OUCH! | 2014 年1月

コンピュータユーザ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...

- 自宅のワイヤレスネットワーク
- OpenDNS
- 自宅の端末

自宅ネットワークを安全にする

背景

数年前まで自宅ネットワークは単純なものでした。一般家庭では、2-3台のコンピュータとそれを接続するワイヤレスのアクセスポイントがあり、用途はインターネットサーフィンやオンラインゲームでしたが、最近の自宅ネットワークは複雑になってきました。接続する端末が多様化しただけでなく、その用途の幅も広がってきました。今月号では、自宅ネットワークを安全にする基本的な方法について説明します。

ゲストエディター

ケビン・ジョンソン（Kevin Johnson）は、Secure Ideas 社のCEOであり、MySecurityScanner.comの運営者でもあるSANS認定シニアインストラクターです。詳細は、www.secureideas.comを参照してください。

自宅のワイヤレスネットワーク

一般家庭のネットワークは、ワイヤレスネットワーク（Wi-Fiネットワークとも呼ばれます）で構成されており、パソコン、タブレット、ゲームコンソール、テレビ等さまざまな端末がケーブルを使わなくてもインターネットに接続できます。このような環境で必要とされるのが、ワイヤレスアクセスポイントと呼ばれる機器です。この機器がインターネットルーターに接続されていて（インターネットルーターと一体型の場合もあります）、無線で各端末とのやりとりをします。端末がアクセスポイントに接続されると、インターネットに接続されるだけでなく、端末間も接続できる状態になります。つまり、ワイヤレスのアクセスポイントは、自宅ネットワークにおいて接続を集約する重要な役割を果たします。このアクセスポイントを安全にするために以下のような方法を推奨します。

- 多くのワイヤレスアクセスポイントの管理用ログイン名とパスワードは、初期設定ではわかりやすいものに設定されており、インターネットで公開されている場合もあります。まず、この初期設定の管理用ログイン名とパスワードを、独自のものに変更してください。他のサービスで利用しているアカウントのパスワードとは異なるものを選んでください。
- 次ぎに、ワイヤレスネットワークの名称（SSIDとも呼ばれる）の設定をします。周辺のワイヤレスネットワークを検索する際に表示される名前です。わかりやすい名前にしておきましょう。ただし、個人を特定する情報は含めないでください。この設定をする際に、ネットワークを隠す必要はありません。スキルのある攻撃者がワイヤ

自宅ネットワークを安全にする

レス検索ツールを使えば簡単に隠れたネットワークを見つけることができるため、あまり意味がないからです。

- 次は、自宅のワイヤレスネットワークへの接続を信頼できる人に限定し、通信を暗号化します。ワイヤレスアクセスポイントで高度なセキュリティ機能を有効にすることで、他人や近所の人がネットワークに接続できないようにします。現時点で一番よい方法は、WPA2と呼ばれる仕組みを使うことです。WPA2を有効にすると、自宅ネットワークへ接続する際には必ずパスワードが必要になります。接続が認証されると、通信は暗号化されます。WEPなどは古くて時代遅れの仕組みなので使わないでください。セキュリティ機能を有効にしないのは最も避けるべきことです。セキュリティ機能を有効にしていないネットワークは、オープンネットワークと呼ばれ、誰もがネットワークにパスワードなしでアクセスできる状態になります。

自宅ネットワークを安全にするには、ワイヤレスネットワークが安全であることを確認し、OpenDNSなどのサービスを使って各端末が最新の状態であることを確認してください。

- 自宅ネットワークの接続用パスワードは強固なものにし、管理用のパスワードとは異なるものにします。各端末でパスワードを1度入力すると保存されるため、次回に再入力の必要はありません。
- 多くのワイヤレスアクセスポイントにはゲストネットワークと呼ばれる機能があります。ゲストネットワーク機能で訪問者がワイヤレスアクセスポイントに接続してインターネットにアクセスすることができますが、他のネットワークにはアクセスできません。ゲストネットワークを追加する際には、WPA2を有効にして、このネットワークには異なるパスワードを設定してください。
- 複数のパスワードを覚えられない場合には、パスワードマネージャーを使って安全に保管してください。

OpenDNS

ワイヤレスネットワークを設定したら、自宅ネットワークのDNSサーバとしてOpenDNSを利用するように設定してください（同じようなサービスにNorton ConnectSafe for Homeがあります）。ブラウザに名前を入力すると、DNSはインターネット上で接続するサーバを確認します。OpenDNSのサービスは、事前にマルウェアなどに感染しているWebサイトを特定し、自宅のワイヤレスネットワークから誤って接続することを防止します。さらに、好ましくないWebサイトへのアクセスをブロックすることもできます。このサービスの利点はソフトウェアをインストールする必要はなく、ワイヤレスアクセスポイントの設定を変更するだけという点です。

自宅ネットワークを安全にする

自宅の端末

最後のステップは、自宅ネットワークに接続されている端末を把握し、各端末が安全な状態であるかを確認することです。以前は、接続されている端末が数台であったため単純でしたが、現在では自宅ネットワークに接続される端末が多様化しました。テレビ、ゲームコンソール、ベビーモニター、スピーカー、家庭用温度計など様々な種類があり、車が端末になることもあります。自宅ネットワークに接続される端末を改めて確認してみると、その数の多さに驚くでしょう。これらの端末を安全な状態にするには、オペレーティングシステムを最新の状態にしておくことです。可能な限り、自動更新を有効に設定しておいてください。自動更新できない場合は、月に1度のペースで確認しましょう。また、契約しているインターネットプロバイダーのWebサイトにアクセスして、自宅ネットワークを安全にするためのツールが提供されているか確認してみてください。

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

日本語版翻訳ー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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network セキュリティスキャナー:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
パスワードマネージャー:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: Eriko Ban, Yoshihiro Sekitori (NRI SecureTechnologies)