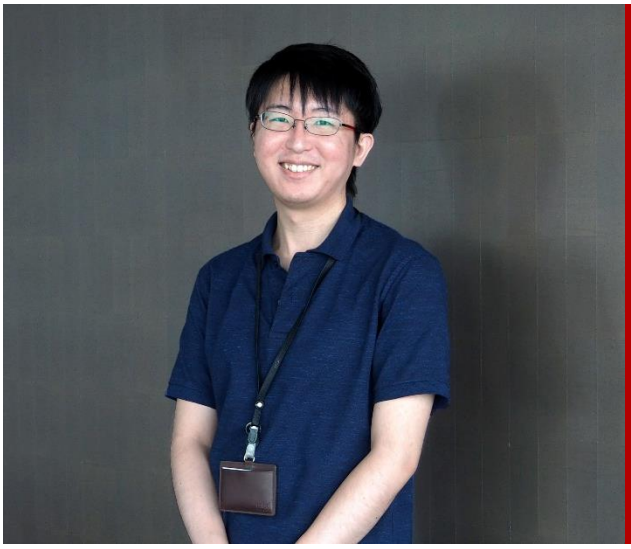
Red Team Technologies

Synack

株式会社ミクシィ様 導入事例

株式会社ミクシィは 1997 年の創業以来、SNS「mixi」やスマホアプリ「モンストライク」など、友人や家族といった親しい人と一緒に楽しむコミュニケーションを軸にしたサービスを展開しています。同社が提供するサービスでは、氏名・生年月日やクレジットカード番号等、多くの個人情報を取り扱うことから、ユーザーが安心してサービスを利用できるよう、セキュリティ対策にも注力しています。

今回、株式会社ミクシィでセキュリティ対策を主導している亀山様に、現在行っているセキュリティ対策や同社において株式会社レッドチーム・テクノロジーズ及び Synack, Inc.が果たす役割についてお話を伺いました。



Point. 1

ガチガチにルールで縛るというより、現場の意見を尊重し、ケースに合わせた柔軟なセキュリティ対策を進めることを大事にしています。

株式会社ミクシィ 開発本部 CTO 室

セキュリティ技術グループ マネージャー 亀山氏

企業ミッション達成のためのセキュリティ

株式会社ミクシィ(以下、「ミクシィ」)では様々な情報資産を守るため、ネットワークセキュリティや標的型攻撃対策などの入り口対策から、エンドポイントや CSIRT の運営などを通じた出口対策、さらには社員に対する定期的な情報セキュリティ教育の実施など、幅広いセキュリティ対策を実践しています。「当社の特徴は、具体的なセキュリティ対策が比較的ボトムアップで行われることが多いという点だと思います。これは、ガチガチにルールで縛るというより、現場の意見を尊重し、ケースに合わせた柔軟なセキュリティ対策を進めることを大事にしているからです。やはり、一律に“コレ”と決めて関所のようにチェックを行うような方法だと、新しいアイディアの創造や事業スピードの足かせになりかねないですからね。」と亀山氏は語ります。

バグバウンティがパッケージ化されたユニークなサービス

このようなセキュリティ対策を進める中、ミクシィの社内では、報奨金をかけてバグや脆弱性を大勢のエシカルハッカーに探してもらう「バグバウンティ」も実施したいと考えていました。それは、例えばアップデートの頻度の高いソフトウェアの場合は、定型的な検査を定期的に繰り返すことで、リスクを低減することが出来ますが、アップデートがほぼないようなソフトウェアの場合、同じ検査を繰り返しても、新しい脅威を発見することは難しいからです。

その点、「バグバウンティ」であれば、大勢の人材が様々な観点・手法で診断を行うため、新しい脅威を発見できるのではないかと同社では考えていました。実際、ミクシィでは過去に「バグバウンティ」を実施したこともありましたが、報告された脆弱性のトリアージや再現を行う人材の確保、リサーチャーへの支払い金額の決定方法や同じタイミングで脆弱性が発見された場合の支払い配分の決定方法など、自社で運用するには負担が大きく、再実施が難しい状況でした。

