"はかる"技術で未来を創る
東陽テクニカ

TOYO Technical Magazine
Webページで公開中!
https://www.toyo.co.jp/magazine/

TOYO Technical Magazine No.33 2022.06
デジタルツイン、Beyond 5G、サイバーセキュリティ
—DX・次世代インフラを支えるテクノロジートレンド

スペシャルコンテンツ Interview

DX時代のセキュリティ教育 —「人」を最後の砦として サイバー攻撃から企業を守る

株式会社東陽テクニカ
情報通信システムソリューション部
次長
大柳 誠一郎

はじめに

新型コロナウイルス感染症の流行がもたらした変化のひとつに、企業のテレワーク推進が挙げられます。従業員がそれぞれ異なる場所で勤務する機会が増え、「人」を狙ったサイバー攻撃もさらに増加しています。企業の情報を守るためには、テクノロジーを活用した対策ももちろん必要ですが、「人」が最後の砦となってサイバー攻撃を防ぐことがより重要となります。DX推進のこの時代に、「人」を教育して巧妙化するサイバー攻撃から企業や個人を守る、というのは一見すると相反することのように思えるかもしれません。

本稿では、情報を守るために何が必要か、「人」を最後の砦とするセキュリティ教育とは何か、その疑問に、株式会社東陽テクニカ 情報通信システムソリューション部 次長 大柳誠一郎がお答えいたします。また、2022年2月に当社が開催した「セキュリティ意識向上セミナー」で特別講師を務めた、 世界的に有名な伝説のハッカーKevin Mitnick(ケビン・ミトニック)氏の、近年のサイバー攻撃の特徴や、これに対抗するための方法についてのコメントもご紹介いたします。

今、必要なセキュリティ教育とは —意識を向上させて維持する

まず、情報セキュリティとは何か教えてください。

情報セキュリティとは、重要な資産である情報を「機密性(Confidentiality)」、「完全性(Integrity)」、「可用性(Availability)」に関する脅威から、保護することです。それぞれの頭文字をとって情報セキュリティの3要素を「CIA」と呼んでいます。

機密性とは、許可された人だけがアクセスできることを指します。ITシステムの機密性が高いかどうかは、ペネトレーションテスト(侵入テスト)を実施して診断します。完全性は、情報の改ざんや破壊が行われておらず、内容が正しい状態にあることです。可用性は、障害が発生しにくいこと、もし障害が発生しても復旧までの時間が短い状態を指します。

図1:情報セキュリティの3要素

では、情報セキュリティを脅かすものは何でしょうか。

情報セキュリティの脅威にも3要素あり、「人的脅威」、「技術的脅威」、「物理的脅威」が挙げられます。人的脅威は、従業員の不正や、偶発的な誤りで発生してしまう脅威のこと。原因は従業員の情報セキュリティに対する意識の低さにあります。一方、技術的脅威は、マルウェアなどに感染して情報漏洩が起こる脅威で、物理的脅威は、災害などを原因とするシステム停止などによる情報破壊の脅威です。

情報セキュリティ脅威から大切な情報を守るためには、何が必要ですか。

システム面では次世代型FW(ファイアウォール)、EDR(エンドポイントにおけるセキュリティ強化)などの対策が挙げられます。一方、人的脅威を最小限にするためには、セキュリティ教育が必要です。テレワークが進み、各々が異なる場所で仕事をする機会が増えたことで、これまでのテクノロジーに頼った対策では不十分になってきました。同じ場所で仕事をしていれば、ちょっとしたコミュニケーションで未然に防げるものもあるかもしれませんが、人が分散すると難しい。近年、攻撃者(ハッカー)は、人をターゲットにして、ソーシャルエンジニアリング(個人を操って情報を入手すること)を活用したさまざまなスタイルで攻撃を仕掛けてきます。それに対抗するために、従業員を教育、訓練して個々の意識を向上させる必要性が高まったのではないかと思います。

DX時代のセキュリティ教育
—「人」を最後の砦としてサイバー攻撃から企業を守る

セキュリティ教育の方法は、従来から何か変化がありますか。

第一世代から第五世代へと変化しています。第一世代は人を頼らないで、テクノロジーに依存する方法。第二世代は集合教育、第三世代はeラーニング、第四世代はメール訓練といった、定期的に教育を行う方法。そして第五世代はヒューマンファイアウォール(Human Firewall)アプローチ、すなわち「人」を最後の砦とするための継続的な教育です。日本ではまだ、第三、第四世代のスタイルが中心と思われます。もちろんこのような研修も大事ですが、人の記憶は薄れやすいものです。従業員それぞれの意識を向上させて維持すること、我々はそこに着目して、第五世代の必要性を伝えようとしているところです。

