

第128回 維持管理研究会 議事録

- 開催日時：2022年4月21日(木) 16:00~17:40
- 場所：Zoomリモート開催
- 出席者(敬称略) 21名

小田、上辻、大下、大島、木村、熊澤、古村、澤田、滝川、柳本、山下、中谷(記)
 地域勉強会：近藤、彦坂、大竹、萩原、鷲山、柳父、中村、松本、梅田

4. 研究テーマ

今月は、最近頻発しているサイバー攻撃について、その中でも身近に発生し騙されやすい標的型攻撃メールに絞り込んで、そのタイプや対策事例について情報提供を行い、メンバー間で情報交換を行った。

<標的型攻撃とその対策 抜粋>

1. 情報漏洩が組織に与える影響

情報漏洩時に発生するコストはインシデント1件あたり平均4億円にも上ることが明らかになっています。そのうち顧客の個人情報情報が漏洩した事例で発生するコストが最も高いという調査結果となっています。

影響	内容
損害賠償	情報漏洩によって損害が生じた人・組織への損害賠償
対応費用	原因調査・再発防止のための費用、謝罪広告等による広報費用
機会損失	サービス中断、社会的信用の低下による売上低下や取引中止など
法的制裁	各国の法令(個人情報保護法・GDPR等)による刑事罰(罰金・入札停止等)

セキュリティ対策を推進、意思決定を行う際は、組織に与える影響を十分に踏まえたうえで、判断することが重要となります。

1-1. 情報セキュリティ10大脅威 2022

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内閣不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる不正アクセス	7	修正プログラムの公開前を狙った攻撃(ゼロデイ攻撃)
スマートフォン利用者の被害	8	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	9	予期せぬIT基盤の被害に伴う業務停止
インターネットバンキングの不正利用	10	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン		

1-2. ランサムウェアの対策

有名企業がターゲットにされたものを目的にすることが多いですが、あまり身近に感じないかも知れませんが、大手の有名企業でなくても、誰しもがターゲットになる可能性のある攻撃の1つです。

被害	対策
① 端末を操作不能にされる	① 不審なリンク・添付ファイルを開かない ランサムウェアの感染源はWebサイトやメールのリンク・添付ファイルが多数を占めている。 閲覧しないリンクや添付ファイルはクリックしない。
② データが見られなくなる	② 攻撃前に外部記憶媒体を接続しない 最も一般的なランサムウェア攻撃であり、感染した端末からデータを暗号化する事により、データを閲覧出来なくなる。 データをバックアップし、暗号化を解除することが必要である。
③ 遠くまでデータを公開される	③ データのバックアップを定期的に取る 最近のランサムウェアは暗号化だけでなく、データを暗号化し、外部に公開された事例も多発している。 暗号化されたデータは、暗号を解読する事ができず、公開されたデータは、暗号化されたまま公開される。

《参考》ランサムウェアの侵入手口(例)

身代金を要求する悪質なランサムウェアの場合、ランサムウェアを駆除しても機密情報や個人情報が漏れてしまう。
ランサムウェア攻撃を受けて身代金を支払った組織の8割が2度目の攻撃を受けている。

3. 標的型攻撃の種類

- ① メールの盗聴・改ざん
- ② 標的型攻撃メール
- ③ フィッシング詐欺
- ④ ビジネスメール詐欺(なりすまし)
- ⑤ 水飲み場攻撃
- ⑥ 従業員による情報漏洩

3-1. 標的型攻撃メール

攻撃者が機密情報の詐取など明確な目的を持って、特定の組織や個人を対象に行うサイバー攻撃のことです。
最近ではサプライチェーンで繋がっている中小企業にターゲットが拡大している。

3-2. フィッシング詐欺と対策

クレジットカードやネットバンキングなどのサービスになりすまし、そこからサイトに誘導し、ログイン情報や個人情報を入力させることで情報の窃取を行う攻撃手法です。
日常生活のほか、最も身近で危険を感じる「メール」攻撃のひとつである。

被害	対策
① 金銭的な被害	① メッセージ内容の確認 フィッシングに用いられるメッセージは、日本語がおかしい・送付アドレスが怪しい・重要な内容がないなどの特徴がある。
② なりすまし、不正利用	② 公式サイトから改めてアクセスする メッセージに記載のURLからアクセスすることは非常に危険なため、改めて公式サイトにアクセスすることが重要である。
③ フィッシング詐欺情報の収集	③ フィッシング詐欺情報の収集 フィッシング詐欺の内容は、似たものが多いので悪質な攻撃を収集して、社内公開し対策に役立てることが重要である。

3-3. ビジネスメール詐欺(なりすまし)と対策

組織の幹部や顧客等になりすましてターゲットの従業員にメールを送信し、添付ファイルのダウンロードや、そのPCからシステムに侵入し、情報窃取などを行う攻撃手法です。
従業員自身にとっては、メールの転手が見知った存在であり、なおかつ幹部や顧客等であらうという点で、信ぴよ性を確かめず対応してしまうことが多いです。

被害	対策
① 情報を読み取られる	① 複製したパスワードの生成 パスワードの追加を拒否することで、参考情報の再取得やパスワードの漏れを防ぐ。ビジネスメール詐欺の可能性を抑えることが出来る。
② メッセージ内容の確認	② メッセージ内容の確認 金銭や情報の要求などを受けられるような内容のメッセージを受信した場合には、十分な注意が必要である。(開封しない！)
③ 連絡先へ問い合わせる	③ 連絡先へ問い合わせる 口座振替や銀行振込などの連絡については、怪しいと判断した場合は、必ず事前に電話等で本人に直接確認して確認すること。

