DNSセキュリティを強化する6つの方法

DNSセキュリティを強化する6つの方法

ドメインネームシステム（DNS）は、インターネットが登場して間もない無邪気な時代に一躍脚光を浴びるようになりました。その頃の初期のインターネットユーザーは、主に政府や教育組織であり、信用が前提条件で、セキュリティなどは考慮されることすらありませんでした。オンラインコミュニティは小さく、インターネットの利用はまれで、DNSの重要性はあまり知られていなかったため、その結果、保護されることなく放置されてきました。

現在へ早送りすると、その結果引き起こされた問題に気が付くでしょう。最近のサイバー攻撃に用いられるテクニックが指摘されています。それによって攻撃者が企業の正当なウェブトラフィックを操作し、資格情報やメールアドレスを不正に収集したり、またフィッシン指摘どの悪意のある活動を行うものです。場合によっては、無料のデジタル証明書（求められる検証が緩い）が、巧妙な詐欺行為に使用され、ブランドや顧客の問題を悪化させています。消費者は犯罪者による個人情報の不正アクセスや流出にうんざりしているため、そのような事案が発生すると、世界中の企業の評判や収益の低下を招きます。また近年、オンラインビジネスをダウンさせるためDNSをターゲットとした分散型サービス拒否（DDoS）という攻撃が急増しています。

ビジネスにとって、攻撃の構図は単純で、DNSのダウンはそのままウェブサイトやインターネットのプレゼンスの停止を意味します。DNSが停止すれば、顧客がウェブサイトを閲覧しようとしても、目的のページは表示できず、従業員は会社のメールも送受信できない状態となります。また電話回線にVoIPを導入している企業は、アクセスが切断されます。DNSがダウンすると、企業は固定電話か携帯電話でしか、顧客と通信する手段はありません。最後に、VPNを使用してシステムにアクセスしている在宅勤務の従業員は、アクセス手段を失い、会社が最も人手を必要としているその瞬間に人手不足に陥ることになります。

CNCは、DNSインフラやドメイン名、デジタル証明書管理を強化し、保護することの重要性を理解し、Neustar®をパートナーに選びました。Neustar®は過去20年以上に渡り、世界最大かつ最も信頼性の高いDNSネットワークを運用し、DNSセキュリティを強化する6つの方法を推奨しています。*

**本ドキュメントは、Neustarによる「Five Ways Neustar Strengthens DNS Security（NeustarがDNSセキュリティを強化する5つの方法）」に基づいて作成されました。*

1 多層保護でDDoS攻撃を軽減

現在の攻撃では、ボリュームDDoS攻撃は、1秒当たり1テラビット（Tbps）を超えるほど爆発的に増えています。最大規模を記録した攻撃のいくつかは、DNSを狙ったものでした。

DNSをターゲットとしたDDoS攻撃には多くの手法があります。

その一つがDNSアンプ攻撃と呼ばれるものです。この攻撃では、攻撃者は、攻撃対象のIPアドレスになりすまして、インターネット上に存在する膨大な数のオープンDNSサーバーを悪用し、すべての小さな検索クエリに応答することができます。それによりターゲットははるかに大きなDNS応答を受けることになり、あっと言う間に容量を超えます。目標：ネットワーク容量を使い切り、正当なDNSクエリをブロックする。

もう一つの一般的なタイプの攻撃として、DNSフラッドが挙げられます。これは特定のウェブサイトをホストするDNSサーバーを狙う攻撃です。これらは、乗っ取られたボットネットマシンでスクリプトを実行して生成されたUDPリクエストが大量に送信されることで、メモリやCPUなどサーバー側資産を流出させようとする方法です。

DDoSの多層保護

あらゆるタイプのDNS攻撃から防御するには、DDoSの多層保護を使用する対策が有効です。

不正なトラフィックや疑わしい場所から送信される大量のトラフィックを常に監視するため、DNSノードにDDoS軽減装置を備えておく必要があります。多くの場合、緩和措置はローカルで行われます。

攻撃が大規模な場合、悪意のあるトラフィックは完全に独立した専用のインフラである緩和用ネットワークへ自動で再ルーティングされます。これにより、ターゲットのネームサーバーの知的財産に対するダメージを制限できます。影響を隔離することで、年中無休のセキュリティ運用チームがより有効な対策を取ることができます。

