法務・コンプライアンス・テクノロジー
責任者必読

ランサムウェア攻撃特有のリスクをどのように管理するか

EY
Building a better working world

新型コロナウイルス感染症が引き起こした恐怖や不確実性に乗じ、サイバー犯罪者たちはフィッシングやランサムウェア攻撃を活発化させ、パンデミックへの対応に追われる組織にさらなるリスクをもたらしています。危機的状況が続く中、リモートワークの拡大や人々の情報を得たいという心理につけ込んだフィッシングメールが急増していますが、国際刑事警察機構（インターポール）が指摘しているとおり、フィッシングメールはランサムウェアの感染を世界中に拡げる最大の経路でもあります。

実際、インターポールはコロナウイルスと闘う重要な組織を狙ったランサムウェア攻撃が大幅に増加していることを確認しています。犯罪者たちは新型コロナウイルス感染症ワクチンの試験設備を攻撃したほか、イタリアの社会保障組織が緊急給付金の受付を開始した際に組織のウェブサイトをダウンさせました。インターポールは、こうした攻撃は今後さらに悪化するとみており、世界中の警察組織に脅威が高まっていると警告しています。

ランサムウェア攻撃から組織を守るために

本編は特に以下の読者を想定：
弁護士
社内セキュリティ担当者
情報セキュリティ責任者
コンプライアンス責任者
リスクマネジメント責任者
内部監査室

攻撃者から送付されたメールに記載されたリンクを1人がクリックするだけで、マルウェアはものの数分で組織のネットワーク全体に拡がり、重要なデータを暗号化します。組織は業務に必要なファイルやシステムにアクセスできなくなるため、犯罪者に金銭を支払って復号鍵を手に入れるか、データを回復する別の方法を探さなければなりません。

従業員の意識向上が重要

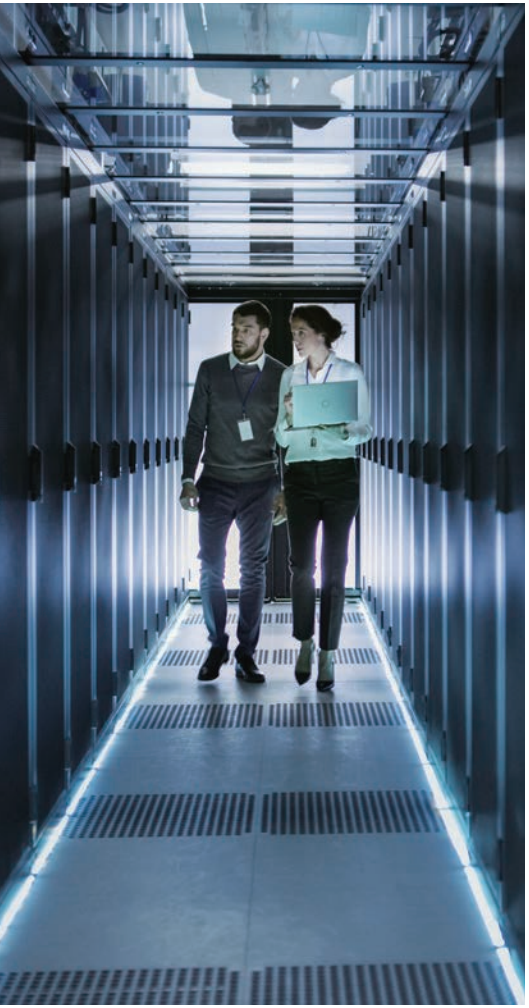
ランサムウェア攻撃は確かに増えていますが、攻撃の成功率を下げるために組織ができることは沢山あります。例えば、増大するランサムウェアの脅威や組織のセキュリティプロトコルを従業員に周知することは組織防衛の第一歩です。2020年に実施された世界規模の調査では、ランサムウェアとは何かを説明できる成人労働者は3人に1人もいませんでした。実際、米国で働いている人の30%近くはマルウェアとは何かという質問に対し、コンピューターシステムの破壊や不正アクセスを狙ったソフトウェアではなく、無線接続を改善するハードウェアの一種と回答しています[1]。

