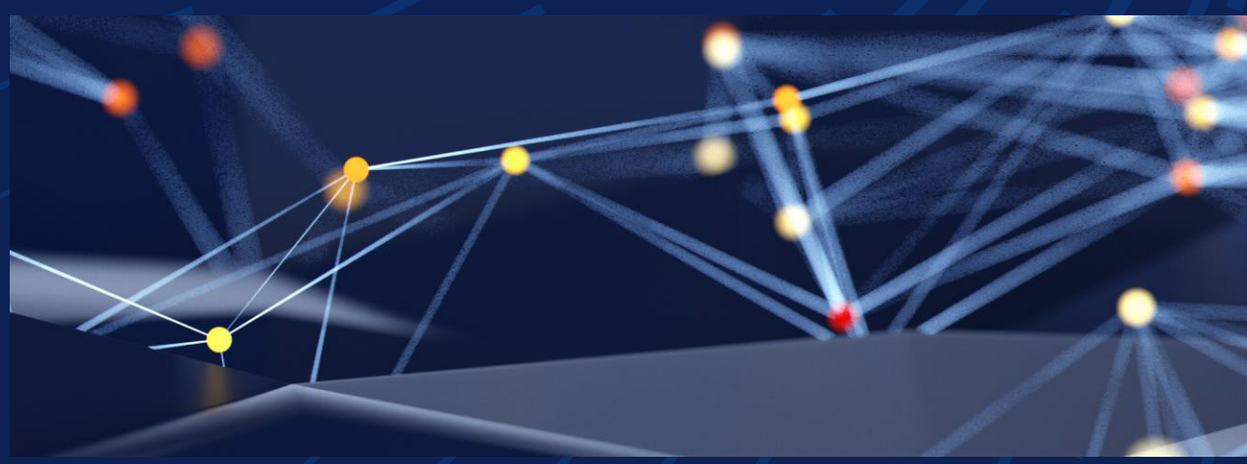
DELL Technologies

サイバーセキュリティの未来：

新しいデジタル時代への適応



サイバーセキュリティの専門家は、攻撃の防止とリカバリー計画の策定に集中することがよくありますが、全体的なセキュリティ環境は絶えず進化しています。そのため、将来に備えた計画を立てることが重要です。

将来に目を向けると、ポスト量子暗号、変化する規制環境、新たな脅威の3つの分野が際立っています。組織は今すぐ行動し、計画を立てて、ソリューションが利用可能になり次第、それを実装するべきです。

ポスト量子暗号の夜明け

量子コンピューティングには、産業の変革への期待があり、古典的なコンピューターの範囲をはるかに超えた問題を解決できる驚異的な計算能力を提供します。ただし、この同じパワーにより、現在の暗号形式手法が時代遅れになる可能性があります。今日の安全な通信の多くを支えるRSAやECCのようなアルゴリズムは、十分に高度な量子コンピューターによって数秒で破られる可能性があります。この脅威が差し迫っており、ポスト量子暗号の緊急性が高まっています。

ポスト量子暗号(PQC)は、量子コンピューティング時代において安全性を維持している暗号アルゴリズムの開発を中心に展開されています。米国国立標準技術研究所(NIST)は、この差し迫ったリスクを認識しており、量子耐性アルゴリズムの標準化を主導しています。

企業にとって、この移行への準備は絶対不可欠です。PQCソリューションを早期に導入すると、攻撃者が量子コンピューティング機能にアクセスできるようになってもデータの安全性を確保できます。

Dellのサイバーセキュリティ担当副社長兼ビジネス ユニット セキュリティ責任者であるBobbie Stempfleyが指摘するように、組織は次の2つの主要分野に焦点を当ててこのプロセスを開始する必要があります。

現在使用しているすべての暗号化モデルを特定してインベントリーを作成する。

静止データだけでなく、実行データも考慮する必要があります。キー管理、コード署名、デバイスID、安全なアクセス、テレメトリーについて考えてください。包括的なインベントリーを作成してから、ロードマップを作成します。

サプライヤーのステータスを理解する。

現代の企業では数千のサプライヤーを抱える可能性があることを考えると、サプライヤーから生じる可能性のあるリスクを認識しておく必要があります。サプライヤーも変革を計画していることを確認します。

こうした出発点に加えて、リスク アセスメントを実施して脆弱なシステムを特定し、移行中の運用を維持するためにハイブリッド暗号化モデルの実装を検討し、量子安全ソリューションをすでに追及しているベンダーと連携しましょう。ただし、ターンキー ソリューションを1社のベンダーや1つのテクノロジーが提供できるわけではないことに注意してください。

グローバル化した世界における規制の変化

サイバーセキュリティの未来を形作るもう1つの重要な要因は、変化する規制環境です。規制は今や、コンプライアンスをはるかに超えています。規制は、相互に接続されたデータ主導型の世界において、説明責任を浸透させ、技術的なアップグレードを推進し、市民を保護するための重要なフレームワークとなりつつあります。しかし、こうしたものは急速に進化し、地域によって大きく異なるため、コンプライアンスがますます複雑になっています。

