SANS SECURITY AWARENESS

OUCH!

月間セキュリティ啓発ニュースレター

セキュリティを維持するシンプルな4ステップ

概要

テクノロジーを安全かつ最大限に活用することは、時にさまざまな情報に圧倒されて混乱を招く可能性があります。でも、安心してください！使用しているテクノロジーや使用方法にかかわらず、セキュリティの維持に役立つ4つの簡単な手順をご紹介します。

1．落ち着いて考える：何よりもまず、テクノロジーだけでは完全に保護することはできないことを理解してください。攻撃者が最も簡単に欲しいものを手に入れる方法は、攻撃の対象をコンピュータやスマートフォンなどのデバイスではなく、あなたにすることだと色々なところで聞いているはずです。　パスワードやクレジットカード、またはコンピュータの操作をさせたい場合、たいていは緊急性を高めるような連絡を通じてユーザーを騙すことで必要な情報を奪取しようとします。たとえば、マイクロソフトのテクニカルサポートを装って、「コンピュータが感染している」と電話で報告してくる場合があるかもしれませんが、実際は、コンピュータへのアクセスを企図しているサイバー犯罪者にすぎません。あるいは、あなた宛の荷物の不在配達に関するメールに、「本人確認などでメールアドレスを認証する必要があるため」と称してリンクをクリックするように誘導してくるかもしれませんが、このパターンもあなたのコンピュータを攻撃するため悪意のあるWebサイトにアクセスするようにしているのです。究極的な言い方をすると、攻撃者に対する最大の防御はあなた自身です。込み入った状況であっても、落ち着いて物事をとらえ、常識で考えれば、多くの攻撃やその前段階の兆候を発見し、被害の拡大を抑えることができるようになります。

2．パスフレーズ：コンピューティング能力の飛躍的な向上によって、古い8文字のパスワードは脆弱になっています。さまざまなサービスなどでパスワードの作成を促された場合は、これらの古いパスワードではなく、強力なパスフレーズを一意に作成してください。パスフレーズは、「ミツバチの蜂蜜とバーボンの雨」など、あなたにとって覚えやすい一連の文章を使用するパスワードの一種であり、一般的にパスワードは長いほど強力になりますが、単純に長いパスワードを考えるのはとても苦痛なので、覚えやすい短文をパスワードとして使ったものです。また、ここで言う一意のパスフレーズとは、デバイスやオンラインアカウントごとに異なるパスフレーズを使用することを意味しています。これにより、1つのパスフレーズが侵害されても、ほかのすべてのアカウントとデバイスの安全を保つことができます。これらのパスフレーズをすべて覚えることが難しい場合、パスワードマネージャーを使用することも検討してください。パスワードマ

ネージャーは、すべてのパスフレーズを暗号化した形で安全に格納する専用のプログラムです（ほかにも優れた特徴が多数あります）。

最後に、二段階認証機能も有効にしてください。これは、ツーファクター認証、あるいはマルチファクター認証とも呼ばれることがあります。この仕組みを採用すると、パスワードを使うだけでなく、別の認証用に作られたコードをスマートフォンに送信したり、コードを生成したりする専用のアプリを使うことで、認証に使われる手順を2段階にすることができます。2段階認証は、オンラインアカウントを保護する上でおそらく最も重要な手順であり、あなたが想像しているよりもはるかに簡単に設定して使用できます。

3．アップデート：コンピュータやモバイルデバイス、プログラム、およびアプリケーションが最新バージョンのソフトウェアを実行していることを確認するようにしてください。攻撃者は、ソフトウェアの新しい脆弱性を常に探しています。 そして、あなたが使用しているコンピュータやデバイスに存在する 脆弱性を発見すると、特別なプログラムを使用して脆弱性を悪用し、使用しているモバイルデバイスを攻略しようと試みます。 一方、これらのソフトウェアを開発した企業は、アップデートをリリースして修正する作業に日夜懸命に取り組んでいます。これらの更新プログラムを迅速にインストールするようにすれば、攻撃者からハッキングされる可能性を低くすることができます。そのため、コンピュータやデバイスの状態を最新にして維持するには、可能な限り自動更新を有効にしてください。このルールは、インターネットに接続されたテレビやセキュリティカメラ、家庭用のルーター、そしてゲーム機や自動車など、ネットワークに接続されたほとんどすべてのデバイスに適用することができます。

4．バックアップとリカバリ：どんなに気をつけていても、攻撃者によってハッキングされる可能性はゼロではありません。そのような場合に備えて、すべての個人情報を復元する唯一の方法であるバックアップも準備してください。そして、重要な情報は定期的にバックアップを取得し、バックアップデータからデータを復元できることを確認するようにしてください。ほとんどのオペレーティングシステムやモバイルデバイスは、外部ドライブやクラウドへの自動バックアップ機能を搭載しています。

ゲストエディタ

SANS Certified InstructorのSteve Anson氏は、世界中のITセキュリティチームや政府に対して、セキュリティ体制を改善するためのコンサルティングなどを行っています。彼はApplied Incident Responseの著者であるほか、ITセキュリティの実務担当者向けにwww.AppliedIncidentResponse.comにおいてさまざまなリソースを提供しています。

リソース

ソーシャル・エンジニアリング:	https://www.sans.org/u/W3G
パーソナライズされた詐欺:	https://www.sans.org/u/W3Q
パスワードを簡単にする:	https://www.sans.org/u/W3V
バックアップを取得しました:	https://www.sans.org/u/W40

 Editorial Board: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Translated by: 小山 裕之, 時田　剛