Secureworks®

導入事例

サイバーレジリエンスの強化に向け「Red Team Lite」による TLPT を実施 セキュアな業務環境の実現に寄与

顧客の資産形成を支える多彩な金融サービスを提供

大和証券グループのインターネット専業銀行として、2011 年 4 月に開業した大和ネクスト銀行。同行では「お客様の資産形成におけるベストパートナー」の経営ビジョンの下、預金を中心としたビジネスを展開。円預金や外貨預金、預金を通して社会貢献できる「応援定期預金」、対象通貨が異なる複数の定期預金をひとまとめにして預け入れる「バスケット定期預金」など、幅広いサービスをラインナップしている。

その同行の事業活動を ICT 面から下支えしているのが、情報システム部門である業務部だ。株式会社大和ネクスト銀行 業務部 次長 中根 啓一 氏は「当行では、各種の業務システムからオフィス環境、システムの介在しない業務フローに至るまで、すべて当部門が一手に引き受けています。お客様の大事な資産をお預かりする以上、高い信頼性や安全性の確保は大前提。とはいえ、使い勝手や利便性もおろそかにはできませんので、高いレベルで両者をバランスさせるよう心掛けています」と説明する。一度導入したシステムは長期間にわたって利用されるだけに、後々の運用も見据えた形で設計・構築を行っているとのことだ。

株式会社大和ネクスト銀行
業務部 次長
中根 啓一 氏

サイバーレジリエンスのさらなる強化を目指す

脅威の悪質化・巧妙化が年々深刻化する中、金融機関にとってはサイバーセキュリティの強化・拡充も重要な課題となっている。同行でも脆弱性診断を毎年実施するなどして、安心・安全な金融サービスの提供に努めてきた。そうした取り組みの一環として、今回同行では、TLPT(脅威ベースのペネトレーションテスト) を実施することとなった。

中根 氏はその背景を「最大の狙いは、サイバーレジリエンスのさらなる強化を図る点にあります。これまで当行が行ってきた脆弱性診断は、主に対外向けの公開システムを対象としていました。しかし、昨今猛威を奮っている『Emotet』の被害状況などを見ても、行員が普段使用している業務端末にマルウェアが侵入し、そこを踏み台として攻撃が拡がるケースも十分想定されます。万一、こうしたインシデントが発生した時に、システムだけでなく人のプロセスも含めてきちんとマニュアル通りの対応が取れるのか、あるいは現状のマニュアルに不足な点はないかといったことを、TLPT によって炙り出したいと考えました」と振り返る。

TLPT 担当ベンダーの選定にあたっては、

株式会社大和ネクスト銀行
業務部
小泉 勇人 氏

大和ネクスト銀行
Daiwa Next Bank

- お客様名：株式会社大和ネクスト銀行
- 資本金：500 億円
- 開　業：2011 年 4 月 15 日
- 所在地：東京都千代田区丸の内 1-9-1
- U R L：https://www.bank-daiwa.co.jp/

■ ソリューション

- Red Team Lite

■ プロジェクトのゴール

1. Active Directory 管理者権限の取得
2. ファイルサーバー内の特定ファイルへのアクセス

■ プロジェクト実施期間

- 2021 年 8 月 ～ 9 月

まず特定のシナリオにあまり捉われすぎず自由な攻撃が行えることが要件として掲げられた。「実際の脅威と同様の形で攻撃してもらわないと、本当に穴があるかどうか分からない」(中根 氏)というのがその理由だ。とはいえ、あまり自由に攻撃し過ぎると、今度は本番業務にまで影響が生じるおそれもある。これは絶対に避けなくてはならないため、攻撃範囲を柔軟に調整できることも重要なポイントとなった。

この相反する要件を満たせるサービスとして採用されたのが、セキュアワークスの「Red Team Lite」である。中根 氏はその決め手を「Red Team Lite であれば、特定のプロセスに限定した形で実践的な攻撃シミュレーションが行えますし、攻めてはいけないところを除外することもできます。また、今回の TLPT は、いかに短期間で最大限の費用対効果が発揮できるかも重視しました」と語る。ちなみにセキュアワークスでは、以前に同行の脆弱性診断を実施した経験もある。その時の実績も評価につながったとのことだ。

