National Institute of Standards and Technology
U.S. Department of Commerce

サイバー サプライ チェーン リスク マネジメントのケース スタディ

業界からの報告

Palo Alto Networks, Inc.

インタビュー:
Jason Ledgerwood - サプライ チェーン オペレーションおよび調達担当副社長
Brian Riggs - サプライ ベース マネジメント専務理事
Jim Sugg - シニア プロダクト マネージャー
Shae Trautwein - サプライ チェーン リスクおよびコンプライアンス マネージャー

2020年2月4日

本書は以下のサイトから無料で入手できます。

https://doi.org/10.6028/NIST.CSWP.02042020-6
(official English language version)

Jon Boyens
Celia Paulsen
コンピュータ セキュリティ部門
ITラボ

Nadya Bartol
Kris Winkler
James Gimbi
ボストン コンサルティング グループ

シリーズの説明

サイバー サプライ チェーン リスク マネジメントに熟達した複数の企業が関わる*サイバー サプライ チェーン リスク マネジメントのケース スタディ*のシリーズです。これらのケース スタディは、2015年に最初に公開された「Best Practices in Cyber Supply Chain Risk Management」のケース スタディをベースにしています。その目的は、新しい産業の新しい組織を網羅し、サイバー サプライ チェーン リスク マネジメントの実践における変化を明らかにすることでした。

NISTのサイバー サプライ チェーン リスク マネジメント プロジェクトの詳細については、https://csrc.nist.gov/projects/cyber-supply-chain-risk-managementを参照してください。

免責条項

商品または組織に関するすべての言及は情報提供のみを目的としたものであり、米国立標準技術研究所(NIST: National Institute of Standards and Technology)による推奨または推薦を示唆するものでもなく、特定された製品が目的に対して最良の選択であると示唆するものでもありません。

目次

企業の概要

Palo Alto Networks, Inc. (通称、パロアルトネットワークス)はカリフォルニア州サンタクララに本拠を置く米国の多国籍サイバーセキュリティ企業です。パロアルトネットワークスは世界有数のサイバーセキュリティ製品メーカーであり、代表的な製品には次世代ファイアウォール(NGFW)、クラウドベースのセキュリティ サービス、先進のエンドポイント プロテクション、脅威インテリジェンスなどがあります。サイバーセキュリティ製品は、官民の区別なく組織の重要なイネーブラーであり、150か国、60,000以上の企業組織でパロアルトネットワークスの製品が採用されています。

リスク プロファイル

セキュリティおよびデータの保護は、サイバーセキュリティ製品の提供者であるパロアルトネットワークスの役割と不可分の関係にあります。世界中の数千にも及ぶ企業および政府組織がこれらの製品を信頼して、機密性の高い情報を保護しています。パロアルトネットワークスにとって、サイバーセキュリティとプロダクト インテグリティは絶対的な企業義務です。

サイバー サプライ チェーン マネジメントの注目すべき実践

- **エンドツーエンドのリスク管理:** すべての製品がパロアルトネットワークスのエンドツーエンドの製品セキュリティ フレームワークに従っています。このフレームワークは、製品ライフサイクルの各段階での多層防御を提供するよう設計されたものです。
- **継続的な改善:** サイバー サプライ チェーン リスク マネジメント(C-SCRM)のプロセスは、脅威をめぐる状況の変化に迅速に対応する必要があります。パロアルトネットワークスの部門横断的なセキュリティ協議会では、C-SCRMプログラムのセキュリティ優先事項を半年ごとに見直しています。
- **官民連携:** パロアルトネットワークスは多くの官民連携の任意プログラムに参加しています。代表的なものには、米国国土安全保障省のICT Supply Chain Risk Management Task Force、米国税関・国境取締局(CBP)のテロ防止のための税関産業界提携プログラムなどがあります。これらのプログラムにおいて、パロアルトネットワークスのサプライヤーおよび幅広いセキュリティ コミュニティは堅牢なサプライ チェーンとサイバーセキュリティの実践を開発するよう促されています。
- **受託製造業者によるサイバー サプライ チェーン リスク マネジメントの簡素化:** 数千にも上るサプライヤーの関係性を管理するのは、あらゆる成熟度の組織にとって困難な課題です。パロアルトネットワークスは、明らかに入念なサイバーセキュリティおよびサプライヤー リスク マネジメントのプログラムを持つ定評ある受託製造業者を活用しています。

サプライ チェーン リスクおよびサイバーセキュリティへの組織的なアプローチ

サイバーセキュリティ ベンダーとしての役割を考えれば、パロアルトネットワークスは潜在顧客からの厳しい吟味の目にさらされるとともに、さまざまな脅威アクターの標的となっています。製品のセキュリティ インシデントが顧客に非常に大きな衝撃を与えかねないという認識に基づき、パロアルトネットワークスはサイバーセキュリティとプロダクト インテグリティを絶対的な企業義務であると考えています。すべての製品がパロアルトネットワークスのエンドツーエンドのセキュリティ フレームワーク(E2Eフレームワーク)に従っています。このフレームワークは、設計、部品調達、製造、フルフィルメント、サービスといった製品ライフサイクルのすべての段階での多層防御を提供するよう設計されています。各段階は個別に評価され、セキュリティ リスクが決定します。特定分野の専門家が、そのセキュリティ リスクを対象とした適切な公的規格およびベスト プラクティスを選択します。選択される規格には、連邦情報処理標準(FIPS)[i]、Common Criteria (CC)[ii]、英国のCommercial Product Assurance (CPA)[iii]が含まれます。

E2Eフレームワークはセキュリティ協議会が管理しています。セキュリティ協議会は、製品エンジニアリング、製品ライン管理、情報セキュリティ、製品セキュリティ、サプライ チェーン リスクおよびコンプライアンス(SCRC)、設備安全およびセキュリティ、法務の各部門から集められた部門横断的な上級管理職から構成されます。四半期ごとに開催されるセキュリティ協議会の会議で、各部門からの貢献者に対して個別に履行スケジュールが指示されます。フレームワークに基づく計画が部門横断的な活動である一方で、その結果としてもたらされる規制は最終的に各部門が所有・運用します。

E2Eフレームワークは、製造プロセスの各段階に対する強力な管理に依存しています。パロアルトネットワークスは、カリフォルニアに本拠を置く受託製造業者(CM) 1社に製品の組み立て、製造、出荷のすべてを集約して、この規制を確実なものにしています。CM、CMの二次サプライヤー、その他パロアルトネットワークスの直接サプライヤーとの関係性は、SCRCチームが一元的に管理します。

パロアルトネットワークスは、さらに広い範囲のC-SCRMコミュニティに積極的に参加しています。また、サイバーセキュリティおよびSCRMの業界カンファレンスを後援しており、ICT Supply Chain Risk Management Task Force[iv]のメンバーでもあります。このタスク フォースは米国国土安全保障省が促進する官民連携の取り組みであり、グローバルなICTサプライ チェーン エコシステムの調査、業界および政府に対する推奨事項の策定を行うことを目的としています。

パロアルトネットワークスは社内で強力なセキュリティ文化を促進しています。ロールベースの物理的および論理的な制御により、権限のある個人だけが知的財産、コンポーネント、完成品、顧客情報にアクセスできるよう徹底しています。これには、パロアルトネットワークスおよびCMの全施設における、多層の境界および内部の物理的なセキュリティが含まれます。

サイバーセキュリティのトレーニングが広範に利用でき、セキュリティは全従業員の役割の一部と考えられています。

サプライヤー管理

サプライヤーの関係性を管理するうえでの重要な側面

サイバー サプライ チェーン リスクを管理するための基準を設定する主要なメカニズムが、契約要求事項です。オンボーディング プロセス時に、新しいサプライヤーが詳細なセキュリティ評価の対象になります。これらの評価は特定のセキュリティ協議会の優先事項、NISTサイバー セキュリティ フレームワーク(NIST CSF)[v]、国際標準化機構/国際電気標準会議(ISO/IEC) 28001[vi]、その他の規格およびベスト プラクティスに基づいています。この評価によって、サプライヤーの全従業員がセキュリティ トレーニングを受けていることを確認します。また、部外者がパロアルトネットワークスのコンポーネントにアクセスできないことを立証するために評価チームがサプライヤーの工場および倉庫の設備を点検していることを確認します。サプライヤーは、FIPS、CPA、米国税関・国境取締局(CBP)のテロ防止のための税関産業界提携(CTPAT)プログラムなど、関連する要求事項への準拠を証明する必要もあります。

CTPATは、サプライ チェーン リスク マネジメント[vii]に関する米国国土安全保障省の最大の官民連携です。この任意のプログラムでは、幅広いサプライ チェーン セキュリティ保証(安全な輸送・保管、人事管理、ITセキュリティを含む)への準拠を証明するための、危険性の低いカスタム指定がパロアルトネットワークスに付与されます。この認証を維持するために、パロアルトネットワークスのロジスティクス パートナーおよびサプライヤーはプログラムのセキュリティ要求事項をすべて満たしていることをCBPに対して個別に証明する必要があります。

サプライヤー オンボーディングおよび年次セキュリティ評価に加え、サプライヤーはコンポーネントの脆弱性、データ損失、セキュリティ インシデントをパロアルトネットワークスに開示する契約上の義務を負っています。このプロセスにより、SCRCチームはサプライヤーのサイバーセキュリティ体制(潜在的なインシデントのリアルタイム アラートなど)の全容をさらに把握することができます。戦略的なサプライヤーは、サイバー インシデントの検出と対応の能力への自信を示すために、パロアルトネットワークスのサイバーセキュリティ製品を使用する必要があります。

内部的には、サプライヤーとの正式なやり取りが厳しく制御されます。初期設計および設計変更はすべて、パロアルトネットワークスの製造パートナーにリリースされる前にリリース プロセスによって管理されます。このプロセスには、設計文書、図面、部品表に対する権限のない変更が生じないよう、複数レベルの部門横断的な確認が必要とされます。権限のある変更はすべて永久的に文書化され、パロアルトネットワークスの特定の従業員が追跡できるようになります。知的財産をはじめとする機密情報は、専用のセキュアなプラットフォームを介してのみサプライヤーと共有できます。

パロアルトネットワークスは、危険性の高いサプライヤーのセキュリティ体制に投資しています。SCRCチームは、これらの企業での内部のサイバーセキュリティおよびSCRMの能力の開発に、技術的なリーダーを積極的に従事させています。専門のセキュリティ担当者がサプライヤーに対応して、パロアルトネットワークスのセキュリティ要求事項を明確にし、成熟度のロードマップを伝えます。このエンゲージメントは多くの場合、サプライヤーが他のダウンストリーム パートナーからの経験と知見を伝えることができるため、双方向のやり取りになります。

パロアルトネットワークスは、特殊コンポーネントのサプライヤーとの緊密な関係を意識的に強化

しています。NGFWなどの製品のセキュリティ ロールのために、これらのサプライヤーはパロアルトネットワークスと協力してセキュリティ パッチを予防的に配布しています。たとえば、パロアルトネットワークスはハードウェア開発会社と協力して、ハードウェアの公開リリースの準備が整う前にハードウェアレベルの脆弱性に対応する必要な緩和策を迅速に実施しています。

サプライヤーのリスクの測定

サプライヤーのリスク測定プロセスは、生産よりはるかに前の段階で開始します。リスク評価は製品開発ライフサイクルの早期に実施され、製品設計に関する意思決定の実現性を判断する際に役立ちます。エンジニアリングによって明確化されたコンポーネントの要求事項は、SCRCチームが評価します。SCRCチームは候補となるサプライヤーを評価してリスク スコアを決定します。このために、コンポーネントの相対感度、サイバーセキュリティ リスク、サプライヤーの財務状態、代替調達先の有無、コンプライアンス リスク(例: RoHS指令[viii]による義務)などの要素を審査します。

パロアルトネットワークスは、サプライ チェーン リスク マネジメントの製品スイートを操作して、各サプライヤーが示すリスクを追跡するためのユーティリティを社内で開発しました。このスイートには、インテリジェンスおよびニュースマイニング サブスクリプション サービスが含まれており、深刻なサイバーセキュリティの脅威、自然災害、政情不安、その他の破壊的な事象に関する生の情報が収集されます。このような事象は、影響を受ける可能性のあるコンポーネントおよびサプライヤーに自動的にマッピングされます。これにより、SCRCチームは混乱または供給の弱体化を予測し、対応計画を準備できます。

品質管理と継続的改善

パロアルトネットワークスは幅広いハンドリング ポリシーによって、一貫した品質管理と製品セキュリティを確保します。パロアルトネットワークスの製品の製造に関連するすべての材料は、厳格なアクセス制御と年中無休の物理的および電子的なモニタリングを用いて、施設内に保存する必要があります。CMは、パロアルトネットワークスの製品にアクセスして操作しようとするすべての対象者の身元、身元照会先、雇用記録を事前に徹底的に調査する必要があります。CMのICTネットワークは、NIST CSFやISO/IEC 27001[ix]など、十分に確立したセキュリティ基準を中核として設計されています。CMは専任のサイバーセキュリティ チームを特徴としており、第三者機関による定期的な評価(侵入テストや脆弱性評価など)を実施する必要があります。パロアルトネットワークスの製品は、特定の顧客向けに構築または実装されるものではありません。それどころか、CMは実装済みのインベントリを準備して、製造段階で売上予測を満足させ、潜在的攻撃者による特定の顧客の標的化を阻止します。

パロアルトネットワークスは、全製品を対象とした機能テストのインフラストラクチャをCMに提供します。これらのプラットフォームは社内で設計されており、ソフトウェア診断を実施してプロダクトインテグリティを確保します。テストはCMが実施しますが、テストのインフラストラクチャはパロアルトネットワークスの管理下のままとなります。テストされた製品には不正開封防止の包装が施され、部品番号やシリアル番号などの固有の製品IDを特徴とする出荷ラベルが貼り付けられます。これにより、運送中に侵害された製品を顧客が受け取らないよう徹底します。パロアルトネットワークスは、顧客の選択した宅配業者が製品の所有権を得る場合に配達のリスクを顧客に移しますが、それと同時に、すべてのハードウェア製品がソフトウェアの整合性チェックを活用して輸送時のソフトウェアの細工を防止しています。

デコミッション済みデバイスからの顧客情報への不正アクセスを防止するために、返却された顧客のストレージ ドライブはすべて、アメリカ国防総省(DOD)の手順に従って論理的に消去されます。除却済みのドライブは破壊されます。顧客は請求すれば破壊証明書を入手できます。

継続的な改善はE2Eフレームワークの組み込み機能であり、パロアルトネットワークスが脅威の状況の変化に確実に順応できるようにします。可視性は部門横断的なE2Eフレームワーク全体の包括的観点を発展させる一方で、継続的な改善のプロセスに不可欠な要件です。セキュリティ協議会は各部門と協力してプログラムの現在の状態の「スナップショット」をキャプチャし、実装スケジュールと比較評価します。この進捗は完全に文書化されるため、セキュリティ協議会は製品セキュリティ プログラムの策定を追跡し、潜在的な盲点または重複を特定できます。セキュリティ協議会は定期的に会議を開いてチェックポイントを確認し、それに応じてプログラムのセキュリティ優先事項を見直します。

顧客は定期的にパロアルトネットワークスのセキュリティと供給の実践に関する情報を要求します。多くの顧客はシステムおよび組織の制御レポートまたはシンプルなアンケートの共通のコピーを要求しますが、顧客によっては、例外的な情報または特定の情報を必要とする場合もあります。SCRCチームは各要求の性質を慎重に追跡して、サイバーセキュリティおよびサプライ チェーン リスク マネジメントのロードマップを伝えます。

インシデント対応と回復

SCRCには、潜在的なセキュリティ インシデントの検出および対応をサプライヤーのコミュニティ全体にわたって行う責任があります。自動モニタリングは別にして、契約で定義された報告義務により、SCRCは影響を受けたサプライヤーから直接インシデント レポートを受領する可能性があります。

また、パロアルトネットワークスは独立したセキュリティ リサーチャーと提携しています。このセキュリティ リサーチャーは、ISO/IEC 29147:2018[xi]で定義された調整済みの脆弱性開示プロセスに準拠する専用のセキュリティ開示サービス[x]を通じて、潜在的なセキュリティ リスクを特定します。

製品の組み立てに伴うすべてのコンポーネントは、シリアル番号、ロット コード、日付コードにより生産のあらゆる段階で個別に追跡可能です。これにより、SCRCチームは製品のセキュリティ インシデントを特定のサプライヤーまたはテストの失敗まで遡って突き止めることができます。パロアルトネットワークスは供給の途絶による影響を緩和し、重要な予備製品のバッファ数を維持するために、可能な限り複数のベンダーからコンポーネントを供給したいと考えています。このバッファはコンポーネントの重要度および可用性に応じて異なります。景気予測の変化、ベンダーの安定性の問題、セキュリティ イベント、または世界的な出来事への大規模な対応の一環に対応するよう、調整することもできます。

確認済みのインシデントによって、正式なインシデント対応計画(IRP)がトリガーされます。SCRCおよびセキュリティ オペレーション センターはそれぞれの領域内でのインシデントの処理を担っていますが、両方の領域に影響を及ぼすインシデントに対応するときはIRPを通じて双方が協力します。契約上、サプライヤーはインシデント発生時にパロアルトネットワークスと協力する義務を負っています。また、両方の会社に影響を及ぼすインシデントをさらに効果的に管理するために、オンボーディング プロセス時に内部のインシデント対応手順を提供する必要があります。

SCRCチームは部門横断的な机上の演習を定期的に実施して、制御された文脈に機能のギャップがないか割り出します。机上演習は動的なインシデントのシミュレーションであり、利害関係者(パロアルトネットワークスおよび重要なサプライヤーからのチームを含む)とともに実施します。

教訓および改善の機会

パロアルトネットワークスのサイバーセキュリティ製品の性質には、膨大な量の複雑なリスク管理が必要です。信頼できるサイバーセキュリティ製品は、製品ライフサイクルのあらゆる段階(設計からサービスまで)での脅威に対応できるものでなければなりません。製品開発の各段階におけるパロアルトネットワークスの徹底的かつ包括的な製品セキュリティのアプローチが固有の課題に対応し、潜在的な脆弱性を発見します。

パロアルトネットワークスが推奨するのは、C-SCRMプログラムの熟成または開発に関心のある組織が以下の信条を考慮したうえでアプローチの設計を行うことです。

- プログラムは、製品ライフサイクルのあらゆる段階をカバーするエンドツーエンドの制御を特徴とするものでなければなりません。
- 組織は補償管理を実施し、多層防御を実践する必要があります。
  各層の防御で攻撃に摩擦を加えるため、基本的な制御であっても、幅広い侵害を抑止、停滞、阻止することができます。
- セキュリティのための資源を無限に利用できるプログラムはありません。したがって、組織は考え抜かれた動的な優先度設定プロセスに投資する必要があります。
- 組織はセキュリティ重視の文化を促進し、基本的なプロセス予防策を実施する必要があります。

これらの信条を効果的に実施するには、経営者/役員の支援が必要です。したがって、プログラム設計プロセスの早い段階で部門横断的な上級管理職が関与することをパロアルトネットワークスは推奨します。

参考資料

[i] Federal Information Processing Standards Publications (FIPS PUBS)、米国立標準技術研究所、https://www.nist.gov/itl/itl-publications/federal-information-processing-standards-fips、(2019年9月26日取得)
[ii] ISO/IEC 15408: Common Criteria、国際標準化機構、https://www.commoncriteriaportal.org/、(2019年9月16日取得)
[iii] Commercial Product Assurance (CPA)、英国家サイバーセキュリティセンター、https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa、(2019年9月26日取得)
[iv] DHS Announces ICT Supply Chain Risk Management Task Force Members、米国国土安全保障省、https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members、(2019年9月24日取得)
[v] Cybersecurity Framework、米国立標準技術研究所、https://www.nist.gov/cyberframework、(2019年9月16日取得)
[vi] ISO/IEC 28001: Best practices for implementing supply chain security, assessments and plans、国際標準化機構、https://www.iso.org/standard/45654.html、(2019年9月26日取得)
[vii] CTPAT: Customs Trade Partnership Against Terrorism、米国税関・国境取締局、https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat、(2019年9月16日取得)
[viii] The RoHS Directive、欧州委員会、https://ec.europa.eu/environment/waste/rohs_eee/index_en.htm、(2019年9月24日取得)
[ix] ISO/IEC 27001: Information Security Management、https://www.iso.org/isoiec-27001-information-security.html、(2019年9月24日取得)
[x] Security Disclosure、パロアルトネットワークス、https://paloaltonetworks.com/security-disclosure、(2019年9月24日取得)
[xi] ISO/IEC 29147: Information technology — Security techniques — Vulnerability disclosure、国際標準化機構、https://www.iso.org/standard/72311.html、(2019年9月24日取得)