Fastly + 株式会社ぐるなび

Next-Gen WAF の導入でサイトへのアタック状況を可視化 シンプルな設定により セキュリティ対策の運用負荷を軽減

飲食店が必要とするすべてのサービスを提供することを目的に、「飲食店のサポーター」として 1996 年に事業を開始した株式会社ぐるなび（以下、ぐるなび）。飲食店検索サービスの先駆者として、インターネットやモバイルの飛躍的な進化とともに事業を拡大してきた同社では、ウェブアプリケーションの脆弱性を悪用する攻撃から事業の中核である飲食店情報サイト「楽天ぐるなび」を保護するための統合型セキュリティソリューションとして Fastly Next-Gen WAF（以下、Next-Gen WAF）を採用している。

社名:株式会社ぐるなび

1996 年に飲食店情報サイト「ぐるなび」を開設。詳細なメニュー情報などを事前に確認して飲食店に行くという外食のスタイルを定着させた。現在「「食でつなぐ。人を満たす。」という PURPOSE（存在意義）のもと、「飲食店 DX のベストパートナー」として、さらなるサービスの拡充を図っている。2023 年 10 月にはサイト名称を「楽天ぐるなび」に変更し、楽天会員向けの機能を強化するなど、ユーザー・飲食店双方にとってメリットとなる新たな価値を提供し、サイトの利用価値を高めている。

住所:〒100-0006 東京都千代田区有楽町 1-1-2
日比谷三井タワー 11F

URL:https://corporate.gnavi.co.jp/

専任の SOC エンジニアがいなくても 作業負荷を軽減できる運用性を評価

ぐるなびでは、日本全国 4 万 2,150 店舗（総有料加盟店舗数 / 2024 年 3 月時点）の飲食店情報を掲載し、月間ユニークユーザー（UU）数 3,200 万人（2023 年 12 月時点）が検索 / 予約で利用する日本最大級の飲食店情報サイト「楽天ぐるなび」をはじめ、飲食店向けモバイルオーダーサービスの「ぐるなびFineOrder（ファインオーダー）」など、飲食店向けの各種業務支援サービスを展開している。

現在、「食」の総合サービス企業としてのポートフォリオをさらに拡充させることを目的に、「食」に関わるあらゆる人とビジネスをつなぐプラットフォーマーへと進化するための取り組みを推進。飲食店の生産性向上に直結する「集客活動」、および「店舗運営」の 2 つの DX にフォーカスし、「飲食店 DX のベストパートナー」になるための施策に取り組んでいる。

施策の 1 つとして、システムに関わるセキュリティリスクへの取り組みを推進。開発部門 開発部 Infrastructure Service セクション 副セクション長の対馬祐治氏は、「これまでWebアプリケーション診断など脆弱性対策を行っている一方でセキュリティを更に補助する一手段として WAF を検討していましたが、他社製品では誤検知が多いことや運用に専任の SOC（Security Operations Center）エンジニアが必要となることが課題でした」と話す。

WAF の導入プロジェクトは、2022 年秋ごろより検討を開始。いくつかの WAF 製品の比較検討を行い、2 製品に絞って実際に PoC（概念実証）を実施して、2024 年 2 月に Next-Gen WAF を採用することを決定した。Next-Gen WAF の採用を決めた理由を、開発部門 開発部 Infrastructure Service セクション Network Service Unit の中澤昌史氏は、次のように話している。

「発生した攻撃を Next-Gen WAF が自動的にカテゴライズしてくれるため、設定が比較的容易で、社内に専任の SOC エンジニアがいなくても運用できることを評価しました。また、しきい値ベースでリクエストをブロックでき、誤検知も少ないので、サービス担当者への説明がしやすく、社内の理解を得やすかったことも採用の理由でした。他社製品も検討しましたが、ネットワーク機器にアドオンするこ

とが必要で、小規模な導入には不向きなほか、膨大なシグネチャーの検討、選定のための専門人材の確保や人的コスト、即時ブロックによる誤検知などの課題がありました。」

株式会社ぐるなび
開発部門 開発部
Infrastructure Service セクション
Network Service Unit
中澤 昌史 氏

株式会社ぐるなび
開発部門 開発部
Infrastructure Service
セクション 副セクション長
対馬 祐治 氏

アタックリクエストのアクセス状況を可視化できたことが最大の効果

Next-Gen WAF の導入にあたり PoC を実施。まずは Next-Gen WAF をテスト環境にリクエストの確認だけでブロックを行わないログモードで導入し、検証を実施。問題がなかったことからブロックモードに移行して、実際にどれだけのリクエストがブロックされるのか検証を行った。ブロックモードでも問題がなかったことから、まずは 2024 年 2 月に本番環境に Next-Gen WAF をログモードで導入して動作の確認を行い、3 月末にブロックモードでの本番運用に移行している。

PoC について中澤氏は、「ぐるなびには、オンプレミスからクラウドまで、プロダクトごとにさまざまなシステム構成が採用されていますが、Next-Gen WAF ではさまざまな導入構成が用意されており、今回はモジュールとエージェントを導入する構成を採用しています。Next-Gen WAF は、しきい値ベースの制御になり誤検知が少ないため本番環境に導入しても大丈夫だと判断しました。誤検知が少ないことと、さまざまなシステム構成に対して導入できることが Next-Gen WAF を採用した決め手でした」と話す。

Next-Gen WAF を導入した効果を中澤氏は、次のように話す。「まだやりたいことが 100% 実現できていないので、効果の測定に関しては今後の取り組みになりますが、現時点では『SQL インジェクション攻撃がありました』など、これまで実現できていなかったアタックリクエストのアクセス状況を可視化できたことが最大の効果です。今後はさらにカスタムルールを活用してセキュリティを強化していきたいと思っています。」

また対馬氏は、「Next-Gen WAF のようなツールの導入は、あくまでもサポート的な位置づけで、よりセキュアなコンテンツを開発することが本筋であり、開発メンバーの意識改革が重要になると思っています。例えば、パッチが提供されていないオープンソースソフトウェアや改修が困難な古いコンテンツに関しては Next-Gen WAF で対応しますが、新たに開発するコンテンツはセキュアに実装する方針です。セキュリティ対策では、ツールの導入とエンジニアの教育をセットで考えることが重要だと思っています」と話す。

Next-Gen WAF の導入における Fastly のサポートについて中澤氏は、「PoC や導入時に、それぞれ選任の担当者にサポートしてもらえたので、スピーディーに作業を進めることができました。導入後は安定して稼働しており、サポートを利用する状況は発生していません。また導入時の不明点について Slack で問い合わせをすると、すぐに回答してもらえたり、設定のサンプルを作ってもらえたりしたのでサポートには非常に満足しています」と話している。

Next-Gen WAF の導入で悪意のあるリクエストを確実にブロック

Next-Gen WAF の導入後の状況について対馬氏は、次のように話す。「悪意のあるリクエストが確実にブロックされていることはもちろん、アタックを受けていることの確認とレポーティングができるようになりました。いまのところ誤検知は無く、検知はしたけれどもブロックはしていないリクエストに関しても把握できています。ルールのチューニングについては今後の取り組みになりますが、『OWASP Top 10』に取り上げられるような基本的なアタックはブロックできるようになったので、セキュリティ強化における一定の成果は得られたと思っています。WAF の運用には専任のエンジニアが必要ですが、Next-Gen WAF では設定がシンプルで容易なためエンジニアがセキュリティ対策に掛ける運用負荷が軽減され、コンテンツ開発により注力できるようになったことも Next-Gen WAF を導入した効果でした。」

今後の取り組みについて中澤氏は、「まだ検討の段階ですが、今後有効であると判断すれば、他の環境に対しても Next-Gen WAF を展開していくことはあると思います。また、ボットを迅速に検出してブロックできる Bot Management に興味があり、タイミングがあえば試してみたいと思っています。今後、Fastly のサポートには、ぐるなびの状況に合わせた提案や最新情報、先端技術などを提供してもらえることを期待しています」と話している。

お問い合わせ

japan@fastly.com
www.fastly.com/jp
@FastlyJapan
@FastlyEdgeCloudJapan

ぐるなび

fastly