マイクロソフトにおける Azure Multi-Factor Authentication を使用したセキュリティの強化

ユーザー名とパスワードの収集が目的のフィッシング電子メールや偽の Web サイトなど、増大するセキュリティ リスクに対処するため、Microsoft IT では、マイクロソフトのすべてのユーザーに対する Azure Multi-Factor Authentication の導入を推進しました。既にリモート アクセスおよび仮想プライベート ネットワーク (VPN) に対して、仮想および物理スマート カードの形式で多要素認証が取り入れられています。しかし、セキュリティを強化し、モバイル生産性に対するサポートを向上させるためには、次のものを提供するオプションが必要でした。

- オンプレミスのリソースおよびクラウドベースのサービスへのアクセスに使用されるフェデレーション ID に対するさらなるセキュリティ強化。
- およそ 19 万人のユーザー、およびスマート カードを使用するようにはセットアップされていない 30 万台を超えるモバイル デバイスに対する多要素認証機能、またはユーザーがスマート カードを所持していない場合のモバイル デバイスに対する多要素認証機能。

オンプレミスの ID の統合

クラウドおよびオンプレミスのリソースにアクセスする際に、認証用の単一のユーザー ID および統一されたエクスペリエンスを実現するため、オンプレミスの Active Directory フォレストを Azure Active Directory (Azure AD) に統合しました。マイクロソフトの地理的に分散された Active Directory 環境には、Windows Server 2016 と Windows Server 2012 R2 の両方が含まれています。マイクロソフトでは、Azure AD Connect および Active Directory フェデレーション サービス (AD FS) を使用します。したがって、Azure ベースのアプリケーションがユーザーの属性 (ユーザーの所在、組織、役職など) を必要とする場合、サービスがそれらの属性に対するクエリを実行するための適切なアクセス許可を持っている限り、その情報を入手できます。

Azure Multi-Factor Authentication のセットアップ

ユーザー ID のセキュリティ保護をさらに強化するため、ユーザーに送信される追加の確認方法として Azure Multi-Factor Authentication を有効化しました。確認オプションには電話やモバイル アプリ通知などがあり、ユーザーは登録時に好みのオプションを選択できます。ユーザー エクスペリエンスは、接続の種類に基づいています。そのため、ユーザーがリモートで接続している場合、2 番目の本人確認方法を求めるメッセージが表示されます。重要なサービスの場合、たとえ企業ネットワーク内での接続であっても、アクセスには多要素認証が要求されます。

ユーザーの登録

サインイン エクスペリエンスのため、携帯電話を使用してのサインインおよびモバイル アプリ通知を使用してのサインインが有効になっています。マイクロソフトの企業ポリシーでは、登録の際ユーザー ID を検証することが求められます。登録プロセスでは、ユーザーが登録時にスマート カードを使用してサインインした場合、電話番号を自動的に検証できるように設計されたポータルが使用されました。スマート カードを持たないユーザーの ID は、マネージャーの承認を要求するワークフローを使用して検証されます。

ユーザー フレンドリなサインイン画面のカスタマイズ

マイクロソフトでは、段階的に Azure Multi-Factor Authentication を有効化し、エクスペリエンスについて、Yammer コミュニティのアーリー アダプターからのフィードバックおよびユーザー サポートからのフィードバック

を収集しました。残りのユーザーに展開する前に、フィードバックに基づいて、AD FS サインイン ページをカスタマイズして、直感的かつガイドなしで使用できるユーザー エクスペリエンスを実現することを選択しました。初期のフィードバックにより、どのサインイン オプションを選択すべきか、どの認証用証明書を選択すべきかなどについて、ユーザーをわかりやすい形で誘導する必要がある場面でのエクスペリエンスを向上させることができました。

サインイン画面を結合し、更新することにより、望ましいユーザー行動を促進できました。ユーザー向けの既定のオプションは、スマート カードを使用してサインインすることですが、ユーザー名とパスワードが選択された場合は、Azure Multi-Factor Authentication を使用して強力な認証を実行しました。インターフェイスも更新され、有効な認証オプションのみが検出および表示されるようになっています。ユーザーが電話またはアプリによる確認のみをサポートしているデバイスを使用する場合には、物理的なスマート カードがサインインの第一オプションとして表示されることはありません。画面では、2 番目の要素として電話による確認を使用してユーザー名とパスワードでサインインするオプションが使用可能ですが、これは意図的に選択すべき限定的なオプションです。

