このホワイトペーパーは、以下のサイトの英文のホワイトペーパーの日本語翻訳です。

Accessing Production Data vs Cybersecurity? Why not both?

March 22, 2022/by Bob McIlvride

https://skkynet.com/accessing-production-data-vs-cybersecurity/

優先すべきは、「生産データへのアクセス」 か 「サイバーセキュリティー対策」か？両方は無理か？

多くの人は、両方は無理だと言います。もしプラントからの稼働中のプロセスデータを必要とする場合、サイバーセキュリティーを妥協しなければなりません。もしくは、可能な限り安全に生産システム（または製造システム）を保持したい場合、完全にそれらをロックダウンする必要があります。可能であればエアギャップする（もしくは生産システムから物理的に切り離す）必要があります。

しかし昨今のシステム要件では、企業がより深く検討することを余儀なくされています。Industry 4.0 と競合企業からの圧力は、企業が生産現場からリアルタイムデータもしくは、履歴データを引き出し、それらをクラウドや本部の IT 部門へ提供するよう要求します。問題は、“それをどのように安全に行うのか？”とういことです。

選択肢の比較検討

いくつかの選択肢があります。それぞれには長所と短所があります。最初に思い浮かぶのは、VPN の使用です。しかし後ほど説明しますが、VPN は期待できるほど安全ではありません。もう一つの選択肢は、OPC と MQTT を組み合わせて、プラント内およびプラントからクラウドへのセキュリティーを確保することです。このアプローチは、両プロトコルの長所を引き出しますが、DMZ を介した分離されたネットワークを接続するという点においては、弱点があります。

３つ目の選択肢として、安全なトンネリングがあります。適切に実装することで、リアルタイムおよび過去の生産データを TCP でトンネリングすることにより、既存のシステムへの影響を最小限に抑え、SSL 暗号化と証明書によるセキュリティーの実装を容易に行うことができます。OT（オペレーションテクノロジー）側の OPC サーバーなどのデータソースは、ミドルウェアコンポーネントにローカル接続し、IT 側の受信クライアントも同じようにローカル接続します。適切なミドルウェアは、DMZ と閉ざされたファイアウォールポートを介して、リアルタイムに双方向にデータを流し、必要に応じてネットワークプロキシをサポートします。
多くのユースケースで、この運用は「生産データへのリモートアクセス」と「サイバーセキュリティー対策」の両方を提供します。

DMZ ― OT/IT サイバーセキュリティーに不可欠なもの

業界や政府機関が推奨している、OT と IT に接続するために最も安全な方法は、DMZ（非武装地帯）を使用してネットワークを分離させることです。昨年、欧州委員会から出された NIS 2 指令により、企業の生産部門とコーポレート部門間のネットワークデータのセキュリティー強化が義務付けられ、DMZ の利用が推奨されました。ほぼ同時期にホワイトハウスから発表されたメモには、こう書かれていました。「企業の“ビジネス機能”と“製造/生産業務”が分離されていることは極めて重要です。業務用ネットワークへのインターネットアクセスを慎重にフィルタリングして制限し、これらのネットワーク間のリンクを特定することが必要です。もし企業のネットワークが侵害された場合でも、ICS ネットワークを分離してオペレーションの継続ができるように回避策や手動制御を開発することが極めて重要です。」

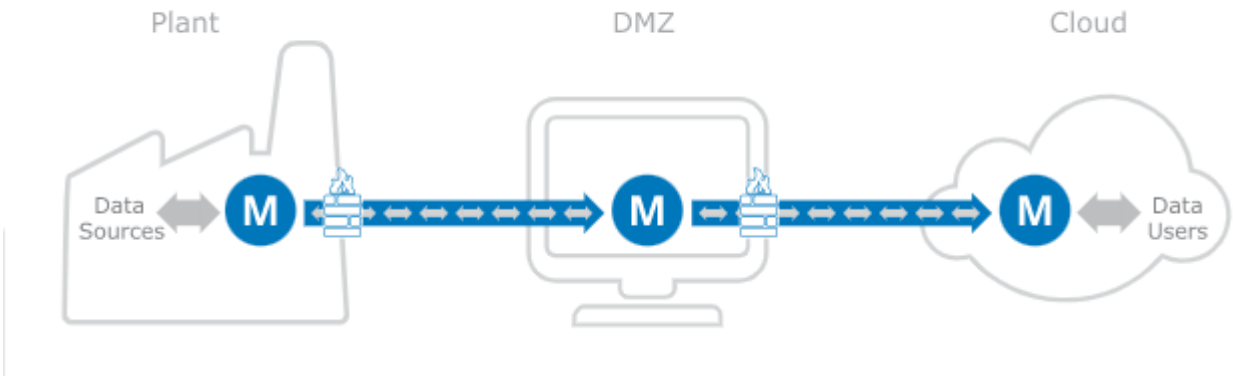
両指令の参照文書、NIST SP-800-82 は、ゼロトラストの OT ネットワーク・セグメンテーションを次のように要約しています。「最も安全で管理し易く拡張性のある、企業ネットワークと制御ネットワークとの分離アーキテクチャは、通常、少なくとも 3 つのゾーンに基づいており、1 つないしそれ以上の DMZ を組み込んでいる。」

