PRESS RELEASE

2019 年 4 月 10 日

Tenable Network Security Japan K.K

テナブル、ポネモン・インスティテュートとの独自調査

過去 24 ヵ月間にサイバー被害による業務混乱を 2 度以上きたした組織が 60%にのぼることが判明

～サイバーリスクの業務コストを定量化できず、取締役会がサイバー攻撃の詳細を把握していない状態～

組織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））は、ポネモン研究所（Ponemon Institute）と実施した独自調査、「業務遂行上のサイバーリスク計測と管理に関する報告書」を発表しました。この調査から、過去 24 カ月間において、世界中の組織の 60%がサイバー被害による業務混乱を 2 回以上経験していることが判明しました（サイバー被害は情報流出、または深刻な業務、工場、機器稼働の混乱や中断と定義）。さらに、組織の 91%が同時期に少なくとも 1 回以上のサイバー被害にあっていることも判明しました。

このような攻撃被害の記録が確認されているにもかかわらず、過半数（54%）の組織はサイバーリスクの業務コストを計測しておらず、把握できていないことが判明しました。報告書では、組織が正確かつ定量化された判断基準に裏付けられたリスクに基づく業務決定ができておらず、結果として、経営陣や取締役会が確実な判断を下すための見識が不足していると結論付けています。

デジタルトランスフォーメーションにより、クラウド、DevOps、モビリティ、IoT などの複雑なコンピューティング環境が構築されました。新たに生まれた現代のアタックサーフェスの一部として全てが繋がっていると言っても過言ではありません。これが今、サイバー・エクスポージャーを正しく理解するための組織能力に常に大きなギャップを生んでいます。6 ヵ国 2,410 名の IT および情報セキュリティ事項決定者を対象に調査を実施したところ、エクスポージャーリスクを効率的に軽減するためのアタックサーフェス（従来の IT、クラウド、コンテナ、IoT および OT を含む）に対する可視性を充分に実現している組織は 3 割以下でした（29%）。また、半分以上の組織（58%）は、セキュリティ機能を使用して脆弱性を即座にスキャンするための人員が不足していると回答し、極秘データのリスク評価が必要だと考えられる場合にスキャンを実施している組織はわずか 35%に留まりました。これは、可視性の欠如をさらに悪化させている一つの要因です。

これらの調査データから、組織が現在使用しているツールやアプローチ方法では、デジタル時代におけるサイバーリスクの管理、計測、軽減に欠かすことのできない可視性と視野が得られていないことが判明しました。

また、サイバーリスクの業務コストを計測している組織の 62%が、計測基準の実際の正確性について確信を持っていないことも明らかになりました。これは、組織が IP の盗難によるコスト、収益の損失、生産性の低下といった重要情報なしに資源配分、技術投資、脅威の優先順位を決めていることを意味します。下記のように、多くの組織がサイバーリスクを評価し、理解する上で重要と考える評価指標(KPI)を活用していないことを認めています。

- 64%の組織は、「評価時間」を重要な KPI として設定しているが、実際にこれを計測しているのは 49%のみ。
- 70%の組織は、「修復時間」を重要な KPI として設定しているが、実際にこれを計測しているのは 46%のみ。
- サイバーリスク KPI を運用可能な段階にまで展開できていると確信しているのは 30%のみ。

このように判断基準に秩序がないため、サイバーリスクが組織にもたらすコストに対して、取締役会が詳細を把握できていないという状態に陥っています。最高情報セキュリティ責任者を含めた全てのセキュリティ責任者が計測の正確性に確信を持てずにいるため、サイバーリスクの業務コストに関する重要情報を取締役会と共有することに消極的になっています。

【米国テナブル本社 Bob Huber(最高戦略責任者)のコメント】

「今日のデジタル経済では、サイバーリスクはビジネスリスクと同義です。組織が業務に影響するサイバー被害を受けながら、結果として生じる経済コストの正確な計測に苦心していることが分かったのは驚きです。本報告書は、ほとんどの組織において、サイバー・セキュリティの役割がビジネスの中心機能であることを反映したセキュリティ基準が取り入れられていないことを明らかにしています。最高情報セキュリティ責任者が資産配分、技術投資、および脅威の優先度付けに関して根拠に基づいた意思決定を行うためには、信頼性の高い計測基準が欠かせません。」

詳細情報および本報告書のコピーは、こちらからダウンロードできます:
https://jp.tenable.com/cyber-exposure/ponemon-cyber-risk-report

【米国テナブル社プロフィール】

Tenable Network Security は、世界中の 27,000 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、組織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を展開。Tenable のセキュリティプラットフォームは、大規模行政機関ならびに、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)に選ばれている組織の 50%以上、世界の有力組織 2000 社の 25%以上に導入されています。詳細は tenable.com へ

【米国テナブル社組織概要】

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

【テナブル社組織概要】

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