セキュリティ

ITマネジメント（内部統制）

修正パッチの管理はサーバセキュリティの盲点

Webサイトからの情報漏えいを引き起こさないために

昨今、Webサイトからの情報漏えい事件・事故が増えていますが、その多くはWebアプリケーションの脆弱性を悪用されたものです。こうした脆弱性が発見されると、開発元などから修正パッチなどが提供されますが、Webサイトでは複数のWebアプリケーションが動作しているため、パッチを適用すると他のアプリケーションに悪影響が出てしまうことがあります。また、企業によっては人的リソースの不足が原因で、対応が遅れてしまうケースも散見されます。本記事では、Webサイトの脆弱性の把握や対策についていかに運用していけばよいのかを、ご紹介していきます。

情報漏えいを招きかねないWebサイトの脆弱性

映画、音楽、ゲーム、本屋、企業、自治体、学校など、インターネットにはさまざまなWebサイトがあり、1つの仮想世界を形作っています。その世界で身分証明書の代わりになるのが、クレジットカードです。企業が保有するECサイトや金融系サービス、会員サイトなどの膨大なカード情報は、サイバー攻撃者にとってお金を生む絶好のターゲットとなります。

サイバー攻撃者がこうした情報を盗み取る場合には、Webアプリケーションの脆弱性を悪用するケースが一般的です。ユーザーやクレジットカードの情報を扱うWebサイトでは、その背後にデータベースサーバーがあり、そこで情報を保存しています。本来、データベースの情報はしっかりと保護されていますが、クレジットカード情報を一時的に自社サーバーに残すケースでWebアプリケーションに脆弱性があると、そこを突かれて外部から不正アクセスされてしまうことがあります。

実際、Webアプリケーションのフレームワークである「Apache Struts 2」に脆弱性が発見されたときは、この脆弱性を悪用するサイバー攻撃が多発し、多くの情報漏えいが引き起こされました。また、世界的に被害が拡大したランサムウェア「WannaCry」も、Windowsの脆弱性を悪用して感染を広げました。このようにWebアプリケーションやOS、ソフトウェアの脆弱性を突いた多種多様なサイバー攻撃が日々生まれているのです。

脆弱性とはソフトウェアの不具合のことで、セキュリティホールとも呼ばれます。脆弱性が発見されると、開発元が脆弱性を解消するために修正パッチやアップデートを開発・提供します。脆弱性にもさまざまな種類がありますが、情報漏えいにつながるような重大なものについては、各省庁などによる公的団体やセキュリティベンダなどによる業界団体からも注意喚起が行われます。サイバー攻撃者は、こうした情報が公開されると同時にその内容を検証し、攻撃するためのエクスプロイトコードを開発。早ければ同日中に攻撃を実施します。このため、修正パッチやアップデートは、重大な脆弱性ほど迅速に適用する必要があるのです。

第一歩は自社のWebサイトの脆弱性の確認から

脆弱性は修正パッチやアップデートを適用することで解消されます。しかし、一般的にWebサイト(Webサーバー)は複数のWebアプリケーションで構成されており、またアドオンやプラグインを使用しているケースも少なくありません。これらは複雑に影響し合っているため、1つのアプリケーションにパッチやアップデートを適用することで、別のアプリケーションに影響が及ぶ可能性もあります。最悪の場合はWebサイトが停止してしまうので、適用する前に十分に検証を行う必要があります。

しかしながら、企業によっては人材不足などによって十分な検証を実施できないのが現状でしょう。そもそも、どのアプリケーションに脆弱性が存在しているのかを把握することさえ難しい場合もあると思われます。このようなときは、まず自社のWebサイトに脆弱性が存在するかどうかをチェックしましょう。例えば、NTT Comが提供している「WideAngle マネージドセキュリティサービス」の脆弱性診断を利用すれば、脆弱性の有無を確認できます。もし存在する場合は、どのような種類の脆弱性かまで判明するので、優先度をつけて対処することが可能です。

「仮想パッチ」で迅速な脆弱性対応を

脆弱性対策には、自社のWebサイトにどのようなWebアプリケーションが動作しており、どのようなアドオンやプラグインが導入されているのかを正確に把握。それぞれのバージョンを明らかにすることが重要になります。これを「バージョン管理」や「パッチマネジメント」と呼びます。いわばWebアプリケーションにおける「棚卸し」です。

そして修正パッチやアップデートの適用がすぐにはできない場合は、「仮想パッチ」を当てる方法が効果的でしょう。仮想パッチは、脆弱性に対して正式なパッチを適用するのではなく、その脆弱性を悪用しようとする攻撃を検知し、ブロックする仕組みです。サイバー攻撃者は、脆弱性を悪用するためにエクスプロイトコードと呼ばれるコード(命令文)を作成し、送りつけてきます。仮想パッチはあらかじめエクスプロイトコードの情報を持っているので、攻撃を検知できるわけです。

仮想パッチを適用することで、脆弱性が存在している状態でも攻撃を防ぐことができるので、修正パッチやアップデートを適用したことと同様の効果が期待できます。こうして攻撃を防いでいる間に、適用の影響などの検証を行うのです。特にアップデートの場合は、脆弱性の解消だけでなく、新しい機能の追加や新しい技術への対応なども行う必要があるので、より効果的といえましょう。

具体的なサービスとしては、例えばNTT Comが提供する「Enterprise Cloud 2.0 ホスト型セキュリティ」が挙げられます。このサービスには、ウイルス対策の「Managed Anti-Virus」、侵入防御やファイアウォールの「Managed Virtual Patch」、そしてWebレピュテーションや変更監視、セキュリティログ監視も行う「Managed Host-based Security Package」が用意されています。「Managed Virtual Patch」では、NTT Comがユーザー環境の脆弱性に対する仮想パッチを作成、提供。ユーザーの手を煩わすことなく脆弱性に対応し、安全な環境を維持します。

仮想パッチ機能は、同じくNTT Comが提供している「WideAngle マネージドセキュリティサービス」にも用意されています。WAFや次世代ファイアウォール、次世代IPSといったセキュリティ機能で仮想パッチに対応。しかも、これらの機器の運用はNTT Comが行い、サイバー攻撃を検知したときにはユーザーへアラートを送り、最適な対処法などを提案します。企業はセキュリティ対策機器の監視や運用にリソースを割くことなく、自社のセキュリティレベルを飛躍的に向上できるのです。

豊富なノウハウを持つNTT Comに運用を任せることで、最新の攻撃手法に対応したセキュリティを維持することができ、リソースをより生産的な業務へ振り向けることも可能になります。Webサイトを安全・安心に運用していくためにも、こうしたマネージドセキュリティサービス(MSS)の利用を検討してみてはいかがでしょうか。

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。