経営幹部と意思決定者のサイバーセキュリティ意識を高めるための効果的な方法

Kaspersky Interactive Protection Simulation

kaspersky BRING ON THE FUTURE

詳細についてはこちらをご覧ください：
kaspersky.co.jp/awareness

Kaspersky Interactive Protection Simulation

「経営幹部が抱えるジレンマ」

最大のセキュリティ課題の 1 つは、経営幹部や部門管理者などの役割が異なればサイバーセキュリティに対する見方が異なり、その優先事項も異なるということです。その結果、意思決定に次のような「セキュリティのジレンマ」が発生する可能性があります：

- 経営幹部は、セキュリティ対策をビジネス目標（低コストかつ迅速に高品質な製品を提供）の達成の阻害要因と考えている
- IT セキュリティ管理者は、サイバーセキュリティを自身の権限外のインフラストラクチャと投資に関する問題と考えている
- コスト管理担当者は、サイバーセキュリティは収益を生むための出費であり、コストを発生させるのではなくコスト削減につながるとは考えていない

これら 3 者間で相互理解と協力を実現することは、サイバーセキュリティを成功させるために重要なことです。ただし、座学や攻撃側と防御側に別れたサイバー セキュリティ技術者向けの演習のような従来のやりかたには、欠点があります。つまり、長い時間をかけて技術的に高度な内容を演習として実施することは、多忙な管理職に適しているとは言えず、日常におけるサイバーセキュリティの重要性についての共通認識を得ることは難しくなります。

KIPS とは

Kaspersky Interactive Protection Simulation （KIPS）は、企業や政府機関のビジネス上の意思決定者である IT セキュリティチームが、一連の予期しないサイバー脅威に晒されているビジネスシミュレーション環境で、最大限の利益を確保し、信頼を維持することを目的とした演習です。

その狙いは、利用できる最適な事前および事後のサイバーセキュリティ対策を選択することにより、サイバー防御戦略を構築することです。次々と明らかになるセキュリティイベントへの対処方法に応じて、その後のシナリオおよび企業の最終的な利益や損失の程度が変化します。

各チームは、現実的なサイバー攻撃に対するコストに対して技術やビジネス、さらにセキュリティの観点から各優先事項のバランスを取りながらデータを分析し、不明瞭な情報と限られたリソースを用いて戦略的意思決定を行います。それぞれのシナリオは実際のイベントに基づいているため、現実さながらの体験をすることができます。

KIPS が効果的な演習である理由

KIPS トレーニングの対象者は業務システム担当者、IT 担当者、および部門管理者であり、稼働中の最新のコンピューターシステムに関するリスクおよびセキュリティ上の問題の認識力を向上させることが目的です。

対戦する各チームは 3 〜 4 人で構成し、コンピューターで制御されている製造施設から成る業務を運営する任務を遂行します。ゲーム中は、製造施設により収益、公益、業績が発生します。ただし、企業の業績に影響を与える可能性のあるサイバー攻撃にも直面してしまいます。

各チームは企業を保護するために、戦略的、経営的、および技術的な意思決定をすると同時に、運営上の制約事項を考慮し、高水準の収益を維持することが求められます。

KIPS ゲームは、次の特徴を持つ動的な「体験型」セキュリティトレーニングプログラムです：

- 短時間で楽しく学べる魅力的なプログラム（2 時間）
- 共同作業でチームワークを育成
- チーム間の競争を通じて取り組みと分析スキルを向上
- ゲームを通してサイバーセキュリティ対策を理解

参加者は KIPS ゲームを通じて、日常業務に生かせる重要な結論を得ることができます：

- サイバー攻撃は収益を損なうため、経営陣による対処が必要
- 適切なサイバーセキュリティ対策の実現には IT 担当者とビジネスサイドとの協力が不可欠
- 効果的なセキュリティを確保するための費用は、収益を損なうリスクに比べてはるかに少額で済み、何百万ドルもかからない
- 特定のセキュリティ管理に慣れてその重要性を理解する（監査トレーニング、アンチウイルスなど）

KIPS トレーニングでは、参加者に対して次の内容を提示します:

