ManageEngine
AD360

過去10年の
3大セキュリティ被害

はじめに

デジタルトランスフォーメーション（DX)は昨今の組織をより柔軟かつ効率的なものへと変えていきました。従業員は自分が所有するデバイスをつかって、いつでもどこからでも業務ができるようになっています。しかしこの変化によって、これまでオンプレミス型のITネットワーク環境を守ってきた従来の方法では、ユーザーIDの保護がもはや立ち行かなくなっています。そのため、従業員やベンダー、パートナーからその他関係者に対するアクセス制御には、必ずID認証を介さなければいけません。そしてなにより、そのユーザーに対するアクセス権は、本来の目的に必要な最低限のものでなければなりません。

従来のID認証方法といえば、パスワード認証、ハードウェアによるトークン認証、またスマートカードによる認証などになります。しかし、今日のIT環境は、日々強大化するセキュリティ脅威と隣り合わせにあるので、バイオメトリクス認証・機械学習（ML）・コンテキストベースの認証方法など、様々なセキュリティ施策によるID保護の強靭化が求められるようになっています。昨今の職場環境において、日々多くのアプリケーションが従業員によって使われていますが、そこで使われるパスワードの多くは、覚えやすく単一なものに設定されがちです。この場合、もし攻撃者にパスワードが奪われてしまうと、そのアプリケーションへのアクセスを許してしまうことになります。

ネットワーク内の全てのユーザーの行動を理解すること（つまり、誰が、いつ、どこから、どのデバイスを使って、どの情報にアクセスしているか）は、ネットワークセキュリティ上重要です。つまり、ユーザーの通常動作を把握しておき、異常な動作を確認後、即座に脅威検知と対応が行えているのが望ましいです。そしてこれらを実現できる高度な分析技術を、組織として実装できていなければなりません。

これらを実現するために、組織として強力なIAM（Identity and Access Management）のフレームワークを採用していかなければなりません。このフレームワークは、攻撃者による特権の昇格や機密性の高いアプリケーションへの不正アクセスを防止し、ITに関する法令の遵守と、より詳細なセキュリティ監査とフォレンジックへの対応を可能にします。このEbookでは、堅固なサイバーセキュリティシステムを備えた組織が、不十分なIAM対策により、いかに壊滅的なデータ侵害の犠牲になったかについて紹介します。

不十分なIAM対策３選

Deloitte社

世界で「ビッグ４」と呼ばれる会計事務所の一つ、Deloitte社は2017年にサイバー攻撃の被害に遭いました。米国最大のコンサルタント会社の1つとして、同社は強力な政府機関や、金融機関、また多国籍企業にサイバーセキュリティ分野でのアドバイザリーサービスを行っていたのもあり、大量の機密性の高い財務データや個人データにアクセスしていました。

2017年の収益だけで370億ドルに上っていたDeloitto社には、堅牢なセキュリティシステムを実装するのに十分なリソースがあったはずです。しかし、これが突破された原因は、たった一つのパスワード漏洩でした。攻撃者集団はどのような手を使ったのでしょうか。

攻撃者たちは、管理者アカウントを介してデロイトのグローバルメールサーバーを侵害しました。この管理者アカウントは、ネットワーク全体に無制限にアクセスが可能で、しかも1つのパスワードでしか保護されていませんでした。つまりDeloitto社は、IAMの重要なベストプラクティスである多要素認証（MFA）の実装をしておらず、管理者アカウントを無防備なまま放置していたことになります。あるレポートによると、攻撃者集団は、Deloitto社のシステム内にある、メールからパスワード、ビジネスアーキテクチャの一覧図や、IPアドレスなどのさまざまな機密情報に対して、約6か月の間アクセスしていました。

皮肉にもDeloitto社は、その事件が起こるまでの間、5年連続でGartnerによるサイバーセキュリティコンサルティング分野で1位にランク付けされていました。

eBay社

人気のあるオンラインECショッピングプラットフォームのEbayは2014年にセキュリティ被害に遭いました。その年の2月下旬から3月上旬にかけて、攻撃者たちは複数の職員のアカウントを侵害し、企業ネットワーク内への侵入に成功していました。

