Optimizing Your Security

“心の隙”を突くサイバー攻撃が急増、被害を抑え従業員の「行動を変える」方法は何か

ミスを犯す「人」をターゲットにしたサイバー攻撃に対し、どう対応するのが正解なのか

ワクチンや給付金をかたったフィッシングメールなど、人の不安や恐怖につけ込んだサイバー攻撃が急増している。「通信相手を信頼せずに攻撃されることを前提とする」コンセプトを持つ“ゼロトラスト”のセキュリティ対策をはじめ、新たな製品やサービスも登場しているが、人間の心の隙を突く攻撃には、十分な対策ができているとはいい難い。こうした状況で、企業はどのようにリスクコントロールすればよいのだろうか。人に焦点を当てたセキュリティ対策と被害が発生した時の備えについて整理する。

INTERVIEWEE

MS&AD
MS&ADインターリスク総研

MS&ADインターリスク総研 株式会社
新領域開発部長兼
MS&ADインシュアランスグループ
ホールディングス
総合企画部イノベーション室 部長

土井 剛 氏

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社
日本代表マネージングディレクター

根岸 正人 氏

iSiD

株式会社 電通国際情報サービス
金融ソリューション事業部
戦略アライアンス部
ソリューションディレクター

赤澤 卓真 氏

iSiD

KnowBe4
Human error. Conquered.

1 テレワーク拡大で、人の不安・恐怖につけ込むサイバー攻撃が急増

IPA(独立行政法人情報処理推進機構)は毎年、「情報セキュリティ10大脅威」を発表している。このランキングには個人編と組織編の2つがあるが、2021年度の組織編でいきなり3位にランクインしたのが「テレワーク等のニューノーマルな働き方を狙った攻撃」だ。

いうまでもなく、これは新型コロナウイルスの世界的なパンデミックの影響だ。対人の活動が制限された結果、テレワークを初めとする新しい働き方が広がり、これまで社外との境界を防御してきた社内ネットワークに、社外の端末から接続する必要性が高まった。その結果、その端末を狙ったサイバー攻撃が急増したのだ。特に顕著なのが、人々の不安・恐怖につけ込んだ攻撃だ。ワクチンや特別給付金などの内容を騙(かた)ったフィッシングメールはその典型だろう。

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの 不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの 不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

情報処理機構(IPA)の「情報セキュリティ10大脅威 2021」は
在宅勤務に関するものが上位を占めた

被害が増えている背景には、急いでテレワーク環境を整備した結果、従業員教育が追いついていない現実もある。本来なら在宅業務に合わせたルールを理解・納得してもらい、徹底する必要があるが、現実にはそこまでできている企業は少ない。

今までなら、不審なメールを受信したら隣の同僚に相談したり、IT部門に確認したりできたのにそれができない。攻撃側にとって、こうした状況は非常に有利だ。仮に関係者が1000人いる場合、そのうちの1人でも"ひっかける"ことができたら成功だからだ。

その結果、個人情報をはじめとする機密情報が漏えいしたら、或いは昨今猛威を振るっているランサムウェアにより事業中断などが発生したら、企業は莫大な損失を被ることになる。経済産業省 商務情報政策局 サイバーセキュリティ課が2020年12月に発表した「注意喚起」には、サイバー攻撃による被害額の平均について、1億数千万円という記載がある。軽微なインシデントが多いことを考慮すると、現実の金額は、これを大きく上回るだろう。

「ソーシャルエンジニアリングと呼ばれる、人間の心理的な隙や、行動のミスに付け込むサイバー攻撃を100%防ぐことはできないため、損害が発生する可能性が高い」「損害をなるべく防ぐため従業員のリテラシーを上げたい」――。従来のセキュリティ対策に加え、新しいスタイルのセキュリティ教育が求められている状況に、企業はどう備えればよいのだろうか。

2 日本初、セキュリティ教育付きのサイバー保険

「100%防ぐことは難しいサイバー攻撃」に対し、損害を補償するのが「サイバー保険」だ。

MS&ADインターリスク総研 新領域開発部長 兼 MS&ADインシュアランスグループホールディングス 総合企画部 イノベーション室 部長 土井 剛氏は、サイバー保険について次のように説明する。

「一般的にサイバー保険は、事故により生じた第三者に対する損害賠償、フォレンジックなどの調査や被害者へのお見舞いにかかる費用、自社の喪失利益を補償する保険です。現在、サイバー保険への引き合いは急速に増えています」(土井氏)

