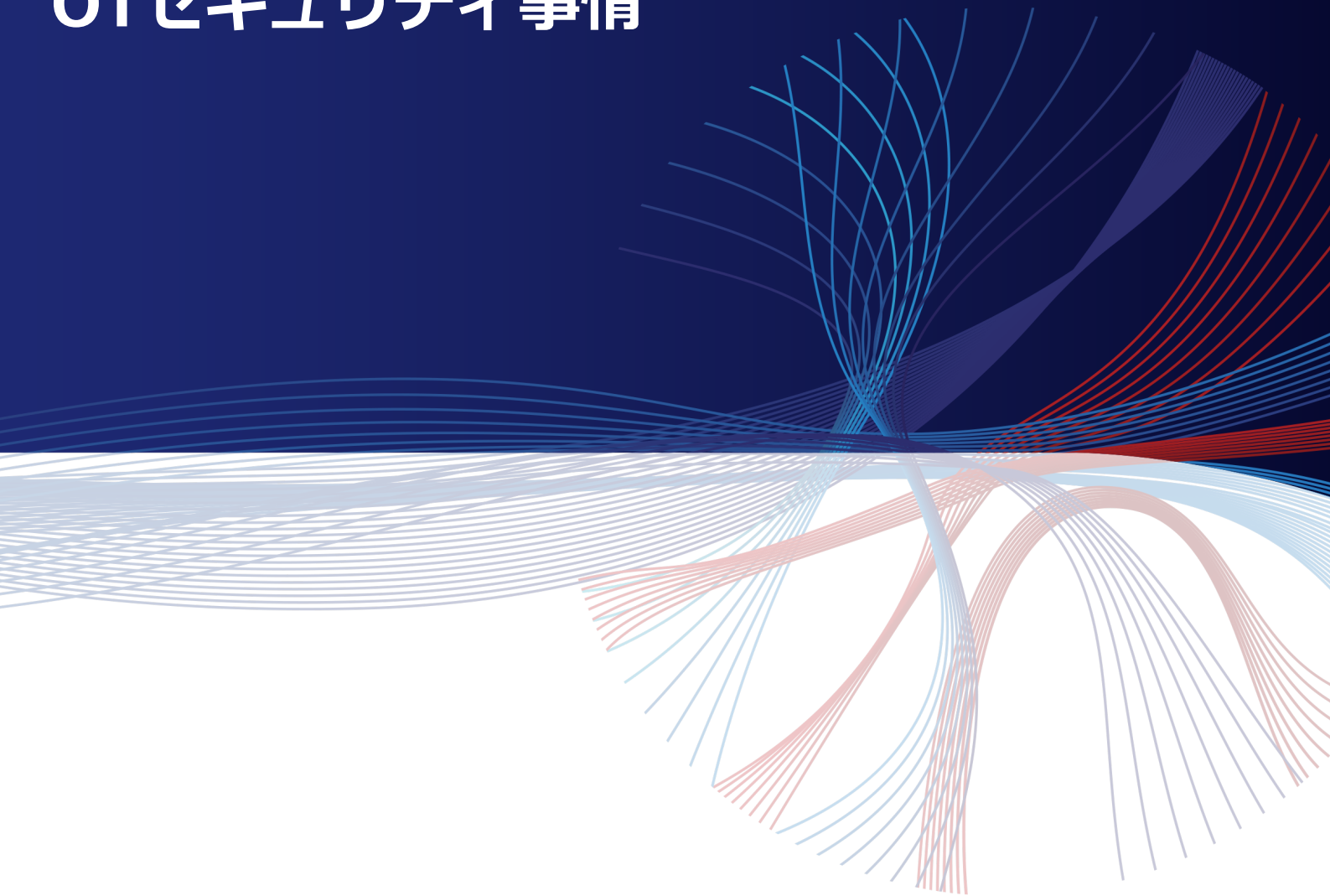
SCADAfence

Technical Whitepaper

リモートメンテナンスの促進で担当者を悩ますOTセキュリティ事情



SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3

Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

新型コロナウイルスの収束を見据えた供給網維持に向けて、工場へのサイバー攻撃をどう防ぐか検討を始めているセキュリティ担当者は多いのではないだろうか。この場合、従来の**OT**環境の運用に沿ったセキュリティ対策に加えて、今後、加速するであろうリモートメンテナンスをはじめクラウド活用が含む脆弱性にもより一層配慮していく必要がある。