従業員には、不審なメールに気付いたり、組織内の窓口に速やかに通報する方法を伝えなければなりません。ある研究では、偽のフィッシングメールを医療機関に送ったところ、従業員の17%近くが悪意あるサイトに誘導される可能性のあるリンクをクリックしました。しかし同様の偽メールをさらに送信し、同時に従業員向けの教育も実施した結果、クリック率は大幅に低下しました[2]。

こうした教育では、ランサムウェアのさまざまな感染経路に言及することも不可欠です。リモートワークをしている従業員には、攻撃者が人々の警戒心のなさに付け入り、リモートデスクトップのようなツールを使って組織のネットワークに侵入し、ランサムウェア攻撃を仕掛けることを理解してもらわなければなりません。従業員は感染したウェブサイトに気付かずにアクセスしてマルウェアをダウンロードしたり、正規のソフトウェアと見せかけたマルウェアに騙されたりする可能性もあります。

1 2020 State of the Phish Annual Report、Proofpoint、2020年 https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

2 William J. Gordon、Adam Wright、Ranjit Alyagari、"Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions"、Journal of the American Medical Association、2019年3月8日 https://jamanetwork.com/journals/jamanetwaorkopen/fullarticle/2727270



複数の防衛策を組み合わせることが不可欠

ランサムウェアから組織を守るためにはデータのバックアップが欠かせませんが、多くの組織はバックアップデータを日常業務に利用しているネットワーク上に保管しています。これでは組織の各コンピュータ上に置かれているファイルと同じくらい簡単にバックアップデータを暗号化されてしまいます。バックアップを守るためには、他のネットワークから切り離されたネットワークかオフライン環境にデータをバックアップする必要があります。例えば、病院を狙った攻撃が続いた後、多くの病院は重要なシステムのバックアップを定期的にオフライン環境に移すようになりました。そうすれば病院の基幹ネットワークが遮断されても、業務の遂行に必要なデータにアクセスできるからです。しかし、たとえバックアップデータを守ることができても、システムの復旧には数日、場合によっては数週間を要することに留意する必要があります。

サイバーセキュリティの衛生管理（サイバーセキュリティ・ハイジーン）を徹底するには、パッチの管理、セキュリティ構成の強化、脅威インテリジェンスを活用した継続的な攻撃検知も欠かせません。ブラウザやプラグインのソフトウェアアップデートがリリースされた時は、できる限り速やかに適用することも重要です。機密情報を予め暗号化しておくことも、身代金を支払わなければ情報を開示すると脅すサイバー犯罪者に対抗する一つの方法です。

ランサムウェアなどのサイバー攻撃に備えてすでに組織内に導入している防衛策も、定期的に中立的な第三者による監査を受ける必要があります。サイバーセキュリティ保険が普及しつつありますが、保険は堅固なセキュリティの代わりにはなりません。組織が適切なセキュリティ手続を講じていない場合、あるいは適切な手続がないことを保険会社に開示していなかった場合、保険会社は保険金の支払いを拒否することがあります。

ランサムウェア攻撃への対応

サイバー攻撃のリスクが高まり続ける中、迅速な検知と封じ込めを重視する組織が増えています。すべての組織がインシデント対応・復旧計画を策定し、かつ計画を定期的に見直してアップデートすることを求められています。IT、情報セキュリティ、法務、コンプライアンス、人事、運用、広報など、関係する部署をすべて巻き込みましょう。インシデント対応計画において各部署の責任を明確に定義し、有事の際に担当者が効果的なリーダーシップを発揮できるようにします。

