多層防御とは何か

100 XP

6 分

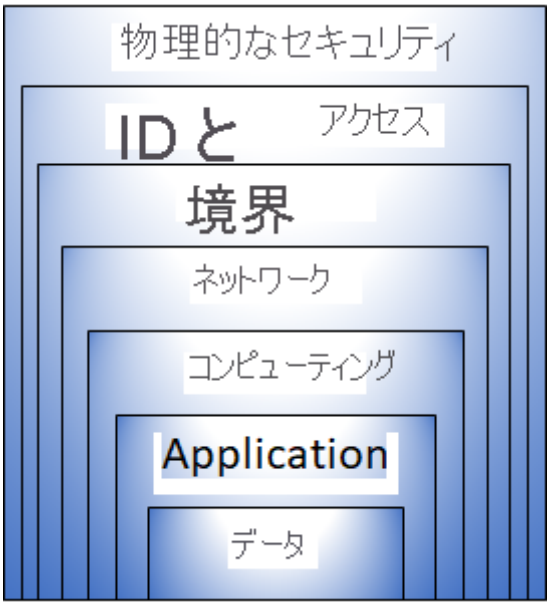
現在 Tailwind Traders 社は、ワークロードをオンプレミスの自社のデータセンターで実行しています。 オンプレミスでの実行とは、建物への物理的なアクセスからネットワークでのデータの送受信方法に至るまで、セキュリティのすべての側面を自社で担当することを意味します。 同社は、クラウドでの実行に対する多層防御戦略を検討したいと考えています。

"多層防御" の目的は、情報を保護し、アクセスを許可されていない人々によって情報が盗まれないようにすることです。

多層防御戦略では、データへの不正なアクセスを目的とする攻撃の進行を遅らせるために、一連のメカニズムが使用されます。

多層防御の層

多層防御は、保護対象のデータを中心とする一連の層として視覚化できます。



各層で保護が提供されるため、1 つの層が破られた場合、後続の層は既に備えができており、さらなる露出を防ぐことができます。 この方法によって、単一の保護層への依存が排除されます。 攻撃の速度が低下し、セキュリティ チームが自動的にまたは手動で対応できるアラート テレメトリが提供されます。

各層の役割の概要は次のようになります。

- "物理的なセキュリティ" 層は、データセンター内のコンピューティング ハードウェアを保護するための防御の最前線です。
- "*ID* とアクセス" 層では、インフラストラクチャと変更制御へのアクセスが管理されます。
- "境界" 層では、分散型サービス拒否 (DDoS) 保護を使用して、ユーザーに対するサービス拒否が発生する前に大規模な攻撃がフィルター処理されます。

- "ネットワーク" 層では、セグメント化とアクセスの制御を通してリソース間の通信が制限されます。
- "コンピューティング" 層では、仮想マシンへのアクセスがセキュリティで保護されます。
- "アプリケーション" 層では、アプリケーションがセキュリティで保護され、セキュリティ上の脆弱性がないことを確認できます。
- "データ" 層では、保護する必要があるビジネスと顧客のデータへのアクセスが制御されます。

これらの層には、アプリケーションのすべての層でのセキュリティ構成を決定するために役立つガイドラインがあります。

Azure では、多層防御という概念のすべてのレベルにセキュリティ ツールと機能を提供しています。 各層を詳しく見ていきましょう。

物理的なセキュリティ

建物へのアクセスを物理的にセキュリティで保護し、データセンター内のコンピューティング ハードウェアへのアクセスを制御することが、防御の最前線となります。

物理的なセキュリティの目的は、資産へのアクセスに対する物理的な保護措置を講じることです。 これらの保護措置により、確実に他の層をバイパスできなくなり、損失や盗難が適切に処理されます。 Microsoft では、クラウド データセンターでさまざまな物理的なセキュリティ メカニズムを使用しています。

ID とアクセス

この層では、次のことを行うことが重要です。

- インフラストラクチャへのアクセスを制御し、変更を制御します。
- シングル サインオン (SSO) と多要素認証を使用します。
- イベントと変更を監査します。

ID およびアクセス層では、ID がセキュリティで保護されていること、必要なもののみにアクセスできる権利が付与されていること、およびサインイン イベントと変更がログに記録されていることのすべてが確実に実行されます。

