エグゼクティブ サマリー

形勢の逆転: サイバーセキュリティのギャップを埋める方法

サイバー犯罪者は、データの窃盗、サービスの悪用、情報フローの破壊を行うため、常に新たな手法を考え、優位な立場を維持しています。このような状態が続くのはなぜでしょうか。攻撃者の技能が勝っていることだけが原因とも言えません。攻撃者と防御者の状況の違いも考慮する必要があります。この状況を把握するため、主要な5業種のサイバーセキュリティ担当者800人を対象に調査を行いました。この調査で3つの重要なギャップが明らかになりました。1つは、会社の組織と犯罪者の特性、2つ目は戦略と実装、3つ目は上級管理者と現場のギャップです。

防御側を不利な状況に追い込む3つのギャップ

攻撃者と防御側	攻撃者は市場が分散し、どこからでも瞬時に攻撃を実行できますが、セキュリティ担当者は、面倒な手続きと思い付きの意思決定に振り回されています。
戦略と実装	90%以上の企業でサイバーセキュリティ戦略が実装されていますが、戦略を完全に実装している企業は半分もありません。
上級管理者と現場	サイバー戦略を設計した上級管理者は、効果とは別の観点でセキュリティを評価しています。

intel Security

会社の組織と犯罪者の特性

サイバー攻撃の標的は縦割りで柔軟性に欠けた組織が多く、サイバー攻撃者は明確な動機を持ち、手段を選ばず自由に攻撃を仕掛けてきます。サイバー犯罪市場は価格シグナルに敏感で、毎日新しい製品やサービスが次々と登場し、古い機能に代わるものがすぐに出現します。サイバー犯罪市場には、豊富なリソースを駆使して非常に巧妙な攻撃を実行する犯罪者、国家の支援を受けた攻撃者、ハクティビスト、サービスとしての犯罪を利用する攻撃者などが存在し、激しい競争を繰り広げています。この市場を詳しく調査するため、サイバーセキュリティの技術担当者と取締機関にインタビューを行いました。

サイバー犯罪市場は、マルウェアのプログラマー、不正なWebサイトのデザイナー、インフラの専門家、エクスプロイトと脆弱性を駆使するハッカー、ソーシャルエンジニアリングの手口を考え出す詐欺師など、特殊な技能を持つもので溢れています。素人でも素質があればすぐに熟練した攻撃者になってしまいます。貢献度が高いほど報酬が多くなるため、能力の低い犯罪者は自然に淘汰され、スキルの高いものだけが残ります。

この激しい競争と補償モデルは、新しい脆弱性やエクスプロイトの使用速度にも表れています。脆弱性の42%は、発見後30日以内に悪用されています。かつて人気のあったAnglerエクスプロイト キット（エクスプロイト キットのアクティビティの82%を占めていました）の作成者が逮捕されると、Anglerを利用していた攻撃者は数週間もしないうちにNeutrinoエクスプロイト キットに乗り換え、攻撃を実行し始めました。犯罪者の大半は自身で調査や研究を行わず、優秀な犯罪者が作成したマルウェアを利用します。このようなマルウェアは闇市場やパッチに時間がかかる大量のシステムを介してすぐに拡散します。この点も攻撃にコストがかからない理由の一つです。

サイバー犯罪者はロシアや東ヨーロッパに多いという説もあります。高等数学やコンピューター サイエンスのレベルが高く、正規雇用の機会が不足している状況を見ると、この説も間違いとも言えないようです。これらの地域のIT企業や通信会社に正規に雇われていても、夜はサイバー犯罪を行っているかもしれません。自分のFacebookに闇サイトのIDを公開している人物もいます。企業のサイバーセキュリティ対策チームは、このような闇市場から多くのヒントを得ることができます。報酬や名声が得られるかどうかで取り組み方や成果が大きく変わることは間違いありません。

戦略と実装のギャップ

回答者の大半は、サイバーセキュリティが組織に対する最大のリスクになっていると答えています。経営陣の70%以上が、取締役会でサイバーセキュリティのリスクについて報告を受けています。この課題は6年前にはリスクのトップ10にも入っていませんでした。また、回答者のほぼ全員（93%）が、既存の脅威だけでなく新たな脅威にも対応できるサイバーセキュリティ戦略を構築していると答えています。

これがギャップの始まりです。上級管理者の多くは、組織全体で戦略が十分に実装されていると考えていますが、同じ見方をする現場のスタッフは30%程度に過ぎません。経営陣も現場のスタッフも、サイバーセキュリティの効果をまず侵害発生数で評価していますが、その後の判断基準は異なります。上級管理者は、侵害からの復旧費用やサイバーセキュリティの費用対効果などを重視しますが、現場のスタッフは脆弱性スキャンや、ペネトレーションテストなどの技術的な結果を重視する傾向があります。調査した経営者の半数以上（54%）は、導入されているサイバー対策の効果よりも、評判に対する影響を気にすると答えています。しかし、問題視すべき点は、サイバーセキュリティ インシデントが収益減につながると考えているのが3分の1に満たないことです（32%）。セキュリティに対して誤った認識が浸透している可能性があります。