2 セグメンテーションでネームサーバーを隔離する

極めて拡張性の高いDNSは、業界全体を通じて、数百または数千の顧客を持つサービスとなりました。それぞれが大量のドメインを抱え、単一ネットワークにクラスターを形成、ネームサーバーを共有しています。

これにより、他の顧客の問題を別の顧客も共有してしまうのです。サードパーティDNSプロバイダーを使用している場合、ネットワークへの攻撃のほとんどは、貴社ではなく、プロバイダーが割り当てたネームサーバーを共有するドメインに向けられます。

DDoS攻撃の影響を隔離するのが賢明です

DNSネットワークをセグメント化するDNSプロバイダーを選択します。各プロバイダーは、少数の顧客グループのみで共有されるネームサーバーアナウンスメントを使用します。ホスト名やIPアドレスを共有している顧客数が少なければ、攻撃の影響を受ける可能性も格段に低くなります。

分かりやすい例にたとえてみましょう。10,000人が入っている大きなホールがあり、ある人が突然立ち上がって叫び出して、スピーチが全く聞こえなったという場面を想像してみてください。また、同じシナリオですが、会場には20人だけいたとしましょう。このとき、スクリーマーの影響は20人に留まります。スクリーマーをDDoS攻撃に置き換えれば、叫び始めた（攻撃が始まった）時、ネームサーバーのセグメンテーションおよびDDoSの攻撃緩和戦略により、行儀のよい観客を会場から防音エリアへ一旦移し、その間にスクリーマーを制止します。影響を受けたのがたったの20人だったことから、攻撃をスムーズに対処することができました。

攻撃を受けたのが自分か他人かに関わらず、あなたは保護されます

このアプローチにより、各ネームサーバーアナウンスメントは、クエリ解決を大きく遅らせることなく、DNSネットワークからDDoS緩和ネットワークへ移送することが可能です。DNSプロバイダーはこういった攻撃に際し、効果的かつ迅速な緩和措置を取る必要があり、DNSネットワークでの副次的な被害を防げるようにしなくてはなりません。

クラウドが提供するDNSサービスを利用する場合、セグメント管理されているサーバーアナウンスメントがDNSトラフィックを保護する効果的な方法なのです。

3 非オープンソースのリゾルバーは避ける

DNS リゾルバー（ドメイン名のリクエストに対応するサーバー）は、正しいサイトへユーザーがルーティングされるようにします。DNS 管理に使用される最も一般的なソフトウェアは Berkeley Internet Name Domain（BIND）です。1983 年カリフォルニア州立大学バークレー校で開発された BIND は今でも世界で最も多くのネームサーバーで使用されています。現在は完全にパブリックドメインとなっている BIND のソースコードはオープンソースとなっているため、悪質なハッカーなどによる不正利用も簡単にできるようになってしまいました。

リゾルバーへの脅威を回避する

CSC が Neustar をパートナーに選んだ理由は、同社がすでに数年前にこの問題を解決していたためです。Neustar は独自のコードを開発し、サードパーティのセキュリティ監査機関に脆弱性チェックを依頼しました。攻撃者は制限された特権を盗んだり、ディレクトリ解決を妨害するために、リモートで悪用できることを発見しました。

DNS の標準仕様や RFC コメントリクエストに対応しているだけなく、DNS 機能を拡張して、リゾルバーを強化し、余分な冗長性とセキュリティの強化も行っています。ほとんどのレガシー DNS サーバー実装とは比べものにならない優れた実装です。

4 DNS セキュリティ拡張機能（DNSSEC）を展開する

インターネットユーザーの求めるサイトを見つけるため、DNS サーバーは互いにクエリを送信します。そのスピードを上げるため、サーバーは指定された時間、クエリの結果をキャッシュとして保存します。リソースレコード期間が切れる前に同じ名前のクエリが来た場合、サーバーは他のマシンにクエリをすることなく、キャッシュされた答えを返します。

ファーミング攻撃を可能にする DNS キャッシュポイズニング

この方法により効率が上がる一方で、キャッシュポイズニングを引き起こすこともあります。これは、通常、犯罪者に侵害された DNS サーバーが、DNS リクエストに対し偽の回答を送った時に発生します。結果としてユーザーが偽サイトへ誘導され、個人情報を要求したり、マルウェアをアクティブにすることもあります。

ポイズニング発生のメカニズムは多くの場合、DNS サーバーは他のサーバーから受け取った応答を元のクエリに関連しているかどうか検証しません。従って、サーバーは不正情報をキャッシュし、侵入されたマシンの他の DNS クライアントに、それを送信します。

