VISION by protiviti

In Focus

7 月 23 日

2024

CrowdStrike に関する障害は テクノロジー・レジリエンスの再起動につながるか？

キム・ボッツェッラ 記

プロティビティ、マネージング・ディレクター兼テクノロジーコンサルティング部門

グローバルリーダー

サイバーセキュリティベンダーの CrowdStrike によるソフトウェア・アップデートが原因で、Windows コンピュータの大規模な世界的な停止が発生しました。その後、世界の IT システムはいまだ再起動と復旧の途上にあります。航空会社、銀行、通信、医療を含む多くの業界の、世界中の企業、政府、および組織が影響を受けました。世界的なシステム障害の具体的な原因や背景についての詳細が明らかになる中で、確かなことの一つは、CrowdStrike のアップデートに含まれる誤ったコードが、私たちのテクノロジーの脆弱性についての大きな警鐘を鳴らしたということです。

なぜそれが重要なのか

Microsoft のブログ投稿によると、全 Windows マシンのうち 1%未満、つまり 850 万台以上が影響を受けました。しかし、CrowdStrike の欠陥パッチの影響は重大でした。専門家は、この史上最も重要な IT 障害がもたらす経済的影響は数十億ドルに達する可能性があると見積もっています。

CrowdStrike の CEO、ジョージ・カーツ氏は、影響を受けた 850 万台以上の Windows デバイスを完全に回復するには、数週間かかる可能性があると述べました。テクノロジーの専門家は、さまざまな業界の重要なサービスを支える基盤システムが相互に接続されているため、さらなる世界的な障害が発生する可能性があると長らく警告してきました。

このような事態を受けて、ビジネスリーダーは直ちに以下の対策を取るべきです。

- **「通常業務」の再開に注力する。**ほとんどの組織がまだこのインシデントに対する正式な対応プロセスにあるため、既知の問題に対処し、必要に応じて回避策を展開しながら通常のビジネスサービスの再開に注力すべきです。
- **既知の問題についての透明性を高める、全社的なコミュニケーションを図る。**即席のテクノロジー修正が利用可能になると、エンドユーザーが企業の慣行と一致しない手順で問題を修正し、それが意図しない問題を引き起こす可能性があります。
- **重要な支援ベンダーへの影響を理解する。**重要なサードパーティと直接連絡を取り、彼らが提供するサービスや取り組みが組織にどのような影響が及ぶ可能性があるかを理解する。ベンダーによる潜在的な影響に対処するための修復戦略を実施します。
- **顧客とコミュニケーションを取る。**影響の範囲と回復の状況について顧客に明確かつ簡潔なコミュニケーションを提供し、問題が適切に管理されていることを伝えて顧客の信頼を得ます。
- **フィッシングメールに注意する。**この問題を解決する際には、コミュニケーションとサポートのプロトコルを遵守し、この問題の解決策を装ったフィッシングメールに警戒する重要性を企業全体に伝えます。

関係者のコメント

トーマス・ヴァルタニアン、
金融技術・サイバーセキュリティセンター　　エグゼクティブディレクター

「自分のお金を見つけたり、アクセスしたりできないことを想像してみてください。その日は私たちが思っているよりも早く来るかもしれません。行動するのは私たちの責任です。企業は先頭に立ち、政府と協力して、私たちの仮想世界を完全に保護するべきです。過去25年間で、もし民主主義国家がアナログ世界で使用されている認証、ガバナンス、執行基準および責任を取り入れた常識的なルールに従ってサイバースペースを再構築していたならば、仮想の脆弱性や世界的な停止の可能性は大幅に減少していたでしょう。」

プロティビティのコメント

残念ながら、これが新しい常態になる可能性があります。さらに相互接続が進むITの未来に向けて、ビジネスリーダーは、CrowdStrikeと同様の特徴を持ち今後同様の脅威をもたらす可能性のある他のサードパーティのエージェント、ツール、製品を評価すべきです。これらの脅威を軽減するための行動計画を策定する必要があります。ビジネスリーダーは既存のリスクシナリオ一覧に「CrowdStrikeタイプのインシデント」を組み込むべきです。その間、サードパーティのリスク管理実践を見直し、CrowdStrikeと同様の特徴を持つものをよりよく識別し、監視するための対策を講じる必要があります。

戦略的には、組織は慎重に検討され、テストされたフレームワークに引き続き投資し、逆境時にも情報に基づいたビジネス判断を下せるようにするべきです。確実なのは、次の障害は前回とは異なるということです。迅速かつ責任ある対応と回復に備えた組織は、将来的により適応力をもつこととなるでしょう。

結論

今回のCrowdStrikeのような事象は、ほぼ確実に再び発生するでしょう。ビジネスリーダーはこのインシデントを機に、テクノロジー・レジリエンス（回復力）を再構築することを検討すべきです。警戒を怠らず、適切なプロトコルと計画を整備している企業は、広範な被害を最小限に抑える準備が最も整っているでしょう。組織は、影響が数日または数週間後に現れる可能性のある二次的影響の可能性も念頭に置いておく必要があります。これらの影響には、コンプライアンス関連の問題、データの整合性、エンドユーザーデバイスからのシャドーITの状況、またはサイクルを完了していない定期的な活動の中断が含まれます。

ビジネスリーダーは、次の大規模な技術障害に備えるために、ソフトウェアのサプライチェーンが可能な限り自動化など、組織が実施できる実践的な変更に引き続き注力するべきです。

この報告書には、プロティビティのサミール・アンサリ、サミール・ダット、アンドリュー・レトラムが寄稿しました。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、85を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、デジタル、オペレーション、人材・組織、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、米国フォーチュン誌の2023年働きがいのある会社ベスト100に選出され、Fortune 100の80%以上、Fortune 500の約80%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half（RHI）の100%子会社です。

プロティビティのVISIONについて

VISION by Protivitiは、今後10年以上にわたってビジネスを変革する大きなトピックを探求するグローバルコンテンツリソースです。*VISION* by Protivitiは、世界中のC-suiteおよび役員室幹部向けに執筆されており、現在および将来の世界を形成する破壊的な力の影響について考察しています。プロティビティの*VISION*は、多様な声と多様な思想を通して、10年後、そしてその先のビジネスがどのようになるかを展望しています。