3-4. 水飲み場攻撃と対策

ターゲットが訪れるWebサイトを改ざんし、不正プログラムを仕掛けることで、当該のWebサイトを訪れた際に不正なプログラムが作動し、PCにウイルス感染などを仕掛ける攻撃手法です。

被害	対策
① 情報漏洩、改ざん	① 不審なWebサイトにアクセスしない ウイルス感染より、攻撃者が不正アクセスするための入口を容易に提供されたことが原因となることが多い。この点には絶対にアクセスしないことが重要である。
② 端末を操作不能にする	② OSやAPLを最新に保つ OSやAPLのアップデートを行い、常に最新状態にすることで、脆弱性を防ぎ、ウイルス感染リスクが低減する。
③ さらなる攻撃の踏み台になる	③ セキュリティソフトの導入・更新 この攻撃を防止するために、外部からの不正アクセスを防止するセキュリティソフトを導入し、常に最新のセキュリティソフトにしておくことが重要である。

5. テレワークにおける脅威と脆弱性

攻撃、盗難、搾取

6. セキュリティ対策の見直し

既存の境界型セキュリティは不要ではなく、「内部は安全」という、今までのセキュリティポリシーが種々のアクセスを評価するポリシー「ゼロトラスト」に向かっていることが重要である。

6-1. サイバーセキュリティ対策(例)

- ① 会社PCの使用制限
 - ① 会社PCでは、インターネット接続先の制限(ホワイトリスト)
 - ② 会社PCのHDD(SSD)に重要データ保存を禁止、又は暗号化
 - ③ 社内システムには登録PC以外では、ログイン不可
- ② 基本的なセキュリティ対策
 - ① 定期的なPWの変更、及びウイルス対策ソフトの定期的更新(毎日の業務開始前にOS・APL・ウイルスソフトの最新状況を確認)
 - ② メール添付ファイルのURLには、安易にアクセスしない
 - ③ 会社PCでは、ブルーWi-Fi(スポット)の使用を禁止
- ③ 情報セキュリティの継続的教育
 - ① 基本的な注意事項(盗難・セキュリティ保護)の継続教育
 - ② 疑心メールを定期的に送付し、注意喚起と指導実施
- ④ パスワード・データ保存
 - ① パスワードは他人に推測されにくい複雑なものにする
 - ② またパスワードをPC本体には絶対に保存しない
 - ③ 認証の強化(多要素認証によるID管理)
 - ④ 重要データのバックアップ強化(3-2-1法則)

7. 発想の転換が必要

「脅威を入れない」
対策

「被害を防ぐ」
対策へ

セキュリティ対策には、一長一短があり**完全な防御策は不可能**である。

7-1. 発生時の対応手順（標準化）

標的型攻撃は、多層的な対策を施しても完全防御することは不可能です。想定できる限りの対策は必要ですが、万が一標的型攻撃を受けたときに何をすべきかを標準化しておくことが重要です。

※IPAが示している確認事項

- ① いつ届いたメールなのか？
- ② 送信者の組織名やメールアドレスと送信者への確認
- ③ 使用しているセキュリティ対策ソフトやハードウェアと検知状況（PC、メールサーバ、Webプロキシ、ファイアウォールなど）
- ④ メールの内容、添付ファイル名、本文記載内容
- ⑤ 同じメールが誰に届き、何人が添付ファイルを開いたか？
- ⑥ メール記載のリンクや添付ファイルを開いた場合、どんな状態になったか？
- ⑦ どんな被害が発生しているか？
- ⑧ 感染したPCのOS/APLのバージョンやアップデート状況
- ⑨ eml形式やmsg形式でのメール検体情報の提供可否
- ⑩ 不正接続先などのインシデント情報の共有可否
- ⑪ 提供情報について統計値や調査への利用可否（提供者情報は匿名）
- ⑫ 攻撃に使われたマルウェアのセキュリティ対策ソフトのベンダ提供可否

10. まとめ

高度に見える「サイバー攻撃」が、実は誰にとっても身近な脅威となっている。一方どうにも対処しようがないというわけではなく、いつでも誰もが実施できる対策が、たくさん存在しています。

「自分には関係ない」とは考えず、「自分も被害者になるかも」という意識を持って、対策をひとつずつ行なっていくことで、自分が被害者になる可能性を減らすことができます。

「これさえやれば大丈夫」というシンプルなルールを作り従業員に徹底することが大切です。
また常に最新環境に保つことを習慣化することが攻撃を防ぐ最大の防御となります。

5. 所見

各メンバーの組織では、直接被害を受けていないこともあり、身近で危険であるという認識を持たれている方が少なく感じました。ただグループ企業においてサプライヤーがサイバー攻撃を受け納品が不可となり、グループ全体に大きな影響があった事例を説明して頂き、参加者にとっては大変身の引き締まる思いであった。

また一番身近に普段なにげなく使用しているメールの危険性と対応策について、認識を新たに持って頂いたことは大変有意義であった。

＜次回予定＞

・令和4年 5月19日（木）16:00～17:30

以上