シスコ サービス導入事例

国内保険 B 社様

高度なマルウエア攻撃演習の実施により セキュリティ対策の必要性、優先度を可視化

製品 & サービス

- シスコ セキュリティ レッド チーム演習
- シスコ セキュリティ アセスメント

課題

- 他の金融機関と比べ、どの程度セキュアな環境であるか
- 自社システムで攻撃を検知、防御できるか
- マルウエアによる社員端末への感染はどの程度成功するのか
- 感染に成功した場合、顧客情報漏えい前に SOC チームにより検知、防御できるか

ソリューション

- 社員に対するスピア フィッシング攻撃テスト
- 社員端末へのマルウエア感染テスト

結果～今後

- 実践的なサーバー攻撃への対応状況の把握
- 今後の対策の重要度、優先度を把握

国内保険 B 社様は、クラウド サービスを活用した保険サービスを提供する大手企業です。

同社では激しさを増すサイバー攻撃への対策を検討するにあたり、シスコ セキュリティ レッド チーム演習とセキュリティ アセスメントを受けました。これにより同社は自社の実態と対応策の必要性、優先度を把握することができました。

お客様はシスコのグローバル レベルの技術力、数多くの実績を踏まえた分析力を信頼した上で依頼されており、分析結果は説得力と納得感がありました。範囲とレベル策定が悩ましいセキュリティ対策において、重要度、緊急度が明確になり、お客様との協議が進めやすくなります。

– B 社にインフラ サービスを提供するベンダーご担当者

課題

大手保険会社である同社では、継続して大切な顧客情報を守るサイバー セキュリティ対策を検討しています。2020 年東京オリンピックなどの影響で今後、さらに激しさを増すと予想されるサイバー攻撃からいかに身を守るか、という対策は広範囲かつ多岐に渡ります。

同社は、自社の対策状況を正確に把握し、重要または喫緊の課題点を見極めることが重要と捉え、シスコ セキュリティ レッド チーム演習とセキュリティ アセスメントを実施しました。

同社としてサイバー攻撃対策の実態として把握したかった項目は、

・他の金融機関と比べ、どの程度セキュアな環境であるか
・自社システムで攻撃を検知、防御できるか
・マルウエアによる社員端末への感染は、どの程度成功するのか
・感染に成功した場合、顧客情報漏えい前に SOC チームにより検知、 防御できるか

というものでした。

ソリューション

実施にあたり、自社にネットワーク基盤および仮想デスクトップを提供するベンダーにも協力を依頼し、シスコと 3 社間で協議を開始しました。

シスコ セキュリティ アセスメントの進め方

対策・改善に向けたサイバー攻撃耐性の点検
お客様の環境に応じた、実践的なサイバー攻撃耐性点検によるシステム / SOC 機能などの実効性判断と必要に応じた対策・改善

シスコ セキュリティ レッド チーム演習概要

シスコの標的型攻撃および侵入のエキスパート チーム（レッド チーム）が、実在するサイバー犯罪者を模した攻撃により潜在的な脅威を顕在化

サーバおよび端末に対して攻撃者の視点に立って、ゴールを達成（機密情報窃取やドメイン管理者権限奪取）するための攻撃を仕掛ける

アセスメントの結果、発見されたリスクと重要度、セキュリティ対策を改善するための推奨事項の提言

シスコ セキュリティ レッド チーム演習の優位性

グローバルにおける実績
米国、ドイツ、フランス、英国、日本を本社とするグローバルに展開されている金融機関、製造業の企業を中心に、世界各地で実績あるサービスです。

リオ オリンピックの経験
2016 年 リオ オリンピックでは世界中で約 50 億人が テレビを視聴し、インターネットやモバイルに 10 億人がアクセスしました。このような史上最も「つながった」コネクテッドな大会の実現をシスコはサポート。強固なセキュリティ インフラを構築するために、シスコはセキュリティ レッド チーム演習を実施しました。

第三者評価
類似サービスは市場に多く存在しますが、そのサービス品質、能力にはバラつきがあります。CRESTによる各ベンダーを差別化（品質、能力）する 第三者評価により、本サービスは Penetration Testing と Simulated Target Attack & Response のカテゴリに該当。シスコは全リージョンで認証を得ており、日本は Asia に含まれます。

CREST – Ethical Security Testers ：
http://www.crest-approved.org/membercompanies/cisco/index.html

ベンダーご担当者は、演習に対して以下のように語ります。

「最初に懸念したのは、お客様サービスへの影響です。実施内容をどの範囲で、どういった内容を、どのくらいのレベルと時期で、といった点を、シスコとの事前打ち合わせの場で 1 ヶ月ほど協議を重ねました。技術面では通信トラフィックの量や、基盤側の機器に不具合を誘発するような行為は実行するのか、などを一つ一つ確認し、細かくシスコに教えていただき安心しました。その上で、演習時に万一、感染行為が発生した緊急時の対応予定もシスコ側、弊社、お客様側での体制も含めて決めていきました。実施を弊社の体制の整っている日中時間帯に合わせていただくなど、海外のレッド チームにも柔軟に対応いただきました。」

この協議を踏まえ、シスコはいくつかのシナリオに沿った演習をカスタマイズし、実在するサイバー犯罪者と同様にインターネット外部から同社の本番環境に侵入し、攻撃者の視点に立った金融機関のセキュアなネットワーク環境を侵害する高度なマルウエア攻撃手法を試みました。また、 E メールを感染経路として社員に対して悪意のあるコンテンツおよびコードを送付し、汎用マルウエアおよび自社開発のカスタム マルウエアによる攻撃を試みました。

そしてその結果と、シスコ レッド チームのさまざまな手法を活用し、同社の要望に応える以下のアセスメントを実施しました。

- 不正ファイルを端末にダウンロードすることを防ぐ機能の調査
- ユーザが不正ファイルを事故で実行してしまうことを防ぐ機能の調査
- 情報の窃取を防ぐ機能の確認
- 攻撃者が侵入した場合に、その端末内で権限昇格ができ得るかの調査
- 侵入された端末から、他サーバなどへの通信を防ぐための機能の確認
- 攻撃者が同一ネットワーク内の他のシステムに影響を広げることができ得るかの確認

結果～今後

アセスメント成果として、お客様環境における具体的な課題が重要度、緊急度とともに明示されました。

「結果報告会に我々も参加し、レッドチームの方々とお客様とで、ビデオ会議でディスカッションを行いました。他の脆弱性検査サービスと比較して、本番環境での侵入検査を実施するという点は特異性を感じましたし、広範囲で網羅的な分析をしてくれた印象です。お客様もシスコのグローバル レベルの技術力、数多くの実績を踏まえた分析力を信頼した上で依頼されていますので、レポートも説得力、納得感があり、お客様としても今後の動きがとりやすいと感じます。セキュリティ対策はやるべきことが多く、どこまでの範囲、レベルで、というのが非常に悩ましい分野ですので、レポートで重要度、緊急度が明示されたことは、お客様と我々での協議においても非常に進めやすくなったと感じています。特にいま以上の対策、新規取り組みについて、予算計画を立てる上でも有効だと感じました。」
（ベンダーご担当者）

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

お問い合せ

1454-1802-000-F