- 事業継続性と収益性を実現するためのサイバーセキュリティの実際的な役割
- 現在発生している課題と現在直面している脅威
- サイバーセキュリティ構築時に企業が陥ってしまうよくある誤り
- サイバー脅威に直面しても安定したビジネスの運用と持続可能性を維持するのに役立つ、ビジネスサイドとセキュリティチームとの協働

参加者は、サイバー攻撃に遭遇した企業として、製造や収益面で受ける影響を疑似体験し、攻撃による影響を最小限に抑えてより多くの利益を確保するために、さまざまなビジネスおよびIT戦略とソリューションを採用することを学びます。

業界によって異なる攻撃経路に特化したシナリオを通じて、それぞれの業界でサイバーセキュリティを構築し、インシデント対応手順を定める際によく見られる誤りを特定し、分析することができます。

2019 年には、自治体における個人データ保護に特に重点を置いた新しいシナリオが作成されました。KIPS GDPR版(自治体)の一連の演習やトレーニングユニットを通じて、自治体職員は、サイバーセキュリティの課題を認識するだけでなく、その認識をポジティブな行動モデルに変換させることが可能になります。このトレーニングでは、チームワークと適切な責任分担の重要性にも重点を置いており、自治体が住民のセキュリティと安全に関してより適切な意思決定をする際に、これらがどのように役立つかについても取り上げています。

すべての業種に対応したエンタープライズ向け KIPS シナリオ

企業版

ランサムウェア、APT、オートメーションセキュリティの不具合から企業を保護

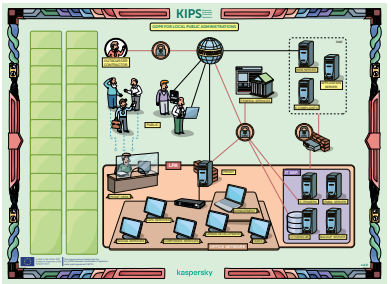
銀行版

Tyupkin、Carbanak のような新しい高度な APT から金融機関を保護

石油ガス版

Web サイトの改ざんから実際に使用されたランサムウェア、高度な APTまでさまざまな脅威の影響について学習

GDPR版(自治体) NEW!



攻撃やエクスプロイトから公開 Web サーバーを保護

発電所版、浄水場版

Stuxnet タイプのサイバー攻撃から産業用制御システムと重要インフラを保護

運輸版

Heartbleed、APT、B2B ランサムウェア、内部関係者から物流企業を保護

KIPS ゲームに関する引用とコメント

Kaspersky Industrial Protection Simulation は実際に驚くべき経験をさせてくれる演習であり、すべてのセキュリティ専門家にとって必須のものです。

Warwick Ashford 氏、
Computer Weekly

CERN は膨大な数の IT およびエンジニアリングシステムを所有しており、そのシステムで数千人にも及ぶ従業員が作業を行っています。このため、サイバーセキュリティの観点からすると、サイバーセキュリティの認識を高めて、より多くの従業員がそれに注意を向けるようにすることは、技術的な制御と同じくらい重要です。Kaspersky のトレーニングは、魅力的、明快、そして効果的であることが証明されています。

Stefan Luders 氏、
CERN CISO

これは実際に驚くべき経験をさせてくれる演習であり、多数の参加者が自社でこのゲームを採用することを提案しています。

Joe Weiss 氏、PE、
CISM、CRISC、ISA フェロー

私たちは提携と協力に基づいて人的ネットワークを構築する必要があります。この際、KIPS はこの作業を開始するための最善の方法です。

Daniel P. Bagge 氏、
Národní centrum kybernetické bezpeč nosti、チェコ共和国

KIPS セッションを準備するための推奨事項

スケジュール：KIPS は、個別のイベントまたは既存のイベント、会議、セミナー内のセッションとして計画します（この場合、KIPS に最適な時間は初日の夜）。

グループ：20 ～ 100 人をそれぞれ 3 ～ 4 人のグループに分けます。管理、技術、CISO/IT セキュリティ部門のメンバーが混在しているのが理想的です。
- それぞれの役割と部門から最低 1 人が参加するのが適切
- チームは、異なるまたは同じ企業や部門の担当者から構成できる
- 参加者はお互いが知り合いでも、知り合いでなくてもよい

