TANIUM

困難を極めるサプライチェーンのセキュリティ：そのあるべき姿とは？

サプライチェーン全体を的確に管理するために、企業は多くの課題を抱えています。セキュリティのベストプラクティスを実践するためには、まず全IT資産の可視化に着手すべきです。

サイバーセキュリティの侵害事例は後を絶ちません。新たなインシデントが起こるたび、セキュリティ担当者やCEOは、自社が被害に遭わなかったことに胸をなで下ろしています。しかし、いつ自社が大規模なサプライチェーン攻撃のターゲットになるかはわかりません。攻撃者は常に次なるチャンスを探っています。

今でも多くの企業は、サードパーティのソフトウェア、ハードウェア、サービスプロバイダなどを盲目的に信頼しており、連携の取れていない多くのレポートやサイバーデータから手作業で集約したスプレッドシートに過度に依存しがちです。

豊富な定量的データと、信頼できるサードパーティの指標や評価を活用したより優れた方法を、業界を挙げて確立しなければなりません。

サプライチェーン全体を管理しようとすると、当然ながら課題はさらに複雑になります。サードパーティがさらに別のサードパーティ製品を利用している場合、セキュリティを保証することはできるのでしょうか？何段階先まで追跡することができるでしょうか？

グローバルに事業を展開する企業は、このような課題に何年も労力を費やしてきましたが、シンプルな答えは存在しません。わかっているのは、サプライチェーンのセキュリティに関するベストプラクティスは、自社や取引先のIT資産の可視化なくしては実現できないということです。

基本に立ち返ることで、まずは「サプライヤーはどの会社か？」、「サプライヤーのセキュリティの成熟度はどの程度か？」、「どのデータにアクセスする権限があるのか？」「そのデータはどう使われているか？」といったリスクを算出するための基本的な問いに答えることができるようになります。

サプライチェーンの問題点

現代のサプライチェーンは複雑化しており、リスクを管理しようとしても、あっという間に手に負えない状況に陥ってしまいます。大企業の多くは、複数の側面からリスクにさらされています。デジタルビジネスでは、SaaS製品、グローバルなデータ処理サービス、サードパーティが提供するハードウェア、アウトソースのソフトウェア開発者、コンサルティングサービスなどを利用することもよくあり、こうしたサードパーティもまた、さらに別のサードパーティを利用しています。

多くの企業は何十年にも渡って、サプライヤーのリスクを算出するために、極端に単純化した質問（「パッチ管理を行っていますか？」など）を使って、手作業のプロセスや監査を進めてきましたが、こうした取組みは役には立ちません。

このようなやり方では、「はい/いいえ」の二者択一の回答や、主観的な回答を引き出すことになり、第三者による検証もできません。

SolarWindsのインシデントが引き起こした事態を例に考えてみましょう。ある企業では、このような質問をサプライヤーに投げかけました。「環境内で、SolarWindsのOrionの影響を受けたバージョンはありますか？」

しかし、この質問に「はい/いいえ」で回答してもらっても、重大なリスクを算出するために必要な情報を得ることはできません。

資産やアプリケーションの管理プロセスが十分に整っていない場合、サプライヤーは明確な回答を持っていない可能性すらあります。部分的なデータや不完全なデータに基づいた情報では、意味がありません。

成熟した企業であれば、自由回答式の質問をサプライヤーへ投げかけます（「脅威に対してどのように取り組んでいますか？」「パッチ管理の手法について説明してください」など）。このように全体像を確認する質問に回答してもらうことで、サプライヤーのセキュリティ対応に関してより広範囲の情報を得ることができます。

また、スプレッドシートを手作業で管理する方法をやめて、サプライヤーのセキュリティ状態をより厳格に評価するためのソリューションを活用しようと考える企業もあります。

しかし、多くのサービスは限定的な基準や主観的な評価をもとにしているため、「外側」から見た不完全な見解しか提供できないことになります。これでは全体像を把握できず、あまり参考にはなりません。このような失敗は、氷山の一角に過ぎません。

