事業継続計画を長期間導入する場合の 5 つのセキュリティ上の盲点

事業継続計画を長期間導入する場合の 5 つのセキュリティ上の盲点

アルバン・クワン（Alban Kwan）、アジア リージョナルディレクター

新しいコロナウィルスの発生（COVID-19）によって、中国本土および香港の多くの組織が事業継続計画（BCP）を導入しました。2003 年のエピデミックのときには、SARS の猛威は 9 ヶ月間続きました。感染率が急速に上昇しているこの新しいコロナウィルスは、長期に渡り商業的混乱を引き起こす可能性があり、事業継続計画への依存が大きくなります。

BCP（事業継続計画）の最も一般的な方法は、VPN を使用して安全なリモートアクセスを確保し、従業員が自宅から仕事ができるようにすることです。VPN はビジネスの世界で既に一般的に使用されていますが、エピデミックによって、影響を受けた地域のリモートアクセスの大規模で長期に渡るデプロイメントが急激に増加したことにより、組織が予期せぬリスクにさらされる可能性があります。この記事では、発生することが考えられるセキュリティ上の盲点について説明します。

1. VPN ハイジャック

2019 年 12 月に、VPN 上の新しい脆弱性 – CVE-2019-14899 – が発見されました [1]。Amazon のエンジニアである Colm MacCárthaigh は、これを「非常に賢い」そして「大変衝撃的」と表現しました。この攻撃は異なる VPN を標的にし、「使用される VPN 技術は問題ではないように見えます」[2]。TCP シーケンス番号予測攻撃のバリエーションのように見えました。TCP シーケンス番号予測攻撃では、攻撃者はさまざまな技巧をこらして、TCP シーケンス番号を観察して特定し、悪意のあるデータパケットを挿入して、効果的に VPN トンネルをハイジャックします。

このタイプの攻撃は、標的を絞ったハイジャック・キャンペーンでは大変効果的なことがあり、あらゆるデバイスと VPN を攻撃します。疑いを持たずに従業員が安全でないホーム Wi-Fi ネットワーク経由で VPN にアクセスすると、影響を受けやすくなります。

Amazon AWS の VPN 製品を開発している MacCárthaigh は、 **DNS スプーフィング**と組み合わせた場

[1] seclists.org/oss-sec/2019/q4/122
[2] zdnet.com/article/new-vulnerability-lets-attackers-sniff-or-hijack-vpn-connections/

合は、攻撃はさらに深刻な脅威をもたらす可能性がある、と警告します[3]。攻撃者は、データパケットのサイズとポジションに基づいて DNS 要求を容易にプロファイリングして応答できます。DNS は、しばしば、シーケンス内の最初のトラフィックであり、DNS クエリは VPN が確立される前に作成されます。その結果、「通常、DNS 経由のハイジャック・トラフィックはペイロード・インジェクションよりもはるかにパワフルであり」[4]、VPN ハイジャック攻撃の一部として使用することができます。この攻撃のバリエーションは、VPN パスワードを盗むために使用されることもあります。VPN パスワードを盗んだ攻撃者は、企業ネットワークに自由にアクセスできるようになります。

2. DNS ハイジャックによって VPN パスワードを盗む

2019 年に起こった「Sea Turtle（ウミガメ）」による有名な DNS ハイジャックキャンペーンの際には、Cisco Talos は、加害者がメールとその他のログインクレデンシャルを盗んで、すべてのメールと VPN トラフィックを攻撃者がコントロールする偽サーバーに転送できた、と報告しています。

攻撃者は ドメイン名レジストラまたは DNS サービスプロバイダーをハイジャックして、被害者である組織のビジネス最重要ドメインにアクセスしました。ドメイン名がハイジャックされると、攻撃者は、標的とするドメイン（例えば vpn.victimcompany.com）の SSL/TLS デジタル証明書を取得して、「傍受したメールと VPN クレデンシャルを解読し、プレーンテキストで見ることができます」。[5]

その他のハッカーは、「Sea Turtle（ウミガメ）」攻撃を模倣しました。これは、その後 DNS ハイジャックが増加したことや、大手レジストラがハッキングされたことで明らかです。

3. ドメイン名と DNS セキュリティが VPN に影響する可能性

VPN は、IP アドレスを使用して直接セットアップしたり、DNS 経由でセットアップできます。DNS は柔軟性を提供するので人気のあるオプションです。そのため、前述のドメイン名と DNS ハイジャックの問題が別の次元のリスクを生み出します。これらのリスクを回避・軽減するために、企業はレジストラと DNS のセキュリティを再確認しなければなりません。

i. **レジストラセキュリティ** – レジストラのアカウントが侵害されると、攻撃者は、ドメインを DNS にリンクしているドメイン名レジストラでホストされているネームサーバーレコードを支配できます。これによって、攻撃者は、コアドメインをあらゆる DNS に転送して、すべてのタイプ

