SOPHOS
Cybersecurity delivered.

ZTNA が重要な理由：セキュリティネットワークの将来

ZTNA はリモートアクセスを保護し、ランサムウェアから企業やデータを保護します。

ソフォス ホワイトペーパー2022年 2月

サイバーセキュリティに関しては、リスクと信頼にすべてがかかっています。ネットワークにログオンしたばかりのユーザー、または企業のアプリケーションにアクセスしようとしているユーザーを信頼しますか？ビジネスパートナーから送信されたように見えているけれども、ビジネスメール詐欺攻撃を示すような通常とは異なる要求やURLが含まれているメールについてはどうでしょうか。「信用しても、確認を怠らない (Trust but verify)」は、1980年代に普及したスローガンとなりましたが、今日、セキュリティ業界の風向きは「何も信頼せず、すべてを検証する」に変わりました。

ゼロトラストモデルでは、ネットワーク上のすべてのユーザーがアクセスを取得するために認証が必要となりますが、それだけではありません。サーバー、アプリケーション、データなどのネットワークリソースにアクセスを試みる際に、リソースへのアクセスに使用されるデバイスまたはアプリケーションもコンプライアンスのために検証され、新しいリクエストが行われるたびに再認証や検証が必要となります。

サイバーセキュリティの観点からは、信頼は付与されるのではなく、獲得するものになります。ユーザー、デバイス、アプリケーションがネットワーク上でアクションを実行するたびに、認証プロセスの再実行が求められます。

ZTNA とは何か？

ZTNA (Zero Trust Network Access) は、「何も信頼せず、すべてを検証する」というゼロトラストの原則に基づいています。これによって、より優れたセキュリティが提供されます。各ユーザー、デバイス、アプリケーションをネットワークの独自のマイクロセグメンテーションの境界のように事実上処理し、企業アプリケーションとデータへのアクセスを許可するために、ID とセキュリティ状態を常に評価・検証します。ユーザーは、ポリシーによって明示的に定義されたアプリケーションやデータのみにアクセスできるため、ラテラルムーブメントやそれに伴うリスクを削減できます。

ランサムウェアの被害者は、ZTNA のアプローチに非常に精通しています。これは、今後の攻撃を防止したいという願望からくるものだと考えられます。このドキュメントの後半で、ソフォスのユーザーの見解や ZTNA テクノロジーをどのように使用するかについて説明します。

ZTNAは、SASE (Secure Access Service Edge) セキュリティフレームワークの基本コンポーネントであり、ネットワークとクラウドのセキュリティがどのように単一のクラウド配信プラットフォームに統合されているかを説明します。2019年に Gartner 社が最初に説明した SASE は、基本的に、クラウドネイティブアーキテクチャを使用して従来の WAN（ワイドエリアネットワーク）管理機能とセキュリティ機能を統合したものとなります。SASE アーキテクチャには、ZTNA に加えて、クラウドアクセスセキュリティブローカー、サービスとしてのファイアウォール (FWaaS)、侵入防御システム、セキュアアクセスゲートウェアが含まれます。

クラウド管理には、すぐに利用を開始できることから、管理インフラの削減、簡単な導入・登録、場所を問わないアクセスに至るまで、大きなメリットがあります。クラウド管理の主なメリットの 1つは、管理サーバーやインフラを追加することなく、ログインしてすぐに利用を開始できることです。また、クラウド管理により、あらゆるデバイスから場所を問わず安全な即時アクセスが可能になり、さまざまな働き方に対応できます。また、ユーザーが世界のどこにいる場合であっても、新規ユーザーを簡単に登録できます。

一方で、ZTNA の導入は、リモートユーザーのセキュリティを向上させ、パンデミックがきっかけとなったリモートユーザーネットワーク環境でのセキュリティを大幅にアップグレードし、マルウェアやランサムウェアの攻撃から企業のネットワークを保護するための重要なコンポーネントとなりました。

VPN の脅威からの脱却

今回のパンデミックは人間界で起きた恐ろしいものでしたが、リモートアクセスの改善に対しては、予想しなかった大きなメリットをもたらしました。それは、脆弱な VPN の代わりに ZTNA を導入するということです。パンデミックにより、数百万人の従業員が企業ネットワークという友好的な場所から離れて、在宅勤務を余儀なくされ、多くの場合、企業の IT スタッフの制御の及ばない数百万の脆弱な新たなエンドポイントが出現しました。

これらのエンドポイントの多くは、企業レベルのエンドポイント保護が適用されていない可能性があるため、攻撃者の恰好の標的です。さらに、新たな何百万人ものリモートユーザーは、このような負荷の高いワークロードを必要としなかった企業の VPN にとって大きな負担となりました。

ZTNA は、リモートユーザーを企業のネットワークに接続する従来のアプローチである問題のある VPN を置き換えながら、ゼロトラストの原則を実現します。技術的に、VPNには、今日の大部分のリモートワーカーにとって重大な欠点が3つあります。

第一に、VPN は、比較的多数のリモート従業員を抱える大企業の要求を満たすようには設計されていません。第二に、VPN クライアントソフトウェアは、古く、放置され、複雑であることがよくあるため、攻撃者の標的になる可能性があります。VPN は、セキュリティに対して従来のユーザー名 / パスワードのアプローチを使用しているため、セキュリティの脆弱性もあります。最後に、VPN を使用してネットワークにアクセスするユーザーは、境界ファイアウォール内のワークステーションと同様に、一旦接続するとネットワークを効率的に実行できます。内部ネットワーク制御によっては、これが問題になる場合があります。

これらの問題と、ZTNA がどのように問題を対処するかそれぞれの項目について説明していきます。

VPN は拡張性に優れていません。制限の中には、VPN の最大帯域幅 (多くの場合 1Gbps に制限されている)、悪用される可能性のある公開ポート、潜在的な中間者攻撃 、過剰な権限が付与されたアクセスがあります。さらに VPN のユーザー使用量は、あらかじめ決まった特定のリモートユーザーの使用量だけを処理するように設計されていることが多く、動的にスケールアップまたはスケールダウンすることはできません。たとえば、ユーザー使用量が大きすぎる場合は、一部のユーザーは、他のユーザーが切断されるまで VPN にアクセスできなくなります。

第二に、アメリカ国家安全保障局は、長年にわたり複数のサイバーセキュリティの報告において VPN の脆弱性があることを指摘しました。2019年には、カナダサイバーセキュリティセンターが、3つの一般的な VPN 製品が悪意のあるアクティビティを検出するための複数の感染の痕跡を持っていたことを発表しました。これらには、認証情報のリセット、および脆弱な独自の SSL / TLS VPN プロトコルが含まれています。

最後に、VPN は、ユーザーをネットワークに参加させてもフィルターは提供されません。基本的に、ユーザーは、企業ファイアウォールの背後にあるワークステーションであるかのように、すべての権限を持っています。

リモートアクセスツールの脅威を減らすには、攻撃者のネットワーク上での移動を制限する 2つの方法があります。一つ目は、ネットワークに接続する際には、ユーザー、デバイス、ソフトウェアを、ネットワークの特定のマイクロセグメントでのみ認証するよう要求します。攻撃者がアクセスに成功したとしても、移動は制限されます。二つ目は、ネットワーク上のすべてのユーザーの権限を大幅に制限します。攻撃者は制限された権限のためにネットワークを参照することができなければ、水平移動することはできません。

Forrester New Wave 社の 2021 年第 3 四半期、Zero Trust Network Access によると、「ZTNA を使用すると、ユーザーはゼロトラストの原則を使用してオンプレミス型アプリケーションにアクセスできると同時に、双方向のビデオ会議のトラフィックをインターネットに直接送信できるため、セキュリティポスチャと従業員のエクスペリエンスが向上します。」と述べられています。「最終的に、ZTNA は従業員の VPN の必要性を減らし、インフラストラクチャチームとセキュリティチームがクラウド配信のネットワーク機能とセキュリティ機能を採用できるようにします。」

