リモートワークとネット詐欺

企業はITセキュリティに少なからずの投資をしています。

ファイアウォール、ウィルスやマルウェアのスキャン、セキュリティが強化されたサーバー、エアギャップで守られているシステム、さらには個人によるベストプラクティスの指導などのすべてが重要なインフラを外部からの絶え間ない攻撃の脅威から守るために役立っています。銀行、法律事務所、国家安全保障機関などの有名な機関では、これらの対策が不可欠であると考え、特定の在宅勤務を禁止している組織も存在します。

コロナウィルスの隔離期間中、従業員が在宅でのリモートワークを行うことで、これらのルールの多くは廃れてしまいました。法律事務所のMintz Levin氏は、National Law Review3月号の記事で、次のようなリスクがあることを指摘しています。国ごとに検疫が行われている状況を見て、彼らは「COVID-19の人から人への拡散を遅らせるためには、リモートワークの取り決めが有効であるかもしれないが、オンプレミスの仕事とは異なるサイバーセキュリティ上の課題がある」と述べています。これらの課題は現在も存在しており、理想的な状況とは程遠いものです。

By Yoav Keren, BrandShield CEO

Apr 2020

課題1：

オフィス外でのコミュニケーション

攻撃は既に実行されている

普段の仕事においても、経営陣から末端の従業員まで、組織の最大の弱点は「人」です。ハッカーは、ソーシャルメディアの不正アカウント、偽装されたウェブページ、オンライン・フィッシングなどの詐欺行為によって、ヒューマンエラーを利用しようとしますが、これらの詐欺行為は、オフィスにいるときも、外出しているときも、従業員を標的にします。ある著名なハッカーグループは、出張中のホテルにいる従業員だけをターゲットにして、リモートワークを利用してデータを盗むことで知られています。

これらの攻撃は衰えてはおらず、セキュリティ専門家は、コロナウィルスの隔離をきっかけに、新しい種類の詐欺を発見しました。その多くは、セキュリティが確保されていない自宅環境からオフィスのシステムにログインするという、セキュリティ上の課題を利用しています。在宅勤務にはさまざまな課題がありますが、その中でも4つの課題を紹介しましょう。

リモートワーカーは、コロナウィルスの隔離期間中、これまでにないほど非同期通信に依存するようになりました。彼らは、ウェブポータルを介して仕事にアクセスし、しばしば電子メールやソーシャルメディアで集中的にコミュニケーションをとっています。しかし一方で、企業のセキュリティシステムにとって最も重要な要素の1つは、そのシステムに対する従業員の警戒心です。
従業員は、ソーシャルメディアや電子メールなど、受信するメッセージの数がこれまで以上に増えている中で、それらを精査する必要があります。さらに言えば、通常の状況下では、機密情報を要求するメッセージや未承諾の添付ファイルを送るメッセージを疑うことができるでしょう。しかし、世界中の人々が自宅で仕事をするようになった今、機密情報は完全に受信箱を経由して移動し、多くの従業員は最新情報や職場のアナウンスを企業のソーシャルメディアに依存しています。

一方、スタッフは毎朝起きて会社のVPNにログインし、コーヒーを入れたり、ニュースをチェックしたり、子供から目を離さないようにしたりしながら、新しいルーチンをマルチタスクでこなしています。ロゴやレイアウトが適切に配置されていれば、毎日ログインしている社員のうち、少なくとも数人は、URLが重要な「https」ではなく「http」で始まっていることに気づかないという事実を、ハッカーは計算に入れているのです。

課題2:

