Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

IT-Sicherheitstipp: Telearbeit ohne Risiko

Telearbeit, auch „eWorking“ genannt, ist im Kommen - so das Ergebnis einer aktuellen Studie des BITKOM-Verbands. Zehn Prozent der berufstätigen Bundesbürger arbeiten bereits ganz oder teilweise von zu Hause aus. Für weitere 58 Prozent der Befragten wäre dies eine interessante Option. Auch Unternehmen profitieren von dieser flexiblen Arbeitsform: sie senken ihre Kosten und erhöhen gleichzeitig die Produktivität der Mitarbeiter. Doch wer mit Laptop, Internet und Smartphone von Daheim aus arbeitet, muss von seinem Arbeitgeber in Sachen IT-Sicherheit besonders sensibilisiert werden. Klare Regelungen für die Mitarbeiter und eine sichere Informationstechnologie sind dabei wichtige Voraussetzungen, um Sicherheitsrisiken auf ein Minimum zu reduzieren. Was genau es zu beachten gibt, erfahren Sie in diesem Sicherheitstipp.

Verwenden Sie einen angemessenen Basisschutz!

PCs, die geschäftlich benutzt werden und sich auch ins Firmennetzwerk einwählen, müssen besonders vor digitalen Bedrohungen aus dem Internet geschützt werden. Dafür brauchen Sie unbedingt ein Antivirenprogramm (verhindert die Infektion und Ausbreitung von Viren, Würmern und Trojanern) und eine Personal-Firewall (regelt nach festgelegten Vorgaben den Datenverkehr zwischen dem Computer und dem Internet). Achten Sie zudem darauf, dass sowohl Ihre Sicherheitssoftware als auch Ihr Betriebssystem sowie alle installierten Programme regelmäßig mit Sicherheitsupdates versehen werden und sich Ihr System damit immer auf dem neuesten Stand befindet.

Verwenden Sie nur sichere Passwörter!

Vergeben Sie für sensible Anwendungen und Dokumente nur sichere Passwörter – jedes Passwort nur einmalig. Ein sicheres und damit starkes Passwort besteht aus mindestens zehn Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), enthält keine persönlichen Daten (z.B. Namen oder Geburtstage) und steht nicht im Lexikon. Nutzen Sie einen Passwortmanager, um die Vielzahl der Passwörter zu managen. Dieser speichert sämtliche Kennwörter verschlüsselt auf der Festplatte Ihres Computers. Einige Produkte wie „Keepass“ oder „Password Safe“ können Sie im Internet kostenfrei herunterladen. Achten Sie darauf, dass der Passwortmanager ein sicheres Verschlüsselungsverfahren verwendet. Empfohlen wird der Advanced Encryption Standard (kurz: AES). Weitere Informationen zu sicheren Passwörtern finden

Sie in unserem bereits veröffentlichtem IT-Sicherheitstipp „Wie erstelle ich ein sicheres Passwort“ [1].

Verwenden Sie eine sichere WLAN-Konfiguration!

Ändern Sie das voreingestellte Passwort für das Konfigurationsprogramm Ihres WLAN-Routers nach den oben angegebenen Empfehlungen. Wählen Sie eine sichere Verschlüsselungsmethode für das Funknetzwerk aus (mindestens WPA, besser WPA 2). Den Namen Ihres drahtlosen Netzwerks können Sie frei wählen. Verwenden Sie aber niemals eine Bezeichnung, die einen Hinweis darauf gibt, wem das Gerät gehört oder gar den Gerätetyp enthält. Ansonsten kann ein Angreifer speziell nach Schwachstellen für Ihren Router suchen und gegebenenfalls in Ihr Netzwerk eindringen.

Nutzen Sie eine verschlüsselte Verbindung zu Ihrem Firmennetzwerk!

Wenn Sie sensible Informationen austauschen, werden diese ohne besondere Sicherheitsvorkehrungen nicht verschlüsselt übertragen. Ein probates Mittel um Daten sicher zwischen zwei räumlich getrennten Netzwerken zu übermitteln, um also zu verhindern, dass sie während des Transports weder mitgelesen noch verändert werden können, ist ein sogenanntes „Virtual Private Network“ (kurz: VPN). Das VPN verschlüsselt die Information beim Sender und entschlüsselt sie erst beim Empfänger wieder. Mitarbeiter können so bequem von zu Hause aus, auf betriebliche Dienste und Dokumente zurückgreifen, da Sie sich dann im gleichen Netzwerk befinden, wie jemand der mit seinem Rechner im Unternehmen physisch vor Ort ist.

Benutzen Sie den Firmen-PC nicht für private Zwecke!

Nutzen Sie den Arbeits-PC ausschließlich für berufliche Zwecke. Zu groß ist die Gefahr, dass Sie das Gerät beim Surfen im Internet oder beim Download von Programmen mit Schadsoftware verseuchen. Wenn Sie sich im Anschluss nichts ahnend mit dem Unternehmensnetzwerk verbinden, kann sich der Schädling unter Umständen im gesamten Unternehmensnetzwerk ausbreiten und einen verheerenden Schaden anrichten. Verwehren Sie auch der Familie und Bekannten den Zugang zum Dienst-Computer. Nur so minimieren Sie das Sicherheitsrisiko auf ein Minimum.

Speichern und Löschen Sie Ihre Daten richtig!

Sensible Dokumente speichern Sie am sichersten mit einer lokalen Verschlüsselung. Selbst wenn sich jemand physisch Zugang zum PC verschafft oder sich in Ihr Netzwerk hackt, sind die Daten ohne das korrekte Passwort bzw. die passende Schlüsseldatei wertlos. Wichtig hierbei ist natürlich, dass Sie ein sicheres Passwort vergeben, welches den oben genannten Anforderungen genügt [1]. Kostenlose Programme wie „True Crypt“ oder „Disk Cryptor“ sind benutzerfreundlicher und verwenden zur Verschlüsselung den als sehr stark geltenden Advanced Encryption Standard. Wird ein PC oder die Festplatte ausgetauscht, ist auch das richtige Löschen von Dateien äußerst wichtig. Formatieren oder in den Papierkorb verschieben reicht nicht aus. Verwenden Sie deshalb zum Löschen Ihrer sensiblen Daten Spezialsoftware (z.B. Eraser, CBL Daten-Shredder oder Secure Era-

ser). Diesem Problem lässt sich allerdings auch ganz analog zu Leibe rücken: Schrauben Sie die Festplatte einfach auf und zerstören Sie die magnetische Scheibe zum Beispiel mit einer Schere. Weitere Informationen zum Thema „Sicheres Speichern und Löschen Ihrer Daten“ finden Sie in unserem bereits veröffentlichtem IT-Sicherheitstipp [1].

Autoren

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

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

[1] http://ratgeber.it-sicherheit.de

Bildquelle: nyul - Fotolia.com

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

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 mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch 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.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit 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.kmu-sicherheit.de