設定：このゲームは 1.5 ～ 2 時間かかりますが、Kaspersky の進行担当チームがゲームの前に準備や設定を行うための時間が 2 時間必要です。

部屋：参加者 1 人あたり 3 ㎡ 程度の広さが確保できる、柱のない通常の形態の部屋。

AV 機器：プロジェクター（6 ～ 8 ルーメン）、スクリーン、音響システム（スピーカー、リモコン、マイク）。

インターネットアクセス可能な Wi-Fi（KIPS ゲームサーバーへのアクセス用）、4 Mbps 以上

各チーム（4 人）1 台の iPad（Wi-Fi 対応）または他のタブレット。

備品：参加者 4 人用のテーブル（75 x 180 cm 以上の長方形、または直径 1.5 m 以内の円形）。参加者は 4 人ずつのグループでテーブルに着席。進行担当者用のテーブル。参加者用の椅子（テーブルと共に配置）。

コメントとケーススタディ

KIPS ゲームは、50か国を超える各産業界のセキュリティ担当者によって実施されてきました。

- KIPS は、英語、ロシア語、ドイツ語、フランス語、日本語、スペイン語（EU）、スペイン語（中南米）、ポルトガル語、トルコ語、イタリア語に翻訳されています。
- KIPS は、重要インフラストラクチャにおけるセキュリティ認識を高めるために、CyberSecurity Malaysia、Czech NSA、Netherlands Cyber Security Centrum などの政府機関で使用され、重要インフラストラクチャ企業の何百人にも及ぶ専門家をトレーニングしてきました。
- KIPS は、BASF （世界トップクラスの化学メーカー）、CERN （大型ハドロン衝突型加速器）、RusHydro、ISA （国際計測制御学会）などの企業や団体で採用されており、技術者、開発者、顧客対応スタッフをトレーニングし、産業用オートメーション環境におけるサイバーセキュリティへの認識を高めるために使用されています。
- KIPS は、SANS Institute などの主要な教育機関に対してライセンス供与されており、世界中の SANS の生徒に対して提供されるサイバーセキュリティトレーニングプログラムで使用されています。
- KIPS は MHPS コントロールシステムズなどのセキュリティサービスプロバイダーおよびベンダーに対してライセンス供与されており、重要インフラストラクチャ部門の最終顧客向けのトレーニングコースとして使用されてきました。

KIPS トレーニングの 2 つの形態

KIPS ライブ (会場実施型)

制約が多い一方で、参加者同士が同じ会場で互いに競争するため、より集中した取り組みが期待できます。チームビルディングイベントとしても実施可能

- 受講者数は、1 部屋につき最大 80 人
- 参加者全員が同一言語
- トレーナーとアシスタントが出席
- 主に印刷された教材を使用

KIPS オンライン

世界的な組織や社会的活動に最適です。KIPS ライブと組み合わせて、遠隔地のチームをオンサイトイベントに参加させることができます。

- 場所を問わず、1 回につき最大 300 チーム（受講者数 1000 人）
- チームごとに異なる言語のゲームインターフェイスを選択可能
- トレーナーは WebEx を使用してセッションを主導

トレーナー養成プログラムの提供

複数の部門や現場の多数の従業員、マネージャー、および専門家にトレーニングを実施するために KIPS を使用する場合は、KIPS トレーニングのライセンスを購入し、お客様自身のご都合に合わせて社内トレーナーを教育し、KIPS セッションを実施するのが便利です。

このライセンスは MHPS コントロールシステムズなどのパートナーから入手可能で、次の項目が含まれています：

- 社内で KIPS トレーニングプログラムを実施するための使用権
- プログラムを使用して再現するためのトレーニング用教材と使用権一式
- KIPS ソフトウェアサーバーへのログインとパスワード
- KIPS トレーニングの実施方法に関するプログラムリーダー向けのトレーナーガイド、教育、およびトレーニング
- メンテナンスとサポート（KIPS ソフトウェアとトレーニングコンテンツのアップデートおよびサポート）
- オプションにより KIPS シナリオのカスタマイズが可能（追加料金が適用されます）

Enterprise Cybersecurity：www.kaspersky.co.jp/enterprise/
Kaspersky Security Awareness：www.kaspersky.co.jp/awareness

www.kaspersky.co.jp

kaspersky