連載「プロマネの現場から」

第 191 回　ランサムウェアの脅威

蒼海憲治（大手 SI 企業・製造業系事業部門・技術総括部長）

システムの運用・保守業務していて、本番障害・トラブルの発生時の緊急度や緊張感はいつになっても慣れることはありませんが、その中でも、トラブルが情報セキュリティ事故を伴うケースは、その重要度合いは格段に高まると感じています。

IPA による「情報セキュリティ 10 大脅威」の２０１６年と２０２２年の報告書（＊１）（＊２）を比べてみて気づくことは、２０１６年時点、組織として７位にランクされていた「ランサムウェアによる被害」が、２０２２年は１位になっていることです。

ランサムウェアは 1980 年代からある古くて新しいウイルスの一種です。PC やサーバが感染すると、端末のロックやデータの暗号化が行われ、その復旧と引き換えに金銭を要求されます。また、暗号化前に重要な情報が窃取され、金銭を支払わなければ、窃取した情報が公開されることで社会的信用を失うおそれがあります。

ここ数年、上海に赴任中も、日本に帰国してからも、お取引している顧客企業でのランサムウェア感染の報告とその後の調査協力やリカバリー要請を受けることが続いています。その原因は、情報システム部門が管理していない、エンドユーザにより構築・利用されている野良システムやクラウド利用における脆弱性をつかれる点にあります。

いったんランサムウェアに感染すると、関連するシステムやネットワークの停止・切り離しを行い、侵害範囲特定や原因の目途がつくまでは業務の停止を余儀なくされます。ランサムウェアにより暗号化された情報に、個人情報が入っていた場合、各国への当局への報告が必須となるため、決められた期限との勝負となります。感染発覚後の対応の大変さと緊張感は、通常の本番障害時の対応に比べて数倍大変なように感じています。

今回は、株式会社ラックのサイバー救急センターの方々が書かれた『ランサムウエアから会社を守る　～身代金支払いの是非から事前の防御計画まで』（＊３）を基に、ランサムウェアの脅威とその対応策について考えてみたいと思います。

本書において紹介されている、Veeam によるランサムウエア被害に関する調査レポート「Veeam 2022Ransomware Trends Report」によると、調査対象企業のうち、サイバー攻撃被害者の大多数(76%)は、攻撃を食い止め、データを回復するために身代金を支払っている、といいます。しかし、そのうち 52%が身代金を支払うことでデータを復旧できた一方で、24%は身代金を支払ってもデータを復旧できなかった。つまり、3 分の 1 の確率で身代金を支払ってもデータが復旧できていません。しかし、実に 76%の組織が身代金を払っていたという調査結果は正直驚きでした。

「身代金の支払いに応じる」場合と「身代金の支払いに応じない」場合のメリット・デメリットには、各々以下のものがあります。

「身代金の支払いに応じない」のメリットとしては、犯罪組織の支援につながる身代金の支払いは行わないとの姿勢を示すことができます。デメリットとしては、要求された身代金の支払いに応じなかった場合、暗号化されたデータの復元はほぼ不可能になります。そのため、システムの復旧にはシステムをもう１回作り直すのと同等の期間と費用が必要となります。また、ランサムウェア攻撃者に「人質」として窃取されていた情報が公開されてしまうおそれがあります。

一方、「身代金の支払いに応じる」場合のメリットとしては、攻撃者から暗号化されたデータを復号するツールを入手し早期にデータ復旧ができる可能性があることと、攻撃者による窃取された情報の公開を止めることができる可能性があります。

しかし、デメリットとしては、犯罪組織への支援となるため世間からバッシングを受け、組織のイメージが低下するおそれがあります。また、身代金支払ったからといって必ず暗号化されたデータを復元できるという保証はありません。さらには、脅せば身代金を支払う組織と思われた場合、攻撃者から身代金の再要求が発生するおそれがあります。

攻撃手口としては、メールの添付ファイルやメール本文中のリンクを開かせることで感染させたり、ランサムウェアをダウンロードさせるよう改ざんしたウェブサイトから感染させたり、ソフトウェアの脆弱性を未対策のままインターネットに接続されている機器に対してその脆弱性を悪用してインターネット経由で感染させるなど様々な経路があります。特に、脆弱性を未対策の機器を放置した場合、自組織の機器を踏み台にされることで被害者から加害者になるおそれもあります。

そのため、ランサムウェアの脅威に対策するためには、ランサムウェアそのものの対策のだけでなく、攻撃者による外部からの侵入や、侵入された場合の侵害行為に対する対策も必要になります。つまり、ランサムウェア攻撃に関しても自組織で利用しているシステムに合わせて全般的なサイバーセキュリティ対策を実施する必要があります。また、もしランサムウェア攻撃の標的になった場合に、ランサムウェア抑えるためには、ウイルス対策ソフトなど一つの対策だけでなく、多層的な防御が必要となります。

