Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- **Ihr drahtloses Netzwerk**
- **Ihre Geräte**

Absicherung Ihres Heimnetzwerks

Überblick

Vor einigen Jahren waren Heimnetze noch relativ einfach aufgebaut, für gewöhnlich nicht viel mehr als ein Drahtlos- bzw. WLAN-Zugangspunkt und ein oder zwei Computer, die zum Internet Surfen, für Onlineshopping oder Spiele genutzt wurden. Seither hat die Komplexität jedoch stetig zugenommen. Heute sind eine große Anzahl weiterer Geräte mit dem häuslichen Netz verbunden, die für viel mehr als das Webbrowsen oder den Medienkonsum genutzt werden. In diesem Newsletter erläutern wir, wie Sie ein sicheres Heimnetzwerk für sich und Ihre Familie einrichten und betreiben können.

Gastautor

Cheryl Conley leitet das Team für Sicherheitstrainings und Sicherheitsbewusstsein bei Lockheed Martin, und erreicht mit der "The I Campaign™" über 100.000 Mitarbeiter. Das umfasst Zielgruppen im gesamten Unternehmen ebenso wie ein globales Phishing Programm. Folgen Sie Cheryl unter **@conleychera**.

Ihr drahtloses Netzwerk

Nahezu jedes Heimnetzwerk basiert auf einem drahtlosen Netzwerk bzw. WLAN. Dadurch können Sie Ihre Geräte kabellos mit dem Internet verbinden, ganz gleich ob es sich um Laptops, Tablets, Spielekonsolen oder den Fernseher handelt. Die meisten WLANs werden von Ihrem Internet-Router verwaltet, dem Gerät, das Ihnen Ihr Internetzugangsanbieter im Haus installiert oder bei Vertragsabschluss zugeschickt hat um sie mit dem Internet zu verbinden. In manchen Fällen ist jedoch auch ein separates Gerät, WLAN Zugangspunkt oder engl. Accesspoint genannt, mit Ihrem Internetrouter verbunden und stellt das heimische WLAN bereit. Unabhängig davon, welche Variante bei Ihnen implementiert ist, arbeiten beide auf die gleiche Art durch das Aussenden von standardisierten Funkwellen. Die verschiedenen Geräte in Ihrem Haushalt verbinden sich über diesen Funkstandard mit dem zentralen Zugangspunkt. Von dort aus können die Geräte das Internet, aber auch alle anderen verbundenen Geräte des Heimnetzes erreichen. Der Absicherung Ihres drahtlosen Netzwerks kommt daher eine Schlüsselrolle beim Schutz Ihres Heims zu. Wir empfehlen dazu die folgenden Schritte:

- Ändern Sie das werksseitig vorgegebene Administratorpasswort Ihres Internetrouters oder WLAN Zugangspunkts, je nach dem, welches Gerät Ihr WLAN verwaltet. Dieser Administratorzugang erlaubt Ihnen, die Einstellungen für das Drahtlosnetzwerk zu verändern. Viele Geräte werden leider mit einem sehr einfachen und/oder im Internet einfach auffindbaren Passwort ausgeliefert. Ändern Sie das Passwort auf ein sicheres, schwer zu erratendes Passwort, das nur Sie kennen.

Absicherung Ihres Heimnetzwerks

Um Ihr Heimnetzwerk zu schützen, sichern Sie Ihr Drahtlosnetzwerk, aktualisieren Sie alle Geräte und versehen Sie sie mit einem Passwortschutz.

