Der monatliche Newsletter für Anwender zum Thema IT Sicherheit

OUCH!

IN DIESER AUSGABE...

- Ihr drahtloses Netzwerk
- OpenDNS
- Ihre Geräte

So sichern Sie Ihr Heimnetzwerk

Überblick

Vor einigen Jahren waren Heimnetzwerke relativ simpel aufgebaut, sie bestanden meist aus nicht mehr als einem WLAN Router und ein bis zwei Computern um im Internet zu surfen oder für Onlinespiele. Heimnetzwerke werden jedoch immer komplexer; nicht nur dass immer mehr Geräte damit verbunden werden, auch deren Nutzungsvielfalt steigt. In dieser Ausgabe werden wir einige grundlegende Punkte ansprechen, mit denen Sie Ihr Heimnetzwerk sicherer gestalten.

Gastautor

Kevin Johnson ist CEO bei Secure Ideas, betreibt die Webseite **MySecurityScanner.com** und unterrichtet als Senior Instructor für das SANS Institute. Weitere Informationen finden Sie unter **www.secureideas.com**.

Ihr drahtloses Netzwerk (WLAN)

Nahezu jedes Heimnetzwerk basiert auf einem drahtlosen Netzwerk (auch Wi-Fi Netzwerk oder WLAN genannt). Dies ermöglicht es eine Vielzahl Geräte, von Laptops und Tablets bis hin zu Spielekonsolen und TV-Geräten, drahtlos miteinander und mit dem Internet zu verbinden. Um dies zu erreichen benötigen Sie einen drahtlosen Zugangspunkt (WLAN Zugangspunkt, AccessPoint). Dies ist ein Gerät welches an Ihren Internet Router angeschlossen ist und die Funksignale verschickt mit denen sich Ihre mobilen Endgeräte verbinden. Oft befinden sich Internet Router und drahtloser Zugangspunkt mittlerweile integriert in einem Gerät, dem WLAN Router. Einmal mit dem drahtlosen Zugangspunkt verbunden, kann ein Gerät sich mit anderen Geräten in Ihrem Heimnetzwerk oder dem Internet verbinden. Aufgrund dieser Tatsache ist Ihr drahtloser Zugangspunkt eine der Schlüsselkomponenten Ihres Heimnetzwerkes und wir empfehlen Ihnen folgende Schritte durchzuführen um ihn abzusichern.

- Für die meisten drahtlosen Zugangspunkte kursieren die Standard Zugangsdaten (Benutzername und Passwort des Standardnutzers oder Administrators) im Internet und sind somit vielen Personen bekannt. Daher sollten sie die Standard Zugangsdaten abändern, so dass nur Sie diese kennen. Stellen Sie sicher, dass Sie ein eigenständiges Passwort vergeben und keines, welches Sie auf anderen Endgeräten oder für andere Benutzerkonten einsetzen.
- Ändern Sie den Namen Ihres drahtlosen Netzwerkes (auch SSID genannt). Dieser Name ist für jede Person sichtbar die nach lokalen drahtlosen Netzwerken Ausschau hält. Denken Sie sich einen individuellen Namen aus um es einfacher zu finden, aber vermeiden Sie es persönliche Informationen einfließen zu lassen. Bedenken Sie, dass es keinen Mehrwert bietet Ihre SSID zu verstecken. Die meisten Werkzeuge zum Aufspüren drahtloser Netzwerke oder erfahrene Angreifer können mit Leichtigkeit auch Informationen und Details von versteckten drahtlosen Netzwerken aufspüren.

So sichern Sie Ihr Heimnetzwerk

- Als nächsten Schritt sollten Sie sicherstellen, dass nur Personen die Sie kennen und denen Sie trauen sich mit Ihrem drahtlosen Netzwerk verbinden und dieses nutzen, und dass diese Verbindungen verschlüsselt sind. Um das Risiko zu minimieren, dass Ihre Nachbarn oder fremde Personen sich mit Ihrem Netzwerk verbinden oder unbemerkt Daten mitlesen, sollten Sie eine starke Verschlüsselung auf Ihrem drahtlosen Zugangspunkt nutzen. Zurzeit ist der Sicherheitsstandard WPA2 die beste Wahl. Um diesen zu nutzen benötigen Sie ein gemeinsames Passwort für alle Personen und Geräte, die auf Ihr Heimnetzwerk zugreifen sollen. Sobald man damit angemeldet ist, ist die Verbindung verschlüsselt. Stellen Sie sicher, dass Sie keine veralteten Sicherheitsstandards wie WEP nutzen oder gar ganz auf Verschlüsselung und somit Sicherheit verzichten, was zu einem offenen Netzwerk führt. Ein offenes Netzwerk erlaubt jedem, sich ohne Anmeldung mit Ihrem drahtlosen Netzwerk zu verbinden und z.B. Daten.