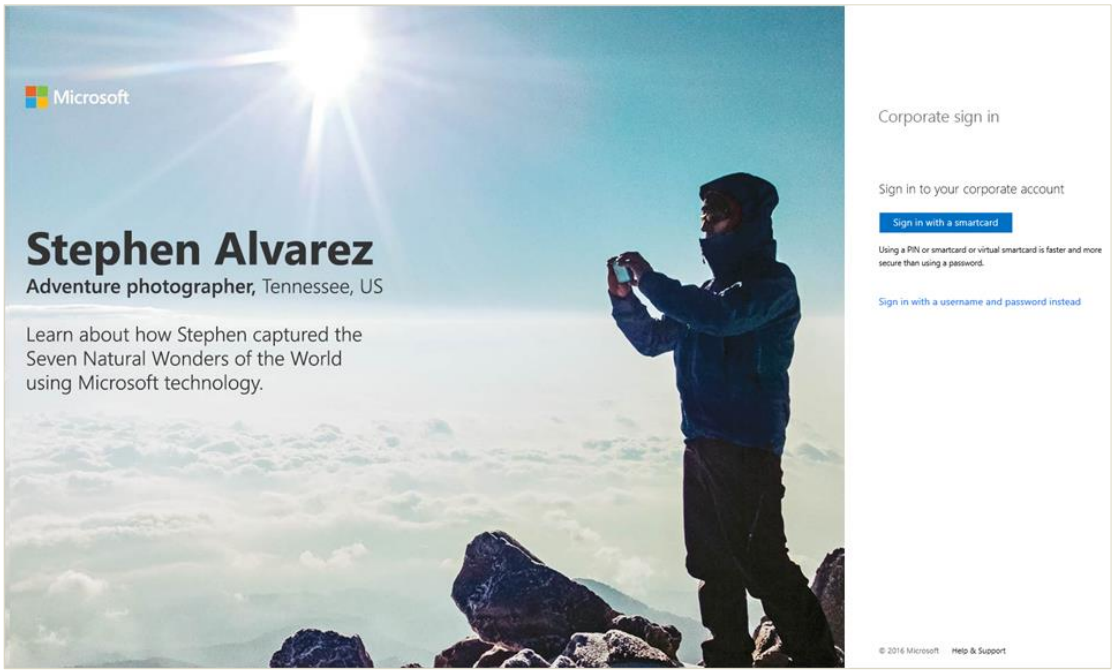

図 1. カスタマイズされたサインイン画面

サインインの失敗画面には、さらなるセルフヘルプ オプションが用意されていて、問題を解決するための手順をユーザーに示します。それらの手順でユーザーの問題が解決されない場合は、グローバル ヘルプデスクの連絡先情報が提示されます。

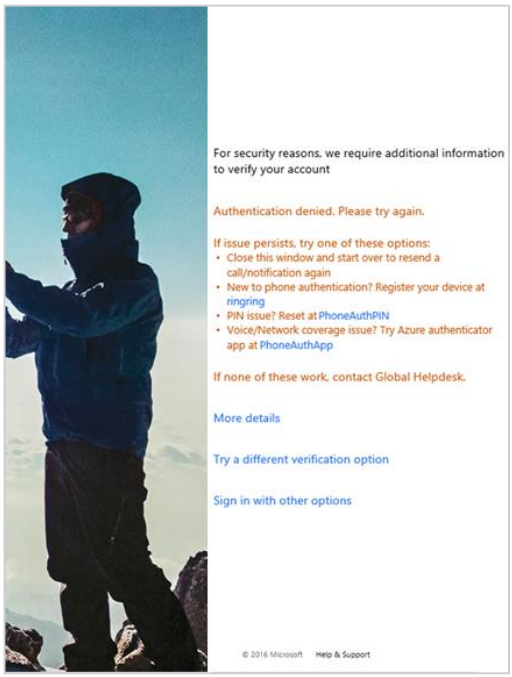

図 2. ユーザーによる問題のトラブルシューティングを支援するためにカスタマイズされたサインオンの失敗画面

AD FS サインイン ページのカスタマイズの詳細については、「AD FS サインイン ページのカスタマイズ」を参照してください。

追加のシナリオ

マイクロソフトでは、ユーザーのエクスペリエンスを向上させ、ヘルプデスクへの問い合わせ件数を減らし、サービスのパフォーマンスを高めるために、いくつかの追加のシナリオを有効化しました。

