Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Fachhochschule Gelsenkirchen

Mitglied im:

Netzwerk Elektronischer Geschäftsverkehr

Sicherer Umgang mit dem Internet

Egal ob privat oder geschäftlich, das Internet ist heute in vielen Bereichen nicht mehr weg zu denken. Kein Wunder also, dass rund 72 Prozent der Bundesbürger bereits regelmäßig im Netz unterwegs sind. Das ist das Ergebnis einer aktuellen Studie der „Initiative D21“. Diesen Trend machen sich auch Internetkriminelle zu Nutze, weshalb die Bedrohung kontinuierlich zunimmt. Wer sich nur unzureichend dagegen schützt, riskiert im Falle eines Angriffs unangenehme oder gar teure Konsequenzen. Was genau Sie beachten müssen, um dies zu verhindern, erfahren Sie in diesem IT-Sicherheitstipp.

Achten Sie auf einen ausreichenden Basisschutz!

Um sich vor den Bedrohungen des Internets zu schützen benötigen Sie zwei Anwendungen: Ein Virenschutzprogramm, das Schadsoftware auf Ihrem PC aufspürt, blockiert und beseitigt und eine Personal Firewall, die wie ein Türsteher den Netzwerkverkehr zwischen Ihrem Computer und dem Internet regelt. Halten sie diese sicherheitsrelevanten Programme und jede weitere installierte Software mit Sicherheitsupdates immer auf dem neuesten Stand, um neu entdeckte Sicherheitslücken zu schließen und Kriminellen weniger Angriffsfläche zu bieten.

Übermitteln Sie sensible Daten nur verschlüsselt!

Damit bei der Übertragung von sensiblen Daten, wie beim Online-Shopping oder beim Online-Banking, keiner zum Beispiel Ihre Kreditkartenummer oder Ihre Zugangsdaten mitlesen kann, benötigen diese Informationen einen besonderen Schutz.

Achten Sie darauf, dass für die Übertragung stets eine verschlüsselte Verbindung zur Verfügung steht. Diese erkennen Sie daran, dass die Adresse mit „https“ statt wie üblich mit „http“ beginnt und an dem kleinen Schlosssymbol in der Statusleiste Ihres Browsers. Die Stärke der Verschlüsselung, die Ihnen beim Doppelklick auf das Symbol angezeigt wird, sollte mindestens 128bit betragen.

Vorsicht bei Spam-Mails!

Unerwünschte Werbe-E-Mails, auch Spam genannt, sind nicht nur nervig, sondern können auch gefährlich werden. Viele E-Mails mit Dateianhang enthalten nämlich Schadprogramme wie Viren, Würmer und Trojaner. Grundsätzlich empfiehlt es sich den Anhang einer E-Mail vor dem Öffnen mittels eines Virenscanners zu überprüfen, der sich stets auf dem neuesten Stand befindet. Einige Viren können aber bereits durch das bloße Aufrufen einer infizierten E-Mail gestartet werden. Deaktivieren Sie in den Einstellungen Ihres E-Mail-Programms die Funktion „Java Script erlauben“, um dies zu verhindern. Löschen Sie Nachrichten, die auf den ersten Blick z.B. durch die Betreffzeile als Spam zu identifizieren sind und antworten Sie keinesfalls darauf. Beim Klick auf Floskeln wie „Wenn Sie keine weiteren Nachrichten von uns erhalten wollen, klicken Sie hier" bestätigen Sie nur, dass es sich bei ihrer E-Mail um eine aktive Adresse handelt. Damit sie gar nicht erst von unliebsamen Spam-Mails belästigt werden, empfiehlt es sich, Ihre E-Mailadresse an möglichst wenigen Stellen zu hinterlassen.

Schützen Sie sich vor Phishing!

Neben der Verbreitung von Schadsoftware ist die digitale Post auch ein beliebtes Mittel, um die sensiblen Daten unvorsichtiger Internetnutzer mittels Phishing zu stehlen. Dazu versenden Kriminelle E-Mails, die vermeintlich aus einer vertrauenswürdige Quelle (z.B. Ihrer Bank) zu stammen scheinen, jedoch gefälscht sind. In der E-Mail wird unter einem Vorwand dazu aufgefordert, einem Link zu folgen, der auf eine gefälschte Internetseite führt. Hier sollen nun vertrauliche Daten, wie z.B. PINs und TANs, eingegeben werden. Machen Sie dies, ist es für Kriminelle ein Leichtes Ihr Konto zu plündern. Seriöse Unternehmen fragen diese Daten niemals auf diesem Wege ab. Geben Sie die Adresse Ihrer Bank in Ihrem Browser immer selber ein und folgen Sie keinen Links, die Sie dazu auffordern.

Verwenden Sie nur sichere Passwörter!

Verwenden Sie bei sicherheitskritischen Anwendungen, wie dem Onlineshop oder dem E-Mail-Account immer ein sicheres Passwort. Ein sicheres Passwort besteht aus mindestens zehn Zeichen, darunter eine Mischung aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen. Es ist auf den ersten Blick sinnfrei, steht nicht im Lexikon und hat nichts mit Ihrem persönlichen Umfeld zu tun (Namen, Geburtsdaten etc.). Ganz wichtig: Verwenden Sie für jeden Dienst ein anderes Passwort! Um den Überblick nicht zu verlieren, empfiehlt sich die Verwendung eines digitalen Passwort-Managers. Einige Produkte wie „Keepass“ oder „Password Safe“ können Sie im Internet kostenfrei herunterladen. Mit diesen Programmen können Sie die Vielzahl der Nutzernamen und Kennwörter verschlüsselt auf der Festplatte Ihres Computers speichern.

Erledigen Sie alltägliche Arbeiten vom Standardbenutzer-Konto!

Wer grundsätzlich mit Administratorenrechten arbeitet, gewährt auch Schadprogrammen uneingeschränkten Zugriff auf sein System. So können Viren, Würmer und Trojaner ihre volle Wirkung entfalten und einen katastrophalen Schaden anrichten. Legen Sie besser ein Benutzerkonto mit eingeschränkten Rechten an und benutzen Sie dieses für alltägliche Aufgaben. Die Möglichkeit dazu finden Sie unter Windows folgendermaßen: Start > Systemsteuerung > Benutzerkonten. Benutzen Sie das Administratoren-Konto nur bei Bedarf, z.B. wenn Sie Änderungen an der Konfiguration vornehmen müssen oder neue Programme installieren wollen.

Machen Sie regelmäßig Sicherungskopien!

Save early, save often (zu deutsch: sichere frühzeitig, sichere häufig) – wer diesen Merkspruch beherzigt, kann sich eine Menge Ärger ersparen, wenn die Festplatte einmal Schaden annimmt und alle gespeicherten Daten unwiederbringlich verloren gehen. Machen Sie aus diesem Grund regelmäßige Sicherungskopien Ihres gesamten Systems auf zusätzlichen Speichermedien, wie externen Festplatten, CD-ROMs oder USB-Sticks. Je häufiger Sie ein Backup durchführen, desto nützlicher wird es Ihnen im Schadensfall sein.

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
http://www.bsi.bund.de

Bildquelle: Spectral-Design - 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