サプライチェーンにゼロトラストを適用し、DMA攻撃を防止する

洗練された国家ベースの敵対者は、技術のサプライチェーンをますます標的にしています。これらの敵対者は、最終製品がエンドユーザに届けられるずっと前に、信頼できるコンポーネントの中に密かに、そして深く脅威を埋め込むことができます。最新のSSDドライブ内のファームウェアは、悪意のある行為者がデバイスを完全に制御し、オペレーティングシステムで実行されている従来のセキュリティ制御を覆す破壊的なDMA攻撃を開始することを可能にする、重要な潜在的標的を表しています。このため、SSDドライブのサプライヤとドライブ認定チームは、サプライ・チェーンのすべての段階を通じてコンポーネントの完全性を確保するために、適切な手法とセキュリティ管理を採用することが重要になります。

このホワイトペーパーでは、組織がゼロ・トラストの中核的なコンセプトを適用して、リスクを軽減し、DMA攻撃のようなファームウェアベースの攻撃を防止する方法について見ていきます。具体的には、以下の通りです:

- DMAおよびファームウェアレベルの攻撃と、それがデバイスに及ぼすセキュリティ上の影響についての紹介
- ゼロ・トラストの原則の概要と、それらがどのようにDMA攻撃およびサプライ・チェーン・セキュリティに関連しているかの説明
- サプライチェーンのすべての段階を通じて SSDの完全性を確保するために適用可能な、一連の具体的なベストプラクティスとテストの提案

本書は、ゼロ・トラストやDMA攻撃の包括的な分析を意図したものではありませんが、ベンダー、検証チーム、ITおよびセキュリティチームに、今後のセキュリティを向上させるための実践的なアプローチを提供することを目的としています。

ファームウェアベースの脅威とDMA攻撃

システム内のファームウェアとそのコンポーネントは、デバイスの起動時に最初に実行されるコードの一部であり、マシン上で最も特権的なコードの一部でもあります。このコードが侵害されると、攻撃者はシステムの起動方法を制御できるようになり、システム上の他のセキュリティ制御を破壊し、最終的にはオペレーティングシステムを完全に再インストールした場合でも、永続性を維持することができるようになります。これは非常に重要な概念で、攻撃者は、従来のセキュリティ制御のほとんどが実行されている、オペレーティングシステムのレベル以下（OSが実行される前）のデバイスを危険にさらすことができるようになるのです。このような侵害が、ストレージが存在する最も重要なシステムで発生した場合、特に問題となる可能性があります。

このリスクは、最も有害なマルウェアやランサムウェアを含む実際の攻撃にも反映されています。マルウェア「Trickbot」は、最近、「TrickBoot」と名付けられた新しいモジュールを追加し、攻撃者がデバイスのUEFI/BIOSファームウェアの読み取り、書き込み、消去を可能にする、よく知られた脆弱性がないかデバイスをチェックするようになりました。これは、ランサムウェアのRyukファミリーを含む、さまざまなマルウェアキャンペーンの持続性を維持するTrickbotの役割を考えると、重要な進展と言えます。

同様に、様々な国家レベルの脅威者が、ネットワーク機器やVPN内のファームウェアを標的とし、標的のネットワークにアクセスすることを行っています。

DMA 攻撃

DMA（ダイレクトメモリーアクセス）攻撃も、ファームウェアの脅威の重要な一例です。ダイレクトメモリーアクセスは、システム動作の正常かつ必要な部分であり、SSDドライブなどのコンポーネントが、メインCPUやOSで処理されることなく、システムメモリに直接、迅速に読み書きできるようにするものです。これにより、システムは、他の方法では不可能な高速でのデータ移動を可能にします。

しかし、攻撃者はこの同じ機能を悪用して、メモリから機密データを盗んだり、そのメモリを上書きして、デバイスのカーネル実行を制御することができます。これは、敵対者がデバイスを完全に制御し、事実上あらゆる悪意ある行為を自由に行えるようになるため、非常に強力な攻撃となります。

