TANIUM

サイバーセキュリティ:
事後の対応より予防が重要

はじめに

今年はサイバーセキュリティにとって過去最悪の年になるのでしょうか？ITプロフェッショナルの3分の2以上（69%）は確実にそうなると考えています。

憂鬱な数字ではありますが、進化する脅威に対応するための明るい情報もあります。タニウムは、IT部門やセキュリティ部門に業界横断的なデータを提供するために「サイバーセキュリティ:事後の対応より予防が重要」と題した調査プロジェクトを実施しました。その調査結果をご紹介します。

増加の一途をたどる攻撃に対応するために、セキュリティチームは経営幹部から戦略的・財務的なサポートを受けられているでしょうか？今後12ヶ月の間にセキュリティの予算は増加する見込みでしょうか？セキュリティ対策に積極的に対応している業界や消極的な業界は？今後どのようなことが予想されているのか、ぜひ詳細をご覧ください

対応が遅すぎる?

調査対象のセキュリティ担当者の多くは、手遅れの状態になるまで自分たちの仕事は軽視されている、あるいは過小評価されていると感じています。実際に今回の調査では、IT部門とセキュリティ部門は実際に問題が発生しなければ、セキュリティへの投資を増やしてもらえないと考えていることが明らかになりました。回答者のほぼ3分の2(65%)がそれに同意しており、このことから「2022年はサイバーセキュリティにとって最悪の年になるのか」と題したレポートの根本的な疑問が導き出されました。

大企業や成長中の企業は共通してスピード感やアジャイルな対応を重視しています。一方で、レジリエンスはあまり注目されておらず、必要になるまでは日の目を浴びていません。調査対象の10人に8人(79%)はデータ漏洩の発生前ではなく、発生後にセキュリティの予算が増えるだろうと回答しており、これは一部のシニアリーダーがビジネスを守る上でサイバーセキュリティが果たす予防的な役割を十分に理解していないことを示しています。

セキュリティインシデントやデータ漏洩を防ぐうえで、積極的な投資が行われないことが問題の引き金となる場合があります。今回の調査では、3分の2以上(71%)はセキュリティに対して「予防的な対応」を行なっていると回答していますが、4分の3(76%)は「回避可能」だったはずの攻撃に遭ったことがあると回答しています。予防への投資はどのように行われているのでしょうか?

これらの結果から、ITやセキュリティ部門が影響力を持ち、コントロールできる部分にも、改善の余地が十分にあることが浮き彫りになっています。例えば、調査対象の企業のほぼ半数(43%)が「従業員の意識向上のためのトレーニング」にもっと投資するつもりであると回答しています。このような予防重視のアプローチが、人為的なミスやセキュリティ問題に関する教育不足によって引き起こされがちな脆弱性を減らす方法の一つとなります。

業界別の傾向:

- **予防対策が最も進んでいる:民間の医療業界では、88%がサイバーセキュリティに対して主に予防的な対応を行なっていると回答**
- **最も消極的:公立教育機関の50%は、主に“問題が起こった場合に対応する”姿勢をとっていると回答**
- **投資が遅い:製造業では80%が、インシデントが発生してから初めて追加資金が投入されると回答**

「企業は回避可能なサイバー攻撃を防止するための
対応にこそ注力し、リソースを集中させるべきです。
脆弱性は、把握している状況やコンプライアンス対応に
差分があるところで発生します。
予防第一のアプローチを採用しないと、
セキュリティ担当者が増大する脅威を把握する能力が、
大きく制限されてしまいます」

「例えば、エンドポイント（企業ネットワークに接続する
機器）の数について、基本的な情報すら把握できて
いないこともよくあります。
リモートワークやハイブリッドワークが増加する中で、
企業ネットワークの攻撃対象領域は広がり、
問題は悪化する一方です」

オリバー・クロン
タニウム EMEA 地域担当 チーフ IT アーキテクト

既知の問題が原因に

ここまでを振り返ると、脅威の展望は「最悪の年」を懸念すべき事態に近いと考えられます。また、企業はサイバーセキュリティ用に「資金を確保する」ことはできるものの、多くの場合、それは問題が発生した後になることが判明しました。しかし、ファイアウォールが破られた場合、具体的にどんな問題を恐れているのでしょうか。さまざまな懸念材料があるため、決定的な答えはありませんが、データを詳しく見ていきましょう。

