Google Cloud

Mandiant の Attack Surface Management で 自社のインターネット公開資産を正確に把握し、セキュリティ対策を万全に

最新の脅威情報の収集とそれに基づく具体的な対策、その双方が求められる企業のセキュリティ対策。しかも、DX 推進により IT への依存度が増し、攻撃の高度化が加速する今日においては、これらを継続的にアップデートしていかなければなりません。そうした中、三井不動産株式会社（以下、三井不動産）は新時代のセキュリティ対策手法の 1 つとして注目を集める Mandiant の「ASM（Attack Surface Management）」をいち早く導入。その成果について同社セキュリティ対策担当者に伺いました。

利用しているサービス

Mandiant Advantage Attack Surface Management　など

三井不動産 MITSUI FUDOSAN

三井不動産株式会社

https://www.mitsuifudosan.co.jp/
〒103-0022　東京都中央区日本橋室町 2-1-1

三井グループの中核企業の 1 つとして、オフィスビルや大型商業施設の開発など「街づくり」を推進する業界最大手の総合不動産デベロッパー。近年は『VISION 2025』のもと、「テクノロジーを活用し、不動産業そのものをイノベーション」することなどを掲げており、ICT を駆使した顧客満足度のさらなる向上や、データに基づく新たな価値創出を追求している。従業員数は 1,898 名（2022 年 3 月 31 日現在）。

インタビュイー

・DX 一部 DX グループ サイバーセキュリティチーム
技術主事 西下 宗志 氏

"現場" が欲しい情報を提供してくれる Mandiant の ASM

ルーターやサーバー、その上で動作するソフトウェアなど、インターネット上に公開されている企業の IT 資産は、公開した瞬間からサイバー攻撃の対象となるリスクをはらんでいます。三井不動産では社内にサイバーセキュリティチームを設けてこれに対応していますが、年々高度化、悪質化するサイバー攻撃への対策は容易ではありません。同チームにおいてインシデント対応とリスクアセスメントを担当する DX 一部 DX グループ サイバーセキュリティチーム 技術主事 西下 宗志氏は、その難しさを次のように説明します。

「インターネット公開資産に対するセキュリティ対策は、脆弱（ぜいじゃく）性スキャンなど一通りのことを行っているのですが、そもそも我々が把握していない資産についてはどうしようもありません。インターネット公開資産は各部署やグループ企業からの申請ベースでの把握が基本のため、どうしても抜けがあります。特にクラウド活用が進んだ昨今は、社員ですら資産状況を正確に認識しきれていないことがあり、課題となっていました。」

不動産業界では、他業界と比べて広く、多くの個人情報を取り扱うほか、オフィスビルの入館システムや空調管理などに IT を活用する動きが今後さらに加速していくことが確実視されており、防犯・防災の観点からもこれまで以上にセキュリティの重要性が高まっていくと言われています。

そうした中、西下氏はサイバー攻撃から自社資産を守る手法として「ASM」に注目。米国のサイバーセキュリティ企業 Mandiant（2022 年 9 月より Google 傘下）の提供する ASM サービス導入を決意しました。

ASM とは、インターネットと自社資産の境界を監視し、把握できていない資産を探索してデータベース化したうえで、設定ミスや、放置された脆弱性などの攻撃の標的となる箇所（Attack Surface）を発見・報告してくれるというもの。Mandiant は動的なサイバー防御、脅威インテリジェンス、インシデント対応サービスのリーダー企業として知られており、もちろん ASM においても大きな実績を誇っています。

Attack Surface Management の検討過程

インターネット公開資産における課題

1. 多数のインターネット公開資産。 全量の状況把握が困難
2. CMSのバージョン、 脆弱性管理が難しい
3. 管理漏れとなっているインターネット公開資産が無いか不安

→ Attack Surface Management での解決が可能

Attack Surface Management を使えば、

1. 管理画面の把握やVPNの把握、 テスト環境、 開発環境の把握ができる
2. CMSの利用状況や脆弱性情報等が把握できる
3. ASMで発見した資産とグローバルIP管理台帳、 Webサイト管理台帳を照合し、 管理できていない資産を把握できる

「実は ASM 導入以前から、Mandiant の脅威インテリジェンス情報提供サービスを利用しており、その知見・感度の高さに感銘を受けていました。そのため同社の提供する ASM であれば信頼できるだろう、と。そのうえで、Mandiant の ASM は、セキュリティ対策現場のエンジニアが欲する情報を丁寧に提供してくれるところが好印象でした。例えばこれまで把握していなかった資産が見つかった際、どのように見つけてきたのかをその根拠とともに報告してくれます。また、脆弱性の通知に関しても、公式や研究機関のレポートなどを併せて提示してくれるため、納得感のある状態で対策を進めることができます。」

ASM はこれからの時代に欠かせないセキュリティ ツール

こうして 2023 年 4 月から ASM を本格導入した三井不動産サイバーセキュリティチームですが、実際に運用を開始したところ、当初想定していたよりも多くの未把握資産が見つかり驚かされたそうです。

