サイバー脅威からの保護

進化するリスク環境に対処する

ランサムウェア：絶え間ない脅威

ランサムウェア攻撃（被害者のコンピュータファイルを暗号化し、身代金を払うまで解除しない）の件数と影響が増加しており、すべての主要なセクターで事件が発生しているため、組織にとって重大な脅威となっています。ランサムウェア攻撃による平均的な被害額が440万米ドルにのぼり[1]、過去最大の支払額が4千万米ドル[2]であることを踏まえると、標的にされれば金銭、運用、評判に重大な影響が及ぶ可能性があることは明らかです。

カーク・ヘイズ
マネージングプリンシパルセキュリティ
コンサルタント | Nettitude

道徳的・法的な理由から身代金を支払うべきではないと言うのは容易ですが、支払いに応じないことによる業務上の影響は、時間とデータの損失という点でさらに大きくなる可能性があります。データが危険にさらされた場合にも、コンプライアンス違反や評判の問題が発生し、ブランドにさらに長期的な影響が及ぶ可能性があります。

最近のランサムウェア

ランサムウェアの影響は、暗号通貨の出現によって大きく変わりました。暗号通貨の普及と匿名性が相まって、ファイルの返却と引き換えに多額の身代金を支払わせる手段を備えた、より大きな標的を狙った高度な攻撃の新たな波が押し寄せています。

もちろん、常に解決するとは限らず、残された損害にかかる費用が、支払った身代金をはるかに上回る可能性があります。2019年、「WannaCry」と呼ばれる兵器化されたマルウェアがWindowsの脆弱性を悪用し、世界中のコンピュータを停止させました。これにより、40億米ドルという驚くべき損害が発生したと推定されています。

組織にとって厄介なのは、ランサムウェアがすぐにはなくならないということです。その理由は単純です。被害を受けた企業は組織への被害を抑えるため身代金を払い続けねばならず、攻撃者にとって容易な収入源になるからです。だからといって、数百万ドルの身代金をたびたび要求するランサムウェア攻撃に対して、組織が身を守る手段がないということではありません。

ランサムウェアからの保護

組織がランサムウェアから自身を保護する最善の方法は、基本を忠実に守ることです。ランサムウェアは一見したところ、比較的単純な攻撃方法です。攻撃者は、セキュリティが緩い組織を標的にしてつけ込み、その緩さが他の領域（重要ファイルの定期的なバックアップなど）の弱点につながることを正確に推測します。

対照的に、セキュリティの層が多ければ多いほど、攻撃者の標的になることは少なくなります。

[1] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
[2] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

ランサムウェア攻撃の平均被害額は

4.4百万米ドル[1]

に上昇

> “組織は世界中であらゆる保護対策を実施できますが、徹底的なテストと保証がなければ、ほとんど意味がありません。”

カーク・ヘイズ
マネージングプリンシパルセキュリティコンサルタント | Nettitude

覚えておいてほしい重要な事実は、ランサムウェアの攻撃者は容易な支払元を求めているため、ファイルやその他の重要データとの間にできる限り多くの障壁を設置することが最善の策になるということです。

多くの場合、最先端のセキュリティソリューションを導入する必要はありません。ランサムウェアからの保護は、基本的なベストプラクティスを導入するというシンプルなものでよいのです。ネットワーク強化の実装、堅牢なデータセキュリティポリシーの導入、全般的なサイバー衛生管理の促進はすべて、このタイプの攻撃の防止・検出に大いに寄与します。サイバーセキュリティに関して言えば、予防が常に治療よりも優れた措置となります。

同時に、サイバー攻撃はますます巧妙になっており、あらゆる不測の事態を常に防げるとは限らないと覚えておくことが重要です。ファイルやその他の重要データの定期的なバックアップを計画しておくことが不可欠なのはそのためです。結局のところ、数時間前のバックアップが取ってあれば、身代金目当てでファイルを保有しても攻撃者にとってほとんど役に立たないでしょう。

保証の役割

組織は世界中であらゆる保護対策を実施できますが、徹底的なテストと保証がなければ、ほとんど意味がありません。システムに厳密な評価やテストが行われていない場合、意図したとおりに機能していることを確認できるでしょうか。