本資料では、新型コロナウイルスの影響で新たに起きるOTセキュリティ対策について、SCADAfenceが考えるOT、セキュリティ、IT運用のそれぞれの担当者の視点から、課題とその解決策について述べる。

増加するOT環境へのサイバー攻撃

新型コロナウイルスの大流行は、世界中のハッカーが企業や個人の機密データにアクセスできる絶好の機会となってしまっている。これは、世界中の人々が在宅勤務を余儀なくされており、会社のシステムへリモートでアクセスしなければならない状況はハッカーが機密データへのアクセスを容易にしている土壌を作っているからだ。

アメリカに拠点を置くセキュリティ企業Barracudaによると、コロナウイルスの感染拡大を悪用する類の攻撃は、世界的に見て667%増加したという（参照：https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/）

現在、新型コロナウイルスに便乗したフィッシング攻撃や詐欺が発生していることからンドユーザーの継続的な教育が求められている。

OT環境も例外ではないが、リモートメンテナンスやクラウドを活用した各種機器のインターネット接続状況が変化する中、セキュリティ対策のために従業員を教育したり、十分な設備を敷いたりする時間はないだろう。

本章では、産業業界における最近の脆弱性の事象、新型コロナウイルスの流行により増加する新たな脆弱性と、OT環境が抱えるセキュリティ対策の新たな問題について述べる。

最近の攻撃例と脆弱性

工場のあらゆる設備や機械、人の作業といったデータをセンサーなどのIoTで集め、生産性向上に役立てるスマートファクトリーが促進される過程で脆弱性の問題が顕著になっている。

米国の天然ガス圧縮施設へのサイバー攻撃

米国土安全保障省（DHS）傘下のサイバーセキュリティ機関であるCISA（サイバーセキュリティ・インフラストラクチャセキュリティ庁：Cybersecurity and Infrastructure Security Agency）は2020年2月18日、米国の天然ガス圧縮施設がサイバー攻撃を受け、2日間の操業停止を余儀なくされたことを発表した。（参考）https://www.us-cert.gov/ncas/alerts/aa20-049a

三菱電機の一部制御システム製品に「URGENT/11」の脆弱性

独立行政法人 情報処理推進機構（IPA）および一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）は2月17日、三菱電機株式会社が提供する「MELSEC C言語コントローラユニット」および「MELIPC シリーズ MI5000」には、Wind River社製のリアルタイムOSである「VxWorks」に起因する複数の脆弱性が存在すると「Japan Vulnerability Notes（JVN）」で発表した。
（参考）https://jvn.jp/vu/JVNVU95424547/

今後、急速に増えるリモートメンテナンスやクラウド活用

今回の新型コロナウイルスの件を機に、ITインフラ、その利用方法やネットワークアクセスを見直す企業は多いだろう。例えば、リモートワーク環境において柔軟にデータへアクセスするために、旧来のファイルサーバを廃止して、クラウドコンピューティングを導入していくだろう。また、サプライチェーンにおいては、これまで以上に相互に連絡を取り合うことで相手方の操業状況を把握するため、工場や拠点間のネットワーク網をグローバルレベルで整備していくだろう。

新型コロナウイルスの発生以降、7割が「セキュリティ脅威や攻撃が増加」

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社（チェック・ポイント）は2020年4月7日、新型コロナウイルス（COVID-19）のパンデミックが企業のセキュリティに与えている影響に関するアンケート調査の結果を発表した。同調査は、チェック・ポイントの依頼を受けてDimensional Researchが実施したもので、世界中の従業員数500人以上組織のITおよびセキュリティ専門家411人を対象としている。調査結果によると、セキュリティ専門家の71%が、新型コロナウイルスの発生以降、セキュリティ脅威または攻撃が増加したと回答した。増加した脅威は、フィッシング攻撃が55%でもっとも多く、パンデミックに関する情報提供または提言を謳う不正Webサイト（32%）、マルウェア（28%）、ランサムウェア（19%）と続いた。また、回答者の95%が、新型コロナウイルスの感染拡大により、対処すべきITセキュリティ課題が増えたと答えている。セキュリティに関する今後の懸念については、迅速にリモートワークに対応すること（61%）、リモートアクセスのセキュリティの強化（55%）、エンドポイントセキュリティを拡大させる必要性（49%）を挙げている。

