GRED（グレッド）Web 改ざんチェック

導入事例

HITACHI
Inspire the Next

株式会社サイバーエージェント様

Web 改ざん対策と同時に WAF を導入
改ざんチェック＋攻撃ブロックでリスク低減を狙う

株式会社サイバーエージェント　全社システム本部　西村将嗣様

導入企業
株式会社サイバーエージェント
設立：1998 年 3 月
資本金：7,203 百万円（2015 年 6 月末現在）
従業員数：3,059 名 (連結 2014 年 9 月末現在）
本社：東京都渋谷区道玄坂一丁目 12 番 1 号
事業内容：
Ameba 事業、インターネット広告事業、ゲーム事業、
メディアその他事業、投資育成事業

インターネット総合サービス企業である、株式会社サイバーエージェント（以下、サイバーエージェント）は、2014 年 7 月に、SaaS 型 Web 改ざんチェックサービス「GRED（グレッド）Web 改ざんチェック」を、自社コーポレートサイトに導入した。大手企業の Web サイトが改ざん被害に遭い、被害を受けたユーザー側からは「加害者」となる報道も多いなかで、未然に Web サイト改ざんによる被害を防ぐのが、その目的。以前から利用していた改ざん検知サービスに変えて、GRED へ変更した理由などを伺った。

国内有数の規模を誇るユーザー数
情報漏えい対策は喫緊の課題

1998 年に創業し、インターネット広告代理店の草分けとして、メルマガ、ブログ、アドテクノロジーと、変化の著しいインターネット業界の最先端を走り続けるサイバーエージェント。コーポレートサイトには、リスク情報の一つとして「情報セキュリティに係るリスク」を明示するなど、意識的な Web セキュリティの取り組みを具体的に行っている企業だ。採用面でも、セキュリティエンジニアの採用を積極的に行い、Web サイトばかりでなく、アプリケーションや社内システムに対してもセキュリティの強化を進めている。

個人情報の扱いについては、昨今の改ざん被害や情報漏えい被害の広がりに伴い、同社でも対策を強化しているという。その理由の一つには、多数のユーザー数を抱えていることが挙げられる。会員数 4,000 万人を超える Ameba 事業、国内有数のユーザーを抱えるゲーム事業など、同社の Web サービスのユーザー数は、いずれも非常に大きな規模を誇る。さらに、採用応募者に関する個人データも、学生をはじめとして数万人以上の規模に上っている。

これらの、数多くのユーザー情報、そして個人情報を扱っている会社として、全社的に改ざん等へのリスクを重要視しており、その重要度合いは年々高まっているという。「テレビのニュースなどでも、企業のサイト改ざん被害が報道され、またそれがネット上の話題になることも多くなりましたから、人ごとではないとの気持ちは強かったですね」と全社システム本部の西村氏は語る。

CMS のぜい弱性は避けられない
GRED で改ざん被害の予防を狙う

サイバーエージェントが展開する、数多くのサービスが抱える個人情報、採用応募者情報、さらに社員の個人情報を対象とした情報漏えいリスク、加えてサイト改ざんのリスク低減は、喫緊の課題だ。その対策として、コーポレートサイトのリニューアルを機に、改ざんチェックサービス GRED Web 改ざんチェックを導入した。クラウド型 WAF「Scutum」も導入し、WAF による攻撃ブロックと改ざんチェックを行っている。静的なコーポレートサイトに GRED によるチェックを導入した最大の理由は、CMS が抱えるぜい弱性だ。

「コーポレートサイトのコンテンツ管理では CMS を利用しています。
ユーザーの多い WordPress ほどではないにせよ、CMS を使っている以上、CMS に起因するぜい弱性は避けられないものだと考えています。弊社の話題がテレビに取り上げられ、急激にアクセスが集まることもあり、閲覧者へ改ざん被害を与える可能性を極力低め、未然に防ぎたいとの考えから採用しました」。西村氏は、GRED 導入の経緯をこのように振り返った。

「慣れ」による見過ごしを防ぐ アラートの仕様が選定の決め手に

GRED を導入する以前から、改ざん検知は行っていたものの、より信頼度の高い改ざん検知運用を求めていたときに、Scutum を運営するセキュアスカイ・テクノロジーから紹介されたのが GRED だった。GRED が選ばれた理由には、検知の信頼性以外に、どのような点があったのだろうか。

西村氏は次のように語る。「改ざん検知のアラート仕様が、我々の考えるイメージ通りだったことが挙げられます。比較した他のサービスでは、更新のアクションをトリガーとしてアラートメールが送られる仕組みだったのです。この仕様だと、複数のユーザーが手分けをしながら CMS で更新する運用の場合、小さな更新でも逐一アラートが届くことになります。正常な更新のたびにアラートが出ると、チェックする側もアラートに慣れてしまい、そのうち無視するようになるのをいちばん恐れていました。GRED では、悪意のある更新や改ざんが検知されたときにだけアラートメールが送られる仕様だったので、アラートが来たときには緊急対応するとの運用が可能でした」。

運用時の「慣れ」によるヒューマンエラー対策に加えて、価格と SaaS 型サービスならではの導入障壁の少なさも、ポイントだったという。

サイバーエージェントのコーポレートサイトのページ数は、1 万 5,000～2 万程度。コーポレートサイトのなかではページ数の多い部類といえるだろう。その多くはプレスリリースのアーカイブだ。GRED の標準サービスでは 1,000 ページがチェック対象となっているが、西村氏の見解は次のようなものだった。

「ウイルス配布等の改ざん目的であれば、アクセス数の多いページが狙われやすいはずです。そこで、アクセス数が多いと思われる URL をチェック対象として、改ざん検知ができればいいと考えています」。

さまざまな観点からセキュリティリスクの低減を目ざす

Web 技術の進歩に伴い、今後も新たなセキュリティ課題が発生することは避けられない。その対策を西村氏は次のように語る。「改ざんチェックと WAF を使って、外部からのサイバー攻撃には一定の防御策を講じられたが、より高度な、悪意のある侵入が発生する可能性も踏まえて、対策のバージョンアップも行わなくてはなりません。
今後は、人間を介しての管理情報漏えいや、それに伴うアカウント乗っ取り、そして社内ネットワークの内側からの攻撃対策が課題と考えています」。
さまざまな観点からセキュリティリスクの低減を目ざしている、サイバーエージェントの着実な取り組みは、今後も注目を集めることだろう。

※本導入事例の記載内容は、2015 年 7 月現在のものです。

株式会社 日立システムズ　本社: 〒141-8672 東京都品川区大崎1-2-1　www.hitachi-systems.com
お問い合わせは

2024.06
Printed In Japan