[3] openwall.com/lists/oss-security/2019/12/05/3
[4] openwall.com/lists/oss-security/2019/12/05/3
[5] csoonline.com/article/3500492/widespread-dns-hijacking-attacks-steal-target-s-vpn-credentials.html and krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

のの中間者攻撃ができるようになります。レジストラ への侵害は**ファイアウォールの完全に外側で**発生します。これは、正しい第三者リスク管理で回避・軽減しなければなりません。効果的なリスク回避・軽減戦略には次が含まれます:

a. エンタープライズクラスのプロバイダーを使用して、過去にセキュリティ違反のあった低コストのセキュリティの低いプロバイダーは回避します。
b. レジストラの提供するレジストリロックサービスを有効にし、DNSSEC（ドメインネームシステムのセキュリティ拡張）を有効にしていることを確認します。
c. レジストラログインポータルに正しい二要素認証（2FA）が導入されていることを確認し、SMS ベースの 2FA は回避します。
d. レジストリで重要なドメインをロックします（レジストラロックと混同しないでください）。

VPN 接続の後ろにあるドメインがコアドメインと異なる可能性があるという点に注意することが大変重要です。社内で使用されているドメイン名は軽視されて、適切な注意とセキュリティ管理が必要な重要なドメインとみなされていなかった可能性があります。これらのドメインは、平穏なときには重要性が低いとみなされていたかもしれません。あるいは、以前の従業員やコントラクターがセットアップしたもので、現在のネットワークエンジニアは、完全に把握していないかもしれません。社内監査を実施して、社内の最重要システム、特に、BCP（事業継続計画）に関係するサービスで使用しているあらゆるドメインを確認し、正しいセキュリティ管理を確保することを強く推奨します。そのようなドメインがハックされると、BCP（事業継続計画）は失敗します。

ii. **DNS セキュリティとアベイラビリティ** – 攻撃者は、DNS サーバーを直接ハイジャックすることもできます。VPN 接続が DNS を使用している限り、レジストラ違反または DNS ハイジャックが BCP（事業継続計画） を完全にシャットダウンできることがあります。次に、DNS ハイジャックを回避・軽減するためのいくつかのベストプラクティスを紹介します:

a. エンタープライズクラスのプロバイダーを使用して、低コストでセキュリティの低い DNS サービス、特に、無料 DNS は回避します。
b. DNS ログインポータルに正しい二要素認証（2FA）が導入されていることを確認し、SMS ベースの 2FA は回避します。
c. DNS プロバイダーが毎日 24 時間週 7 日体制のサポートを提供しており、システムを通して修正する能力があることを確認します。サービスを使用するために、チケットをログして、ゾーンを手動で更新しなければならない場合は、非常時のリスクが高すぎます。
d. DNS ゾーンファイルの変更を監視します。DNS ハイジャックの場合には、レジストリ・レジストラロックが WHOIS（フーイズ）内のドメインネームサーバーレコードの不正な変更を防止しますが、ゾーンはロックしません。監視を提供できるプロバイダー、または、監視を SIEM と統合できるプロバイダーと提携します。

DNS の安全確保に関する詳細については、 **DNS セキュリティを強化する 6 つの方法** を参照してください。

4. SSL VPN とデジタル証明書管理のリスク

VPN は IPSec または SSL 経由で暗号化できます。導入が容易であり、低コストで、スケーラビリティが高いので、SSL VPN はますます人気が高まっています。ライセンスがなく、IPSec VPN システムの導入が難しいことから、大規模な BCP（事業継続計画）の際に、企業は在宅勤務する従業員向けに SSL VPN を導入したかもしれません。

その場合は、デジタル証明書管理に関係するリスクを考慮することが重要です。そのようなリスクは、しばしば悪い習慣から発生します。残念ながら、LinkedIn などの大きい組織でも、不手際はむしろ定期的に発生し、企業にとって大きな損失をもたらします（ 例 1、例 2、例 3）。

