SANS SECURITY AWARENESS
NRI SECURE TECHNOLOGIES
OUCH! | 2018 年 01 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...

- 無線ネットワークについて
- デバイスについて
- パスワードについて
- バックアップについて

自宅を安全なサイバー環境にするには

はじめに

自宅をサイバー的に安全な状態にするのも数年前は簡単でした。多くの家には、無線ネットワークと数台のパソコンが置かれているだけだったからです。現在は、テクノロジーも複雑になり、生活に密着した環境になっているはずです。モバイルデバイスやゲームのほか、温度の自動調節機能があるエアコンや冷蔵庫などがネットワークに接続されているのも珍しくありません。今月のニュースレターでは、自宅のネットワークを安全にするためにできる 4つのステップを紹介します。

ゲストエディタ

マット・ブロマイリー氏は、クライアントの大小に関わらず、データ漏えいなどに関するインシデントレスポンスを行っています。SANS インストラクターとして FOR508 Advanced Digital Forensics and Incident Response を教えているほか、ツイッター (@mbromileyDFIR) でも情報を発信しています。

無線ネットワークについて

多くの自宅のネットワークは、無線 (Wi-Fi) ネットワークで構成されており、このネットワークを使い、様々なデバイスをインターネットに接続しています。多くのネットワークは、ルータやアクセスポイントによって制御されていますが、どちらも、無線によって情報をやり取りすることから、無線ネットワークを保護することが自宅を守ることにつながります。以下のステップを紹介します：

- ルータやアクセスポイントなど、無線ネットワークを管理する際に使用しているデバイスの管理パスワードを、デフォルトのものから変更してください。この管理用アカウントは、無線ネットワークの設定を行うために使われています。
- 自宅の無線ネットワークには、信頼できる人のみ接続を許可してください。そして、セキュリティの強度を上げてください。現在、WPA2 と呼ばれるメカニズムが一番適切です。これを有効にすることで、ネットワークに接続するためにパスワードが必要となり、接続した後は通信が暗号化されます。
- 無線ネットワークに接続するためのパスワードは、強いものを設定してください。また、管理用アカウントのパスワードとは異なるものを設定してください。このパスワードは、それぞれのデバイスで一度だけ入力すれば、デバイスがパスワードを保存してくれるため、いちいち入力する必要は通常ありません。
- 多くの無線ネットワークは、ゲストネットワークを提供する機能を備えています。これは、自宅を訪問した人たちにインターネット接続を提供しながら、ネットワーク内の他のデバイスに接続できないようにすることができます。ゲストネットワークを有効にする場合は、WPA2 を有効にし、固有のパスワードを設定することを忘れないでください。

自宅を安全なサイバー環境にするには

これらのステップについて不明なことがあった場合は、インターネットサービスプロバイダに問い合わせたり、ルータやアクセスポイントに付属している取扱説明書、あるいはデバイスメーカのウェブサイトを確認してみてください。

この 4つのステップに従って、自宅を安全なサイバー環境にしてください： Wi-Fiネットワークを安全にする、自動アップデートを有効にする、固有のパスフレーズを利用する、そしてバックアップを有効にするという流れになります。

デバイスについて

次のステップは、自宅の無線ネットワークに接続されているデバイスを把握し、これらのデバイスが安全な状態であることを確認してください。以前は、パソコンが1、2台だけであったことから簡単な作業でしたが、現在はスマートフォンをはじめとして、テレビ、ゲーム、ベビーモニター、スピーカーおよび車など、ほぼすべての電子機器が自宅のネットワークに接続可能となっています。自宅のネットワークに接続されているデバイスを特定できたら、安全な状態にする必要があります。最良の方法は、自動アップデートの機能を有効にすることです。攻撃者は、様々なデバイスや OS に含まれる脆弱性や、利用できるものを探して攻撃しかけてきます。自動アップデートを有効にすることで、パソコンや各種デバイスは常に最新のソフトウエアで動作することになり、ハッキングが難しくなります。

パスワード

次のステップは、それぞれのデバイスやオンラインアカウントに強い、固有のパスワードを設定することです。ここでのキーワードは、「強い」と「固有」です。記憶することが難しく、入力するのが難しいパスワードにうんざりしていませんか？ そうならないために、パスフレーズを使用してください。パスフレーズは、記憶することが簡単な単語を組み合わせたものです。例えば、“WHERE IS MY COFFEE?” または “SUNSHINE-DOUGHNUTS-HAPPY-LOST”といった一連のフレーズがあるでしょう。いずれにしても、パスフレーズが長ければ長いほど、強固なものになります。固有のパスワードとは、それぞれのデバイスやオンラインアカウントに対して、異なるパスワードを設定することを意味します。こうすることで、一つのパスワードが漏えいしても、他のデバイスやアカウントが危険に晒される可能性を下げることができます。

この強い、固有のパスワードをすべて覚えるのは困難ではないでしょうか？みな同じです。そのため、パスワードマネージャの利用を推奨します。これは、特殊なセキュリティプログラムで、すべてのパスワードを暗号化し、仮想金庫の中に安全な状態で保管してくれるものです。最後に、オンラインアカウントにおいては可能な限り2要素認証を有効にしてください。2要素認証は、通常の認証よりも強力です。従来通りパスワードを使いますが、2ステップ目が追加されることで2要素となります。例えば、スマートフォンに送信されるコードまたはアプ

自宅を安全なサイバー環境にするには

リが生成するコードを使います。2要素認証は、インターネット上において自分を保護するためにできる一番重要なステップであり、考えているよりも容易に有効にできます。

バックアップについて

どんなに気をつけても、ハッキングされることがあります。こうなった場合、個人情報を復旧するにはバックアップから復元する方法しかありません。重要な情報については定期的にバックアップを取得し、復元可能であることも確認してください。多くのモバイルデバイスは、自動的にクラウド上へバックアップする機能を備えています。パソコンの場合も、購入する必要はありますが、安価で利用も簡単なバックアップ用のソフトウエアやサービスが提供されています。

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。
securingthehuman.sans.org/ouch/archives

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、国内でも有数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などの提供を通じて、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/2017#april2017
パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2017#september2017
ログイン情報を保護する:	https://securingthehuman.sans.org/ouch/2017#december2017
バックアップと復旧について:	https://securingthehuman.sans.org/ouch/2017#august2017

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Translated By: 内山　貴之, 時田　剛