FORTINET

WHITE PAPER

デジタルイノベーションの実現に欠かせないゼロトラストアクセス

攻撃対象領域の拡大に伴い、新たなリスクに直面する CISO

概要

ビジネスを加速させ、競争力を維持するため、企業はデジタルイノベーション（DI）イニシアチブの採用を急ピッチで進めています。これは、ビジネスアプリケーションやデータが会社から遠く離れた場所に分散したことで、従業員がさまざまな場所から数多くの企業資産にアクセスできるようになったことを意味します。このため、従来の境界は消滅しつつあり、拡大する攻撃対象領域に内部ネットワークが取り込まれ始めています。これは CISO にとって最大の懸念事項です。

組織がこのような脅威に対応するには、「誰も何も信じない」というアプローチでセキュリティに取り組む必要があります。具体的には、CISO はゼロトラストアクセス（ZTA）ポリシーに基づいてネットワークを保護することで、すべてのユーザーとデバイス、そしてクラウドからのすべての Web アプリケーションが信頼され、認証され、適切なアクセス権を付与されるようにする必要があります。ゼロトラストは、個々のプロジェクトの特性に関係なく、デジタルイノベーションを実現する上で不可欠です。

組織のリーダーの 81% が、モバイルセキュリティの最大のリスクは従業員であると回答しています [1]。

ネットワークエッジの進化

あらゆる規模の企業において、DI イニシアチブはビジネスの成長を促進するものです。成長の 1 つの側面として、新しいネットワークエッジの普及が挙げられます。プライベート / パブリッククラウドインフラストラクチャ、IoT（モノのインターネット）やモバイルデバイス、ソフトウェア制御（SD）型の支社などのネットワークエッジでは、データ、アプリケーション、ワークフローの量が急増しています。ユーザーのアクセスを管理し、ネットワーク内部と外部の両方でさまざまな場所にあるデバイスを相互接続するため、企業はこうしたネットワークエッジに配備するデバイスの数を増やしています。

これは CISO にとって悪夢のような出来事です。近年、ネットワークエッジが爆発的に増加していることで、従来型の境界線は意味をなさなくなり、攻撃しやすいオープンな環境が誕生しています。サイバー脅威はますます増殖し、絶えず適応しています。かつての境界セキュリティは、「信頼せよ、されど検証せよ」というアプローチに基づいていました。しかし、ネットワーク上には非常に多くのユーザー、デバイス、アプリケーションが存在しており、信頼できる対象を判断するのは困難です。認証情報の窃取やマルウェアなどのエクスプロイトにより、攻撃者は正規のアカウントにアクセスできるようになります。また、侵入に成功した攻撃者は、水平移動する方法を容易に特定し、フラットで信頼されている内部ネットワークを利用して瞬時に拡散します。エッジデバイスにアクセスできるようになると、侵入者は攻撃を開始して、業務のダウンタイム、データの窃取、金銭的損失、評判の失墜などを引き起こす可能性があります。

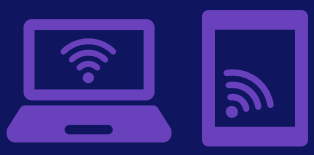
セキュリティリーダーにとって、従来のネットワークアクセスの方法では、増加する攻撃に対応することは不可能です。ネットワーク上のすべてを信頼するモデルから、すべてを信頼しないモデルへの転換が起こっているのはそのためです。ゼロトラストアクセスモデルがうまく機能していれば、CISO はネットワークエッジの中で信頼できないと考えられる特定の脆弱なエリア（ネットワーク内外のユーザー、デバイス、資産）に基づいてアプローチを整理することができます。

誰がネットワークに接続しているかを把握する

セキュリティリーダーは、誰がネットワークに接続しているかを常に把握する必要があります。しかし、従業員が脆弱なパスワードを使ってネットワークに接続している場合、組織のリスクは高まります。現在、多くのアカウントが認証を必要としているため、単純すぎるパスワードが数多く使用されており、フィッシング攻撃などによって簡単に盗まれてしまいます。組織にとっては、すべてのユーザーを把握し、ユーザーが社内でどのような役割を果たしているかを知っておくことが重要です。その情報があって初めて、それぞれの役割や職務に必要なリソースへのアクセスを安全な方法で許可し、他のユーザーにはケースバイケースで追加のアクセスを許可することができます。

BYOD（私用デバイスの活用）は、ユーザーや管理者の間では人気があるため考慮が必要ですが、CISO の中には危険性を見落としている人もいます。攻撃対象領域が広がるため、進化した脅威が従来の境界防御を突破して内部ネットワーク内を水平移動することが容易になります。これが、セキュリティ侵害が長期間発見されない原因の 1 つです。甚大な被害をもたらすセキュリティ侵害の一部は、不正ユーザーによるネットワークへのアクセスや、信頼されているユーザーに対する不適切なレベルのアクセス権付与が原因で発生しています。企業内では BYOD が定着し始めていますが、セキュリティリーダーの 83% は、自社組織がモバイル脅威のリスクにさらされていると回答しています [2]。