Red Team Lite による TLPT を実施 これまでの対策の有効性を実証

2021年8～9月に掛けて実施されたテストでは、「ファイルサーバー内に設置した特定フォルダへのアクセス」がゴールとして設定された。中根 氏は「シナリオ検討の過程では、他にも様々な業務システムが候補に挙がりましたし、セキュアワークスからもいろいろ形での攻撃が可能との提案を貰いました。しかし、前述の通り本番データを扱うシステムを対象とするのはリスクが高いですし、期間的な問題もあります。そこで今回は、権限設定の異なる2種類のフォルダをテスト用に作成。ここに保存されたファイルにアクセスできるかどうかをチェックすることにしました」と説明する。

Red Team Lite では、脅威が侵入したことを仮定した段階からテストを開始するため、業務端末への疑似マルウェア導入作業などは同行側で実施。併せて、セキュアワークスが用意した攻撃用デバイスも社内 LAN に接続している。「TLPT を実施していること自体は、行内のメンバーに対して特に伏せてはいません。とはいえ、あくまでも普段通りのプロセスで脅威に対処できるか確認することが今回の目的です。このため、『どういう攻撃が来るぞ』とか『ここに気を付けて下さい』といったことは一切伝えませんでした」と中根氏は語る。

攻撃を仕掛ける過程では、思わぬ発見もあった。業務端末に導入した疑似マルウェアを起動したところ、その都度セキュリティシステムに検知されてしまい、なかなかテストを始められなかったのだ。「当行では、入口・出口・内部の多層防御をしっかりと作り込んでいます。これがかなりの効果を発揮したことで、逆にテストが難しくなってしまった」と中根氏は苦笑する。

図らずも、これまでの対策の有効性が実証された形になったわけだが、その一方で新たな気づきも得られたという。中根 氏は「こんなにすぐに検知されるようでは、攻撃者もあきらめてしまうのではないかと感じました。しかし、セキュアワークスによれば、決してそのようなことはなくスピード勝負で何度も攻撃を繰り返してくるとのこと。これを聞いて、インシデント対応を迅速に行うことの大事さを改めて再認識しました」と語る。

実地対応の経験が貴重な財産に マニュアルの改善にも寄与

今回の TLPT を実施したことで、得られた成果も大きかったとのこと。大和ネクスト銀行 業務部 小泉 勇人 氏は「元々当行では、強固なセキュリティ態勢を築いています。このため、これまでは実際にマルウェアを検知したりする機会がありませんでした。今回のTLPTによって、これを体感できたことは非常に良い経験になりました」と語る。

いくら取るべきアクションや確認事項などがマニュアルに記載されていても、いざその場に遭遇すると混乱も起きがちだ。「こうした点でも、TLPT を実施したメリットは大きかった。今回、私はブルーチーム側のメンバーとして参加しましたが、インシデント発生時にどう動けば良いのかがシミュレーションできましたので、いざという際もあわてず対応できると考えています」と小泉 氏は続ける。

セキュアワークスが提供したレポートも、今後の対策強化に大きく貢献している。小泉 氏は「今回のテスト結果を踏まえて、既にマニュアルの改訂を実施しました。これにより、従来よりも幅広いパターンの攻撃に対応できるようになっています。セキュアワークスのレポートでは、様々な改善点やリスクが優先順位別に示されますので、迷うことなく的確な手を打つことができました」と語る。

「今回実施した TLPT は、サイバーレジリエンスの強化という目的に十分資する取り組みでした」と高く評価する中根 氏。もちろん今後も、引き続き環境改善に注力していく考えだ。中根 氏は今後の展望を「たとえば当行でもゼロトラスト化を進めていますが、境界防御型の対策とは変わる部分もでてきますので、適切な対策を施していきたい。セキュリティ分野は変化が激しく、ユーザー企業だけではなかなか追い付かない面もあります。セキュアワークスには、いろいろな知見やソリューションがあると思いますので、ぜひ今後も積極的な情報提供や提案を期待したいですね」と述べた。

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®