「実際にスキャンしてみたら 、当初見積もっていた総資産数の 3 倍以上の件数が出てきてびっくりしましたね。ただ、Mandiant の ASM はそれぞれのイシューに重要度を設定してくれているため、まずはクリティカルなものから対応していくことで、効率的に対策を進めることができました。この際、エンジニア的には、なぜクリティカルなのかを生データで確認できるのがありがたかったです。事態を正確に把握しやすいだけでなく、上長らに報告する際にも具体性を持って説明できるメリットがあります。もちろんサマリーも用意されていますから、非エンジニアでも使いやすいツールと言えるのではないでしょうか。なお、個人的に気に入っているのが、発見された脆弱性について、現時点ですぐに悪用可能なのか、あるいは将来的に悪用される可能性がある程度なのかを分類してくれること。これは現場ではとても役立つ機能なのですが、なかなかここまで踏み込んでくれるツールはなく、さすがは 脅威インテリジェンスに強みを持つ Mandiant だと感心しています。」

そのほか同社では「バーチャル インシデント対応」という形でも ASM を活用。他社のインシデント事例が自社でも起こりうるかの調査を ASM を用いて行い、リスクがある場合はすぐにパッチの適用などのアクションにつなげることができているとのことです。

「Mandiant の ASM を導入してまだ数か月ですが、もう 1 つ印象に残っているのがサポートの手厚さです。まだ導入したばかりということもあり、定例ミーティングで質問や要望を細かく出させていただいているのですが、日本法人の担当者はもちろん、カスタマー サクセス エンジニアのレスポンスも早く、とても助かっています。あるときはミーティングの最中に米国の担当者につないでいただき、その場で質問の回答を得られたということもあったんですよ。」すでに ASM の機能には満足していると言う西下氏ですが、生成 AI の実用化など、最新の IT ムーブメントを受け、その重要度はさらに増していくだろうと予測します。

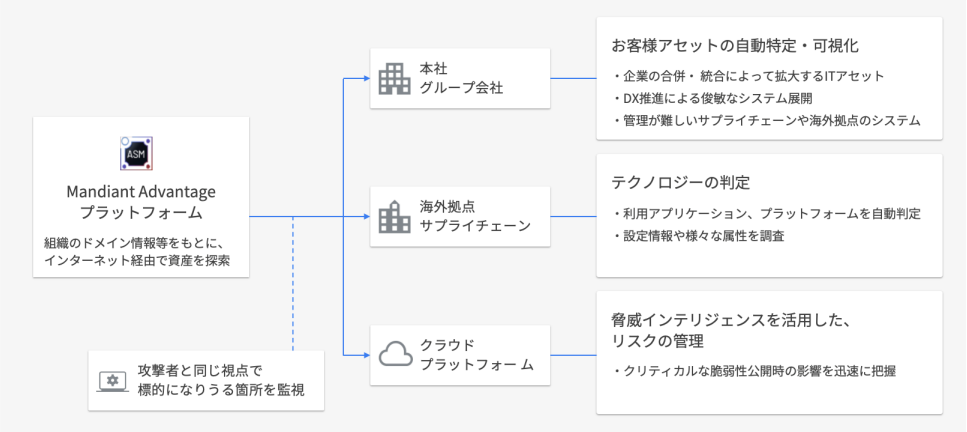
「生成 AI はサイバー攻撃をする側にとっても便利なツールで、これによって今後、マルウェアの亜種作成が自動化されたり、フィッシング メールがより巧妙化することなどが予測されています。攻撃件数もこれからどんどん増えていくでしょう。我々の仕事は、そうした中でも情報をアップデートし続け、社内に展開していくこと。ASM はそのためにも極めて重要なツールだと認識しています。」

したがって、ASM 単体の機能向上だけでなく、Mandiant が Google 子会社となった強みを生かした、Google Cloud との連携や統合が求められると西下氏は言います。

「Google は世界最大規模のテレメトリー情報を保有する企業であり、同時に、おそらく世界で最もサイバー攻撃を受けている企業ではないかと想像しています。そんな Google が提供する生成 AI をはじめとする技術や保有する脅威情報が、今後、Mandiant のソリューションに生かされていくことに期待しています。また、次世代 SIEM（Security Information and Event Management）として話題になっている Chronicle など、Google Cloud の既存セキュリティ ソリューションとの連携も楽しみにしています。」

Attack Surface Management - ASM とは

攻撃者視点でデジタル アセットがもたらすリスクを把握し、 攻撃者が悪用する前に、対策を行うことを実現する



攻撃者から狙われる箇所こそ 「自動で定常的に監視」 し 「優先的に対応」 する

Google Cloud を活用することで、ビジネスの将来に注力できるようになります。インフラストラクチャの管理やサーバーのプロビジョニング、ネットワークの構成などに起因する負担を軽減することができます。つまり、イノベーターもプログラマーも、自分の本来の仕事に集中することができます。

お問い合わせはこちらから
https://goo.gl/CCZL78

Google Cloud

Google Cloud の詳細については、右記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。