グローバルインテリジェンス From MITスローンマネジメントレビュー

ランサムウエアと法規制

標的となる前に備えよ

近年、「ランサムウエア」の悪質なサイバー攻撃によりシステムがまひさせられる被害が世界で急増している。経営者は、身代金の支払いを受け入れる事態に直面する前に、6つの質問を顧みて備えておこう。

近年、「ランサムウエア（身代金要求型ウイルス）」による悪質なサイバー攻撃による被害が急増している。ランサムウエアは、感染させた機器のデータを暗号化し、解読できなくしてコンピューターシステムを事実上まひさせる。2019年から21年の間に、米国のサイバー攻撃は200%も増加した。被害は甚大で、足をすくわれるリーダーは後を絶たない。攻撃者はファイルを解読して感染したシステムを復元する代わり、被害者にデータの身代金を要求する。

ランサムウエアの攻撃は1980年代に始まり、2010年以降には犯罪者が決済手段として好む暗号通貨が台頭していることもあり、多くの組織にとってより大きな脅威だ。何よりつらいのは、脅威が不確実性に満ちており、対策を練ることが非常に困難である点だ。多くの組織は結果が確実でないにもかかわらず、経済的な負担も大きい身代金を支払うことで、最も迅速な解決策に走りがちだ。

取り戻したのはわずか8%

300社を対象とした最近の調査では、64%の組織が過去12カ月以内にランサムウエアの攻撃を受け、そのうちの83%が身代金を支払ったことが明らかになった。しかし身代金を支払った組織のうち、全データを取り戻したのはわずか8%で、63%は約半分しか取り戻せていない。

最初の身代金を期限内に支払ったにもかかわらず、2回目の（より高額な可能性のある）身代金の要求を受ける組織もある。最悪なのは、支払ったものの復号化キーを受け取れない、あるいは復号化キーが意図したとおり動作せず解除されない場合だ。

一方、支払わないと決めた組織は事業を一定期間停止し、収益上の損失発生に直面する。信頼できるバックアップシステムや緊急時対応計画を持たず、準備不足の状態を放置していた組織は、攻撃で、経済的な面だけでなく、評判の面でも最も大きな被害を受ける。ランサムウエアの攻撃を受けたら、警察やデータ保護当局に攻撃の事実を知らせなければならない。その後の決断は、組織がサイバー攻撃に対処するための準備をどの程度整えているかに依存する。

本稿で、経営陣は6つの明確な質問を通して何をすべきか判断できる。ランサムウエア攻撃を受ける前に質問について検討を進めることで、攻撃のダメージを和らげたり、攻撃された場合に組織がより適切に対応し

フィリップ・レオ *Philipp Leo*
レオ&マリーサイバーアドバイザリーパートナー兼スイス軍サイバーコマンド大尉

経営コンサルティング、銀行、メディアなどを経験。スイス軍でサイバー専門家候補を指導。データ保護とサイバー犯罪に関する欧州警察機構（ユーロポール）の専門家ネットワークの一員。

オイコー・イシュク *Öykü Işık*
IMDデジタル戦略・サイバーセキュリティー教授

デジタルの強靱な回復力、破壊的な技術が社会や組織にもたらす課題を専門とする。論壇における新進気鋭のリーダー（Thought Leaders）を選ぶThinkers 50 Radar 2022に選出された。

ファビアン・マリー *Fabian Mably*
レオ&マリーサイバーアドバイザリーパートナー兼スイス・ローザンヌ大学犯罪学研究員

スイス・ローザンヌ大学で犯罪学を研究。サイバーリスクの人的要因や知識を与える革新的な方法を扱う。データ保護とサイバー犯罪に関する欧州警察機構（ユーロポール）の専門家ネットワークの一員。

身代金を要求されてからでは遅い

●ランサムウエアに備える6つの質問

Q1 技術的な準備はできているか?

