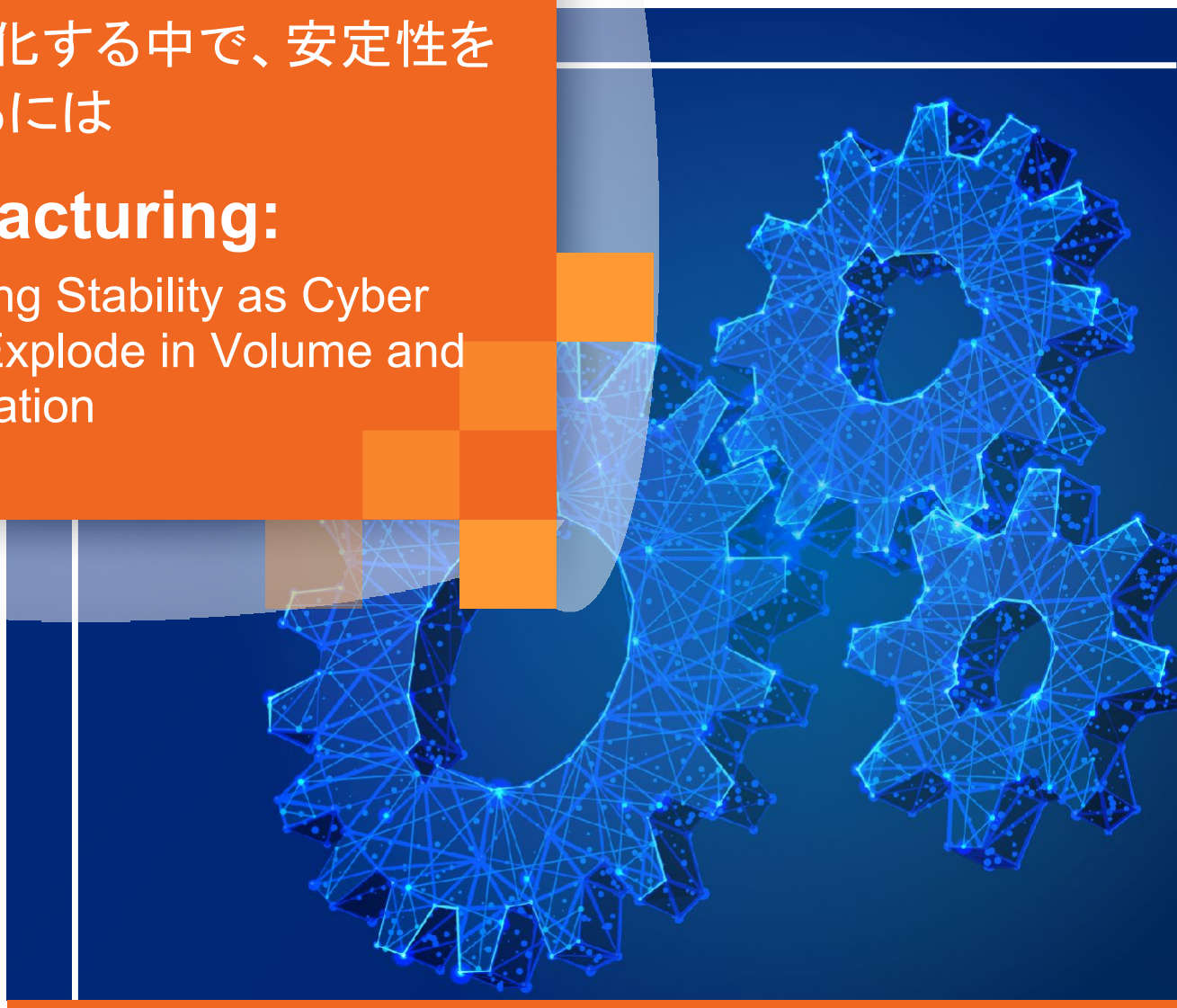
KnowBe4

製造業:

サイバー脅威が爆発的に増大し、高度化する中で、安定性を維持するには

Manufacturing:

