導入事例

Secureworks®

おもてなし文化が標的に！？
敵対的友好関係としての Red Team の存在価値とは

新宿区 SHINJUKU CITY

Red Team テストに至る新宿区の背景

多くの自治体の中でも、特に、最適な ICT 基盤運用と堅牢なセキュリティ対策で知られる新宿区。自治体を取り巻く情報保護の動向として、総務省が 2018 年 9 月に改定した「自治体情報システム強靭性向上モデル」が記憶に新しい。自治体情報セキュリティ対策の抜本的強化に向けて、「個人番号利用事務系」、「LGWAN 接続系」、「インターネット接続系」のネットワーク 3 分割と、外部ネットワークとの厳密な通信制御が求められる。新宿区ではシステム強靭化の考え方として、過剰な対策・反応・対応は極力避け、サービスレベル・運用レベル優先のセキュリティ対策を掲げ、さらに多層防御により、抜け漏れのない合理的なセキュリティ対策を行っている。

一方で、新宿区の公式ホームページやファイアウォールへの攻撃件数を集計すると、1 日あたり平均 190 件ものサイバー攻撃を受けている。中でも、リオネジャネイロオリンピックの開催前後の 2016 年 5 月から 8 月にかけて、新宿区への攻撃が大幅に増加していた。2018 年の平昌オリンピックでは、五輪組織委員会への大規模なサイバー攻撃が報じられ、開会式直前にシステム障害が発生するなど、大会運営に大きな支障が生じた経緯もあり、「リオ五輪や平昌五輪でのサイバー攻撃被害実績から、東京 2020 大会ではさらなる攻撃被害の拡大を懸念していました」と新宿区 総合政策部情報システム課 課長補佐の村田 新氏は語る。新宿区では、東京 2020 大会に向けて、実際のサイバーテロ攻撃を想定した実践的・客観的・総合的な情報セキュリティ対策の検証・評価が喫緊の課題であった。万一のサイバー攻撃に備えて、

① リスクの想定に漏れはないか？
② リスク分析を踏まえた設定が正しく施されているか？
③ OSI 参照モデルの上から下まで、抜け漏れはないか？
④ 多層防御・多層防御連携は、正常に機能するか？
⑤ 標的型攻撃にどこまで耐えられるか？

といった不安を払拭する方法として、Red Team テストの導入に至った。

カスタマープロファイル

お客様名 新宿区

職員数 2,717 人
（令和 2 年 4 月 1 日 現在）

人口 344,816 人
（令和 2 年 12 月 1 日 現在）

所在地 東京都新宿区歌舞伎町 1-4-1

公式 HP https://www.city.shinjuku.lg.jp/

ソリューション：

Red Team テスト

プロジェクトのゴール：

1. リモートからのマルウェア感染
2. 端末の管理者権限の取得
3. Active Directory の管理者権限の取得
4. 重要情報の持ち出し
5. 公式ホームページの改ざん
6. 物理的侵入
（庁舎、執務室、サーバー室等）

プロジェクト実施期間：

2019 年 6 月 ～ 2019 年 9 月

導入事例

Secureworks®

Red Team テストのベンダー選定のポイント

Red Team テストは、提供するベンダーによってそのサービス内容は様々であり、実際には脆弱性診断やペネトレーションテストで終結するようなサービスもある。「新宿区では、実際のサイバー攻撃をほぼ 100% 再現してくれる『本物の Red Team』を探していました。当然のことですが、「攻撃するだけ」ではなく、攻撃プロセスの開示や、テスト後の復旧、実現可能な改善提案までカバーしてくれるのは、セキュアワークスの Red Team テストだけでした」と村田氏は語る。庁内の SOC ／ CSIRT 機能の実践的な評価・検証だけでなく、組織の危機対応能力の評価・検証、そして改善へ大いに有効であったという。

新宿区 総合政策部情報システム課
課長補佐 村田 新 氏

難易度の高いサイバー攻撃プロジェクト

攻撃者の観点を理解する重要な点として、最も効率的な手法（難易度が低く、かつ効果の高い手法）を優先的に取り入れることが一般的だ。また、侵入経路も正規ルートだけではなく、抜け穴などがないか入念に調査する。セキュアワークスの Red Team テスト全体を通して、新宿区のセキュリティレベルが非常に高い状態にあることが確認できた。