Aktivieren Sie auf Ihrem Tablet-PC einen Passcode- oder PIN-Schutz, aktualisieren Sie immer auf die aktuellste Version des Betriebssystems und der Apps, und achten Sie auf die Einstellungen zu Privatsphäre und Cloud-Speicher.

- Die Passwörter, welche die Nutzer zum Zugang in Ihr drahtloses Netzwerk nutzen, sollten stark und schwer zu erraten sein und sich vom Passwort des Administrators unterscheiden. Höchstwahrscheinlich werden Sie das Passwort nur einmal auf jedem Gerät eingeben müssen, welches es dann speichert.
- Viele drahtlose Zugangspunkte unterstützen sogenannte Gast-Netzwerke oder Gastzugänge. Diese ermöglichen es Besuchern, sich in Ihrem drahtlosen Netzwerk anzumelden um im Internet zu surfen, verhindern aber dabei ein Verbinden auf Ihre Geräte im Heimnetzwerk. Wenn Sie einen solchen Gastzugang einrichten aktivieren Sie dafür ebenfalls WPA2 und erstellen Sie ein eigenständiges Passwort für dieses Netzwerk.
- Wenn Sie sich die verschiedenen Passwörter nicht merken können, benutzen Sie einen Passwort Manager um diese sicher aufzubewahren.

OpenDNS

Sobald Sie Ihr drahtloses Netzwerk konfiguriert haben, empfehlen wir Ihnen Ihr Netzwerk so zu konfigurieren, dass OpenDNS als DNS Server verwendet wird. Sie können aber auch einen ähnlichen Dienst wie Norton ConnectSafe for Home nutzen. Wenn Sie einen Namen in Ihren Webbrowser eingeben, teilt DNS Ihrem Browser mit welchen Server er im Internet ansteuern soll. Dienste wie OpenDNS kennen bekannte infizierte Webseiten und unterbinden die Kommunikation zwischen Ihren Endgeräten und diesen Webseiten falls diese versehentlich angesteuert werden. Zusätzlich bieten Ihnen diese Dienste die Möglichkeit, anstößige Webseiten zu filtern und zu blockieren. Was diesen Ansatz so wirksam macht ist die Tatsache, dass keine Software auf Ihren Endgeräten installiert werden, sondern nur zentral eine Einstellung im drahtlosen Zugangspunkt konfiguriert werden muss.

So sichern Sie Ihr Heimnetzwerk

Ihre Endgeräte

Als nächstes gilt es zu wissen, was mit Ihrem Heimnetzwerk verbunden ist und sicherzustellen, dass diese Endgeräte sicher sind. Das war früher einfach, da nur ein paar wenige Endgeräte angeschlossen waren. Heutzutage kann sich jedoch nahezu alles im Haushalt zu Ihrem Heimnetzwerk verbinden, einschließlich Ihrer Fernsehgeräte, Spielekonsolen, Babyüberwachungsanlagen, Lautsprecher, Ihre Heizungsanlage/Thermostate, sogar Ihr Auto. Haben Sie alle Endgeräte identifiziert werden Sie überrascht sein, dass es dann doch so viele sind. Der beste Weg, all diese Geräte sicher zu beitreiben, st sicherzustellen, dass sie jederzeit mit dem aktuellen Stand des Betriebssystems laufen. Wenn möglich prüfen Sie ob ein automatisches Aktualisieren eingebaut und aktiviert ist. Wenn diese Option nicht gegeben ist prüfen Sie ihre Geräte mindestens einmal im Monat auf Updates und installieren Sie diese. Außerdem sollten sie die Internetpräsenz Ihres Internetanbieters besuchen, eventuell bietet dieser freie Anwendungen oder Dienste an welche Ihnen helfen Ihr Netzwerk sicher zu gestalten.

Weiterführende Informationen

OpenDNS

http://www.opendns.org

Norton ConnectSafe

https://support.norton.com/sp/de/de/home/current/solutions/v53247012_EndUserProfile_de_de

Netzwerksicherheit-Scanner:

http://www.sophos.com/de-de/products/free-tools/network-security-scan.aspx

Passwort Manager:

http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis