セキュリティ

ITマネジメント（内部統制）

“ひとり情シス”の環境には要注意！

修正パッチやアップデートを放置した際の多大なリスク

企業で使用するPCやサーバーでは、OSに加え複数のアプリケーションが動作しています。これらのOSやアプリケーションにはしばしば脆弱性が発見され、修正パッチやアップデートが提供されます。しかし、パッチやアップデートを適用するためには多くの作業工数をこなさなくてはならず、特に担当者がひとりだけの“ひとり情シス”の環境では、手が回らずに脆弱性を放置したままということも。そこで今回は、修正パッチやアップデートを適用しないことにより生まれるリスクについて解説します。

ソフトウェアで発見される脆弱性とは

マルウェア感染や不正アクセスによる情報漏えい事件がしばしばニュースとなりますが、その原因はソフトウェアの脆弱性にあることが少なくありません。脆弱性はセキュリティホールとも呼ばれ、ソフトウェアで発見される不具合のことです。脆弱性にはさまざまな種類があり、日本では米国の非営利団体MITRE社が規定した脆弱性の分類を使用しています。

脆弱性は、例えば非常に多い文字数を入力するなど、想定されていなかった操作を行うことで現れることがあります。これをサイバー攻撃者が悪用することで、マルウェアへの感染やシステム内に侵入されるなどして、結果的に情報漏えいやシステムの停止といった被害を招きます。脆弱性の悪用はサイバー攻撃を行う上で非常に有効であるため、サイバー攻撃者は常に脆弱性を探しているのです。

ソフトウェアの開発者やサイバーセキュリティの研究者も、そうした脆弱性を突かれないよう、日々調査を行っています。脆弱性が発見された場合には、それを修正するためのパッチやアップデートを用意し、情報を公開します。しかしサイバー攻撃者は、公開された脆弱性情報をもとに、その脆弱性を悪用するためのコード（エクスプロイトコード）を用いてサイバー攻撃に使うために、パッチやアップデートを適用していない場合は標的にされてしまうのです。

サイバー攻撃者がエクスプロイトコードを作成するまでの時間は日を追うごとに短くなっており、脆弱性の情報が公開されたその日のうちにサイバー攻撃が行われることもあります。それゆえ、ユーザーは一刻も早くパッチやアップデートを適用する必要があります。なお、ソフトウェアの開発元が脆弱性に気付く、あるいは修正パッチやアップデートを提供する前に、その脆弱性を悪用したサイバー攻撃が行われることもあり、これを「ゼロデイ攻撃」と呼びます。

修正パッチやアップデートの適用が困難な環境も

個人ユーザーの場合は、比較的容易に修正パッチやアップデートを適用できますが、企業の場合は単純ではありません。企業のシステム上では複数のソフトウェアが動作しており、1つのソフトウェアに修正を適用することで、別のソフトウェアに悪影響を及ぼすことがあるからです。最悪の場合、システム全体が停止してしまい、ビジネスや業務に多大な影響が出てしまう可能性もあります。また、適用の際にシステムの再起動を伴う場合もあり、この際には入念な準備が必要です。

こうした理由から、適用の前にはあらかじめテスト環境で影響を確認しておくべきですが、多くの作業工数がかかるため、システム担当者が少ない、あるいは専任のセキュリティ担当者がおらず、別部署の人間が兼任で“ひとり情シス”をやっているような環境では、なかなか適用できないという事情があります。その結果、脆弱性が放置されてしまい、マルウェア感染や不正アクセスを受けやすくなってしまうのです。

また、ソフトウェアには一般的にサポート期間が設定されています。例えば、マイクロソフトが提供しているOS「Windows 7」と「Windows Server 2008」は、2020年1月14日にサポート終了となります。これを「EoS（End of Support）」と呼びますが、EoS後はたとえ重大な脆弱性が発見されても修正パッチやアップデートが提供されなくなるため、マルウェア感染や不正アクセスを受けるリスクが急激に高まります。そのようなリスクを未然に防ぐため、OSなどの重要なソフトウェアについては、ユーザー側でサポート期間をきちんと把握しておきましょう。

修正パッチやアップデートを適用できない場合の対策

修正パッチやアップデートを確実に適用していくためには、社内で使っているソフトウェアを棚卸し、リストを作成し、かつそれぞれのバージョンも記載しておきます。そして、新たなパッチやアップデートが提供されたときには、各ソフトウェアに適用するタイミングを計画し、あらかじめテスト環境で検証するなどの準備を進めていきます。「バージョン管理」や「パッチマネジメント」と呼ばれる作業です。

それでも、場合によっては修正パッチやアップデートをすぐに適用することは難しいというケースもあるでしょう。その場合の対策としては、まず「脆弱性診断」で自社のシステムにどのような脆弱性が存在するかをチェックします。そして、「WAF（Webアプリケーションファイアウォール）」や「UTM（統合脅威管理）」、脆弱性保護機能のある次世代ファイアウォールや次世代IPSなどを導入します。

こうした製品では、脆弱性を解消するのではなく、その脆弱性を悪用しようとする攻撃を阻止することで、パッチやアップデートを適用するのと同じ効果を実現します。この機能は「仮想パッチ」などと呼ばれており、脆弱性を悪用しようとする攻撃をブロックしている間に、余裕をもって正式な修正パッチやアップデートの適用を行うことが可能になります。現在では、サイバー攻撃のほとんどが脆弱性の悪用をきっかけとして発生しています。例えば、2017年5月に世界規模で被害を出したランサムウェア「WannaCry」は、Windowsの脆弱性を悪用していました。この脆弱性を修正するためのパッチは同年3月に提供されており、これを適用していればWannaCryに感染も防げたでしょう。リソースに余裕のない“ひとり情シス”の企業こそ、WAFなどによる「仮想パッチ」での対策が効果的でしょう。

関連サービス

Managed Firewall	Enterprise Cloud 2.0 のテナント内で利用することができるファイアウォール機能です。グローバルレベルのセキュリティ運用体制を持つセキュリティオペレーションセンター(SOC)から、本メニューの運用監視を行います。
Managed UTM	Enterprise Cloud 2.0 のテナント内で利用することができる統合的なセキュリティ機能(ファイアウォール機能を含む)です。不正アクセス、ウイルス感染、不要なWebアクセス、スパムメールなど、様々なセキュリティ脅威からお客さま環境を守る為に必要なセキュリティ機能をオールインワンで提供します。
Managed WAF	Enterprise Cloud 2.0 のテナント内で利用することができ、Webアプリケーションサーバーに対する不正アクセスや攻撃通信などのセキュリティ脅威を検知/防御する機能です。脆弱性を突いた攻撃通信、不正アクセス、ウイルス感染など、様々なセキュリティ脅威からお客さまのWebアプリケーションサーバーを守る為に必要なセキュリティ機能をオールインワンで提供します。
WideAngle マネージドセキュリティサービス	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが、ICT環境を24時間365日サポート。高度なセキュリティ監視により、実在するリスクと潜在リスクを可視化します。 また、「NWセキュリティ」をはじめとするセキュリティ対策パックメニューや、「リアルタイムマルウェア検知」などの機能をご用意、様々なご要望に応じて総合的なセキュリティソリューションを提供します。