



「盗まれるデータはない」と思い込んでいる 企業が見落としがちな“あれ”とは

セキュリティ対策にはさまざまな誤解や過信がある。「盗まれるようなデータはない」という考えもその一つ。対策をアウトソーシングする際の責任範囲も誤解が多い。では、こういった心構えや対策が必要になるのか、そのポイントは。

「盗まれるデータはない」と思い込む企業は“あれ”を見落としていないか？

セキュリティ対策を巡るさまざまな誤解がある。自社のデータが攻撃者にとって魅力的なものではないと考えてしまうこともその一つだ。全ての組織が講じなければならないデータ保護策とは何か。

「盗まれるようなものは何もない」

自社のデータの価値を過小評価し、攻撃者に狙われるようなことはない考える企業がある。しかしこれは誤解だ。どのような企業でも、顧客情報や従業員の個人情報、財務情報など、攻撃者にとって魅力的になり得る情報を扱っている。データの価値とは別に、コンプライアンス（法令順守）の観点からもデータ保護策を講じることは欠かせない。

実例

バーミンガムの小規模物流会社は攻撃を受け、顧客の配送情報が盗まれた。攻撃者はこの情報をダーク Web（通常的手段ではアクセスできない Web サイト群）で販売。詐欺事件が発生し、会社の信頼は失われた。

対策

- データのインベントリ化
 - ・ 企業が扱っている全てのデータを棚卸しし、重要度に応じて適切な保護措置を講じる。
- アクセス制御
 - ・ 機密データへのアクセスを、業務に必要な従業員に限定する。

「ITアウトソーシングなら安全」は幻想？ 法律事務所がはまった“わな”とは

自社に十分な人的リソースがないために、IT 運用を第三者にアウトソーシングする組織は少なくない。その際に注意しなければならないのは、セキュリティの責任範囲だ。IT 運用をアウトソーシングすることで、セキュリティ確保の全て責任も任ってもらえると考えるのは誤解だ。第三者の力を借りつつセキュリティを確保するためのポイントは何か。

「IT をアウトソーシングしているから安全」

IT のアウトソーシングは業務効率の向上をはじめとしたさまざまなメリットをユーザー組織にもたらす。だがアウトソーシングをする場合も、セキュリティの責任はあくまでユーザー組織側にある。IT のアウトソーシングを決める前、MSP（マネージドサービスプロバイダー）や MSSP（マネージドセキュリティサービスプロバイダー）が提供するサービスの責任範囲を念入りに確認しよう。クラウドストレージに重要なデータを保存する場合も、同様の確認が必要だ。

実例

リーズの小規模法律事務所は、システム管理を外部の IT サービスプロバイダーに委託していたが、セキュリティの責任範囲を明確には確認していなかった。その結果、ソフトウェアのパッチ（修正プログラム）が未適用であることが原因で、システムがマルウェアに感染して停止した。復旧に多額の費用を要したという。

対策

- 責任範囲の明確化
 - ・システム管理に関わっている全ての第三者に対し、セキュリティの範囲を詳細に把握する。
- 監査の実施
 - ・セキュリティの実施状況について認識に相違がないかどうかを確認するために、セキュリティ対策を定期的に評価する。

セキュリティを強化するには

以下では、規模や予算を問わず、全ての組織が実行できる基本的なセキュリティ対策を紹介しよう。

- 多要素認証（MFA）
 - ・ 認証情報が流出しても不正アクセスを防げるように、業務用アカウントのログインに MFA を導入する。
- 定期的なアップデートとパッチ適用
 - ・ 攻撃者に悪用される脆弱（ぜいじゃく）性を減らすために、システムを常に最新の状態に更新する。
- セキュリティ意識向上のトレーニング
 - ・ フィッシングメールの不審なリンクをクリックしないよう、脅威を認識するためのトレーニングを従業員に提供する。
- パスワードマネジャーの利用
 - ・ アカウントごとに異なる強固なパスワードを設定し、パスワードマネジャー（パスワード管理ツール）で安全に管理する。
- 定期的なバックアップ
 - ・ 重要なデータを定期的にバックアップし、バックアップシステムの信頼性を定期的に検証する。
- ネットワークセグメンテーション
 - ・ 機密データを取り扱う重要なシステムを安全性の低いネットワークから分離し、侵害時の影響を最小限に抑える。

セキュリティに関する誤解や思い込みは油断につながり、ユーザー組織を重大なリスクにさらす可能性がある。誤った認識を修正し、自社のセキュリティ戦略を確立することで、巧妙化する脅威に対処しよう。被害発生後の復旧コストと比較すれば、事前にセキュリティ対策の強化を図ることははるかに安価だろう。