これは、今日のSSDドライブの文脈では特に懸念されることです。近年、多くのSSDドライブが従来のSATAインターフェイスの使用から、より高速なPCIeやNVMeの技術へと進化しています。しかし、これらのドライブは、PCIeインターフェイスを使用しているため、任意のメモリ・アドレスに対してより自由に読み書きすることができます。これは、SATAホスト・バス・アダプタ（HBA）にも当てはまります。このようなメモリへのアクセスは、PCIe/NVMe または SATA HBA の脆弱なファームウェアや侵害されたファームウェアがあれば、攻撃者がプリブート環境においてリモートでコードを実行できるようになることを意味します。このようなコードは、OSの初期状態を変更し、ハードウェア/ファームウェア層における共通の仮定を破り、OSレベルのセキュリティ制御を破壊する可能性があります。つまり、開発者がSSDからのデータ転送の高速化を追求するほど、DMA攻撃のリスクも高まるということです。

ゼロトラスト、DMA、そしてサプライチェーン

「ゼロトラスト」（ZT）は、防御を静的なネットワークベースの境界線から、ユーザー、資産、リソースに焦点を当てるように進化した一連のサイバーセキュリティパラダイムを表す用語です。「ゼロトラスト」は、物理的な場所やネットワークの場所（ローカルエリアネットワークとインターネットなど）、資産の所有権（企業所有と個人所有）に基づく資産やユーザーアカウントに、暗黙の信頼が与えられていないことを前提としています。

米国標準技術局（NIST）の特別刊行物「SP 800-207」は、ゼロトラストの概念と、そのセキュリティ運用への適用方法について詳しく説明しています。その中核となる概念の1つは、次のとおりです。

> **どのようなリソースも本質的には信頼できない。**すべての資産は、企業所有のリソースへの要求が許可される前に、PEP（Policy Enforcement Point）を通じてそのセキュリティポストを評価する必要があります。

2021年の「国家のサイバーセキュリティの改善に関する大統領令」でも、同様に「ゼロ・トラスト」の重要性がうたわれています。この大統領令は、サイバー攻撃防止のための新しい視点と方向性を導入する画期的な文書です。大統領令の2つのセクションは、連邦機関のサイバーセキュリティチームに対する明確な指令であると同時に、新たな敵の戦術に対抗する戦略を改善する必要がある民間チームに対する革新的で新しいアプローチとしても際立っています。

1. 1つは、「連邦政府のサイバーセキュリティの近代化」を求めるセクション3であり、特に政府ネットワークにおけるゼロトラストアーキテクチャの設計と実装に焦点が当てられています。

2. セクション4は、ソフトウェアのサプライチェーンを強化し、安全性を確保することに重点を置いています。大統領令の全10章は、連邦政府機関に対する明確な指示と、民間企業のCISOに対する先進的なガイダンスとなっていますが、この2章はこれまでのベストプラクティスから大きく逸脱した内容になっています。

DMA攻撃の背景におけるゼロトラスト

この2つの指令は、DMA攻撃の文脈で重要な意味を持ちます。設計上、DMA はより良い性能と引き換えに、SSD ドライブのようなコンポーネントに対して暗黙の信頼レベルを提供します。先に述べたように、これはPCIe/NVMe SSD ドライブの場合に特に当てはまります。DMA は、システム上で最も機密性の高いリソースの 1 つに直接アクセスするデバイスを信頼します。

これは、ゼロ・トラストの原則から根本的に逸脱しています。

他のセキュリティ管理によって、このような侵害がそもそも起こらないようにできると仮定して、このようなトレードオフを正当化しようとする人もいるかもしれません。しかし、ファームウェアレベルおよびブートプロテクションは、デバイスによって大きく異なり、最善の状況であっても脆弱である可能性があります。また、インサイダー攻撃に対する保護は、存在しないか、考え始められたばかりである。

©2022 Eclypsium, Inc.

もし、デバイスやコンポーネントのファームウェアが、サプライチェーンの中で危殆化した場合、それは、しばしば、システムの有効な部分として、本質的に信頼されなくなる。例えば、多くのファームウェア・チェックは、ファームウェアが予期せぬ変更を受けていないこと を検証するために、単にファームウェアの測定を行うだけである。もし、そのような UEFI の測定が行われる前に、あるコンポーネントが、サプライ・チェ ーンにおいてすでに侵害されている場合、システムは、本質的に、侵害されたコンポーネントのファーム ウェアを信用することになる。

このため、チームは、デバイス内部と、より大きなサプライチェーンの文脈の両方において、ゼ ロトラストについて考えることを余儀なくされる。内部コンポーネントとファームウェアは、本質的に信頼されることはありません。同様に、パートナーやサプライヤーから提供されるコンポーネントやシステムも、本質的に信頼できるものではありません。

SSD デバイス・メーカーと SSD の消費者にとって、これは、御社のファームウェアがもはや信頼に足るものであると仮定することができないことを意味する。SSDの信頼に値するかどうかを検証するために、ドライブの検証および適格性確認プロセスが採用されなければなりません。CISO が、より懐疑的にドライブのファームウェアを見るようになったため、ベンダーは、自社のファームウェア が侵害されていないことを保証するために、ファームウェア開発とサプライチェーンの完全性を検証する一連の慣行を 示すことができるようにならなければならない。

ガートナーは、2020年のレポート「Roadmap for Improving Endpoint Security」の中で、この議論を強調しています。"スクリプト制御が厳しくなるにつれ、ファームウェアが上級敵にとって次のエンドポイントの戦場となるかもしれない "と。

これは、実際の現場のエンジニアと同様にCISO、セキュリティ・アーキテクトの注意を喚起する論理の連鎖を引き起こします:

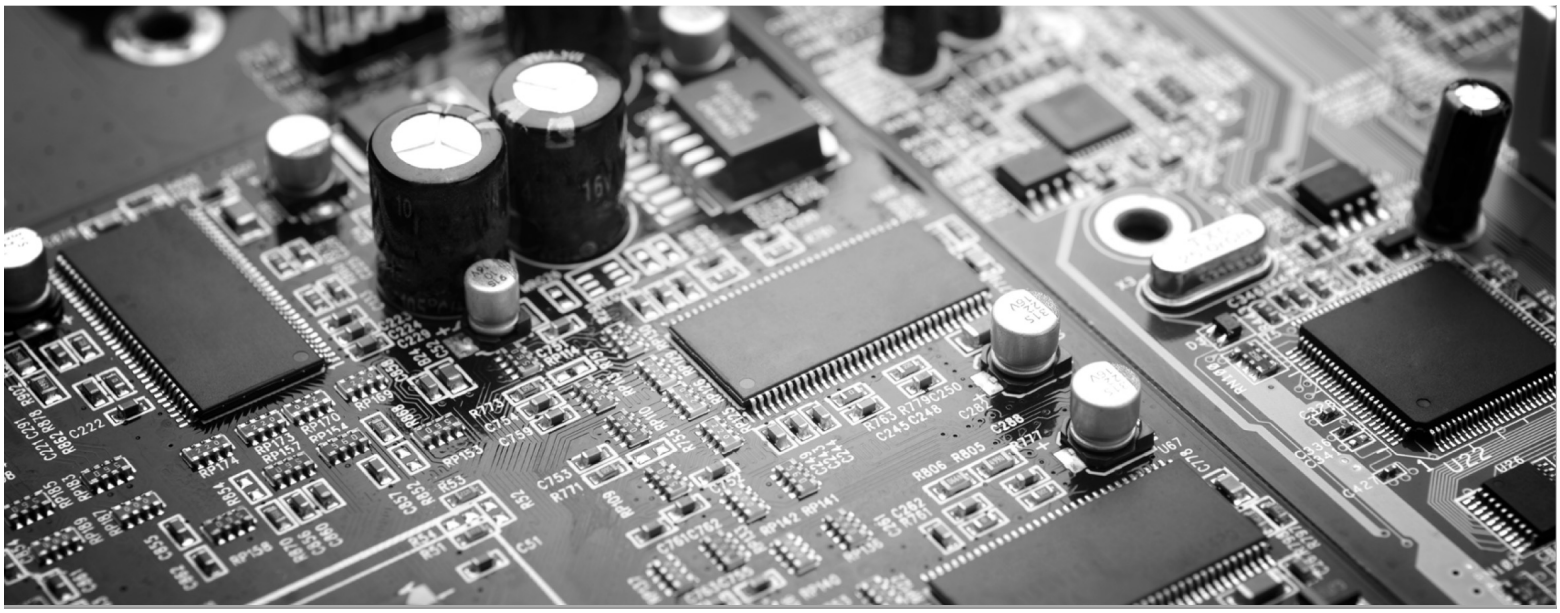
- サイバーセキュリティプログラムを成功させるためには、ゼロ・トラストの戦略、戦術、態勢に依存しなければならない。
- ゼロ・トラスト・プログラムを成功させるには、デバイス・インテグリティについて積極的に理解を深める必要がある
- デバイス・インテグリティには、ファームウェアおよびハードウェアレベルの深い発見、評価、修復の能力が必要

さらに、Equation GroupのHDDインプラントのような悪意のあるファームウェアにより、攻撃者はホストOSから見えないように悪意のあるコードをHDDに隠蔽することができました。

ゼロトラストを確立し、DMA攻撃を防止するためのベストプラクティス

技術のサプライチェーンや開発プロセスは当然ながら複雑であり、事実上すべてのステップでリスクが発生する可能性があります。システムインテグレーターとOEMは、プロセス全体を通じて、いくつかの方法でゼロ・トラストの原則を適用する必要があります。下図に示すように、SIやOEMの観点から、これらを3つの高いレベルの段階（上流サプライチェーン、完成品の統合または製造、下流チャネルを通じた配送）に分けています。次に、各フェーズでゼロトラストを実現するために適用可能なベストプラクティスの例を示しています。

なお、SI/OEMは、上流および下流のパートナーと密接に連携し、セキュリティの観点から各組織に期待されることを定義する必要があります。しかし、ゼロ・トラストは、SI/OEMがパートナーの義務を果たすことを信頼できないことを意味します。そのため、以下の各セクションでは、最終的なエンドユーザーにとって可能な限り安全で監査可能なプロセスと製品を作るために、SI/OEMができることに重点を置いています。



©2022 Eclypsium, Inc.

① ゼロトラストを上流サプライチェーンに適用する

ゼロ・トラストの一環として、OEM/SI組織は、ベンダーが提供するいかなる技術も決して暗黙のうちに信用してはなりません。すべての受信ファームウェアは、既知の脆弱性、誤設定、および既知の脅威について、スキャンされなければならないのです。評価プロセスは、供給されるファームウェアやコンポーネントを、既知の脆弱性や脅威に対してスキャンすることによって、サプライヤーを選択する以前から、開始することができます。この同じ評価は、納品されたコンポーネントの完全性を検証するために、納品された商品に対しても実施されなければなりません。Eclypsiumのようなファームウェア・セキュリティ・プラットフォームは、ベンダーを評価するために使用できるツールの一例です。主な手順は以下の通りです:

- **すべてのサプライヤのセキュリティ要件と期待を定義する** - SI/OEMは、サプライヤと協力して、サプライヤが、契約しているサブシステムサプライヤのコードを含め、納入するすべてのコードのセキュリティに責任があることを各サプライヤが認識するようにする必要があります。SI/OEM は、当然、後続のステップですべてのコードを検証する必要があります。しかし、このステップは、サプライヤが信頼できる下請け業者と協力し、サプライチェーンにセキュリティチェックをできるだけ早く導入することを保証するのに役立ちます。

- **コンポーネントとファームウェアに既知の脆弱性と設定ミスがないかスキャンする** - これらは、攻撃者が脅威を挿入することを可能にするコードの弱点です（下記を参照）。多くのベンダーが同じライブラリを再利用するため、同じよく知られた脆弱性が様々な製品に現れる可能性があります。SSD ファームウェアに脆弱性があれば、敵対者がファームウェア内に悪意のあるコードを埋め込み、DMA攻撃を行うことができるようになる可能性があります。SI/OEM サプライヤーは、すべてのファームウェアをスキャンし、既知の弱点や設定ミスを確認する必要があります。同様に、ファームウェアの保護は、ファームウェアが簡単に改ざんされることを防ぐために、適切に実装されるべきです。ファームウェアのアップデートは、ファームウェアが適切に署名されていない限り、許可されるべきではない。チームは、オープン・コンピュート・プロジェクト（OCP）のテスト（PDF）を参照し、推奨されるコンフィギュレーションや、これらのタイプのアセスメントを自動化するためのファームウェア・セキュリ ティ・プラットフォームを確認することができます。

- **受け取ったファームウェアの完全性を検証する** - SI/OEMは、サプライヤーと協働して、サプライヤーから承認された最新のファームウェアを特定し、ファームウェア部品表（SBOM）を開発するべきです。サプライヤーは、有効なバージョンと期待されるSBOMと一致することを確実にするために、構成部品を納品する前に、各機器においてこのBOMを検証しなければなりません。これは、観測されたファームウェアのハッシュ値を、それぞれのファームウェアの期待されるバージョンと暗号的に比較することによって行うことができ、また、新しいOCP 1.0 規格を参照して、ファームウェアが意図されたファームウェアであることを確認するプロセスチェックを行うことができます。

- **既知の脅威とインプラントのためにファームウェアをスキャンする** - インプラントやバックドアのようなファームウェアの脅威は、ファームウェアに埋め込まれた悪意のあるコードです。また、組織は、既知のインプラントについて、ファームウェアを評価する必要があります。善意のサプライヤーであっても、攻撃者によって無意識のうちに侵害されている可能性があります。攻撃者は、以前の悪意のあるインプラントのコードを繰り返し再利用しているため、これは重要なステップです。例えば、2020年に発見されたMosaicRegressorインプラントは、5年前にリリースされたHacking Teamインプラントと同じコードの多くを再利用しています。

©2022 Eclypsium, Inc.

- **堅牢な検証プロセスの導入** - これらのプロセスは、配信されたファームウェアが、内部者によって侵害されていないことを確認する必要があります。これは、攻撃者が有効な開発プロセスを危険にさらすという、ソーラーウインズ流の攻撃を特定するための重要なステップです。期待されるアクションとしては、コードの独立したレビュー、およびドライブの通常の使用期間中に発生する可能性のある異常な動作を探すライフサイクル認定テストが含まれるはずです。これらの認定ステップは、ファームウェアを作成する開発チームから切り離された、知られざる別個のチームによって実施される必要がある。テストは、ファームウェアの動作を監視し、未知の脅威を示唆するような異常な動作を特定するものでなければならなりません。このモニタリングを実現するために、サプライヤーは、未知の脅威を示す可能性のある 異常なアクションをスキャンする、ファームウェア・セキュリティ・プラットフォームまたはサービスを実装しなければなりません。テストまたはサービスには、Teledyne LeCroy Oakgate のメモリフェンスで見られるような、PRPおよびSGLのメモリアクセス位置を検証する手段が含まれている必要があります。不正なメモリ・アドレスを確認し、停止させることができれば、ユーザーが不正なコードをメモリ内の隠れた場所に配置することを防ぐことができます。

② ゼロトラストをOEM/SI製品の開発および生産に適用する

ゼロ・トラストの一環として、買収組織は、ベンダーが提供する技術やベンダーが実行する検証手順を決して暗黙のうちに信用してはいけません。すべてのファームウェアは、既知の脆弱性、設定ミス、および既知の脅威について、スキャンされるべきです。前の評価フェーズが、サプライヤーとそのサプライチェーンの明らかな弱点や問題を特定するのに役立つ一方で、SIの検証プロセスは、個々のコンポーネントと最終製品の両方のセキュリティについて、もう1つの詳細かつ積極的な評価を提供します。

例えば、チームは、環境をモデル化することによって、ドライブが実際にどのように動作するかを検証するテストを取り入れたいと思うでしょう。以下のステップのいくつかは、SI/OEMに存在しないレベルのファームウェアの専門知識を必要とし、組織は、プロセスを自動化するために、ファームウェア・セキュリティ・プラットフォームまたはファームウェア・セキュリティ・サービスを検討することを望むかもしれません。

- **サプライヤーの監査の実施** - SI/OEMは、SSDのような重要なコンポーネントについて、上記の許容可能なセキュリティ慣行を満たしていることを確認するためのチェックリストを、コンポーネントサプライヤーレビュープロセスの一部として実装する必要があります。安全なファームウェアを確保するための負担は、セキュリティの堅牢性のレベルを向上させるために、バリューチェーンに還元されるべきです。

- **ファームウェアの完全性を検証し、既知の脆弱性と脅威を特定するために、スキャンを繰り返す** – 品質管理チームは、既知の脆弱性、設定ミス、脅威に対して、サプライヤーが行ったのと同じスキャンを適用するべきです。このテストは、脆弱性や脅威が、最終製品の製造や組み立ての間に導入されなかったことを確認するためのものなのです。チームは、最終的に組み立てられたシステムだけでなく、個々のコンポーネントも評価することができます。ファームウェアのアップデートは、ファームウェアが適切に署名されていない限り、許可されるべきではありません。

- **ファームウェア・レベルの挙動に異常がないか観察する** - ほとんどのファームウェア・コンポーネントは、非常に予測可能な挙動を示すはずです。ファームウェア・セキュリティ・プラットフォームやサービスは、未知の脅威やカスタム脅威の存在を示す、異常な振る舞いを識別することができると判断します。そのような異常の 1 つは、SSD が、PRPとSGLメモリ記述子を尊重することになっていることです。しかし、この信頼された状態によって、プラットフォーム上の内部悪意者がDMA攻撃を開始することができます。SI/OEM は、OakGate のメモリフェンシング技術やEclypsiumのファームウェアセキュリティプラットフォームやサービスのようなツールを活用した独自のテストセットを実装する必要があります。この第2レベルのテストは、見えにくいインサイダー攻撃に対する追加の保護を提供します。SI/OEMは、サプライヤーがX国でのみ製造しているからと言って、インサイダーが侵入することはできないと仮定すべきではありません。

- **ファームウェアBOMをシステム全体のBOMに組み込む** - SSDからのファームウェアは、システム上のファームウェアのサブセットとなります。すべてのファームウェアは、パッケージングされ、最終顧客やチャネルに出荷される前に、システム上でチェックされる、独自のファームウェアSBOMに含まれるべきです。

- **サードパーティによるコード・レビューの実施** - 可能であれば、組織は、未知の潜在的な弱点や脆弱性をプロアクティブに識別するために、内部のチームやファームウェアのスペシャリストに、提供されたファームウェアのソースコードの解析を実施させるのが理想です。

©2022 Eclypsium, Inc.

③ ゼロトラストを製品流通経路に適用する

SI/OEMチームは、製品の安全性を確保し、最終顧客だけでなく下流のパートナーも容易に監査できるようにするための措置を講じる必要があります。SI/OEMの管理下を離れた製品のセキュリティをSI/OEMが直接管理することは、当然ながら難しくなります。その結果、このフェーズでは、あらゆるファームウェアが不正な改変から保護されていることを確 実にすること、パートナーと協働して、必要となり得る追加の検証を確立すること、および、パートナー と最終顧客が、受け取った製品の完全性を容易に検証できるようにすることに焦点を合わせる必要があります。

- **ファームウェア・レベルの保護とセキュリティ構成の検証** - SI/OEMは、SSDや他のコンポーネントのファームウェアが、第三者によって容易に変更できないように適切に構成されていることも検証する必要があります。たとえば、チームは、すべてのファームウェア・アップデートが、コミットされる前に、暗号化された 署名が要求されることを確認する必要があります。この基本的な保護がなければ、ファームウェアは、サプライチェーンのどの時点においても、容易に改変される可能性があるのです。もう一度言いますが、OCP テスト、あるいは、専用のファームウェア・セキュリティ・プラットフォームは、これらの問題を特定するために使用することができるのです。

- **重要なファームウェアのためのSBOMを確立する** - 前述の大統領令のセクション4は、「重要なソフトウェア」が、その意図した完全 性を維持することを保証するために、ソフトウェア部品表（SBOM）を持つという要件に、大きく焦点を当てています。この命令では、買収と配備のプロセスを通じて、自社の機器を検証するために、ベンダーに完全なSBOMを求めるよう、組織に特に奨励しています。SI/OEM は、自社のファームウェアのSBOMを秘密裏に提供することで、下流のパートナーや消費者が、自社製品の完全性を検証することを、より容易にすることができます。箱を開け、コンポーネントを追加するチャネル・パートナーは、SI/OEMによって、組み立てプロセスの一部として、SBOMを検証するよう要求されるはずです。追加されたコンポーネントがファームウェアを持つ場合、SBOMは、最終顧客に送る前に更新される必要があります。これは、SI/OEM、チャネルパートナー、エンドユーザーの間で製品が変更されていないことをエンドユーザーが確認する方法を提供するため、特に重要です。

- **下流チャネル・パートナーのためのセキュリティ要件を設定する** - ファームウェアの完全性と脆弱性のチェックは、製品が開かれたり変更されたりした場合は常に適用されるべきです。パートナーが製品を開封して変更を加える必要がある場合、SI/OEMは、製品が変更されていないことを保証するために、チャネルパートナーが適切なコントロールを持っていることを要求する必要があります。これらの要件は、防衛産業やその他の重要なインフラストラクチャを対象とする製品に特に当てはまります。

要約/結論

SSDを使用したDMA攻撃などのファームウェアの脅威は、非常に大きな被害をもたらす可能性があるにもかかわらず、発見が困難です。このような脅威をサプライチェーンに導入することで、敵対者や脅威主体は、個々のターゲットに侵入することなく、幅広い顧客に脅威を提供することができます。現代のサプライチェーンは複雑であるため、システムインテグレーターやOEMはこのリスクについて深く考え、プロセス全体にゼロ・トラストの原則を適用することが必要です。低いレベルでは、これらの組織は、システム内の個々のコンポーネントが決して信頼されていないことを確認する必要があります。特に、DMA対応のコンポーネントには、ダイレクトメモリーアクセスに関連する固有の信頼性があるため、注意を払う必要があります。同様に、組織はパートナー、サプライヤー、顧客との関係のレベルでもゼロトラストにアプローチする必要があります。システムインテグレータとOEMは、サプライヤから受け取るコンポーネントの状況と整合性を継続的に検証するプロセスを導入しなければなりません。同様に、下流のパートナーや顧客も、受け取る最終製品を検証できるようにしなければなりません。

これにはある程度の計画と努力が必要ですが、組織はこのプロセスを自動化し、製品の最高レベルのセキュリティを確保するために必要なツールやサービスを備える必要があります。

©2022 Eclypsium, Inc.

参考文献

Ross Stenfort (Facebook), Ta-Yu Wu (Facebook), Lee Prewitt (Microsoft) ,Paul Kaler (HPE), David Derosa (HPE), William Lynn (DellEMC), Austin Bolen (Dell EMC), (2021) Open Compute Project.The Open Compute Project: データセンター向けNVMe SSD仕様
https://www.opencompute.org/documents/datacenter-nvme-ssd-specification-v2-0r21-pdf

Scott Rose (NIST), Oliver Borchert (NIST), Stu Mitchell (Stu2Labs), Sean Connelly (DHS), (2020) ゼロトラストアーキテクチャ, SP 800-207
https://csrc.nist.gov/publications/detail/sp/800-207/final

Peter Firstbrook (Gartner)（2018）エンドポイントセキュリティ向上のためのロードマップ、G00343353
https://www.gartner.com/en/documents/3879573/roadmap-for-improving-endpoint-security

ホワイトハウス（2021年）国家のサイバーセキュリティの改善に関する大統領令
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

©2022 Eclypsium, Inc.