デジタルファクトリーにおけるデータの保護：コネクテッドファクトリーをサイバー脅威から守るには

verizon business

先進的なネットワーク機能とテクノロジーを採用するにつれ、工場の機密データを危険にさらし、製造オペレーションを混乱させる可能性のあるサイバー脅威への扉も開かれます。コネクテッドファクトリーをサイバー攻撃から保護することは、重要な情報の完全性、機密性、可用性を確保する上で極めて重要です。

デジタルファクトリーにおけるデータ保護の戦略とベストプラクティスを見出すには、以下のインサイトをご覧ください。

製造業に影響を与える主な脅威：

サイバーセキュリティの脅威は増加の一途をたどっており、日に日にその頻度と巧妙さを増しています。この傾向により、機密データは常に侵害のリスクにさらされ、重大な課題となっています。

次のようなリスクがあります。

- ランサムウェア攻撃：身代金を支払うまでデータを人質に取られる
- フィッシング：メールやWebページで人をだまし、機密データを開示させたり、マルウェアをダウンロードさせたりします
- 中間者攻撃：ハッカーが会話を傍受して操作し、相手が互いに情報を共有する代わりにハッカーに情報を共有するように騙します

このようなデータ漏洩/侵害は、研究開発（R&D）の機密資料、知的財産、市場調査、機密性の高い顧客情報、財務記録など、さまざまなデータを危険にさらす可能性があります。

製造業は現在、サイバー攻撃で一番の標的にされている

製造業は金融および保険業よりも狙われています。

新型コロナウイルス感染症の流行によって、サプライチェーンやリモートワークにおけるサイバーセキュリティリスクが浮き彫りにされました。供給の不足や一刻を争う業務、安全でないネットワーク上で個人所有のデバイスを使用する従業員などが該当します。その結果、組織データへのデバイスのアクセスを管理することが困難な課題となっています。

2022年には、サプライヤーへのサイバー攻撃が疑われた日本の自動車メーカーが、国内の全工場を閉鎖するという事件が発生しました。1日の操業停止で、14の工場と13,000台の自動車製造に影響が出ました。

また、クラウドベースのセキュリティカメラプロバイダーへの攻撃によって、米国の大手自動車メーカーの工場や倉庫のカメラがハッカーにアクセスされるという事件も起きています。

サイバーセキュリティとインダストリー4.0：スマートファクトリーがセキュリティ強化を必要とする理由

製造業がインダストリー4.0に移行し、機械、製品、人、そしてさまざまなパートナー企業がネットワークでつながるにつれ、工場内でも新たな課題が浮上しています。

この移行に伴い、従来はITから切り離されていた機器のセンサーやHVACシステムなどの運用技術（OT）は、高度な製造技術により、現在では企業のITインフラストラクチャとサプライチェーンパートナーの両方と統合されつつあります。

OTは通常、ラップトップやスマートフォン、タブレット端末ほどセキュリティが確保されていません。多くの企業は、最新の脅威の検知やその対応のための機能を持たない古いシステムを含め、このテクノロジーを適切に監視していません。このため、製造業者は、自社の全てのテクノロジーエコシステムと潜在的な脅威を正しく評価できない可能性があります。

さらに、OTはITと同じデータガバナンスの要件に従わない場合もあります。運用技術に関する決定は通常、企業のIT部門やセキュリティ担当者が関与することなく、製造現場で行われます。

このような課題と制約の中、製造業におけるOTの重要な役割と相まって、OTはハッカーにとって魅力的な標的となっています。憂慮すべきことに、運用技術に関わるデータ漏洩/侵害は昨年50%も急増しています。

このような状況が進む中で、サイバー攻撃を受ける機会も増えています。その結果、最先端のテクノロジーインフラストラクチャを備えた製造業者は、さらに高度なサイバーセキュリティ基準と強固な保護対策を必要としています。

多くのスマートファクトリーは保護対策が不十分

2021年にMcKinseyが実施した調査では、さまざまな業種にわたる100以上の企業や機関のサイバーセキュリティの成熟度を評価しました。その結果、銀行や医療の分野では大きな進展が見られたものの、あらゆる業界の大半の組織では、進化する脅威や攻撃から貴重な情報資産を守るには、まだ長い道のりが必要であることが示されました。IT/OTのサイバーセキュリティへの投資が足りないだけでなく、システムに関連するリスクに対する理解不足のために、多くの企業がデータの保護に失敗しているようです。

セキュリティ対策が十分でない企業は、次のような問題に直面しています。

- 財務的影響
- 知的財産や機密情報の損失
- 生産性の低下
- サプライチェーンの問題
- 顧客やパートナーからの信頼の失墜

重要なサイバーセキュリティ防御策の構築

企業が自らを守るためにできる最初のステップは、従業員にセキュリティソフトウェアの使い方を熟知させ、定期的に更新し、利用可能なすべてのパッチを適用させることです。

時代遅れのモノのインターネット（IoT）デバイスは、攻撃者の標的にされやすいものになっています。しかし、ファームウェアのアップデートを積極的に進める方針であるのなら、これらのデバイスに限界があることを考慮すべきです。IoT デバイスの動作は、通常、帯域幅が低く接続性が弱いため、アップデートの際にシステムに過負荷をかけ、重要な機能を停止させてしまうことがないように、バランスを取ることが極めて重要です。デバイスの安全性と最適なパフォーマンスの維持との間のスイートスポットを見つけることが重要です。

データ漏洩/侵害の80%は、盗まれた認証情報の悪用に関連しています。製造業者はIoTの認証情報を活用し、「認証された」デバイスだけをネットワークにつなげられるようにすべきです。