	教育方法	ツール
第一世代	人への教育はなし	セキュリティ対策製品
第二世代	集合研修	パワーポイント資料
第三世代	勉強会 / e-ラーニング	セキュリティ教育ビデオ
第四世代	メール訓練	標的型攻撃訓練メール配信システム
第五世代	ヒューマンファイアウォール・アプローチ	セキュリティアウェアネス教育製品

図2:セキュリティ教育の変化

第五世代のヒューマンファイアウォール・アプローチとは、具体的にどのようなものでしょうか。

従業員の意識を向上させて維持することを目的とした「セキュリティアウェアネス教育」、いわゆる「SAT」と呼ばれるもので、海外ではかなり浸透してきています。簡単に言うと、従業員に対して短時間で継続的に教育して、無意識でも行動できるようにさせることです。

新型コロナウイルス対策を例にするとわかりやすいでしょう。我々はウイルスの専門家ではないので、細かい分子構造などの知識は必要ありませんが、発症したときの症状や、感染を防ぐための方法を知っています。テレビやインターネットの情報、外出先でのアナウンスなど、いたるところで目や耳にしているため、自然と情報が頭に入り、自分を守るための行動をとっているのです。セキュリティに関しても同様で、専門家のように全てを細かく理解する必要はない。従業員一人ひとりが、脅威のあるメールに引っかかったら何が起こるか、騙されないためには何をすればよいか、わかっていて行動できればよいのです。企業の情報資産を守るだけでなく個人の私生活を守ることにもつながります。

実際にセキュリティ教育を行う上での課題はありますか。

セキュリティ教育を企画・運用する側(企業側)の課題としては、多くの企業が、システムへの対策には毎年投資をしますが、セキュリティ教育には投資をしないという傾向があり、セキュリティ事故に遭って初めて教育の必要性が見直されることが多いです。また、実際にセキュリティ教育を行うことになっても、管理・運用者の負荷が高いことや、企業・国ごとに言語や文化が異なる点、また攻撃は日々変化しているためそれに合わせたコンテンツ作成における難しさもあります。

一方、セキュリティ教育を受ける側(従業員側)の課題としては、日常業務で忙しいのに教育に割く時間が無駄だと感じるような内容の教育が多い、毎回同じような内容だと飽きてしまう、などがあるのではないかと思います。従業員が飽きずに楽しみながら続けられて、さまざまな攻撃(例えば、標的型メール攻撃、ランサムウェア、エモテットなど)に、自然と対応できるようになることがベストです。

KnowBe4社とセキュリティ教育製品について

なぜKnowBe4社に注目したのでしょうか。

今から4年前の2018年、私はこれからのICT(情報通信技術)やセキュリティ市場について調べていました。アナリストから、これからDXの時代が来る、という話を聞くことも多くなりました。そこで、“ゲームチェンジ”が起きると言われる分野の中から、セキュリティを中心に市場調査を行い、特にSAT市場について調査を進め、日本におけるSAT市場は2024年に600億円規模に急成長するという予測があることがわかりました。その中で見つけたのがKnowBe4社です。当時、KnowBe4社には日本国内での販売パートナーがいないことがわかり、2018年12月25日に正式に契約をしました。その後、2019年6月に開催された「Interop Tokyo 2019」で初公開した際、製品の需要を確信し、2019年8月に販売・サポートを開始することになりました。

KnowBe4社の製品の特長や利点についてお聞かせください。

KnowBe4社が提供する教育はSATが中心で、「人」をヒューマンファイアウォールにするために必要な機能が盛り込まれています。セキュリティ意識向上トレーニング&フィッシングシミュレーション「KnowBe4」は、模擬的なフィッシング攻撃、動画による教育コンテンツなどを豊富に取り揃え、教育・訓練・分析までワンストップで提供します。

1 全従業員を教育する(セキュリティ意識向上トレーニング)
継続的に社員のスキル向上を実現

2 全従業員にサイバー攻撃被害の擬似体験を経験(訓練)
豊富なテンプレートとランディングページを活用した本番さながらの訓練

3 現状把握、分析、効果を数字で可視化(レポーティング)
定期的に実施することで被害リスクを可視化

図3:「KnowBe4」の教育の特徴

また、契約期間中であれば無制限に利用できる点、約40言語に対応している点、そして日々変化する攻撃に合わせたコンテンツのアップデートなどがポイントかと思います。また、受講者に最適な学習を自動で管理できるため、運用コストを大幅に下げることができます。さらに、内容も興味を引くものが多く、お客様から「次のコンテンツを早く見たい」という従業員の声が出ているとの話も聞きます。

