御堂筋監査法人ニュースレター Apr 2024

個人の情報セキュリティチェックポイント

公認会計士　川中 敏史
大手監査法人を経て 2022 年から御堂筋監査法人にて勤務。主に医療法人の内部統制指導、監査業務に従事。
保有資格：公認会計士

企業や医療機関を対象としたサイバー攻撃被害が断続的に発生している中、各組織では限られた予算や人員に応じて対応可能な範囲で対策を練られていることかと思います。
特に金銭（身代金）を要求する「ランサムウェア」を利用した事例は後を絶ちません。この点、「ランサムウェア」と聞くと、経営者又はシステム管理者による対策であって、一般職員にはあまり関係が無いという認識をお持ちの方も多くいらっしゃるのではないでしょうか。
しかし、「ランサムウェア」や「ウイルス」をはじめとする悪意のあるソフトウェアへの感染は一般職員個人の隙も狙われるのが現実です。
そこで、今回は一般職員個人に求められる対策に絞ってご紹介したいと思います。

1. 代表的な手口

① フィッシングメール

銀行、EC サイト等の実在する組織を偽装したメールをユーザーに送りつけ、「ID やパスワードの変更」、「購入確認」等と称してリンク先をクリックさせ、あらかじめ用意した正規サイトにそっくりな偽サイトにユーザーを誘導する。
そこでクレジットカード番号や口座番号、パスワード等を入力するよう促し、入力された情報を盗み取る非常にメジャーな手口である。
また、メールにウイルス等を直接添付しなければメールのセキュリティ対策をすり抜けることも可能。

② 不正サイトへのアクセス

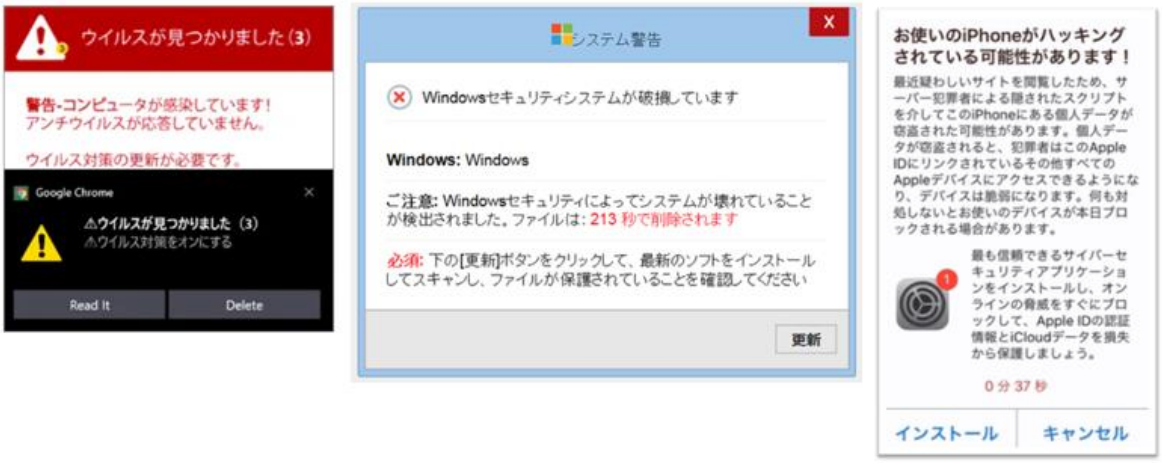
・水飲み場型攻撃

ターゲットがよく訪れるサイトを改ざんし、不正なプログラムを仕掛けておく。サイトを訪れた際に、マルウェア等の不正プログラムが端末にインストールされる。

・フェイクアラート

Web サイト内に表示される広告のクリックや開発元が不明なアプリのインストールにより、突如現れる偽の警告メッセージ。
「Windows セキュリティシステムが破損しています」、「マルウェアやウイルスに感染しました」、「パソコンが破損する可能性があります」、「セキュリティ向上のため、最新バーションにアップデートしてください」といった不安を煽るようなメッセージがポップアップ通知される。
指示通りに「続行」ボタンや「更新」ボタンをクリックすると、端末のハッキングや高額な金銭の要求、重要な情報が盗まれる可能性がある。
中には、警告音を鳴らすことで動揺を誘うパターンもある。

《フェイクアラートイメージ》



③　内部不正による情報漏えい

関係者が機密情報を持ち出したり漏洩したりする不正行為であり、現在勤めている職員だけでなく、外注先や業務委託先、退職者等によって行われる。

主なケースは、「退職者による意図的な漏えい」「現職職員の誤操作・誤認などによる漏えい」「現職職員のルール不徹底による漏えい」。

2. チェックポイント

代表的な攻撃手口を把握したうえで、最低限チェックすべきポイントを列挙しました。

※これらチェックポイントを全てクリアしたとしてもセキュリティリスクがゼロになることはありません。

【全般】

①　不審な情報を見た場合の通報

PC 画面上やプリンター、メール、電話等で不審な情報を見聞きした場合は、直ちにシステム管理者へ連絡をする。

②　インシデント発生時

所属組織でマニュアルが作成されている場合は、マニュアルに従う。

マニュアルがない場合は、直ちにシステム管理者へ報告し対応方法を確認する。

【Web サイトへのアクセス時】

①　アドレスバーに表示される URL の確認

✓ **鍵マーク**

常時 SSL 化（Web サイト通信全体の暗号化）が行われていることを意味し、該当サイトのページ内で送受信されるデータは常に暗号化される。

✓ **https**
「https」から始まる URL のサイトは SSL 化されていているが、「http」から始まる URL のサイトは SSL 化されていない。