これら 3 つのゾーンは、コントロールゾーン（ＯＴ）、コーポレートゾーン（ＩＴ）、そしてＤＭＺそのものです。DMZ を使用することで、企業ネットワークと制御ネットワーク間を直接的に繋がないようにし、既知の認証済みのユーザー／デバイスのみがシステムに入ることができます。SP-800-82 文書には、これらのゾーンを分離し、適切なデータのみがあるゾーンから別のゾーンへ通過できるようにするためのファイアウォールの価値と使用方法について説明されています。

DMZ 経由の接続

Industrial IoT 環境下での DMZ の実装は、OPC　UA と MQTT 両方にとって問題があります。DMZ を経由でプラントのデータを取得するためには、たいていはそれぞれが互いに繋がれた 2 台以上のサーバーを必要とします。OCP UA プロトコルは単純に複雑なため、このようなデイジーチェーンにおいてうまく再現することができません。情報は最初のデイジーチェーンのホップ（数珠繋ぎの 1 段目の情報伝達）で失われます。DMZ を介してデータを渡すために必要とされる同期的なマルチホップ相互作用は、最も信頼できるネットワーク以外では、すべてにおいて脆弱で、高い遅延が発生します。そして、チェーンの各ノードでデータにアクセスできなくなります。MQTT は、チェーン化することは可能ですが、チェーン内の各ノードがチェーンの一部であることを認識し、そしてそれらを個別に設定する必要があります。MQTT の QoS 保証は、チェーンを介して伝達することができないため、チェーンの末端ではデータの信頼性が低下します。

一方で、安全なトネリング実装は、各ノードで設定されたすべてのデータセットをミラーリングすることができるので、DMZ を通してデイジーチェーン接続されたサーバーをサポートすることが可能です。中間に位置するミドルウェアは、資格のあるクライアントと、チェーン内の次のノード両方にデータへのアクセスを提供します。使用されるトンネリング ミドルウェアは、チェーン内のどのクライアントまたは中間ポインでもオリジナルのソースと一致するように、一貫性を保証できるものである必要があります。



ファイアフォールのオープンポートの保護

最高レベルのサイバーセキュリティーを提供するため、安全なトネリングはすべてのインバウンド通信を許可するファイアウォールポートを閉じておきます。これはほとんどの産業用プロトコルが想定していないことです。例えば、OPC DA と OPC UA はどちらもクライアント/サーバー アーキテクチャを使用しており、クライアントが接続を開始し、サーバーがそれを受け入れます。サーバーは、TCP ポート上の接続をリッスン（待機）する必要があり、そのポートはサーバーのファイアウォール、およびクライアントとサーバー間にある上流ファイアウォールで受信接続用に開かれている必要があります。OPC 経由でデータにアクセスするとういことは、それらのファイアウォールにて、少なくとも 1 つのポートを開くことになり、重大なリスクとなります。

この様にファイアウォールのインバウンド接続を許可するポートが開いているという事は、セキュリティー上の脅威にさらされていることを意味します。ネットワーク攻撃は、ポートやプロトコルでは無く、アプリケーションに対して行われます。リスクは、リッスン（待機）しているアプリケーションに、プロトコルの実装に起因するまたは起因しない、悪用可能な欠陥があることです。

例えば、アプリケーションが OPC UA　プロトコルを完璧に実装していても、OpenSSL の欠陥に対して脆弱である場合があります。このアプリケーションには、OPC UA や SSL に悪用可能な欠陥がなくても、受信データに対して実行される文字列処理関数にバッファー・オーバーランが発生する可能性があります。バグがないアプリケーションはありません。開いているすべてのインバウンド接続用の受信ポートは、攻撃者がアプリケーションの悪用可能な欠陥を調査する機会であり、発見されれば即座にネットワークにアクセスすることが可能です。

安全なネットワークのファイアウォールでは、受信ポートを一切開けないことがセキュリティー上、最も良い方法です。適切な設計をすれば、トネリングによるアプローチは、この要件を満たすことができます。
もしトネリングミドルウェアがサーバー側からクライアント側へアウトバウンド TCP 接続をする場合、インバウンドのファイアウォールポートを一切開けておく必要はありません。これにより、攻撃対象が完全に排除されます。

MQTT オプション

おそらく、プラントのファイアウォールのポートを閉じたままアウトバウンド接続を行う最も一般的な方法は、ＭＱＴＴを使用することです。機器とプログラムは“ブローカー”と呼ばれるサーバーに接続し、データをブローカーへ公開したり、ブローカーからデータを受信したりします。MQTT ブローカーはデータのペイロード自体を調査せず、単にそれぞれのパブリッシャーからすべてのサブスクライバーにメッセージを渡すだけです。

この“Push”アーキテクチャは、ＯＰＣのクライアント-サーバーのアーキテクチャ問題を回避し、デバイスがファイアウォールポートを一切開くことなくアウトバウンド接続を行うことを可能にするものです。そして、MQTT ブローカーを使用することにより、互いに多くの接続が確立でき、複数のパブリッシャーが複数のサブスクライバーへ接続できるようになります。このように、ＭＱＴＴは、いくつかの IoT 通信とセキュリティー問題を解決します。