（参考）https://www.checkpoint.com/press/2020/increase-in-remote-working-and-coronavirus-related-threats-creating-perfect-storm-of-security-challenges-for-organizations-new-survey-finds-2/）

リモートワーク拡大で産業制御システムへのRDP接続に潜むBlue Keepの脆弱性

RDP（Remote Desktop Protocol）を使ってリモートデスクトップ接続が可能なインターネットに露出した産業制御システムは増加している。そして、新型コロナウイルスの感染拡大に伴い、リモートワークを採用する企業が世界的に増える中、RDPを使ってリモートデスクトップ接続を受け入れる産業制御システムの増大は加速するだろう。現在、MicrosoftがRDPの旧バージョンの脆弱性「BlueKeep」に関するセキュリティ情報を公開し、顧客へ迅速なアップデート作業を推奨したが、OT環境はIT環境に比べて動作が不安定になるような恐れがある変更は避ける傾向にあり、脆弱性を抱えたまま稼働している可能性が高い。

（参考）https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

攻撃の傾向に対するOT環境が抱える新たな問題

これまでは、攻撃者が工場のシステムや扱っているデータに詳しくないことが多く、システム停止やHMIの操作不能など生産性に影響を及ぼすような被害は未だ多くは無い。

また、場当たり的でポートスキャンなど意図しない攻撃も多い反面、多段階の攻撃における初期段階の情報収集である危険性も含んでいる可能性もある。

今後、リモートワークの拡大により、OT環境へ簡単にアクセスできるようになり、且つ、セキュリティの教育を受けていない社員が攻撃に晒されることが増えてくると、被害が大きくなる可能性が十分に考えられる。社員が退職した後も引き続きリモートアクセス出来るような運用や、攻撃者の偽メールに対してOT担当者が情報提供をしてしまうといったケースなどが想定される。

そして、サプライチェーンの強化により、セキュリティ対策の手薄な委託先を狙った攻撃、気付かないうちに納入物へのマルウェア混入や取引先へサーバーへのメール攻撃、生産システムの稼働率が低下することによる納期の遅れなどが増えることも想定される。

リモートメンテナンスを見据えて取組むべき課題

IT運用におけるセキュリティ対策の常識が、そのままOT運用には通用しない状況で、どの部門や部署が主体性を持ってOTセキュリティ対策を推進していくのかは業界や企業によって様々である。

そして、冒頭で述べたようにリモートワークが急速に拡大してく中で待った無しのOTセキュリティ対策が求められているが、OTセキュリティ担当者をアサインし、OTとセキュリティの両方を同時に教育している時間はないだろう。

各社とも、セキュリティに関わるコンサルティング会社、製品ベンダーや、普段から自社の業務をサポートしているSIerなどに相談するのが一般的だ。この場合、OTセキュリティ初心者であっても、すぐに導入できるような即効性のあるソリューションを自社の状況に沿って、ロードマップとともに提案を受けることが多いのではないだろうか。

本章では、SCADAfenceが普段の提案活動において、OTセキュリティをこれから開始あるいは強化するお客様から受けるご相談を中心に、リモートワークによって増加する新たな脆弱性への取組む際の課題を述べる。

特に、OTセキュリティ初心者とは誰を指すのか、を考えた場合、主に、OT担当者、セキュリティ担当者、IT運用担当者の3者の視点があると考えている。

IT運用担当者がセキュリティ施策のプロジェクト全体をリードし、セキュリティ担当者は自社における要件を整理、OT担当者が現場の生産ラインを止めない安全第一による実装を心掛けるというケースが多い。

そして、それぞれの視点での課題を集約したものがOTセキュリティ初心者の領域だと考えている。

OT担当者のセキュリティ定義と目線を合わせる

工場・制御システムでは稼働、製造ライン・供給ラインを動かし続けることこそが利益であり、そこにIT部門やセキュリティ部門が踏み込むことは現実的には難しい。

そして、工場・制御システムにおける情報セキュリティの考え方は可用性であり、仮にパッチを適用することが脆弱性対策としては推奨されていたとしても、安定して安全に稼働している環境に手を入れるケースは非常に少ない。

