ホワイトペーパー

5Gネットワークトラフィックのセキュリティ確保のために考慮すべき重要事項

verizon

IoT（モノのインターネット）の導入が劇的に増加していることもあり（2025年までにデバイスの数は310億台から750億台にまで増加することが予測される[1]）、企業データの膨大な増加によって、ITエンジニアには、データのセキュリティとガバナンスを確保しつつ、ネットワークの高速化とデバイスの高密度化の実現が求められています。今年度のベライゾンのデータ漏洩/侵害調査報告書（DBIR）では、すべての侵害の90%近くが金銭的な動機によるものであることが明らかにされています[2]。これだけ多くの機密データが生成、ネットワーク伝送、保存されている状況にあって、全ての企業にとって5G技術の導入がセキュリティ体制全体に影響を与えることは明らかです。

このホワイトペーパーでは、今日の脅威の状況に目を向け、5Gによって可能になる新しいワイヤレス環境における機会とリスク要因に焦点を当てています。

進化する脅威の状況

ネットワークセキュリティの現状は、5Gネットワークへの移行とともに、企業が直面することになる脅威を示唆しています。2020年度のDBIRによると、データ漏洩/侵害の全体の45%はハッキングによるもので、22%は運用上のミス、ユーザの操作ミス、または設定ミスによるものでした。侵害の4分の3近くは外部の攻撃者によるもので、その55%は組織的な犯罪グループによるものでした。

全体としては、データ漏洩/侵害の抑制力は向上しています。DBIRによると、多数の侵害は数日以内に鎮静化されています。しかし、被害者の半数以上が個人情報の侵害であったものの、侵害の72%が大企業を狙ったものであったことなどから、侵害の背後には犯罪的な要素が目立ってきています。侵害行為がビジネスとなっていることは明らかです。調査報告書によると、金銭的な動機が全体の86%を占めており、マルウェアインシデントの27%がランサムウェアの身代金要求につながっています。

データの漏洩/侵害が増加している要因の1つは、センサーやその他のIoTデバイスなど、従来型とM2M（Machine to Machine）型の両方のエンドポイントが増えていることです。2023年までにIPネットワークに接続されるM2Mデバイスの数は150億台近くになると予測されており[3]、それまでにデバイスの数は人間の数を少なくとも3倍以上上回る模様です。IoTデバイスが現在のネットワークに与える影響を測ることは困難です。残念なことに、多くのデバイスは、悪意のある攻撃者によって容易に侵害される単純なデフォルトパスワードが設定され、出荷されているからです。

5Gの導入におけるセキュリティ上のメリットとデメリット

企業が新しい5Gサービスの大規模な導入を計画する際には、サービス、デバイス、セキュリティの各プロセスに関して、全体的なリスクを低減するため考慮すべき重要な要素がいくつかあります。

5Gは、ワイヤレス接続で単にIPトラフィックをより速く、より効率的に低遅延で移動させる方法であるため、それ自体が新たな攻撃の対象になることはありません。しかし、プライベート5Gネットワークが導入されると、当然、4Gネットワークですでに見られた脅威が少しずつ拡大していくことや、設計の上でも意図の上でもまったく新しい脅威が持ち込まれることに直面すると予想されます。

したがって、5Gネットワークが新しいアプリケーションをサポートし始めると、これまでアプリケーションの多くは有線ネットワークでの使用が多かったため、警戒をさらに強めることが重要になります。例えば、より多くのM2Mインタラクションを必要とし、多数のワイヤレスエンドポイントを使用し、扱うデータ量が多くなるアプリケーションの場合、ネットワークに接続していても管理されていないIoTデバイスを介して情報にアクセスする手口をとる産業スパイなど、金銭的利益を得るための新たな攻撃を生み出す可能性があります。

4Gの既存のセキュリティ対策は5Gでも活用されますが、未知のリスクを軽減し、信頼性を確保するために、多くのセキュリティイノベーションが追加されています[4]。それらには以下のような強化策が含まれています。

- 帯域内ユーザデータと帯域外シグナリングの両方でエンドツーエンドの暗号化を行なえるようになり、伝送中のデータを傍受することがほぼ不可能になっています。すべてのアクセスはホームネットワークまたはプロバイダーネットワークによって認証され、加入者を管理するネットワークがそのアクセスの正当性を検証できるようにしています。
- 5GまたはWi-Fi経由で接続されているかどうかに関わらず、同一のネットワーク認証を行うことで、国際モバイル加入者IDキャッチャー（IMSIキャッチャー）として活動する不正な基地局を排除することができます。ネットワークに依存しないこの認証フレームワークにより、どのような使い方をしているデバイスであっても、ホームネットワークによる管理を向上させ、認証情報をキャッチするスヌーピングを防止します。
- 安全性の低い相互接続されたネットワーク経由の脅威が、接続先の5Gネットワークに危害を加えることを防ぐ新しいセキュアエッジプロテクションプロキシ（SEPP）。
- ネットワークスライシングとは、ソフトウェアで定義されたネットワーク構成を利用して物理ネットワークを論理的に細分化し、異なるネットワーク機能を持つ複数の仮想「スライス」に分割し、ネットワークトラフィックを他のスライスから分離するメカニズムです。これまで、このような差異のある機能とトラフィックをそれぞれ分離させるには、物理ネットワークを別々に構築する必要がありました。5Gネットワークスライシングを利用すれば、サービスプロバイダーは、特定のアプリケーションニーズに合わせてネットワーク機能をより正確に「調整」し、重要なアプリケーションを独自のスライスに分離して、他のアプリケーションからの影響を軽減することができます。

