金融機関にTLPTを導入するための検討

Study to introduce TLPT to financial institutions

岩下央・マネジメント分科会・情報セキュリティ大学院大学

In recent years, as cyber attacks have become increasingly sophisticated and persistent, it is an important responsibility for financial institutions to enhance their cyber resilience. In this context, financial authorities in various countries have provided guidelines on the Threat-Led Penetration Test (TLPT), which is a useful tool for enhancing cyber resilience. However, the TLPT is not widely used among Japanese financial institutions. The reasons for this are considered to be the lack of understanding by management, the need to take countermeasures against adverse effects on production operations, the need for reliability in testers, and the difficulty and cost being higher than those of vulnerability assessment and penetration testing, which are considered barriers. In this paper, we surveyed the current status of TLPT, clarified issues, and discussed countermeasures. We also compared the differences among industry sectors and with penetration testing, and showed the advantages of conducting TLPT as one of the efforts to enhance cyber resilience.

1.研究の背景・目的

2018年に、G7サイバー・エキスパート・グループが策定した，Threat-Led-Penetration Test(TLPT)に関する「脅威ベースのペネトレーションテストに関するG7の基礎的要素」が公表された．本研究では，TLPTが推奨されている金融分野に焦点を絞り，金融機関にTLPTの優位性を理解してもらうことを目的とする．この金融機関は，サイバーセキュリティ対策についての予算を確保しており，どのような手法での対策をするか検討している者を対象としている．TLPTの優位性を示すために，TLPTの普及の現状と課題について調査し，対策を提案している．また，分野ごとの違いについて考察を行い，ペネトレーションテストとの比較を行っている．本研究の知見は，金融機関がサイバーレジリエンスを高めることに役立つと考えられる．

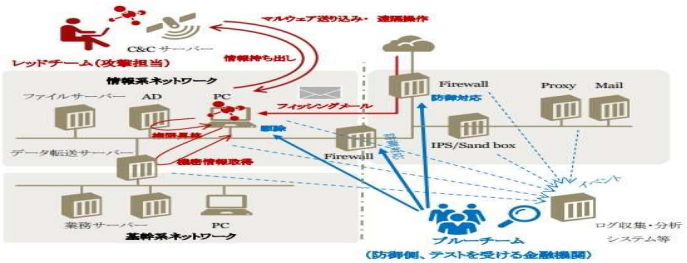
2.TLPTとは

日本の金融機関におけるTLPTの実施率は、脆弱性診断やシステムへの攻撃試行等による検査を行っている先の2割程度（全体の1割程度）にとどまっている

TLPTの定義

（金融機関の）コントロール下において，実在の攻撃者の戦術，テクニック，手順をまねることにより，金融機関のサイバーレジリエンスを侵害しようとする，攻撃の試行である．これは，特定の脅威情報（threat intelligence）に基づき攻撃を試行するものであり，予備知識と，業務への影響を最小限に抑えつつ，金融機関の職員，プロセス，テクノロジーに焦点を当てた攻撃を試行するものである

（出典：脅威ベースのペネトレーションテストに関するG7の基礎的要素）



（図：諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書）

3.ペネトレーションテストとの比較

項目	ペネトレーションテスト	TLPT
目的	対象としたシステムの中で，できるだけ多くの脆弱性を特定することを主目的とする	攻撃者からの攻撃の検知と組織的な対応能力を強化することを主目的とする
テストゴール達成	システム、IT資産： どこに脆弱性があるのか、侵入後システムログが取られているか、検知はできたかを確認することができる 人、組織： 結果は得られない	システム、IT資産： どこに脆弱性があるのか、侵入後システムログが取られているか、検知はできたかを確認することができる 人、組織： 検知後のエスカレーション対応，被害拡大防止の対応，対応時間を確認することができる
テストゴール未達成（または途中まで達成）	システム、IT資産： 脆弱性はないことが確認できる．または、どこで検知・防止ができたのか（できなかったのか）を確認することができる 人、組織： 結果は得られない	システム、IT資産： 脆弱性はないことが確認できる．または、どこで検知・防止ができたのか（できなかったのか）を確認することができる 人、組織： 検知後のエスカレーション対応，被害拡大防止の対応，対応時間を確認することができる

4.課題と分野ごとの違いに対する対策

課題

①経営層の理解不足がある

＜対策＞

経営層が主体となるテスト計画を策定する，普及活動を行う

②本番業務への悪影響について対策を行う必要がある

＜対策＞

テスト環境の構築を行う，上手くいかなかった場合の対応策を考えておく

③テスターに対する信頼性が必要である

＜対策＞

資格や実績を確認する

④難易度・コストが，脆弱性診断とペネトレーションテストと比べて高い

＜対策＞

補助金や人材確保の政策を推進する，テスト計画の工夫を行う

⑤TLPTの高度化，より高度な専門人材の育成が必要である

＜対策＞

教育を行う、先行事例を参考にする，IT人材が活躍できる場を広げる

分野ごとの違い

①脅威インテリジェンス導出部分で違いがある

＜対策＞

個々の金融機関がもつ脅威を導出する必要がある

②TLPTが上手くいかなかった場合のサービス障害の違いがある

＜対策＞

サービス障害の違いについて把握し，悪影響について対策を行う．

③デジタル化の進展による新たなリスクに関するシナリオの違いがある

＜対策＞

最新のサイバーセキュリティ情報の収集，関係者を巻き込んだシナリオを作成する

5.まとめと今後の課題

まとめ

- TLPTという手法について取り上げ，金融分野における現状と課題について調査し，対策を検討した
- 産業分野ごとの違い，ペネトレーションテストとの比較を行い，優位性を検証した

今後の課題

- TLPTに関する関連研究があまりないため，RED TEAMING，ペネトレーションテストについて調査を行ったが，他に似た手法がある可能性がある
- 一般的な課題について取り上げたが，より実務的観点からの考察を深めることで，TLPTの優位性を示すことができる可能性がある