NO.64
2023.04

DDK News Letter

DDK通信

通信・ITネットワークの分野では、日々新しい技術が開発され、より効率的で、より安価なサービスが次々と生み出されています。知らないことは、イコール企業利益の損失です。そこで私たち大和電設工業は、情報通信やITソリューションの『知って得する最新情報』を、お世話になっている皆様に定期的にお伝えしていきます。隔月発刊のDDK通信、ぜひお楽しみください。

ランサムウェアの侵入経路と対策

ランサムウェアは、身代金を意味する「Ransom（ランサム）」と「Software（ソフトウェア）」を組み合わせた造語で、「身代金要求型ウイルス」とも呼ばれます。暗号化することでファイルを利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに金銭（身代金）を要求する特徴があります。警視庁が公表した2022年の犯罪情勢（暫定値）によると、ランサムウェアによる被害は警察が把握しただけでも230件。2021年は146件の被害数だった為、1年で57%増となり被害が急速に拡大しています。今回は、ランサムウェアの侵入経路とその対策を見ていきたいと思います。

感染経路はVPNが最多

侵入経路としては、大きく以下の3つにわけられます。

ランサムウェアの侵入経路

ダウンロード	添付ファイルや メールのURLからダウンロード
送り込み	別のウイルスに感染させ送り込む 「エモテット」
ネットワーク侵入	**「VPN」リモート接続などから 社内ネットワークに侵入**

参考　NHK　https://www.nhk.or.jp/shutoken/newsup/20220302a.html

ダウンロード型は古典的な方法ですが、企業を装ったメールに記載されているURL、興味が湧くようなメールに記載されたURLやファイルのダウンロード等によって感染してしまうケースが依然としてあります。

2021年のランサムウェアによる被害の内、侵入経路として最も多かったのは、VPN（仮想施設網）機器からのネットワーク侵入によるものでした。次いで多かったのが、パソコンを遠隔から操作するリモートデスクトップです。新型コロナウイルス下で広がったテレワーク等の普及を利用して侵入したと考えられるものが、全体の約7割を占めました。

なぜVPNが狙われやすいのか？

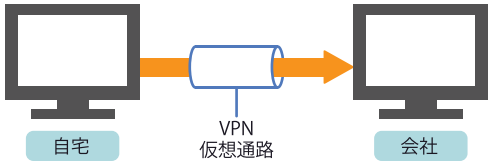
VPNとは、Virtual Private Networkの略でインターネット上に仮想の専用線を構築して通信を行う方法です。

VPN機能付きのルーターなどを自社で設置・設定すれば、専用の回線を構築した際と同じような安全な通信ができるようになります。

しかし、VPNはアクセス元とアクセス先のネットワークが同一になるため、例えばリモートワーク時に自宅のパソコンがウイルス・マルウェア感染してしまった場合に社内のネットワークにも広がってしまう可能性があります。

具体的には、外部からの接続を可能にするネットワーク機器にみつかった脆弱性を悪用したり、接続するための認証情報を何らかの手段で違法に入手したりして、社内のネットワークに侵入し、感染させるケースです。

ネットワーク経由によるランサムウェア対策を講じる必要性が高まっていると言えます。



ランサムウェアへの対策と備え

- ログイン時、生体認証などの多要素認証
- 外部接続は限られた人に絞る
- 機器やソフトのアップデート
- 脆弱性ある機器や認証情報の変更
- 2重3重のデータバックアップ
- 相談先、報告先の周知
- ゼロトラストネットワークアクセス（ZTNA）への移行

社内のVNP機器を、常に脆弱性に対応した最新のソフトウェアに更新しておくことは重要です。また、ランサムウェアに感染してしまった場合、データの復旧はほぼ不可能であると想定しておき、日ごろから二重、三重にデータのバックアップ体制をとっておくことが望ましいです。

新手法としては、VPNが及ぼす悪影響を受けて、それに代わるソリューションが模索されています。それが、ゼロトラストネットワークアクセス（ZTNA）です。ゼロトラストとは、「何も信頼しない」を前提に対策を講じるセキュリティの考え方のことで、例えば、テレワーク時に社外から社内のネットワークにアクセスする際には、毎回端末の安全性を検査し、信用できる場合だけアクセスを認証する方法などがあります。今後は、VPNサービスからZTNAサービスへの移行が進んでいくのではないかと考えられています。