事例で学ぶセキュリティインシデント（第1回）

端末の隔離など的確な対応でランサムウエア感染拡大を防ぐ

2023.06.27

「あれっ、おかしいな。パソコンが動かない。フリーズでもしたのかな」

出社後、パソコンの異変に遭遇したのは、西日本に工場がある自動車部品メーカーA社の設計担当者だ。程なくその理由が分かった。パソコン画面に「ロックを解除してほしければ指定の宛先に暗号資産のビットコインで振り込め」と表示されたからだ。設計担当者はすぐに本社の情報システム担当者に電話をかけて状況を説明した。情報システム担当者はそのパソコン画面を確認しなくても、ランサムウエアに感染したことを理解した。

「対岸の火事」では済まされない―ランサムウエアの感染被害

ランサムウエアはパソコンやサーバーにウイルスを感染させ、端末のロックや、端末内のデータ、ファイルを暗号化して使えなくするサイバー攻撃だ。攻撃者はロックの解除やデータの復号化と引き換えに暗号資産などの金銭を要求することから、身代金要求型ウイルスとも呼ばれる。攻撃者の手口も巧妙化しており、企業・組織の機密データを盗み取った後に暗号化し、身代金を支払わないと機密データをネット上に公開すると脅迫するケースもある。

国内でもランサムウエアの感染被害は後を絶たず、「対岸の火事」とは言っていられない状況だ。医療機関のシステムがランサムウエアに感染し、患者の電子カルテが暗号化され、診療業務に支障を来すといった例も報告されている。

インシデント対応で重要な初動対応

感染状況によっては長期間の業務停滞が余儀なくされ、システム復旧費用の負担のみならず、機密データの漏えいや取引先への感染拡大などのリスクもある。企業はランサムウエア感染の被害者ではなく、意図せずに加害者になる恐れもあるのだ。

ランサムウエアに限ったことではないが、セキュリティインシデント対応では、発生した場合の被害をあらかじめ想定し、被害と影響範囲を最小限に抑えつつ、迅速に復旧、再発を防止する取り組みがポイントになる。

A社は関西に本社を構え、西日本に2カ所の工場がある従業員数80名ほどの企業だ。情報システムやセキュリティの専任部署はなく、本社のITに詳しい技術者が情報システム担当を兼任する。そして、製造現場のシステム化とともにセキュリティ対策にも力を入れてきた。取引先の自動車部品サプライヤーから提供される設計データなどの機密データを取り扱うためだ。サプライヤーからは定期的にセキュリティ対策の報告が求められることもあり、情報漏えい対策には特に配慮してきた経緯がある。

「ついにうちもランサムウエアに感染してしまったのか。感染被害を広げないよう、今すぐ対策を打たなければ」。設計担当者からパソコンがロックされたとの電話連絡を受けた本社の情報システム担当者は、同業他社の情報システム担当者からもランサムウエアが猛威を振るっていることは聞いていたが、想定外の出来事だった。

とはいえ、すぐに初動対応をしなければならない。ランサムウエア感染というインシデント発生の中で、「不幸中の幸い」ともいえるのが、感染被害に気付いたのが早く、初動対応も的確だったことだ。情報セキュリティにかかわるインシデント対応では、発生時の検知と報告、ネットワークの遮断・隔離といった初動対応が重要になる。

まず、情報システム担当者は電話をかけてきた設計担当者にパソコンを社内ネットワークから切り離すように指示。他のパソコンやサーバーに感染被害が広がらないようにするためだ。そして、全従業員に工場のパソコンがランサムウエアに感染したこと、むやみにメールの添付ファイルを開かないこと、メールやSNSに記載されたリンクにアクセスしないことを通知し、注意喚起した。

端末を守る事前対策に加え、検知など事後対策を強化

そして、原因究明に向けて設計担当者に聞き取り調査を実施した。それによると、海外の工作機械メーカーの新製品を案内するメールが届き、メールに記載されたリンクをクリックしてランサムウエアに感染したようだ。A社では従来から知らない相手からの添付ファイルはむやみに開かないように注意していたが、工作機械メーカーの名称が正しかったこともあり、特に気にも留めずリンクにアクセスしてしまったという。

情報システム担当者は上司と一緒に経営層にインシデントを報告。そして攻撃者に身代金を支払うかどうか検討した結果、支払いを拒否することにした。ランサムウエアに感染したパソコンが限定的だったことと、攻撃者に身代金を支払っても、パソコンが復元できるとは限らないからだ。また、支払った場合、攻撃者が味を占めて再び攻撃してくる懸念もあった。

ランサムウエアの復元ツールも提供されているが、A社は情報セキュリティに詳しい人材がいないこともあり、同社のシステムやネットワークの構築・運用を支援してもらっているIT事業者に感染パソコンの復旧と他の端末やサーバーが感染していないどうかの調査を依頼した。パソコン内の設計データなどは社内のファイルサーバーに保存しており、データの復旧はスムーズに進められた。そして、調査の結果、今回の感染は設計担当者のパソコンのみと判明したが、社内ネットワーク上のファイルサーバーなども感染した場合、バックアップデータが暗号化され、復元が難しくなるリスクもある。そこで、オフラインのサーバーにバックアップデータを保管することや、クラウドストレージサービスの活用を検討することになった。

そして、社内のセキュリティ対策を改めて徹底。パソコンとサーバーのOS(基本ソフト)を最新版に更新することや、パソコンなどエンドポイントセキュリティの強化といった事前対策に加え、インシデント発生時の検知や対処、復旧といった事後対策をIT事業者と検討することとした。併せて、従業員に対してはメールやSNSで送られてくるメッセージのリンクを安易に開かないことなどを伝え、セキュリティ意識の向上を図った。A社は自動車部品のサプライチェーンを担う企業として、ランサムウエア感染を教訓にセキュリティの強化とインシデント対応を徹底していく考えだ。