企業が直面しているもう 1 つの課題は、従業員の地理的な分散です。従業員は、本社、支社、キャンパス、さらに最近ではホームオフィスなど、さまざまな場所で仕事をしています。多くのユーザーがリモートでネットワークにアクセスするようになったことで、攻撃対象領域は拡大しています。たとえば、従業員はコーヒーショップ、空港、自動車、公共交通機関などで、ホットスポットや公衆 Wi-Fi を使って接続します。このような接続は、重大なセキュリティリスクをもたらします。ユーザーと企業ネットワークの間でやり取りされるすべての情報は、第三者に盗聴される可能性があります。攻撃者は、パッチが適用されていないソフトウェアの脆弱性を悪用してエンドポイントデバイスにマルウェアを注入することで、ローカルの情報にアクセスできるだけでなく、エンドポイントデバイス経由で企業ネットワークにアクセスできます。



近年、組織が甚大な被害を受けた攻撃の多くは、エッジのネットワーキングデバイスを標的としたものです [3]。

テレワーカーが過半数を占める環境では、こうした課題が特に深刻化するという事実を、2020 年の COVID-19 パンデミックの際にすべての組織が目撃しました。それまでは、リモートワークの従業員の割合を 15% 未満と想定していたほとんどの組織が、突如 90% 以上の従業員に適切なインフラストラクチャとセキュリティ管理を提供しなければならなくなりました。

このようなニーズがあるからこそ、ゼロトラストアクセスが重要になります。デバイスはネットワークとの接続と切断を頻繁に行っているため、セキュリティリーダーはどのユーザーがネットワークに接続しているのか、そしてそのユーザーが適切なレベルのアクセス権を持っているのかを把握することが重要となります。また、営業部門から業務部門への異動など、従業員の役割が変わるタイミングで、それまでの役割と同じ領域へのアクセスが不要になることがあります。その場合、セキュリティチームはシームレスな移行を実現する必要があります。

何がネットワークに接続しているかを把握する

セキュリティリーダーは、誰がネットワークに接続しているかだけでなく、どのデバイスが接続しているのかも常に把握する必要があります。しかし、モバイルデバイスや IoT 製品が普及したことで、従来のネットワーク境界は分解されて多くのマイクロ境界となり、その結果、組織の攻撃対象領域は大幅に拡大しています。それぞれのマイクロ境界は各ユーザーデバイスに関連付けられているため、エンドポイントはマルウェア感染や高度なエクスプロイトの格好の標的となります。

このようにエンドポイントが爆発的に増加し、攻撃対象領域が拡大した結果、どのデバイスがネットワークに接続しているのかがもはや把握できていないという点で、多くの組織はネットワークを根本的に制御できなくなっています。実際、BYOD や IoT にはデバイス構成標準が実質的に存在していません。BYOD に関して言えば、モバイルデバイスがネットワークを大きなリスクにさらす可能性があります。その原因として、データ漏洩、セキュリティ保護されていない Wi-Fi、ネットワークスプーフィング、フィッシング、スパイウェア、解読可能な暗号、不適切なセッション処理などが考えられます。しかし、エンドポイントの攻撃対象領域が最も拡大しているのは、IoT デバイスの爆発的な増加によるものです。

組織がより多くの「スマート」デバイスをネットワークに接続しているため、IoT デバイスに対するサイバー攻撃が急増しています。攻撃者はこれらのデバイスを悪用して、分散型サービス拒否（DDoS）攻撃やその他数々の不正活動を行っています。

BYOD や IoT のエンドポイントを完全に保護するためには、各デバイスがどこにあり、何をし、どのような方法でネットワークトポロジー上の他のデバイスに接続するのかを可視化する必要があります。可視性が欠けている組織は、目に見えないリスクに対して脆弱になります。セキュリティリーダーは、ネットワークのエッジにあるデバイスを追跡できなければなりません。しかし、サイバーセキュリティの専門家の 10 人中 9 人が未来の脅威に対して懸念を表明しているにもかかわらず、約半数は IoT デバイスへの攻撃に対処する計画がないと回答しています [4]。

一部の組織では従来型のネットワークセグメンテーションが採用されていますが、すべての承認済みユーザーとアプリケーションが同時にアクセスでき、他のすべてのユーザーは一切アクセスできないような安全なネットワークベースのセグメントを定義することは困難です。ベストエフォートのセグメンテーションであっても、ネットワークアーキテクトが想定していなかったアクセス方法など、ネットワーク防御にギャップが生じ、攻撃者に悪用される可能性があります。

さらに、検証済みデバイスの信頼性に基づいてアクセスが許可されている場合、組織は攻撃を受け続けることになります。それまで信頼していた従業員や契約社員から攻撃を受けて驚く企業は後を絶ちません。また、デバイスの紛失や盗難によってパスワードが漏洩し、将来的にネットワークが攻撃を受ける可能性もあります。これが、ゼロトラストアプローチが極めて重要な理由です。サイバー犯罪者が多様なネットワークデバイスへの攻撃に重点を置いていることを受け、セキュリティリーダーは、ネットワークに接続しているすべてのデバイスの可視化と検出機能を向上させる必要があります。