境界

この層では、次のことを行うことが重要です。

- DDoS 保護を使用して、ユーザーのシステムに対する可用性に影響が出る前に大規模な攻撃をフィルター処理します。
- 境界ファイアウォールを使用して、ネットワークに対する悪意のある攻撃を識別し、警告します。

ネットワーク境界で、リソースに対するネットワークベースの攻撃から保護する目的があります。 これらの攻撃を識別し、影響を排除し、これらの発生時に警告することは、ネットワークを安全に保つために重要なことです。

Network

この層では、次のことを行うことが重要です。

- リソース間の通信を制限します。
- 既定で拒否します。
- 必要に応じて、インターネットの受信アクセスを限定し、送信アクセスを制限します。
- オンプレミス ネットワークへのセキュリティで保護された接続を実装します。

この層では、すべてのリソースに対するネットワーク接続を制限して、必要な接続のみを許可することに重点が置かれます。 この通信制限によって、ネットワーク内の他のシステムに攻撃が拡散されるリスクが軽減します。

Compute

この層では、次のことを行うことが重要です。

- 仮想マシンへのアクセスをセキュリティで保護します。
- デバイス上にエンドポイント保護を実装し、システムに修正プログラムを適用して最新の状態に保ちます。

マルウェア、パッチが適用されていないシステム、適切にセキュリティ保護されていないシステムのために、ご利用の環境が攻撃を受けやすくなってしまいます。 この層の焦点は、コンピューティング リソースが確実にセキュリティで保護されていること、およびセキュリティ上の問題を最小限に抑えるための管理が適切に実行されるようにすることです。

Application

この層では、次のことを行うことが重要です。

- アプリケーションを確実にセキュリティで保護された脆弱性のないものにします。
- 機密性の高いアプリケーション シークレットをセキュリティで保護されたストレージ メディアに格納します。
- セキュリティをすべてのアプリケーション開発の設計要件にします。

アプリケーション開発のライフサイクルにセキュリティを統合することは、コードに取り込まれる脆弱性の数を減らすのに役立ちます。 すべての開発チームは、アプリケーションが既定でセキュリティによって保護されるようにする必要があります。

データ

ほとんどすべての場合、攻撃者は次のようなデータを狙っています。

- データベースに格納されているもの。
- 仮想マシン内のディスク上に格納されているもの。
- Office 365 などの SaaS (サービスとしてのソフトウェア) アプリケーションに格納されているもの。
- クラウド ストレージを通して管理されているもの。

データを格納し、そのアクセスを制御するユーザーには、それが適切に保護されていることを確認する責任があります。 多くの場合、規制上の要件によってデータの機密性、整合性、

可用性を確保するために適用する必要がある制御とプロセスが示されます。

セキュリティ体制

"セキュリティ態勢" とは、セキュリティの脅威から保護し、セキュリティの脅威に対応する組織の能力です。 セキュリティ態勢を定義するために使用される一般的な原則は、"機密性"、"整合性"、"可用性" です (CIA と総称されます)。

- **機密性**

  "最小限の特権の原則" とは、情報へのアクセスを、各自の仕事をするために必要なレベルのアクセス権を明示的に付与されたユーザーのみに制限することを意味します。 この情報には、ユーザーのパスワード、電子メールのコンテンツ、およびアプリケーションと基になるインフラストラクチャへのアクセス レベルの保護が含まれます。

- **整合性**

  情報に対する不正な変更を禁止します。
  - 保存時: 格納されているとき。
  - 転送中: ローカル コンピューターからクラウドへなど、ある場所から別の場所に転送されているとき。

データ転送で使用される一般的な方法は、一方向のハッシュ アルゴリズムを使用してデータの一意のフィンガープリントを作成する送信者のためのものです。 ハッシュはデータと共に受信者に送信されます。 データのハッシュは受信者によって再計算され、元のものと比較され、データが転送中に失われたり、変更されたりしていないかが確認されます。

- **利用可能性**

  サービスが常に機能し、承認されたユーザーだけが確実にアクセスできるようにします。 "サービス拒否攻撃" は、システムの可用性を低下させてユーザーに影響を与えることを目的としています。