回答者の最も多く（56%）は、侵害後に最も大きな影響をもたらすのは「生産性の低下」だと考えており、次いで「顧客の喪失 および/または 収益の損失」（52%）という結果になっています。この2つの回答には、ダウンタイムという共通点があることに注目すべきです。2年以上にわたるパンデミックによる混乱を受けて、企業は当然ながら通常のビジネスを妨げるものに敏感になっています。

他にも「身代金の支払いによる金銭的損害」（49%）、「評判の悪化」（48%）、「インシデントの復旧にかかるスタッフの時間」（47%）、「知的財産/データの損失」（46%）などの懸念事項が挙げられています。「シニアリーダーがどのようなことに懸念を抱いていると思うか」という質問は、さらに興味深い結果となりました。結果は先ほどの質問とほぼ同じでしたが、「知的財産や所有するデータの損失」が役員に大きな警鐘を鳴らすと考える人は、わずか36%でした。

このような潜在的な問題を考えると、セキュリティの担当者が手一杯で資金不足を感じるのは当然のことだと思われます。半数以上（55%）は「サイバーセキュリティの予防に十分に取り組む」ための人員が不足していると考えています。

しかし、事後対応よりも予防が大切という考えが強まっています。81%がサイバー攻撃やデータ漏洩を阻止するための予防対策への支出が増えれば、「回避可能なインシデント」の影響を「最小化」できると考えています。

業界別の傾向：

- **生産性への影響を最も懸念：電気通信業界（100%）、民間医療業界（88%）**
- **知的財産/データ損失の心配が最も少ない：国民保健サービスと教育を除く公共サービス機関のうち、懸念を表明したのはわずか26%**
- **サイバーセキュリティに関する人材が最も不足している：国民保健サービスの回答者の83%が、人的リソースが不足している回答**

「サイバーセキュリティに対する考え方は、社内での立場によって異なるように、業界によっても差があります。当社のデータによると、銀行や大学は侵害がもたらす経済的な影響を懸念しているのに対し、民間の医療機関、IT、電気通信会社では、ダウンタイム中の生産性の低下をより懸念していることが明らかになりました。しかし、このことは IT やセキュリティチームが“心配事から逃れることはできない”というビジネスレベルの懸念を理解していることを示唆しています」

「つまり、IT やセキュリティチームは予防を重視する戦略のメリットを経営幹部に説得する努力を重ね、適切な投資を促す必要があります。そのためには、ビジネスリーダーが決断力を持って行動できるように、わかりやすい情報を使って脅威の展望を状況に沿って報告することが最も効果的です」

オリバー・クロン

タニウム EMEA 地域担当 チーフ IT アーキテクト

監視が弱まると犯罪が増える

今年はサイバーセキュリティにとって史上最悪の年になるかもしれないというトピックに戻り、前後関係を少し整理してみましょう。2021年だけでも、DDoS攻撃（11%増）やフィッシング（36%増）など、サイバー攻撃は31%増加しました*。今後、この悪化の傾向が緩和される見込みはあるのでしょうか？

調査に参加した企業の42%は来年度以降、新しいデバイスへの支出を増やす、つまりエンドポイントの数を増やすと回答しています。企業ネットワークに接続するデバイス（モバイル端末、パソコン、プリンタ）の台数がそれほど増えないと見込んでいるのは、わずか18%でした。実際、テクノロジーを進んで導入する電気通信業界は、デバイスが確実に増加することを見込んでおり、75%がエンドポイントは減少するどころか増加すると予測しています。

エンドポイントが増えれば、その保護が必要になります。リモートワークの急増に伴って、ネットワークに接続する会社所有のデバイスに限らず、個人所有のデバイスも保護が必要になっています。厳密には、これらのデバイスもセキュリティ上のIT資産の一部となります。

