ホワイトペーパー

産業用制御システム(ICS)サイバーセキュリティ

運用の安全性、セキュリティ、信頼性を
向上するためのインサイト

splunk>
turn data into doing™

概要

産業用制御システム(ICS)のサイバーセキュリティは、現場の問題であり、かつ経営レベルの問題でもあります。ICSへのサイバー攻撃は従業員、顧客、環境の安全を脅かすと同時に、組織の収益と評判を低下につながるため、まずは意識を高めることが重要です。ステークホルダーは深刻なサイバーインシデントの増加状況や全体的なサイバーリスクについて透明性を求め、CEOやCISOは、ICS環境に関する以下のような難しい質問への対応を絶えず迫られます。

- 現在、セキュリティリスクはどのレベルにあり、ビジネスへの影響はどの程度あると想定しているか。
- 従業員はICSに対するサイバー脅威を認識し、適切なトレーニングを受け、必要なときに防止策や緩和策を実行できるか。
- ITチームとOTチームの両方に対応するインシデントレスポンス計画を作成し、文書化しているか。

このガイドでは、ITネットワークとOTネットワーク間でのサイバー攻撃の連鎖、考えられるさまざまなリスク、OTネットワークへのサイバー攻撃に備えるための推奨事項について説明します。

つながり続ける世界

今日、工場内のPLCから、ガスパイプラインに沿って設置されたネットワークルーターまで、さまざまなIIoT(Industrial Internet of Things)デバイスがつながって運用を支え、データに基づく意思決定を可能にして、生産性の向上、生産や出荷の遅延防止、現場の資産の可用性向上などの成果を生み出しています。これらのスマートデバイスは、私たちの働き方にも変化をもたらしています。

従来、ICSは、固有のプロセス、プロトコル、ネットワーク、技術を使用する独立した存在でした。たとえば、オペレーターは多くの場合、工場内を歩き回って、温度や圧力などの測定値を手動で記録する必要がありました。近年では、ICSが進化して、よりオープンなアーキテクチャを使用し、インターフェイスが標準化され、社内ネットワークや場合によってはインターネットとも接続するようになっています。

この進化により、OT(Operational Technology)、生産ラインやシステムの制御に関する運用技術とITの統合はもはや不可避です。そこには、ネットワークを活用して、予知保全、資産と車両利用の最適化など、ニーズの高い新しいサービスを導入し、ビジネスの価値を向上できるというメリットがあります。一方で、テクノロジーの進化とデジタル化は、脆弱性を増やし、標的型と無差別の両タイプのサイバーセキュリティ脅威にさらされるリスクを高めるというデメリットもあります。IIoTのROIを実現するには、最終的に、ICSさらにはOT環境全体を適切に管理し、セキュリティを確保することが欠かせません。

OTとITがつながる世界とは

産業界では、ここ数年の間でITシステムとOTシステムの統合が進んでいます。多くの産業施設ではすでに、Windows PCでHMI (ヒューマンマシンインターフェイス)アプリケーションを使用して、現場や機器の状態をチェックし、指示を送っています。組織全体でデバイス、人、プロセスをつなぐという考え方は新しいものではありませんが、ネットワークに接続するアプリケーションやサービスの活用は近年になって活発化しています。

OTとITが完全に統合した環境では、OTネットワーク上のインテリジェントデバイスが社内アプリケーションや社内インフラに接続します。これにより、データに基づくより的確な意思決定が可能になります。しかし、制御システムやデバイスが多様化する中で、ネットワークについては多くの企業がセグメント化の基本方針を維持し、ITネットワークとOTネットワークを切り離しています。これでは、IIoTを最大限に活用することはできません。

ただし統合環境では、OTネットワークを出入りするトラフィックを完全に可視化して管理できなければ、サイバー攻撃を受けたときに、攻撃者はIT環境とOT環境の間を容易にすり抜けてしまいます。制御システムや、ネットワークに接続する資産(PLC、オペレーターのワークステーション、従来型のサーバーなど)への侵入を許してしまうと、重要なインフラやサービス、環境全体、ときには人間の命までをも脅かす物理的かつ破壊的な被害につながりかねません。

