OUCH! | 2016 年 02 月

コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- 自宅の無線ネットワーク
- 保持しているデバイス

自宅のネットワークを安全にするには

はじめに

数年前までは、自宅ネットワークは比較的簡素なものでした。無線のアクセスポイントがあり、そのポイントを通じて1、2台のパソコンがインターネットにアクセスし、オンライン上で買い物やゲームをしたりしていたでしょう。しかし、最近の自宅ネットワークは、複雑になってきており、このネットワークに対して様々なデバイスを接続し、ウェブ閲覧に代表されるような情報を見聞きしたりする以上のことをするようになってきています。このニュースレターでは、自分自身、そして家族が安心して利用できる安全な自宅ネットワークを構築する方法を紹介します。

ゲストエディター

シェリル・コンリー氏は、ロッキード・マーチン社のSecurity Education and Awarenessチームのリーダーであり、I Campaign™を使って100,000人にも上る従業員にサイバーセキュリティの意識啓発活動を行っています。この中には、社内のアライアンスやフォーカスグループの支援のほか、グローバルなフィッシングプログラムも含まれている。シェリルはツイッター（@conleychera）を通じても情報を発信しています。

自宅の無線ネットワーク

多くの自宅ネットワークには、無線ネットワーク（Wi-Fiネットワークとも呼ばれる）が存在しています。これにより、どのデバイスでも無線経由でインターネットに接続することが可能になっており、接続されるデバイスの中には、ノートパソコン、タブレット、ゲームやテレビが含まれます。多くの自宅無線ネットワークは、ルータによって制御されていると思いますが、このデバイスは、通常インターネットサービスプロバイダによって自宅内に設置され、インターネットへの接続を可能にしていますが、無線アクセスポイント呼ばれるルータに接続されているシステムによって制御されている場合もあります。どちらの場合においても同じように無線信号を発信しており、この信号を経由してそれぞれのデバイスが無線ネットワークに接続すると、これらのデバイスはインターネットに接続できるようになるだけでなく、同じ自宅ネットワーク内にある他のデバイスにも接続可能になると思います。そのため、自宅の無線ネットワークを安全にすることは、自宅の全てのデバイスを守るために重要になるのです。以下のステップを確認して、安全にすることをお勧めします。

- 無線ネットワークを制御しているルータまたは無線アクセスポイントに設定されているデフォルトの管理者パスワードを変更してください。この管理者アカウントを使って、無線ネットワークの設定を変更することが可能です。多くのルータや無線アクセスポイントは、管理者ユーザとパスワードがデフォルトで設定されており、インターネット上にこれらの情報が公開されています。そのため、この管理者パスワードを任意でかつ自分自身しか知らない強力なパスワードに変更してください。
- 無線ネットワークの名称（SSIDとも呼ばれる）をデフォルト設定から変更してください。この名称は、デバイスがローカルネットワークの探索をする時に見える名称です。ネットワーク名には、簡単に識別可能になるような

自宅のネットワークを安全にするには

名称をつけることが重要ですが、個人的な情報が含まれないようにしてください。ネットワークを隠ぺい（ブロードキャストしない）する設定にしてもそれほど意味はありません。なぜなら、多くの無線ネットワーク探索ツールや、高度なスキルを持つ攻撃者の手にかかれば、隠れた無線ネットワークを発見することは非常に簡単だからです。

- 自宅の無線ネットワークに接続、利用する人は、すべて信頼できる人となるようにしてください。また、通信も暗号化してください。WPA2と呼ばれる暗号化方式が、現在利用できるもの中で最良の手法です。これを有効にすることで、自宅ネットワークに接続するためにパスワードの入力が必要になるだけでなく、接続した後の通信はすべて暗号化されます。WEPなどの古い、時代遅れとなった暗号化方式を使ったりセキュリティ機能を全く使用しないでオープンネットワークとすることはやめてください。オープンネットワークとは、誰でも認証無しで無線ネットワークに接続可能なネットワークのことです。
- 無線ネットワークに接続するためのパスワードが強力なパスワードとしますが、管理者アカウントのパスワードとは異なるパスワードを設定してください。それぞれのデバイスは、パスワードを記憶することができるため、入力は一度しか行われないことが多いので、できる限り強力なパスワードを設定しましょう。
- 多くの無線ネットワークは、ゲストネットワークと呼ばれる機能をサポートしています。これは、来客などに提供する無線ネットワークのことで、インターネットに接続はできますが、自宅ネットワークに接続されているデバイスへのアクセスを遮断することで自宅ネットワークを保護する仕組みです。ゲストネットワークを有効にした場合、WPA2と一意となるパスワードを忘れずに設定してください。
- WiFi Protected Setup は、パスワードや他の設定を知らない状態でも、簡単なボタン操作などでネットワークへ接続できる機能ですが、これらの機能はすべて無効にしてください。
- 複数のパスワードを覚えることに苦労している場合は、パスワードを安全に保管してくれるパスワードマネージャと呼ばれるツールを使用することをお勧めします。

自宅ネットワークを保護するには；無線ネットワークを安全にし、ネットワーク上にあるすべてのデバイスを更新し、パスワードで保護することが重要。

ここまでご紹介した機能を設定する方法が分からない場合は、インターネットサービスプロバイダに問い合わせを行ったり、ルータまたは無線アクセスポイントの付属文書を参照する、ウェブサイトに掲載されている情報などを確認するなどの対応を行ってください。

保持しているデバイス

次のステップは、自宅ネットワークに接続されているデバイスを把握することと、それぞれのデバイスが安全な状態であることを確認することです。これは、接続されているデバイスが数台だった頃は、簡単な作業でしたが。現在の「

自宅のネットワークを安全にするには

常時接続」が当たり前となっている世の中では、ほとんどのデバイスが自宅ネットワークに接続可能となっており、テレビやゲームだけではなく、ベビーモニター、スピーカー、温度自動調節器、そして車も含まれます。自宅ネットワークに何が接続されているか調べる方法として、Fingと呼ばれるネットワーク探索ツールを使用する方法があります。このアプリは、パソコンまたはモバイルデバイスにインストールし、無線セットワークを探索した後で、そのネットワークに接続されているすべてのデバイスを通知してくれるものです。自宅ネットワークに接続されているすべてのデバイスを特定した後は、これらデバイスの安全性を確保しなければなりません。最良の方法は、最新のオペレーティングシステム・ファームウェアに更新することです。また、可能な限り、自動アップデート機能を有効にしてください。デバイスにパスワードを設定できる場合は、一意で強力なパスワードを設定してください。最後に、インターネットサービスプロバイダのウェブサイトを訪問し、自宅ネットワークをより安全にするツールを提供しているかどうかも確認してください。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。
http://www.securingthehuman.org

日本語版翻訳チーム

日本語版翻訳－NRIセキュアテクノロジーズ株式会社

NRI　セキュアテクノロジーズは、国内最大の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。 http://www.nri-secure.co.jp

リソース

パスフレーズについて:	https://securingthehuman.sans.org/ouch/2015#april2015
パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2015#october2015
タブレットを安全に使用するには:	https://securingthehuman.sans.org/ouch/2016#january2016
自宅ネットワークをマッピング:	http://l.rud.is/home-network-mapping

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 内山　貴之, 時田　剛