FEDERAL NEWS NETWORK

エグゼクティブブリーフィングシリーズ：

ゼロトラストアーキテクチャ

Sponsored by TANIUM

TANIUM

ゼロトラストの実践に向けて

新たな戦略による大胆な対応で、サイバーセキュリティ対策を最新化

柔軟性が高く動的な ゼロトラストネットワークを構築する方法

著者：トム・テミン

連邦機関はホワイトハウスからの大統領令と、実際のサイバーセキュリティの強化の両方への対応に迫られており、ゼロトラストモデルを迅速に推進し、ネットワークへのアクセスを制御しようとしています。そして、ゼロトラストはまるでケーキのようにさまざまな要素で構成されており、一度組み合わせると分割するのは困難であることに気づき始めたのです。「ゼロトラストとは、マインドセットである」と言われています。それは正しくもありますが、一方でゼロトラストは、技術的な戦略、製品、手順を意味することもあります。マインドセットを定量化することは難しいですが、ゼロトラストは実際の作業が伴い、投資の対象となるものであることから、マインドセットと完全に同義というわけではありません。

米国中小企業庁(SBA)の最高技術責任者であるサンジェイ・グプタ氏は次のように述べています。「ゼロトラストアーキテクチャとは概念であり、戦略であり、マインドセットです。サイバーセキュリティに対する考え方の本質的な転換を指すものとも言えます。このように、ゼロトラストにはさまざまな側面があるのです」

グプタ氏は、ゼロトラストは基本的に境界防御モデルに取って代わるものだとも話します。

「ゼロトラストは『境界防御モデル』の考え方を180度転換しました。環境内の各要素をすべて保護しなければならないと考えるようになったのです。データ、アプリケーション、デバイスといったそれぞれの資産は、それ自体を保護する必要があり、本質的には何も信用しないという考え方です」

これは、境界のファイアウォールがその先にあるものをすべて保護するという境界防御モデルの前提とは対極の考え方になります。

グプタ氏は、Federal News Networkが主催した連邦政府のエキスパートや業界のサイバーセキュリティ担当者によるパネルディスカッションで自身の見解を述べました。ここでは、ゼロトラストを実現するために、実際に何をすべきかについてディスカッションが行われました。

すべてを包含するアプローチ

ゼロトラストは、多くの公的機関で採用されているハイブリッドのコンピューティングモデルに対する統合的アプローチにもなるとグプタ氏は語ります。「ゼロトラストは、オンプレミスのコンピューティングモデル、クラウドコンピューティングモデル、モバイルコンピューティングモデルの枠にとらわれないものです」

米国国務省のITインフラストラクチャ部門ディレクターであるロブ・ハンキンソン氏も、この点を強調しています。

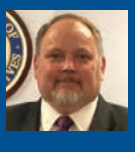
「クラウドを考慮すべきです。また、海外の270拠点で開発されたオンプレミスのソリューションも忘れてはなりません。さまざまなデータセンターアプリケーションの存在を把握し、対応する必要があります」

エキスパートパネル

サンジェイ・グプタ氏 米国中小企業庁(SBA)最高技術責任者(CTO)

マシュー・マースデン タニウム行政機関担当テクニカルアカウントマネジメント部門バイスプレジデント

ロブ・ハンキンソン氏 米国国務省 ITインフラストラクチャ部門 ディレクター



ランディ・ビッカース氏 米国下院 最高情報セキュリティ責任者(CISO)

ハンキンソン氏は、米国にはすでにゼロトラストのテクノロジコンポーネントが多数導入されていると話します。しかし、それらは再構成が必要で、中にはデュアルモードで運用しているものもあります。総合的なプランニングを進めている段階で、NIST Special Publication 800-53で概要が提示されているサイバーセキュリティの制御や、国防総省のゼロトラストロードマップに対し、IT資産のマッピングを行っています。

「現在ギャップ分析を進めており、こうした分析は、共通の制御プロバイダ、アイデンティティプロバイダ、データプロバイダと共に行っています。ソリューションアーキテクチャを構築するために、こうしたプロバイダと協業しています。

そのアーキテクチャがあれば、IT担当者が今何を所有していて、何を調達すべきか、どのような資金が必要で、いつ投入すべきかを把握できるようになるからです」とハンキンソン氏は語ります。

ゼロトラストアーキテクチャの基本的な要素に、アイデンティティ(ID)管理があります。米国下院の最高情報セキュリティ責任者(CISO)ランディ・ビッカース氏は、下院ではそれが最初の関門だったと述べています。

「部署も職責も変わらない人が必要になるからです」

ある人に特定のリソースに限定した権限を付与しても、職責の変更や離職・復職の際には別のリソースに対する権限が必要になります。

「それでも、まずはIDから対応すべきです。環境のプロビジョニングを行う場合はIDを検証することが必要不可欠です」とビッカース氏は話します。

ビッカース氏によると、下院では公開鍵(パブリックキー)インフラシステムの構築が進められており、IDとアクセスのセキュリティを保護するために暗号化を組み込もうとしています。

ゼロトラストを効果的に実現するには、テクノロジのサイロ全体にわたって、個人とさらにはロボットによるプロセスに信頼性のある単一のIDを使用する必要があります。

「環境内に複数のIDソリューションを導入するのではなく、サイロを解消し、エンタープライズレベルでIDソリューションなどを検討しなくてはなりません」とグプタ氏は語ります。