● 複数のセキュリティ製品による多層防御が有効

前述のとおり、新宿区ではインターネット分離をはじめとする通信制御、さらに多要素認証や複数のセキュリティ製品による多層防御が導入されており、高度なセキュリティ機能が実装されていることが確認できた。万一、フィッシング等でマルウェアに感染した端末が存在しても、インターネットと分離されていることから容易に外部と通信ができない状態であった。また厳格なアクセス制御により、不要な通信を許可しないようにネットワークが設計されているため、万一の攻撃者からの侵入があっても、攻撃の影響を最小限に抑えられることがわかった。技術的には非常に強固なシステムが構築されていることが確認できた。

● 迅速なインシデント対応

Red Team テスト期間中、攻撃者の存在に早い段階で気づき、締め出すための取り組みが継続して行われたことも大きな特徴だ。新宿区では、エンドポイント環境に仮想デスクトップ端末を導入しており、不審な通信を行う端末にいち早く気づいたセキュリティ担当者が、その都度、検知・対応する姿が見られた。さらに、管理者パスワードの変更やアカウントの無効化など、攻撃を阻止する取り組みがプロジェクト期間中、継続して行われており、インシデント対応力の高さを確認することができた。

● 不正端末の迅速な発見と撤去

Red Team テストでは、ターゲットのネットワーク環境に不正な端末を設置し、境界突破を行うことがある。新宿区の Red Team テストでも、不正な端末の設置を試みたのの、即日撤去されたことが確認できた。これは検疫ネットワークや MAC アドレスフィルタリングなどによる不正デバイス検知の仕組みが実装され、正しく機能できていることが確認できた。

導入事例

Secureworks®

「リスク分析の適正、それに応じた設計を繰り返すことで、真の情報セキュリティレベルの評価と成熟度の向上につながります」と村田氏

おもてなし文化が標的に！？ Red Team テストで実感したこと

一方で、運用面や体制面の課題が明るみになったのも事実だ。システムアカウントの管理不備、部分的な設定漏れ、想定外からの侵入とその対応など、新たなセキュリティ対策の検討が必要となっただけでなく、人の往来が多い区役所ならではの課題も指摘された。中でも日本人の「おもてなし」文化が、リスクにつながることを再認識した。「フィッシングメールなどの注意喚起は随時行っていますが、実業務を装ったなりすましメールの場合は、職務上、開封や返信が必要と判断せざるを得ないケースがどうしても生じます。不審メールの開封を 100% 回避することは困難という前提で、必要な対策を講じることが求められます。」と村田氏は語る。「区役所に限らず、『ドアの前に立っていれば、誰かが扉を開けてくれる』などの日本特有のおもてなし文化は、反面、攻撃の対象となりやすく、今後も注意が欠かせません」と村田氏は語る。

Red Team テストの成果

「リスクを想定・分析・設計しても、必ず抜けは生じます。守り側だけでは対応は不十分で、友好的敵対関係として、Red Team テストは実践に即したリスクの再評価をすることができます」と村田氏は語る。また技術面・運用面・人員面で潜在的な脆弱性の是正が必要であることを再認識したという。そしてインシデント対応手順にも改善が必要なことがわかった。「机上での手順は実際の攻撃を受けた場合、完全に防御できないことがわかりました。各担当者・部署が一丸となって、インシデントに対応できる仕組みを作ることが重要です」と村田氏は強調する。

新宿区では Red Team テストの結果をもって、翌年度には新たなセキュリティ対策の検討・実施に至った。「リスク分析の適正、それに応じた設計を繰り返すことで、真の情報セキュリティレベルの評価と成熟度の向上につながります。今後も Red Team テストは定期的に行いたいと思います」と村田氏は語る。

サービスに関するより詳細な内容に関しては、下記までご連絡ください。

セキュアワークス株式会社

SCWX_PreSales@secureworks.com

03-6893-2317

www.secureworks.jp