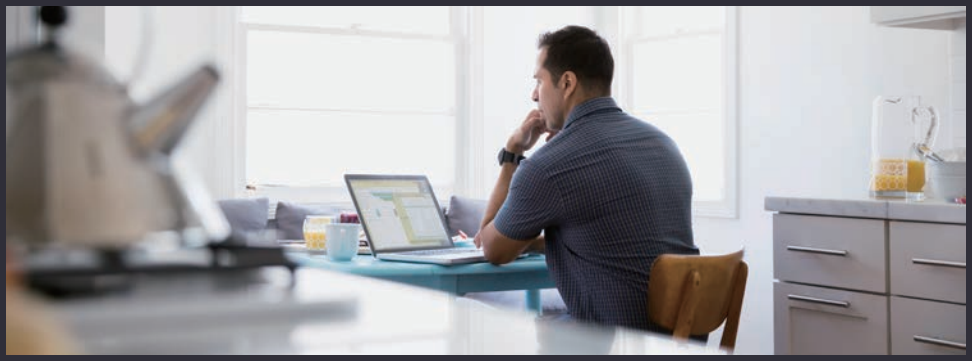
攻撃を発見した時は直ちに顧問弁護士を関与させます。顧問弁護士は、その国や地域で要求される調査の水準、データ保護やプライバシーに関する規制で定められた通知要件の順守について助言することができます。外部弁護士を関与させれば、セキュリティ侵害が訴訟に発展した場合も秘匿特権を維持できます。

ランサムウェア攻撃に対応する際の留意点

一般に、サイバー攻撃に対応するプロセスには、調査、封じ込め、根絶、復旧という4つの並列した活動が含まれます。この4つの活動は、ほぼすべての種類のサイバー攻撃に当てはまりますが、ランサムウェアの場合は特に留意すべき点があります。

ランサムウェアの調査でエビデンスを収集する際、攻撃者はどのようにして環境に侵入したのか、マルウェアはどのように使われ、攻撃者はシステム内をどのように移動したのか、盗まれたデータや暗号化されたデータがあれば、それは何のデータであるかに重点を置く必要があります。また、ビットコインウォレットのランサムノート（身代金の要求メッセージ）や攻撃者とのやり取りは、封じ込め、根絶、復旧の段階で重要になるため、慎重に文書化する必要があります。

攻撃が発生した時は、その影響を受けていないシステムにも調査の範囲を広げます。影響を受けなかったように見える環境から、別のマルウェアや休眠しているランサムウェアが発見されたケースは珍しくないからです。インシデントの再発を防ぐためには、ネットワークに隠されているマルウェアの痕跡をすべて取り除かなければなりません。



規制上の通知義務

一部の地域では、ランサムウェアへの感染は法規制上、通知義務のあるサイバー攻撃に指定されています。攻撃の影響を受ける地域を特定することは、組織が適切な手続をとる助けになります。米HIPAA法（医療保険の相互運用性と説明責任に関する法律）は医療機関に対し、ランサムウェア攻撃を受けた場合はセキュリティインシデントとして報告すること、またランサムウェアへの感染を防ぐためのセキュリティ措置（データのバックアップなど）を講じることを義務付けています。

攻撃の影響を受けた個人情報がないか否かも確認する必要があります。そのような個人情報があれば詳細を確認し、顧問弁護士と相談の上、それがデータの喪失にあたるか、データ保護やプライバシーに関する法規制（例：EUの一般データ保護規則、カリフォルニア州消費者プライバシー法）で定められた、通知を要する事象に該当するかを判断します。

身代金の支払に係る法規制上の懸念事項

他のサイバー攻撃と異なり、ランサムウェア攻撃にはそれを終わらせ、暗号化されたファイルを復号する簡単な方法があります――要求された身代金を支払うことです。しかし、犯罪者に身代金を渡すという判断は、倫理的ジレンマはもちろん、多くの法的問題を含んでいます。

世界中を見渡しても、身代金の支払を勧めている法執行機関はありません。米国の連邦捜査局（FBI）は一般的なマルウェアの復号鍵を一部公開しており、欧州の警察機関が支援するNo More Ransomは復号鍵の公開だけでなく、各国規制当局のサイバー犯罪通報窓口もウェブサイトに掲載しています。プルーフポイントによる2020年の調査では、組織の29%が身代金を支払ったにもかかわらずデータにアクセスできなかったと回答しました。何らかの理由から、複数回にわたって身代金を支払った組織もあります[3]。

