アイデンティティのセキュリティチェックリスト

アイデンティティへのサイバー攻撃から組織を守るための40の質問

過去1年間におけるセキュリティ侵害は、アイデンティティがサイバー犯罪者や国家的脅威アクターにとって、重要な攻撃ベクトルであることを明確に示しています。アイデンティティは単なるログインボックスではなく、企業の最も機密性の高いデータや、インフラストラクチャに対する最初で最後の防御線です。

このことはデータが裏付けています。クレデンシャルを再利用する問題が蔓延しており、Web アプリケーションの侵害の 86% は漏洩したクレデンシャルに起因しています[1]。当社の「The State of Secure Identity Report 2023」によると、Customer Identity Cloud の顧客アプリケーションの半数以上が、漏洩したクレデンシャルを使用した攻撃を少なくとも 1 回経験しています[2]。さらに、ソーシャルエンジニアリングを実行するコストが低下し続けているため、MFAをバイパスすることが攻撃者の焦点であり続けています。当社のプラットフォームでは、MFA試行の12.7%がMFAバイパス試行で占められていました[2]。

これらのデータから明らかなのは、アイデンティティはセキュリティであるということです。

Oktaはアイデンティティ攻撃との戦いにおいて、お客様と業界を支援する最前線にいます。全世界で100億回以上のログインをサポートし、18,000社以上のお客様を、月間20億回以上の悪質な要求から保護しています。業界のリーダーとして、当社はこのチェックリストのようなベストプラクティスを共有することで、お客様が可能な限り強力なアイデンティティセキュリティ態勢を導入できるようにご支援してまいります。なお、これは一般的なアドバイスであることをご留意ください。

[1] ベライゾン： 2023年データ漏洩/侵害調査報告書
[2] Okta : The State of Secure Identity Report 2023

統合アイデンティティセキュリティとゼロトラスト

基礎編

1. 御社のアイデンティティセキュリティソリューションは、アイデンティティとアクセス管理、インシデント対応、リスク管理、継続的改善への取り組みを含む、総合的なサイバーセキュリティ戦略に寄与していますか？
2. 御社ではアクセス要求のコンテキストにおいて、ユーザー、デバイス、アプリケーションを動的に認証・認可する手段を導入していますか？
3. 管理者ロールを定期的に見直し、更新するためのプロセスを確立していますか？
4. 攻撃対象となる可能性のある領域を最小限にするために、アイデンティティセキュリティソリューションに最小特権アクセスを実装していますか？特に、可能な限り管理者権限を削除していますか？

上級編

1. ユーザーやデバイスの行動を継続的に監視・評価し、異常な行動や不審な行動を検出する強固な戦略がありますか？
2. ITサポートスタッフが、高度な特権を持つユーザーに対して操作を実行できないように、ITサポートスタッフの権限を制限していますか？例えば、これらのユーザーにカスタム管理者ロールを作成し、割り当てていますか？
3. 最も重要なリソース内で、ユーザーのやりとりを通じ、継続的にユーザーのアイデンティティを確認するための手段を講じていますか？
4. サブプロセッサー（業務を委託する第三者）にゼロトラストのセキュリティを要求していますか？特に、サードパーティがネットワーク境界を維持する能力を暗黙のうちに信頼するのではなく、サードパーティの態勢を検証し、監査していますか？

アイデンティティとアクセス管理

基礎編

1. すべてのアカウントに多要素認証（MFA）を導入し、特権アカウントにはフィッシング耐性のあるMFAを導入していますか？
2. 保護されたアクションにステップアップ認証が必要ですか？
3. フィッシング耐性を、従業員の登録/入社から回復に至るまで、従業員のライフサイクル全体にわたっていますか？
4. アカウントのMFA要素がすべてリセットされたとき、ユーザーに自動的にアラートを発しますか？
5. アイデンティティガバナンス戦略を策定し、業界標準やベストプラクティスとどのように整合させていますか？
6. オンボーディング、オフボーディング、アクセスレビューなど、アイデンティティのライフサイクル管理を自動化し、正確性と効率性を確保していますか？
7. 組織では、どのような基準でアイデンティティアカウントを休眠アカウントとして定義していますか？休眠アカウントのレビューはどのくらいの頻度で行っていますか？
8. すべてのサービスアカウントのパスワードを積極的にローテーションしていますか？