このように、MQTT はアーキテクチャ上に利点ではある一方で、OT/IT と産業 IoT 通信のシナリオに真に有益であるためには、対処すべき欠点もあります。

- MQTT はトランスポート・プロトコルです。それはペイロードフォーマットを指定していないため、異なるベンダーのアプリケーションとの間で相互運用性に問題が生じます。この問題を解決するために作られたのが「Sparkplug B」であり、ベンダーやユーザーの間で支持され始めています。
- MQTT ブローカーは別のトピック間でのデータ値の時間の順序を保存しません。つまり、物理システムで A→B→C で発生したイベントが、アプリケーションには、C→B→A の順序で送られる可能性があり、これば多くの産業制御ユースケースでは、エラーとなります。
- MQTT ブローカーは、データソースが切断されているということを表示する方法がありません。消費している（受信）アプリケーションは不具合が起こっているセンサーからの古い値と、最近変換していない現在の値との区別がつきません。これに対処するために設計された MQTT の“last will”メカニズムでは、データのプロデューサー（送信者）とコンシューマー（受信者）間の不合理なレベルの結合を必要とし、結果的には、設定の重複を起こし、統合とメンテナンスコストを増大させます。
- MQTT の QoS（Quality of Service）レベルは、それらが単一の接続のみ適合できるので、DMZ を超えて使用するには適切ではありません。DMZ を介しての接続は様々なホップが必要なため、データプロデューサー（生産者）は、選択した QoS に関係なく、MQTT メッセージがユーザーに届いたかどうかを知ることができません。必要なのは、最終的に一貫性を保証することであり、プロデューサー（生産者）が送信した各値は、ユーザーに届けられるか、もしくはより最新の値に取って代わられるかのどちらかです。。

- MQTT ブローカーは、オーバーロード（過負荷）の状況を適切に対処することができません。もしコンシューマー（消費者）が処理できる能力よりも早くデータが到着すると、データプロデューサー（生産者）とコンシューマー（消費者）間のデータの整合性と時間の順序は失われます。

まとめると、MQTT はインバウンドファイアウォールを閉じたままにすることができるので、一部の産業 IoT アプリケーション、特に組込み機器からのデータ収集の“ファーストワンマイル”に有益です。しかし、そのパブリッシャー（生産者）とサブスクライバー（消費者）間のデータの一貫性保証できないため、特に DMA を経由した場合は、OT/IT 接続にとって理想的な候補にはなりません。

VPN の回避

DMZ を使用し、全てのインバウンドファイアウォールポートを閉じることは、VPN を使用するよりも遥かに安全です。実際、VPN は産業システムによって必要とされているセキュリティーレベルを提供していません。その代わりに、VPN はプラントネットワークだけではなく、IT ネットワークにもセキュリティーの境界を効果的に拡張します。VPN 上のセキュリティー侵害は、両ネットワーク上のすべてのシステムを攻撃にさらします。

IoT に VPN を使用する欠点は、マイクロソフトの開発者、Clemens Vasters に詳しく検証されています。「VPN は偽りの友か？」というタイトルのインターネット関連の論文の中で、Vesters は次のように述べています。「VPN は、仮想化されたプライベート・ネットワーク空間を提供します。安全なトンネルは、その空間の中へ適切に保護されたパスを実現するための仕組みであり、その空間そのものは全く保護されていません。」

ネットワーク全体への外部アクセスを提供するための効果的な理由はないのです。指定のデータソースから DMZ への一方向のトンネル接続を確立することにより、これらのソースだけでなく、システムの残りの部分も保護することができます。内部ネットワークを外部に露出することなく、データにリモートアクセスすることができます。

トンネル通信の保護

DMZ の使用とインバウンドファイアウォールポートを閉じたままにしておくことに加え、セキュリティーの最善策は、トンネル接続自体に実装しておくことです。例えば、

- SSL 暗号化は必須で、TLS1.2 や TLS1.3 のような最新バージョンに対応していることが望ましいです。システムは、サーバー証明書の使用と適用する必要があります。
- ユーザー認証は、接続ごとに適用するのが最適です。各クライアントプログラムは、認証のためにユーザーネーム、パスワード、アクセストークンか、クライアント証明書を送信する必要があります。

- パスワードを含む暗号化されていないデータはネットワークパケットキャプチャプログラムで取得される可能性があるため、平文（テキスト）転送での接続は避けるべきです。

データアクセス と サーバーセキュリティー

競争力を保つため、あらゆる規模の企業が、リアルタイム、アラーム、履歴ログなど、産業プロセスデータへのリモートアクセスを要求しています。 しかしこれらの要求を満たすために、サイバーセキュリティーにおいて妥協を強いるべきではありません。その選択肢があってはいけないのです。トネリング技術は、OT と IT システムを安全に接続し、一方向または双方向のデータフローをリアルタイムで実現する方法を提供します。プラント内ネットワークに準ずるセキュリティーレベルを実現しながら、必要な生産データにアクセスすることは可能です。