セキュリティの定義がITとは異なるOT担当者に対しては、PLCやSCADAにおける制御コマンドを解読し、通常の制御機器に対するオペレーションと一緒にセキュリティ対策の必要性を説く必要がある。例えば、リモートワークの拡大によりPLCやSCADAへのアクセスが増えることで、これらの制御に機器に対して停止コマンドが発行され可能性がある場合、停止コマンドの解読と、それが意図しないオペレーションによる脆弱性を突いたものであるかを同時に説明していく必要がある。

OT環境に対する典型的な攻撃パターンを説くよりも、この攻撃の結果、可用性に影響を及ぼすであろう具体的な制御機器へのコマンドを中心に議論することが、セキュリティの定義の物差しをOT担当者と合わせることになると考えている。

セキュリティ専任者もOT環境の基本構成を把握する

工大規模な工場や制御プラントでは、品質管理部門やIT部門にセキュリティ専門のチームがある。中小規模の企業では、他の業務と兼任しながらセキュリティ対策の責任者がアサインされているケースも多い。OT担当者がセキュリティ施策も任せられているケースでない限り、セキュリティを主要業務とする担当者は、自社のOT環境の詳細な構成まで把握していることは稀である。

セキュリティ部門のOT環境に対する主な業務は、CVEなどの公表された脆弱性に対して自社の制御機器が該当するのかどうかの調査、あるいはSOARやSOCなどの仕組みにおいてOT環境で発生したセキュリティインシデントのハンドリングである。

この際、脆弱性のある制御機器を発見したり、OT環境のセキュリティインシデントを検知したりしても、対象となる制御機器の場所を特定する、パッチ適用やアップグレードを始めとした具体的な対処まで提示する、担当者や担当部門を割りだし影響する業務や生産ラインまで洗い出す、といったフェーズまで踏み込むことは難しい。

現場のOT担当者とコミュニケーションを取るためには、制御機器の資産管理として、IPアドレス、MACアドレス、デバイスタイプ、項目番号などの機器の情報をはじめ、その機器の通信の宛先などをセキュリティ担当者の視点で割り出し共有することだと考えている。特に、セキュリティ監視ツールなどを利用することで自動的に収集できるOT資産情報もあるが、事前にOT担当者と連携することによって、自動収集できないロケーション情報や担当者といった情報までを登録しておくとコミュニケーションがより円滑になる。

IT運用者がOTセキュリティ全般をけん引する

既存のIT部門がネットワークも含めて把握していることから、リモートワークの拡張のおけるメンテナンスの勘所を理解しており、最終的にはOTセキュリティの設計、実装から運表まで全体をリードするケースが多い。そして、OT担当者の意見を聞きながら、セキュリティ担当者が提示する要件に沿いながらIT部門の運用体制やプロセスを整えていく。

この場合、既存のITセキュリティの運用に大枠は合わせるケースが多い。例えば、資産管理、セキュリティインシデントのハンドリング、セキュリティフレームワークに沿ったガバナンス管理などが挙げられる

しかし、OTセキュリティ特有の管理が必要となるため、IT起点でそのまま管理を拡張するのは難しい。例えば、資産管理であればPLCやSCADAにおいて、それぞれのベンダーが持つ固有の情報を新たに管理する必要がある。また、インシデントハンドリングであれば、OT担当者が迅速に対応できるようにロケーション情報や推奨する対処の提示なども新規に登録していくことになる。さらには、セキュリティフレームワークを導入する場合には、既存のIT資産とは異なる準拠レベルの指定が求められる。

IT部門が持つ体制、プロセスや既存の管理ツールへ、新たにOTセキュリティを吸収していくためには、構成管理の拡充、監視ツールの統合やSOC連携、あるいはセキュリティインシデントを検知した後に自動制御するためのフロー策定などが挙げられる。これらの既存のIT運用の管理基盤をOTセキュリティ向けにアップデートすることが、OT担当者とセキュリティ担当の橋渡しにつながる。

