TOPICS

法的リスクマネジメント講座 第89回

中小企業を狙い撃ちにするサイバー攻撃にどう備えたらよいか（続々編）

長谷川俊明法律事務所
弁護士
長谷川 俊明

はじめに

2023年2月初め、警視庁公表の「犯罪情勢（暫定値）」によりますと、2022年のランサムウェア攻撃の国内被害が、前年比約6割増の230件に上りました。被害増だけでなく、手口の悪質化が進んでいるそうです。

ランサムウェアの攻撃については、前々号の本欄で取り上げましたが、近年で目立つのが、ランサム（身代金）の支払がなければ機密データを公開する、と脅す「二重脅迫型」のサイバー攻撃です。2022年後半には、だれでもアクセスできるウェブサイトにデータを掲載してランサム(身代金)の支払いを迫る手口が登場しました。（図1）これは、いわゆる「劇場型」の暴露手法で、中小企業をいわば狙い撃ちにします。

実践的で役立つサイバーセキュリティのチェックリストに基づく対策検討

本稿では、中小企業の為のコストをかけないサイバー攻撃防御方法を考えます。前々号、前号につづき、“対策チェックリスト”による検討をします。

チェック項目3

テレワークの実施に際し、スキを見せないセキュリティ対策を行っていますか。	Yes / No

ポイント

コロナ禍もようやく収束の兆しが見えてきましたが、感染者数は一定水準を保っており、当面感染予防策は続けなくてはなりません。ウイルス感染予防対策の決め手は、日常生活のなかで「密を避ける」ことの徹底です。とくに、満員電車で通勤するリスクを避けるために、なるべくテレワークで仕事をする慣行が生まれ、「働き方改革」の一環として、今後も定着するとみられます。

テレワークは、自然界のウイルスの感染リスクを減らせる反面、コンピュータウイルスの感染リスクは増大させます。サイバー攻撃は、サプライチェーンやテレワークの“拠点”を狙って多く仕掛けられるからです。

在宅でオンライン会議に出席する場合、セキュリティ対策が十分に施された会社支給のパソコンなどの端末を使わないことがあります。企業は、規模の大小を問わず、業務遂行に欠かせないデータを、ネット流出させずに、適切に管理しなくてはなりません。近時のランサムウェア被害増大をみますと、やはりサイバー攻撃からのデータ防衛に注力すべきでしょう。

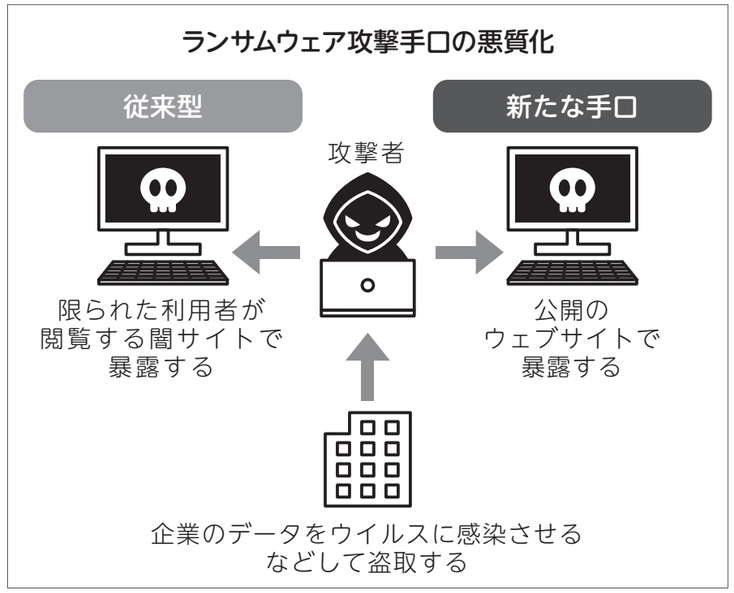
怖いのは、セキュリティの脆弱な端末を通じて会社のシステムに侵入されることです。防御方法には、社内システムのセキュリティ体制を整備・強化し、日頃から、不正アクセスの有無を、その兆候を含めて確認し、攻撃側にスキを見せないことです。

相手は膨大な数に上る標的のうち、“備えの弱い”ところを狙います。国や大企業などとネットワークでつながっていながら、情報管理が甘そうな企業が、なかでも狙われます。

コンピュータウイルスへの感染防止策は、何よりもまず、犯人から狙われないようにすることです。部品メーカーが、大手メーカーA社のネットワークに組み込まれているとします。重要なサプライチェーンの拠点となっている点は、眼をつけられやすいのですが、これを“逆手に取った”感染防止策を講じるべきです。それは、サプライチェーン・ネットワークの中心的大手メーカーA社の高度な「サイバー防衛戦略」の下で、日常的にやるべきことを地道に実践することです。

たとえば、サプライチェーンの、原材料供給者との調達契約は、情報セキュリティデューデリジェンス（事前調査）でしっかりチェックして取り交わすなどです。近時は、取引先になりすまし、「エモネット」というマルウェアで、過去のメール返信を装って感染させる手口も横行しています。社員研修で怪しいメールは開かないようにすることを徹底すべきでしょう。

図1



チェック項目4

ギグワーカー(※1)などとの業務委託契約の締結にあたり、委託先との緊急連絡網整備など、非常事態対策を行っていますか。	Yes / No

ポイント

サイバー攻撃からの防衛策の基本は、「ウイルス保有者」との接触を避け、いつもサイバー環境を“清潔”に保つことです。加えて、注意しても、なお感染が生じ、ネットワークからデータを盗み出される事態に、日頃から備えておくことです。

DX（デジタル・トランスフォーメーション）(※2)を推し進めるなかで、専門の事業者にデータ処理を委託する企業が増えています。ネット経由で単発の仕事を請け負う個人事業主のギグワーカーもいます。

そうした委託先が、委託元にIT機器を持ち込んで作業をするため、そのネットワークとつなぐことも多くなるのですが、機材がウイルスに感染されてないことを必ず確認しなくてはなりません。

万が一同機器を通じて、サーバーに侵入されたと知ったら、直ちに侵入を“ブロック”し“遮断”するなどの善後策をとらなくてはなりません。持ち込み機材は委託先の別会社所有のため、思うように動けない恐れがありますので、そこで、必ず委託先と緊急連絡網をつくっておき、協働して有事対応ができるようにすべきです。

おわりに

身近にできることを着実に行うのがベストの対策です。

これを可能にするのは、何よりも経営陣がこの問題の重要性をよく理解し、社内に意識変革を行き届かせることに尽きます。

（※1）ギグワーカーとは、インターネット上のプラットフォームサービスを介して単発の仕事を請け負う労働者のこと。多くは企業に属さない個人事業主やフリーランスの労働者ですが、企業に雇用されながら副業として取り組む労働者も存在します。

（※2）「DX（デジタルトランスフォーメーション）」とは、企業がAI、IoT、ビッグデータなどのデジタル技術を用いて、業務フローの改善や新たなビジネスモデルの創出だけでなく、レガシーシステムからの脱却や企業風土の変革を実現させることを意味します。

参考URL
・警視庁　令和4年の犯罪情勢について【暫定値】
https://www.npa.go.jp/news/release/2023/20230202001.html