PRESS RELEASE

2018 年 9 月 27 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」

約半数の組織が、サイバーリスク対策の基盤として戦略的脆弱性評価ソリューションを使用していると発表

※本リリースは 2018 年 8 月 8 日（米国時間）に米国で発表されたプレスリリースの抄訳版です。原文は下記 URL を参照ください。

https://www.tenable.com/press-releases/tenable-research-reveals-nearly-half-of-organizations-use-strategic-vulnerability

企業の様々な情報資産の脆弱性を手間なく自動で可視化、改善するソリューションを提供する『Tenable Network Security』（以下：テナブル、所在地：メリーランド州コロンビア、代表：Amit Yoran（アミット・ヨーラン）が結成したデータサイエンスチーム「Tenable Research」は、2,100 の組織を対象とした、サイバーリスクに対する組織の評価を分析した『The Cyber Defender Strategies Report』を公開しました。

本調査によると、世界の 48 %近くの組織が戦略的脆弱性評価（ビジネス視点において情報資産を正確かつ的確にスキャンし、優先順位付けをするプログラムとして認められるものとする）を取り入れ、サイバーリスク対策の基本的な要素として、またリスクを軽減するための重要ステップとしています。しかし、包括的な情報資産管理がプログラムの基盤となっているプログラムを有している組織のなかで、情報資産のサイバーリスクを正確に把握できている組織はわずか 5 %であることが判明しました。一方、組織の 33%は脆弱性評価に対してミニマリスト的なアプローチで、コンプライアンス規則が必要とする最低限の対策を講じ、事業に致命的に影響を与えるサイバーリスクの危険性を増長させています。

レポートのダウンロード：https://jp.tenable.com/cyber-exposure/attackers-advantage

Tenable Research が前回公開したレポート「Quantifying the Attacker's First-Mover Advantage」では、防御側が脆弱性を初めて評価するまでに、約 7 日間かかるということが判明しました。この間、攻撃側が脆弱性をエクスプロイトする期間が生じていたこととなります。結果として生じる 7 日間のギャップの中で、企業が戦略的かつ深いアプローチで脆弱性評価を意識すればするほど、事業へのリスクを最小限に抑えることができます。

【米国テナブル社 Tom Parsons 氏（プロダクト責任者（シニアディレクター））のコメント】

「近い将来、組織は二つのタイプに分かれるでしょう。すなわち、サイバーリスクの軽減という課題に立ち向かう組織と、絶えず進化し加速化する現代のコンピューティング環境におけるサイバーリスクの脅威に適応できない組織の二種類です。この調査は組織に対して、サイバー防御者が先行者利益において優位に立つことの重要性を呼び掛けているもの

です。そのためには、まず正確かつ熟練した脆弱性管理を基礎として、最終的にはサイバー・エクスポージャーの基盤を整えることが重要です。」

Tenable Research は、組織のサイバーリスク管理者をサポートするために、60 カ国以上の組織から 3 ヶ月以上の遠隔測定データを分析して、組織によるサイバーリスクの管理、測定、および究極的な軽減に役立つ明確なセキュリティ熟練度のスタイルと戦略的洞察を特定しました。

■主な調査結果

情報資産管理の熟練度において、組織は次の 4 つのカテゴリに分類されます。

◇Minimalist（ミニマリスト）

コンプライアンス規制に従って、最低限の脆弱性評価を実行します。このカテゴリに分類される組織は 33%であり、一部の資産についてのみ限定的な評価を行います。これは、全体の 3 割の企業がリスクにさらされていて、KPI を達成するなどの事項よりも優先して、さらなる脆弱性対策が必要であることを表します。

◇Surveyor（サーヴェイヤー）

広範囲の脆弱性評価を頻繁に実施しますが、スキャンテンプレートの柔軟性と信頼度が低いのが特徴です。このカテゴリに分類される組織は 19%であり、情報資産管理において低~中程度の熟練度です。

◇Investigator（インベスティゲイター）

脆弱性評価を高い質で実行しますが、評価するのは一部の資産のみであることが特徴です。このカテゴリに分類される組織は 43%であり、適切なスキャン数、豊富なスキャンテンプレート、幅広い資産の認証と優先順位付けに基づく戦略的脆弱性評価を実施しています。これは、脆弱性の管理、支出の管理、IT 運用、スタッフとスキルの維持等の多様な事業部門との連携、規模の複雑さといった課題を考慮すると、優秀な成績であり、将来的な情報資産管理において堅固な基盤を築けているといえます。

◇Diligent（ディリジェント）

情報資産管理において、最高レベルの熟練度を有し、高い評価頻度で、資産が安全か危険か、またどの程度までサイバーリスクを把握できるかをほぼ連続的に可視化させることに成功しています。このカテゴリに該当する組織はわずか 5 %で、ケースに応じてカスタマイズされた包括的な資産管理を実行できているといえます。

全熟練度の組織に共通することは、脆弱性評価への分散アプローチを回避するのはもちろんですが、脆弱性評価を専門とする人材の確保、また戦略的決定を下すよりも、信頼度と評価頻度の高いスキャナを導入することが組織の情報資産管理において最も効率的だということが判明しました。

調査の詳細については、テナブル・リサーチのブログ記事をご参照ください。

https://www.tenable.com/blog/how-mature-are-your-cyber-defender-strategies

【米国テナブル社プロフィール】

Tenable Network Security は、世界中の 24,000 社を超える組織に対し、総合的なセキュリティソリューションにより、将来のビジネスニーズに合わせてそのテクノロジーを変革し、企業組織の情報保護に向けた有効的な対策を提供しています。Nessus®を開発した Tenable は、脆弱性対策の技術をさらに発展させることで、あらゆる情報資産やデバイスの脆弱性を管理、保護できる世界初のセキュリティプラットフォーム「Tenable.io®」を展開。Tenable のセキュリティプラットフォームは、米国ビジネス誌 Fortune が選定する『Fortune 500』（総収入に基づいた全米上位 500 社）に選ばれている企業の 53%、世界の有力企業 2000 社の 29%に導入されています。詳細は tenable.com へ

【米国テナブル社企業概要】

商号： Tenable Network Security
代表： Amit Yoran アミット・ヨーラン
住所： 7021 Columbia、
Gateway Drive Suite 500 Columbia,
MD 21046

【テナブル社企業概要】

商号：Tenable Network Security Japan K.K.
住所：東京都千代田区丸の内 2-3-2
郵船ビルディング 1 階