OUCH! | 2014 年 10 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...

- はじめに
- 5つの重要なステップ

セキュアに保つための5つのステップ

はじめに

テクノロジーが通常生活の中で重要な役割を担っていく中、複雑さも増しています。テクノロジーが目まぐるしく変化する中、セキュリティに関する様々なアドバイスは混乱を招きます。それは、どうすれば良いか、またはどうしたらいけないのか、といった新たな助言が次から次へと出てくるからでしょう。時が経つにつれ、セキュアでいるための手法の詳細部分は変化していきますが、自身を保護するためにできる基本的な事があります。使用しているテクノロジーと利用場所に関わらず、以下の5つの重要なステップを守ることを推奨します。

ゲストエディター

レニー・ゼルツァー氏は、NCRコーポレーションで、クライアント企業のITシステムのセキュリティ対策や、SANSでマルウェア対策コースのインストラクターです。ツイッター（@lennyzelster）や、blog.zelster.comのブログでも積極的に情報発信をしています。

5つの重要なステップ

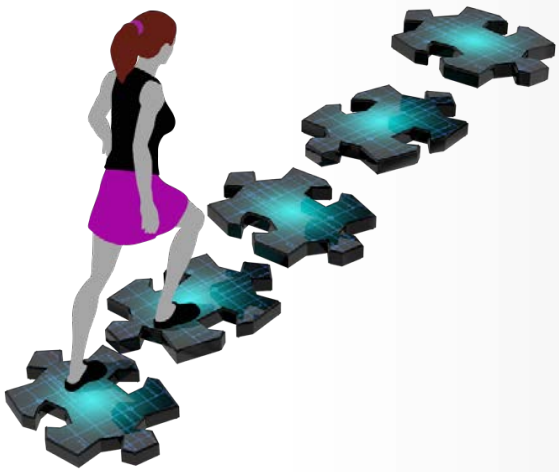
下記に記載する5つのステップは、簡単な概要でしかありません。各ステップの詳細については、本ニュースレターの最後にあるリソースを参照してください。

1. **自分自身**: まず、テクノロジーだけでは、自分自身を守ることができないことを理解してください。攻撃者は、セキュリティテクノロジーを回避する一番簡単な方法は人間を攻撃することであることを理解しています。攻撃者は、パスワードやクレジットカードの情報が欲しいと思った場合、　相手を騙して、これらの情報を提供させるという方法が一番簡単です。例えば、マイクロソフトのテクニカルサポートだと偽って、パソコンが何かに感染したと伝えますが、実際にはサイバー犯罪者がパソコンへのアクセスをしたいだけだったりします。または、郵便物を配達できないと説明をし、住所確認のためにリンクをクリックさせますが、実際には悪意あるサイトにアクセスさせてパソコンをハッキングすることもあります。結局のところ攻撃者に対する最大の防御は自分自身なのです。警戒心を持ち、常識的な考えも併せ持つことで、様々な攻撃を探知し、止めることが可能です。

2. **アップデート**:　パソコン、モバイルデバイス、アプリケーションなどのネットワークに接続可能なデバイスが、常に提供されている最新バージョンのソフトウェアを実行している状態にしてください。サイバー犯罪者は、常にテクノロジーに潜んでいる脆弱性を探しており、弱点などを見つけた場合、特殊なプログラムを使って、脆弱性を突く攻撃を実施し、利用しているテクノロジー、例えばネットワークやパソコン、モバイルデバイスにハッキングをしかけてきます。テクノロジーの開発者も、利用しているテクノロジーが常に最新の状態で保たれるために一生懸命頑

セキュアに保つための5つのステップ

張っています。脆弱性が発見されると開発者は、脆弱性を修正するためのパッチを作成し、このパッチを一般に公開します。それを受けて、システムの管理者は、パソコンやモバイルデバイスにパッチやアップデートを適用し、世の中に知られている脆弱性の数を減らすことで、ハッキングされる確率を低くすることに取り組んでいるのです。最新の状態を保つために、自動更新の機能がある場合は、この機能を有効にしてください。このルールは、インターネット接続可能なテレビ、ベビーモニター、ホームネットワークルータ、ゲーム機、果ては果ては自動車などのネットワークに接続可能なすべてのテクノロジーに適用できます。パソコンのオペレーティングシステム、モバイルデバイスなどサポート終了してしまい、アップデートが提供されない場合、サポートされているバージョンに移行することを推奨します。