Maintaining Stability as Cyber Threats Explode in Volume and Sophistication



製造

サイバー脅威が爆発的に増大し、高度化するなかで、安定性を維持するには

製造業のモノづくりを形成する原材料、工程、設備、労働力の4つの要素は、世界のビジネスにとってのファンダメンタルであり、世界経済の健全性の基盤となるものです。これこそが、製造セクターはサイバー攻撃者から最も頻繁に標的される理由であり、世界経済を支える製品やサービスの継続的な安定提供のためには、安全な生産環境を維持し、サイバー攻撃攻撃を防止することが、製造産業においての重要な優先事項となっているのです。

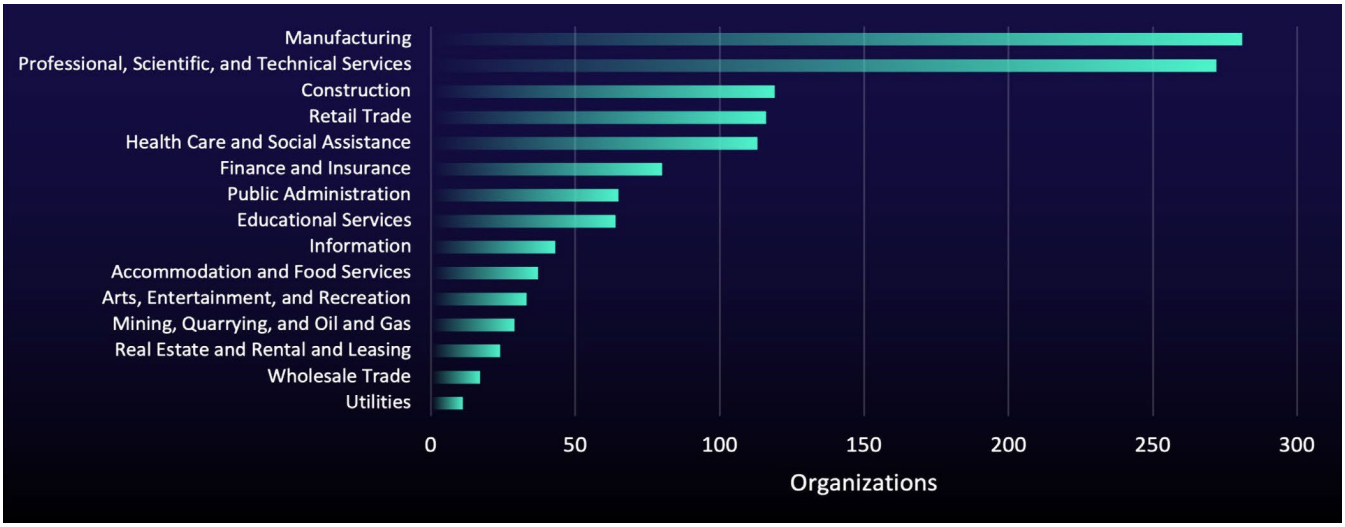
IBM X-Force脅威インテリジェンス・インデックス2024[1] によると、3年連続で製造業がサイバー攻 撃 の影響を最も受けた分野であり、そ上位10業種の全インシデントにおいて製造業の割合は25.7%に達していると報告しています。また、マルウェア攻撃は、これらのインシデントの45%を占めています。

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

X-forceの調査結果は、ReliaQuestが2024年7月に発表したレポートでも紹介されています。同レポートでは、サイバー攻撃がもたらす潜在的なインパクトの大きさとITとのOT（Operational Technology）環境との相互依存性によって、ランサムウェア攻撃の身代金要求額に決まると指摘しています。また、同時に、被害企業が身代金を支払うか否かの決定要因もこの潜在的なインパクトの大きさに依存すると指摘しています。これこそ、サイバー攻撃者にとって製造業が魅力的であることを裏付けるものです。

1 IBM X-Force脅威インテリジェンス・インデックス2024、サイト



本レポートにある2023年の統計の中には、警鐘を鳴らすべきものもあります。

- 工業製品製造業および関連サービスセクターへの攻撃が**24%増加**
- 航空宇宙産業セクターへの攻撃が**195%増加**
- 化学産業セクターへの攻撃が**92%増加**
- 自動車・関連部品産業セクターへの攻撃が**53%増加**