エンドユーザの観点から

米国国務省のように世界各地での業務が発生する場合、位置情報サービスがゼロトラストに影響を及ぼしますが、このように、国外での業務には本土とは異なるデバイスが必要となることがあるとハンキンソン氏は指摘しています。ビッカース氏は議会でも同様に、定期的に本土外に出張することがある議員や職員は、ゼロトラストの実装について考慮しなければならない場合があると述べています。

考慮すべき事項が複雑になり得るため、データセットのレベルまでチャレンジレスポンス認証が必要となることもあります。

「データセットについて考慮する際、あるデータセットでゼロトラストを実現するためのロードマップは、すぐ隣にあるデータセットや組織内の別の場所にあるデータセットとは根本的に異なる可能性があります」とハンキンソン氏は話します。

テレワークの普及や、BYOD（個人所有デバイスの業務使用）ポリシー導入の拡大も、ゼロトラストの実装をいっそう複雑にしています。

タニウムのテクニカルアカウントマネジメント部門バイスプレジデント、マシュー・マースデンは、このような状況の中で「社員、文化、マインドセットに投資し、システムを活用する人に最小権限という前提を理解してもらい、『バッジがあれば何にでもアクセスできる』という考え方から脱却する必要がある」と示唆しています。

ゼロトラストにおいては、IDの検証に加え、ユーザがログインに使用するIDとデバイスの両方に対する継続的なアセスメントと認証が必要です。

このプロセスには基本的には3つのコンポーネントがあります。1つ目がユーザの認証、2つ目が多要素認証（SAMLに基づくことが望ましい）によるログインの許可、そして3つ目がデバイスの認証です。

デバイスの認証においては、スマートフォンやPCが会社支給のものか、プライベートで利用しているものかを区別する必要もあります。

マースデンは「次に、これらの2つの要素に基づいて、ポリシーの動的な割り当てが必要となります」と話します。

会社支給のパソコンなど既知のデバイスを使う信用できるユーザに表示する内容と、信用できるユーザであっても、未知あるいは信用できないデバイスを使用する場合に表示する内容は違うものになります。そして後者では、一部のデータにアクセスできない場合もあります。

マースデンはさらにこのように述べています。「ユーザやデバイスの要件が変化することで、ネットワーク上には新たな脆弱性が生まれることがあります。あるいはデバイスの状態が変化することもあります。このため、認証やアクセスを常に評価し、必要に応じて即座にポリシーを適用する機能が必要になります」

規模やユーザ数、取り扱うデータの範囲を考慮すると、政府機関は手作業ではとても対応できない膨大なデータを扱わなければなりません。

「これには、機械学習や人工知能などのツールを活用した大規模な自動化が必要になります。これは基本的には皆さんがお考えのとおり、すべての情報を投入すると、動的エンジンがその人のその時点でのアクセスレベルを即座に判断して表示する仕組みです」とグプタ氏は語ります。

デバイスの所有者は誰か?

グプタ氏は、支給されたデバイスのみがアプリケーションやデータにアクセスできるというポリシーをSBAが改訂したことについて言及し、実際に「私たちがこのポリシーを廃止した」と話します。

その理由は非常にシンプルです。パンデミックの初期に議会が官庁に数千億ドルの救済金を配布することを指示した際、SBAは雇用する職員全員に配布できる数の端末を用意できなかったのです。

「職員の生産性を向上する必要がありましたが、十分な数のノートパソコンを用意できませんでした」

その解決策となったのが、グプタ氏の言うところの条件付きアクセスです。これをリスク管理フレームワーク内で実行することで、従来の制約事項を回避できるようになったのです。

そこで、デバイス調査として知られるプロセスが効力を発揮します。調査から検証へ、そして適切だと判断されれば、認証へと進みます。デバイスにパッチが適用されているか、ポリシーに則って設定されているか、ユーザが承認済みの認証リクエストの方式を使用しているかという情報を調査し、自動認証プロセスに提供します。「これにより、認証済みのユーザが今使用しているデバイスでネットワークへのアクセス権を持っているかを情報に基づいて判断できるようになります。そして、ユーザやデバイスに付与された特権や権限に応じて、適切な動的ポリシーを適用するのです」とマースデンは語ります。

最終的には、ゼロトラストアーキテクチャは連邦機関のリスク管理フレームワークのもとで運用されるべきであるというのが、パネリストに共通する見解です。情報の機密性はそれぞれ異なるため、すべてのアプリケーションやデータベースを同じように扱う必要はありません。

ビッカース氏は「誰でもアクセスできるアプリケーションのみを使用する場合にも、さまざまな確認をすべて行う必要があるのか?と問われれば、その答えは『ノー』でしょう。しかし、別の場面では、たとえユーザから不満の声が上がっても、各種確認を行う必要が生じることもあります。どのようなリスクを軽減しようとしているのか?どのようなリスク体制を維持または変更しようとしているのか?といったことが鍵となります」

機密情報を扱うネットワーク上の信頼できるデバイスから公共のWi-Fiを使用した個人所有のスマートフォンまで、あらゆる環境に対応できるゼロトラストがポリシーとして目指すべきところです。そのため、ソリューションにはどれ一つ同じものはありません。

「ゼロトラストの実装には一つの答えがあると期待しているかもしれませんが、そうではありません。ゼロトラストの実装がどれも同じだと期待すべきではないのです」とグプタ氏は述べます。

しかし、ゼロから着手する必要はないとビッカース氏は話します。「実装について他社の事例から学ぶことができます。そこから、自社に適用できる要素やフレームワークを取り入れればよいのです」