リモート アクセスのセキュリティ保護

リモート アクセスの場合、VPN インフラストラクチャは長い間、安全にサインインするために物理または仮想スマート カードを必要としてきました。Azure Multi-Factor Authentication が追加されたのに伴い、マイクロソフトでは、既存の VPN/RADIUS インフラストラクチャとの統合が可能になり、ユーザーは、電話またはモバイル アプリによる確認を使用してサインインすることも可能になります。これには、Microsoft Windows Server ベースの VPN クライアントのコンポーネントである Connection Manager 内でこのオプションを使用できるようにすることも含まれます。ユーザーは、リモート アクセスでそれぞれ好みの強力な認証方法を使用することができるようになりました。このことは、ユーザーが、スマート カードの入手に時間がかかる場所にいるときに、より高速なリモート アクセスを可能にするために役立ちます。

パスワードの変更

マイクロソフトのユーザーは、内部の、クラウドベースのセルフサービス パスワード管理ソリューションを使用してパスワードを変更できるようになりました。Azure Multi-Factor Authentication は、電話やモバイル アプリを使用した確認を含めて、プロセスの一部として統合されています。ユーザーは、パスワードを変更する際、追加の確認のための質問に答えることを求められます。ユーザーがパスワードの変更を必要とするときは、すぐに変更できるようになりました。グローバル ヘルプデスクに問い合わせる必要はありません。

パフォーマンスおよび高可用性の実現

マイクロソフトの Azure Multi-Factor Authentication サーバーは Windows Server 2012 R2 AD FS で構成されています。高可用性および冗長性を提供するため、認証トラフィックをプライマリ Multi-Factor Authentication サーバーに向けることはありません。これにより、パフォーマンスの問題を抱えることなしにサーバーの更新が可能になるよう支援します。

分散されたセカンダリ Multi-Factor Authentication サーバーには、プライマリ サーバーの Multi-Factor Authentication 構成データベースの読み取り専用コピーが格納されます。セカンダリ サーバーは、プライマリ サーバーに接続され、プライマリ サーバーとの間でデータが同期されます。セカンダリ サーバーにより、フォールト トレランスとアクセス要求の負荷分散が実現されます。Azure Multi-Factor Authentication Server は、AD FS と同じサーバー上では実行されていないため、AD FS を実行しているサーバーに AD FS 向けの Multi-Factor Authentication アダプターをローカルにインストールしました。各仮想アダプターは、Multi-Factor Authentication サーバー上の Web サービス SDK への証明書認証向けに構成されています。

マイクロソフトでは、負荷分散のために、DNS ラウンド ロビンとハードウェアの組み合わせを使用します。Azure Multi-Factor Authentication Server のインストール手順の詳細については、「Azure Multi-Factor Authentication Server の概要」を参照してください。

サービスの正常性の監視

サービスの正常性およびパフォーマンスを監視するため、マイクロソフトでは、Multi-Factor Authentication および AD FS インフラストラクチャを通じて代理クライアント フローを開発しました。企業ネットワーク上のライブ アプリケーションやリソースに対する権利を何も持たないテスト アカウントを使用して、エンドツーエンドのクライアント フローをテストする代理トランザクションを実行しました。1 日の代理トランザクションの絶え間ない流れを使用して、サービスの低下をすばやく特定し、ユーザーに影響が及ばないうちにそれらを解決することが可能です。AD FS サーバーに対する詳細な監視、レポート、およびアラートのために、Azure AD Connect Health を使用しています。Azure Active Directory Premium の機能である Azure AD Connect Health は、クラウドおよびオンプレミスの ID インフラストラクチャを監視し、セキュリティで保護するのに役立ちます。「AD FS での Azure AD Connect Health の使用」に、Azure AD Connect Health に関する詳細情報が記載されています。

また、Visual Studio Application Insights のリアルタイムの指標を使用して、要求の負荷、サーバーのパフォーマンス カウンター、および依存関係間の応答時間を分析します。これは、例外および失敗した要求を診断し、それらをイベントおよびトレースに関連付けて、標準指標と比較した多次元分析を行うことを支援します。Visual Studio Application Insights は、アドホック クエリを通じてパフォーマンス挙動の原因を特定するのに役立ちます。Web アプリおよびサービスにおける問題の検知、トリアージ、および診断方法の詳細については、「Visual Studio Application Insights」を参照してください。