図4:「KnowBe4」イメージ

「KnowBe4」製品情報については、こちらをご覧ください。
https://www.toyo.co.jp/ict/products/detail/knowbe4-cbt.html

東レ株式会社様、株式会社資生堂様の「KnowBe4」導入事例紹介はこちらをご覧ください。

東レ株式会社様の「KnowBe4」導入事例
https://www.toyo.co.jp/ict/casestudy/detail/id=35883

株式会社資生堂様の「KnowBe4」導入事例
https://www.toyo.co.jp/ict/casestudy/detail/id=35884

KnowBe4セキュリティ意識向上セミナーとケビン・ミトニック氏

東陽テクニカは2022年2月17日、企業の情報セキュリティを担う方々を対象としたオンラインセミナー、『「Human Firewall」を実現するKnowBe4セキュリティ意識向上セミナー』を開催しました。世界的に有名な伝説のハッカーであり、KnowBe4社のCHO(Chief Hacking Officer)でもあるKevin Mitnick(ケビン・ミトニック)氏の特別講演を中心に、「KnowBe4」の紹介や、国内で「KnowBe4」を導入しているグローバル企業二社の事例についての講演を行いました。

ケビン・ミトニック氏を招いてセミナーを開催しようと考えた理由を教えてください。

DX時代になり、セキュリティに対する考え方も、信頼できる社内と信頼できない社外を分けてその境界で対策を講じる「境界線防御」から、何も信頼しないという前提で対策を講じる「ゼロトラスト」対策に変わりつつあります。さらに、テレワークが進むと今まで以上に「人」への対策が重要になってきます。境界線防御だけでは不十分なことを皆さんに知っていただき、人への対策を重要視してほしいという願いから、今回のセミナーを企画しました。

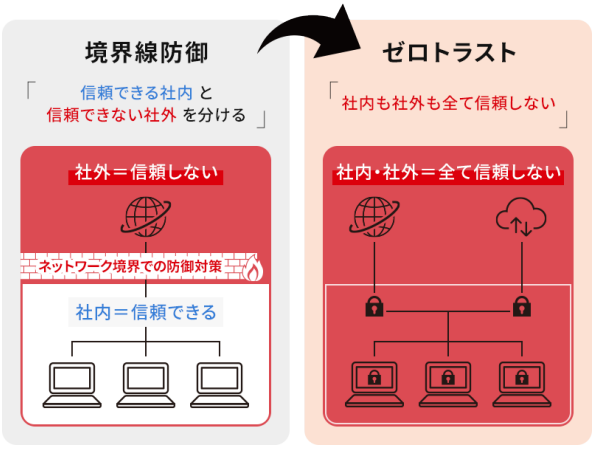

図5：境界線防御とゼロトラストの違い

ケビン・ミトニック氏と実際に話してどのような印象でしたか。

彼を直接知ったのは「KnowBe4」がきっかけですが、世界的に有名で天才的なハッカーであるとは認識していました。過去にさまざまな企業をハッキングして逮捕されたとの情報など、個人的には少々悪いイメージを持ってしまっていたのも事実ですが、ハッキング技術に関しては桁違いに凄い人なのだろうと思っていました。なにせ某ファストフード店のドライブスルーで待っている間にシステムに侵入して、データの改ざんを行うようなことが簡単にできてしまうのですから。

今回のセミナーの事前打ち合わせをオンラインで行いましたが、非常にフランクでユーモアがあり、お付き合いしやすい人だと感じました。また、過去に捕まった原因は金銭目的ではなく、自分の技術能力を試すためだと知って安心しました。今では自身でセキュリティ会社を運営し、エシカルハッカー(ホワイトハッカー)として、エクスプロイト(セキュリティの脆弱性を攻撃するプログラム)とソーシャルエンジニアリングを組み合わせ、企業からの依頼で侵入テストを行い、100%侵入に成功しています。

セミナーを終えて、お客様からの反響はありましたか。

セミナーは、700名強の方にご参加いただきました。事前のアンケートでは、ミトニック氏を知らなかった方も半数近くいらっしゃいましたが、実際のハッキングデモを交えた話を聞いて、非常にわかりやすかったという声が多かったです。また、導入事例は今後の参考になるという声も多かったですね。セキュリティ教育に興味を持たれた方も多くいらっしゃいました。

