セキュリティ

ITマネジメント（内部統制）

リスクの高いシャドー IT を把握

外部からのアクセスを安全なデバイスのみに限定するには

スマートフォンやタブレットといったスマートデバイスの進化によって、個人が持つデバイスでも業務が可能になりました。これは業務効率を向上させるという意味では効果的ですが、一方で大きなリスクも伴います。その1つが、個人用のデバイスを社内ネットワークに接続するリスクです。また、業務用のファイルなどがコピーされた個人用のデバイスが紛失や盗難に遭うというリスクも存在します。ここでは、個人用のデバイスを社内ネットワークに接続するリスクと、それにまつわる課題を解決するNTT Comのソリューションについて解説します。

個人用のデバイスが社内に入り込むリスク

最近のスマートデバイスは、PCの代わりに業務が行えるほど高性能、高機能になっています。また、クラウドサービスの多様化と信頼性の向上、Wi-Fiネットワークの充実により、場所を選ばず業務を行えるようになりました。スマートデバイスやノートPCで業務を行えるようになれば効率は上がりますが、一方で企業が把握していないデバイスが社内ネットワークに接続されたり、業務用のファイルなどが持ち出されたりする「シャドー IT」のリスクも顕在化します。

シャドー ITとは、従業員個人が持ち込む企業が把握していないIT機器のことです。これを放置しておくと、社内にある重要なファイルがシャドー ITにコピーされたり、不正なプログラムが社内に入り込んだりするリスクがありますし、紛失や盗難によって重要なファイルが第三者の手に渡ってしまう可能性もあります。さらに、物理的に社内に持ち込まれなくても、クラウドサービス経由で社内のファイルにアクセスすることもできます。

実際、システム担当のスタッフが個人用のデバイスを充電しようと社内のPCに接続したところ、外部ストレージとして認識。それが悪心の引き金となり、業務用のファイルをコピーし、社外へ持ち出した事例がありました。

シャドー IT を把握するためには

シャドー IT対策を行う際には、まず自社にあるIT機器の棚卸しを行い、その利用状況を把握します。また社内ネットワークには、接続されるデバイスを監視する仕組みや、把握していないデバイスからのアクセスを検知する仕組みを構築します。こうした対策としては自社にあるIT機器を自動的に検出して把握できる、IT資産管理システムが有効です。例えばNTT Comが提供する「WideAngle マネージドセキュリティサービス」では、ネットワーク監視やUTM(統合脅威管理)などが用意されているので、これらで検知することが可能です。

IT資産管理システムやネットワーク監視、UTMなどでシャドー ITを検知したら、利用を許可するかどうかを判断し、許可する場合にはデバイスの保護を行います。デバイスの保護には、統合セキュリティ対策が効果的です。NTT Comの「マイセキュア ビジネス」なら、新種のマルウェアやランサムウェアにも対応。高い検出率を誇る上、安全か危険かを判定できないものについては、一挙一動を継続監視(ふるまい監視)します。その後、怪しいふるまいを検出すると即座にブロックし、ファイルを元の状態に戻します(ロールバック)。

「マイセキュア ビジネス」では、Webベースの管理コンソールから端末(PC)の集中管理ができます。この際にポリシー管理を行うことで、不正利用の制限も可能です。また端末が紛失・盗難などにあった際には、位置情報の取得やリモートロックが行えます。さらに、定義ファイルがクラウド上にあるので、バージョン管理や端末へのファイル配布が不要であることもポイントです。

業務に不要なソフトウェアも「シャドーIT」の1つ

シャドー ITは、ハードウェアだけとは限りません。従業員が勝手にインストールするソフトウェアも、企業が把握していないIT資産になります。その多くはフリーウェアであるため、信頼性が十分に担保されていない可能性が高く、システムに悪影響を及ぼしたり、不要な動作を行ったりするおそれがあります。また、便利なツールのふりをした悪意あるソフトウェアも存在しますので、従業員が会社の許可なくソフトウェアをPCにインストールすることがないよう、しっかり管理することが重要です。

最近、無料のファイル共有サービスで大規模な情報漏えいが発生し話題になりましたが、このようなサービスは、容量が大きすぎてメールに添付できないファイルを手軽に送る手段として重宝されていました。このサービスは個人・企業を問わず広く利用されていたので、提供が中止された現在、他のサービスを利用している人も多いと思われます。しかし、便利な機能をうたうサービスやフリーウェアが実は悪意のあるものであることも少なくなく、従業員にこうしたサービスを自由に使わせていては、セキュリティのリスクを招きかねません。企業は業務で利用できるソフトウェアを信頼の持てるものに統一し、不要なサービスやソフトウェアによるインシデントを防ぐべきです。

例えば、ファイルの保存や共有、転送などの機能を持つNTT Comの「Box over VPN」は、信頼と実績のあるファイル共有サービス「Box」とVPNを組み合わせたサービスです。ストレージの容量が無制限なので、新たにファイルサーバーを構築することなく大容量のストレージを利用でき、検索にも対応します。社内での共有はもちろん、ファイル共有サービスのような使い方も安全に行えます。ファイルは常に暗号化されているので安全ですし、多くの世界的なセキュリティ基準も満たしています。

このように、シャドー IT対策にはさまざまな手法があります。自社に合った対策を行い、外部環境からのアクセスにおける安全性を高めていきたいものです。

関連サービス

WideAngle マネージドセキュリティサービス NWセキュリティ	ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。 セキュリティ運用基盤(SIEM)とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。
マイセキュア ビジネス	標的型ウイルスなどの新たな脅威からPC、スマホなどを守る超高速・超軽量の次世代型エンドポイントセキュリティサービス。Webベースの管理コンソールひとつで、すべてのエンドポイント端末の集中管理が可能なため、働き方改革のセキュリティ対策を強化できます。
Box over VPN	社内・取引先とのファイル共有や、Salesforceなどの業務アプリケーションとのシームレス連携を可能にする“コンテンツ・マネジメント・プラットフォーム”です。 ファイルの保管時にAES256bitでファイルを暗号化。ISO27001と27018という世界標準の情報セキュリティマネジメントシステムに準拠しています。
Global Management One	ICT環境の監視、運用並びに最適化業務をワンストップで行うリモート・インフラストラクチャ・マネジメントサービスです。ITILのベストプラクティスにもとづき、高度な運用プラットフォームや幅広いスキルを持ったサービスマネージャーとサービスデスクによって、お客さまのICT環境の個別のニーズに即したサービスを提供し、ITシステムの投資対効果の向上に貢献します。