なんと攻撃者たちは7カ月の間検知されることなく、暗号化されたパスワードや個人情報など、膨大な量のデータを盗み取っていました。盗まれたパスワードは全て暗号化されいたものの、eBayは万が一に備えて、1億4500万人の顧客に対してパスワードを変更するよう促しました。

このデータ侵害で財務データが無断公開されるようなことはありませんでしたが、長い目でみればハッカー集団たちが得た情報は今後、更に大きな問題へと発展する可能性があります。つまり、名前やメールアドレス、電話番号、生年月日、そして1億4500万人分の登録されている住所があれば、スピアフィッシング攻撃やソーシャルエンジニアリングなど、多数の攻撃を仕掛けることができてしまうということです。

Home Depot社

アメリカ合衆国最大のホームセンター小売チェーンであるHome Depotは2014年に大きなデータ侵害の被害に遭いました。当初、この侵害は5,600万人のクレジットカード所有者に影響を及ぼしたと報告されていましたが、その後、侵害の範囲には5,300万通のメールも含まれていることが明らかになりました。では、このような大規模なデータ侵害はどのようにして発生したのでしょうか。

Home Depotのネットワーク侵害の足がかりとなったのは侵害された第三者ベンダーのアカウントしたが、これはMFAの実装で回避できた可能性が高いです。その後、一切の検知の目をかいくぐり、ハッキングされたアカウントで権限昇格が行われた後、カスタマイズされたマルウェアがシステム内に埋め込まれました。更に、これら機密データは検知されることなく簡単に盗み取られました。当時のHome Depot社には、イベント情報のキャプチャリングや、分析とレポートといった検知機能がなかったため、この悪意のあるアクティビティを時間内に見つけて攻撃を阻止することができませんでした。

Home Depotはデータ侵害は6200万ドル（日本円で約73億円）の損害を被るとされていました。しかし、その後の調査でその被害総額はもっと多いことが判明したと同時に、その2年後の訴訟により、和解金2500万ドル（日本円で約30億円）が追加されました。

より効果的なIAMにAD360がどう貢献するのか

AD360は、ユーザーIDを管理し、リソースへのアクセスを管理し、セキュリティを強化し、コンプライアンスに準拠するためのIDガバナンスおよび管理ソリューションです。AD360では、ユーザープロビジョニングから、セルフサービスによるパスワード管理、Active Directory（AD）変更監視からエンタープライズアプリケーションのシングルサインオン（SSO）まで、IAMの実装に必要な機能をすべて実装することができ、また使いやすくシンプルなUIで管理が可能なソリューションです。

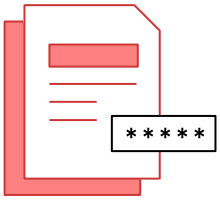
AD360はこれらの機能性をWindows AD, Exchange Server, Office 365プラットフォーム向けに提供します。AD360では、オンプレミス、クラウド、ハイブリッド環境問わず、一つの管理コンソールよりIAMに関わる管理が可能です。

1 アクセス権限のプロビジョニングとディプロビジョニングを自動化する

新しく入社した社員に対して職務・役職に応じたアクセス権限を付与し、承認ベースのワークフローを適用することによって、信頼性を高めます。既に退社している従業員のアクセス権限の剥奪を自動化しておくことで、人為的ミス（アクセス権の剥奪し忘れやアカウントの無効化し忘れなど）による副次的な被害の可能性を減らします。

AD360では、ユーザーのプロビジョニング及びディプロビジョニングタスクのルーティン作業を簡略化する自動化プロセスを設定することができます。シンプルなユーザーリストを用意しておくだけで、その他のルーティン作業、例えばドメインアカウント作成や、グループ追加、またMS365ライセンスの付与などの一切をAD360が請け負います。

2 複雑なパスワードポリシーの作成と適用

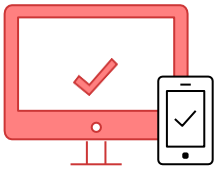


パスワードの複雑性を増すようなポリシーを強制適用することによって、従業員に弱いパスワードを使わせないようにできます。特殊文字、数字、文字列をバランスよく組み合わせたパスワードは、ハッカーにとってブルートフォース攻撃やパスワードクラックを難しくさせます。