サプライチェーンのセキュリティの主な課題

セキュリティチームやリスクチームの関与が遅すぎる

新規のサプライヤーとの取引を開始する際に、サプライチェーンのガバナンスが機能し始めるタイミングが遅すぎるために、検出されたリスクの軽減や排除に十分な時間をとれないことはよくありがちです。セキュリティチームやリスクチームは、会社から新しいサプライヤーを承認しろという大きなプレッシャーを受けることもあり、「Noしか言わない部署だ」と思われたくないあまり、最高情報セキュリティ責任者（CISO）が承認せざるを得ないと感じる場合もあります。

状況の見直しを行わない

取引を開始する際に厳しいチェックを行うのと同様に、関係性を定期的に再評価することも重要です。

たとえば、当初は少数の開発者がテストデータのみを扱うために契約したSaaSプロバイダのサービスでも、時が経てば何百人もの従業員が利用し、重要なビジネス情報を扱うことになる場合もあります。

リスクが進化するのに合わせて動的なリスク管理を行うためには、定期的な状況の見直しが不可欠です。しかし残念なことに、サプライチェーンのセキュリティにおいては、「一度設定したらほったらかし」にしている企業が多いのが現状です。

全体を可視化して保証することが困難

サードパーティのリスク管理以外にも、上流であれ下流であれ、幅が広がるにつれて課題も増加します。

サプライヤーのサプライヤーはどう管理すればいいのでしょうか？さらにその先のサプライヤーはどうでしょう？サプライヤー全体のリスクを管理するにあたって、業界全体で利用できる、一貫性のあるベストプラクティスがないことが問題です。

サプライヤーに、脅威モデルやリスク分析に基づく詳細なデータの提供を依頼しても取引先に対して、簡易でおざなりな調査しか行わない可能性があります。サプライチェーンの各コンポーネントが異なる場合、リスクを総合的に判断することは、非常に困難になります。

次に何が起こるのか？

成熟したサイバーセキュリティプログラムを導入している企業の多くはここまで挙げてきた課題に苦労しています。だからこそ基本に立ち返り、サプライヤーの実態やそのセキュリティ成熟度、提供したデータの利用方法など、基本的な問いに答える必要があります。

このような課題の答えは、結局は可視化に行き着きます。自社が保有するIT資産は何か、そこで何が実行されているか、サードパーティとはどのような依存関係が存在するかを把握しなければなりません。

これはシンプルなことですが、簡単にできるとは限りません。**タニウムの調査**によると、グローバルに活躍するITエグゼクティブやマネージャの94%が存在を認識していなかったエンドポイントが環境内で見つかったことがあると回答しています。

サプライヤーに対しても状況の可視化を要求する必要があります。サプライヤーはIT資産について全てを網羅した正確なインベントリを提供し、状態やインストールされているソフトウェアのバージョンなどを把握しておくべきです。また、リスクに対応するために迅速にパッチを適用できる仕組みも必要です。

このようにインベントリを1つの要素として、サプライヤーのセキュリティ状態の総合的な成熟度を判断する、包括的な取組みが求められます。一時しのぎの局所的なパッチ適用や脆弱性の測定だけではなく、脅威モデリングやセキュリティを確保したソフトウェア開発、セキュリティアーキテクチャなどに対するアプローチも考慮する必要があります。

単に「このソフトウェアのこのバージョンを使っていますか？」と質問するだけではなく、社内の人材育成や技術開発のプロセスも考慮しなくてはなりません。

「マルウェアが埋め込まれていたSolarWindsのOrionのアップデートを実行していましたか？」といった慣例的な質問をすれば、一時的な見せかけの保証は得られるかもしれませんが、次に世界的なサイバー攻撃が発生した場合には何の役にも立ちません。サプライチェーンのセキュリティを実効性のあるものにするためには対象範囲を大幅に拡大したアプローチが必要です。把握すべきは次のような項目です。

- 重要なパッチの適用にかかる平均的な時間
- CISベンチマークハードニング標準(CIS Benchmark Hardening Standard)に準拠していないエンドポイントの割合
- 企業の定めたエンドポイントセキュリティツール（AV、パッチ/脆弱性管理エージェント）がインストールされていないエンドポイントの割合

こうした定量的なデータを入手できたら、サードパーティの指標や評価と合わせて、各サプライヤーのリスクについて360度可視化することができます。**ISO 27001**など国際的な基準を活用することもできます。

