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… 続きを読む