PROTECTORS
STORIES

CrowdStrikeお客様事例

株式会社三菱UFJ銀行

セキュリティ施策の実効性を確認すべくレッドチーム演習を実施
海外拠点を含めたグローバルでのサイバーレジリエンス強化に貢献

グループ・グローバルでのセキュリティ対策を推進

日本を代表するグローバル金融グループである三菱UFJフィナンシャルグループ(以下、MUFG)の中核企業として、多彩な金融サービスを展開する三菱UFJ銀行。同行では多様なチャネルを通して個人／法人顧客のニーズに応えると共に、金融DX(デジタル・トランスフォーメーション)の実現に向けた取り組みも意欲的に推進している。

社会・経済活動の根幹を担う業種だけに、サイバーセキュリティ対策にも抜かりはない。「お客さまの大切な資産や情報をお預かりする以上、サービスの安心・安全確保は最優先事項です。セキュリティの司令塔役を担う当部門でも、各種セキュリティ製品の導入を進めると共に、サイバー攻撃をすみやかに検知・対処できる態勢を整備しています」と語るのは、三菱UFJ銀行 サイバーセキュリティ推進部　サイバーセキュリティグループ 調査役 中村 仁美氏。そうした取り組みの一環として、グループ・グローバルで脅威の監視・対策を行うMUFG-CSFC(MUFG Cyber Security Fusion Center)を同部門内に設置。また、グループ全体のインシデント対応を統括するMUFG-CERTも併せて設置している。

サプライチェーンを狙う攻撃に備え
海外拠点から日本国内への侵害を対象とした
レッドチーム演習を実施

セキュリティを高いレベルで維持し続けるための施策として、同行ではTLPT(Threat Led Penetration Testing：脅威ベースのペネトレーションテスト)を定期的に実施している。中村氏はその狙いを「前述の通り、行内では様々なセキュリティ対策を行っています。日々のオペレーションを通じて一定の有効性は確認できていますが、より高度な攻撃への対応能力を第三者にて評価してほしいと考えました。そこで、『People』『Process』『Technology』のすべてを含めた組織のレジリエンスを、第三者の客観的な視点で確認するために定期的なTLPTを実施しています」と説明する。

同行ではTLPT実施にあたり、毎年異なるテーマを設定しているが、2022年の題材となったのが「海外拠点を踏み台にした攻撃」である。三菱UFJ銀行 サイバーセキュリティ推進部 サイバーセキュリティグループ 調査役 福野 貴仁氏は「近年のセキュリティインシデントの中には、関連会社や取引先などのサプライチェーンを突いた攻撃も少なくありません。他社事案において海外拠点を踏み台にした日本国内への不正アクセスが確認されていることから今回は海外拠点から日本国内への侵害を対象としたTLPTを実施することとしました」と語る。

卓越した攻撃力・技術力を評価し
クラウドストライクのレッドチーム演習を採用

同行ではTLPTの実施にあたり、複数のセキュリティベンダーに提案を依頼。綿密な比較・検討の結果選ばれたのが、クラウドストライクの「レッドチーム演習サービス」である。このサービスでは、現実のサイバー攻撃と同等の手法を用いたサイバー攻撃シミュレーションを実施することにより、お客さま環境の侵害につながる問題点を特定し、防御・検知体制を強化・改善するためのヒントを提供する。

クラウドストライクのレッドチーム演習サービスを採用した理由を、福野氏は「実際に攻撃を担当するレッドチームの技術力です。高いスキルを有するテスターに攻撃してもらえば、それだけ多くのリスクを明らかにできます」と語る。中村氏も「提案書の内容が、一番具体的だった点も良かったですね。海外拠点と日本国内をテストする上で、どうすれば一番網羅的、かつ効率的にテストが行えるのかといったところまで、深く踏み込んだ内容となっていました。成果物、報告のタイミングやスケジュールも明確でした」と続ける。

業種
金融業

所在地
東京都千代田区丸の内2-7-1

株式会社三菱UFJ銀行

三菱UFJフィナンシャル・グループのビジネスの中核を担う企業として、個人／法人顧客に対し多彩な金融サービスを提供する都市銀行。現在は2021年度を初年度とするグループ中期経営計画の下、「企業変革」「成長戦略」「構造改革」の三本を柱とする経営戦略を推進。「金融とデジタルの力で未来を切り拓くNo.1ビジネスパートナー」となることを目指している。また、持続可能な社会・環境への貢献を果たすべく、サステナビリティ経営にも力を入れている。

https://www.bk.mufg.jp/

採用サービス

- クラウドストライク
レッドチーム演習サービス

実施期間：2022年9月下旬～2023年3月

中身の濃いテストを短期間で効率的に実施
クラウドストライクのグローバルな知見も
大きな威力を発揮

レッドチーム演習を実施する上では、限られた期間内でどれだけ成果を上げられるかも重要なポイントとなる。そこで今回は、攻撃スタートのターゲットに設定した海外拠点内へのマルウェア導入をあらかじめ同行側で実施。これをクラウドストライクのテスターが利用する形で演習をスタートしている。