リモートメンテナンス対応策におけるOTセキュリティ最新動向

OT、セキュリティ、そしてIT担当者が連携してOTセキュリティを進めていくことになるが、最低限へ押さえておくべきポイントがある。例えば、外部ネットワークとの接続点が増えていく際には、境界を適切に保護し整理しておく。また、リモートメンテナンスで使用されるリモート接続回線での、接続相手の認証や通信のセキュリティを確保しておく。さらには、事前に導入している制御機器の開発・提供者を確認し、問題が発生した場合にはすぐに対応できるようにしておく、といったポイントである。

一方で、ネットワーク経由でのOT向けの攻撃性は多様化しており、OTセキュリティ初心者は、その動向にも配慮しておくことが求められる。

本章では、SCADAfenceの考えるリモートメンテナンスの増加に伴い増える攻撃の傾向と、その対策について、OT、セキュリティ、IT担当者のそれぞれの視点で補足する。

OT担当者は潜在する新たな脆弱性へ対処する

産業業界に置けるセキュリティインシデントとしてはWannCry、BlackEnergy、Havex、IndustroyerやTrisisなどが挙げられるが、昨年、報告されているUrgent11やBlueKeepへの対処も必要だと考えている。両者とも、現時点では大きな被害報告は挙がっていないが、リモートメンテナンスが増えることによって脆弱性のある制御機器への不安が高まる。

Urgent11

これは、組込み機器向けOSの「VxWorks」の脆弱性に起因するもので、工場・エレベーター・産業機器や医療機器の制御システムから、ファイアウォール・ルータ・VoIP電話・プリンタ等のネットワーク機器まで、20億以上のデバイスに搭載されていると言われている。CVE-2019-12255～CVE-2019-12265の11個発見されたことから、「URGENT/11」と呼ばれている。既に、VxWorksの開発元であるWind River社では、修正パッチもリリースしている。しかし、上記に挙げたような多種多様なデバイスが対象であり、ネットワークの接続点に設置されるような機器を含めて、すぐにパッチを適用することは安定稼働の観点では難しいであろう。OT担当者としては、管理対象の制御機器がVxWorksを搭載しているかどうかを検査するとともに、パッチ適用が難しいのであれば、外部ネットワークとの接続点に、Urgent11の攻撃パターンを検知するソリューションを導入していく必要がある。具体的には、IPパケット中にSSRRやLSRRオプションを含んでいたり、TCP Urgent flagを制御したりするような疑わしい通信を検知する仕組みだ。

BlueKeep

この脆弱性は、旧バージョンのWindowsに影響を及ぼすリモートデスクトップサービスに関係している。攻撃者は、Windowsの脆弱性を悪用することにより、リモートデスクトッププロトコル（RDP）を実行している脆弱なマシン上でリモートコードを実行する可能性がある。そして、この脆弱性はワームに転用することが可能であり、極めて短時間で世界中に拡散し、数百万ものシステムに危害を加える恐れが考えられる。既に、マイクロソフト修正プログラムをリリースしているが、速やかにパッチ適用を開始するのが難しい場合は、ネットワークレベル認証を有効する、あるいはファイアウォールの設定でリモートデスクトップサービスのアクセスを制限することになる。OT担当者としては、リモートメンテナンスで制御機器へのアクセスを行う際に、リモートデスクトップの利用があるかないか運用面と通信内容の両方の観点で棚卸することだ。そして、リモートデスクトップは利便性が高い反面、脆弱性を突かれると、攻撃された場合のインパクトが大きいことを利用者と共有することだ。リモートデスクトップサービスのアクセスをネットワーク設定で制限するのが難しい場合は、パケットキャプチャをベースとしたセキュリティソリューションをネットワークの接続点に設置して、いち早く、疑わしいアクセスを検知することも求められる。

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

セキュリティ担当者には事前と事後の観点でOT環境を把握する

セキュリティ担当者の業務は、インシデントの生成前と生成後の２つに分類できる。インシデントの生成前は、日々の事前作業として、自社の資産が一般公開された脆弱性に該当しないかどうか検査する業務を指す。一方、インシデントの生成後は、事後のトラブルシューティングとして、迅速な現場への通知、影響範囲の切り分け、一時的な対処の実行、関係者への報告などを指す。