ZTNA でセキュリティ向上

コーポレートガバナンスの観点から、誰がネットワークに接続し、何をしているかを管理することは、企業の重要な関心事の一つです。企業の運営方法を決定する方針と手続きを持ち、財務的な存続につながる堅実で倫理的な事業活動を行うことが、コーポレートガバナンスの機能目的です。例えば、悪意ある攻撃者がネットワークに侵入し、機密データを盗んだり、ランサムウェアやその他のマルウェアをインストールしたり、あるいは単にステルスモードで攻撃のタイミングを待っていることもあり得ます。これは、コンプライアンス規制に違反し、企業に多額のコストをもたらすだけではなく、企業の市場価値を大幅に低下させる可能性があります。

一般的にゼロトラストネットワークモデル、特にZTNAを導入すると、ネットワークの侵入者、悪意 / 良性のアプリケーション、所属していないユーザーを特定するだけではなく、企業ネットワークの攻撃対象領域を大幅に減らし、企業全体のリスクプロファイルをさらに向上させることができます。

ユーザーが ZTNA を備えた企業ネットワークにアクセスすると、デバイスは、常に評価、検証される独自のマイクロセグメント化された境界上のネットワークリソースにアクセスします。ゼロトラストでは、従来の「企業ネットワーク上」にある場合と異なり、暗黙的な信頼とアクセス権はなくなります。代わりに、認証されたユーザーやデバイスのネットワークの部分にのみアクセスできます。このことは、従来の VPN 接続の場合には当てはまりません。

従来のネットワークでは、企業のファイアウォールが攻撃者の侵入を防いでいましたが、侵害したユーザーの認証情報が承認されると、攻撃者は自由に動き回り、ネットワークのより安全な部分にアクセスできる認証情報を探して、データを盗み、コピーし、破壊し、暗号化して身代金を要求することが可能になります。

ゼロトラストインフラストラクチャを実装すると、認証情報の盗難が減るだけでなく、企業のファイアウォールはデータやアプリケーションに対する多くの防御手段のうちの最初の1つに過ぎなくなります。在宅勤務の従業員のコンピューターが侵害された場合でも、攻撃者が企業のネットワークにアクセスした時点で、ユーザーの認証情報は十分ではありません。

ZTNA アプローチでは、ネットワークの限られた部分へのアクセスしかできません。これは、承認されたアプリやデータのデバイスおよびソフトウェアを認証するための認証情報を持っていることが前提となります。

ランサムウェアを打開

ソフォスのランサムウェアの現状 2021版レポートによると、回答者の 37% が前年にランサムウェア攻撃を受け、54% がサイバー犯罪者によりデータが暗号化されたと回答しています。

良いニュースは、データ流失の観点から見ると、回答者の 96% が少なくとも一部のデータを取り戻したということです。しかし、悪いニュースは、身代金を支払ってもすべてのデータが取り戻されることはめったにないということです。暗号化されたデータのうち、身代金の支払い後に復元されたデータは 65% だけでした。