レッドチーム（高度な攻撃に対する組織のレジリエンスを継続的に高めることを使命とするグループ）は、セキュリティのレジリエンスを構築する効果的なソリューションです。これは、倫理的なハッカーのグループが、制御された環境でお客様のシステムを攻撃し、脆弱性を発見し、修正することを任務とするものです。

ISO 27701（情報セキュリティマネジメントシステム（ISMS）の要求事項を定義）のような、国際的に認められた規格もあります。LRQA のような認証機関による ISO 27001 の独立した認証を通じて、ベストプラクティスが行われていることを実証し、効果的なリスクマネジメントプロセスが実施・文書化されていることを確認できます。これにより、ランサムウェアの脅威の増大に対処するための措置が確実に実施され、攻撃が発生した場合に主要担当者が適切な対応を調整できるようになります。

独立して認証された ISO 27001 は、情報セキュリティ活動の支援（特に脅威と脆弱性の特定と報告）における自身の役割をスタッフが理解するのにも役立ちます。これにより ISO 27001 は、多くの点で、より広範なサイバーセキュリティ戦略・保証プログラムの重要な基盤となっています。プログラムでは、組織のすべてのレベルにおいて問題特定のスキルを高め、全社レベルの保護を推進します。

無くならないランサムウェア攻撃

攻撃は高度化が進む一方であり、ランサムウェア攻撃の被害額が増加し続ける中、発生の規模も拡大しています。

基本的なセキュリティ対策と強固な情報セキュリティ管理の文化を導入することで、組織はランサムウェア攻撃の犠牲者となるリスクの大半を排除できます。

サイバーセキュリティのあらゆる側面をターゲットに、お客様と一緒に取り組む

LRQAの保証分野での深い経験と、受賞歴のあるサイバーセキュリティサービス、脅威主導のインテリジェンスを組み合わせることで、お客様のビジネスが直面する独自の脅威に対する洞察と防御を提供することができ、今日、明日、また将来のサイバーリスクに先手を打つことが可能になります。

LRQAは世界の主要な国際規格・スキームに準拠した審査、教育研修、認証サービスを展開するとともに、世界の市場から高い評価を得たスペシャリストであるNettitudeを通じて、幅広い高度なサイバーセキュリティサービスを提供しています。

お客様のビジネスと協力して、直面している具体的な脅威を特定し、それらを軽減する戦略を構築する支援をします。LRQAがお客様と協力して認証、脆弱性の特定、ブランドの整合性、財務、業務に影響を与えうる攻撃やインシデントの防止を支援します。

情報セキュリティ

LRQA のコンプライアンス・認証サービスが、ビジネスに不可欠な情報の保護と、国際的に認められたベストプラクティスの実証を支援します。

詳細情報 >

オペレーショナル・レジリエンス

認証、教育研修、ガバナンス、リスクとコンプライアンスサービスを提供し、混乱を防止、対応、復旧できるよう準備します。

詳細情報 >

サイバー脅威からの保護

あらゆる種類のサイバー攻撃に対して、第一線の防御と対応を提供するカスタマイズされたソリューションで、サイバー脅威の一歩先を行くことができます。

詳細情報 >

YOUR FUTURE. OUR FOCUS.

LRQA について

認証・サイバーセキュリティ・検査・教育研修分野の比類なき専門知識を結集することにより、当社は世界的な認証のリーディングプロバイダーの地位を確保しています。

その伝統は誇るべきものですが、顧客との今後のパートナー関係を構築する上で、本当に重要なのは現在の当社の姿です。揺るぎない価値・リスク管理、軽減における数十年の経験・未来への的確なフォーカスを組み合わせることで、より安心・安全・持続可能なビジネス構築に向けてお客様をいつでも支援します。

独立した審査・認証・教育研修から、リアルタイムの認証技術・データによるサプライチェーン改革まで、当社の革新的なエンドツーエンドのソリューションが、変化の速いリスク環境に積極的に対処できるようお客様をサポートします。つまり、未来の状況を成り行きに任せるのではなく、お客様が自ら構築できるようになるのです。

お問い合わせ

詳細については、
https://www.lrqa.com/ja-jp/
をご覧ください。

LRQAリミテッド
〒220-6010
横浜市西区みなとみらい2-3-1
クイーンズタワーA10階