保護のカギは DNSSEC

DNSSEC は DNS 応答の認証を可能にするセキュリティ拡張機能セットです。秘密は、情報リソースにサインする公開鍵と秘密鍵を組み合わせることです。これは、ユーザーのリゾルバーが、DNS の回答を暗号化バージョンとマッチできるか確認するために、公開鍵を提供します。すべてのトランザクションが署名されるため、攻撃者はパケットを偽装することが不可能になります。

もっと簡単に言うと、DNSSEC はキャッシュポイズニングやファーミング攻撃、その他の深刻な脅威を防ぐことで、DNS プロセスを保護するのです。これがオンになっているか必ず確認しましょう。

DNSSEC の採用

CSC サイバー セキュリティ レポートによると、過去数年、各種業界を通して大手国際企業による DNSSEC の導入率は 0%～5% と、驚くほど低い数値で推移しています。

5 プライベートDNSネットワークで回復力を強化

英語のことわざに「鎖の強さは、その中の一番弱い輪の強さである」とあるように、セキュリティはあなたの最も弱い部分に左右されます。弱い輪を取り除くことで、対策を強化できるとしたらどうでしょう？パブリックインターネット接続への依存を減らせば、プライベートネットワークは、DDoS攻撃やDNSキャッシュポイズニングの多くが発生しているDNSトランザクションの中間部分（最も危険な部分）を排除しました。お使いのプロバイダーがこういったサービスも提供しているか、ぜひ確認してください。

プライベート導入による重要な3つのメリット

低レイテンシー
場合によっては、DNSが完璧に機能している場合でも、他のインターネット接続の問題によりDNSのパフォーマンスが低下し、ユーザーエクスペリエンスが低下する可能性があります。プライベートネットワークは、DNSトラフィックが一般のインターネットネットワーキングを避けるため、高速かつ効率の良いオンラインエクスペリエンスを提供します。

セキュリティ強化
IoTで力を得て、インターネット接続を妨害する現在のDDoS攻撃は間もなく過去のものとなるでしょう。プロバイダーのネットワーク内DNS情報検索を目的としたプライベートネットワーク設定により、DDoS攻撃やキャッシュポイズニングなど外部からの脅威を最低限にまで減らします。

信頼性向上
DDoS攻撃や重大なダウンなどが発生した場合、クエリはDNSが展開されているプライベートネットワーク内で引き続き解決されます。このような回復力により、ウェブサイトやその他の重要なオンライン資産を探すユーザーには極めて快適なインターネットエクスペリエンスが保証されます。

6 重要なデジタル資産のセキュリティの盲点を特定

企業は業務上重要なドメインを識別し、継続的にモニターして、適切な保護措置が確実に取られているようにしなければなりません。

当社はこの点で企業に支援する会社がないことに着目し、CSC Security Center℠を開発しました。これは、重要なドメインに対する、またはそれが存在しているDNSインフラ内の脅威を把握し、企業にリスクエリアを警告するインテリジェントなプラットフォームです。

この独自のアプローチは、ドメインやDNSの保護方法を変え、企業がセキュリティの盲点をしっかりと把握できるよう支援します。CSC Security Centerは特に次の点でお客様をサポートいたします。

- どのドメインがミッションクリティカルであり、100%のDNSアップタイム保証が必要かを特定する
- 現在のDNSプロバイダーを特定し、ベンダーのセキュリティリスクを評価する
- DNSキャッシュポイズニングやドメインDNSハイジャック、ドメインシャドウイング、DDoS、フィッシングなどのリスクを増加させる不足しているセキュリティ機能を特定する

CSCセキュリティセンターと当社のDNS管理サービスが、サイバー犯罪の脅威からお客様をお守りする方法について、ぜひ詳細をお問い合わせください。

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、企業をサイバー資産からのデジタル資産への脅威から保護し、GDPRなどのポリシーによる、収益の損失、ブランドへの中傷、重大な経済的ペナルティを回避します。CSCは、インターネット資産と共に、偽造サイト、詐欺、IP侵害を介して悪用されるオンラインブランドを保護、監視および緩和し、多くの世界最大手ブランドの保護およびアドバイザリーサービスを提供しています。詳細につきましては、cscdigitalbrand.services/jpをご覧ください。

cscdigitalbrand.services/jp