事例紹介 ▸▸▸ サイボウズ株式会社 様

サイボウズのセキュリティ施策「脆弱性報奨金制度」にVEXが挑戦。複数の脆弱性を検知し、導入が決定。

自社パッケージ製品・クラウドサービスのセキュリティ向上のために
社外のバグ発見者による報告に対して報奨金を支払う
「脆弱性報奨金制度」を実施しているサイボウズ株式会社。
検査ツールであるVEXが複数の脆弱性を検知したことをきっかけに
評価していただき、サイボウズ株式会社にVEXをご導入いただきました。

導入企業様のご紹介 ▸▸▸ サイボウズ株式会社 様

クラウドベースのグループウェアや業務改善アプリを軸に、世界中の「成果を生み出すチーム」を支援するサイボウズ株式会社。学生やNPO、在宅医療などの少人数プロジェクトからグローバルに拠点をもつ大企業まで、多様なチームが製品・サービスを利用中。
また、サイボウズ株式会社CSIRT（略称Cy-SIRT）を立ち上げ、社外の組織・専門家と協力して、インシデント発生の予防、早期検知、早期解決、被害が発生した場合の最小化を主眼とした活動を行っている。グローバル開発本部品質保証部検証グループでは、組織内の情報セキュリティに関する施策全般を検討する会議体を主催。Cy-SIRTの運用支援や脆弱性報奨金制度の運営にも携わっている。

グローバル開発本部
品質保証部 部長

明尾 洋一 様

グローバル開発本部
品質保証部
検証グループ 兼
Cy-SIRT

伊藤 彰嗣 様

セキュリティ向上のためにサイボウズが取り組む脆弱性報奨金制度

サイボウズは延べ400万人以上のビジネスユーザーが利用するクラウドサービス及びパッケージ製品を取り扱う事業者として“お客様の情報資産を保護する”ことを最重要課題とし、各種セキュリティ施策を行っています。特徴的な施策の一つである「脆弱性報奨金制度」は、サイボウズが提供するサービスに存在する脆弱性を早期に発見し改修することを目的とする制度です。社内の力のみでは発見できない未知の脅威を外部の協力者の力を借りて早期に発見し、製品の品質を向上させようとするもので、2013年の試行期間を経て2014年から常設しています。
サイボウズではバグハンターと呼んでいる一般ユーザーを対象に、本番環境への影響を考慮せず検査を行うための「脆弱性検証環境提供プログラム」を用意。報告された脆弱性の深刻度に応じて一定の報奨金をお支払いしています。またご協力いただいた方のお名前や報告内容は、コーポレートサイト内「サービスの品質向上にご協力いただいた皆様」というページにて公開しています。
2014年に報告いただいた脆弱性の件数は241件、そのうち脆弱性として認定されたものは158件、報奨金総額は700万円でした。2015年は報告件数208件、認定は119件、報奨金総額は448.2万円となりました。この制度により、2013年と2014年を比べると脆弱性認定件数は約7倍に増えており、報奨金制度に大きな効果があることを実証できています。
基本的な検査、製品仕様の理解、ソースコード解析などの自社施策と、報奨金制度による発見が相互補完することでサイボウズのセキュリティ向上を実現しています。

VEXが検査ツールとして初めて脆弱性を報告

検査ツール VEX を導入したのは、この脆弱性報奨金制度がきっかけです。バグハンターを対象としたこの制度に対して、ツールであるVEXがどこまで挑めるか試させてほしいというお問い合わせをユービーセキュアさんからいただきました。企業の参加は前例のないことでしたが、セキュリティ向上を目指す意味では是非チャレンジしたい事案でしたので、制度のルールを一部変更しご参加いただきました。
結果、VEXが検出した複数の脆弱性をご報告いただきました。検査ツールのみでここまで検出できるのかと驚いたのが正直なところです。過去、他の自動検査ツールを利用したことはありましたが、検出内容が十分ではありませんでした。そのため、近年は補助ツールを利用した手動検査が主となっておりましたが、作業効率化が図れ、かつ検出内容が優れた検査ツールを引き続き求めていたこともあり、この機会にVEXの導入を全社で検討することとなりました。

