AKAMAI お客様事例

セキュリティ侵害復旧サービス会社、ランサムウェアへの対応とそこからの回復に Akamai を活用

包括的なネットワーク可視性

IT インフラ全体のセグメンテーション

ランサムウェアの脅威への対応

お客様

米国に拠点を置くセキュリティ侵害復旧サービス会社が、重大なセキュリティインシデントが発生した後、ある世界的な機器メーカーと契約を結びました。

課題

高速拡散型ランサムウェア

あるグローバル機器メーカーで、ビジネスの運営に影響を与えるマルウェア攻撃が拡散されました。その後、同社の環境内のセキュリティを復元し、改善するために、このセキュリティ侵害復旧サービス会社との連携が開始されました。従業員のノート PC から開始された攻撃は、同社のバックアップサーバーに侵入するだけでなく、ほとんどの拠点に瞬く間に拡散し、影響を与えたのです。

ソリューションの選択

ファイアウォール全体にインターネットアクセス制限ルールを適用するなどの最初の封じ込め方法ではスピードが追いつかず、すばやく拡散される侵害を封じ込めることができませんでした。分散されたエンタープライズ環境の複雑さと実際のネットワークから判断すると、ファイアウォールを使用した制限ルールの実装と適用は、スピードが遅く非効果的なプロセスでした。

さらに、レガシーマシンの可視化は、侵害の調査と封じ込めを担当するインシデント対応者にとって大きな問題でした。このセキュリティ侵害復旧サービス会社は、横方向への拡散によってさらに多くの資産に影響が与えられる前にセグメンテーションを緊急に進めていく必要があると判断し、Akamai Guardicore Segmentation を推奨しました。

Breach Remediation Company

業種
情報テクノロジー

ソリューション
Akamai Guardicore Segmentation

主な効果

- ラテラルムーブメントによるランサムウェアの拡散を緩和する
- ネットワークフローのきめ細かな可視性を提供する
- 最新マシンとレガシーマシン、両方のセキュリティを確保する
- 迅速なインシデント対応を可能にする

Akamai

Akamai Guardicore Segmentation のメリット

瞬時に可視化

セキュリティ侵害復旧サービス会社は、3 時間以内に 3,000 台以上の企業サーバーに Akamai エージェントを迅速にプロビジョニングしました。導入後わずか数分で、ネットワークと通信フローの詳細な可視化が開始され、インシデント対応チームは、侵害を調査して封じ込めを検証するために必要なコンテキストと正確なデータを取得できました。

迅速にポリシーを適用

必要な可視化を実現するとすぐに、インシデント対応チームは広範な環境から重要な資産をセグメント化するための行動をとりました。製造ラインを機能させることに特化した 2 つの重要な生産アプリケーションを迅速に特定し、保護しました。Akamai Guardicore Segmentation を使用して、感染したサブネットやデータセンターの一部からアプリケーションへの接続を制限するポリシーをすぐに導入しました。これは、レガシーファイアウォールでは数週間かかるタスクです。

また、単純なクエリーを実行することにより、インターネットに接続されたレガシーマシンがレガシーファイアウォールをバイパスし、封じ込め制限を試みたことも明らかになりました。インシデント対応チームは、非準拠の通信を検出した後、数分以内に、レガシーマシンを含むすべてのサーバーのインターネットアクセスを効果的に制限するポリシーを作成しました。

回復時のラテラルムーブメント（横方向の移動）を防止

回復プロセスにおける次の段階では、メーカーのアプリケーションクラスターを再作成し、Akamai エージェントを組み込みました。すべての着信接続をブロックする初期ポリシーを設定し、Akamai Guardicore Segmentation を使用して依存関係を特定しました。その後、要件を検証してコンテキストを把握した後、接続が必要な通信についてのみ許可リストに登録しました。この手法により、再感染のリスクを負うことなく、ランサムウェア攻撃の影響を受けたアプリケーションを回復させ、オンライン状態に戻すことができました。

将来の保護

セキュリティ侵害復旧サービス会社は、ランサムウェア攻撃からの回復をサポートしながら、顧客であるメーカーに対して大きな付加価値を提供しました。それを可能にしたのが Akamai Guardicore Segmentation です。これにより、セキュリティ侵害復旧サービス会社は収益を増加させ、事業を拡大するとともに、顧客が IT とセキュリティの目標を達成できるようサポートする機会を開拓することができました。

段階的な回復プロセス中に導入した、顧客社内のデータセンターのセグメンテーションにより、アタックサーフェスが大幅に削減されました。現在、その顧客企業のセキュリティ体制は強化され、今後の侵害から受ける影響は大幅に減少しています。

その他の詳細については、akamai.com/guardicore をご覧ください。

> Akamai のおかげで、攻撃の拡散を阻止し、基盤となるネットワークを変更することなく、ダウンした生産ラインを「無菌」のネットワークセグメントに復元するまでに 4 時間かかりませんでした。IR 調査と封じ込めもすべて同時進行でした。
>
> セキュリティ侵害復旧サービス会社、CISO