ランサムウエアの脅威への備えと対策 NIST フレームワークと最近の事例から得られた 13 の教訓

June 18, 2020

ランサムウエアによる攻撃が世界中で後を絶たず事業の妨げとなっている。企業側も対策を強化してはいるが、ランサムウエアもより進化したものとなり、いたちごっこの様相である。かつてはランサムウエアといえば企業のコンピュータ・システムを暗号化ソフトでロックし、ロックを解除するためのキーと引換えに金員を要求するだけのものであった。

しかし、最近はそれに加え、被害企業への圧力を高める手段としてデータを盗み出すことが行われている。2020 年 6 月には、ランサムウエアの攻撃グループであるレヴィルが、カナダの農業会社のものと思われる 22000 個のファイルの入った 3 つのデータベースをオークションにかけるという事件があった。同農業会社が要求された金員を支払わなかったためだと思われている。オークションの開始価格は 5 万ドルであった。このような攻撃を受けた場合には、被害企業がバックアップシステムを稼動させていて、ランサムウエアによるロックを解除する必要がないとしても、盗まれた秘密情報を公にされることを避けるために、要求された金員の支払いを検討せざるを得ない。

また、ランサムウエアは、新型コロナウィルスによる影響を受けて困難に直面している病院、法律事務所、金融機関、IT 企業、政府機関などへの攻撃にも使われている。
ランサムウエアによる攻撃は、攻撃の効果を最大化するため、システムに侵入後により長い時間をかけて（数日間、時によっては数週間もかけて）システムを研究したうえで行われるようになってきている。

このような攻撃が成功しているのをみると、米国の CISA（国土安全省の管轄下にある Cybersecurity and Infrastructure Security Agency）が 2020 年 5 月に指摘した問題点の重要性を改めて認識させられる。CISA は、企業がランサムウエアの攻撃に対して脆弱であり続けている原因として「ソーシャルエンジニアリング攻撃についての従業員教育が不十分であること及びシステムの復元・緊急時対応計画がないこと」を指摘している。CISA の指摘のとおり、また、フィッシング攻撃や使用していたソフトウエアが古かったために起こったいくつものランサムウエア事件からも分かるとおり、ランサムウエアの攻撃による被害を防止・軽減するためにはテクノロジーそのものとテクノロジー以外の両面での備えが必要である。

NIST のデータ・インテグリティ・フレームワーク案

ランサムウエアのリスクへの対処法を検討するに当たっては、NIST（National Institute of Standards and Technology）の 2020 年 1 月のデータ・インテグリティ・フ

レームワーク案が参考になると思われる。NISA は公的及び私的機関・企業等のために各種ガイダンスを発表する米国の機関であり、同フレームワークは、ランサムウエア等の攻撃を発見しそれに対処する方策の骨子をまとめたものである。NIST は米国の機関ではあるが、サイバーセキュリティの分野においては国際的な影響力が大きくなりつつあり、NIST の規準に従う機関・企業等も増えている。

発表されたフレームワークはドラフトの段階であるが、以下に記す 6 項目はランサムウエアのリスクに対処するに当たり有用である。

- **インテグリティ・モニタリング**
  システム運用のベースラインを決めておくことにより、攻撃の発見と評価が容易になる。本来あるべき状態が分かっていれば、ファイルが変更されたかどうか、また、誰が変更を加えたかも分かり易くなる。
- **事件の発見**
  システムへの侵入、マルウエア、ユーザーの異常事態等を発見するツールを使用するとよい。
- **ロギング（ログを残す）**
  しっかりとログを残し常にモニターすることにより、異常を発見しやすくなる。また、詳細なログを残すことで、システムに侵入された場合に侵入された箇所や不正にアクセスされたものを特定しやすくなり、どう対処すべきか決定するのに役立つ。
- **被害の軽減策と攻撃の封じ込め**
  攻撃を受けた場合にとりうる被害軽減策を、攻撃を受ける前に検討しておく必要がある。バックアップを隔離する、システムをネットワークから切り離す、ネットワーク全体をシャットダウンする、などの方策がある。これらの方策を実際に取るとするとその影響は大きいが、攻撃を受ける前にテストを行い、技術上および運用上もとり得る方策であるかどうか確かめておくことが大切である。攻撃を受けてからぶっつけ本番という事態は避けたい。特にバックアップシステムは重要であり、ランサムウエア攻撃に十分な余裕を持って耐えられるようにしておかなければならない。失うデータを少なくするため、バックアップをできるだけ頻繁に行うようにし、定期的にテストすべきである。
- **フォレンジックと分析**
  攻撃を封じ込めた後は、どのような攻撃を受けたのかよく調査し、攻撃を可能としてしまった脆弱な点がどこにあったのかを理解することが、同様の攻撃を再度受けるリスクを低減するために重要である。
- **報告ライン**
  攻撃を受けた際に対応し問題解決に当たるべき関係者に情報がいきわたるよう、事前に社内・社外の報告ラインを決めておくことが重要である。

