覚えておきたい情報セキュリティ&ネットワークのキホン（第3回）

サイバー攻撃の脅威に対し、企業はどんな情報セキュリティ対策をすればよいのか？

2022.03.25

サイバー攻撃の件数は年々増加しており、自社サービスに関する情報はもちろん、顧客情報や従業員情報といった機密情報が漏えいする危険性が増しています。

企業が情報セキュリティ対策に取り組み、機密情報を悪意ある第三者から守るには、その手口を学ぶ必要があります。相手の手口が分かれば、それに応じた情報セキュリティ対策も採りやすくなります。本記事では、企業が被害を受ける恐れがあるサイバー攻撃の手口を紹介します。

企業が知っておきたいサイバー攻撃の手口

企業を狙ったサイバー攻撃の手口には、主に以下のようなものがあります。

マルウエア

マルウエアとは、malicious（悪意のある）とsoftware（ソフトウエア）を組み合わせた造語で、悪意のあるプログラムやソフトウエアを総称する言葉です。ウイルスやコンピューターウイルスと表現される場合もあります。

マルウエアは、パソコンやスマートフォンなどの端末からソフトウエアに入り込み、プログラムを改ざんして増殖します。その改ざんの過程で機密情報が漏えいする恐れがあるため、未然に侵入を防ぐ必要があります。

ランサムウエア

ランサムウエアはマルウエアの一種で、ransom（身代金）とsoftware（ソフトウエア）を組み合わせた造語です。感染したパソコンやスマートフォンなどの端末をロックして、解除と引き換えに身代金を要求する手口からそう呼ばれています。多くの場合、スパムメールやWebサイトから不正サイトに誘導され、ソフトウエアや端末の脆弱性を利用することで感染します。

業務が行えなくなるからと身代金を支払ったとしても、ロックされた端末が元通りになる保証はありません。むしろ身代金を支払ったという情報が他の攻撃者に連携され、再三にわたり狙われる可能性もあります。近年では端末をロックするだけではなく、身代金の要求が飲めない場合に「ハッキングしたデータを公開する」といった、二重の恐喝を行うランサムウエアも発生しています。

標的型攻撃

標的型攻撃とは、明確な目的を持って個人や企業に対して、スパムメールやハッキングといったサイバー攻撃を仕掛けることです。標的型攻撃の目的としては、対象企業への嫌がらせや情報の奪取・金銭の要求など、多岐にわたります。政府機関などでは、サイバー攻撃の中でも極めて大きな脅威である「高度サイバー攻撃」の1つとされています。

標的型攻撃の特徴は、特定の個人や企業が執拗に狙われる点です。従来のサイバー攻撃はスパムメールや不正なWebサ

イトにアクセスしたあらゆるユーザーを対象にしていました。しかし、標的型攻撃は特定のターゲットにだけ攻撃が継続されるため、ターゲットが抱えるソフトウエアや端末の脆弱性が徐々に見抜かれ、結果的に甚大な被害が発生するケースが多くなっています。

ゼロデイ攻撃

ゼロデイ攻撃とは、メーカーがソフトウエアの脆弱性（不具合や弱点）の修正プログラムを提供する前を狙ったサイバー攻撃です。

通常、脆弱性が発見されると、ソフトウエアを提供するメーカーはその情報を公開するとともに、修正プログラム（パッチ）を提供してユーザーに適用を求めます。しかし、脆弱性の情報は数多くのサイバー攻撃者も調査しているため、メーカーが修正プログラムを提供する前を狙って攻撃を仕掛けることがあります。脆弱性を発見する前にサイバー攻撃が行われた場合、ユーザー側では対策できないという点が特徴です。

ブルート・フォース・アタック

ブルート・フォース・アタックとは、ユーザーのIDやパスワードに対して可能な組み合わせをすべて試して解読するサイバー攻撃です。攻撃者は専用のシステムを利用し、自動で何度も入力を行うことで、いわば「力ずく」でログインします。

昨今、テレワークの普及や業務でのクラウドサービスの利用が広がったこともあり、使い回しのIDやパスワードが解読されて社内のネットワークに侵入されるケースもあります。ブルート・フォース・アタックでは、内部データをロックして金銭を要求するランサムウエアが組み込まれるケースも多く、被害が拡大する可能性があるため注意が必要です。

企業ができる情報セキュリティ対策・取り組みポイント… 続きを読む