まずはご来訪いただきVEXについての概要・機能に

ついて詳しくご説明いただいた上で、試用を開始。試用時には、操作性、既知の脆弱性の検出具合、誤検出の程度、報告書の見やすさを重視して評価しました。
その結果、通常サイボウズで行っている検証項目を含め、多岐にわたった項目が検出可能でした。また、レポートが充実しており分かりやすいことも導入の決め手となりました。送信したリクエストの確認や検出された脆弱性の詳細が出力される点、脆弱性に関する影響や対処方法の記載があり理解しやすい点などが評価したポイントです。日本語で詳しく説明されているので、検査担当者が内容をしっかり理解した上で、開発者へフィードバックできるようになりコミュニケーションもスムーズになると予想できました。
導入検討から導入までに要した期間は半年ほどです。稼働前に検査担当者がVEXの操作トレーニングを受講しましたが、このことが実際の試験に非常に役立ちました。特にサイボウズのような仕組みが複雑なアプリケーションの検査を実現するハンドラー機能など細かな操作まで知ることが出来るため、操作トレーニングはVEXを利用する際には欠かせないものだと感じました。

手動による検証とVEXの相互補完により高い効果を実現

検査フローに大きな変化はなく導入はスムーズに行えましたが、近年の検査はすべて手動で実施していたため検査方法は大きく変わりました。
まず、診断パターン数が圧倒的に増えたことが上げられます。手動による検査の場合、なるべく少ないパターンでより効率の良い検査を行う必要があります。そのため、製品の作りとして効果の薄い検査については、検査パターンから除外することがありました。VEXの場合、数千という検査パターンのリクエストで検査できますし、担当者の技術力に頼らない検証が可能なため、結果にムラがなくなります。また、パラメーターに対して一つ一つ攻撃コードを入力する必要がある脆弱性（クロスサイトスクリプティング・SQLインジェクション）についても見落としがなくなります。
多様な脆弱性のシグネチャも用意されており、かつシグネチャの更新頻度も高いため新しい技術に対応した検査ができることも効果の一つです。また、VEXはWeb上で動作するため情報共有や検査データの一元管理が可能となりました。疑問点や検査項目のレビュー等、他拠点とのやり取りが円滑にできています。
ほかにも、VEXは決まった検査項目だけでなく、希望の検査方法にカスタマイズできるところも特徴です。サイボウズ仕様にカスタマイズすることができるので今後ますます活躍する機会は増えると思います。
導入以降、ユービーセキュアさんには頻繁に問い合わせをさせていただいていますが、その都度迅速に対応いただき、要望についても対応可能な点については取り入れていただいています。その分今後の期待も大きく、クライアントサイドで発生する脆弱性に対する検出精度の向上など、更なるグレードアップを望んでいます。
VEXを導入することで、従来の検査方法では検出できなかった脆弱性も検出できるようになりました。これからもサイボウズ社内での手動検査、フローの精査、情報共有等と、VEXによるムラのない検査との相互補完により、高いセキュリティレベルの向上を実現し続けたいと思います。
今後とも安心して利用できる検査ツールを開発していただきたいです。

取材を終えて　～ユービーセキュアより～

バグハンターのマインドを忘れずに VEXのさらなる検出精度向上を目指します

この度は脆弱性報奨金制度に企業として初めて参加させていただき、まことにありがとうございます。また導入事例の取材にご協力いただき、ありがとうございます。今回は検査ツールを開発するベンダーとして、初心にかえる大変貴重な機会となりました。これからもご意見ご要望に真摯に対応し、みなさまに選ばれる製品開発に邁進いたす所存です。

関連製品 vex

Webアプリケーション検査の内製化を支援

従来では手動でしか検査を行うことができなかった画面遷移が複雑なWebアプリケーションや、入力画面と出力画面が異なるセカンドオーダーの脆弱性に対しても検査の実施が可能です。

製品についての詳細・お問い合わせはこちら　http://www.ubsecure.jp/vex/vex.html

製造・販売元

UBsecure 株式会社ユービーセキュア

〒104-0045　東京都中央区築地4丁目7番5号　築地KYビル4階

販売代理店

201703版