導入事例

お客様の情報資産を守るための重要施策である脆弱性管理に TENABLE.IO を導入 ～ 三菱 UFJ 銀行

東京に本拠を置き、国内 519、海外 107 の支店を持つ株式会社三菱 UFJ 銀行は、世界でも屈指の銀行です。昨今、同社システムにおける脆弱性管理の自動化・集中化のために「Tenable.io」を導入しました。その経緯や導入効果などについて、常見氏と打田氏にお話を伺いました。

導入企業について

企業名: 株式会社三菱 UFJ 銀行

資本金: 1 兆 7199 億円(単体)

従業員数: 30,000 人以上

支店数: 国内 519、海外 107

業種: 金融

導入効果

- 脆弱性管理の自動化により、管理集中化に向けたスタートを切ることができた
- OS やミドルウェアの設定における主要なセキュリティ基準に対する準拠状況を評価するためのコンプライアンスチェックの自動化にも活用予定

公式HP: https://www.bk.mufg.jp/

ソリューション

tenable.io

インタビューイ

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
次長(特命)常見敦史様

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
上席調査役 打田悠様

株式会社三菱 UFJ 銀行一問一答

脆弱性管理サイクルの頻度向上が課題に

三菱 UFJ 銀行様のセキュリティの取り組みについて教えてください。

打田氏: 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をミッションとして、各種サイバーセキュリティ対策を全方位で展開しています。

常見氏: インシデント対応チームとして MUFG-CERT を立ち上げ、グローバル SOC や脅威分析の専担ライン組成などのサイバーセキュリティ施策を推進しています。また、金融機関同士でサイバー攻撃情報などを共有し、対策していく取り組みにも参加しています。

今後一年で優先的に実施するセキュリティ対策について教えてください。

打田氏: 情報システムの堅牢化や脆弱性管理、ID アクセス管理といった内部防衛力の強化につながる領域を重点施策として対応を継続しています。特に脆弱性管理については、脆弱性を発見し、評価し、対処していくというサイクルを高頻度で実施するために、プロセスを可能な限り自動化・集中化することを目指しています。

Tenable.io の導入につながった課題について教えてください。

打田氏: インターネット公開システムに対するセキュリティ侵害リスクや、OS やサーバーなどに脆弱性が残置されているリスクへの対応として、これまでは脆弱性診断ツールを手動で実行していました。そのため、前述のとおり脆弱性管理のサイクルの頻度を高めて強化していくうえでは、さらなる効率化が大きな課題となっていました。

脆弱性の内容にもよりますが、脆弱性情報が公開され、それを悪用した攻撃が行われるまでの時間は想像以上に短いです。手動での脆弱性診断を継続していては、重要な脆弱性に迅速に対応できず、攻撃者に悪用の機会を与えてしまうことに繋がる恐れがあります。

常見氏: セキュリティベンダーの調査レポートによると、数年前までは不審なメールや Web サイトを見てマルウェアに感染するケースの報告件数が多かったのに対し、近年では外部公開サーバーやデバイスの脆弱性が悪用されることによる情報漏洩やランサムウェア感染被害の報告件数が上位にくるなど、脅威環境も変化しています。昨今多くの被害が確認されている二重脅迫型ランサムウェアについても、脆弱な VPN 装置や RDP の設定不備が侵入経路として狙われたケースが確認されており、脆弱性管理や設定不備の確認はより細かいサイクルで実施していくことが重要になっています。

コンプライアンスチェックや手厚いサポートなどを評価

解決策を選んだ経緯、そして Tenable.io を選んだ理由を教えてください。

打田氏: 主要な脆弱性スキャンツールを中心に、多くのベンダーの製品やソリューションについて情報収集し検討しました。最終的には、検出可能な脆弱性の種類が幅広いこと、OS やミドルウェアの設定における主要なセキュリティ基準に対する準拠状況を評価するためのコンプライアンスチェック機能も有していること、Tenable 社の国内におけるサポート面の手厚さなどを理由に、Tenable.io を選びました。