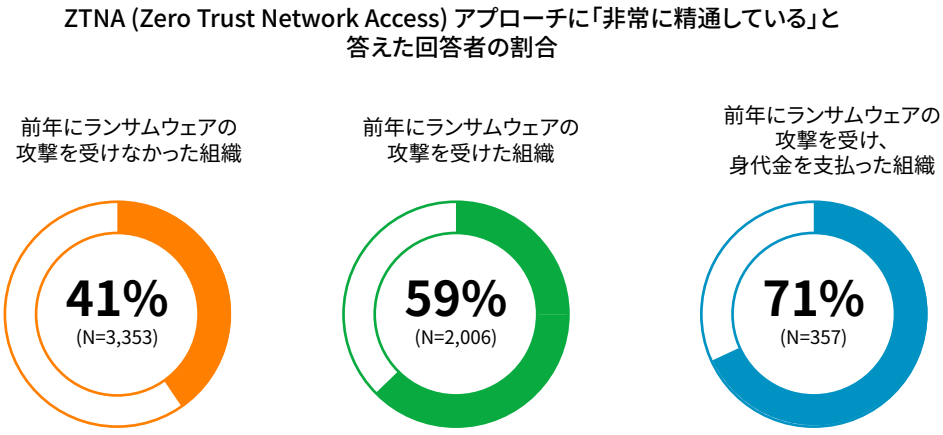
報告書によると、中堅規模の組織が 2020年に支払った身代金の平均額は 170,404 米ドルでした。ただし、これは全体的な修正請求額の一部にすぎません。直近のランサムウェア攻撃の影響を修復するために要した平均費用 (ダウンタイム、人件費、デバイスのコスト、ネットワークのコスト、逸失利益、支払った身代金およびその他のコストを含む) は 185 万米ドルで、2020年に報告された費用 (761,106 米ドル) の 2 倍以上であったと回答しています。

Vanson Bourne 社が世界的に実施し、ソフォスが引き受けた 5,400人の IT 専門家を対象とした最近の調査では、回答者の 20% がすでにゼロトラストアプローチを実施していると述べ、他の 41% はゼロトラストの導入をすでに開始し、2022年の年頭までには導入を完了する予定であると述べています。さらに別の 20% は、2023年の初頭までには完了する予定だと回答しています。

ZTNA ソリューションは、ランサムウェアやその他のネットワーク侵入攻撃の一般的な攻撃手法を排除します。ZTNA ユーザーはもはや「ネットワーク上」ではなく、企業のネットワークのマイクロセグメント上に存在しているため、VPN を介して足がかりとなる可能性のある脅威は、ZTNA では行く場所がありません。

ランサムウェア攻撃が ZTNA の導入を促進

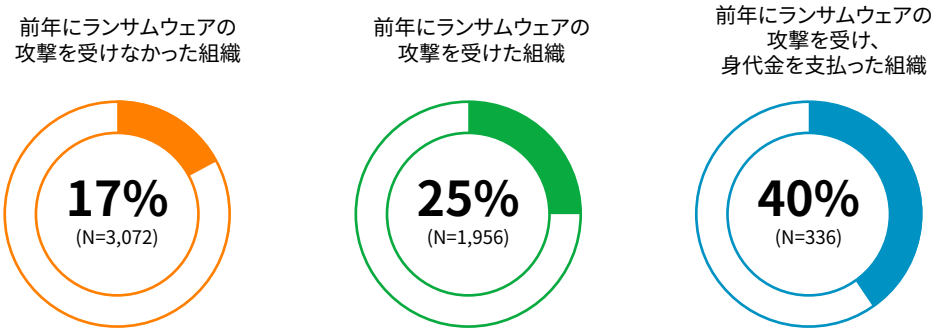
前年にランサムウェアの被害を受けた組織の IT 専門家は、被害を経験していない組織の IT 専門家よりも、ZTNA アプローチに「非常に精通している」傾向が約 50% となっていることが調査で示されています（59% 対 39%）。攻撃を受け、身代金を支払った組織は 71% となりました。



この点をさらに説明すると、ランサムウェアの被害者のわずか 10% が、被害者とならなかった 21% の組織と比べて、ZTNA にほとんど、またはまったく精通していません。

また、この調査では、ランサムウェアの被害者の方がゼロトラストの採用において、より進んでいることが示されています。前年にランサムウェア攻撃を受けた組織の 4分の 1（25%）は、すでにゼロトラストアプローチを完全に採用しているため、攻撃を受けて、身代金を支払った組織は 40% となっています。それに対して、攻撃を受けたことがない組織の 6 分の 1 (17%) は、すでにこのアプローチに完全に移行しています。