5Gの規格を公布する団体である3rd Generation Partnership Project (3GPP)では、特にIETF（Internet Engineering Task Force）やNIST （National Institute of Standards and Technology）などの機関のセキュリティプロトコルを活用して、基地局、アンテナ、基幹ネットワークの安全性を確保しています。ワイヤレス通信のセキュリティの脆弱性に対処するために、5G規格ではこれらの設計強化が施されています。

5Gのセキュリティを確保するためのベストプラクティス

データセキュリティに関して言えば、最高の防御策があります。ここでは、5Gの導入を計画する際に考慮すべき点をいくつか紹介します。

サイバーセキュリティフレームワークは、セキュリティプロファイルの構成要素に対して方法論的なアプローチを提供してくれるため、企業が一から作り上げる必要はありません。このフレームワークは、広く採用されている規格に基づいており、5Gネットワークのような重要なインフラストラクチャに対するサイバーリスクを低減するように設計されています。NISTのフレームワークは、ネットワークの無数のコンポーネント、特に脆弱性のあるインターフェイスが存在するものについて、組織が把握できるようにします。悪意ある攻撃者がアクセスを得るための径路にするコンポーネント、インターフェイス、移行ポイント、その他の要素ごとにデータセキュリティプランを練ることでフレームワークは防御の第一線となります。

暗号化はあらゆる場所に適用すべきものです。5Gは、セットアップシグナリングとユーザデータトラフィックの転送中の両方で、エンドツーエンドの暗号化を行ないます。ただし、データのセキュリティを確保するには、暗号化を有効にする必要があります。データとシグナリングの両方がデフォルトで暗号化されるようにします。次に、全てのアプリケーションに対してゼロトラストのスタンスをとります。トランザクションごとに認証を行なうことで、データの機密性に関係なく、全てのデータと音声に対して最高レベルのセキュリティを確保することができます。セキュリティ強化を最大限まで引き上げるには、信頼の輪や境界線があってはならず、全ての人が疑われ、確認の対象にされるべきです。今日のネットワークは非常に複雑なため、信頼の境界線をどこに設定すべきかは簡単ではありません。

規格に準拠することと同様に重要なのは、5Gサプライチェーンを深く理解することです。企業は、チップレベルに至るまで、5Gのハードウェアを信頼できる企業から調達し、それらのデバイスにバックドアアクセスメカニズムがないことを確認しておく必要があります。同様に、全ての組織は、デバイスを動作させる5Gのファームウェアとソフトウェアについて安全性の観点から十分に理解している必要があり、例えば、コードリポジトリから引き抜かれたオープンソースのマルウェアに、デバイスや通信事業者の5Gのコア部分が感染することは許されません。

最後に、どの組織においても、全てのアプリケーションの安全性を確保するために、企業のベストプラクティスを採用すべきです。ここでは、業界のリーダーが認めているベストプラクティスをいくつか紹介します。

職務の分離：企業全体のセキュリティプロセスが一個人によって破壊されないようにします。

役割に基づくアクセス制御：情報やリソースへのアクセスは、許可されたユーザの役割またはそのアクセスを必要とするアプリケーションのみに制限します。

最小特権の原則：各ユーザには、それぞれの職務に必要なアクションを実行できる最小レベルのアクセスのみを許可します。

多要素認証：可能な限りリモートログインに複数の認証方法を要求することで、セキュリティを全体的に強化します。

最新化：現在のネットワークに古い管理されていない資産が接続されている場合は、それらをアップデートすることを検討します。古いデバイスやセンサーのセキュリティが適切に設定されていることを確認します。ネットワークが安全に構成されていない場合は、攻撃者に脆弱面を晒すことになります。

ガバナンス：IoTの普及が高まるともに、ウェアラブル接続の医療機器の成長が予想される中、HIPAA、ペイメントカード業界（PCI）、その他のガバナンスガイドラインなどの規制要求の遵守が5Gの課題となります。デバイス、ソフトウェア、ネットワークの各プロバイダーと協力することで、組織はこれらのデバイスが安全なデータチェーン内で壊れたリンクにならないようにすることができます。

