Secureworks®

導入事例

サイバーレジリエンス強化に向け 脅威ベースのペネトレーションテスト（TLPT）を実施 安全・安心な金融サービスの実現に寄与

お客さまからの信頼を守るべく 全方位でセキュリティを強化

「お客さまの大切な資産を守ること、並びに金融サービスを安全かつ安定的に稼働させることが我々三菱 UFJ フィナンシャル・グループ（以下、MUFG）の社会的責務です。これが揺らぐことのないよう、各種サイバーセキュリティ対策を推進しています。」こう強調するのは、三菱 UFJ 銀行 システム企画部 サイバーセキュリティ推進室 サイバーセキュリティGr. 調査役 中村 仁美 氏だ。

一般にも広く知られている通り、同行もその一員である MUFG は、日本を代表するグローバル金融グループである。国内外に数多くのグループ企業や拠点を展開し、長年にわたり個人／法人顧客の多様な金融ニーズに応え続けてきた。多種多様な攻撃から金融システムを守り、安全・安心な金融サービスを提供し続けるために、サイバーセキュリティ推進室を中心として、様々な取り組みを全方位で展開している。

三菱 UFJ 銀行 システム企画部 サイバーセキュリティ推進室 サイバーセキュリティGr. 上席調査役 常見 敦史 氏は「サイバーセキュリティ推進室内に脅威インテリジェンス分析やセキュリティ関連業務を提供するセキュリティセンターとして、MUFG CSFC（MUFG Cyber Security Fusion Center）を立ち上げ、グループ・グローバルでのセキュリティ監視運用を日夜実施しています。また MUFG ではサイバーセキュリティ・インシデントに即応できる態勢としてインシデント対応チームの整備を進めており、グループ全体の統括として MUFG-CERT を設置しています。」と説明する。

Red Team テストの実績に 基づく多彩な攻撃力を高く評価し、 セキュアワークスの TLPT を選定

こうした取り組みの一環として、今回同行では「脅威ベースのペネトレーションテスト」（以下、TLPT）を実施した。中村 氏はその背景を「サイバー攻撃の高度化・巧妙化は、年々加速する一方です。当行でも、これまで様々なサイバーセキュリティ施策を推進してきました。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るものの、より高度な攻撃への対応能力を第三者の視点で評価したいと考えました。」と語る。

株式会社三菱 UFJ 銀行 システム企画部
サイバーセキュリティ推進室 サイバーセキュリティGr.
上席調査役
常見 敦史 氏

株式会社三菱 UFJ 銀行 システム企画部
サイバーセキュリティ推進室 サイバーセキュリティGr.
調査役
中村 仁美 氏

株式会社 三菱 UFJ 銀行

- お客様名：株式会社三菱 UFJ 銀行
- 資本金：1 兆 7199 億円（単体）
- 従業員数：30,554 名（2021 年 3 月末現在：単体）
- 所在地：東京都千代田区丸の内 2-7-1
- 公式 HP：https://www.bk.mufg.jp/

■ ソリューション

- TLPT（脅威ベースのペネトレーションテスト）

■ プロジェクトのテーマ

1. 標的型サイバー攻撃による不正取引
2. 標的型サイバー攻撃による情報漏えい

■ プロジェクト実施期間

- 2020 年 10 月 ～ 2021 年 3 月

SOC とは
Security Operation Center の略称。
インシデント監視・分析を担う組織。

同行が TLPT を実施するのはこれが初めてではなく、数年前から異なるテーマを選定して継続的に実施している。今回のテーマには標的型サイバー攻撃が選ばれたが、同テーマでの TLPT も以前に実施済みである。

「前述の MUFG CSFC によるグループ・グローバルのセキュリティ監視運用が新たに開始されるなど、以前 TLPT を実施した時とは社内の組織や体制も変わっています。そこで、現在の仕組みがきちんと機能しているか、何らかの脅威が侵入した場合に的確に検知してエスカレーションできるかを確認する狙いもありました。」と常見 氏は語る。

同行では、今回の TLPT 実施に向け、複数のセキュリティベンダーの提案を比較。その結果、パートナーに選ばれたのが、セキュアワークスである。中村 氏はその理由を「一番の魅力は、セキュアワークスの Red Team が保有する攻撃の多彩さです。標的型攻撃に使われる最新の手法から古典的な手法まで幅広く対応して頂きました。また、実際に TLPT を実施する上では、攻撃側に対してどの程度の情報をいつ開示するか、スケジュールとテストの目的を踏まえた様々な調整も必要です。提案時におけるコミュニケーションを通じて感じられた高い調整力も評価しました。」と語る。