- Ändern Sie die werksseitig vorgegebene Bezeichnung für Ihr WLAN Netzwerk (manchmal SSID genannt). Das ist der Netzwerkname den Ihre Geräte sehen, wenn sie nach erreichbaren Netzwerken suchen. Benennen Sie Ihr Netzwerk möglichst einzigartig, so dass Sie es einfach erkennen können, aber vermeiden Sie die Preisgabe von persönlichen Informationen. Es bringt heute nahezu keinen Mehrwert, Ihr WLAN als „versteckt“ zu konfigurieren, da die meisten Werkzeuge zum Suchen nach Drahtlosnetzen diese trotzdem finden können und jeder erfahrene Angreifer mit diesen Werkzeugen umgehen können.
- Stellen Sie sicher, dass nur Personen denen Sie vertrauen auf das Netz zugreifen können, und die Verbindung verschlüsselt erfolgt. Aktivieren Sie hierfür den derzeit besten Sicherheitsmechanismus „WPA2“ und vergeben Sie ein starkes Passwort, so dass alle Verbindungen stark verschlüsselt sind. Nutzen Sie keine veralteten und unsicheren Verschlüsselungsstandards (z.B. WEP), Deaktivieren Sie nie die Verschlüsselung (“offenes Netzwerk”), denn ein offenes Netz erlaubt es jedermann ohne Anmeldung, sich mit Ihrem Netzwerk zu verbinden.
- Stellen Sie sicher, dass das Passwort zum Zugriff der Nutzer auf das Netz möglichst komplex ist, und dass es sich vom Administrator-Passwort unterscheidet. Schließlich müssen Sie dieses Passwort nur einmal auf jedem Gerät eingeben, da es dort für die weitere Verwendung gespeichert wird.
- Viele WLAN-Zugangspunkte unterstützen sogenannte Gast-Netzwerke. Damit wird Besuchern der Zugang zum Internet erlaubt, es schützt jedoch die Geräte in Ihrem Heimnetzwerk in dem es keine Verbindung zu diesen zulässt. Auch im Gastnetzwerk sollten Sie WPA2 mit einem starken, natürlich wieder einzigartigen, Passwort aktivieren.
- Deaktivieren Sie die „WiFi Protected Setup“ (WPS) genannte Funktion, die es neuen Geräten erlaubt sich ohne Eingabe eines Passworts mit dem Netzwerk zu verbinden.
- Wenn Sie Schwierigkeiten haben sollten, sich die ganzen Passwörter zu merken, empfehlen wir Ihnen die Nutzung eines sog. Passwortsafes, einem Programm zur Verwaltung und sicheren Speicherung von Passwörtern.

Wenn Sie sich bei bei der Umsetzung dieser Schritte unsicher sind, bitten Sie Ihren Internetanbieter um Hilfe, lesen Sie die Dokumentation die mit dem Internetrouter oder Drahtlos-Zugangspunkt geliefert wurde oder konsultieren Sie die entsprechenden Webseiten.

Absicherung Ihres Heimnetzwerks

Ihre Geräte

Der nächste Schritt besteht darin zu wissen, welche Geräte mit dem Heimnetz verbunden sind und zu gewährleisten, dass alle sicher sind. Das war früher einmal leicht, als nur wenige Geräte im Heimnetz waren. In der heutigen, „immer verbunden“ Welt kann jedoch nahezu jedes Gerät mit dem Heimnetz und dem Internet sprechen, darunter Fernseher, Spielekonsolen, Baby-Überwachungsgeräte, Lautsprecher, Heizungsthermostate, ja sogar Ihr Auto. Ein einfacher Weg um zu überprüfen, welche Geräte mit dem Netz verbunden sind, ist die Nutzung eines einfachen Netzwerkscanners wie Fing. Diese Programme, die Sie auf einem Computer oder Mobilgerät installieren können, durchsuchen Ihr Heimnetzwerk und melden jedes damit verbundene Gerät. Sobald Sie alle Geräte identifiziert haben müssen Sie deren sichere Konfiguration prüfen. Dies ist am einfachsten, wenn die Geräte immer mit dem neuesten Betriebssystem bzw. der neuesten Firmware laufen – aktivieren Sie hierfür die Funktionen zum automatischenv Update, wenn verfügbar. Wenn eines der Geräte ein Passwort verlangt, vergeben Sie immer ein starkes, einzigartiges Passwort. Auch Ihr Internetzugangsanbieter bietet auf seiner Webseite möglicherweise Programme an, die Ihnen bei der Absicherung des Netzes und der Geräte helfen.

Weiterführende Informationen

Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Passwort-Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016
Kennenlernen Ihres Heimnetzwerks (engl.):	http://l.rud.is/home-network-mapping

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

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns 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