「初期侵入をゼロから始める手もありますが、それだと時間もコストも余計に掛かってしまいます。その点、この方法であれば、短期間でスムーズに演習を行うことができます。また、昨今のセキュリティにおいては、内部侵入を前提とした対策が求められます。そうした意味でも、マルウェアに感染した段階から始めた方が、より実情に即した形でテストすることができます」と福野氏は語る。

取り組みを進める中では、クラウドストライクの技術力の高さを実感する場面も多かったとのこと。中村氏は「たとえば今回のレッドチーム演習には、日本のテスターだけでなく、海外のテスターも参加しています。その結果、海外のスキル、知識も含めた様々な攻撃を試してもらうことができました。グローバルに事業を展開する当行としても、こうした体験ができたことは非常に有意義でした」と満足感を示す。

また、テスト内容や日程の調整、突発的な事態への対応など、様々な事柄に柔軟、かつ真摯に対応してもらえた点も高く評価しているという。

得られた結果を今後のセキュリティ対策に反映
経営トップも含めた意識向上にも貢献

レッドチーム演習の結果、同行では多くの学びや気付きを得ることができた。福野氏は「当行では外部からの攻撃に対して多層防御によるセキュリティ対策を行っています。しかし、万一侵入された場合に備えて、より改善・強化すべきポイントもあることが分かってきました。今回の演習を通して、改善できる点がまだあることをより強く実感できました」と語る。

現在はクラウドストライクの指摘を元に、新たなセキュリティソリューションの導入や運用面での改善など、様々な取り組みを進めているとのこと。レポートの内容にも、高い評価が寄せられている。「クラウドストライクのレポートは他社と比べても非常に中身が充実しており、どういう流れで攻撃されたのか、どうすれば防げるのかが詳細に述べられています。おかげで社内の技術者からも非常に好評でした」と中村氏は語る。

また、経営トップ向けのエグゼクティブサマリも、セキュリティ強化の取り組みに大きく貢献。中村氏は「経営トップにもTLPT結果とリスク認識を報告することでグループ全体でセキュリティ対策をさらに進めていくとの意識を高められました。この点については、大変感謝しています」とにこやかに語る。

机上の検討だけでは見えてこないことも多いため、同行では今後も今回のような実機検証を積極的に推進していく考えだ。TLPTの発見事項を踏まえた課題についてグループ・グローバルに横展開する上で、現行の人員だけでは国内外の拠点をすべてカバーすることが難しいため、各拠点から協力を得ながら対応中とのこと。

クラウドストライクのレッドチーム演習は、システム面や運用面だけでなく、組織・体制の強化にも一役買うことができたのである。

「TLPTに加えて、行内でも実機検証できる部分については、私たち自身でも行っていきたい。もちろん、エキスパートでないと難しい領域も多いので、そうした点についてはクラウドストライクの支援や力添えも期待しています。グローバルに展開するMUFGグループ各社や金融業界のセキュリティを守ることが私たちのミッションです。その目標に向けて、今後も力を尽くしていきたいと思います」と中村氏は抱負を述べた。

株式会社三菱UFJ銀行
サイバーセキュリティ推進部
サイバーセキュリティグループ
調査役
中村 仁美 氏

株式会社三菱UFJ銀行
サイバーセキュリティ推進部
サイバーセキュリティグループ
調査役
福野 貴仁 氏

POINT

- 海外拠点を踏み台とした日本国内へのサイバー攻撃を実際に仕掛けることで、リスクを洗い出すことに成功
- グローバルの知見を活かした高い技術力を発揮しつつ、柔軟なプロジェクト運営を実施
- サイバーリスクへの認識を経営層全体で共有することに寄与
- レポートの報告内容を元にセキュリティ強化の取り組みをさらに推進

© 2023 CrowdStrike, Inc. All rights reserved.
CrowdStrike、Falconのロゴ、CrowdStrike Falcon、CrowdStrike Threat Graphは、CrowdStrike, Inc.が所有するマークであり、米国および各国の特許商標局に登録されています。CrowdStrikeは、その他の商標とサービスマークを所有し、第三者の製品やサービスを識別する目的で各社のブランド名を使用する場合があります。

CROWDSTRIKE

we stop breaches

クラウドストライク合同会社
お問い合わせ: **http://crowdstrike.jp/contact-us/**