AKAMAI お客様事例

ランサムウェア攻撃を受けた大規模金融サービス企業が、Akamai でリモートアクセスをセキュリティ保護

包括的なネットワーク可視性

迅速なポリシー適用

テレワーカーのセキュリティ確保

お客様

ブラジルを拠点とする大手金融サービス会社。

課題

リモートアクセスの増加

COVID-19（新型コロナウイルス感染症）の世界的な流行により、この金融サービスプロバイダーでは多くの組織と同様にリモートアクセスのニーズが高まり、同行の IT スタッフの多くが社給デバイスを使用して在宅勤務を行うようになりました。ユーザーは主に、企業ネットワークの外部から、仕事に必要なデータやアプリケーションにアクセスするようになったため、組織のアタックサーフェスが急速に拡大しました。

防げなかったランサムウェアのインシデント

在宅勤務モデルに移行した直後に、同行の重要な Oracle Cloud データベースを標的としたランサムウェア攻撃が仕掛けられ、被害が発生しました。後に、VDI 環境を利用して攻撃が行われたことが判明しました。セキュリティと IT 部門は、機密性の高い財務データの損失を抑えるために迅速な措置を講じる必要があることを認識していました。さらに、最初に経路となった攻撃ベクトルを特定して適切な対策を講じることができなければ、ランサムウェアがバックアップサーバーや組織の本番環境へと横方向に拡散するという現実的なリスクがあることを理解していました。このリスクが現実化すれば、重大なデータ損失と金銭的損失を被ることは間違いありません。

ソリューションの選択

Akamai Guardicore Segmentation は、すでに同行の他の分野で広く使用されていました。ランサムウェア攻撃を受ける以前、このプラットフォームは、オンプレミス、仮想、ベアメタル、VDI インフラ、Azure および OpenShift コンテナなどの環境にわたるワークロードを擁する 23,000 台以上のサーバーのセグメンテーションポリシーの管理と適用に使用されていました。

Large Financial Services Company

業種
金融サービス

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
- VDI 環境をセグメント化することで、リモートアクセスを保護する
- 迅速なインシデント対応を可能にする

Akamai

同行では、ソフトウェアベースのセグメンテーションソリューションであるこのプラットフォームを、セキュリティとコンプライアンスに関するいくつかの取り組みを実現するために使用してきました。たとえば、管理者によるジャンプ・ボックス・アクセスや Swift アプリケーションのセグメンテーションの管理などです。このプラットフォームが優れた可視性を提供し、ポリシーを迅速に適用することを熟知していた対応チームは、Akamai Guardicore Segmentation の機能を利用してセキュリティ侵害に対応するという決断を速やかに下しました。

Akamai Guardicore Segmentation のメリット

プロセスレベルの可視性

このプラットフォームを使用して、同行の対応チームは過去の通信フローを調査しました。その結果、ランサムウェアが最初に侵入したのは Oracle Cloud データベースと通信するデータベース管理者のリモート VDI 接続であったことを突き止めました。

迅速なポリシー適用

攻撃ベクトルを特定した後、チームは VDI のセグメンテーションを最優先として取り組みました。ポリシー計画プロセスは土曜日に開始され、Akamai Guardicore Segmentation の可視化機能を使用して、潜在的なポリシーニーズを吟味しました。次の火曜日には、Oracle Cloud への 3,000 を超える VDI 接続に適用できるポリシーが完成していました。

ランサムウェアからの復旧

対応チームは、Akamai のエージェントをバックアップアプリケーションに展開し、アプリケーションのリングフェンシングを設定して、資産と通信できるものをプロセスのレベルに至るまで定義しました。その後、攻撃を受けた領域に展開し、グローバルな拒否ルールを使用してランサムウェアのさらなる増殖をブロックしました。

また、テレワーカーのアクセスによってさらなるリスクが生じるのを防ぐため、コールセンターの従業員が使用している 2 種類の VDI ソリューションについてもポリシーを設定し、行内のエンドポイント間での不正なラテラルムーブメントを阻止しました。

この金融サービス組織では、わずか 3 日間でセグメンテーションポリシーを適用することができたため、ランサムウェアのインシデントによる影響を大幅に低減するとともに、今後のリモートアクセスのセキュリティを大幅に強化することができました。

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

> [Akamai Guardicore Segmentation] が提供する可視性は、暗闇を照らし出す明るい光線のようなものでした。
>
> 大手金融サービス会社のインフラセキュリティ責任者