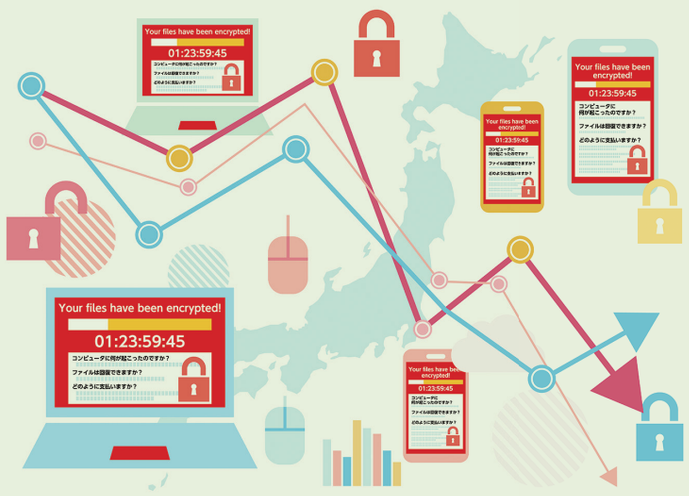
Q2 サイバー脅威情報へのアクセスは可能か?

Q3 サイバー保険に加入しているか?どこまで実際に被害を補償するだろうか?

Q4 財務上のリスクはどの程度だろうか?

Q5 身代金を支払うことの法的な意味合いとは?

Q6 交渉は可能か?



回復させたりするきっかけとなろう。

質問1　技術的な準備はあるか

21年7月にランサムウエアグループが米ソフトウエア会社を攻撃したとき、ハッカーはわずか2時間でサーバーの下流にある数十万もの組織にランサムウエアをインストールした。検知と回復のプロセスを優先するため、システムに対し「侵害されている」と想定しながら取り組めば、組織はより能動的に考え、予防と同じくらい対応に力を入れられる。絶えず最新のバックアップを持ち、ランサムウエアの攻撃からバックアップを守ることが最初の戦略的優位だ。だがそれだけでは不十分だ。

緊急時にバックアップを使用して、最小限の損失や障害でシステムを元通りに復旧する能力を構築・保持しなければならない。多くの組織が不十分で、バックアップデータの58%は、復旧に失敗している。定期的にバックアップの復元能力をテストすべきだ。またランサムウエアはバックアップの場所を特定し攻撃するので、バックアップを遠隔地に置き他のネットワークに接続しなければ見つかりづらくなる。

準備と情報、備えはあるか

また、組織のリーダーはIT（情報技術）チームが緊急時対応のマニュアル通りに詳細な行動を計画し、その計画が最新で、関連するスタッフが計画をよく理解し、頻繁に実践していることを準備の際に確認する必要がある。これは不正プログラムの拡散を防ぎ復旧を早めて証拠を保護するために不可欠となる。米国土安全保障省傘下のサイバーセキュリティー専門機関（CISA）は、対処するためのベストプラクティスを詳述したランサムウエアガイドを提供し、米国立標準技術研究所（NIST）はランサムウエアからデータを保護するための優れた指針を提供している。

質問2　脅威情報を得られるか

ランサムウエアは出現以来進化してきたが、防御策も進化した。ランサムウエアを解読した研究者は解読キーとともにオープンアクセスのリソースをオンラインで公開する。攻撃された後の選択肢を検討する際、こうした情報源や警察に確認し、解決策がすでにあるかどうか確認する必要がある。またサイバーセキュリティー研究機関などの「脅威インテリジェンスリポート」を確認し、自社を標的にする特定の犯罪組織に関するあらゆる情報を得る必要がある。

ランサムウエアを用いた攻撃者は後を絶たず、相手を正確に理解することに大きな価値がある。「ランサムウエア・アズ・ア・サービス（ランサムウエアをサービスとして提供する）」というビジネスモデルが出現して以来、ランサムウエアのギャングと提携すれば誰でもハッキングできる。多くは感染量を増やすことにしか興味がなく、身代金支払い後に復号化キーを送信しない。ランサムウエアで攻撃してきた犯人と、身代金支払い後に暗号化キーを実際に送信する者が一味だと確認できているかどうかは重要な情報となる。

