2024 年にスモール ビジネスが警戒すべき 4 つの主なサイバー セキュリティ関連トレンドとリスク

近年、テクノロジーはさまざまな分野で急速な進歩を遂げています。中でも自動化と人工知能*(AI)*の発達はビジネスに多大なメリットをもたらしており、時間の節約やマーケティングをはじめとする業務の効率化に貢献しています。

しかし、テクノロジーの進歩に伴い、従来よりも高度なサイバー脅威が新たに出現しています。強固なサイバー セキュリティ システムは、ウイルスやマルウェアなどの一般的なリスクからビジネスを保護するために役立ちますが、サイバー脅威もますます巧妙化しているため、経営者が被害を受けるリスクは依然としてあります。

2024 年に警戒すべき主なサイバー セキュリティ関連トレンドとリスクをご紹介します。

生成人工知能

生成人工知能（生成 AI）は、まったく新しいコンテンツや音声、コード、画像、動画などを生成する際に利用できるテクノロジーです。ChatGPT は生成 AI の一種です。GPT は「Generative Pre-trained Transformer」の略称です。

ChatGPT は、時間とリソースの節約に役立つことから、経営者の間で特に高い支持を得ています。すでに多くのスモール ビジネスの経営者が、ChatGPT を活用して、マーケティング資料の作成やデータの整理、Web サイトのコーディングを行っていますが、その機能は急速に進歩を遂げています。

ChatGPT の最新版では、ほんの数秒のサンプル発話データから、人間の声と区別できないほどリアルな合成音声を生成できます。音楽配信サービスの Spotify はすでにこのテクノロジーを使って、ポッドキャストを同じポッドキャスターの声で各国語に翻訳する、音声翻訳機能を試験的に導入しています。

ChatGPT の開発元である OpenAI 自体が「このような機能には、悪意のある人物が著名人を装ったり詐欺を働いたりするなどの新たなリスクもある」と認めています。

2024 年、スモール ビジネスの経営者はこの問題に注意する必要があります。生成 AI はまだ登場したばかりのテクノロジーであり、今後、より巧妙でターゲットに合わせてパーソナライズされたフィッシング詐欺に悪用さ

れるかもしれません。最終的に E メールやテキスト メッセージ、通話で他人の声を模倣できるようになる可能性があるため、何か不審な点がないか警戒するようにしてください。

サイバー レジリエンス

最近、あるスモール ビジネスの経営者に話を聞いたところ、目まぐるしく変化するサイバーセキュリティ リスクに対応し続けることがいかに大変であるかを語っていました。そこで重要になるのが、次の主なトレンドであるサイバー レジリエンスです。

サイバー セキュリティとサイバー レジリエンスは同じような意味で使われることがよくありますが、この 2 つの概念は若干異なります。サイバー セキュリティはビジネスを攻撃から保護するのに役立ちますが、サイバー レジリエンスは攻撃を受けた場合でもビジネスを継続できるようにします。

ほとんどの企業は、どれほど優れたサイバー セキュリティでも絶対確実な保護を保証できないことを認識しています。サイバー レジリエンス戦略を策定しておけば、サイバー攻撃やデータ侵害を受けても速やかに対応できます。

サイバー レジリエンス計画には以下の内容が含まれます。

- ミッションクリティカルなプロセス、システム、テクノロジーを特定し、そのセキュリティを強化する
- ビジネスで特に重要な部分をバック アップするために、クラウド テクノロジーを導入する
- サイバー インシデント対応計画を策定し、サイバー攻撃を受けた場合の対処方法と復旧方法を明確に決めておく

ゼロ トラスト

ゼロ トラストとはサイバー レジリエンスの実現に向けた動きの 1 つであり、100%安全なシステムは存在しないという考えに基づいています。

ゼロ トラストというセキュリティ戦略では、ユーザーに職務上必要最小限のアクセス権のみを付与し、それ以上の権限は与えません。ユーザーを確認し、継続的にアクセス権を再承認する必要があります。

ゼロ トラストでは以下の点を考慮に入れます。

- 誰がいつ何にアクセスできるようにするのか
- ツールや資産へのアクセスに必要な認証手段は何か

- どの情報にネットワークへのアクセス権を付与または制限するか

Google ドライブなどのクラウド ストレージやファイル共有プラットフォームを利用していて、ゼロ トラスト戦略の適用を始めようとしている場合、最も簡単なのは、利用可能な権限をチェックし、必要に応じてアクセス権を制限することです。権限は定期的に見直し、アクセス権が不要になった場合（フリーランスとの契約期間が終了した場合など）は、そのアクセス権を直ちに無効にする必要があります。

ベスト プラクティスの標準化

サイバー セキュリティにおいて大きな課題の 1 つは常に、サイバー セキュリティの強度は、最も脆弱な部分である従業員によって決まるということです。ご存じのように、2017 年に起きた英国の国民保健サービスに対する WannaCry サイバー攻撃があれほど大きな被害につながったのは、地方のトラスト（国立病院が移管した公営企業体）が古いコンピューター システムのアップグレードを怠っていたことが原因でした。

直近の 6 年間で、サイバー セキュリティという問題の認知度は大きく向上しました。デジタル システムを扱う人の多くはその重要性を認識しています。また、多要素認証やパスワード マネージャーをはじめとするサイバー セキュリティ ツールもかつてないほど普及し、利用しやすくなっています。

その結果、ビジネスの世界でサイバー セキュリティの実践は当たり前になりつつあります。この傾向は 2024 年も続くだろうと私たちは予測しています。組織のセキュリティを確保する責任は、特定の個人が抱えるべきではなく、一人ひとりが自分自身の行動目標として担うべき課題なのです。

サイバー セキュリティに関するチームのスキルを高めるコスト パフォーマンスに優れた方法をご紹介します。