ベライゾンによるサポート

5Gを推進するベライゾンは、5Gのワイヤレスネットワークへの移行を進める多くの組織によって選ばれるプロバイダーとなっています。米国国内で2,000店を超える店舗を含め、グローバルな事業展開、知識豊富な専門技術者を配置しており、自身がエンタープライズ5Gのユーザでもあり、PCI、HIPAA、およびその他のコンプライアンス義務の遵守からセキュリティについて学んできました。私たちはその経験を、世界中に提供しているサービスや製品に取り入れています。

ベライゾンでは、セキュリティを5Gエコシステムに組み込んでいます。ベンダーと製品の厳格な選定プロセスを通じてセキュリティ保護を採用しており、機能の選定のみにとどまらず、セキュリティ管理を備えた製品モデルを構築しています。つまり、デバイスだけでなく、物理的、デジタル的なサプライチェーンも強化しています。ベンダーのソフトウェアのアップデートやパッチを提供する際には、セキュリティホールのない、安全でセキュアな製品の確保に努めています。

私たちが誇るのは、さまざまな業界のパートナーとの提携です。ベライゾンは、2つの主要な5Gセキュリティ組織である「セキュアなデジタル経済に向けた国際評議会（Council to Secure the Digital Economy）」と「O-RANアライアンス」の創設メンバーとして、IoTのセキュリティを推進し、オープンで相互運用可能な規格ベースの仮想化された5G無線基地局とアンテナを推進するための世界的な取り組みをリードすることに尽力しています。また、ベライゾンは、米国の通信インフラやサービスのセキュリティと信頼性を高めるために、セキュリティ機関やその他の通信企業が米国政府のパートナーとともに召集される、米国国土安全保障省の一部であるコミュニケーション情報共有分析センター（Communications Information Sharing and Analysis Center: Communications ISAC[4]）とも提携しています。

このため、ベライゾンの5Gにおけるセキュリティアーキテクチャに関する3GPP規格には、IETFおよびNISTによる勧告が含まれています。例えば、ユーザの機器と基地局を相互に認証することで、不正アクセスや盗聴者への認証情報の漏洩を防ぐことができます。シグナリングもデータもすべて暗号化されていない状態で伝送されるべきではないからです。

また、ベライゾンは、弊社のスマートフォンやその他の一般小売の5Gユーザ機器が業界のセキュリティ基準だけでなく、弊社独自のデバイスセキュリティ要件やプロセスに準拠させるようにしています。例えば、ユニバーサル移動体通信システム（UMTS）のSIMに保存されているネットワーク認証や加入者のプライバシー認証情報の漏洩を防ぐために、耐タンパー性のあるUMTS SIMカード[4]の使用を義務付けています。

このようにして自動化されたテストパイプラインを活用し、電話、MiFiデバイス、ルーターなど、ネットワークの各コンポーネントに焦点を当てた安全な5Gネットワークを構築するために、規格化された構成にテストと検査を行ない、使用しています。全てのコンポーネントは、業界規格とベライゾンの厳しいデバイスセキュリティ要件の両方に適合していなければなりません。

ベライゾンの5Gサービスが採用している新しいソフトウェア定義ネットワークアーキテクチャでは、各種のアプリケーションやサービスをリソースやトラフィックのスライスに分解し、仮想プライベートネットワークのように簡単な割り当てと分離を行なうだけで、セキュリティをさらに強化することができます。このような方法で、基幹システムを管理されていないIoTデバイスから切り離して保護することができるため、ビジネスクリティカルな機能が分散型サービス妨害（DDoS）攻撃の影響を受けることはありません。

最後に、ベライゾンは企業ネットワークの管理に数十年の経験を有しており、過去のネットワーク構築作業で得た教訓を5Gネットワークとデバイスに適用しています。ベライゾンは、パートナーやエンドユーザのお客様が自社のセキュリティ体制を理解し、5Gの進化に合わせてセキュリティ戦略を進化させていくためのツール、製品、人材をとり揃えています。

次のステップ

ベライゾンは、商用の5Gワイヤレスサービスを開始した最初の企業として、お客様の5G環境でのセキュリティ確保のお手伝いをいたします。ベライゾンの5Gサービスによって、どのようにして貴社のビジネスに強固なセキュリティプロファイルを維持させることができるか、詳細についてはベライゾンのビジネススペシャリストにお問い合わせください。

verizon

1 “The Future of IoT Miniguide: The Burgeoning IoT Market Continues,” Cisco, July 19, 2019.
2 “2020 Data Breach Investigations Report,” Verizon, 2020.
3 “Cisco Annual Internet Report (2018–2023),” Cisco, March 9, 2020.
4 “First Principles for Securing 5G,” Verizon, December 2019.