China Management News

（KPMG 中国マネジメントニュース）

2020 年 8 月

フォレンジックの視点―新型コロナウィルス感染拡大に伴うサイバー上の検討事項と脅威・対応―

CIO と CISO が考えなければならないこと

新型コロナウィルスのパンデミック（世界的大流行）は私たちの生活を変えつつあります。人々は不安を抱き、情報と安全、支援を求めるようになります。組織犯罪グループは、新型コロナウィルスがもたらす恐怖、不安、疑いをさまざまな形で利用し、個人や企業をターゲットにして攻撃してきます。

新型コロナウィルス・パンデミックの規模と影響への懸念が広がり、企業も対応や事業継続に必要な対策を検討するようになりました。最高情報責任者（CIO）や最高情報セキュリティ責任者（CISO）には、パンデミック封じ込め策が実施されたときに組織を確実に機能させるという重要な役割があります。

リモートワークは円滑に機能しましたか

会社がリモートでもフレキシブルに機能するようにしなければなりません。また、そのような職務形態について社員に自信を持たせなければなりません。そのためには、アクセス権、各種権限、リスク管理方針の決定に関して再検討が必要かもしれません。

検討すべきポイント：

- リモートワークを必要とする多数の社員にリモートアクセスを可能とするために、VPN、ポータル、ゲートウェイの拡張を行いましたか。
- 拡張実現のために、追加のサプライヤー・請負業者・ベンダーについて検討しましたか。
- インフラをテストし、予想した負荷の処理が可能かどうかを確認しましたか。
- インフラに単一障害点はありますか。システム復旧について強化しましたか。
- アクセス制御を緩める必要がありますか。または、リモートログイン・アカウントもしくは認証情報を追加で提供する必要がありますか。
- ログインできないユーザーやリモートワークに慣れていないユーザーからの問い合わせに対応するヘルプデスクの体制は整っていますか。
- 社員がリモートワークで使用できるノート・パソコンは用意できていますか。必要な台数を新たに調達し、業務上必要なソフトをインストールできますか。どのように優先順位でノート・パソコンを貸与しますか。
- 手持ちの機器に限りがある場合、必要不可欠なサービスを検討し、代替的なアクセスソリューションに分割してアクセスすることを検討しましたか（例：Office 365 と One Drive の併用と社内用独自アプリの活用）。
- 特定のアプリケーションのホワイトリスト（注意警戒不要リスト）を作成し、不要なサービスをすべてブロックすることを検討しましたか。
- ビデオ・音声電話会議システムの使用に制約はありますか。拡張するためにできることはありますか。
- 代替的なクラウドベースのカンファレンスとテレワーキング・ソリューションを検討する必要がありますか。
- ビデオ・音声電話会議システムにアクセスするために必要な番号／リンクをスタッフ全員が持っていますか。トレーニングの資料はすぐに使えま

すか。ヘルプラインを設置すべきですか。

- ヘルプデスクのスタッフを在宅勤務にしなければならない場合、リモートで対応できますか。
- 下記のようなヘルプデスク関連のよくある問合せについて、スタッフに配布する簡単な手引きを用意していますか。
  - ログイン方法
  - パスワード変更
  - 主なサービスへのアクセス
  - ヘルプデスクの利用方法
  - 主な連絡窓口

特定の IT 担当者に依存していませんか

社員が感染する可能性もあります。あるいは社員が移動できなくなったり、家族の看護にあたらなければならなくなったりすることもありえます。したがって、多数の社員の欠勤に備えて計画を立てるべきです。

- 特定の IT 担当者（請負業者を含む）が移動できなくなったり、ウィルスに感染したりした場合はどうなるでしょうか。少数の特定人員に頼っていませんか。
- どうすればその依存度を軽減できるでしょうか。たとえば、他の管理者が重要なシステムにアクセスできるようにするために、緊急時の手順を定める方法があります。
- セキュリティチームはどうでしょうか。重要な人は誰でしょうか。CISO が指示を出せない場合、誰がセキュリティ方針についての重要な決断を下し、会社が容認できるリスクを判断するのでしょうか。

サイバーインシデントが発生した場合

組織犯罪グループは新型コロナウィルスへの恐怖心を利用して、ターゲットを絞り込んだスピアフィッシング攻撃を実行し、偽のウェブサイトを立ち上げます。その結果、サイバーセキュリティ・インシデントのリスクが高まります。

- 新型コロナウィルス・パンデミックや新型コロナウィルスに対する会社の対応についての確実な情報をどこで入手できるか、社員に明確に伝えていますか。
- 新型コロナウィルスについての作り話を使ったフィッシング攻撃のリスクが高まっていることをスタッフに警告していますか。
- クラウドサービスとして調達したものを含め、代替システムまたは代替ソリューションに依存している場合、これらのシステムに関わるセキュリティ・インシデントを誰が処理しますか。

感染拡大時には、セキュリティ・イベントの監視に関する手配を含めたセキュリティ対策を変更する必要がありますか。

IT インシデントが発生した場合

インフラへの要求の変化やオポチュニスティック型サイバー攻撃の可能性を考えれば、新型コロナウィルスがメディアを賑わせている間も、IT 障害の可能性に注意を払うべきです。