AD360のパスワードポリシーエンフォーサー機能によるカスタムパスワードポリシーを適用することで、組織のサイバーセキュリティレベルを強化できます。また、経営幹部レベル、IT管理者、IT以外のスタッフなど、さまざまな権限を持つユーザーに、それぞれ違うポリシーを適用させることができます。パスワードの複雑性を高めるために、AD360では次のことが可能です。

- 回文、辞書の文字などがパスワードとして使われないよう防止する
- 「Have I Been Pwned APIサービス」との連携により、パスワード変更やリセットの際に侵害されたパスワードを使わせないようにする
- 特権ユーザーに対して特定のより厳格なポリシーを設定する柔軟性を保ちながらも、OUやグループ毎にパスワードポリシーを設定する
- 古いパスワードやユーザー名からの連続した文字列の使用禁止や、同じ文字、数字を2回続けて使用することを禁止する、など

3 多要素認証（MFA）の有効化



多要素認証（MFA）を実装することで、パスワードが侵害されたとしてもアカウントの乗っ取りを防ぐことができ、セキュリティをもう一段階強化することができます。MFAでは様々な要素を認証に追加することができます。例えば指紋認証や、SMSでの認証コード送信、またプッシュ通知などが挙げられます。また、シングルサインオン（SSO）にMFAを実装することで、従業員のID認証をより一層強固なものにできます。

AD360のMFA機能では、様々な端末（Winodws、Linux、MacOSなど）に対して2段認証を実装することができます。また100以上のアプリケーションへのMFAによるSSOに対応可能です。加えて、SAMLに対応しているカスタムアプリケーションであっても、SSOを実装できます。この機能で、ユーザーによるエンタープライズアプリケーションへのアクセスをよりセキュアにすることができます。

4 特権アカウントの制御

重要なデータやリソースへのアクセスを持っている特権アカウントユーザーは、攻撃者にとって恰好のターゲットとなります。組織は特権アカウントとそのアクセス権限を正確に把握すると共に、それらのアカウントによるアクティビティも追跡できていなければなりません。ユーザーの振る舞い検知（User Behabior Analytics、以下UBAという)を導入することによって、組織は特権ユーザーによって行われた異常なアクティビティを一早く検知し、能動的に対処することができます。

5 ユーザーアクティビティの監視

ユーザーのアクティビティを追跡することは非常に重要です。だれが、いつ、どこでログオンし、ログオンに失敗し、特権によるアクセスを行い、特権アクセスを変更したのかを追跡できているのが望ましいです。また、法令遵守に係る監査対応においては、それらの詳細を文書化しておくことが一般的です。

AD360は、どのユーザーがどのリソースにアクセスしたか、またそれらのリソースに対して何が行われたかを詳細に示す包括的な監査証跡を残すことができます。また、SOX、HIPAA、GLBA、GDPR、PCI-DSS、FISMA向けの監査レポートが標準搭載されています。他にも、カスタマイズされた監査レポートが生成され次第、定期的にメールで送信するような設定も可能です。

6

ゴーストアカウントや非アクティブなアカウントを特定

非アクティブのアカウントを放っておくと、不正アクセスの温床を招きます。特に退職する役職高い従業員アカウントは、財務データや知的財産などの重要なリソースに対して不正アクセスを引き起こす可能性があります。攻撃者たちは、ソーシャルメディアなどの様々な情報源から偵察活動を続けます。そして、退職がきまった上級の従業員を見つけ、これらのアカウントを標的として、検知を免れながら侵入の足掛かりを作ります。

AD360では、非アクティブアカウントの発見から削除までを定期的に行う自動化機能があります。また、申請承認のフローと連携させれば、どの非アクティブアカウントが削除されるのかを確認することができ、誤削除なども防ぐことができます。

過去10年の3大セキュリティ被害について

2022年3月発行

本製品に関するお問い合わせ
ゾーホージャパン株式会社ManageEngine事業部
〒2220012 事業部神奈川県横浜市西区みなとみらい三丁目 6 番1 号みなとみらいセンタービル

AD360 製品ページ：https://www.manageengine.jp/products/AD360/
ホームページ：https://www.manageengine.jp/

■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。
ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。
当社は、本ガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

ZJMR2022391015