この統計値に示すように製造業へのランサムウェア攻撃の数は顕著な増加傾向にあり、同時に、被害組織が支払う身代金額も増加しています。2024年6月、アメリカ、ヨーロッパ、中東、アフリカ、アジア太平洋地域の製造業のITおよびサイバーセキュリティのリーダー585名を対象に実施されたVanson Bourneの調査[2]によると、昨年、製造および生産組織においてランサムウェア攻撃と恐喝による支払いが過去5年間で最高を記録したことが明らかになりました。同調査によると、製造業における平均的な身代金支払額は、昨年88%増加し、ほぼ240万ドルに達しました。

製造業がサイバー攻撃者のターゲットとしてますます魅力的になっているのには、次のようないくつかの要因があります。

サプライチェーン（業界企業間で相互に繋がる関連性）： 原材料、設備機器、電子装置、構成部品、あるいは商品や製品を市場に運ぶ自動車、トラック、船舶、航空機の輸送網など、どのようなものであれ、調達、製造、在庫管理、配送、販売、消費までの商品や製品が消費者の手元に届くまでの一連の流れであるサプライチェーンを構成するすべての要素に依存しているのです。サプライチェーンのどこかで生産ラインが停止すれば、そこで発生した欠品がサプライチェーンの全体に波及して、この影響は世界中に連鎖する可能性があるのです。

ダウンタイム（システム障害）に対する低い耐性：その他の問題としては、サイバー攻撃による生産停止が供給部品の不足を引き起こし、その結果として、継続的な製品や商品の提供を確保するには、部品調達先の変更を余儀なくされることもあります。確立されたサプライチェーンの中で部品業者を変更することはかなりの影響と困難が伴います。また、このような正規業者以外からの部品調達は、短期的にも長期的にもメーカーの収益を引き下げることになります。このようなすべての関連経費が、復旧費用やフォレンジック費用に加えて発生するものであることを明確に理解しておく必要があります。

高価値のデータ：不正に入手された企業秘密は、魅力的なものです。競争の激しい製造業の世界で競合他社の知的財産を入手することは、製品開発研究にかかる数百万ドル（数十億ドルとは言わないまでも）コストを削減でくるだけではなく、それと同時に、製品の市場投入までの期間を短縮することができます。

2 Kapko, Matt, “Ransomware attacks hit manufacturing hard in 2023," Cybersecurity Dive, June 14, 2024,, Site.

サイバー脅威の地域別の現状と代表的な攻撃事例

IBM X-forceのレポートによると、昨年に引き続き、アジア太平洋地域が最も頻繁に攻撃を受けており、報告されたサイバー攻撃の54%を占めています。2番目に多かったのはヨーロッパで26%、次いで北米が12%、ラテンアメリカが5%でした。

公表された最も影響の大きかった攻撃の代表的なインシデントをいくつかご紹介します。

ヨーロッパ

2024年8月10日、ルクセンブルクの大手化学品製造会社のOrion社は、ビジネスメール詐欺（BEC）で6000万ドルを失ったことを明らかにしました。同社によると、同社の一般社員がビジネスメール詐欺（BEC）に騙されて、第三者の口座に送金してしまたと報じています。

2024年4月、ドイツの大手自動車メーカーが、ハッカーに同社の基幹システムが侵入されたことを報告しています。ガソリンエンジン、トランスミッション開発、燃料電池、電気自動車への取り組みに関する詳細など、数年にわたって機密情報が盗み出されており、同社の研究開発に関連する少なくとも1万9000件の文書が流出したことを公表しています。

2024年4月、オランダの大手半導体メーカーNexperia社がランサムウェアグループDunghill Leakに侵入されました。Dunghill Leakは身代金を要求し、設計、製品、エンジニアリング、商業、マーケティングデータ、機密の人事ファイル、顧客ファイルなどを公開すると脅してきました。同社のクライアントには、SpaceX、IBM、Apple、Huaweiなどが名を連ねています。[3]