ケビン・ミトニック氏のコメント紹介
—攻撃されることを想定した訓練が大切

今回のセミナーで特別講演をしたケビン・ミトニック氏に、改めて話を聞きましたので、ご紹介します。

今回の講演を引き受けた理由を教えてください。

ミトニック氏：セキュリティアウェアネスの意識を高め、日本企業がソーシャルエンジニアリング攻撃に対抗できるように支援したいと思ったからです。ソーシャルエンジニアリング攻撃は、現在、最も使用されている攻撃方法です。

最近のサイバー攻撃についてどのようにお考えですか。

ミトニック氏：ニュースでもよく報じられている通り、サイバー犯罪は拡大しています。サイバー犯罪者集団LAPSUS$は、ランサムウェアのペイロードをデプロイして（実行ファイルをばらまいて）、世界中の企業に大損害を与えてきました。その中には大企業も含まれます。LAPSUS$は欧州の10代の若者による集団だそうで、自身を無敵だと考えて侵入とランサムウェア攻撃を行っています。彼らは主にソーシャルエンジニアリング攻撃を仕掛けてきます。

Microsoft社のレポートによると、彼らの攻撃には、電話によるソーシャルエンジニアリング、SIMスワップによるアカウント乗っ取り、標的企業の従業員の個人メールアカウントへのアクセスなども含まれます。また、標的企業の従業員、取引先、パートナー企業を買収して、資格情報や多要素認証（MFA）へアクセスしたり、標的企業の進行中の危機管理通信に侵入したりもするとされています。

多くの企業が年に1回の情報セキュリティ教育を行っていますが、近年のサイバー攻撃に対抗するのに十分と思われますか。

ミトニック氏：十分とは思いません。攻撃の方法は常に変化しているため、セキュリティアウェアネス訓練を、継続的にアップデートして実施する必要があります。

「KnowBe4」のようなセキュリティアウェアネス教育と実践訓練を定期的に行うことで、近年のサイバー攻撃に対応できると思いますか。

ミトニック氏：はい。世界中の企業がKnowBe4を導入し、従業員の意識向上のトレーニングを継続的に行うことを期待しています。フィッシング詐欺、なりすまし電話、スマホやソーシャルメディアのメッセージなどの攻撃シミュレーションを通じて、ソーシャルエンジニアリング攻撃への耐性を付けてもらいたいです。

最後に、東陽テクニカルマガジンの読者にメッセージをお願いします。

ミトニック氏：攻撃者が従業員を危険にさらすために用いる方法をよく理解してほしいです。以前、フランク・アバグネイル（映画「キャッチ・ミー・イフ・ユー・キャン」の原作『世界をだました男』の著者）が、「詐欺について知ったら、騙される可能性はぐっと低くなる」と言っていました。

私のモットーは、「試す、突き詰める、訓練する」です。半年ごとに、レッドチーム演習（模擬的なサイバー攻撃を仕掛け、企業のセキュリティ対策を検証）または侵入テストを行い、セキュリティホールを見つけ出してください。そして、攻撃対象領域を縮小してください。ゼロトラストセキュリティについて調べるのもよいでしょう。そして最も重要なことは、従業員を訓練して、新旧のソーシャルエンジニアリング攻撃に対抗できるようにすることです。

ぜひ、先を見越した行動をしてください。「もし攻撃されたら」ではなく、攻撃されることを想定して行動することが大切です。

コメントをいただき、どうもありがとうございました。

おわりに

本稿では、DX時代におけるセキュリティ教育の必要性、特に、継続的な教育で「人」の意識を向上させる、ヒューマンファイアウォール・アプローチについて、ご紹介いたしました。東陽テクニカでは、「KnowBe4」以外にも脆弱性診断スキャナ、セキュリティ診断、ダークウェブ監視などセキュリティ分野にフォーカスをした製品を取り扱っています。ICT、セキュリティ分野において、海外市場では成長していても日本ではまだ知られていない、新たなソリューションを発掘することで、皆さまの情報セキュリティを守ることに貢献してまいります。

プロフィール

株式会社東陽テクニカ
情報通信システムソリューション部
次長
大柳 誠一郎

アジレントテクノロジー（旧横河ヒューレット・パッカード）とフルークネットワークスでネットワーク関係のSE、プロジェクト管理業務などを経験し、2008年に東陽テクニカに入社。2015年にCySec （国際化サイバーセキュリティ学特別プログラム）を履修し、そこで得た知識と経験をもとにサイバーセキュリティに関わる。ニッチな市場や製品を中心に海外の製品やサービスを日本国内で啓蒙活動を中心に活躍。手掛けた市場は脅威インテリジェンス、ダークウェア監視、セキュリティアウェアネス。そのうちのひとつの製品が今回ご紹介する「KnowBe4」になります。