Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Fachhochschule Gelsenkirchen

if(is) internet-sicherheit.

Mitglied im:

Netzwerk Elektronischer Geschäftsverkehr

Wie schütze ich mein WLAN vor Dritten?

Kabelsalat gehört mit dem Wireless Local Area Network (kurz: WLAN), oder zu Deutsch dem „drahtlosen lokalen Netzwerk“, der Vergangenheit an. Besonders Nutzern von mobilen Endgeräten, wie Notebooks oder Smart Phones, beschert das mehr Freiheit. Besitzer von WLANs, ob privat oder geschäftlich, haben aber einige Verpflichtungen: Sie sind dafür verantwortlich, dass ihr Funknetzwerk ausreichend vor dem unberechtigten Zugriff durch Dritte abgesichert ist. Nach einem Gerichtsurteil im Mai 2010, muss ein WLAN-Inhaber eine Abmahnung in Höhe von 100 Euro zahlen, weil über seinen ungesicherten Anschluss illegal Musik heruntergeladen wurde. Aber: Mit einigen Klicks können Sie Ihr Netzwerk sicher machen!

▸ Verwenden Sie Ihr WLAN ausschließlich mit einer Verschlüsselung!

Wenn Sie eine Funkverbindung über WLAN einsetzen, sollte diese in jedem Fall verschlüsselt sein. Ist die Funkverbindung nicht verschlüsselt, werden einerseits alle Daten, z.B. Passwörter Ihrer Bank, im Klartext übertragen und können von Angreifern einfach mitgelesen werden. Andererseits können Dritte meist unbemerkt Ihr WLAN mitbenutzen. Die Angreifer brauchen sich dazu auch nicht in Ihrer Wohnung aufhalten, denn Ihr Funknetzwerk ist mit speziell angefertigten Antennen in Entfernungen bis zu 2km zu empfangen. Werden Straftaten, wie das illegale Herunterladen von Musikdateien über Ihr WLAN und damit letztendlich über Ihren Telefonanschluss begangen, fallen diese bei den Ermittlungen auf Sie zurück!

Wählen Sie die Verschlüsselungsmethode WPA2 aus!

WLAN-Module bieten häufig eine Verschlüsselung mit drei unterschiedlichen Verfahren an (WEP, WPA und WPA2). Bei WEP handelt es inzwischen um eine unsichere Verschlüsselung, die binnen einer Minute geknackt werden kann. Setzen Sie für die Verschlüsselung daher nur noch WPA oder besser WPA2 ein (Stand Q2/2010). Sofern Sie z.B. über eine alte Windows XP Version verfügen, ist eine Aktualisierung (ein so genanntes Update) Ihres Betriebssystems für die Verwendung von WPA/WPA2 erforderlich. Nähere Informationen finden Sie auf der jeweiligen Internetseite des Herstellers.

Achtung: Gerade bei älteren Geräten, die WLAN nutzen können, ist es nicht immer adhoc möglich die Verschlüsselungsmethode WPA2 auszuwählen. Besuchen Sie dazu die Webseite des Geräteherstellers und schauen Sie dort, ob Updates auf der Webseite für das Gerät zur Verfügung stehen. Ggf. lässt sich mit einem Update die Verschlüsselung WPA2 nachinstallieren. Nicht alle Geräte unterstützen jedoch mit einem Update die Verschlüsselungsmethode WPA2. Diese kann daher in einigen Fällen nicht nachinstalliert werden. Sprechen Sie dazu mit Ihrem Computerfachhändler, ob Ihr Gerät (z.B. ein WLAN-Stick) bei der Verwendung eines sicheren WLANs mit WPA2-Verschlüsselung überhaupt genutzt werden kann oder welche alternativen Sicherheitsmechanismen Ihnen zur Verfügung stehen.

Verwenden Sie für die Verschlüsselung ein starkes Passwort!

Das Passwort für die WLAN-Verschlüsselung – in diesem Kontext auch Passphrase oder Schlüssel genannt – sollte mindestens 13 Stellen lang, sinnfrei zusammengesetzt sein und aus Zahlen, Zeichen und Sonderzeichen wie "!" oder "$" bestehen. Es schadet aber auch nicht alle 63 möglichen Stellen auszunutzen. Verwahren Sie die gewählte Passphrase an einem sicheren Ort auf. Sie müssen die Passphrase pro Computer nur einmalig eingeben, da sich der Computer die Verbindung merkt.

Schützen Sie die Konfiguration Ihres Routers!

Das Gerät was Ihnen WLAN ermöglicht, ist zumeist ein Router. Dieser wird mittels eines Browsers, wie dem Internet Explorer oder Mozilla Firefox konfiguriert. **Um sicher zu gehen, dass Ihre Konfiguration nicht von Dritten ausgelesen oder manipuliert werden kann (z.B. Abschalten der Verschlüsselung), ist die Wahl eines starken Passworts notwendig!**

Verwenden Sie für Ihr WLAN keine konkrete Bezeichnung!

Jedes WLAN hat eine Bezeichnung, die Sie frei definieren dürfen. Um sich mit einem Funknetzwerk zu verbinden, muss man dieses zuvor auswählen oder eingeben, wenn die Bezeichnung (SSID) nicht extra ausgestrahlt wird. In diesem Fall spricht man von einem verborgenen WLAN. Gerne werden für die Bezeichnung eines WLANs der Hausname oder die Gerätebezeichnung verwendet. Ein Angreifer weiß daraufhin sofort, dass das WLAN Ihnen gehört oder kann bei einer Gerätebezeichnung speziell nach Schwachstellen für das genutzte Gerät suchen, um daraufhin in Ihr Netzwerk einzudringen! **Verwenden Sie daher bei der Bezeichnung Ihres WLANs einen Namen, der nicht auf Sie zurückzuführen ist und keine technischen Details Ihres WLANs preis gibt.**

Schalten Sie die sogenannte SSID-Kennung Ihres WLANS ab!

Alle Funknetzwerke in Reichweite werden Ihnen angezeigt, sofern Sie das Netzwerk nicht extra verborgen haben. Nahezu jeder aktuelle WLAN-Scanner, ein Programm, welches Angreifer verwenden, um WLANs zu finden, kann heutzutage auch verborgene Netzwerke erkennen. Das Abschalten der SSID-Kennung bietet daher keinen Schutz vor Angreifern. Alle anderen Sicherheitsvorkehrungen müssen zusätzlich getroffen werden.

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

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

Ausführliche Informationen rund um das Thema finden Sie direkt unter:
https://www.it-sicherheit.de/topthema/wlan-sicherheit/

Weiterführende Informationen:
http://www.internet-sicherheit.de/de/institut/buch-sicher-im-internet/videos/screenvideos/video/9/
https://www.it-sicherheit.de
http://www.bsi-fuer-buerger.de
http://www.ec-net.de/sicherheit/

Das 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. 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 sowie unter: http://www.ecc-handel.de/sichere_e-eschaeftsprozesse_in_kmu_und_handwerk.php

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.

Bildquelle: Andre Bonn – Fotolia.com