ウェブポータル

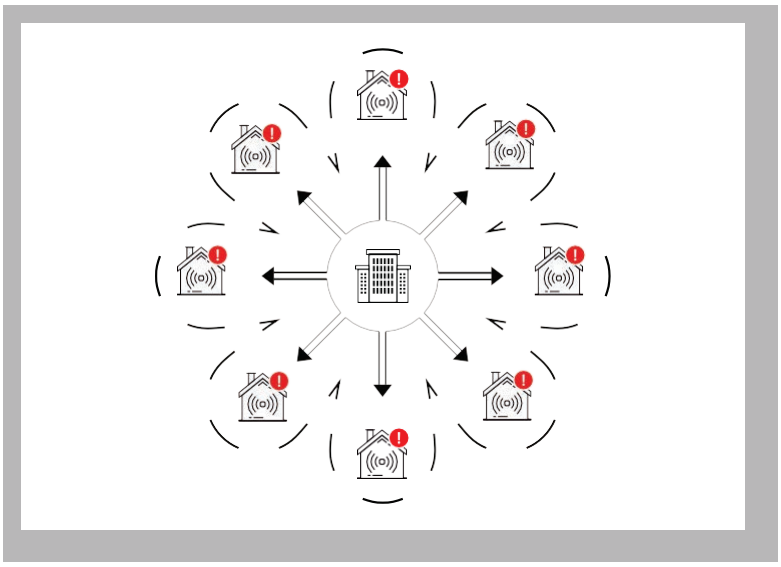
コロナウィルスをきっかけに、ウェブ会議が日常化し、「Zoomする」という動詞も生まれました。かつてはニッチだったこのビデオチャット会社ほどの成功と成長を遂げた企業はあのAmazonですらなかったでしょう。

その成長にはリスクも伴います。

ビデオチャットなどの遠隔コミュニケーションツールの多くは、必ずしもセキュリティを考慮して作られているわけではありません。オフィスでは、コラボレーションとシームレスなコミュニケーションを重視しているため、これらのスイートを使用していますが、情報の伝達が容易であるため、ハッカーにとってはチャンスでもあります。

今では、会社のリーダー、企業グループ、顧客担当のPRチームなどを名乗る相手からのミーティングへの招待状など、偽のリンクが蔓延しています。また、ハッカーや単なる破壊者が、企業イベントへの正当なリンクを手に入れてしまう場合もあります。特に「Zoom爆弾」の問題は、隔離期間中の有名な現象となっています。このような破壊行為では、個人がリンクを手に入れて、プライベートなビデオ通話に参加します。不適切な映像を流したり、仕事に支障をきたすような行動をとることも少なくありません。時には、裏に潜んで機密情報を集めようとすることもあります。

最悪の場合、顧客や取引先の前で恥ずかしい思いをしたまま、再起を図ることになるかもしれません。最悪の場合、その内部資料がどのようにして公開されたのかを考えなければならないかもしれません。



課題3:

オフィス外のネットワーク

従業員全員をオフィスの外に移動させると問題が生じます。Jones Dayのセキュリティ対策チームが指摘するように、企業のITスタッフは、ソーシャルディスタンスをとることで、すでに能力が低下しているにもかかわらず、さまざまなニーズに注意を払わなければならなくなっています。

同時に、従業員は、はるかに脆弱な環境でビジネスを行うようになりました。ホームネットワークには、オフィス環境のようなファイアウォールやセキュリティ層がなく、攻撃を受けても安全性を確保することができません。

ユーザーが悪意のあるファイルをダウンロードしたり、スピアフィッシングサイトに情報を入力したりしても、オフィスのネットワークは自らを守ることができます。基本的なルーターでは無理です。つまりハッカーにとっては、ホームネットワークが格好の標的になっているということです。強化された企業のシステムに詐欺的に侵入するのではなく、ほとんど保護されていない個人のネットワークを乗っ取ることができるのです。サーバーはリモートログインを期待しており、法務チームのメンバーと、その従業員の無線ネットワークを自分専用のVPNとして使用しているハッカーとの区別がつかないかもしれません。

課題4:
パーソナルデバイス

個人所有のノートパソコンを子供に使わせている社員はどれくらいいるでしょうか。ダウンロードしたファイルや閲覧したウェブサイトに無頓着な人はどれくらいいるでしょうか。ウィルス対策やマルウェア対策を最新の状態に保っている人はどれくらいいるでしょうか。アップデートを促すポップアップボックスをクリックしない人はどれくらいいるでしょうか。

