Secureworks®

導入事例

「Red Team Lite」を活用し システムの安全性を短期間で実証 サービスの信頼向上に寄与

顧客企業の DX を後押しする 革新的なサービスを幅広く展開

市場を取り巻く環境が大きく変化する中、企業には自社のビジネスを変革する取り組みが強く求められている。ここで重要なポイントとなるのが、最新のデジタルサービスをいかに業務に取り入れていくかという点だ。「出会いからイノベーションを生み出す」を企業ミッションとする Sansan も、そうした先進デジタルサービスを提供する事業者の一つである。

同社の法人向けクラウド名刺管理サービス「Sansan」は、企業・自治体をはじめ 7000 件以上の契約を有し、この分野におけるデファクト・スタンダードとなっている。また、個人向け名刺アプリ「Eight」も、ビジネスを加速するツールとして 280 万人を超えるユーザーに活用されている。さらにその他にも、クラウド請求書受領サービス「Bill One」など、業務効率化に寄与するサービスを展開。日本企業の DX を強力に後押ししている。

加えて注目されるのが、「セキュリティと利便性を両立させる」を企業理念の「Premise」として掲げている点だ。Sansan 株式会社 CISO 補佐 CSIRT マネジャー 河村 辰也 氏は「当社のサービスでは、お客様の大事な個人情報を取り扱いますので、セキュリティの確保はビジネスの大前提です。お預かりした名刺情報が、不正に使用されるようなことは絶対にあってはなりません。とはいえ、あまりセキュリティばかりに傾き過ぎてしまうと、今度は自由なチャレンジが行いにくくなってしまう。我々に求められているのは、セキュリティと利便性を高いレベルで両立させることだと考えています」と語る。

Sansan 株式会社
CISO 補佐
CSIRT マネジャー
河村 辰也 氏

このような思想のもと、同社ではサービスの安心・安全を担保する取り組みを全方位で展開。システム面での対応はもちろんのこと、全社員が個人情報保護士の資格を取得するなど、人・プロセスの面でも万全の態勢を築き上げている。

ペネトレーションテストに 「Red Team Lite」を採用

こうした取り組みの一環として、同社では外部ベンダーによるペネトレーションテストを毎年実施している。河村 氏はその狙いを「各サービスを支えるインフラについては、当社のエンジニアが細心の注意を払って環境を構築し運用しています。しかし、内部だけの視点だと、見落としなどが生じる可能性も否定しきれません。そこで、外部の第三者に攻撃者の目線で環境をチェックしてもらうことで、対策や運用に綻びが生じていないかを確認しているのです」と説明する。

同社では各サービスのペネトレーションテストを順番に実施しているが、今回のテスト対象には前述の個人向け名刺アプリ「Eight」

sansan

- お客様名：Sansan 株式会社
- 資本金：63 億 33 百万円
  （2021 年 8 月 31 日時点）
- 従業員数：979 名（2021 年 8 月 31 日時点）
- 所在地：東東京都渋谷区神宮前 5-52-2
  青山オーバルビル 13F
- 公式 HP：https://jp.sansan.com/

■ ソリューション

- Red Team Lite

■ プロジェクトのゴール

1. 社内 Active Directory の管理者権限取得
2. Eight データベースからの顧客情報取得

■ プロジェクト実施期間

- 2021 年 3 月 ～ 6 月

が選ばれた。ベンダー選定にあたっては、Red Team テスターの攻撃力を特に重視したとのこと。その結果、最終的に選ばれたのがセキュアワークスであった。

「ペネトレーションテストに関する技術資格を保有するなど、優秀なエンジニアが数多く在籍している点が決め手となりました。また、当社ではセキュアワークスのマネージド・セキュリティ・サービスを導入していますが、そこでの対応にも十分満足しています。さらに、セキュアワークスのインシデント管理リテーナーを利用したコンサルティングも受けましたが、的確な助言と成果物を得ることができました。こうした総合力の高さも評価につながりました」と河村 氏は語る。

