OUCH! | 2015 年 09 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
・パスワードについて
・2段階認証について
・2段階認証の利用方法

2段階認証について

はじめに

自分が自分であることを証明するプロセス（認証と呼ばれている）は、自分に関する情報を守るために重要です。強い認証とは、メール、画像や銀行口座などの自身に関わる機微な情報に対し、自分しかアクセスできないように制限することです。自分が自分であることを証明するには、3つの方法があります　①何を知っているかー例えばパスワード、②何を持っているかー例えば運転免許、③自分が何かー例えば指紋が挙げられます。これらの方法には、それぞれ利点と欠点があります。一般的に良く利用されるのは、何を知っているか、つまりパスワードです。このニュースレターでは、2段階認証を活用して自分を守る方法をお教えします。これは、パスワードだけを利用するよりもはるかに安全なだけでなく、活用も容易です。2段階認証を正しく理解するには、まずパスワードについて触れなければなりません。

ゲストエディター

キース・パームグレン氏は、30年以上もの間、情報セキュリティ業界で活躍しています。SANS　Instituteの認定講師であり、SANS SEC301 の著者でもあります。このコースは、情報セキュリティの基本を5日間で学ぶものですが、講師を担当していない時は、コンサルティングや執筆活動などを行っています。@kpalmgren からキースをフォローすることができます。

パスワードについて

パスワードは、自分が知っていることを基にして、自分が自分であることを証明するものです。そのためパスワードの危険性は、単一障害点になり得ます。つまり、パスワードを推測されたり、パスワードを第三者に取得されたりしてしまうと、自分自身になりすまされ、そのパスワードによって保護されているすべての情報にアクセスできてしまうということです。このような事態を防ぐために、パスワードを守るための手法を学んだりしますが、推測されにくいパスワードを設定したり、各アカウントで違うパスワードを設定したり、パスワードを第三者に教えない、などがあるでしょう。これらのアドバイスは、今でも有効ですが、パスワードだけでは限界があり、特にこの時代においては、パスワードだけでは、情報を守り切れないのです。最新のテクノロジーを使うと、サイバー攻撃者によって比較的容易にパスワードを取得されてしまいます。今、必要なのは簡単に利用でき、かつ強い認証を提供する手法なのです。幸いにも、一般的に利用可能で、これらの要求を満たす2段階認証と呼ばれる手法があります。

2段階認証について

2段階認証（または、2要素認証、2FA）は、パスワードだけを利用するよりも安全です。1つでなく、2つの手法を使い、自分が自分であることを証明するというものです。一例として、ATMカードがあります。ATMを利用する際、実は2段階認証を使用しています。ATMからお金を下ろす際には、2つのものが必要です。1つ目は、ATMカード（持っているもの）、2つ目

2段階認証について

は、暗証番号（知っているもの）です。ATMカードを紛失しても、お金は安全です。カードを拾われてしまっても、暗証番号を知らない限り、（暗証番号をカードに書いてある場合は別です！　これは良いアイデアではありません。）第三者がお金を下ろすことはできません。また、暗証番号を知っていても、カードを持っていない状態でも同じことです。攻撃者は、二つの情報を揃えないと、口座に対して操作を行うことができません。2段階認証がより安全である理由、2段階認証のセキュリティは、ここにあるのです。

2段階認証が利用可能な時はぜひ利用してください。自分自身の情報を守るために利用できる強力な手法です。

2段階認証の利用方法

2段階認証は、それぞれのアカウントで個別に設定するものです。幸いにも多くのオンラインサービスは、2段階認証の機能を提供しています。2段階認証を率先して提供した企業の中に グーグル があります。グーグルのアカウントは、サイバー攻撃者から頻繁に狙われています。なぜなら、無料で多くのオンラインサービスを提供しており、世界中に利用者が多くいるからです。そのため、グーグルは、強い認証を提供する必要があり、オンラインサービスで 2段階認証を提供したのは、数多ある企業の中でも早かったと言えるでしょう。グーグルの2段階認証がどのように機能しているかを理解するだけで、他のサイト、例えば、ツイッター、フェイスブック、アップル、インスタグラムや多くの銀行サイトが提供する 2段階認証の機能を理解することができます。

まず、グーグルのアカウントで2段階認証を有効にしてから、携帯電話の番号を登録します。この手続きが完了すると、2段階認証は、以下のように機能します。はじめに通常通りユーザ名とパスワードを使ってログインを行います。これは、必要な2要素のうち、1つ目ー知っているものーです。しばらくすると、グーグルから携帯電話にテキストメッセージが届きます。このメッセージには、固有のコードが含まれており、6桁の数字となっています。ユーザは、パスワードと同様に、この 6桁の数字をウェブサイトに入力します。これが、2要素目になります。アカウントにログインするためには、パスワードを知っているだけでなく、固有のコードを受信するために携帯電話を持っている必要があります。攻撃者がアカウントのパスワードを知っていても、自身の携帯電話を持っていない限り、グーグルのアカウントにログインできません。アカウントをより安全にするため、グーグルは、ログインの度に別の固有のコードを送るようになっています。

グーグルや他の多くのサイトで利用可能な　2段階認証の方法が他にもあります。SMSテキストメッセージで固有のコードを受信する代わりに、スマートフォンに認証用のアプリをインストールして利用することです。このアプリは、ログインしたい時に、毎回固有のコードを生成してくれます。このモバイルアプリの利点は、電話回線に繋がっていなくても

2段階認証について

利用できることであり、電話自身がコードを生成してくれます。また、コードは電話に送られるのではなく、電話内で生成されるため、通信傍受といった盗聴被害に遭うこともありません。

注意すべきことは、2段階認証はデフォルトで有効になっていないシステムが存在することです。そのため、自身で有効にしなければなりません。最初のうちは、2段階認証が煩わしいと感じることがあるかもしれませんが、利用できるのであれば2段階認証の利用を強く推奨します。特に重要なサービス、メールアカウント、オンラインバンキングやオンラインストレージで適用すると良いでしょう。2段階認証は、パスワードを単体で利用するよりも、情報を第三者に窃取される確率を減らせることができます。

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

パスフレーズについて:	http://www.securingthehuman.org/ouch/2015#april2015
2段階認証をサポートしているサイト集:	https://twofactorauth.org
Stop! Think! Connect!:	http://stopthinkconnect.org/2stepsahead
グーグルの2段階認証:	http://www.google.com/landing/2step/
本日のワンポイントアドバイス:	http://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 内山　貴之, 時田　剛