2024年3月7日、ベルギーの大手ビール醸造会社Duvel Moortga社がシステム内に侵入者を検知し、生産ラインの停止を含むシャットダウンを即座に実施しました。ランサムウェアグループのStormousは、同社の醸造所から88ギガバイトのデータを盗んだと、この犯行を表明し、身代金を要求してきました。

アジア/日本

2024年3月、日本の光学製品メーカーであるHOYA株式会社は、Hunters International（ハンターズ・インターナショナル）と名乗るランサムウェアグループに侵入されました。このグループは、170万種ものファイルを盗んだことを公表しました。この攻撃により、生産と販売活動が停止し、同社グループの国内外の事業所ではしばらくの間、受注業務を行うことができませんでした。[4]

2023年11月、北米でグローバルに事業を展開する中国の**自動車**内装**部品**メーカーである延鋒汽車内飾系統有限公司（YFAI：**Yanfeng** Automotive Interiors）は、コンピューターシステムに侵入され、北米での生産を停止しました。その後、ランサムウェアグループのQlinはこの犯行を証明するために、財務書類、機密保持契約、見積もりファイル、技術データシート、内部報告書などのファイルを公開しました。数か月後、プジョー、シトロエン、オペル、クライスラー、ジープ、フィアット、アルファロメオ、マセラティなど14ブランドを擁する多国籍自動車メーカーであるStellantis（ステランティス）社は、部品供給不足により生産を一時的に停止せざるを得なかったとして、Yanfengに対して2600万ドルの賠償金を請求しています。[5]

---

3 Toulas, Bill, "Optics giant Hoya hit with $10 million ransomware demand," Bleeping Computer, April 11, 2024, site

4 Bell, Sebastian, "Stellantis Demands $26M In Damages From Chinese Supplier Sparking Lawsuit," Car Scoops, April 18, 2024, site.

5 Toulas, Bill, "Chipmaker Nexperia confirms breach after ransomware gang leaks data," Bleeping Computer, April 15, 2024, site

オセアニア

2024年8月、オーストラリアの大手鉱業会社はサイバー攻撃を受けたことを発表しました。同社は、セキュリティ侵害は封じ込められたと、このインシデントについて報告しましたが、それ以上の詳細については明らかにしませんでした。

日本の大手自動車メーカーは、2024年3月にサイバー攻撃によりオーストラリアとニュージーランドの約10万人分の個人情報が流出したと報告しました。同社は、不明の脅威アクターが同社の現地法人のITサーバーにアクセスし、侵入したとこのインシデントを公表しました。

北米

2023年8月、米国カリフォルニア州オークランドに本社を置く、消費者向けおよび業務用製品の製造販売業者であるクロロックス（The Clorox Company）社が、ハッカーに侵入されました。ファイルを暗号化して、身代金を要求するランサムウェア攻撃を展開しました。本番システムはランサムウェアによる直接的な被害は受けなかったものの、受発注処理は業務支援システムなしでは、困難になりました。復旧費用は、5000万ドルを超えました。[6]

イリノイ州に本社を置くブランズウィック・コーポレーション（Brunswick Corporation）は、24カ国で事業を展開する10億ドル規模のボート製造会社です。2023年6月、同社はサイバー攻撃により基幹システムがダウンし、いくつかの地域で業務に支障が生じました。全システムの復旧に9日間を要し、この攻撃の推定被害額は8500万ドルに達しました。

カリフォルニアに本社を置くアプライド マテリアルズ（Applied Materials）社は、半導体の技術を提供する数十億ドル規模の企業です。2023年2月、同社は自社のサプライヤーの一社から発生したランサムウェア攻撃を受けました。この攻撃の推定被害額は2億5000万ドルに達しています。[7]

2023年10月、カリフォルニアに本拠を置く建材メーカーはサイバー攻撃を受けました。攻撃者は基幹システムをオフラインにし、業務を中断させました。同社の基幹システムは数ヶ月間、完全復旧することができず、同社の株価は1ヶ月で9.4%下落しました。[8]

