# ???????

translated with "MixerBox translate" using chatgpt4 as i suck at reading japanese still im not sure if its correct or not its just meant to help me speak and read it

セキュリティコントロールは、機密データをプライベートで安全に保つために不可欠です。最も一般的なコントロールの一つは、最小権限の原則とも呼ばれる PoLP または最小権限です。最小権限の原則は、ユーザーがタスクや機能を完了するために必要な最小限のアクセスと認証のみが付与されるセキュリティ概念です。

最小権限は、情報の機密性、完全性、可用性（ CIA ）の三位一体を支える基本的なセキュリティコントロールです。この読み物では、最小権限の原則がリスクをどのように減らし、一般的にどのように実装され、なぜ定期的に監査されるべきかを学びます。

アクセス制限によるリスクの軽減

すべてのビジネスは、データ盗難、悪用、乱用のリスクに対する計画が必要です。最小権限の原則を実装することで、データ侵害のような高額なインシデントのリスクを大幅に減らすことができます。

敏感な情報へのアクセスを制限する

データの誤変更、改ざん、または損失の可能性を減らす

システムの監視と管理を支援する

最小権限は、特定のリソースを特定のユーザーに接続し、彼らが何をできるかに制限を設けることで、成功する攻撃の可能性を大幅に減らします。これは、任意の資産に適用すべき重要なセキュリティコントロールです。ユーザーが誰であるか、または何であるかを明確に定義することは、通常、最小権限を効果的に実装する最初のステップです。

注: 最小権限は、別の基本的なセキュリティ原則、つまり職務分離と密接に関連しています。これは、重要なビジネス機能に対する完全なコントロールを単一のユーザーに与えることを防ぐセキュリティ概念です。アイデンティティとアクセス管理に関する別の読み物で、職務分離について詳しく学びます。

アクセスと認証の決定

最小権限を実装するためには、まずアクセスと認証を決定する必要があります。そのためには以下の二つの質問をする必要があります。

ユーザーは誰ですか?

彼らは特定のリソースにどれだけのアクセスが必要ですか?

ユーザーが誰であるかを決定することは通常、直截的です。ユーザーは、顧客、従業員、またはベンダーのような人を指すこともあります。また、ビジネスネットワークに接続されているデバイスやソフトウェアを指すこともあります。一般的に、すべてのユーザーは自分自身のアカウントを持つべきです。アカウントは通常、組織のディレクトリサービス内で保存および管理されます。

これらは最も一般的なユーザーアカウントのタイプです:

注：ほとんどのディレクトリサービスは、不審な活動のシステム管理者に警告するように設定することができます。

キーテイクアウェイ
最小権限の原則は、敏感な情報とリソースへの不正アクセスのリスクを減らすことができるセキュリティコントロールです。適切なレベルのアクセスと認証を持つユーザーアカウントを設定し、設定することは、最小権限を実装するための重要なステップです。ユーザーアカウントを監査し、不必要なアクセス権を取り消すことは、情報の機密性、完全性、および可用性を維持するための重要な実践です。

Revision #2
Created 2023-07-19 08:34:17 UTC by naruzkurai Updated 2023-08-15 18:44:10 UTC by naruzkurai