上級編

1. 御社のアイデンティティガバナンスソリューションは、セキュリティの脆弱性につながる可能性のあるコンフリクトを防ぐために、職務の分離を強制していますか？
2. ユーザーのアクセス権を定期的に証明・認証する仕組みがありますか？
3. 特権アカウントは、 堅牢なフィッシング耐性のある多要素認証で強化され、高度なセキュリティレベルが確保されていますか？
4. 包括的な特権アクセス管理（PAM）ソリューションを導入し、重要なシステムやデータへのアクセスを正確に制御し、継続的に監視を行っていますか？
5. カスタマーサポートの提供で利用するアプリケーションだけでなく、すべての業務で使うアプリケーションについて、サポート契約者がIAMソリューション経由で認証することを要求していますか？
6. 重要なリソースへのユーザー認証にIPバインディングを適用していますか？APIまたはWebリクエスト中に観察されたIPアドレスが、セッション確立時に記録されたIPアドレスと異なる場合、管理者は管理セッションを自動的に取り消すことができますか？

修復と軽減の戦略

基礎編

1. 御社では特権アカウントの監視を強化するために、どのような既存の方法やツールを使っていますか？
2. 検知と対応能力を高めるために、どのようにユーザー行動分析を全体的なアイデンティティセキュリティ戦略に統合していますか？
3. オンプレミスのADエージェントに変更が加えられたときに、自動的にアラートが出ますか？
4. 自動化ツールや、TerraformのようなInfrastructure as CodeツールでAPIコールを行う際に、APIトークンを使用していますか？
5. 不明なデバイスからの不審なサインイン試行をブロックすることで、正当なユーザーのアカウントロックアウトを防ぎ、不明なデバイスがロックアウトの原因となっても正当なユーザーがロックアウトされないようにしていますか？
6. 企業デバイスと個人デバイス（ノートPCとモバイルの両方）を使うリモートユーザーに対して、リソースへのセキュアでシームレスなアクセスを保証する仕組みがありますか？

上級編

1. 攻撃者やマルウェアがSSWSトークンを盗んだり、不正アクセスのために指定されたIP範囲外で再生したりするのを制限するために、APIに対して許可されたネットワークゾーンのリストを強制していますか？
2. 管理者は、IPアドレスがアノニマイザーのアドレスに関連付けられているかどうかの評価に基づいて、アノニマイザーからのリクエストを検出してブロックできますか？
3. 所有証明を使用して機器間（M2M）統合のトークンバインディングを強制して、認証されたアプリケーションのみがトークンを使用してAPIにアクセスできるようにしていますか？
4. サードパーティのスコアやエッジベースのコンポーネントシグナルを使用して、ボット検知と保護を強化していますか？
5. セッション管理制御を拡張し、トークンのセキュリティを強化していますか？特に、セッションの完全なプログラム制御を顧客に提供し、独自のセッション制御ダッシュボードを構築して、ユーザー体験をカスタマイズできるようにしていますか？

従業員トレーニングと意識向上

基礎編

1. 最新のセキュリティ脅威やベストプラクティスについて従業員を教育するために、定期的にフィッシングに関する意識向上トレーニングや一般的なサイバーセキュリティトレーニングを実施していますか？
2. 従業員は、強力なパスワードポリシーとパスワードレス認証オプションの導入と利点について、情報を与えられ、教育されていますか？
3. フィッシングの模擬演習を実施し、従業員のフィッシング攻撃に対する耐性をテストし、そのような攻撃の被害に遭う可能性のある従業員に的を絞ったトレーニングを提供していますか？

上級編

1. 従業員がセキュリティ上の懸念を報告したり、セキュリティ関連事項について説明を求めたりできる仕組みがありますか？
2. 従業員は、パスワード回復フローの一部として個人メールアカウントを持つことの脅威について知らされていますか？攻撃者は、個人メールアカウントを認証の最も弱いリンクと見なしていることを知っていますか？