現在の状況：攻撃者はさらに進化している

製造業におけるデジタル化の進展とデジタル接続によって、攻撃対象領域と脆弱性は拡大し、この傾向はさらに加速しています。同時に、製造業に対する攻撃の頻度と被害額は増大し続けています。チェックポイント・ソフトウェアが発表した 2024 年第 2 四半期の調査結果[9] は、恐喝を伴うランサムウェア攻撃の総数を測定したところ、製造業が再び最も攻撃されたセクターになり、製造業に対する攻撃は前年比で56%増という驚異的な伸びを示したことを明らかにしています。

---

6 Kovacs, Eduard, "Clorox Says Cyberattack Costs Exceed $49 Million," Security Week, February 2, 2024, site.

7 Greig, Jonathan, "Semiconductor industry giant says ransomware attack on supplier will cost $250 million," The Record, February 17, 2023, site.

8 Stewart, Ellis, "Simpson Manufacturing Yanks IT Systems Offline After Cyber Attack," EM360, October 12, 2023, site

9 Check Point Team, "Check Point Research Reports Highest Increase of Global Cyber Attack seen in last two years," Check Point, July 16, 2024, site.

Industry	Percent out of Published Ransomware Attacks	YoY Change in Number of Published Attacks
Manufacturing	29%	+56%
Healthcare	11%	+27%
Retail/Wholesale	9%	-34%
Finance/Banking	7%	-8%
Education/Research	6%	-3%
Software vendor	6%	-57%
Government/Military	6%	+31%
Transportation	6%	+40%
Insurance/Legal	5%	-25%
Communications	5%	+177%
Leisure/Hospitality	3%	+0%
Consultant	2%	-76%
Utilities	2%	+186%
Energy	1%	-25%

[10]

製造業者への攻撃の波は、攻撃者の攻撃拡大・実行能力および侵入の新手段開発能力の規模への高まりを示すものです。ランサムウェア・アズ・ア・サービス（RaaS）モデルが開発され、高度化されたことで、ハッカー予備軍の参入障壁が低くなったことも、攻撃の拡大を後押ししています。これは、人工知能（AI）の進歩によるところが大きく、今後数年間で攻撃者の脅威実行能力がさらに拡大・進化することが予測されています。

KnowBe4，Inc.創業者兼CEOのStu Sjouwerman（ストゥ・シャワーマン）はForbes誌で、生成AIは「ソーシャルエンジニアリングの脅威を著しく増大させている」と指摘しています。生成AIは、不自然な言い回しや誤字脱字のない、より洗練されたフィッシングメールを作成することを可能にしています。また、音声クローニングの精度が向上したことで、例えば家族を装い、家族に緊急事態が発生したとして被害者に送金させるといった詐欺が可能になるなど、その能力には憂慮すべきものがあります。

また、ストゥ・シャワーマンは、「AI大規模言語モデルが実現するようなタスクを体系的に実行できる自律型エージェントがあれば、攻撃者は高度に標的化したソーシャルエンジニアリング攻撃を大規模に仕掛けることができる」と警鐘を鳴らしています。[11]

---

10 Check Point Team, July 16, 2024

11 Sjouwerman, Stu, "How AI Is Changing Social Engineering Forever," *Forbes Magazine*, May 26, 2023, site.

製造業は進化するサイバー脅威に対してどの程度準備ができているのだろうか？

2024年7月、Infosecurity Magazine*は*、[12] は、世界の製造業の半数以上が、メールセキュリティプロトコルDMARCを適切に実装できていないなど、不必要な余分なサイバーリスクを招いていると報告しています。

世界大手製造業のる4,700以上のドメインを対象とした調査で、調査対象の5分の3（61%）が、なりすましと思われる受信メールにフラグを立てブロックすることでフィッシングを防止するDomain-based Message Authentication, Reporting and Conformance（DMARC）プロトコルを導入していることが判明しました。

しかし、DMARCを使用している製造業の44%は、プロトコルを最も安全性の低い設定にしており、スプーフィングと判定されたメールを隔離または拒否できませんでした。スプーフィングを拒否するようにプロトコルを設定していたのは、5分の1ほどでした。

