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9回）

情報セキュリティのリスクとは？脆弱性を狙う脅威からどう身を守ればよいのか？

2022.03.25

ビジネスを行ううえで、顧客情報などの漏えいや社内データの改ざんといった情報セキュリティリスクへの対策は欠かせません。そのためには、そもそもどういったリスクがあるのか、リスクを避けるにどうすればよいのかを知っておく必要があります。

本記事では、企業が留意すべき情報セキュリティリスクとその対策について紹介します。

情報セキュリティリスクとは

情報セキュリティリスクとは、情報システムやデータの破損、改ざんなどで損害を受けること、あるいは情報漏えいなどでマイナスの影響を受けることを示します。企業活動においては、社会的な信用を失い事業存続に関わる可能性もあるため、情報セキュリティリスクへの適切な対策は不可欠です。

では、情報セキュリティのリスクにはどのようなものがあるのでしょうか。情報セキュリティリスクは、主に「脆弱性」と「脅威」の2つに分けることができます。

情報セキュリティにおける脆弱性とは？

脆弱性とは、インターネットに接続するシステムや端末のプログラム、設計に不具合があることで生じる情報セキュリティ上の弱点を表す言葉です。放置しておくと不正アクセスやウイルスの感染に利用されるリスクがあります。

脆弱性に対応するには、ソフトウエアを常に最新版にしておくことが重要です。Windowsをはじめとするosや各種ソフトウエアには日々新たな脆弱性が発見されており、その脆弱性を修正するためには、ソフトウエアを常に最新版に更新することが脆弱性への対策の基本となるためです。

しかし、該当する脆弱性に対応した後に、新たな脆弱性が発見されることはしばしばあります。近年では、メーカーが脆弱性への修正プログラムを配布する前に、その脆弱性を狙う「ゼロデイ攻撃」という脅威も増加しています。

情報セキュリティにおける脅威とは？

情報セキュリティの「脅威」とは、情報システムやデータに対して、何かしらの危険・被害がもたらされることを示します。情報セキュリティの脅威には「人為的脅威」と「環境的脅威」の2つがあります。

人為的脅威

人為的脅威には、攻撃者が意図的に行う「意図的脅威」と、意図的ではない行動を端に発する「偶発的脅威」の2つが存在

します。

意図的脅威には、サイバー攻撃や、悪意のある従業員による情報漏えいなどの内部不正が含まれます。前者を防ぐには各種情報セキュリティツールの導入、後者を防ぐにはデータを扱える人物の権限設定などが必要です。

偶発的脅威は、アクシデントが原因でデータが破損・紛失した場合などが該当します。メール誤配信などの“うっかりミス”も、偶発的脅威の1つです。偶発的脅威を防ぐには、情報セキュリティに関する運用ルールの定期的見直し、従業員への情報セキュリティ教育の継続的な実施が必要となります。

環境的脅威

環境的脅威とは、例えば落雷によって停電が起きたり、台風によってケーブルが断線したりと、自然災害がもたらす脅威を示します。

環境的脅威を確実に防ぐのは困難です。ただし、「自然災害に遭いにくい地域にオフィスやデータセンターを構える」などは、環境的脅威を低減させるための選択肢といえます。

情報セキュリティリスクへの対策例

情報セキュリティのリスクには、代表的なものとして以下の3点が挙げられます。

情報漏えい

企業はさまざまな機密情報を取り扱っています。従業員のPCの脆弱性を狙われて不正アクセスを受けた場合や、従業員のミスによって端末をどこかに置き忘れた場合、機密情報は漏えいの危機にさらされます。

機密情報が外部に流失してしまうと、自社はもちろん取引先にも被害が及びかねません。情報漏えいを防ぐには、各種情報セキュリティツールの導入と、従業員に対する情報セキュリティ教育の実施が必要です。

サイトの改ざん・機能停止

企業が運営するWebサイトに不正アクセスされると、記載された情報が改ざんされたり、入力フォームや決済機能が停止したりする恐れがあります。

Webサイトの改ざんを防ぐためには、不正アクセスを事前に検知する仕組みが必要です。加えて、Webサイトの管理画面にアクセスできる権限を限定するといった設定も大切です。

マルウエア感染

マルウエアとは、各種システムに入り込んで悪意のある動作を行うようプログラムされたもので、ウイルスやスパイウエアなどもマルウエアの一種です。マルウエアに感染するとシステムの重要な機能が使えなくなり、解除のために金銭を要求される、といったケースもあります。

マルウエアに感染しないためには、情報セキュリティツールの導入、各種システムの最新バージョンへの更新、定期的な脆弱性診断などが求められます。

NTT西日本の関連サービスを紹介

こうした情報セキュリティのリスク対策のために、NTT西日本は「セキュリティおまかせプラン」を提供しています。

セキュリティおまかせプランは、日々進化するサイバー攻撃の脅威に対し、インシデント発生前に行う「事前対策」と、インシデント発生後に対応する「事後対策」の両面をカバーする企業向けの情報セキュリティサポートサービスです。

事前対策

セキュリティおまかせプランが提供する事前対策は、以下の5つです。

ゲートウェイセキュリティ（UTM）

IT機器とインターネット環境の間にゲートウェイセキュリティ（UTM）を設置し、ウイルスメールや不正通信など外部からの脅威を事前にブロックします。

エンドポイントセキュリティ
PCやスマートフォン、タブレット端末などにエンドポイントでの情報セキュリティツールを導入することで、外部脅威を検知します。

クラウドプロキシ
クラウド上にプロキシサーバーを用意し、従業員が悪意のあるWebサイトへアクセスしないようにブロックします。

セキュリティスイッチ機能
社内ネットワークの脆弱性を狙って進入したマルウエアの攻撃を検知・ブロックし、感染拡大を防止します。

標的型攻撃メール訓練機能
従業員教育として、標的型攻撃メールの模擬訓練を実施。従業員の情報セキュリティ意識向上を推進します。

事後対策

セキュリティおまかせプランで提供される事後対策は、以下の2つです。

通信監視・復旧支援
不正な通信やウイルスによる攻撃を監視し、インシデント発生時は電話やメールで状況を知らせます。通信監視状況は月次レポートで報告されます。

訪問サポート（オプション）
インシデントが発生し、PCやタブレットの初期化あるいは復旧が必要となる場合は、最寄りの保守拠点からオフィスに駆け付けてサポートします。

まとめ

企業がビジネスを続けるうえで、顧客データや取引先情報といった機密データの取り扱いは必要不可欠です。しかし、サイバー攻撃などで情報が漏えいした場合、大きな損失を被ることになります。とはいえ、すべての情報セキュリティ対策に自社で対応するのは難しいもの。本記事で紹介した「セキュリティおまかせプラン」など、外部パートナーの知見も活用しながら対策を講じておきましょう。

※掲載している情報は、記事執筆時点のものです