この五つのステップを守ることで、最新のテクノロジーを駆使しながら、ある程度、自分を守ることが可能です。

3. **パスワード**:　自分自身を守るための次のステップは、強度があり、且つ固有のパスワードをそれぞれのデバイス、オンラインアカウントおよびアプリケーションで設定することです。ここで重要なのは、「強度がある」と「固有の」です。強度があるパスワードとは、ハッカーが使用する自動的にパスワードを解析するツールなどで簡単に探し当てることができないもののことです。一つの単語だけを使用するのではなく、複数の単語と記号や数字を含むパスフレーズを使用してください。固有のパスワードとは、それぞれのデバイスおよびオンラインアカウントで異なるパスワードを使用することを指しています。このような運用をすることで、一つのパスワードが漏えいしても、他のアカウントやデバイスは安全なままです。強度があって、異なるすべてのパスワードを記憶するのは大変だと思いますし、我々もすべてを把握しきれません。なので、パスワード管理ソフトウェアを利用すること推奨しています。このソフトウェアは、スマートフォンやパソコン用のアプリケーションで、すべてのパスワードを暗号化した状態で保存するものです。最後に、アカウントの中で2段階認証をサポートしているものがあれば、有効にすることを強く推奨しています。この手法は、アカウントを守るための手法としては他の手法と比べて強いものです。

4. **暗号化**:　3つ目のステップは、暗号の利用です。暗号は、自分および信頼できる人たちのみがデータにアクセス可能な状態を作ることができます。データは、2つの状態で暗号化可能で、それは保存されている状態と通信が行われている状態です。保存されている状態のデータを暗号化することは、ハードディスクや USB などの記憶媒体のファイルを保護することを指します。多くのオペレーティングシステムは、Full Disk Encryption などの機能を有していて、すべてのデータを自動的に暗号化します。この機能が存在する場合、有効にすることを推奨します。通信が行われている状態での暗号化は、自身のパソコンまたはデバイスから他人にデータを送る際に暗号化を行なうことを指します。例としては、オンラインバンキングを利用している時です。インターネットを利用している際に暗号化

セキュアに保つための5つのステップ

が有効になっているかを確かめる方法としては、ブラウザのアドレスバーで、閲覧しているサイトのアドレスが、「HTTPS」で始まることを確認し、南京錠の画像が隣にあることも確認してください。

5. **バックアップ**: どんなに気をつけていても、デバイスまたはアカウントが乗っ取られることがあります。このような場合、パソコンやモバイルデバイスがマルウェアに感染していないことを保証するには、初期化を行い、初期設定に戻すしか方法はありません。攻撃者の中には、個人情報やファイル、写真など、デバイスに保存されている情報にアクセスできないようにする場合があります。このような場合は、バックアップから個人情報を復元するしか復旧の方法ありません。重要な情報は定期的にバックアップを行い、このバックアップからデバイスを復元可能なことを確認してください。多くの OS やモバイル機器デバイス動バックアップ機能を有しています。

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。
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

E-mail を使ったフィッシング攻撃:	http://www.securingthehuman.org/ouch/2013#february2013
タブレットをセキュアに保つために:	http://www.securingthehuman.org/ouch/2013#december2013
強固なパスワードとは:	http://www.securingthehuman.org/ouch/2013#may2013
パスワード管理ツール:	http://www.securingthehuman.org/ouch/2013#october2013
２段階認証:	http://www.securingthehuman.org/ouch/2013#august2013
暗号化:	http://www.securingthehuman.org/ouch/2014#august2014
バックアップについて:	http://www.securingthehuman.org/ouch/2013#september2013