ランサムウエア攻撃を避けるための 13 の方策

ランサムウエアの脅威に対抗するため、以上の項目をどのように実行しすべきか決定するに当たり検討すべき 13 のステップを以下に述べる。

技術的なコントロール

ランサムウエア攻撃を受けないようにするために採りうる技術的方策には以下のようなものがある。

１．ソフトウエアのアップデートと修正
アップデートや修正のされていないソフトウエアは攻撃を受けやすい。定期的にアップデートや修正を行うルールを決めておくことが攻撃を受けるリスクの低減につながる。

２．機器の管理
リスクベースでアップデートや修正を行うために、ネットワーク（古いサーバーや使っていないサーバーをも含む）に属するデバイスやシステムを把握しておく必要がある。

３．想定できる拡散方法による攻撃を受けることを防止
ランサムウエア攻撃に対応しているフォレンジック専門家は、ネットワーク上にランサムウエアをばらまくためのメカニズムとしてサーバーメッセージブロック、リモートデスクトッププロトコル、リモートパワーシェルなどのポートやプロトコルがよく使われていることを突き止めている。可能な限りこれらのポートやプロトコルを使った社内の通信をできないようにしたり防御・保護機能を追加したりすることを検討すべきであろう。

研修

すべてのレベルの従業員がランサムウエアに対して第一線で防御機能を果たしうる。

４．フィッシング研修
ランサムウエア攻撃のはじめに最も多く使われているのはフィッシングメールである。フィッシングメールについての研修とテストを常時行うことにより、ランサムウエア攻撃を受けるリスクを大幅に減らすことができる。

５．模擬訓練
ランサムウエア攻撃を受けているという想定で、模擬対応訓練を行うことが有用である。社内の関係部署の責任者が集まり、攻撃の初段階から各段階においてどのような意思決定を行うか、どの段階で誰に報告がなされるべきか、社内および対外的な発表はどうするかなど、具体的な対応を練習してみるのである。攻撃を受けている最中に攻撃者の要求に応じるべきかどうか正しく判断することは難しい場合が多く、どのような場合であったら攻撃者の要求に応じざるを得ないかを予め決めておくことが望ましい。模擬訓練で具体的な対応を検討することが、どのような場合に要求に応じるのか検討し決定するのに役立つ。

６．取締役会および社内トップへの状況の周知
社内のトップを含めた役員、取締役等がそれぞれ、会社がランサムウエア攻撃を受けた場合に果たすべき役割を理解していることが重要である。特に、当局がサイバー攻撃等の問題についてシニアレベルの役員が準備や対応にどのように関わっていたかに注目していることからもそのようにいえる。

ランサムウエアへの対応計画

企業は以下のような手段を事前に講じておくことによってもランサムウエア攻撃の影響を小さくすることができる。

７．フォレンジック・コンサルタント
事前に社外の技術コンサルタントやサイバーセキュリティ分野の弁護士に依頼しておけば、いざ攻撃を受けた場合に素早い対応が可能となり、社内の意思決定を担う責任者に対して重要かつ的確な情報を迅速に報告することにつながる。専門家は、ランサムウエアにどのような種類があるかを熟知しているので、専門家の助けを借りることでより迅速に攻撃を封じ込めることができよう。当局との繋がりのある専門家も多く、犯人の目安がつく場合もある。そして、犯人の目安がつけば犯人と交渉を行うこととした場合や犯人の要求に応じないこととした場合のリスクがどの程度のものかという判断もつく可能性がある。また、専門家がいれば、交渉することとした場合には交渉自体を任せたり、犯人の要求に応じざるを得ない場合にはビットコイン等の電子通貨の入手を依頼したりすることもできる。

