei einem Brand oder Diebstahl wären andernfalls neben Ihren Originaldaten dann auch Ihre Datensicherungen in großer Gefahr!

Löschen Sie Ihre Daten richtig!

Um Speichermedien, wie externe Festplatten, USB-Sticks oder Flash-Speicherkarten restlos von Daten zu befreien, reicht es nicht aus diese einfach zu löschen. Vernichtet wird dabei lediglich die Dateizuordnungstabelle, vergleichbar mit einem Inhaltsverzeichnis. Die Informationen sind meist weiterhin auf dem Datenträger hinterlegt und können mit speziellen Programmen in kürzester Zeit wiederhergestellt werden. Verwenden Sie Spezialsoftware, um Ihre Daten effektiv zu löschen. Neben kommerziellen gibt es auch viele kostenfreie Angebote, die zuverlässig arbeiten. Dies sind unter anderem Eraser, CBL Daten-Shredder, Secure Eraser und Darik's Boot and Nuke (DBAN).

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

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

Weiterführende Informationen:
[1] http://www.truecrypt.org/

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

Bildquelle: RubinoNero - 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 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