新たなリスクを防ぐために導入した対策が問題になる場合もあります。非常に多くの回答者（71%）が、既存の技術と新しい技術を統合するセキュリティ プラットフォームを利用していますが、64%は重複するセキュリティ技術を利用していると答えています。これも実装戦略の一つかもしれませんが、重複するセキュリティ技術を適切に統合せずに使用すると、新たなセキュリティ ギャップが発生する可能性があります。たとえば、設定が異なると、モニタリング システムで一貫したセキュリティ ポリシーを施行することが難しくなります。

上級管理者と現場のギャップ

サイバー犯罪者は、金銭や名声を得たり、標的に被害を与えるなど、攻撃に対する明確な動機があります。調査結果を見ると、経営陣はサイバーセキュリティの現場よりも自社のセキュリティ対策に自信を持っているようです。

調査した現場スタッフの約半数は、組織に明確な指針がないと答えています。この数は、同じ回答を行った経営陣の5倍以上になっています。組織階層の下に行くほど、業績に対して満足していない従業員が多く、正当な評価を受けていないと感じています。しかし、幸いなことに、調査した65%の専門家は、組織のサイバーセキュリティの強化を自身の目標として設定しています。

サイバーセキュリティ担当者に対するインセンティブを経営陣に聞いたところ、60%が金銭的な補償と答え、58%が評価と答えました。経営者以外の場合、同じ項目に対する回答の割合は15～25ポイント低くなります。現場のスタッフに聞いたところと、金銭的な補償という回答が63%、評価が62%でした。これは他の調査でも同様ですが、技術者はボーナスよりも専門技能の習得機会を重視する傾向があります。

サイバー犯罪者からの教訓

これらのギャップを埋めるには、ブラックハットのコミュニティが役立ちます。サービスとしてのセキュリティは、サービスとしての犯罪に対抗できる十分な柔軟性を備えています。必要な経験を積んだ専門のコンサルタントが社内チームをサポートすることで、リソースを有効に活用することができます。実績の評価は防御対策の強化やパッチサイクルの短縮にも役立ちます。適切な評価システムは組織によって異なります。最適なものが見つかるまで試行錯誤が必要でしょうが、スピードの向上と防御の集中、セキュリティの強化はすぐにでも実現することができます。

エグゼクティブ サマリー

犯罪市場からヒントを掴む	犯罪市場	防御策
市場原理	**サービスとしての犯罪** 犯罪市場はオープンで、分散型です。市場原理が働き、誰でも簡単に参加できます。また、新たに参入しても、すぐに結果を出すことができます。	**サービスとしてのセキュリティ** 外部委託とオープンな契約により競争原理が働きます。コストを抑え、最も効率的なセキュリティ技術や手法を選択できます。
情報公開	**一般に公開されている脆弱性を攻撃** 公開されている脆弱性を狙うことで、脆弱性の調査やエクスプロイトの開発にかかる手間を省いています。新たに公開された情報をすばやく取り込み、防御側がパッチを適用する前に攻撃を実行します。	**パッチ適用プロセスの改善** 発見された脆弱性にすばやく対応できるように、パッチの適用方法を改善します。古いシステムも迅速に更新することで、セキュリティ対策を強化し、簡単に攻撃が実行されないようにします。
可視化の強化	**オープン フォーラムとオンライン広告** オープン フォーラムや広告を利用して、成功した攻撃の手口や犯罪モデル、ベストプラクティスを広めています。	**情報の共有とコラボレーション** 情報共有を進めることで、作業の重複を排除し、防御コストを低減できます。セキュリティを大幅に強化する新しい技術とプラクティスを瞬時に浸透させることができます。
誰でも簡単に参加	**コンピューターに詳しい人物であれば誰でも可能** 資格や地理的な制約に関係なく、誰でも犯罪のエコシステムに参加し、最大限の利益を得ることができます。	**世界的な人材プール** 若手や外国のICT専門家など、広範な人材プールを利用してサイバー犯罪に対応します。企業のサイバースキルのギャップを解消し、犯罪市場から人材を取り戻します。
ギャップを埋める	**フリーランス市場** フリーランスの犯罪市場では、攻撃チェーンの様々なレベルや機能領域の活動が評価され、ニーズに合わないものは淘汰されます。	**業績の評価** 上級管理者と現場のスタッフの間に存在するギャップを最小限に抑え、適切なセキュリティ対策を実施できるように、報酬やボーナスなどのインセンティブを用意する必要があります。

戦略国際問題研究所（CICS）が発表した『形勢の逆転: サイバーセキュリティのギャップを埋める方法』（2017年3月）では、サイバーセキュリティのギャップを解消する方法について、国別、業界別に詳しく分析しています。ダウンロードしてご確認ください。

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810-0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com