✓ **ドメイン名**
アクセスしようとしているサイトの名称等に関係しているか。

② 「お気に入り」や「検索エンジン」からのサイトアクセス
インターネットサイトへは、メール内のリンクからではなく、あらかじめ「お気に入り」登録したリンクや検索エンジンからアクセスするようにする。

③ フリー素材の不用意なダウンロード
フリー素材の画像やファイルのデータにマルウェアが仕掛けられていることもあるため、業務上の指示や信頼性が確保されている場合を除いて、外部サイトからデータのダウンロードをしない。

④ 意図しないバナー広告やポップアップ通知
不安を煽る文言が出てきても、決して「許可」や「更新」、「ダウンロード」等のボタンはクリックしない。

⑤ QR コードの偽装
QR コードの上から不正サイトの QR コードが記載されたシールを貼りつけ、不正サイトへ誘導する手口もあるため、QR コードを読み取る際には不自然なシールが貼りつけられていないか注意する。

【メール受信時】

① 差出人のメールアドレス
本文中で名乗っている人物・組織と差出人のメールアドレスの整合性が取れていることを確認する。特に@より後ろの部分が組織のドメイン名かどうかは必ず確認する。

② 本文の文脈や文法
本文に記載されている内容が自分に関係ある内容であるか否か、脈絡の無い内容であれば疑う。また、使用する単語や全体の文脈の文法に不自然な点が無いかを確認する。

③ 添付ファイルのマクロ有効化
マクロ機能を悪用したマルウェア（マクロウイルス）が仕込まれた Excel や Word を開いて有効化した場合、端末がマルウェアに感染するため、送信元の信頼性が確認されない場合は、不用意に有効化しない。

④ 添付ファイルの拡張子
アイコンや拡張子偽装はよく使われる手口の一つであるため、添付ファイルを開く前に拡張子を確認する。拡張子が「.exe」となっているファイルは、プログラムが記述されたファイルであり、開くとプログラムが実行される仕組みとなっている。

【メール送信時】

① 宛先アドレス

メール送信前に必ず宛先を確認する、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能）やメール送信の取消機能等を活用する。

② 重要な個人情報等を本文に記載しない

重要な情報は電子メール本文に記載せず、添付ファイルに記載しパスワード等で保護する。なお、パスワードは電話等の別手段で知らせる、あるいは事前に取り決めておくといった方法とセットで行う。

【ソーシャルエンジニアリング】

① ID やパスワードを安易に教えない

メールや口頭等で ID・パスワードや個人情報の問い合わせを受けた場合、その者の信頼性や問合せの理由、リンク先やメールアドレスの確認をした上で回答する。

② クリアスクリーンの徹底

食事やトイレ、会議等で自席や居室を離れるときは、必ずコンピュータのログアウト（ログオフ）やスクリーンロックを行い、第三者が自分の利用権限でコンピュータを操作したり、画面を盗み見たりできないようにする。

③ ショルダーハッキングの防止

背後からのぞき見られる危険性があるときは、 ID・パスワードの入力を行わないことや端末画面にのぞき見防止フィルタをつける。

【ログインパスワードの設定】

① 推定困難なパスワード

例えば、英数字、記号を混在させた 8 桁以上もしくは 10 桁以上のパスワードを設定する。電話番号や固有名詞、生年月日、職員コードなど、他人から類推しやすい情報やユーザーID と同じものは避ける必要があります。

日本特有として、sakura、doraemon、himawari、daisuki 等もよく使われるパスワードとして知られています。

《世界でよく使われたパスワードランキング 2023》

順位	パスワード	クラックタイム	順位	パスワード	クラックタイム
1	123456	1秒	11	UNKOWN	17分
2	admin	1秒	12	1234567	1秒
3	12345678	1秒	13	123123	1秒
4	123456789	1秒	14	111111	1秒
5	1234	1秒	15	Password	1秒
6	12345	1秒	16	12345678910	1秒
7	password	1秒	17	000000	1秒
8	123	1秒	18	admin123	11秒
9	Aa123456	1秒	19	*******	1秒
10	1234567890	1秒	20	user	1秒

引用：Nord Pass 社公表の 2023 年版「世界で最もよく使われたパスワード トップ 200」抜粋

なお、パスワードの定期的な変更については、頻繁な変更に伴うパスワードのパターン化や使い回しになることが懸念されています。
そのため、定期的な変更ではなく、パスワード等を用いた知識認証に加えて、IC カード等を用いた所持認証や指紋や顔・虹彩等を用いた生体認証を組み合わせることもセキュリティ対策上有効と考えられています。

【USB の管理】

① 組織指定 USB のみの使用
市販の USB を使用せず、組織が管理している USB のみを使用する。
※システム管理者によって、端末ごとに USB の接続制限が設けられているケースもある。

② USB の社外持ち出し
許可がある場合を除き、家に持ち帰る行為や外部への持ち出しをしない。

3. まとめ

日々進化し続けるサイバー攻撃に対して、組織としての課題が無くなることは無いと考えるべきですが、個人での対策は限界がある故に対策可能な事項は明日からでも取り組むことができます。
本記事を通じて、新たに気付いた事項があればセキュリティ対策として意識して頂けると幸いです。

以上