ただし、サイバー保険はあくまで"事後対策"の1つだ。事故を防ぐため或いは被害を早く見つけ最小化するための対策、特に従業員への教育は、各企業が独自に準備・推進しなければならなかった。しかし2021年3月、サイバー保険と、従業員のITリテラシーを上げる「従業員教育」を組み合わせたサービスが誕生した。

MS&ADグループと従業員のセキュリティ教育をクラウドで提供するKnowBe4(ノウ・ビフォー)、同社の販売代理店である電通国際情報サービス(ISID)の3社の協業により、「セキュリティ教育サービス付きサイバー保険」がリリースされたのである。

この損保業界で初めての取り組みは、具体的には、三井住友海上とあいおいニッセイ同和損保が提供するサイバー保険(※)に加入すると、KnowBe4の教育コンテンツを利用できるというものだ。このサービスにより、「損害補償」と「従業員教育」の両輪での対策が可能になり、"リスク発生時の効果"と"リスクの予防効果"を同時に併せ持つ新たなサイバーセキュリティを実現できるようになったのだ。

※ 各社商品名は異なり、三井住友海上は「サイバープロテクター」、あいおいニッセイ同和損保は「サイバーセキュリティ保険」となっている。

KnowBe4 Japan 日本代表マネージングディレクター 根岸正人氏は、「従業員教育」を担うKnowBe4の特徴を次のように述べる。

「どんなにセキュリティ対策を徹底しても、心の隙、人の脆弱性を突く攻撃を防ぐことは困難です。したがって、従業員のセキュリティ意識を改革し、行動変容を起こさせ、組織内にセキュリティカルチャーを醸成することが重要です。KnowBe4は、それを実現するためのクラウド型サービスです」(根岸氏)

3 “ネットフリックスさながら”の短編映画でランサムウェアを学ぶ

日本のセキュリティ教育はIT部門主導によるIT教育の一環として実施されるが、従業員のセキュリティ意識を改革し、行動変容を起こさせ、組織内にセキュリティカルチャーを醸成するには、セキュリティ教育の「中身」、つまりコンテンツをこれまでとまったく違うものに変える必要がある。

従来のセキュリティの教育コンテンツというと、「つまらない」「退屈」「単調」といった印象を抱くものが多かった。しかし、KnowBe4のコンテンツはまったく違うと、根岸氏は次のように説明する。

「従来のセキュリティのコンテンツは、3日もすればすべて忘れてしまいます。テストをしても、『合格すればいい』というその場限りの考え方では、とても意識改革はできません。KnowBe4では、従来型のコンテンツに加え、ゲーム感覚のクイズや動画コンテンツを豊富に用意して、楽しみながらセキュリティ・リテラシーを身につけることができます」(根岸氏)

たとえばランサムウェアであれば、ネットフリックスのオリジナルムービーさながらの12本の短編動画が用意されている。もしもランサムウェアに感染したら何が起きるのかを、従業員はサスペンス映画を見るように、楽しみながら学ぶことができる。

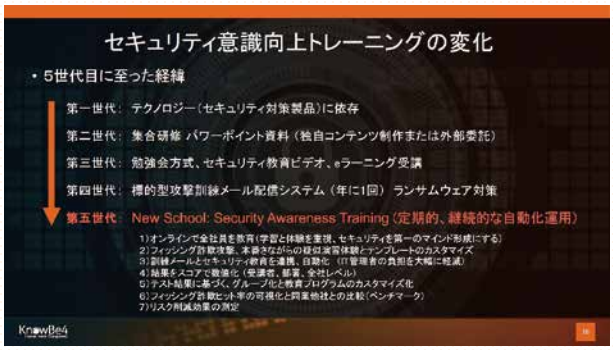
The Inside Man Season 2 Trailer - Japanese
KnowBe4のセキュリティ意識向上ビデオ動画シリーズ
「The Inside Man シーズン2:外部から忍び寄る内部犯行」
日本語吹替予告編
https://youtu.be/Fi415m-pihE

土井氏も、はじめてKnowBe4のコンテンツに触れたときの印象を次のように語る。

「私が初めてKnowBe4を知ったのは2018年でしたが、『こんなに楽しく学習できるサービスがあるとは！』と衝撃を受けました。コンテンツが攻撃者目線であることにも感心しましたし、攻撃者が何を考えて、どういうところを狙っているのかが非常によく分かるのです」(土井氏)

