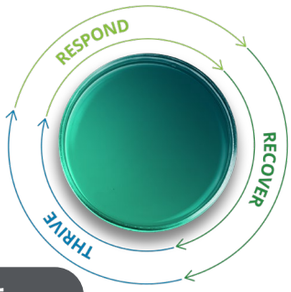
Issue 5| May 6, 2020

Deloitte.



The rise of cyber threats to supply chains amid COVID-19

COVID-19 におけるサプライチェーンに対するサイバー脅威の増加

Deloitte Cyber Threat Intelligence (CTI) が明らかにした、最新のサイバー脅威とその動向に焦点を当て、世界的な流行であるCOVID-19 パンデミックに対応、回復、成長するためのサイバーリスク管理について短期的な提言をまとめました。

COVID-19 におけるサイバー脅威の増大はサプライチェーンにとって脅威につながります.

製造業者の
10社に4社

調査の結果、過去12ヶ月*においてサイバー攻撃の影響を受けていることが判明しました。

2017年から2018年の間に、サイバーインシデントは次のように増加しています。

ランサムウェア **+3.5倍**
スピーフィング（なりすまし）**+2.5倍**
スピアフィッシング（特定のターゲットに対するフィッシング詐欺）**+0.7倍**

製造業は一貫して最も標的とされる産業の一つ

主なサイバーリスク

87% 不正アクセス
86% オペレーションの停止
85% 知的財産の窃取

$330,000
IoTに焦点を当てたサイバー攻撃による財務影響の平均、

$7.5M
2018年のデータ侵害による財務影響の平均

過去60日間で、よく知られた組織(例:UPS)を標的とした攻撃など、 COVID-19 に関連したサプライチェーンに対する攻撃が増加しています。セキュリティ要件を定義し、サードパーティ（および第四者）のサービスを評価するサイバーリスク管理プログラムを持つことで、組織はサプライチェーンへの攻撃のリスクを低減することができます。サプライチェーンでは、さまざまなベンダーが電子メールで相互にやり取りしています。2020年4月上旬、FBIは、COVID-19 パンデミックに関連したビジネスメール詐欺（ BEC ）の増加が予想されることを示す声明を発表しました。BECは、サプライチェーン上の関係を利用して、1つまたは複数のベンダーをだまし、悪意のある攻撃者へ送金させるものです。FBIによると、BEC攻撃は2019年に約17億7000万ドルの損失を組織にもたらしています。外国企業と取引を行っている企業は、従業員が外国企業の異常な行動を認識できない可能性があるため、BEC攻撃の影響を受けやすくなっています

サプライチェーンにおけるサイバー脆弱性が増加しています

この世界的大流行を踏まえてサプライチェーンがどのように変化しているかをより深く理解することは、小売業者やその他の企業が、この未曽有の困難な時期に、安全を確保、適応し、前進するのに役立つでしょう。2019年には、製造業者の40%がサイバー攻撃の影響を受けました。サプライチェーンは既に閉鎖のリスクに直面しており、ソーシャルディスタンス（社会的距離）による今後の事業の縮小や、個人用防護具を製造するための事業再構築などで、サイバーインシデントによる更なる混乱は、より深刻な影響を与える可能性があります。今週は、サプライチェーンの要素を標的とした脅威の高まり(4月22～28日付の脅威報告書より)について取り上げます。

フィッシングキャンペーンによる大手運送会社への影響

影響範囲:全業種|地域:グローバル

2020年4月、Deloitte CTIは COVID-19をテーマにしたフィッシング詐欺2件とマルウェア1件を確認しました。これらの COVID-19 のフィッシングキャンペーンは、「FedEX」「DHL」「UPS」といった有名な運送会社になりすまし、悪意のある添付ファイルを用いて米国を拠点とする医療機関を標的にしたものでした。

ビジネスメール詐欺 (BEC) による不正送金

影響範囲:全業種|地域:グローバル

2020年4月15日、Deloitte CTIは、COVID-19 をテーマにビジネスメール詐欺を行っている企業に対して複数のスパムキャンペーンを観測しました。これらの攻撃では、給与計算、電信送金、法務関連のソーシャルエンジニアリングなど、 COVID-19 をテーマにしたメールを使い、標的に不正な送金を要求していました。

根本原因 | COVID-19 期間中の制御システム (OT) 環境におけるリスクの軽減

多くの大手メーカーが、個人用防護具や人工呼吸器、さらには新しいワクチンなど、重要な COVID-19 対応製品の生産に向けて世界規模で競争しているため、貴重な知的財産につながる脆弱性を悪用しようとするサイバー攻撃者によって、盗難や恐喝の標的にされる可能性があります。事業環境がダメージを受ける可能性は、収益に大きな影響を与え、事業を完全に停止させる可能性があります。拡張されたサプライチェーン全体にわたるリスク管理は、しばしば困難を極めます。大企業では、サブコンポーネントに何かを組み込んでいるサプライヤであろうと、ソフトウェア製品であろうと、第三者、第四者および第五者といったさまざまな関係者を考慮する必要があります。接続されたコンポーネントが増え、データを通信し保存するようになると、リスクが高まり、攻撃対象が拡大します。新型コロナウイルスによる不確実性の時代は、私たちが思っていたほど「何にでも」備えているわけではないことを示しています。ITエコシステムとOTエコシステムの間には、人、プロセス、テクノロジーが重なる部分が多くあります。以下では、ITとOTの事業全体での統合を目指す製造業者が認識すべき、サイバー上の重要な懸念事項に焦点を当てています。

