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...

- 自分自身
- パスワード
- アップデート
- バックアップ

安全を保つための4つのステップ

はじめに

テクノロジーは、生活する上で重要な役割を担う中、さらに複雑になっています。そのため、テクノロジーが目まぐるしく変化する中で、セキュリティに関するアドバイスはあなたの混乱を招くかもしれません。同時に、やるべき事と、やるべきでない事に関して常に新しいガイダンスが出ています。しかし、セキュリティを保つための細かい事項は、時とともに変わるかもしれませんが、自分自身を守るためにできる基本的な対策は存在します。どのようなテクノロジーをどこで使用していても、以下に記載する4つのステップを採用することを推奨します。さらなる詳細に関しては、本ニュースレター末尾のリソースに記載されているリンクを参照してください。

ゲストエディター

ライアン・ジョンソン氏は、企業で発生する不正アクセスを適切に対応するための準備を事前に整えることに注力しています。SANS Institute では、Advanced Network Forensics コースの講師でもあります。また、ツイッター(@ForensicRJ) でも積極的に情報を発信しています。

1. 自分自身

覚えておかなければならない一番重要な事は、テクノロジーだけでは自分自身を守れないということです。攻撃者たちは、最新のセキュリティテクノロジーを回避するための最良の方法は、ユーザ、つまりあなたを攻撃する事だと学んでいます。攻撃者は、パスワード、クレジットカード番号または個人情報が欲しいと思ったら、入手する一番簡単な方法は、騙して暴露させることです。例えば、マイクロソフトのテクニカルサポートと偽って電話をかけ、パソコンがウイルスに感染していると言ってきます。しかし、これはパソコンに対するアクセス権を入手するための手法です。また、メールを送り、荷物を届けることができなったため、住所を確認するためにリンクをクリックさせようとします。このリンクをクリックすると悪意あるウエブサイトに接続し、パソコンが攻撃を受けてしまいます。このようにして、ランサムウエアやCEO詐欺の攻撃が開始されます。最終的に、攻撃者に対する最大の防御策は、自分自身なのです。常に疑いを持って下さい。一般常識を駆使することで、多くの攻撃を見つけ、止めることが可能です。

2. パスワード

自分自身を守るためにできる次のことは、すべてのデバイスやオンライン上のアカウントに対し、一意の強いパスワードを設定することです。ここで重要なのは、「一意の」と「強い」ということです。強いパスワードを設定することで、攻撃者が推測しにくくなるだけでなく、自動ツールを使った攻撃にも耐性を持たせることができます。複雑で覚えるのが難しいだけでなく、打ちづらいパスワードに疲れていませんか？この場合、パスフレーズを使ってみてください。一

安全を保つための4つのステップ

つの単語だけでなく、簡単に覚えられる複数の単語を使ってください。例えば、「WHERE IS MY COFFEE?」のような感じです。パスフレーズが長ければ長いほど、強度は増します。一意のパスワードを使うということは、すべてのデバイス、すべてのオンラインアカウントで異なるパスワードを設定することです。こうすることで、一つのパスワードが漏えいしても、他のアカウントやデバイスの安全が保たれます。でもすべての強い、一意のパスワードを覚えられますか？安心してください。そのためにパスワードマネージャと呼ばれるソフトウエアを使うことを推奨しており、誰も覚えるように助言はしていません。このソフトウエアは、パソコンやスマートフォン上で利用することができるもので、暗号化した状態ですべてのパスワードを保管してくれる便利なものです。

この4つのステップを守ることで、あなた自身を守りつつ、最新のテクノロジーを活用することができるでしょう。

どのようなアカウントでも安全にするためにできる最後の手段は、2段階認証を使うことです。パスワードだけでは、アカウントを守ることはできません。そのため、さらに強力な手段が必要です。2段階認証は、強力な手段です。自分自身が設定したパスワードも使いますが、生体情報(バイオメトリクス)や所持情報(スマートフォンに送信されるコードまたはスマートフォンアプリが生成するコード)という2段階目を認証の要素として追加するものです。パスワードマネージャも含め、利用しているすべてのアカウントで2段階認証を有効にしてください。2段階認証を有効にすることは、自分自身を守るためにできる最大の対策であり、活用もそれほど難しくはありません。

3. アップデート

インターネットに接続しているパソコン、モバイルデバイス、アプリなどが最新のバージョンになるように心がけてください。サイバー犯罪者は、日頃からデバイスで利用しているソフトウエアに含まれる新たな脆弱性を探しています。脆弱性を発見すると、特殊なプログラムを使って攻撃を行い、デバイスに攻撃をしかけます。その傍らで、ソフトウエアの開発者は、日頃から脆弱性を対策するためのアップデートを提供しているのです。これらのアップデートを適用することで、攻撃者はあなたが普段利用しているパソコンやモバイルデバイスを攻撃しにくくなります。常に最新版を利用するために、自動更新の機能がある場合は、有効にしてください。これは、インターネットに接続されているすべてのデバイスに対して行ってください。例えば、インターネットに接続されている、テレビ、ベビーモニター、ホームルータ、ゲーム機がこれらにあたり、いずれ車も対象になることでしょう。利用しているオペレーティングシステムやデバイスが古く、セキュリティアップデートの対象外の場合は、サポートされている新しいデバイスに買い替えることをお勧めします。

安全を保つための4つのステップ

4. バックアップ

どんなに気をつけても時には、攻撃に遭う可能性はあります。この場合は、パソコンまたはモバイルデバイスから完全にマルウエアを削除するためには、デバイスを初期化することしか方法はありません。攻撃者は、個人用のファイルや画像、その他の保存されているファイルへのアクセスを拒否するようにしてしまうかもしれません。個人用のファイルを復元するためには、バックアップから復元するしか方法はありません。定期的に重要なファイルや情報のバックアップを取り、そのバックアップから情報の復元が可能であることを確認してください。現在、多くのオペレーティングシステムやモバイルデバイスは、自動バックアップの機能をサポートしています。最後になりますが、バックアップは、サイバー犯罪者から保護するためにクラウドまたはオフラインに保存することをお勧めします。

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

フィッシングについて:	https://securingthehuman.sans.org/ouch/2015#december2015
パスワードマネージャ:	https://securingthehuman.sans.org/ouch/2015#october2015
2段階認証について:	https://securingthehuman.sans.org/ouch/2015#september2015
パスフレーズについて:	https://securingthehuman.sans.org/ouch/2015#april2015
バックアップと復旧:	https://securingthehuman.sans.org/ouch/2015#august2015