とはいえ、こうした規制はコンプライアンス違反に対する罰則というだけではなく、サイバーセキュリティ慣行を改善するための触媒として機能します。規制要件に合わせてポリシーを積極的に調整する企業は、新たなレベルの信頼と運用効率を引き出すことができます。そのために、組織はガバナンス フレームワークを確立して、法の変化に適応するための柔軟性を維持し、定期的なコンプライアンス監査を実施する必要があります。またトレーニングに投資して、従業員が最新の基準に従って機密情報を処理できるようにする必要があります。

セキュリティ エグゼクティブがコンプライアンスに備える際には、理解しやすいことと、理解されていることを確認することが重要です。セキュリティの専門家は、セキュリティの専門用語で話すことがあまりに多いため、お客様や規制当局などのステークホルダーの共感を得られない可能性があります。理解してもらう責任はセキュリティの専門家にあり、聞き手側が解釈する責任はありません。

DELL Technologies

> ポスト量子暗号への移行について考えてみてください。それは、家具がすべて揃った家を持ち上げて動かすようなものです。非常に複雑なものになり、課題となるのは、その過程で何も壊さないことです。
>
> ***Bobbie Stempfley***
> デル・テクノロジーズ、サイバーセキュリティおよびビジネス ユニット セキュリティ担当*VP*

脅威（および防衛）の環境の進化

AIは、ビジネスに革命をもたらし、生産性を向上させ、人間の可能性を引き出す新たな機会を生み出しています。サイバーセキュリティについては、AIは悪意のある攻撃者と防御者の両方にメリットをもたらしています。

攻撃的な利用：AIにより、説得力の高いスピア フィッシングやディープフェイクなど、より高度な攻撃が可能になっています。

防御的な利用：AIは次のような方法で防御者を支援します。

- 膨大なセキュリティ データの迅速な処理。
- 脅威へのより効果的な優先順位付け。
- 検出および対応機能の向上。

セキュリティ ツールは今後も進化し続けます。自然言語処理の進歩により、セキュリティの専門家はさらに直接的にシステムと連携できるようになり、システムはサイバーセキュリティ対策をプロアクティブに実行できるようになります。

組織は、トレーニングやその他の防御メカニズムを確実に最新の状態に保ちながら、同時にそれらの機能を活用するよう取り組む必要があります。トレーニングは、従業員がさらに高度な攻撃の被害に遭わないようにするための最善の方法です。

パスワード不要への移行

パスワードは、IDとアクセスの管理にとって最も安全な方法ではなくなりました。従来のパスワードベースのシステムには重大な脆弱性が存在し、最新のサイバーセキュリティのニーズに対応するソリューションとしては十分ではなくなってきています。パスワードは、認証情報のスタッフィング、フィッシング、ブルートフォース攻撃などの攻撃を受けやすく、多くの場合、組織は不要なリスクにさらされます。さらに、パスワードの再利用や脆弱なパスワードの作成など、ユーザーの不適切な行動により、こうした脆弱性が悪化します。

生体認証、証明書、ハードウェア トークンなどのパスワード不要の認証方法は、パスワード関連の脅威クラス全体を排除することで、より強力で安全な代替手段となります。パスワード不要のシステムへの移行は、IDとアクセスの管理における重要な進化を表しており、サイバー脅威の高度化に合わせたセキュリティ対策です。

パスワード不要の技術の採用には、攻撃対象領域の縮小、迅速でシームレスなログインによるユーザー エクスペリエンスの向上、パスワード関連のインシデントの減少によるITコストの削減など、多くのメリットもあります。高度な方法を使用することで、セキュリティ体制が確実に強化され、組織が規制基準を遵守する上で役立ちます。パスワード不要システムへの移行は、単なるトレンドではありません。個人と組織の両方にとって、より安全で効率的なデジタル エコシステムの構築に向けて必要なステップです。

まとめ

サイバーセキュリティは、量子コンピューティング、規制の変化、さらに高度化する脅威によって形成される変革の時代に入りつつあります。一歩先を行くには、ポスト量子暗号、AI主導の防御、パスワード不要認証などのイノベーションを採用する必要があります。準備、コラボレーション、戦略的投資を優先することで、企業はより安全でレジリエントなデジタル環境を構築できます。今こそ、行動を起こす時です。

お役に立つDellの製品とソリューションは、次のとおりです。

注目の**Dell**ソリューション	説明
サイバーセキュリティ アドバイザリー サービス	現在および新たな脅威を含む、進化する脅威環境に対する計画に役立つエキスパート ガイダンス。
vCISO	リスクの特定と管理を支援し、戦略的な意思決定に導く、仮想最高情報セキュリティ責任者およびサイバーセキュリティ エキスパート。

dell.com/cybersecuritymonthで今日のサイバーセキュリティの重要な課題に対処する方法をご紹介しています