要旨

『IE08 最新セキュリティ動向』 研究内容要旨

背景

2020 年のセキュリティを見据えるため、過去のセキュリティインシデントを調べたところ、標的型攻撃が IPA 発表の情報セキュリティ 10 大脅威に過去 10 年ランクインし続けていることが判明した。

また、ニュースでも大きく取り上げられた近年の悪質な標的型攻撃に以下がある。

年	事例	流出件数
2014 年	大手航空会社を狙った攻撃	約 73 万件
2015 年	年金機構の個人情報を狙った攻撃	約 125 万件
2016 年	大手旅行代理店の個人情報を狙った攻撃	約 678 万件

【近年の悪質な標的型攻撃例】

以上の内容より、本研究グループでは、今後も被害が予想され、プロアクティブな対策が求められる、標的型攻撃の研究を行った。

背景から導き出される問題点

大きく分けて、システムの問題とヒトの問題の 2 つの視点があると考える。

- システムの問題
  - マルウェア配布方法が巧妙化され入り口防御のみでは防げない
  - 振る舞い検知など標的型攻撃に特化した防御策の費用対効果がわかりにくい
  - そもそもどのレベルでシステムを整えるべきか基準がない

- ヒトの問題
  - セキュリティへの認識が甘い、知識が乏しい
  - 情報の価値を理解しないまま取り扱っている
  - ルール自体はあるが、知らないあるいは守らない

研究方法

「システムの問題」に着目した場合、企業ごとの予算・セキュリティポリシーにより汎用的な対策案を提示することは難しい。そこで「ヒトの問題」に着目し、

「守るべきものを明確にし、個人に意識させることでセキュリティホールを小さくできる」

と仮説を立て、ヒトに対してアプローチすることでの汎用的な対策案の提示を目標に研究を進めていくものとする。

©2016 UNIRITA Users' Group

要旨

研究の概要としては、教育効果を見込んだアンケートを擬似標的型攻撃の前に実施したグループと、擬似標的型攻撃の後に実施したグループに分けて対照実験を行い、擬似攻撃成功の確率を調査した。

●グループ１：　　擬似標的型攻撃　→　事後アンケート
●グループ２：事前アンケート　→　擬似標的型攻撃　→　事後アンケート

研究成果

本研究での成果物は以下の通り。
・セキュリティ意識向上アンケート
・コストレスで構築する擬似標的型攻撃実施ノウハウ

研究結果

グループ２のほうがグループ１よりも攻撃の成功率が低い結果となった。よって仮説通り、守るべきものの認識や確認点などのポイントの意識を強めることで、セキュリティ意識が向上し、標的型攻撃の成功率が低下したといえる。

また、アンケートで得たパスワードの管理方法、標的型攻撃への対応ルールの理解、標的型攻撃を回避した理由等から、ヒトのセキュリティ意識の傾向を考察した。

まとめ、今後の課題

この研究によって、ヒトのセキュリティに対する意識を高めることで標的型攻撃に対して効果があるということが実証された。

しかし、実施の母数が少なく、また対象者が SE に偏りがあったため、もともとセキュリティの基礎知識が豊富な集団である可能性が高い。より精緻なものへブラッシュアップするにためには対象者数や職種の範囲を広げ、企業トータルでの効果を検証する必要がある。

参考文献

サイト
・情報セキュリティ 10 大脅威 2016～個人と組織で異なる脅威、立場ごとに適切な対応を～ https://www.ipa.go.jp/files/000051691.pdf、独立行政法人 情報処理推進機構セキュリティセンター、2017/02/08 閲覧
・JAL 顧客情報システムへの不正アクセスによるお客さま情報の漏えいについて〈最終報告〉 https://www.jal.co.jp/info/other/140924.html、日本航空株式会社、2017/02/08 閲覧
・不正アクセスによる個人情報流出の可能性について http://www.jtbcorp.jp/jp/160824.html、株式会社ジェイティービー、2017/02/08 閲覧

※文章内の記載の会社名および製品名は、各社の登録商標および商標です。

©2016 UNIRITA Users' Group