- インシデントをリモートで調整できますか。必要な会議設備を持っていますか。インシデント管理サイト／プロセスおよびガイドにアクセスできますか。
- 物理的アクセスが限定または制限される場合に備えたバーチャル会議室を設けていますか。
- インシデント対応に関して特定の人員に依存していませんか。依存している場合、その依存度を軽減するために何ができますか。
- 主要なインシデント管理者／リカバリー責任者が業務にあたれない場合、緊急事態／インシデント対応危機管理体制はどう変わりますか。
- バックアップは最新で、最悪の場合でも会社の重要なデータとシステムを回復できると自信を持って言えますか。
- 労働力の大部分が在宅勤務になった場合、大規模なランサムウェア・インシデントにどう対処しますか。

脅威

KPMG は、2 月半ば以降、サイバー犯罪者が新型コロナウィルスを題材にしたスピアフィッシング攻撃を開始し、Office 365 の認証情報を収集することを目的として、偽のウェブサイトに誘導するためのインフラを急速に構築するのを目の当たりにしてきました。
以下に仕掛けられた攻撃の事例を挙げます。

- 新型コロナウィルスを題材にしたフィッシングメールに、Microsoft の既知の脆弱性を利用した悪意の Microsoft 文書を添付し、悪意のあるコードを実行する。
- 新型コロナウィルスを題材にしたフィッシングメールに、マクロを有効にした Microsoft Word 文書を添付する。健康情報を含むこの文書が、

Emotet（エモテット）または Trickbot（トリックボット）マルウェアのダウンロードを開始する。
- 標的ユーザーを米国疾病予防管理センター（CDC）の偽ウェブサイトに誘導し、ユーザーの認証情報とパスワードを盗み取ろうとするフィッシングメールが大量に送信された。
- 偽のカスタマー相談窓口が新型コロナウィルスの影響によるサービス停止の最新情報を顧客に提供すると称し、マルウェアをダウンロードさせる。
- 保健省などの政府機関や世界保健機関を名乗り、予防策を案内するフィッシングメールを送る。これらのメールにマルウェアが埋め込まれている。
- 新型コロナウィルス関連の税還付を語るフィッシングメールで、偽のウェブサイトを閲覧するよう促し、何も知らないユーザーから財務・税務情報を収集する。

多数の既存の組織犯罪グループは戦術を変え、新型コロナウィルス絡みの健康関連情報、偽りの治療法、財政政策、緊急給付金、モノやサービスの供給不足などを題材として利用するようになりました。

疑わしい E メールの典型的な特徴は以下の通りです。
- 文法、句読点、綴りが間違っている。
- E メールのデザインが稚拙で質・レベルが低い。
- 宛先が個人名ではなく、「社員各位」「親愛なる友人へ」「お客様各位」などになっている。
- 遠回しな脅迫や見せかけの切迫感が含まれている。
- 個人情報や財務情報を直接要求する。

当然のことながら、あまりによくできた話であれば、それはおそらく虚構のものです。

対応

特にリモートワークに移行する場合、組織や社員へのリスクを軽減するためにとるべき重要な対策がいくつかあります。
- 新型コロナウィルスを題材にしたフィッシング攻撃のリスクが高まっていることを警告し、チームの意識を向上させましょう。
- 安全維持のために確実な助言が得られる情報源を共有し、新型コロナウィルス感染拡大に対する対策策を定期的に伝えましょう。
- すべてのリモートアクセスアカウント（特に Office 365 へのアクセス）について堅牢なパスワード（できれば二段階認証）を設定しましょう。
- リモートワークに移行する社員に、リモートワーキング・ソリューションの使い方（セキュリティを維持する方法やフィッシングの発見についてのヒントを含む）に関するわかりやすいガイダンスを与えましょう。
- 貸与するすべてのノート pc に最新のアンチウィルス・ソフトウェアとファイアフォール・ソフトウェアがインストールされていることを確認しましょう。
- 社員が簡単にアクセスし、アドバイスを求めたり、セキュリティ上の問題（フィッシングの可能性など）を報告したりできるヘルプラインまたはオンライン・チャットラインを設けましょう。
- 盗難のリスクを想定し、リモートワークで使用するノート pc のデータを事前に暗号化しておきましょう。
- マルウェアのリスクを避けるため、USB ドライブを無効化し、社員には別のデータ転送手段（コラボレーション・ツールなど）を提供しましょう。

さらに、財務処理手続きでは、新型コロナウィルス・パンデミックが続く間、比較的金額額大きい支払い請求については、財務チームがチェックを必ず行うようにしてください。これにより、増大するビジネスメール詐欺や CEO 詐欺のリスクから身を守ることができます。電話やメールなど複数のチャネルを利用して、E メールによる請求をチェックするのが理想です。

クリティカル・セキュリティ・パッチを適用し、リモートワークで使用するノート pc を含む IT 資産全体でファイアウォールとアンチウィルスソフトのアップデートを行いましょう。このパンデミックに乗じて、組織犯罪グループは IT システム・メンテナンスの不備を狙っていると考えるべきです。

すべての重要なシステムのバックアップを必ずとるようにし、バックアップの完全性を検証しましょう。バックアップのオフライン・ストレージを定期的に準備するのが理想です。新型コロナウィルス・パンデミックが続く間はランサムウェアのリスクが高まると考えてください。組織犯罪グループが、新型コロナウィルスを題材にしたフィッシングを利用するからです。

最後に、インシデント・危機管理チームと協力し、代替的な音声・ビデオ会議環境を利用できるようにしましょう。IT システムを破壊するランサムウェア・インシデントが発生した場合に、主たる会議サービスプロバイダーの容量や使用可能性に問題がある場合の代替プラットフォームとして機能してくれます。

以上

Contact us お問合せ先

KPMG 中国
GJP China Markets, パートナー
杢田 正和
Tel: +86-21-2212-2247（日本語）
E-mail: masakazu.mokuta@kpmg.com