OTのサイバーセキュリティの課題

SANS Institute社が公開した「ICSのセキュリティに関するインサイト」によると、脅威は変化し続け、攻撃の特定が難しい一方で、基本的なセキュリティ対策が無視されがちです。これらの課題の一因は、従来、OTネットワークがサイバーセキュリティ対策の対象から外れているか、独自のセキュリティツールで管理されているために、セキュリティ態勢を包括的に把握できないことにあります。

レガシーテクノロジーを使用した運用システムは稼働が止められない

パッチ未適用のシステムが攻撃されたというニュースは近年でも盛んに報じられています。それにもかかわらず、ICSにパッチを定期的に適用していない企業や、パッチ適用のポリシーと手順を定めていない企業がいまだ少なくありません。多くの場合、これらのシステムはかなり以前に開発され、古いバージョンのMicrosoft Windowsに依存しています。「WannaCry」をはじめとするランサムウェアが猛威を振るったとき、Microsoft社は、攻撃対象になるコンピューター数を減らすため、Windows XPを含め、サポートが終了したオペレーティングシスム用のパッチを提供しました。しかし、産業用システムは稼働し続けなければならないため、多くの現場では脆弱性の修正パッチの適用は検討すらされません。

ITチームとOTチーム間でセキュリティに対する意識が違う

ITとOTの間でセキュリティ戦略に差があることは明らかです。ITチームは動的な環境で業務を行い、総じて、財務情報、顧客情報、知的財産、企業情報などのデータを保管するシステムのセキュリティを重視しています。そのため、多くの時間を費やして、ソフトウェアやハードウェアテクノロジーを最新の状態を保ち、システムのパッチ適用、アップグレード、リプレースを行います。

一方、OTチームにとってセキュリティの優先度は高くありません。OTチームの業務は、生産現場、プロセスオートメーション、生産システムを管理することであり、最も重要なのは物理資産やデジタル資産の円滑稼働、安全性、可用性を維持することです。しかし、アップデートやパッチ適用を怠ると、生産ロスにつながることがあり、場合によっては機器の障害が人命にかかわるおそれもあります。

皮肉なことに、セキュリティのベストプラクティスを軽視することは、結果として、OTチームの最大の関心事であるシステムの可用性やパフォーマンスに大きな悪影響を及ぼすことがあるのです。

OT環境のセキュリティに関する知識が不足している

注目されるスタートアップ企業が提供する製品を含め、新しいOTセキュリティツールを導入することは、OTチームのセキュリティに対する意識を高めるための第一歩として理にかなっています。セキュリティツールを導入すれば、資産やOTネットワークの可視性が向上します。ただし、それだけで未知の脅威を検出、調査、緩和したりOT/ITの壁を越えて状況を明らかにしたりするための知識がOTチームの身に付くわけではありません。

運用に影響を及ぼすリスクを正確に特定してすばやく対処できないことも、ICSのセキュリティ確保を妨げる主な要因の1つです。OTチームにセキュリティに関する知識が欠けていること、そしてSCADA/ICS向けのセキュリティツールを過信しがちなこと、さらにはツールベンダーにシステムへの高いアクセス権を与えてしまうことが、問題を深刻化させています。これらの課題が相まって、ICSセキュリティ市場にちょっとした「未開の地の開拓」のような状況を生み出しているのです。

サイバー攻撃の影響

OTネットワークが外部とつながるようになった今日、攻撃に対する警戒を強め、重要なシステムを守ることが不可欠です。以下の数々の事例から、どれだけ状況が切迫しており、手遅れになる前にセキュリティ対策をとることが重要であるかがわかります。ここでは、米国の戦略国際問題研究所(CSIS)が報告した産業界のOTに関するインシデントの概要を年代をさかのぼって紹介します。これらのインシデントやその他のインシデントの詳細は、こちらからご覧いただけます。

2020年5月：ドイツのエネルギー、水道、電力企業のITサプライチェーンを攻撃してネットワークに不正アクセスしたハッキンググループをドイツ当局が特定したと報じられました。このグループは、ロシア政府の治安機関である連邦保安庁(FSB)と関連があります。