2024年7月に米国国防総省の支援を受けたデジタル製造業研究所MxD（Manufacturing x Digital）とNational Center for Cybersecurity in Manufacturing（製造業におけるサイバーセキュリティのためのナショナルセンター）は、米国の製造業がサイバーセキュリティ態勢を強化することが急務であることを明らかにする報告書「Behind the Firewall（ファイアウォールの背後にあるもの）」（[13] ）を発表しました。この報告書によると、製造業はセキュリティ分野において自らの能力を過大評価しています。

- 製造業者の76%は、自社の組織がサイバーリスクを防止し、サイバー攻撃に対応できると確信している。
- 包括的なSystem Security Plan：システム・セキュリティ計画（SSP）を策定している製造業者は34%に過ぎない。これはサイバーセキュリティの基本的な要件であり、多くの場合、コンプライアンスに必要なものである。
- 最高情報セキュリティ責任者（CISO）やサイバーセキュリティ担当ディレクターなど、サイバーセキュリティ専任のリーダーがいる製造業者は、全体のわずか43%に過ぎない。大企業（従業員数500人以上）の88%に配置しているのに対し、中小企業（従業員数500人未満）では35%である。この格差は、特に顕著である。
- また、82%のメーカーが次回の予算編成でサイバーセキュリティへの支出を増やす予定である。

---

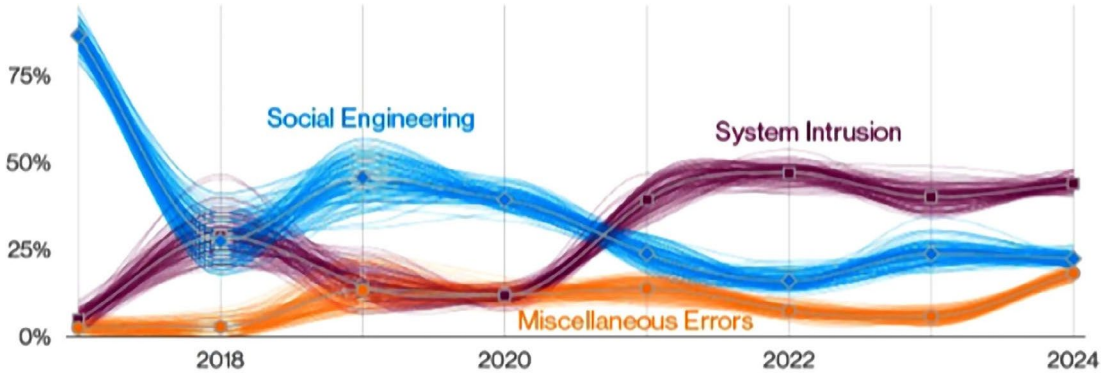
12 Muncaster, Phil, "Just a Fifth of Manufacturers Have Strongest Anti-Phishing Protection," *Infosecurity Magazine*, July 9, 2024 site.

13 Assessing Cyber Resilience in U.S. Manufacturing, MxD USA, site

フィッシングが初期侵入経路のトップ

IBMの「2024 X-Force Threat Intelligence Report（脅威インテリジェンスレポート）」は、初期感染経路のトップにフィッシングを挙げ、次いで一般公開アプリケーションの悪用を挙げています。これは、全く驚くことではではありません。

また、2,305件のインシデントを調査したベライゾンのデータ侵害調査報告（Data Breach Investigations Report）[14] は、さらに厳しいものでした。次の図に占めるように、システム侵入（System Intrusion）、ソーシャルエンジニアリング（フィッシングやプリテキスティング含む）、と「人」が関与している雑多なエラー（Miscellaneous Errors）が、インシデントの 83% の初期ベクターであると同報告書は指摘しています。システムへの侵入は、過去4年間、ソーシャルエンジニアリングを凌ぐ侵入経路となっていますが、重要なのは、侵入の25%で、盗まれた認証情報が侵入に使用されていることです。どのようにして認証情報を盗むのですか？これは、フィッシングです。