OTシステム特性*	サイバー上の懸念
ITとOTの統合の複雑さ	• OTは通常、ITではなくエンジニアリング、自動化、運用によって管理されます。 • 一般的に、すべてのOTシステムとその基礎となるセキュリティに責任を持つ単一のチームは存在しません • 適用や脆弱性スキャンなどの従来のセキュリティ制御の適用は、通常、詳細な評価を行わないと実行できません。 • 産業プロセス、テクノロジー資産、ネットワークアーキテクチャ、リスク、およびセキュリティアプローチに関する深い知識が不可欠な場合が多く、ITとOTの両方で共に作業する統合されたチームが必要になります
更新のパラドックス	• システムにパッチを適用したり更新したりするためのアプローチは単一ではありません。そのため、脆弱性が検出されたときの対応が難しくなり、多くの場合、多層防御（Defense in depth）のアプローチを採用する必要性が生じます
レガシーシステムの挫折	• 多くのシステムはライフサイクルが長く (10年以上)、外部から接続するように構築されていません。エッジコンピューティング、クラウドプラットフォーム、およびその他のスマートファクトリーテクノロジーの採用の増加に伴い、エアギャップはもはや実行可能な選択肢ではなくなりました。
不安定なインフラ	• 古い機器では独自の通信プロトコルを使用していることが多く、ネットワークセグメント内のデータ通信が増加すると簡単に中断されます。 • 既存のネットワークおよび関連アーキテクチャは、これらの新技術の採用に必要なデータフローを処理するようには設計されていません。 • 新しいテクノロジーの取得や導入に伴うセキュリティリスクを理解するための審査プロセスは限られており、この新しいテクノロジーおよび同じネットワーク上の他のレガシーテクノロジーの両方に影響を与える攻撃のリスクが高まっています。
運用上の制約	• リアルタイム機能は一般的に不可欠ですが、セキュリティ制御を追加すると、遅延が発生する可能性があります。 • ネットワークやその他の変更を行うと、ダウンタイムや停止が必要になる可能性があります。メンテナンスによるダウンタイムは、最小限に抑える必要があります。 • 製品や契約の独自性や機器の老朽化によりソフトウェアの更新ができない場合が多いです。 • 機能 (ITおよびOT) 全体にわたる明確な責任の確立が極めて重要です。各グループが何を得意としているかを考慮の上、部門横断的なチームを編成してサイバーセキュリティのリスクに対処することが重要です。

*出典: Cybersecurity for smart factories

回復と成長|「Next Normal」(新しい常識・新しい世界) に向けてサプライチェーンをセキュアに – スマートファクトリーに着目

製造業者は、COVID-19 パンデミックにおいてプロセスやプロトコルを進化させていく中で、サイバー攻撃を特定、防御、対応、復旧するため、全社規模 (ITおよびOT) の包括的なサイバー管理プログラムに投資する必要があります。具体的には、効果的な製造業サイバーセキュリティプログラムを構築するプロセスを開始する際に、以下の4つのステップを考慮すべきです。

開発された新しいテクノロジーについてサイバーセキュリティの成熟度を評価しましょう。
スマートファクトリーにおける実証実験または生産における新しいユースケースのたびに、新たに脅威へさらされることになります。評価には、OT環境、ビジネスネットワーク、そして知的財産保護、制御システム、コネクテッド製品、および産業エコシステムに関連するサードパーティのリスクなどの高度な製造業サイバーリスクを含める必要があります。

COVID-19 への対応としてOTの進化を考慮した、正式なサイバーセキュリティガバナンスプログラムを確立しましょう。
これらのガバナンス構造におけるビジネス中心の表現は、ITチームとOTチームが実用的な場面で協力し、ビジネスを管理できるようにするために重要です。製造業のセキュリティチームは、現場と密接に連携してリスクと適切な緩和戦略を検討する必要があります。

COVID-19 におけるリスクプロファイルと需要に基づいてアクションの優先順位を決定しましょう。
サイバーセキュリティの成熟度評価の結果を利用して、戦略とロードマップを作成し、経営幹部や必要に応じて取締役会と共有して、組織のリスク許容度と能力に見合ったリスクに対処します。

COVID-19 関連の技術変革にセキュリティを組み込みましょう。
多くのスマートファクトリーのユースケースはまだ計画中であり、初期段階にあるので、今こそ、これらのプロジェクトと自社のサイバーリスクプログラムを調和させる時です。プロジェクトのフロントエンドに適切なセキュリティコントロールを設計し、組み込みましょう。考慮すべき重要なコントロールには、安全なネットワーク・セグメンテーション・モデルの使用、パッシブ監視ソリューションの導入、安全なリモートアクセス、リムーバブルメディアの管理、特権アクセス管理の改善、一貫性のあるバックアッププロセスの実行などがあります。

We're by your side to help you through COVID-19

関連情報:

- **ポッドキャスト:** レジリエントポッドキャスト:企業が COVID-19 の危機に立ち向かう方法(英語)
- **記事:** スマートファクトリーにおけるサイバーセキュリティ(英語)
- **記事:** COVID-19 :組織とサプライチェーンの回復(英語)

Deloitte Cyberはダイナミックで接続された世界の進歩を促し、複雑な問題を解決して自信に満ちた未来を築きます。人間の洞察力、技術革新、包括的なサイバーソリューションを駆使して、あらゆる場所でサイバーを管理することで、社会、そしてあなたの組織がどこにいても成長できるように貢献します。


Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com


Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca


Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk


Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com


James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au


Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@Deloitte.de


Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber

Deloitte Cyberグローバルの翻訳になります。