ネットワーク内部と外部の両方で資産を保護する

セキュリティリーダーにとってもう 1 つの重大な問題は、モバイルデバイスがオフラインや他のネットワークで使用されるケースが増えていることです。これらのデバイスが企業ネットワークに再びログインすると、マルウェアやボットネットなどのセキュリティ脅威が発生します。たとえば、多くの従業員は、BYOD デバイスを個人的なニーズと業務の両方に使用しています。ネットワークにログインしていないときには、インターネットの閲覧、ソーシャルメディアでの他のユーザーとの交流、個人的な E メールの受信などを行っています。しかし、オンライン状態からネットワークに再び接続した場合に、ウイルス、マルウェア、その他のエクスプロイトなど、さまざまな脅威にデバイスや企業リソースが不用意にさらされる可能性があります。

企業ネットワークの外側にあるエンドポイントデバイスを監視する機能がない組織は 63% を占めています。また、過去 12 ヵ月でマルウェア感染エンドポイントが増加した企業は、全体の 53% にのぼります [6]

このようにデバイスの私的利用と業務利用が混在していることで、多くの企業はネットワークに出入りするエンドポイントの数に対応しきれなくなっています。Ponemon Institute が最近発表したレポートでは、企業の 63% がオフネットワークのエンドポイントを監視できていないと回答しており、半数以上の企業がエンドポイントデバイスのコンプライアンス状況を判断できないとしています [5]。膨大な数のデバイスがネットワークに接続されているため、すべてのエンドポイントを可視化することが困難になっています。その結果、CISO とセキュリティチームは、大量に発生するリスクの管理に苦慮しています。

すべてのデバイスを識別、セグメント化し、継続的に監視する ZTA フレームワークに移行することで、組織は高リスクでフラットなネットワークの置き換えが可能となるため、内部リソースのセキュリティが確保され、データ、アプリケーション、知的財産は保護された状態を継続できます。この戦略によって、境界中心のセキュリティ戦略に伴うリスクが軽減されるだけでなく、オフネットワークのデバイスの可視化と制御が強化され、ネットワークとセキュリティの管理全体が簡素化されます。

結論：必要なのはゼロトラストアクセスのアプローチ

DI イニシアチブは、ビジネス成果を加速させます。また、DI イニシアチブは、企業の攻撃対象領域を拡大 / 変化させ、サイバー脅威で悪用可能な新たな攻撃ベクトルを生み出すため、CISO やセキュリティチーム、およびセキュリティリソースにとって負担となります。攻撃者はますます巧妙になって進化しており、従来の境界セキュリティアプローチではもはや対応できません。脅威の性質や巧妙さにもよりますが、企業のセキュリティインフラストラクチャにおいて、たった 1 つのポイントから脅威のあらゆる側面を把握することはできません。ゼロトラストアクセスを採用すれば、CISO はネットワークに接続するユーザーやデバイスに焦点を絞ってアイデンティティを確認し、適切なアクセス権と信頼を確保することができます。

攻撃対象領域が拡大している主な理由の 1 つは、ネットワークに接続される IoT デバイスやスマートデバイスの急増です。多くの場合、セキュリティリーダーはネットワークにアクセスする膨大な数のデバイスを完全に可視化できません。そのため、CISO は「目に見えないものによって被害がもたらされる」という厳しい教訓を学んできました。このようなエンドポイントデバイスを完全に保護するには、企業はネットワーク全体にゼロトラストアクセスポリシーを導入し、各デバイスがどこにあり、何をしていて、ネットワーク上の他のデバイスとどのように接続しているかを可視化するとともに、脅威の兆候となる異常な振る舞いを検出するための継続的なモニタリングを行う必要があります。

セキュリティリーダーは、さまざまな場所で作業をし、個人のデバイスと仕事用のデバイスの両方を使用してネットワークにアクセスする従業員を管理するために、ネットワークエッジですべてのエンドポイントを保護する方法が必要です。組織はゼロトラストアクセスのアプローチを採用することで、ネットワーク内外の全デバイスの可視性を向上させ、高度な保護機能を実現し、動的なアクセス制御を導入しながら、攻撃対象領域の縮小が可能になります。

[1]「Mobile Security Index 2019」、Verizon、2019 年（英語）：https://enterprise.verizon.com/resources/reports/mobile-security-index/2019/executive-summary/

[2] 同上

[3]「Living on the Edge」、Neil Jenkins、Natasha Cohen 共著、Cyber Threat Alliance、2019 年 4 月 30 日（英語）：https://www.cyberthreatalliance.org/living-on-the-edge/

[4]「Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices」、Help Net Security、2019 年 11 月 8 日（英語）：https://www.helpnetsecurity.com/2019/11/08/handle-attacks-iot-devices/#:~:text=Fewer%20than%20half%20(47%25),Security%20Council%20(NISC)%20research.

[5]「The Cost of Insecure Endpoints」、Ponemon Institute、2020 年

[6] 同上

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Securing-Digital-Innovation-202104-R1