[15]

システムのアクセス後に何を目的としているか

サイバー攻撃者がアクセス権を獲得した後の行動は、製造業分野で変化しています。ランサムウェアは依然として報告されたインシデントの17%を占めていますが[16] 、製造業から取得できるデータの価値の入手は旧来の「暗号化して恐喝する」ランサムウェアの身代金を追い越し、主流になりつつあります。

製造業では、電子メール、ソーシャルメディア、メッセージング・アカウント、銀行口座情報などのログイン情報やその他の認証情報を盗むために、システムに仕込まれる情報窃盗マルウェアが266%増加しています。これらのマルウェアは、盗んだ認証情報を使って犯罪者が繰り返しシステムへアクセスすることを可能にするだけでなく、ダークウェブ上で高価格で取引されています。そのため、製造業による攻撃で最も一般的な影響の36%を認証情報の窃取が占めているのです。

重要な製造活動を守る

サイバー攻撃が個々の企業だけでなく、グローバルなサプライチェーンにも壊滅的な影響を及ぼします。このような背景の中で、製造業にとって、サプライチェーンを包括する事業継続を確保するための協調的な戦略（事業継続計画：BCP）を持つことがますます重要になってきています。このために最も基本的なセキュリティ要件を満たすには、IT人材への投資に加えて、BCPのために的確に統合されシステムが不可欠です。また、同時にシステムは最新の状態に更新することも必須です。

強固な認証や高度な脅威検知システムの導入、ソフトウェアの定期的なパッチ適用、セキュリティ監査の実施など、技術的な防御を強化することで、悪意のあるメールがITインフラに侵入しないようにすることができます。

14 Verizon Business, “2024 Data Breach Investigations Report” site
15 Verizon, 2024 DBIR
16 IBM X-Force Threat Intelligence Index 2024

しかし、サイバー攻撃の行き着く先がどこであれ、どの分野においても、ほぼすべてのサイバー攻撃（79～91%）は、フィッシングやソーシャルエンジニアリングによってサイバー犯罪者がユーザーアカウントやサーバーにアクセスすることから始まります。最後の防衛ライン、そして最も重要な防衛ラインは、最終的にはキーボードに向かう従業員です。

フィッシングやBEC攻撃を想定した定期的なトレーニングや訓練など、スタッフやユーザーがフィッシングメールや不審なアクティビティなどの潜在的な脅威を認識し、報告できるようにするためのセキュリティ意識向上トレーニングは、攻撃者がアカウントにアクセスするのを防ぐだけの守りだけではなく、サイバーセキュリティ文化を醸成し、組織全体に浸透することを可能にしてくれます。

従業員を攻撃に対する防御壁に変える

KnowBe4は毎年、ユーザーのオンライン行動を分析し、セキュリティ意識向上トレーニングを受けていない個人がフィッシングメールの不正リンクをクリックしやすいかどうかの基準値「Phish-prone Percentage™ (PPP)」をベンチマークとして測定しています。このベンチマークためのフィッシングセキュリティテストは、KnowBe4プラットフォームによるセキュリティ意識向上トレーニングを実施していない組織において、各種の業種や規模の1,100万人のユーザーを対象に実施されました。テストは事前の警告なしに実施され、専門的なセキュリティトレーニングを受けずに日常業務を行っている個人を対象としました。このベンチマークテストの基準値「Phish-prone Percentage™ (PPP) 」によると、セキュリティ意識向上トレーニングを受けていないユーザーの34%がフィッシングに引っかかりやすいという結果が出ています。つまり、セキュリティ意識向上トレーニングを受けていないコンピューターユーザーの3人に1人以上が、フィッシングメールの不正なリンクをクリックしてしまう可能性があるということです。

このベンチマークの業界別統計結果によると、小規模製造業（従業員数250人未満の製造業）では、セキュリティトレーニングを受けていない場合、フィッシングに遭いやすい割合（PPP）は27.9%と平均を下回りました。これに対して従業員数1,000人以上の大規模企業では、セキュリティトレーニングを受けていない場合、37.5%がフィッシングメールの不正なリンクをクリックしましたという結果が出ています。