不正アクセスのアラート機能は、ユーザーがリソースへのアクセスを試みる際に不正なアクセスであることを報告できるように構成され、セットアップされています。不正な疑いがあるアクセスが報告されると、マイクロソフトは、調査を行い、サービス レポートに含まれているアカウントのロック アウトなどのアクションを即座に実行することができます。

Multi-Factor Authentication サーバーから単一のデータベースにテキストベースのログ機能を統合しました。サポート チームは、スクリプトを使用してそれらのレポートに対するクエリを実行します。また、サポート チームがより大きな問題に目を向けることができるように、Microsoft SQL Server Reporting Services レポートを作成しました。

レポート機能により、どのような問題が発生しているのか、より良いユーザー エクスペリエンスを提供するにはどうしたらいいのかなどに対する見識が得られます。レポートは、サービス管理チームによって使用されて、ロールアウト時の傾向を把握するのに役立ちました。ロールアウト後、サービス マネージャーは、電話による認証のために電話を使用したユーザー数、およびモバイル アプリケーションを使用したユーザー数に関する利用統計情報につい

て、ユーザー エクスペリエンス サービスの正常性レポートを監視しました。サービスの正常性レポートによって、サービス マネージャーは、特定の日に認証されたユーザー数や、サービスがどのように実行されたかについて知ることができます。

条件付きアクセス制御

AD FS ルールを使用してアプリケーションへの条件付きアクセスを提供することができます。多要素認証をどの程度きめ細かく適用するかは、アプリケーション レベルで変えることができます。AD FS には柔軟性があります。AD FS によって、アプリケーションにアクセスできるユーザー/グループを指定したり、企業ネットワーク上または企業ネットワーク外でのそれらユーザー/グループの認証方法を決めることができます。企業ネットワーク上のアプリケーションにアクセスするほとんどのユーザーは、単一認証が許可されており、インターネットからアクセスされるアプリケーションでは、多要素認証が求められます。一部のアプリケーションは、重要なため、ユーザーが企業ネットワークからアクセスする場合でも多要素認証を要求します。

Windows Server 2016 へのアップグレード

Windows Server 2012 R2 上の AD FS を Windows Server 2016 上の AD FS に移行することは、従来よりもはるかに簡単になっています。Windows Server 2012 R2 ファームに新しい Windows Server 2016 サーバーを 1 つ追加するだけで、このファームは Windows Server 2012 R2 ファームの動作レベルで動作するので、外観と動作は Windows Server 2012 R2 ファームのようになります。その後、新しい複数の Windows Server 2016 サーバーをファームに追加し、機能を検証して、ロード バランサーから古いサーバーを削除します。ファームのすべてのノードで Windows Server 2016 が動作した時点で、ファームの動作レベルを 2016 にアップグレードして新機能を使い始める準備が完了します。

ベスト プラクティス

- 管理のしやすさを向上させます。他のサービスとの共通のレポートおよびレポート ダッシュボードへの統合により、すべてのサービスのエンドツーエンドのビューが提供されます。
- ユーザー エクスペリエンスに重点を置きます。これは、セキュリティの取り組みおよび普及のサポートに関しては特に重要です。新しいセキュリティ対策がユーザー エクスペリエンスを低下させると思われている場合、経営陣やユーザーは変化に抵抗する可能性があります。
- 代理トランザクションを使用して、Azure Multi-Factor Authentication 環境のパフォーマンスを定期的にテストします。これは、ユーザーに影響が及ばないうちに対処できるように、早期にサービスの低下を特定するのに役立ちます。
- 代理トランザクション向けのテスト アカウントを作成します。ライブ アプリケーションやリソースへのアクセス権を持たないアカウントを使用することで、お使いの環境のサービス パフォーマンスをテストする間、情報のセキュリティを確保するのに役立ちます。
- 今後の変更について広範囲に意思疎通を図り、ユーザーにとっての負担が最小限になるようにします。ユーザーの認知と利用方法に関するガイダンスの徹底は、変更管理のキーです。マイクロソフトでは、Yammer のソーシャル チャネル、電子メールによるキャンペーン、印刷物、ポスター、およびデジタル サイネージを組み合わせて使用しました。

詳細情報

Microsoft IT

Microsoft.com/ITShowcase

Microsoft Azure Multi-Factor Authentication