この場合、それぞれの業務においてOT環境をどのように把握しておくかがポイントとなるが、単なる制御機器のカタログ情報や通信内容を可視化しておくだけでは不足しており、リモートメンテナンスが進んだ場合を想定した多様な機器との構成や依存関係も配慮したうえでの対処が必要になってくる。さらには、疑わしい制御機器へのオペレーションを誤検知とのバランスを取りながら管理することが求められる。

制御機器どうしの依存関係を把握

制御機器単位で情報を収集し、制御機器どうしの通信内容を把握することは初期の運用であるが、ネットワークの接続点が増えるとともに、制御機器どうしの依存関係も把握しておくことで、セキュリティインシデントの事前および事後対処においてOT担当者とのコミュニケーションが円滑になる。

例えば、工場や生産ラインのPLCやSCADAの情報収集には注意を払うが、建物の電源や空調といった機器の脆弱性までを同時に配慮するケースは少ない。電源の供給に問題があると稼働率にも影響あるし、空調の温度をコントロール出来ないと故障の原因につながったりコストの増大にもつながったりする。工場の生産に直接関わる機器はもちろんのこと、間接的に関わるBACnetをはじめとしたプロトコルでつながっている機器にも一緒に管理することで、全体最適を図れる。

さらには、複数のコントローラやオブジェクトとPLCが主従の関係で構成されているケースが多いが、これらの依存関係も配慮することが求められるだろう。生産ラインシステムをメンテナンスする、あるいは段取り替えのタイミングでこれらの構成にアップデートがあった際には最新情報を反映して把握しておくことで、セキュリティインシデントが発生した後に、OT担当者と影響範囲を特定して共有するとインシデントハンドリングが迅速になる。

制御機器に対するオペレーションを重要度で選別する

制御機器に対するリモートメンテナンスの中には、脆弱性の選別が難しいものも含まれるだろう。例えば、PLCに対する停止/起動/再起動コマンドや、PLCからのPLC停止/起動通知、PLCへの時間設定などは制御機器に対するオペレーションであるが意図した内容であるかどうかの判断は難しい。一方で、PLCに対するプログラム書き込みコマンド、PLCに対する有効範囲を超えた値の設定や、新しいIPアドレスによるHMI/PLC/IOへ接続など疑わしいオペレーションであるが、リモートメンテナンスの一環だとすると不要なセキュリティインシデントが誤検知として生成されることになる。

そのため、通常時のリモートメンテナンスにおける制御コマンドの振る舞いを、セキュリティインシデントを生成する際の基準値として設定したり、制御コマンドに対するアラートの重要度を柔軟に変更したりすることが、事前作業としては求められる。

IT担当者はセキュリティ情報を自動的に分析する仕組みを導入する

リモートワークの整備に対して最も忙しくなるのはIT担当者である。特に、外出の自粛に伴いンラインでのWeb会議ツールの導入が加速している。これらは業務ネットワークの整備を対象としているが、OTネットワークと業務ネットワークの接続が進む現在では、リモートワーク向けのアプリケーションが新たな脆弱性の起点になる可能性が高い。

最新のOT環境やネットワーク変更に伴い、リモートワークに伴う新しいアプリケーションの利用などへも注意を払う必要がある。IT担当者としては、OTおよびセキュリティ担当者を橋渡しする際、最新情報を常に提供することが求められるが、手動で対応していたのでは負担が大きい。そのため、多角的な観点でOT環境の脆弱性を可視化できることに加えて、それが自動化されている仕組みが求められていく。

多角的な観点でOT環境の脆弱性を可視化

OT環境の脆弱性を管理する際の主な機能は、セキュリティインシデントの生成、OT資産の管理、攻撃パターンに対する脆弱性の管理の３つである。そして、これらの３つの機能が連動している必要がある。OT担当者は、セキュリティインシデントをもとに管理対象の制御機器の調査を開始するが、その際にはOT資産の管理をもとに進めていく。セキュリティインシデントとOT資産の紐づけはIPアドレスなどの制御機器情報だけではなく、通信の送受信の帯域や方向性などの流動性のある情報も把握することで、リモートメンテナンスに関連する脆弱性に対処できる。セキュリティ担当者にとっては脆弱性管理が軸になるが、産業向けに公開されているCVEなどの攻撃パターンの設定はもちろんのこと、セキュリティインシデントを複数生成した場合は相関処理によって、根本原因となっているセキュリティインシデントに絞り込むといったアラート対応の効率化も求められる。