もちろん、コンテンツはすべて多言語対応で、かつ各国の最新事情を反映している。

「たとえばフィッシング詐欺の訓練メールは、給付金詐欺や都市銀行など実際に国内で出回っているメールのテンプレートが用意されています。テンプレートをカスタマイズしたり、新しく作ったりすることもできます。コンテンツは多言語対応していますので、グローバル企業は海外の従業員も含めて教育することが可能です」(根岸氏)



セキュリティ意識向上トレーニングを続けることで
どんどん従業員の意識が変化していく

さらに、KnowBe4ならではの特徴が、成績やリスクを可視化できることだ。電通国際情報サービス 金融ソリューション事業部　戦略アライアンス部 ソリューションディレクター 赤澤 卓真 氏は、その意義を次のように説明する。

「従来はセキュリティ・リテラシーの“習得度”を、数値化することが不十分でした。しかしKnowBe4では、個人の成績はもちろん、部署単位や組織全体のリテラシー習得度をリスク値などで数値化し、リテラシーが高いのは、どの部署なのか、誰なのかを把握し、その結果をもとに習得度に応じた個別のトレーニングを実施できます。たとえば、過去1年間に実施したメール訓練で2回クリックしてしまった人にフィッシングに関する講義を受講させること、SNSなどのソーシャルメディアに関するリテラシーが低い人にソーシャルメディアに関する講義を受講させるなど、一連の取り組み(理解度テストやリスクスコアなどを自動集計し分析結果からメンバーを動的にアサインし、補習教育の配信及び受講を促す)を自動化する仕

組みまで用意されています。習得度を数値で管理することにより、経営者に対して導入効果を適切に報告すること、従業員に対しても個人の習得度に応じた適切な量や内容を受講してもらうこともできます。自動化の仕組みなどを使って管理者の運用負荷も軽減し、本来行わなければならない最新セキュリティ脅威の把握や対策に時間を割くことができます。そうすることによって社内関係者(経営者・従業員)が教育全般に対して理解が深まり、協力的になることで、従業員の受講率の向上などにもつながります」(赤澤氏)

KnowBe4のダッシュボード。
組織全体のリスクをスコア化

数値化により個人、部署、組織全体のリスク値や
セキュリティ・リテラシー習得度を管理

4 リスクの発現を抑え、発現したときの経済的負担を最小化する未来のサイバー保険

KnowBe4のセキュリティ教育サービス付きのサイバー保険には、すでにいくつかの大手企業から問い合わせがきているという。

「大手企業の場合、技術的なセキュリティ対策には、これまでかなりの投資を行っています。しかし、ソーシャルエンジニアリングのような人間の心理的な隙や、行動のミスに付け込むサイバー攻撃に対する対策は、なかなか決め手がないのが現実です。そうした中、KnowBe4のような従業員のセキュリティ・リテラシーの向上を目的とした新しい教育プラットフォームに関心を抱く企業が非常に多いです」(赤澤氏)

確かに最近はゼロトラストのセキュリティ対策が強調され、人工知能(AI)を使って未知のマルウェアを検知・駆除するソリューションも登場している。今後も、最新のテクノロジーがセキュリティ対策に組み込まれるだろう。

一方で、テクノロジーの進化から取り残されているのが人間だ。セキュリティ対策が高度化すればするほど、人間そのものがシステム全体の脆弱性になってしまう。

「MS&ADインシュアランスグループでは、リスクをいち早く見つけお伝えし、リスクの発現を防ぎ、その影響を最小化するとともに、リスクが現実となったときの経済的負担を小さくするお手伝いをすることを、『価値創造ストーリー』と呼んでいます。今回のKnowBe4とサイバー保険の組み合わせは、この価値創造ストーリーに沿った『未来のサイバー保険の1つの形』だと考えています」(土井氏)

テクノロジーが進化し、サイバー攻撃も、それに対抗するセキュリティ対策も高度化・複雑化している。一方で、旧態依然のままなのがセキュリティ教育だ。KnowBe4は、そこを変革する。

ただし、それでもリスクをゼロにすることはできない。だからこそ、KnowBe4とサイバー保険の組み合わせ、つまり「損害補償」と「従業員教育」の両輪での対策に意味があるのだ。セキュリティ対策を次のレベルに引き上げる意味でも、ぜひ検討していただければと思う。

株式会社電通国際情報サービス(略称 ISID)
金融ソリューション事業部　戦略アライアンス部

〒108-0075 東京都港区港南 2-17-1
E-mail：g-security@group.isid.co.jp
Tel：03-6713-7030
ソリューション紹介 URL：https://security.isid.co.jp/knowbe4/

ソリューションの
詳細情報はこちら