このベンチマークが明らかにしたことは、継続的なサイバーセキュリティ意識向上トレーニングが有効であるということです。トレーニングを 90 日間実施した結果、従業員数が 250 人未満の製造業では、フィッシングに遭いやすい割合（PPP）が 19.6% に低下しました。中堅企業では31.6%から19.8%へ. 大規模製造業では37.5%から17.4%へと激減しました。

12ヶ月以上の継続的なトレーニングとフィッシングの模擬演習後のテストでは、従業員がフィッシングに対するサイバー防御力を大幅に強化していることが示されました。中小規模の製造業では、フィッシングに遭いやすい割合（PPP）が4.1%に低下し、大規模製造業では4.3%に低下し、全業界平均の4.6%を下回りました。

製造業がITやOTへの依存度を高めているのは疑う余地のない事実です。また、世界のモノつくりがグローバルサプライチェーンへの依存度を高めていることも疑いのない事実です。この2つの現状は、製造業の脆弱性が増大し、サイバー攻撃者にとっての魅力がさらに高めています。製造業を標的とするフィッシングやソーシャルエンジニアリング攻撃を阻止するためには、この増大・高度化する脅威に対する認識を高め、セキュリティ意識向上のためのトレーニングを実施することが、個々の企業、そして、グローバルの組織全体で、さらにグローバルサプライチェーンでの製品供給の安定性を維持する上で、ますます重要になってきています。増大するサイバー攻撃の被害の多くは、たった1回の従業員の不注意なクリックから始まっています。

その他の関連情報

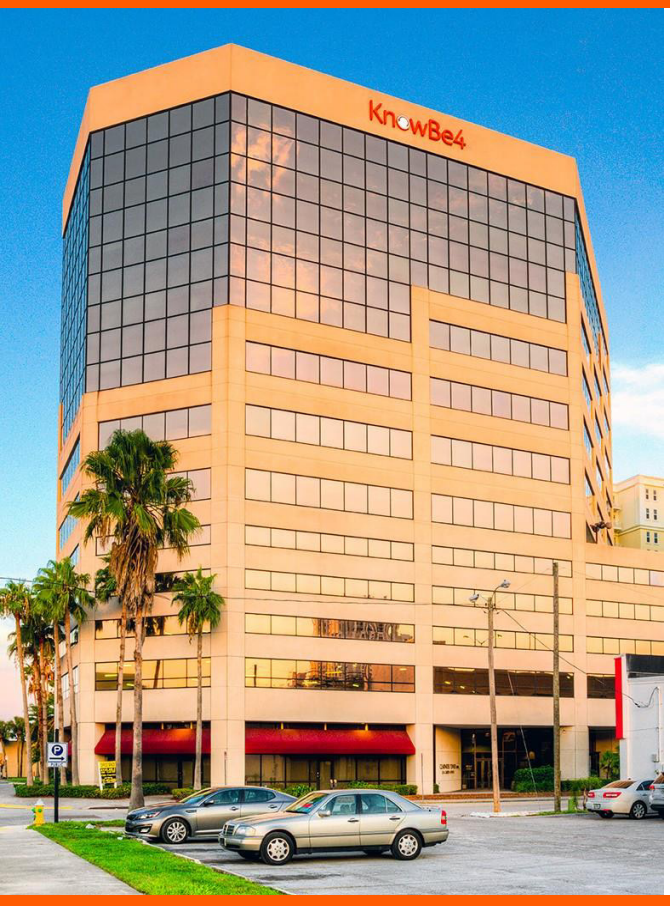
フィッシングセキュリティテスト
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。

セキュリティプログラムビルダー
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

Phish Alertボタン
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

無償Email Exposure Checkツール
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

無償なりすましドメインテスト
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。



＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、ビッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、7万社を超える企業や団体がKnowBe4を採用して、防御 の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

詳しくは、www.KnowBe4.jpをアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社 〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F EGG 内
Tel: 03-4586-4540 | www.KnowBe4.com／www.KnowBe4.jp |