ニューヨーク州は現在、サイバー攻撃に対する身代金の支払を違法とする2件の法案を審議しています。攻撃者が既知のテロ集団のメンバーであることが判明した場合、身代金を支払うことは米国のテロリスト制裁措置への違反とみなされる恐れがあります。

攻撃されたデータの回復に外部のサービスを利用する場合も、組織が知らないところで身代金が支払われる可能性があることに留意する必要があります。プロパブリカの調査では、独自の復号手法を用いてデータを回復すると言っていた米国企業2社が、実際には身代金を支払って復号ツールを入手していたことが判明しました[4]。データの回復に外部のリソースを使う場合は、業者を慎重に選ぶだけでなく、身代金を支払うかどうかも明確に尋ねる必要があります。

[3] 2020 State of the Phish Annual Report、Proofpoint、2020年 https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

[4] Renee Dudley、Jeff Kao、"The Trade Secret - Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hacker"、ProPublica、2020年5月15日 https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

最後に

新型コロナウイルス感染症の危機は、ランサムウェア攻撃がもたらすリスクを高めています。この傾向は、利用できるリソースが少ない組織では特に顕著です。しかし予防策を講じ、たとえ侵入されても速やかに検知し封じ込めることができれば、リスクを軽減することができます。組織で働く人の多くがサイバーセキュリティをITの問題と捉えていることを考えると、ランサムウェアの脅威を従業員に周知することは組織防衛に欠かせないステップです。組織はデータのバックアップ計画を適切に策定することで、喪失したデータを迅速に回復し、システム復旧までの時間や生産性の低下を最小限に抑えることが可能になります。

ただし、予防だけでは問題は解決しません。ランサムウェア攻撃を速やかに検知し、封じ込め、短時間で復旧することができれば、事業の継続や経済損失の阻止に貢献するでしょう。効果的な対応戦略は組織が将来の攻撃を検知し、対処する能力を高めることにもつながります。暗号化されたデータを復号するために身代金を支払う場合は、システムからマルウェアが完全に排除されているかを徹底的に確認しましょう。

法律とコンプライアンスの専門家は、ランサムウェア攻撃がもたらす法規制上の問題を理解することで組織の対応を支援できます。ランサムウェア攻撃は組織に壊滅的な影響を与える可能性がありますが、この攻撃に対応するための効果的な戦略を策定することはIT専門家だけでなく、リスクの軽減に携わるすべての人の努めであることを忘れないでください。

詳細については、EY Japan Forensic & Integrity Services Technologyチームにお問合せください。

E-mail : forensics.cyber@jp.ey.com
Tel : 03 3503 3292

EY | Assurance | Tax | Transactions | Advisory

EYについて

EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYについて詳しくは、ey.comをご覧ください。

EY Japanについて

EY Japanは、EYの日本におけるメンバーファームの総称です。EY新日本有限責任監査法人、EY税理士法人、EYトランザクション・アドバイザリー・サービス株式会社、EYアドバイザリー・アンド・コンサルティング株式会社などから構成されています。なお、各メンバーファームは法的に独立した法人です。詳しくはwww.eyjapan.jpをご覧ください。

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものではありません。法人名および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

eyjapan.jp

Contacts:

Global

Todd Marlin
todd.marlin@ey.com

Americas（北・中・南米）

Shawn Fohs
shawn.fohs@ey.com

Manish Khera
manish.khera@ca.ey.com

Asia-Pacific（アジア・パシフィック）

Chi Chen
chi.chen@cn.ey.com

Jack Jia
jack.jia@hk.ey.com

Nick Robinson
nick.robinson@hk.ey.com

杉山 一郎
ichiro.sugiyama@jp.ey.com

Matthew Westwood-Hill
matthew.westwood-hill@au.ey.com

EMEIA（欧州、中東、インド、アフリカ）

Lorenz Kuhlee
lorenz.kuhlee@de.ey.com

Bodo Meseke
bodo.meseke@de.ey.com

Brenton Steenkamp
brenton.steenkamp@nl.ey.com