このサイバーセキュリティ対策を実施する費用を無駄なコストと考えて、抑制・手抜きする企業や組織が多いのが実態だと思います。そのため、本社の情報システムやネットワークを情報システム部門が管理・統制している場合でも、支社や海外現地法人、パートナーなど取引先などへの管理まで手が回らず、一番弱い部分の脆弱性を狙ってランサムウェアだけでなく様々なマルウェアが侵入するケースが多々あります。しかし、いったん感染してしまうと、被害は大きく、かつ、組織の社会的信用が失墜するおそれがあります。

経済産業省では「サイバーセキュリティ経営ガイドライン」の中で『経営者が認識すべき３原則』として次の３つを定めています。

①経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

②自社は勿論のこと、ビジネスパートナーや委託先含めたサプライチェーンに対するセキュリティ対策が必要

③平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

サイバーセキュリティ対策を、自組織が存続し続けるための「保険」や「投資」と捉えること。

セキュリティ対策は考慮すべき範囲があまりに広いため、一部の情報システム部門に任せるのではなく、経営者がリーダーシップを取り、組織全体で対応していく必要があります。

以下、ランサムウェアへの対応策の一例になります。

１．侵入されうる経路を考えること

１．１．自組織の資産棚卸し

自組織のネットワーク構成・IT 資産管理状況、アカウント管理状況、それらを踏まえて脆弱性管理状況を把握する必要があります。

これまで組織内のセキュリティ対策により保護されていたコンピュータが、テレワークによる組織外への持ち出しにより無防備になってしまう問題も生じています。また、クラウドサービスを利用することで、組織内のデータが外部からアクセスされやすくなっています。利用される機器も、PC だけではなく、スマホやタブレット等に広がり、統一した運用管理やウイルス対策ソフトでの管理が難しくなっています。どの脆弱性を悪用して攻撃者が侵入するおそれがあるか把握する必要があります。

１．２．ペネトレーション（侵入）テストで弱点を知ること

実際に攻撃者の視点で自組織の環境に侵入できるか試す方法として、ペネトレーションテストを活用します。専門家による疑似的な攻撃を仕掛けることで、現状実施しているセキュリティ対策の有効性をチェックすることができます。

１．３．各種バックアップをとること

ランサムウェア攻撃を受けてファイルが暗号化されてしまった場合、スムーズにシステムを再構築するためには、バックアップの有無が重要になります。バックアップから復旧が可能であれば、身代金を払うことを検討する必要はなくなります。

しかし、バックアップの保存場所に問題があると、バックアップも同時に暗号化されてしまうケースが生じます。また、バックアップの方法に問題があると、必要な情報が欠落し、バックアップを取っていたにもかかわらず正しく復旧できないケースも生じます。差分データだけを取得の場合、データ復旧に数日どころではなく、数か月以上かかるという試算になるケースもあります。

２．インシデントに備えた防御策

ランサムウェア攻撃による被害を防ぎ、影響を少なくするために、様々な防御策を、多段階で実施する必要があります。

２．１．ウイルス対策ソフトの導入。ただし、ウイルス対策ソフトを導入するだけでなく、パターンファイルが常に最新になっているか、後から解析できるように検知したファイルを「駆除」ではなく「隔離」する設定とする等、考慮すること。

２．２．自組織で利用している IT 資産に関する脆弱性情報は常に注視し、新たな脆弱性やセキュリティパッチの配信を確認し、対応すること。

２．３．自組織で利用しているサービスやコンピュータのアカウントのパスワードは十分長く複雑なものを設定し、使いまわさないようにすること、また定期的に更新すること。

２．４．攻撃者の侵害範囲を拡大させないために、社内ネットワーク上の重要サーバや共有フォルダ、クラウドサービスへのアクセス権限を必要最小限にとどめられるよう IP アドレスでの制限をかけること。必要に応じてネットワークセグメントの分割やネットワーク構成の見直しを行うこと。

２．５．重要データの保護のため、データの暗号化などのデータ保護ソリューションをの活用する。この対策により、重要データを窃取された場合でも、攻撃者が中身を読むことができなくなり、「身代金を払わないとデータを公開する」という二重脅迫への対策になります。

２．６．情報漏えい対策としては、DLP (Data Loss Prevention)と呼ばれる製品を導入することで、監視対象のファイルが持ち出される際、アラートによる通知や送信の防止がされることで重要データの流出を防ぐことができます。

２．７．インシデントに備えた事業継続計画とトーニング

以上のようなインシデントに備えた防御策を講じたとしても、修正パッチが提供されていない脆弱性を悪用したゼロデイ攻撃や、パッチ適用前に攻撃をしかけてくるおそれがあり、攻撃の脅威をなくすことはできません。

