シスコ サービス導入事例

国内金融機関 A 社様

本番環境へのサイバー セキュリティ攻撃演習により顧客情報流出防止対策の強化を目指す

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

- 自社保有機器を含めた実践的なサーバー攻撃態勢の把握
- 短期、長期の対応ロードマップ策定

国内金融機関 A 社様は、日本国内の大手保険会社の 1 つであり、クラウドサービスを利用した保険業を展開しています。

サイバー攻撃が激しさを増す中、経営層および CSIRT 主導のもと自社クラウド サービス環境におけるサイバー攻撃対策の実態を把握するため、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。これにより自社の現状を把握するとともに、今後どのようなセキュリティ対策を実施すべきかが明確となりました。

事前に攻撃範囲や時間なども協議した上で、本番環境で実施される点が一番の違いでした。実施後は自社の対策レベルが把握できるとともに、今後どのようなセキュリティ改善策を進めていく必要があるのかが明確になりました。

– 国内金融機関 A 社 IT サービスご担当者

課題

日本国内における大手保険会社であるお客様の第一の懸念事項は、社員端末がマルウエアに感染し、それにより顧客情報が侵害されることでした。2020 年東京オリンピック、パラリンピックに向けさらにサイバー攻撃が激しさを増していくと予想され、今回の実施に踏み切りました。

「ホールディングス全体での取り組みとしてこの数年、セキュリティ テストの実施は懸案事項であり、ベンダー各社から情報を収集していました。最終的にはシスコと国内 2 社との比較だったのですが、他社はいずれも開発環境で実施されるペネトレーション テストであったのに対し、シスコは本番環境でテストが実施される点が最大の違いであり、採用の決め手です。」

同社がクラウド サービス環境における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。

▲グローバルチームを交えた報告会の様子

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

ソリューション

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、お客様と協議しながら攻撃対象とゴールを決定。そして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、他サーバ等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

「シスコ セキュリティ レッド チーム演習は本番環境で約 2 週間実施されました。その前に 2 ヶ月ほどかけて、攻撃の影響範囲や実施時間帯などを細かく調整していただき、その後のアセスメントにおいて報告いただきたい項目についても協議しました。本来、ブラック ボックスで実施されるテストではありますが、本番環境での実施ですのでお客様と業務に影響が出ないという配慮が欠かせませんし、他部署との調整、連携も必要です。その点、事前協議で不明点が払拭でき、満足しています。」

結果～今後

今回のアセスメントの成果として、お客様環境において具体的ないくつもの課題が提示されました。これらの課題を解決することをゴールに、高度なマルウエア攻撃による脅威について、短期および長期での必要な対策が明確になりました。

「テストとアセスメントの結果、自社環境においてどのような攻撃が仕掛けられると危険なのかが把握できるとともに、今後どのようなセキュリティ改善策を進めていくことで高度な攻撃を軽減、もしくは防ぐことができるのかを理解することができました。実践的なサイバー攻撃耐性の評価、自社で保有する IPS 、ファイアウォールなどのセキュリティ機器が実際に反応するか、防御できるか、といった点や、社内体制の問題点が具体的に明らかになった点も非常に有意義でした。今回、第一弾としてまずは相対的な評価と、セキュリティ テストの手順を把握したかった、という目的もありました。次回、アプリケーションなど、もう少し広い範囲での実施を検討したいと思っています。」

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

1453-1802-000-F