ゼロトラストアプローチをすでに採用している組織の回答者の割合



加えて、ランサムウェアの被害者は、ZTNA を採用する動機が異なっています。

- 回答者は、ゼロトラストアプローチを採用する同期について質問を受け、そこには、いくつかの共通点はありましたが、明確な違いもありました。被害者と非被害者の両者の中で最も一般的な動機は、全体的なサイバーセキュリティ対策を改善することでした
- ランサムウェアの被害者の間で 2番目に多い動機は、「サイバーセキュリティ運用の簡素化」への欲求 (43%) であり、複雑なセキュリティが前回の攻撃に寄与したことを反映している可能性があります
- また、ランサムウェアの被害者は、「 CAPEX から OPEX モデルへの移行」が、ゼロトラストアプローチの採用を支えている主な要因の 1つであると言う可能性も高くなりました (27% 対 16%、ランサムウェアに見舞われ、身代金を支払った組織のうち 34%)
- ランサムウェアの被害者は、「クラウドの使用拡大に向けてソフォスが移行をサポートしている」ことが大きな動機にもなっています (42%)。これにより、最近の攻撃を受けていない組織が 30% に減少しました

今後の展望

攻撃者がマルウェアを仕掛ける前に停止したために、攻撃に失敗したのか、それとも単に発生しなかったかを証明するのは難しいことがあるため、ゼロトラスト環境の利点を上級管理職や株主に説明するのは難しい場合があります。とはいえ、ゼロトラストによりリスクを大幅に減少させることが、企業の収益化にもつながることを実証することは可能です。

たとえば、企業のリスクを軽減することで、保険料のコストを削減したり、サイバー保険の条件を改善し、企業の評価を高めることができます。サイバー保険ブローカーや保険会社は、リスクが低いほど請求が低くなり、保険金の支払いも少なくなることを理解しています。その結果、サイバー保険業界は現在、このようなポリシーを作成するための利用規約を再評価および変更しており、リスクを積極的に削減する企業に対してより良い条件を提供しています。

2021年 5月にジョー・バイデン大統領が発行した米国のサイバーセキュリティ改善に関する大統領府令では、連邦政府は「セキュリティのベストプラクティスを採用し、ゼロトラストアーキテクチャに向けて前進を必要とする」と述べています。連邦政府によるゼロトラストモデルの採用は、このアプローチがリスクを軽減する前進への道と見なされていることを明確に示しています。

Gartner 社も、ゼロトラストこそがサイバーセキュリティの将来の道であると考えています。「道の途中にある大企業も道を歩き始めたばかりの大企業も共に、データを保護することは最優先事項である必要があります」と Gartner 社は述べています。Gartner 社によると、82% の企業が、従業員がしばらくリモートで勤務できるように計画をしています。「企業がリモートワーカーを長期計画に組み込み始めているので、セキュリティが優先事項になってきています。しかし、多くの企業は、従来のセキュリティアプローチがクラウドネイティブのリモートワーカーには適していないことに気づき始めています」と Gartner 社は述べています。

また、Forrester 社もこれに同意しており、ゼロトラストは物理的なネットワークではなくリソースを保護するものだと考えています。Forrester 社は、「簡単に言えば、ゼロトラストモデルは、さまざまな種類の認証やアクセス制御から、機密データストア、アプリケーション、システム、およびネットワークに関する状況に合わせた制御へと焦点を移します」と述べています。「これらの制御は、ID を活用し、ユーザーのコミッション / デコミッションを行い、定義された役割に基づいてアクセスを仲介します。」

将来がゼロトラスである場合、すべてはネットワーク上の誰が、何に、どのようにアクセスできるかを制御することから始まります。これが ZTNA の大切なことであり、サイバーセキュリティが将来にとって不可欠であるかの理由です。

詳細は以下をご覧ください
sophos.com/ztna

ソフォス株式会社営業部
Email: sales@sophos.co.jp

22-02-06 JP (MP)