2020年5月：イランのハッカー集団がサウジアラビアとクウェートの輸送機関と政府関係者にサイバー攻撃を仕掛けた疑いがあります。

2020年5月：イスラエルのハッカー集団がイランの港を攻撃したと見られ、運用が数日にわたって混乱し、大渋滞と大規模な遅延を引き起こしました。当局はこの攻撃を、4月にイラクのハッカー集団がイスラエルの排水設備の制御システムに対して行った未遂の攻撃への報復と見ています。

2020年5月：三菱電機社に対するサイバー攻撃で最新ミサイルの詳細が漏えいした疑いがあり、日本の防衛省が調査に乗り出す事態に発展しました。

2020年5月：台湾で蔡英文総統の2期目の就任直前に2つの石油化学工場がマルウェア攻撃を受けたと報じられました。

2020年4月：イランのハッカー集団がイスラエルの下水道、水処理設備、ポンプ場の制御システムに攻撃を仕掛けた疑いがあります。

2020年4月：新型コロナウイルスワクチンの開発に取り組む米国保健福祉省の機関、医療機関、医薬品メーカーに対する攻撃の背後に中国のハッカー集団がいると米国当局が断定しました。

2020年4月：アゼルバイジャンの政府とエネルギー施設が、正体不明のハッカー集団から風力タービンのSCADAシステムを標的とした攻撃を受けたと報じられました。

2020年3月：国家が支援するハッキング集団がイランの産業分野の企業に攻撃を仕掛けた疑いがあります。

2020年1月：米国の弾劾公聴会で取り上げられたウクライナのエネルギー企業がロシアのハッカー集団に攻撃されたと報じられました。

2019年12月：バーレーンの国営石油会社であるBapco社がイラン産のワイパー型マルウェアの攻撃を受けたと報じられました。

2019年11月：米国の電力網を含む数千の組織を標的にした一連のパスワードスパイ攻撃にイランのハッカー集団が関与していることがわかりました。

2019年9月：Airbus社のサプライチェーンに含まれる4社の下請企業で、企業秘密を盗もうとするハッキング攻撃があったと報じられました。

2019年7月：中国政府が資金援助するハッカー集団が米国の複数の公益事業者に対してスピアフィッシング攻撃を仕掛けた疑いがあります。

2019年7月：ドイツの産業分野の複数の大手企業が、中国政府が資金援助するサイバー攻撃を受けたと報じられました。標的にされた企業には、Siemens社、BASF社、Henkel社が含まれます。

2019年3月：ロサンゼルス郡、カリフォルニア州、ソルトレイク郡、ユタ州の送電網運用事業者がDDoS攻撃を受けたと米国のエネルギー省が発表しました。これにより運用が一時停止しましたが、停電にはいたりませんでした。

2019年3月：世界各国の200社以上の石油/ガス企業および重機企業の数千人の関係者がイランのハッカー集団から攻撃を受けたと報じられました。この攻撃は、企業秘密を盗み出した後、攻撃対象のコンピューターからデータを消し去ることが狙いであったと見られます。

2018年7月：イランのハッカー集団が、米国、欧州、東アジア、中東の電力会社のICSを標的に攻撃を仕掛けた疑いがあります。

2017年12月：Schneider Electric社が、1つの電力プラント(場所は非公開)でICSを標的としたマルウェア攻撃を受け、運用を停止したと発表しました。識者の多くは、攻撃を受けたのは中東のプラントと見ています。

2017年10月：米国の国土安全保障省とFBIは、ロシアが関与するハッカー集団が米国のエネルギー企業をはじめとする基幹インフラ企業のICSを標的とした攻撃を計画していると警告しました。

米国の国土安全保障省とFBIは、ロシアのハッカー集団が米国政府機関および原子力、水道、航空、エネルギー関連企業のICSとその他の基幹インフラへの攻撃を計画していると警告するレポートを発表しました。