ITチームがオフィスのハードウェアとソフトウェアに注意を払うのには理由があります。

専用のノートPCなどを社員に持たせている企業もありますが、現在では多くの社員が個人のPCやスマートフォンを使ってリモートワークを行っています。これらのデバイスには、桁違いに多くのセキュリティ上の問題があり、ITチームは、現在ネットワークにログオンしているすべてのラップトップを物理的に検査し、オーバーホールしなければ、これらの問題に対処することができません。これはお勧めできません。

個人所有のデバイスは、あなたのワークスペースに深刻なリスクをもたらします。ホームネットワークと同様に、ハッカーが従業員を騙して悪意のあるソフトウェアをコンピュータにインストールした場合に、お客様の情報を保護する技術的なセキュリティ層がありません。さらに悪いことに、潜在的な脆弱性のポイントが多くあります。

専用のオフィス環境では、従業員が個人的な仕事をすることがありますが、仕事上のデータを処理する同じマシンが、個人的な行為もすべて処理してしまうのです。ハッカーは、会社のウェブサイトを改ざんしたり、同僚を装って攻撃したりするだけでなく、技術サポートのツイッターアカウントを偽装したり、「昔の友人」からのFacebookのメッセージを偽装したり、ダウンタイムに従業員のコンピュータを乗っ取るマルウェアをダウンロードしたりして、従業員を攻撃します。

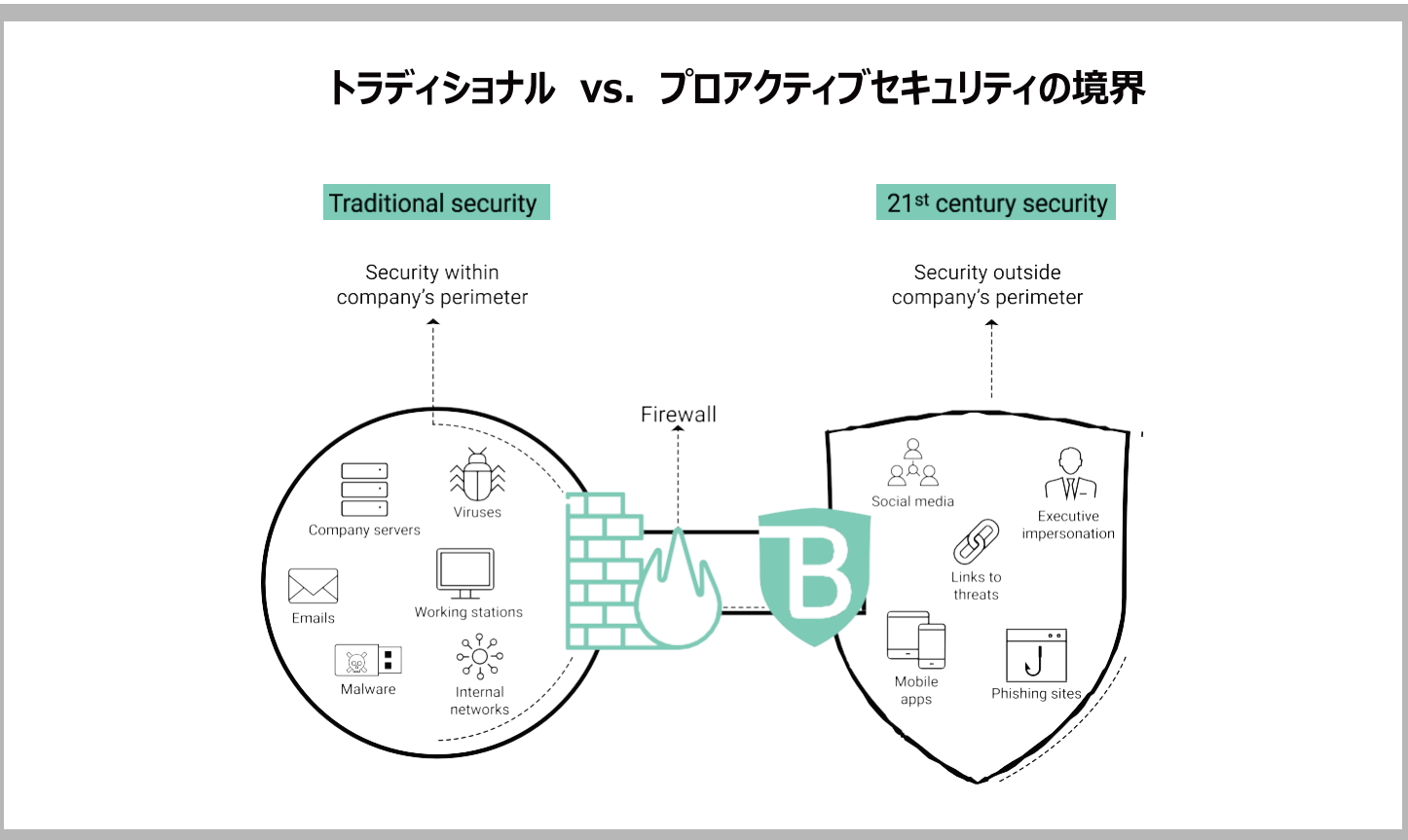
さらに、キーロガーを知らず知らずのうちにインストールしてしまうと、企業のサーバーにログオンしている間に書いた機密情報を一言一句漏らさず記録してしまうことになります。