組織が BCP（事業継続計画）プロセスに SSL VPN を導入している場合は、ポリシーを再確認して、証明書の有効期限が切れていないことを確認することが大変重要です。次にいくつかのベストプラクティスを紹介します:

i. 組織に大量のデジタル証明書がある場合は、社内および社外証明書向けの自動更新とインストールを有効にできるデジタル証明書管理サービスを考慮します。
ii. 自動更新を有効にしないと、デジタル証明書の有効期限が切れることに気付かない可能性があります。マーフィーの法則は「失敗する余地があるなら、失敗する」と言っています。インシデントの場合に迅速に対応できるベンダーの能力が大変重要になります。毎日 24 時間週 7 日体制のサポートを提供するベンダーを選択し、「オンラインのみ」および/または Web フォームでしかアクセスできないベンダーは回避します。
iii. デジタル証明書のガバナンスフレームワークを構築することに役立つ CAA（Certification Authority Authorization）レコードを導入します。こうすることで、ドメイン上の SSL サーバー証明書の誤発行を防止して、従業員が不正なベンダーから購入することを防ぎます。

5. 非常時のフィッシング攻撃

非常時にはサイバー犯罪者が状況を利用しようと待ち構えているという事実は極めて残念なことです。「人々が武漢のコロナウィルスに懸念を募らせているときに、サイバー犯罪者たちは、保護安全対策について助言すると偽るフィッシング詐欺メールで人々の不安を食い物にしています。そのようなメールが英国と米国で見つかっています」。[6]

[6] darkreading.com/endpoint/coronavirus-phishing-attack-infects-us-uk-inboxes/d/d-id/1336946

これまで、CSC は、情報提供サイト、マスクを販売する e コマースサイト、特定の医薬品を購入することを推奨する巧みな情報サイトなどで、「corona」という単語を含むドメイン登録を 63 件検出しました。あなたの会社が医療用品や医薬品に関係している場合は、あなたの会社の製品がコロナウィルスと実際に関係あるかどうかにかかわらず、模倣品業者が、フィッシングキャンペーンを使用して模倣品を宣伝している可能性があることに注意しなければなりません。

一方、アンチウィルスソフトウェアが容易に検出できるために、フィッシング詐欺師が電子メールやドメイン名でウィルスの名前を使用することは考えられません。フィッシング詐欺師は、ブランドを使用して被害者を引っ掛けて、マクロ対応 Word 文書または感染した PDF 上のレポートを閲覧するようにし、マシンを感染させます。企業は、ブランドがフィッシング詐欺の手段として使用される可能性があることに注意しなければなりません。そのような場合、あなたのクライアントが被害を受け、あなたのブランドが傷つけられることとなります。

フィッシング攻撃は、内部的に、スピアフィッシング、ホエーリング、または、取締役や従業員のビジネスメール詐欺（BEC）によって会社を標的にしたり、あるいは、外部的に、ドメインまたはブランドスプーフィング・フィッシングキャンペーンでブランド名を使用してクライアントを標的にします。これらの攻撃は、情報セキュリティチームのレーダーで捉えることができなければなりません。

内部に焦点を当てたフィッシング詐欺では、DMARC プロトコルを導入して、SPF レコードでセットアップされたメール拒否ポリシーを管理することを推奨します。電子メールゲートウェイが DMARC に対応することを確認して、従業員またはパートナーを装うなりすましメールを効果的にフィルタリングできるようにします。

外部に焦点を当てたフィッシング詐欺では、不正防止監視サービスを導入することを推奨します。これは、保護するための高度なファイアウォールや電子メールゲートウェイを持たないクライアントを保護する唯一の方法です。

BCP（事業継続計画）を使用して、危機の間に事業を通常通りに行うことができるようにします。しかしながら、VPN、DNS、ドメイン、デジタル証明書など、ファイアウォールの外側にある BCP（事業継続計画）が使用するシステムが危険な状態であれば、BCP（事業継続計画）それ自体が組織を脆弱性にさらすことになります。セキュリティ上の盲点に留意し、適切なセキュリティ管理とポリシーを実施することで、事業継続リスクを回避・軽減できます。

CSC について

CSC は、ドメイン名、DNS、デジタル証明書などの基本的なインターネット資産内に存在する盲点を開示することにより、セキュリティ体制に多大な投資を行っている企業をサポートします。CSC は独自のセキュリティソリューションを活用することで、デジタル資産へのサイバー攻撃の脅威から企業を保護し、GDPR などのポリシーによる、収益の損失、ブランドへの中傷、重大な罰金などを回避します。CSC は、インターネット資産と共に、偽造サイト、詐欺、知的財産権侵害により、悪用されるオンラインブランドを保護、モニタリング、緩和し、多くの世界最大手ブランドを保護、コンサルティングを提供しています。

詳細につきましては、**cscdigitalbrand.services/jp** をご覧ください。