その結果、調査対象の担当者の4分の3（75%）が新型コロナウイルスの流行前と比較して、サイバー攻撃やデータ漏洩に対して「より高いレベルの説明責任を負っている」と回答しています。また、ほぼ3分の2 (64%) が、セキュリティチームはサイバー攻撃の量と種類についていくのに苦労していると回答しています。サイバーセキュリティ業界全体が一丸となって、企業が脅威を乗り越えるためのサポートを行う必要があります。

そのためには、セキュリティ部門が使用するツールやテクニックを検証する必要があります。サイバー脅威と犯罪者に効果的に対処するための適切なツールがそろっているのでしょうか？

業界別の傾向：

- **生産性への影響を最も懸念：電気通信（100%）、民間医療（88%）**
- **エンドポイント保護を重視：大学や製造業の60%がエンドポイントセキュリティへの投資を増やすと回答**
- **サイバーセキュリティへの責任が増大：製造業（83%）、医療（83%）、銀行・金融（74%）で働くIT・セキュリティ担当者は、新型コロナウイルスの登場以降、より大きな責任を負うように**

「セキュリティチームが自社のネットワークや分散した
エンドポイントに潜む脅威を把握できてなければ、
それを排除することはできません。予防のための
セキュリティ戦略を進めているという担当者の言葉を
信用しがちですが、実際には、新たに確保した資金は
侵害が発生した後の修復に費やされているのが現状です。
この点は皆、否定せずに認めています」

「サイバー攻撃の規模や性質を考えると、企業や行政には
より積極的な取組みが求められています。そのためには
IT 資産を侵害を受けるエンドポイントが 1 つもない、
健全な状態を維持することから始める必要があります。
IT 資産の検知とインベントリ管理をすばやく強力に行える
ツールを使用することで、IT やセキュリティ部門は
残すべきものと削除すべきものをより簡単に特定することが
できます。まずは IT 資産を可視化し、クリーンな状態を
維持するために制御する機能が必要です」

出典 : TechTarget (2022 年 3 月 15 日)

最終的な見解

業界調査は、トレンドの素となるトレンドを検証することで、より有益なものとなります。サイバーセキュリティは最悪の状況にあると言われており、業界のデータによると、より巧妙な手法と継続的な悪意ある活動により、脅威は拡大しています。そして攻撃を開始する前に、検出されないままネットワーク内に長く滞在する傾向にあります**。データの損失やダウンタイムが発生することでセキュリティチームだけでなく、あらゆる部門に影響を与えてしまいます。

一方、IT資産となるデバイスの数は、管理・非管理を問わず指数関数的に増加しており、必然的に新たな脆弱性が発生しています。このような状況下で、特にデータへのゲートウェイアクセスが増加し、ネットワークの監視が弱まればサイバー攻撃者は増え続けることになります。

実際、大半の企業はビジネスを継続し、パンデミックの影響を最小限に抑えるために、この数年またはそれ以上の間、バックエンドインフラへのパッチ適用に対応してきました。その過程で、連携しない各種ツールを使用したことで、エンドポイントを可視化して精度の高いデータを維持することが難しくなっています。これにより生産性の低下を招き、最悪の場合、財務面の負債や評判の低下を招いてしまいます。

このような状況を考えると、企業が今年をサイバーセキュリティにとって「最悪の年」になると感じるのも当然です。ですが、それは単純で悲観的な見解でもあります。先進的な企業は、すでに古いシステムの技術的な問題を解決するために行動を起こしています。調査に参加したセキュリティ担当者の85%は「セキュリティインシデントに対応し回復するには、インシデントの防止よりも多くの費用がかかる」と認めています。これだけは確かなのです。

しかし、セキュリティを最新化するために、必ずしも多くのテクノロジーや費用が必要なわけではありません。それどころか、IT資産を合理化することで、全体的なリスクを低減することができます。これは、IT、セキュリティ、ビジネス部門の各リーダーが「予防」という共通の目標に向かって団結できる、魅力的な取組みなのです。

出典: “Ransomware attacks are on the rise and the criminals are winning”
New Scientist

調査の概要

銀行、金融、教育、医療、製造、小売、電気通信業界で、英国に拠点を置き、従業員250人以上の企業に所属する300人を対象に調査を実施。23%がCレベルや役員レベル、77%がITやセキュリティを専門とする人です。

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。