メンテナンスが不要な自動的な管理

セキュリティソリューションを導入した場合、リモートメンテンナンスの拡大に伴い接続点にアップデートがあり、利用するアプリケーションの多様化によって追従する必要がある。

セキュリティソリューションのアップデートは、資産情報の追加や、シグネイチャなどの攻撃パターンのアップデートなどが主になる。しかし、メンテナンスの頻度が高くなり、意図しない脆弱性に全て対応してくための作業は負担が大きいし、最新の攻撃に対応出来なくなる可能性がある。

そのため、セキュリティソリューションには通常時のOT環境へのアクセスや通信内容を自動的に閾値として設定して、異常なアクセスなどの振る舞いがはっせいするとセキュリティインシデントを生成するといった、自社のOT環境の傾向を学習する自動的なメンテナンス機能も要求される。

まとめ

ここまで、新型コロナウイルスの影響によりリモートメンテナンスが加速することでのOTセキュリティの脆弱性に対する、OT、セキュリティ、IT担当者のそれぞれの視点で課題や対策を述べた。今後、リモートワークが推奨されることで在宅勤務も増え、これまで現場で作業していたOT業務の一部が自宅に取り込まれる可能性が出てくる。この場合のOT業務というのは、単に制御機器へのアクセスだけに限ったことではなく、打ち合わせや取引といった制御機器を直接操作するようなリモートメンテナンスだけには留まらない。仮に、ネットワーク上で、機密性の高いOT環境に関わる情報を発言したりチャットしたりすることにより、結果的にそれがOTセキュリティの脆弱性にもつながっていく。

インフラ面のセキュリティ対策以上にOT担当者へのセキュリティ教育は重要になる可能性があるが、一方でこれらの新しい取り組みは自社の競争優位性につながることも十分にあり得る。インフラ面でのセキュリティ対策は、多様なツールやソリューションを導入することで対策が図れることから、自社にとっての基本的な脆弱性についてはセキュリティベンダーのノウハウや製品を活用することをお薦めする。 本資料が、新型コロナウイルスのショックをチャンスに変えようとしている読者のヒントになれば幸いである。

筆者紹介：
梅根 庸一： SCADAfence (Japan) シニアソリューションコンサルタント
Hewlett-Packard社でITエンジニアとしてのキャリアをスタートさせ、インフラ、ネットワーク、仮想環境、クラウド、ユーザーエクスペリエンスなど、時代の変化に沿った監視ソリューションの提案、設計や開発に一貫して携わってきた。現在は、産業分野のサイバーセキュリティ対策を担当し、セキュリティ責任者、産業機器エンジニア、IT運用オペレーター、ネットワーク担当者といった異なる価値観の視座に立った提案をモットーにしている。国内の産業とセキュリティの2つの分野が重なる領域を活性化させ、スマートファクトリやスマートシティの促進をセキュリティ面で下支えするべく、日々、奮闘を続けている。

SCADAfenceについて

SCADAfence は、大規模な産業ネットワーク（OT ネットワーク）をもつ様々な企業が、その運用からサイバーリスクを軽減し、運用健全性を向上させることで、企業の IoT/デジタルトランスフォーメーションの推進を支援します。SCADAfence のパッシブ型プラットフォームは、大規模なネットワーク全体をカバーし、クラス最高レベルの検出精度と、機器・通信の特定及び可視化を行い、ハイレベルなユーザエクスペリエンスを提供します。SCADAfence は OT セキュリティの機能を既存のセキュリティ運用へシームレスに連携し、IT/OT の融合を促進させます。SCADAfence は、ヨーロッパ最大の製造工場を含む、世界でもっとも複雑な産業ネットワークに高度なセキュリティと運用健全性を担保する機能を提供し、製造・ビルマネジメント及び社会インフラの分野における安全かつ効率的なデジタルトランスフォーメーション推進を支援します。詳細は https://www.scadafence.com/ja をご覧ください。

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence