Akamai | TechnologyAdvice

マイクロセグメンテーションでコマース業界のゼロトラストに変化を起こす

小売業、旅行業、ホテル業を営むコマース企業は、サイバー犯罪者やランサムウェアギャング、それに機密性の高い企業データや財務データを盗み金銭を得ようと企んでいる犯罪者にとって格好の標的です。RH-ISAC の業界動向に関する報告書によると、盗難の被害に遭いやすい情報の種類には、クレジットカードや決済の情報、リワードプログラムやロイヤリティプログラムから得られる個人を特定できる情報（PII）、知的財産があります。

このような組織とそのセキュリティチームは、すでに攻撃者の視界に入っており、攻撃者がランサムウェアやその他のタイプのマルウェアを忍ばせる可能性がある多くのネットワーク侵入ポイントに対策を講じる必要があります。あらゆる組織がフィッシングメールや VPN 認証情報の盗難、ゼロデイ攻撃の被害からの影響に直面していますが、コマース企業の場合は、キオスク端末、IoT デバイス、店舗に置いているタブレット、POS 端末、フリー Wi-Fi などに存在するリスクにも手を打たなければなりません。煩雑さはそれだけではありません。それぞれの小売店舗は、オープンに人が出入りする環境で営業するため、物理的なアタックサーフェスも露呈し、ありとあらゆるタイプの脅威にさらされます。

セキュリティインシデントの 82% を占め、事故の大きな要因となっている人的ミスを何とか防ごうとしているエンタープライズのセキュリティ担当者にとって、不正な利益を生むデータと数多くの攻撃ベクトルの存在は頭痛の種となります。Payment Card Industry（PCI）や政府の規制（GDPR、SEC など）の監視の目が強化されると、プレッシャーが増し、すでにひっ迫している IT のセキュリティ予算とリソースの消費に拍車がかかっています。

すべてのリスクを解消することは不可能ですが、今日のコマース企業は「侵害は発生するもの」という前提に立って、回避不可能な感染の拡大や境界防御の迂回をいち早く検知し防止できるようにする必要があります。Akamai のゼロトラスト・セグメンテーション・ソリューションなら、コマース企業はアプリケーション、サーバー、ネットワーク環境のセキュリティを容易かつ迅速に確保でき、有害な暗号化の被害も機微な情報の流出も防止できます。

マイクロセグメンテーションは、ソフトウェア定義アプローチに基づく手法であり、ゼロトラストのセキュリティフレームワークの基盤となり、コマース企業に 3 つの大きなメリットを与えます。第一に、マイクロセグメンテーションは、ラテラルムーブメント（横方向の移動）を阻止するため、自然に、ランサムウェア拡散の潜在的な影響が制限されます。第二に、PCI コンプライアンスの達成と維持にかかるコストの削減に役立ちます。第三に、マイクロセグメンテーションは、ハイブリッド環境、マルチクラウド環境、マイクロサービス環境だけでなく、旧来のインフラも入り、いっそう複雑さを増した最新のエコシステムの保護に必要な、きめ細かい可視性と網羅性を可能にします。

ランサムウェアの潜在的な被害を抑える

フィッシングメールのリンクのクリック操作、セキュリティの設定ミス、RDP ポートの開放、脆弱な認証情報は、攻撃者にとって侵入の糸口となります。攻撃者は、その糸口をたどって組織の大切な情報がないかネットワーク内を探し回り、ランサムウェア攻撃を仕掛けるための準備をします。大規模なデータ暗号化の被害を受けた場合、その企業は、さらにデータ窃取による二重脅迫を受ける可能性があります。それにより、さまざまなレベルの経済的損失が発生し、事業にダメージを受けることになります。

直接的な事業上の損失はすぐに表面化するでしょう。たとえば、オンライン注文や店舗業務が滞ったり、停止したり、あるいは顧客が商品を購入できなくなったり、ホテルや飛行機の予約ができなくなったりします。E コマースの業務でも、既存の注文の処理、履行、出荷ができなくなる可能性があります。重要なシステムやサーバーにアクセスできなくなったり、攻撃範囲の拡大を抑制するためにオフラインに切り替えたりするからです。

間接的な事業上の損失も発生するでしょう。機密性の高い企業データや顧客データが流出した場合は、公共的なイメージが失墜し、ブランドの評判を大きく落とすことになります。ランサムウェアギャングがよく使う手口は、「名指しで恥をさらす」サイトで攻撃の事実を公表し、その証拠として流出データをさらすという方法です。こうして、被害者への脅迫を強め、支払いの要求に応じるよう強く迫ります。また、最近の米国証券取引委員会（SEC）要件では、事業への重大な影響が生じた場合、4 日以内に SEC に通知することが義務付けられています。このような被害が発生すると、新聞のトップ記事になり、組織の評判を著しく落とすことになります。

復旧にかかる費用も高額になります。ランサムウェア被害からの復旧に直接的に関係する費用としては、法手続き上の費用、インシデント対応、データの科学的分析、侵害からの回復があり、そのために、コンサルタントや IT チームがデータの復旧、バックアップの復元、システムのオンライン復旧に携わることになります。しかし、このような費用だけでなく、訴訟費用や、機微な情報の漏えいに課される規制上の罰則や罰金が発生することもあります。サイバー保険料が劇的に高くなったり、ランサムウェア被害に基づく請求の支払いが拒否されたり、あるいは完全に補償の対象から除外される可能性があります。

リスクは至るところにあります。したがって、ランサムウェア攻撃が 2024 年に小売業界とホテル業界の CISO が抱く懸念事項の第 1 位に挙げられ、セキュリティリーダーたちが攻撃者によって踏み台が築かれた後のリスク軽減に役立つ制御手段に投資する準備を整えていることは、驚くべきことではありません。しかし、ランサムウェアを拡散させるためには、攻撃者は初期アクセス権限を得た後に、攻撃の方向を変え、横方向に移動し、影響範囲を最大限に広げられなくてはなりません。『Microsoft デジタル防衛レポート 2022』によると、ランサムウェアのインシデントの 93% は、ラテラルムーブメントに対する制御が不十分であるため、攻撃者に重要なアプリケーションやインフラの占有を許してしまうことが原因であり、攻撃者が企業ネットワークのエンドポイントから横方向への移動を開始するまでの時間の中央値はわずか 1 時間 42 分です。

Akamai が最近公開した『セグメンテーションの現状』（英語版のみ）のデータによると、E コマース企業は過去 12 か月間で、他の業界と比較して最も多くのランサムウェア攻撃を報告しました。そのため、CISO とセキュリティ担当者は、ランサムウェア拡散のリスクを減らし、アタックサーフェスを最小限に抑え、ランサムウェアのキルチェーンを「断ち切る」ために、マイクロセグメンテーションのようなゼロトラストベースのセキュリティツールに注目しています。

ラテラルムーブメントによる探索行為を検知し、ブロックすれば、攻撃者が特権への昇格、機微な情報の検索、大規模なランサムウェア攻撃の伝播に必要な IT 資産に簡単にアクセスすることはできなくなります。Akamai のアナリストの高い評価（英語版のみ）を受けているマイクロセグメンテーションソリューションは、コマースのインフラ全体を通して重要なワークロードには最小限の権限のみを付与するという原則を適用しており、アプリケーションやワークロードの横方向のデータフローを深いレベルまで可視化できます。また、ラテラルムーブメントを制限し、攻撃者の攻撃が機能しないようにソフトウェア定義ポリシーできめ細かく保護できます。

大手のサイバー保険会社も、マイクロセグメンテーションの価値を認識しています。ランサムウェアが保険の加入件数の増加と、請求額の高騰に拍車をかけているため、多くの保険会社は、セキュリティ制御の要件と検査の厳格化、保険料の値上げ（前年比で 96% の値上げになるケースもあり）、重大な損失を考慮した身代金支払い補償限度額の引き下げに走らざるを得ない状況になっています。中には、法外な料金を設定されてサイバー保険市場から追い出された企業や、一切の補償を拒否された企業も出ています。サイバー保険だけでは、有害な侵入による被害やその結果生じた経済的損失を補うことはできませんが、マイクロセグメンテーションのようなセキュリティ制御を導入すれば、ここ最近の保険引受の要件を満たしやすくなります。

「マシンにエージェントを 1 つ組み込むだけで、ラテラルムーブメント（横方向の動き）によるエンドポイント攻撃の問題を完全に解決できました」

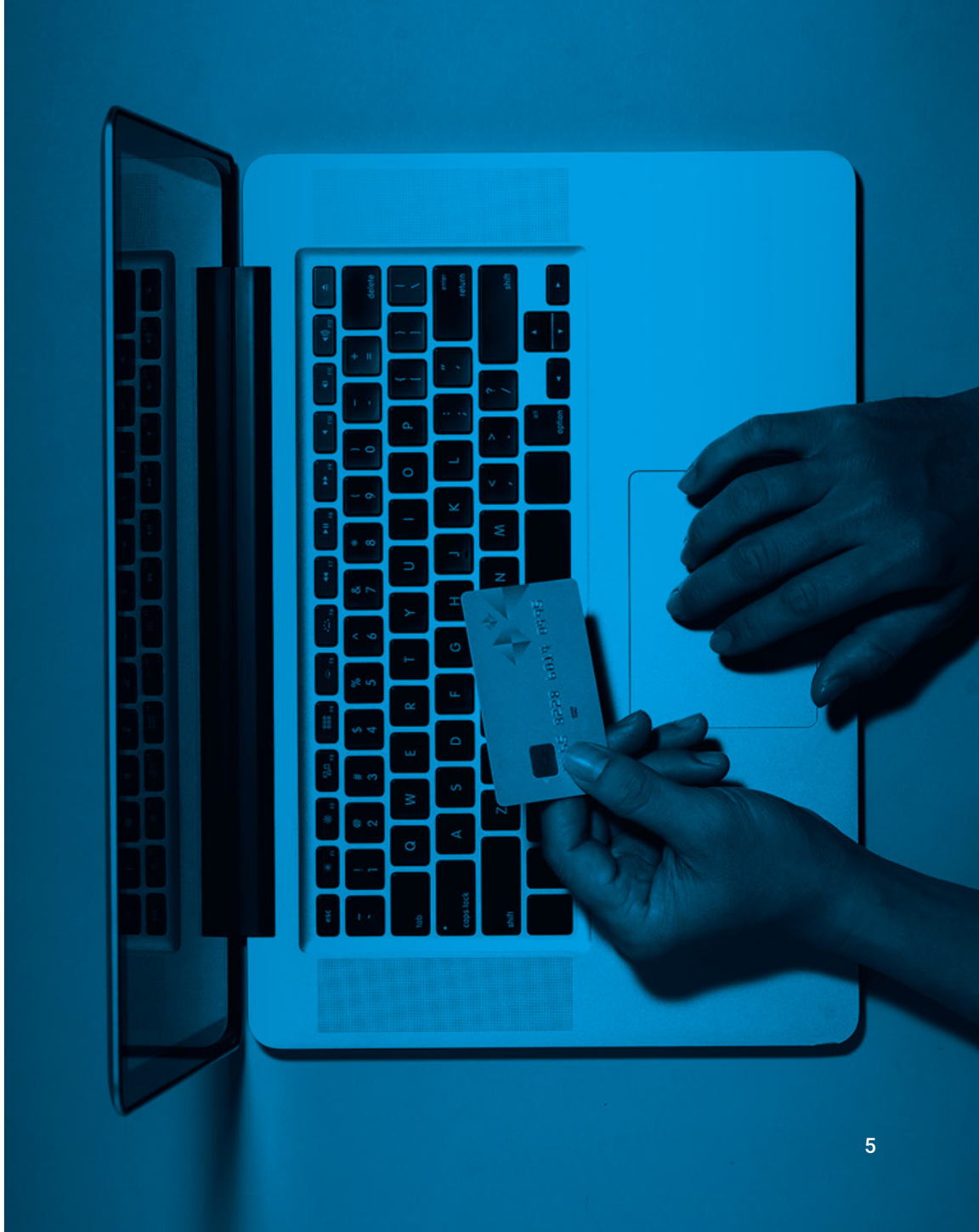
Global Retail & Consumer Goods Manufacturer
Infrastructure Architect

PCI コンプライアンス監査の範囲の縮小

E コマース企業にとっては周知の事実ですが、PCI コンプライアンスの要件達成と維持にかかるコストは、ガバナンス、リスク、コンプライアンスにかかわる年間予算のかなりの部分を占めており、セキュリティの FTE とリソースに大きな負担をかける傾向があります。PCI Data Security Standard（PCI DSS）は、カード所有者データ環境（CDE）を保護するためのセキュリティポリシーとセキュリティ制御を継続的に監査することを求めています。PCI のスコーピングとは、カード所有者データ（CHD）のセキュリティに相互的な関係を持つか、または影響を与える可能性がある人、プロセス、テクノロジーを特定することを指しますが、このスコーピングも、PCI 監査の実施に伴うコストを劇的に上昇させる可能性があります。

ネットワークセグメンテーションは、**PCI DSS の正式な要件ではありません**が、コマース企業は長年、vLAN や ACL、内部ファイアウォールなどの従来方式のネットワークセグメンテーションを使用して、コンプライアンス維持の範囲、コスト、リスク、困難さを軽減しています。しかし、ここ最近の小売エンタープライズの IT 環境は、ハイブリッド、マルチクラウド、マイクロサービスなど複数のアーキテクチャにまたがる、より動的なものになっているため、従来のセグメンテーションの技術や手法ではその流れに追いつけなくなり、運用上のオーバーヘッド、複雑さ、アプリケーションのダウンタイムが増えているだけでなく、セキュリティギャップも生まれています。

これは、従来型のセグメンテーション手法の管理と維持が煩雑になっていることが原因です。CDE の境界の内側にあるシステム、ネットワーク、アプリケーションを適切にセキュリティ確保、制御するためにリソースを消費しているのです。組織の運用の幅がデータセンターからクラウド、コンテナベースの資産へと広がったため、多くの組織はアプリケーションやシステムの通信フローを包括的に可視化できなくなり、PCI が求めているファイアウォール設定標準の維持が困難になっています。



その結果、セグメンテーションの徹底が疎かになり、セキュリティギャップを生み出し、PCI 監査が不合格になる状況を作り出しています。このような背景を受けて、コマース企業は**ソフトウェア定義のセグメンテーションに注目しています**。それは、インフラ全体を通して、CDE と対象外のシステムの分離が容易になり、PCI 監査の範囲を減らし、コンプライアンス準拠を速めることができるからです。従来のツールで対応可能なレベルを超え、セグメンテーションとルール適用の範囲がレイヤー 7 プロセスレベルまで対応可能になります。Akamai のエージェントは負荷が軽く、ファイアウォール、ネットワークの変更、サーバーの再起動が不要で、基盤のインフラとは独立して稼動するため、アプリケーションのダウンタイムがなく、変更の制御やメンテナンスのための時間枠を設ける必要もありません。

ソフトウェア定義のセグメンテーションは、基盤となるインフラやオペレーティングシステムからセキュリティを切り離すため、セグメンテーションをネットワークやアプリケーションと切り離し、単独で実行できます。コマース企業は、このアプローチを採ることで、ソリューションが分散型ステートフルインスペクションファイアウォールとして機能し、全体をカバーできるようになり、環境全体を通してネットワークと資産をきめ細かく可視化できます。しかも、導入と管理に要する労力とリソースが減るだけでなく、**SecOps の生産性が約 95% 向上**するため、組織はセキュリティ対策を強化するとともに、PCI コンプライアンスが招く「頭痛の種」の多くを解消することができます。他にもメリットがあります。Akamai のソリューションでは、監査時のコンプライアンス検証に、ネットワークのリアルタイムの状況と過去の状況の視覚的なデータを活用できます。

「ソフトウェア定義のセグメンテーションにより、プロセスレベルでセグメンテーションポリシーを作成して適用できるようになり、セキュリティ体制と PCI-DSS 技術要件を満たすための能力の両方が大幅に強化されました」

The Honey Baked Ham Company
Sr. Infrastructure Engineer

IoT と従来のインフラ全体の可視性と網羅性を確保

コマース企業は、ランサムウェアの拡散防止から PCI コンプライアンスのセキュリティ制御の管理に至るまでのセキュリティを、実店舗、生産施設、物流倉庫などの物理的な拠点でも確保しなければならないため、複雑さがさらに増します。航空業界では、IoT のセンサーとデバイスで航空機システムをリアルタイムで監視できれば、性能と安全性を向上させるための予防的な保全対策を講じることができます。また、ホテル業界では、IoT 駆動のデバイスを展開すれば、客室をスマート化し、顧客体験と運用効率を向上させることができます。

このような拠点や環境の多くには、ホストベースのセキュリティエージェントを実行できない、モノのインターネット（IoT）やオペレーショナルテクノロジー（OT）の資産が無数に存在するため、ハードウェアやソフトウェアの脆弱性が高くなる傾向があります。Forrester の 2023 年版『The State of IoT Security』の調査によると、世界中の経験豊富なセキュリティ責任者の 33% が、**外部からのサイバー攻撃を受けるデバイスのトップとして IoT デバイス**を挙げています。そのため、組織は、IoT 環境や OT 環境を保護できるエージェントレス機能を備えたセグメンテーションソリューションを導入し、攻撃者がデバイスの脆弱性を悪用して幅広い IT インフラへのアクセス権限を手に入れるリスクを、最小限に抑える必要があります。

このタイプのソリューションは、新しいコネクテッドデバイスがないか継続的に監視し、ネットワーク通信を許可されていないデバイスを自動的にブロックします。Akamai のソリューションは、デバイスのフィンガープリンティング機能を備えており、コネクテッドデバイスを自動的に検出し、スケーラブルで抽象的なセキュリティポリシーの基礎となる論理的なグループに分類します。IoT デバイスと OT デバイス用のセグメンテーションポリシーは、統一インターフェースで作成することができます。また、このポリシーは、他のポリシーと同様に、フィンガープリント対象のデバイスがどこにあろうと（デバイスが新しいネットワークロケーションに移動したとしても）、環境内に何台存在するかに関係なく、そのデバイスを追跡します。

ゼロトラストベースのポリシーは、ネットワークスイッチの ACL で適用されるため、エージェントの必要がなく、IoT の導入環境と OT の導入環境との間でポリシーの適用にギャップが生まれることも、リスクを生む可能性もありません。このようなセキュリティ上の境界を設けることで、IT 管理システム、アップデート専用サーバー、ロギングサーバーとの間で必要な接続がそのまま継続され、セキュリティ上のフリクションの発生を抑えることができます。当社のソリューションは、エンタープライズ資産を一元的に把握できるように、IT インフラだけでなく IoT システムと OT システムをすべて検出、可視化、マッピングします。

小売企業の多くは、IoT ／ OT 資産やその他のエアギャップエンドポイントのセキュリティ確保に加えて、古すぎる、あるいはサポート切れのためにパッチを適用できないオペレーティングシステムやインフラで稼動するシステム、サーバー、アプリケーションに依存しており、そのことが深刻なリスクを生み出しています。このような古いサーバーの多くは廃止できません。未だに組織の収益向上に貢献していたり、企業のバックボーンとしての役割を負っていたりするからです。この傾向は特に「クラウド生まれ」ではない E コマースエンタープライズに顕著です。広範囲に及ぶ業界最先端の網羅性と互換性を備えた Akamai のエージェントは、オペレーティングシステムの新旧に関係なく機能し、Windows と Linux のいずれについても、個々のプロセスやサービスレベルまで、ネットワークフローを完全に可視化します。また、MacOS のエンドポイントにも対応しています。

他のソリューションは、古いオペレーティングシステムを部分的にしか可視化できず、Windows Server 2008 R2 より前の Microsoft Windows システムにいたっては、まったく可視化できません。これは、従来のマイクロセグメンテーションソリューションのエージェントが、2002 年以降のシステムでのみ使用できる Windows ファイアウォールにポリシー適用を任せているためです。Linux システム対応のエージェントは、Linux 環境用のレイヤー 7 プロセスレベルのルールを持たず、ポリシーを適用する際に iptables に依存するため、レイヤー 4 までしか可視化できません。Akamai Guardicore Segmentation の機能は、新旧を問わず Windows と Linux のほぼすべてのオペレーティングシステムでサポートされ、基盤となるインフラから完全に切り離された状態で稼動します。

シンプルで手早く直感的、そして高い安全性

本社から小売店に至るまで、そしてデータセンターからクラウドに至るまで、さらにそれ以外の領域にゼロトラストを導入し、重要な IT 資産を安全に保護するのであれば、マイクロセグメンテーションが不可欠です。

Akamai Guardicore Segmentation はシンプルな作りになっているため、時間がかかる従来のネットワークセグメンテーション手法と比べて、導入と適用、監視、インシデント対応にかかる時間と労力が劇的に減ります。ポリシーの変更もすぐに実施でき、複雑なネットワーク変更を必要としません。このことは、セールスのピーク時やプロモーション、製品ローンチ、その他の注目イベントの開催に必ず必要になります。

結論：顧客や来賓、乗客に品質と安全性のどちらを選びますかと聞くこと自体があり得ないのと同様に、マイクロセグメンテーションを利用する場合も、セキュリティとアジリティのどちらかを選ぶことにはなりません。苦労してセグメント化する時代は終わっているのです。

もっと詳しい情報をご希望ですか？

Akamai ゼロトラスト・ポートフォリオの Akamai Guardicore Segmentation でアタックサーフェスを減らし、重要なアプリケーションのセキュリティを確保し、コンプライアンスを合理化する方法をご紹介しています。

詳細はこちら

TechnologyAdvice | Akamai