最良の防御は優れたオフェンス

実際のところ、このような環境でお客様の情報を安全に保つために、ITチームができることは限られています。日々のサービスに対するユーザーの要望に応えようとしている時に、その脅威は急速に迫ってきています。

むしろ、分散した職場環境で情報を保護するための最善の方法の一つは、外に目を向けることです。従業員は世界中、インターネット上に散らばっており、そこに注意を払わなければなりません。企業ブランドやプレゼンスを模倣したウェブサイトを作成しようとしていないか、特に社内のログイン画面を複製しようとしていないか、注意して確認してください。自社のイントラネットやVPNのログインアドレスに似たURL文字列がないか、簡単なタイプミスがないか、企業ロゴや商標、スローガンなどの識別情報が使われていないかを常に監視します。

同時に、ソーシャルメディアサイトを監視し、自社やそのブランドを模倣したプロフィールがないかを確認します。公式発表を謳っているアカウントや、従業員や顧客を対象としたアカウントを探し、実質的に類似したユーザー名、ブランド名、イメージ、商標、企業スローガンを再度検索します。



最後に、従業員の日常生活に注意を払うよう訓練してください。

共感と強調：多くの人が仕事と家庭を両立させなければならない今の状況に共感すると同時に、現在の環境ではさらなる注意が必要であることを強調する必要があります。イントラネットのログイン画面など、重要なウェブサイトへのダイレクトリンクを配布し、URLを記憶して入力するのではなく、公式リンクをクリックしてアクセスするように促します。そして、定期的にベスト・プラクティスを従業員に伝えてください。

IT部門が何週間も前に送ったメールを従業員が忘れてしまったときに、イライラしても仕方がないでしょう。

しかし、私たちBrandShieldはそのお手伝いをすることができます。当社の専門家チームは、ウェブ上でお客様のアイデンティティを保護してきた7年以上の経験を持っています。ソーシャルメディア上でIDを盗用したり、企業のウェブサイトを複製したりするなど、オンライン上の偽造者を検出します。そして、ドメインレジストラ、ウェブホスト、ソーシャルメディア企業、オンラインマーケットプレイスと協力して、不正行為を取り締まっています。

攻撃を阻止する最善の方法は、攻撃が始まる前にあります。私たちは、従業員が偽のイントラネット・ログインを発見する前に、その偽のイントラネット・ログインを確実に見つけることができるように支援します。

※本ドキュメントは株式会社アズジェントが自動翻訳システムを利用して翻訳したものです。
原文は英語であり，この訳文はオフィシャルなものではありません。