８．通報先（捜査当局）を知っておくこと
管轄の FBI フィールドオフィスの電話番号（米国以外であればその地の捜査当局の連絡先）を有事の対応計画やランサムウエア対応計画に記載しておけば、通報の遅れを防ぐことができ、早期に当局から犯人に関する有用な情報を得ることができる可能性がある。犯人グループが経済制裁の対象と関係があるか、金銭と引換えに暗号を解く鍵を引き渡した実績があるかどうか、将来も繰り返し攻撃を行い脅迫してきそうかどうかなど、捜査当局から情報が得られるかもしれない。そのような情報が得られれば、金銭の支払い要求に応じるかどうか決定するのに役立つ。

９．情報伝達・公表計画
ランサムウエアの被害を受けた場合に、社内外の主な関係者に対してどのように対応するか（しないか）も予め考えておくべきである。誰が文案を作成するか、また、公表前に誰の承認を得なければならないこととするか等を決めておくことで適切な情報管理と伝達が可能となろう。

10. 非常時に備えた予備の情報伝達システム
ランサムウエア攻撃により、企業のメールなど情報伝達システムに被害が生じて使えなくなる場合がある。そうなった場合に社内の情報伝達に遅延が生じないようにするため、非常用に予備の情報伝達方法を用意しておくべきである。G-Suite や ProtonMail を利用したバックアップアカウントは安価であり、インターネットにつながっていさえすればどのようなデバイスからもアクセス可能であるため、非常時には予備の通信ネットワークとして使うことができる。

11. 保険の確認
サイバー保険に加入している場合には、犯人に支払う金銭がカバーされているか、また、支払う前に保険会社に通知を行わなくてもカバーされるかどうか、確認しておくことが重要である。場合によっては、保険会社が、犯人の要求にどのように対応するか、金銭の支払い要求に応じるかどうかなどの決定に関与することを前提としている可能性がある。

12. 何を優先するか

犯人に対して金銭を支払うかどうかのは、被害企業のそれぞれの事情により異なった決定が行われるものである。決定の際に考慮すべき事項は、システムが使えないことによる被害の大きさと情報漏えいの事業への影響の程度、要求をのめば犯人が約束どおり行動する可能性が高いかどうか、支払いを行うことの適法性などである。

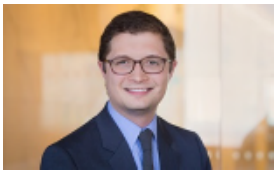
13. 情報開示義務を理解する

ランサムウエア攻撃を受けた場合の記録保存義務および開示義務は複雑であり、よく検討し理解しておくことが望ましい。情報の盗み出しを伴うランサムウエア攻撃では、仮に犯人の要求に応じることにより情報を返してもらったとしても、情報漏えいの通知義務（個人や当局に対して）が生じる場合があるのでなおさらである。GDPR の適用される企業は個人情報にアクセスできない状態が生じたこと自体で（米国の法制度上は通知義務が生じなくても）当局と当該個人への通知義務が生じる場合があることに注意すべきである。弊事務所では情報漏えい時の通知義務について、全米 50 州の州法および連邦法上どのような対応が必要かがわかるツールとして Debevoise Data Portal を作成中である。Health Insurance Portability and Accountability Act や Gramm-Leach-Bliley Act もカバーしている。現在何社かのクライアントの協力を得て試験中である。

ほとんどのサイバー・セキュリティに関する問題に共通することであるが、ランサムウエアの脅威は技術的・非技術的な準備を行うことにより大幅に小さくすることができる。攻撃を防ぐことができたり、攻撃を受けてしまっても被害を最小限にとどめることができるのである。


Luke Dembosky
ldembosky@debevoise.com


Avi Gesser
agesser@debevoise.com


Christopher S. Ford
csford@debevoise.com


Robert Maddox
rmaddox@debevoise.com


Friedrich Popp
fpopp@debevoise.com


HJ Brehmer
hjbrehmer@debevoise.com


Mengyi Xu
mxu@debevoise.com