また、常見 氏も「もう一つのポイントとして、セキュアワークスの豊富な実績が挙げられます。特に国内では、TLPT で実績あるベンダーやテスターがまだそれほど多くない。その点、セキュアワークスは今回のテーマである標的型サイバー攻撃の分野において海外含め多くの実績があり、力のあるテスターも多数在籍しています。また、質問や相談へのレスポンスが非常に速く的確であったことから、技術力と調整力の両面で信頼がおけたため、今回はセキュアワークスに依頼することにしました。」と続ける。

標的型サイバー攻撃を想定し、幅広い領域にわたる攻撃シミュレーションを実施

2020 年 10 月～ 2021 年 3 月にかけて実施された今回の TLPT では、「標的型サイバー攻撃による不正取引」と「標的型サイバー攻撃による情報漏えい」の 2 点を具体的なテーマに設定。事前調査から初期侵入、侵入後のマルウェア感染、他端末への横断的侵害、そして目的遂行といった標的型サイバー攻撃の典型的なプロセスに則り、最終的にはテスト用に設置された端末の不正操作が行えるかどうかを検証した。「加えて、最近ではコロナ禍にともないテレワークが増加していますので、リモートアクセス用端末に対する攻撃シミュレーションも実施しています。本番環境でのテストを前提に、業務影響が懸念される部分では適宜テスト環境を組み合わせて TLPT を行いました。」と中村 氏は説明する。

実施した TLPT の内容は、非常に満足のいくものだったとのこと。常見 氏は「たとえばインターネットバンキングを対象にテストを行う場合には、関連するシステムや業務が限られますので、ある程度シナリオも絞り込めます。ところが今回は、数万台規模のエンドポイントとそこにつながる業務システムを組み合わせたテストですから、想定される脅威や攻撃手法も相当幅が広い。そこで、テストシナリオとして抜けや漏れがないよう留意しながら、結果としてかなり幅広い内容で TLPT を行いました。おかげで、標的型サイバー攻撃に関しては、我々のやりたいことがほぼ網羅できました。」と語る。

対策の有効性を見事に実証 今後も継続的な改善を推進

さらに大きいのが、同行の標的型サイバー攻撃対策への取り組みが、十分な効果を発揮していると実証できた点だ。常見 氏は「SOC チームの監視対応が正しく機能しているかは、日々のアラート対応や定期的な訓練でも確認していますが、今回は TLPT の高度な攻撃に対しても正しく対応できるかを確認すべく、監視メンバーにテスト実施を知らせないブラインド形式で行いました。TLPT の内容や実施時期（いつ・どのようなテストが行われているか）を知らされていない SOC チームが「疑わしい事象がある」と判断し、私宛にエスカレーションをしてくれましたので、今回のテストシナリオに対してもセキュリティ監視が適切に機能することが確認できました。大きな成果だったと思います。」と満足げに語る。

本番環境を用いた TLPT を行うことには、いろいろと難しい点もあるとのこと。しかし、これをあえて実施したことで、「人・システム・プロセスそれぞれの観点で、想定通りの監視が実施できていることが確認できました。」（常見 氏）

もちろん、TLPT の結果からさらに強化すべき点もいくつか見つかっている。「リスク度の高・低に関わらず、すべての指摘事項に対する対応方針を決定しています。ひとつひとつの指摘はリスクが低くとも組み合わせて悪用されたらどうか、当行が定めるシステム開発のルールや手続が十分か、など関係部署と協議しながらセキュリティ対応態勢の見直しを進めています。」と中村 氏は説明する。

セキュアワークスが提供したレポートも、こうした取り組みに大きく貢献。常見 氏は「技術的に非常に詳細なレポートであることに加え、今後に向けた提言やアドバイスも盛り込んでもらえました。これを最大限に活用し、セキュリティの継続強化に取り組んでいきたい。それにより、お客さまに信頼される安全・安心な金融サービスをより一層盤石なものにしていきたいと思います。」と抱負を述べた。

セキュアワークス株式会社

お問い合わせ SCWX_PreSales@secureworks.com 03-4400-9373 www.secureworks.jp

Secureworks®