そのような時に出会ったのが、アメリカのセキュリティ企

業である Synack, Inc.(以下、「Synack」)が提供するセキュリティ検査サービスです。Synack のセキュリティ検査サービスの最大の特徴は、厳しい身元調査と技術審査に通過した世界各国の 1,500 名以上のエシカルハッカーが、バグバウンティの利点を応用した仕組みで実施するペネトレーションテストを定額料金で提供している点です。「Synack のサービスは、定型的な検査やペネトレーションテストだけではなく、バグバウンティまでがパッケージ化されており、非常にユニークなサービスだと思いました。特に Synack のバグバウンティは、身元、スキルの面においても、厳格な審査を通過したエシカルハッカーのみで構成されるリサーチャーなので、安心感がありましたし、海外で実績が豊富だったのもポイントが高かったです。また、日本人だけではなく世界各国の人材が、様々な観点から診断をしてくれる点も魅力的でした。」と亀山氏は明かします。

Point. 2

API の仕組みなどをきちんと理解していないと見つけられない脆弱性もあり、品質としては大変満足しています。

株式会社ミクシィ 開発本部 CTO 室

セキュリティ技術グループ マネージャー 亀山氏

24 時間の稼働、何度も検査・再診断が出来るなどリアルタイム性に優れたサービス

ミクシィでは、金銭を扱うようなミッションクリティカルなシステムやテストに膨大な工数がかかるシステムの診断に Synack のサービスを導入しました。

「当社のアプリケーションは、特殊なつくり方をしているものも多く、ツールなどで診断するとすべてエラーになってしまい脆弱性が発見できないといったこともよくあるのですが、Synack の診断結果は、ツールでは発見できない脆弱性を検出してくれているのはもちろん、API などの仕組みをきちんと理解していないとみつけられないような脆弱性もあったので、品質としては大変満足しています。また、Synack のサービスで一番よかったのは、検査中でも再診断をいつでも何回でもできる点です。やはり、深刻な脆弱性がみつかった場合は即座に修正し、その修正が反映されているか即座に確認したいですからね。他社のサービスの場合、深刻な脆弱性についてはすぐに報告してくれるものの、再検査についてはすべての検査が終わってからという流れになるので、なかなかそれが実現できませんでした。特に Synack は、24 時間稼働してくれるので、私の業務時間外に検出された指摘事項を業務時間中に確認・対策できるなど、リアルタイム性に優れていると感じました。」と亀山氏は説明しました。

また、日本国内では、Synack の唯一のパートナーである株式会社レッドチーム・テクノロジーズが、言語面や技術面でのサポートに入るため、実施に対する負担が少なかった点も評価が高いとのことでした。

ミクシィでは今後も、情報セキュリティを強化するため、幅広い対策を推進していくとのこと。その中で、バグバウンティのように、社内リソースではコスト・工数的に対応が難しいものについては積極的に外部サービスを活用し、効率的な運営を実施していく方針です。「Synack が提供しているようなマネージドサービスは、効率的な運用には欠かせないものなので、今後ますます需要は高くなっていくと思います。」(亀山氏)

株式会社ミクシィについて

ミクシィグループは、“ユーザーサプライズファースト”の企業理念のもと、ユーザーの皆さまの想像や期待を超える価値提供に取り組んでいます。これからも、“フォー・コミュニケーション”と定めたミッション（私たちのやるべきこと）を遂行するため、人々の生活がより豊かになる未来を思い描き、IT の側面からコミュニケーションの活性化を促す事業・サービスを推進し、より良いコミュニケーションの創造に取り組んでいきます。

Synack, Inc.について

Synack では、厳格な審査を通過した世界中のエシカルハッカーで構成される人間によるバグバウンティの利点を応用したサービスと、高度な AI テクノロジーをシームレスに融合したクラウドソース・ペネトレーションテストを定額制で提供しています。Synack の詳しいサービスについては synack.com（英語）または、redteam.jp(日本語)をご確認ください。

本サービスに関するお問い合わせ先

株式会社レッドチーム・テクノロジーズ

住所：東京都新宿区西新宿 3-20-2 東京オペラシティビル 41 階

電話：03-5333-1233

E メール：rt2_sales@redteam.jp

Red Team Technologies