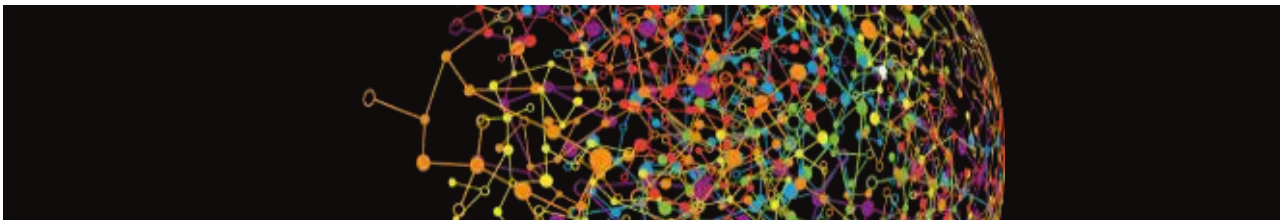

新型コロナウイルス感染症：グローバルパンデミックにおけるサイバー考慮事項

私たちが目にしているもの

コロナウイルスの影響が世界に及ぶ中、政府や企業の最大の関心は、市民、従業員および顧客の安全に向けられています。一方サイバー攻撃者は、システムや機密情報にアクセスできる機会をもたらす行動を引き起こそうと、不安をかきたてる目的を持った悪意あるメール攻撃を通して、保健機関（例えば、WHO[1]や医療組織等）やその他の政府省庁になりすましています。慎重に考えてアプローチすることで、組織は異常事態にあってもサイバーの問題に積極的に対処できます。以下は、新型コロナウイルス感染症（COVID-19）関係で戦略や労働力を調整するにあたり、組織が考えるべきサイバー考慮事項です。

異常事態におけるサイバー考慮事項

組織が社員に在宅勤務を推奨すると、基幹ビジネスシステムへのモバイルデバイスからのアクセスやリモートアクセスの利用が増加します。｜組織のIDアクセス管理とSIEM監視を強化しましょう。

サイバーセキュリティリスクは、在宅勤務の更なる推奨に伴い増加します。積極的に対策をとれば、リモートアクセスのユーザーエクスペリエンスやセキュリティを向上し、テレワーク機会を安全に実現できるでしょう。一方、保護されていないデバイスの使用は、データ損失、プライバシー侵害およびシステムの乗っ取りにつながる可能性があります。以下は、組織が行うべき行動です：

- アクセス要求の重大度に基づいた、多要素認証（MFA）層の継続的な実施、およびステップアップ認証の設置
- ID・アクセス管理プロセス、万全なセキュリティの第三者IDアクセスネットワークの確保
- 孤立アカウントの検知・予防・削除手段を含む、IT環境内における特権IDによる包括的ビューの確保

サイバー攻撃者はしばしば、危機を利用して悪意あるスキームを仕掛けてきます。｜脅威への意識を高めましょう。

新型コロナウイルス感染症関連のフィッシング攻撃は増加しており、例えば信頼のできる保健機関等に巧妙になりすましています。組織は、新型コロナウイルス感染症関連の詐欺に対して慎重である必要があります。サイバー攻撃者は悪意ある添付ファイルや不正サイトへのリンクのあるメールを送り、被害者が機密情報を漏らしたり、偽の支援先や支援目的に募金をするよう仕向けてくるかもしれません。このような攻撃は素早く増殖し、企業ネットワーク全体に広範囲の影響を及ぼしたり、個人情報盗難の原因や、振込プログラム、福利厚生プログラムの不正請求の原因となったりする可能性があります。

「フィッシング」を回避するコツ

- 新型コロナウイルス感染症関連のタイトル、添付ファイルおよびリンクのあるメールに対処する場合の注意を喚起し、新型コロナウイルス感染症に関連するソーシャルメディアの勧誘、メッセージおよび電話に注意しましょう。
- 信頼できる情報源（正式な政府系ウェブサイトの最新情報や、新型コロナウイルス感染症に関する事実に基づく情報等）を利用しましょう。
- メールで個人情報や金融情報を公開しないようにし、これらの情報の勧誘メールに返信しないようにしましょう。

2020年1月以降のコロナウイルスマルウェア攻撃

- コロナウイルスをテーマにした、ISOディスクイメージファイルが添付されたマルスパムによるLokiBot配信
- コロナウイルスをテーマにしたマルスパムによる、Remcos RAT配信
- 攻撃キャンペーンによる、新型コロナウイルス感染症（COVID-19）のテーマを利用したRemcos RAT配信
- コロナウイルスをテーマにしたマルスパムによる、Formbook配信
- コロナウイルスおよび中国人をテーマにしたmaldocs付き新規パッチワークマルスパムキャンペーン
- コロナウイルスをテーマにしたマルスパムによる、Emotet配信

デジタル変革により組織はセキュリティの予防手段やシステムを発展させ、重要システムへの侵入・アクセスを阻止することができます。｜サイバーリカバリー

あらゆる場所にサイバーが存在する時代において、技術変革やクラウドの使用が広まり、ネットワークケイパビリティの幅が広がるにつれて、脅威は増加の一途をたどっています。また、サイバー犯罪者は、企業全体に及ぶ破壊的なサイバー攻撃につながるような高度に洗練された方法で、運用システムとバックアップ機能を同時に攻撃することを考えるようになります。組織は、健全なサイバー衛生、危機対応戦略、サイバーリカバリーソリューションのアーキテクチャと実装により、防御態勢と攻撃対応準備を改善し、サイバー攻撃の影響を緩和することができます。サイバーレジリエンシープログラムが実行可能なものであれば、従来のリスク領域との境界を広げ、社員サポートサービス、アウトオブバンドのコミュニケーションツールやコラボレーションツール、Cyber Recovery Vault等の新たな機能も追加できるようになります。

どのような事象や状況であってもデロイトは、運用に深刻な混乱を与えたり、レピュテーションを傷つけたり、株主価値を破壊する可能性のある、重大な被害をもたらしたりするようなサイバーインシデントに対して、組織が戦略的に準備、対応して、そこから回復、変革を遂げられるよう支援をします。サイバー戦略は、ビジネス、業務、ビジネス継続性や技術レジリエンス、危機管理機能にわたって一気通貫している必要があるだけでなく、企業独自の手法を用いることでネットワークの露出を発見し、高度脅威を検知し、体系的インシデントレスポンスのプロセスギャップを明らかにするものでなくてはなりません。

[1]World Health Organization (2020) https://www.who.int/about/communications/cyber-security

デロイト豪州・お問合せ先

Ian Blatchford
Australia Cyber Lead Partner
+61 2 9322 5735
iblatchford@deloitte.com.au

David Boyd
Risk Advisory Japan Practice Partner
+61 3 9671 7077
davidjboyd@deloitte.com.au

Shin Takenaka
Japan Practice Leader
+61 2 9322 7737
stakenaka@deloitte.com.au

Wenda Gumulya
Japan Practice Director
+61 2 9322 3000
wgumulya@deloitte.com.au