そのため、セキュリティインシデントに備えての事業継続計画(Business Continuity Plan)の策定とそれに基づくトレーニングが必要になります。

２．８．侵入を検知するためのログの取得・保管

攻撃者による不審な活動を捉えるためには、その活動の痕跡を記録する仕組み、すなわちログの取得が必要になります。

ログは、セキュリティインシデントが発生した際の調査にも非常に有用になります。

ログには、機器やソフトウェアにより様々ありますが、ネットワーク関連ログ・セキュリティ製品のログ・Windows/Windows Server のイベントログ・Linux のログ・クラウドサービスのログ等を押さえる必要があります。

また、バックアップと同様、保管していたログを、攻撃者により暗号化されないように保管場所に注意する必要があります。また、保存期間が短すぎるとインシデント発生時もしくは発覚時に必要な調査が実施できなくなるおそれがあるため、たとえば、重要なサーバに関しては少なくとも１年分のログは保管するためのコストやストレージを確保する必要があります。

２．９．EDR による不審な活動有無の監視

攻撃者による不審な活動を記録し検知するシステムとして、EDR (Endpoint Detection and Response)というソリューションがあります。コンピュータに対する防御として、ウイルス対策ソフトは警備員とすると、EDR は防犯カメラにたとえることができます。ウイルス対策ソフトは、「ウイルス」への対策であり、ウイルスなどのファイルを利用しない「ファイルレス攻撃」などを検知することはできません。一方、EDR は、コンピュータで実行されるすべてのプログラムの挙動を記録し、不審な挙動がないか監視し検知することができることと、検知に対しコンピュータの隔離などを即時対応できます。

３．管理体制の整備

サイバー攻撃から組織を守るために具体的にやるべきことが整理できたら、これらのサイバーセキュリティ対策を実施するための管理体制を構築する必要があります。

管理体制が構築されていない場合、だれが何の役割を担い、何をすべきなのか、どこまで責任を持つのかわからず、統率が取れなくなり、対応が遅れることにより被害が拡大するおそれがあります。

３．１．セキュリティリスクの洗い出しとセキュリティポリシーの策定

管理体制の構築の前に、自組織の抱えるセキュリティリスクと、それに対してすべきことを洗い出すことが必要になります。

テレワークやクラウドサービスなど新しい環境やサービスの利用は日々変化しているため、定期的に自組織のセキュリティリスクの見直しをします。

次に、リスクの洗い出しができたら、それらの対応指針を示すセキュリティポリシーを検討します。

セキュリティポリシーは、どのような情報資産を、どのような脅威から、どのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制・運用規定・基本方針・対策基準などを定めたものになります。

このセキュリティポリシーは、セキュリティ担当者や経営層だけでなく、自組織内のすべての社員に周知すること必要があります。そうすることで、組織全体のセキュリティ意識向上を期待できます。

３．２．シーサートやセキュリティに関する管理体制の構築

セキュリティポリシーを策定できたら、組織全体のセキュリティ対策やインシデント対応を行うチーム「シーサート(Computer Security Incident Response Team の頭文字より、CSIRT)」を設置します。シーサートを設置することで、組織全体のインシデント対応を一元管理し、円滑に対処できるようになります。シーサートの役割には、平時においては、セキュリティ対策の強化および見直し・監視の運用・組織内外の情報共有などがあり、インシデント発生時においては、状況把握・被害拡大防止・復旧と対策の実施などがあります。

また、セキュリティ対策としてのタスクの中には、ペネトレーションテストやセキュリティ監視など、一部外部委託できるものもあるため、自組織のリソースや対策方針に応じて外部サービスの利用も検討する必要があります。

３．３．組織内外の情報共有

インシデントが発生した場合、情報のエスカレーションが重要になります。インシデントを現場のみで対応しようと、組織内に報告せず、無視したりした場合、被害や影響範囲が広がり、手遅れになってしまうおそれがあります。

人間はミスをするものですが、そのミスを責めるのではなく、ミスを無視・放置・隠ぺいすることこそが、ミス自体よりも問題であるこという共通認識を組織内に確立することが重要になります。

また、組織外との情報共有も大切になります。日本シーサート協議会や FIRST (Forum of Incident Response and Security Teams) 等に加盟することで、他組織で発生したインシデントの原因や対策といった情報を把握するおくことで、万が一同じ問題に遭遇した際に円滑な対応をとれることが期待できます。

また、他組織のインシデントや新しいセキュリティ製品などの情報など収集し、脆弱性情報を含め、セキュリティに関する注意喚起を行うことが大切になります。

冒頭にも述べましたが、いったんランサムウェアに感染すると、通常の業務を中断してで、最優先で対応する必要が生じます。セキュリティ対策は多岐にわたり対応範囲が広いため、経営者がリーダーシップを取り、組織全体で対応していく必要があります。

（＊１）IPA「情報セキュリティ 10 大脅威 2016」
（＊２）IPA「情報セキュリティ 10 大脅威 2022」
（＊３）佐藤敦・漆畑貴樹・武田貴寛・古川雅也・関宏介『ランサムウエアから会社を守る　～身代金支払いの是非から事前の防御計画まで』、日経 BP、2022 年刊