質問3　保険はどこまで補償するか

多くの保険会社が00年代初頭にサイバー攻撃の被害に対する補償を

写真=PIXTA

提供し始め、それ以来市場が発展してきた。現在、サイバー保険の保険金請求のうち、ランサムウエアによるものが75%を占める。

「戦争認定」で保険不払い

結果、仏アクサをはじめとする生命保険大手は、身代金の支払いを補償せず、事業損失のコストのみを補償するようになった。また、17年のランサムウエア「NotPetya」攻撃のように国家の資金提供が疑われる場合は、保険会社が攻撃を戦争行為と分類して保険金支払いの責任から逃れる場合もある。リーダーは、契約するサイバー保険が思うように活用できない事態に直面する前に、保険の契約条件、特にランサムウエアの補償を提供しているかどうかを知っておくべきだ。

質問4　財務上のリスクは?

まず復元コストを把握し、ビジネスへの影響と失われたデータの復旧にどれだけ費用がかかるか計算する。それで情報セキュリティーに投資しないことのトレードオフを理解できるだけでなく、他に方法がない場合に身代金を支払うことが経済的に妥当な選択かどうかを評価できる。

質問5　身代金支払いの法的意味

最新の完全なバックアップと綿密な復元計画や包括的な保険がない場合、身代金を支払うしかない場合もあろう。だが米国の司法権の下で活動する組織（または支払いの実行責任者が米国籍の場合）は難しいかもしれない。21年9月米財務省は、制裁を科すサイバー犯罪者に身代金を支払ったり支払いを促したりすることは違法で、刑事訴追を受ける可能性があると注意喚起した。欧州当局もランサムウエアへの支払いの法的規制を議論中だが、まだ施行されていない。司法の枠組みや脅威の主体に関する正確な知識は不可欠だ。


脅威はどこにあるか分からない

質問6　交渉は可能か?

身代金支払いが最も被害が少ないと判断した場合も、攻撃者と直接連絡するなら専門の交渉人を検討すべきだ。韓国のウェブホスティングプロバイダーNAYANAのケースでは、被害者が交渉人の助けを借り、身代金を大幅に減らせた。だがランサムウエアには、被害者が交渉のプロを雇った場合、復号化キーを削除し、システム復旧の希望をすべて打ち砕くと脅すものもある。ここでは先に述べた脅威インテリジェンスが、リスク評価に役立つ場合がある。

仮にあなたの組織がサイバー犯罪者の標的になった場合、身代金の支払いにどう決断するにしろ、ランサムウエア事例を当局に報告した方がよい。米国では、重要インフラとみなされる分野の組織は、ランサムウエア攻撃をCISAに速やかに報告することが義務付けられる予定だ。

欧州では、一般データ保護規則にサイバーインシデント（サイバー攻撃事例）の報告義務が含まれる。サイバー攻撃は、専門家が似た事件に関する情報を入手し、被害を受けた当事者の協力を得ることでより効果的に調査できる。急速に進化する環境では他人の経験が最良の学習機会となり得るため、情報開示が必要だ。信頼できる仲間同士のネットワークで情報共有を促進する取り組みもある。

ランサムウエアまん延に対する理想的な解決策は犯罪者にお金を払わないことだ。だが新型コロナウイルスの経済的影響に悩んだり、デジタル変革の取り組みに予算を優先させたりしている組織では、サイバーセキュリティーへの予算が足りない。現在はアンチウイルス／アンチ不正プログラムや多要素認証などの予防機能に資金が費やされ、検知、対応、復元のプロセスは見落とされている。

全組織がサイバー衛生レベルを最低限の水準に引き上げるまでは、脅威を受け入れ、身代金を支払うのが有効な場合もあろう。攻撃の影響を完全になくすには不十分かもしれないが、6つの質問を顧みて、意思決定プロセスで危機感を持ち冷静になるきっかけとなることを願う。 NB

写真=PIXTA