加えて、もう一つのポイントが、特定のプロセスに限定してリアルな標的型攻撃を可能な限り忠実に再現する「Red Team Lite」の存在である。「できればサイバーキルチェインに沿ったフルスコープでの Red Team テストを実施したかったのですが、今回はあまり時間的な余裕がなかった関係で、できるだけ短期間で実施できるサービスが求められました。その点、「Red Team Lite」であれば、脅威に侵入されたフェーズからテストを開始できます。このように柔軟にニーズに応えられるサービスが用意されている点も良かったですね」と河村 氏は続ける。

充実したテストを短期間で実施
セキュリティレベルの高さを確認

今回のテストでは、「社内 Active Directory の管理者権限取得」と「Eight データベースの顧客情報取得」の 2 点がゴールとして設定された。社内ネットワーク内に感染端末／攻撃デバイスを設置したり、マルウェアを実際に起動したりする作業については同社自身で実施。これにより、限られた期間内で最大限のアセスメントを実施することができた。

「テスト実施に向けたプロセスでは、セキュアワークス側のスタッフと綿密な打ち合わせを行いました。様々な情報のやりとりもタイムリーに行えましたし、技術者の言葉で会話できたので、非常に話が早かったですね。おかげで大変スムーズにテストを行えました」と河村 氏は語る。

「Red Team Lite」による攻撃は約 2 週間にわたり行われたが、これに対する社内の対応も的確だったとのこと。マルウェアの活動はセキュリティ製品や SOC による監視でいち早く検知され、ネットワーク内での横断的侵害や Eight データベースの顧客情報へのアクセスもしっかりと防御された。「総じて高いセキュリティレベルが確保できており、当社のビジネスに致命的な影響を及ぼすような攻撃が容易には実行できないことが確認できました」と河村 氏。この結果は経営トップにも報告され、継続的に取り組むよう指示がなされているとのことである。

「今年から社内のログを横断的に検索する仕組みを導入したのですが、その効果がはっきりと見えたことも大きな成果でしたね。ログ基盤に収集された情報を分析することで、Red Team がどのような手段や経路で攻撃を仕掛けたか追うことができました。当社の対策レベルが着実に向上していることを実感できたのは、非常に良い経験でした」と河村 氏は続ける。

今後も継続的な改善を推進
サービスの安心・安全を追求

ペネトレーションテストを実施する際には、本番業務への影響を避けるために様々な制限を設ける企業も多い。しかし同社で実施されるペネトレーションテストは、一切の制限を設けずに実施するように、ベンダーに依頼しているという。「驚かれることも多いのですが、やはり何らかの制限があると、見つかるべきリスクも見つからなくなってしまう。そのため、あらゆる攻撃手法にて、テストを実施することに意義があると思っています」と河村 氏は説明する。当然、今回のテストも同様の形で実施されたが、それでも重大な問題が確認されなかったことには非常に大きな意義がある。

加えて、さらなるセキュリティ強化に向けた手がかりが得られた点も見逃せない。「今回のプロジェクトを担当した診断員の方は、非常に細かい部分まで当社の環境をチェックしてくれました。おかげで、今後やるべきことが具体的に洗い出せました。小さなことの積み重ねが重大なインシデントにつながりかねないので、頂いたレポートを今後の改善に活かしていきます。ちなみに次回のペネトレーションテストでは、ぜひフルスコープでの Red Team テストを実施したいと考えています」と河村 氏は語る。

同社のビジネスは急速な拡大を続けているだけに、グループ全体を見据えた支援も期待したいとのこと。河村 氏は「サービスの数もグループ会社の数も増え続けているので、社内の要員だけだとなかなか手が廻り切りません。こうした面でも、セキュアワークスには数多くの知見が蓄積されていると思いますので、コンサルティングなども積極的に活用していきたい」と語る。

出会いからイノベーションを生み出す革新的なサービスを、今後も世に送り出していくSansan。「その取り組みをセキュリティ面からしっかりと支えて行きたい」と河村 氏は抱負を述べた。

セキュアワークス株式会社

お問い合わせ SCWX_PreSales@secureworks.com 03-4400-9373 www.secureworks.jp

Secureworks®