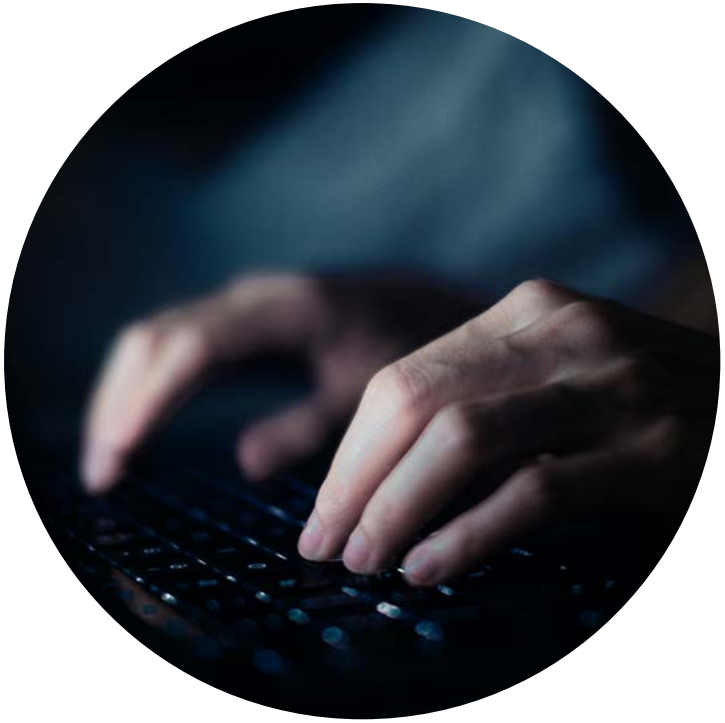
サプライチェーンの保護をプロセスの一部に

次のステップでは、最低限の要件を定義し、それを契約に入れ込みます。これにより、多くの企業が依存しているスプレッドシートを使った確認方法に代わって、一貫性の高いデータ主導型のアプローチを取ることが可能になります。

サプライチェーンの保護を実践する方法は他にもあります。

- 新規サプライヤーのチェックプロセスに、セキュリティチームとリスクチームが早い段階で関与する。提供されるサービスの機密性に基づいて要件を決定する。
- セキュリティの認定を定期的に実施し、提供されるサービスの重要性との整合性を保つ。
- 総合的な脅威モデリングとリスク分析を実行し、主な攻撃者は誰か、どこをどのように攻撃される可能性があるかの理解を深める。これをサプライチェーンのセキュリティ戦略に活用することができる。
- サプライヤーが、最悪のシナリオが発生した場合の侵害通知プロセスを明確に定めていることを確認する。
- セキュリティソフトウェア開発ライフサイクル（SDLC）に対するサプライヤーの取組みを把握する。サプライヤーの開発者はアプリケーションセキュリティについてどのようにトレーニングや認定を受けているか、静的分析や動的分析のプロセスはどのようなものかを理解する。
- インシデント対応のためのプレーブックを定義し、最悪の事態が発生した場合にどのような対応が必要かを把握する。

ここに挙げた項目ではすべてを網羅できておらず、サプライチェーン全体を保証するにあたっての課題を解決するものではないことにお気付きになったかと思います。これは、私たちが業界として注意深く検討すべきトピックなのです。



自社が抱えるリスクを知りたい方は

Taniumを使ってリスクを可視化してみませんか？
詳細はぜひお問合せください。

お問合せはこちら

業界唯一の統合型エンドポイント管理（XEM）プロバイダであるタニウムは、複雑なセキュリティとテクノロジー環境を管理するための従来のアプローチにおけるパラダイムシフトをリードしています。デバイス間の包括的な可視性、統一されたコントロールセット、そして「機密情報と大規模インフラの保護」という単一の共有目的に向けた共通のタクソノミを提供する単一のプラットフォーム内にIT、コンプライアンス、セキュリティ、リスクを統合することで、タニウムは、すべてのチーム、エンドポイント、ワークフローをサイバー脅威から保護します。タニウムは、「Fortune 100 Best Companies to Work For」に含まれ、6年連続で「Forbes Cloud 100」に選ばれています。実際、Fortune 100の半数以上と米軍は、タニウムが人々を保護し、データを守り、システムを保護し、あらゆる場所のあらゆるエンドポイントを監視して制御することを信頼しています。これが“The Power of Certainty”です。

www.tanium.jpをご覧いただき、**Facebook**と**Twitter**でフォローしてください。