クラウドとオンプレミスの両方で、データの保管を適切に構成する必要があり、重要なデータをすべて一か所に保存すべきではありません。クラウドサービス、マネージドセキュリティ、その他のリソースを活用することで、製造業者は新たなサイバー脅威に対し、先回りして警戒することができます。

新しいテクノロジーを導入する前に、企業はサイバーセキュリティの成熟度、リスクプロファイル、サイバー攻撃に対する準備態勢を評価する必要があります。サイバー攻撃を模倣した脆弱性テストは、組織のIoTネットワークの欠陥を特定するのに役立ちます。

Manufacturing Leadership Councilの最近の調査によると、製造業の83%がサイバーセキュリティを非常に重要なビジネス課題として位置づけており、79%が来年に攻撃が増加すると予測しています。しかし、サイバーセキュリティに関して社内の専門知識に高い自信を持っている企業はわずか40%に留まります。

保護を強化するための強固なサイバーセキュリティフレームワークの構築

サイバーセキュリティ対策の重要なステップでありながら見落とされがちなのは、優れたサイバーセキュリティガバナンスプログラムです。このプログラムには以下が含まれます。

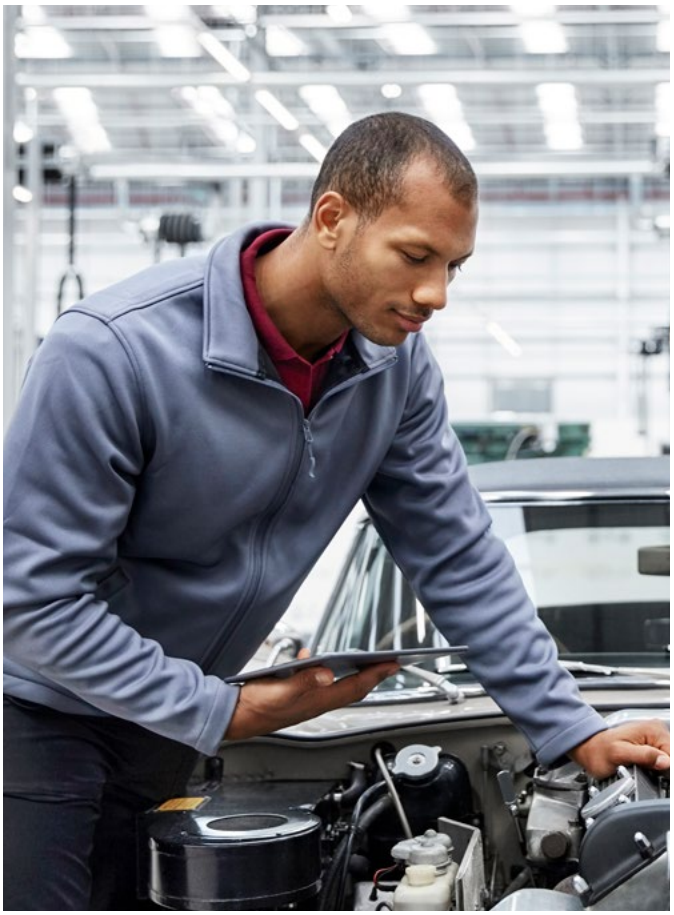
- 企業のリスクプロファイルを示すリスクマップ
- 報告のための閾値を設定したリスクエスカレーションのフレームワーク
- リスクプロファイルに基づき優先順位をつける迅速な対応と封じ込め計画
- すべてのOTおよびIT資産、それらが収集するデータ、および両者間の相互接続の最新インベントリ
- リモートワーカー、さらに、機密データ、産業用制御システム、またはネットワーク接続された製品を扱うリスクの高い従業員グループに対する特別な配慮をしたトレーニング
- ミッションクリティカルなシステムのバックアップにより、データを簡単に復元できるようにする
- 産業用制御システムおよびセキュリティ機能のセキュリティパッチおよびアップデート
- 安全に保管されバックアップされた暗号化キーによるデータの暗号化

製造業者は、リスクを効果的に管理し、十分な情報に基づいた投資決定を下し、産業用制御システムやコネクテッド製品の複雑性をナビゲートできる有能なリーダーを任命する必要があります。最高情報セキュリティ責任者（CISO）は、必要な変更やデータおよびプロセスの安全確保を導く専門知識を持つ外部パートナーを見つけるなど、これらの措置を確実に講じる上で重要な役割を果たします。そして、製造業者は、強固なセキュリティ対策への投資を厭わず、これらのソリューションによって達成される成果を真摯に評価しなければなりません。

工場の環境において、OTとITシステムの統合が進むにつれ、製造業者は組織全体の脅威を完全に可視化する必要があります。

sponsored by

verizon business



ベライゾンは、予防、検知、対応のための強力な戦略を提供しています。さらに、エッジコンピューティングやプライベート5Gなどの先進テクノロジーは、ベライゾンのプライベート5G、モバイルエッジコンピューティング、クラウドベースのサービスなどのソリューションを通じて、低レイテンシー、広帯域幅の接続を可能にします。

適切なアクションプランとソリューション、そしてベライゾンとパートナーシップを結ぶことで、今日の製造業は最も貴重なリソースであるデータを保護しながら、エンタープライズインテリジェンスへの旅をより良く進めることができます。

ベライゾンがどのようにサイバーセキュリティのオペレーションを変革し、チームが本当に重要なこと、つまり、貴社のビジネスの推進に集中できるようにするのかについてご覧ください。