常見氏: ダッシュボードで脆弱性情報を一元的に管理できることも、脆弱性管理の集中化を目指す弊社においては選定の決め手のひとつでした。

検討から導入までの期間について教えてください。

打田氏: もともとコンプライアンスチェック強化の目的で Tenable.io を検討していました。その後、脆弱性管理の強化もあわせて必要であるという課題認識から、2019 年頃より脆弱性管理とコンプライアンスチェックのソリューションの導入を加速させていきました。

2019 年の 11 月頃に Tenable.io を用いた概念実証を実施し、翌年 6 月頃に導入を決定しました。本番環境での利用は 2020 年の 11 月から開始しています。脆弱性スキャンの自動化は弊社の国内システム向けには初の試みであったため、課題分析や要件定義には時間をかけました。導入は完了しましたが、今後は利用範囲を順次拡大していく予定ですので、やっとスタートを切ったという感覚です。

導入自体は問題なく進んだのでしょうか?

打田氏: 実現したいことは 2 点ありました。ひとつはクラウドからグローバル IP アドレスをスキャンする仕組みを作ることですが、これはクラウドスキャナーを有する Tenable.io のライセンスを契約するだけですぐに使えますので、特に問題はありませんでした。もうひとつは、内部ネットワークに繋がる機器のスキャンをすることです。これの実現のためには、オンプレミスのスキャナー用サーバーの設置が必要でした。データセンターが複数の場所にあり、多数のシステムを有する弊社において、最も効率的なサーバー設置場所やネットワーク構成を決めるのには時間を要しました。

脆弱性管理の自動化・集中化を実現するためのスタートラインに立てた

Tenable.io を導入したことによる変化や効果について教えてください。

打田氏: 自動化・集中化を実現するためのスタートラインに立てたことが、何よりも大きな変化であると考えています。これは、弊社における脆弱性管理やコンプライアンスチェックの強化、ひいては内部防衛力の強化のために必達と考えているからです。また、弊社はミッションクリティカルなシステムが多数あり、脆弱性スキャン実施時にはシステムに影響が出ることを想定して立ち会うこともありますが、頻度を高めるにあたっては安全安心に脆弱性診断ができる状態を作ることも重要です。Tenable.io はこうした観点からの診断時のきめ細かい設定が可能であることも評価ポイントだと思います。

常見氏: 脆弱性診断の質を維持しながら頻度も向上させるというのは、これまでのやり方では困難な課題でした。Tenable.io を導入したことで自動化の可能性が見えたことは、間違いなく成果だと思っています。

三菱 UFJ 銀行様の今後の取り組みについて教えてください。

打田氏: 脆弱性管理やコンプライアンスチェックの領域においては、前述のとおり Tenable.io を中心とした自動化・集中化をさらに推進していきます。脆弱性管理はサイバー攻撃への耐性を高め、安定した金融サービスの提供を維持するという観点からも重要で、これを確りと徹底することが企業の信頼性の維持にもつながります。是非 Tenable 社と共に解決していけたらと思います。

Tenable 社に対して、感想やご意見があればお願いします。

打田氏: Tenable 社は脆弱性管理ソリューション一筋というイメージです。それはとても素晴らしいことだと思っています。専門ベンダーならではの脆弱性分析レポートや、使い方を説明するウェビナーなども有用ですし、いろいろな相談にも乗っていただいています。今後も脆弱性管理の強化に向けて、共に歩んでいけたらと思います。

Tenable について

Tenable, Inc. は、脆弱性管理ソリューションを提供します。世界中の 4 万以上の企業と組織がサイバーリスクを正確に把握し、削減するために Tenable を活用しています。Nessus® の開発者である Tenable は、脆弱性に対する専門性を基盤に、あらゆるコンピューティングプラットフォーム上のあらゆるデジタル資産を管理、保護できる世界初のプラットフォームを展開しました。Tenable は、フォーチュン 500 の半数以上、およびグローバル 2000 のおよそ 4 割の企業や、大規模な政府機関などで採用されています。詳しくは、jp.tenable.com をご覧ください。