紹介した攻撃の多くは、巨額の経済的損失につながり、人命をも脅かすリスクがあります。しかも、このような攻撃は増加の一途をたどっています。ハッカーの世界ではICS専用の攻撃フレームワークが次々と出回り、その多くでは、標準的なICSセキュリティツールと同じような資産検出方法が使用されています。ICS専用マルウェアやランサムウェアを含むこれらの攻撃ツールキットは簡単に手に入り、すでに外部の攻撃者や内部犯行者の手に渡っています。これらのツールキットは、一度仕掛けてしまえば、内蔵のスクリプトやアプリケーションによって重要なデジタル資産が検出され、破壊されます。その被害から完全に回復するには長期間、ときには数カ月以上かかります。

将来に備える：ICSセキュリティの推奨事項

制御システムはもはや、社内ネットワークやその他のネットワークと切り離すことができなくなっています。ITシステムばかりを重視してOTを無視したセキュリティ戦略では、攻撃対象の想定が不十分となり、内外からの脅威にその弱点を突かれることになります。ITとOTの統合やデジタル化が進めば攻撃対象はさらに増えるため、対策は急務です。

OTネットワークに対するサイバー攻撃のリスクに対処するための推奨事項を以下に示します。

1. **OT環境を可視化して、セキュリティチームが状況を把握できるようにする**

   OTシステムを出入りするトラフィックとOTネットワークで通常行われるアクティビティを把握することは、組織を守るために役立ちます。定期的にパッチを適用できない古いWindowsコンピューターやその他のレガシー資産は特に注意深く監視する必要があります。

   ネットワークを通じたICSデバイスの監視と保護は重要な第一歩です。ルーター、スイッチ、ファイアウォールなどの既存のネットワークデバイスや生産現場に固有のテクノロジーで生成されるマシンデータを活用すれば、OT環境に対する脅威をより的確に監視、検出できます。たとえば、OT Security Add-on for Splunkでは、Splunkの先進的なセキュリティ監視/調査/分析フレーム枠をOT環境に直接適用することで、調査を迅速化し、可視性を大幅に向上して、ICS全体のリスクを低減できます。

2. **ITとOTのセキュリティ目標を整合させ、両チームが協力して目標達成に取り組む**

   ITチームとOTチームが共通のビジネス利益のために協力し合う文化を築くには、企業の上層部がリーダーシップをとることが大切です。組織のセキュリティ態勢を改善できるかどうかは、両チームが効果的に協力して相互理解を深め、重要なインフラの信頼性向上とセキュリティ強化に取り組めるかどうかにかかっています。

   この戦略は、IT/OTの統合が進みIIoTへの投資が拡大する今後数年間で重要になります。IIoTの導入が進めば、そこがセキュリティ上の弱点になる可能性があるため、重要課題として早急に取り組む必要があります。

3. **OTネットワークのセキュリティを戦略的に考える**

   アクセス制御、セグメント化、適切な暗号化レベルなど、重要かつ基本的なサイバーセキュリティコントロールは必ず実装します。また、組織のガバナンス/インシデントレスポンス計画にOTネットワークを組み込みます。セキュリティチームは、ICSについてもIT環境と同様に攻撃を検出、調査し、対応できるよう態勢を整える必要があります。OTネットワークのアクティビティを、信頼できるソースのシグネチャや動作と比較して、既知と未知の脅威を監視します。ネットワークトラフィックに異常が見つかった場合は、脅威に対する警戒を強めて、組織の環境やビジネスに大きな被害をもたらす前に対処しましょう。

   攻撃を受けてしまった場合に備えて、すばやく対処して問題を修復できるようにしておくことも重要です。OT Security Add-on for Splunkを使用すれば、SIEM市場とセキュリティ分析プラットフォームのリーダーとしてGartner社が認めるSplunkのデータドリブンテクノロジーをOTのセキュリティ対策に取り入れて、迅速に対応することが可能になります。

Splunkを使用してOT、IT、IoTのサイバーセキュリティを強化する方法については、こちらをご覧ください。

splunk>

営業へのお問い合わせはこちら：https://www.splunk.com/ja_jp/talk-to-sales.html
〒100-0004 千代田区大手町1-1-1 大手町パークビルディング 8階

www.splunk.com/ja_jp
splunkjp@splunk.com

20-14554-SPLK-ICS Cybersecurity-A4-WP-JA-202203