Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Multifactor Authentication Recommendations (多要素認証に関する M³AAWG 推奨) February 2017

この文書への URL: www.m3aawg.org/multifactor-authentication-bp

I. はじめに

ユーザが選んだ単純な単語からランダムな文字列を含む複雑なフレーズまで，パスワードは多くの欠点を持っている．例えばブルートフォース型のパスワードクラッキングはより高速化、高効率化しており，不正なログインは個人と会社の両方に対して，壊滅的な損失をもたらすようになってきている．そして最もクラック耐性の高いとされるパスワードでさえも破られる可能性がある．

しかしながらパスワードはユーザアカウントをセキュアに保つための標準的なソリューションであり続ける．M³AAWG は，過去にアカウント乗っ取りの被害を受けた，ないし，今後高い確率で被害を受ける可能性があるサービスの防御を向上させるために，サービス提供事業者が，シンプルなパスワードに代わって多要素認証を要求すべき時が来たと考えている．

II. 多要素認証とは何か？

多要素認証は以下のうち 2 つ以上の組み合わせによってアカウントのセキュリティを強化する:

- ユーザが"知っている"要素(パスワードあるいは PIN)
- ユーザが"所持している"要素(ハードトークンあるいは登録されたスマートフォン)
- ユーザが"ユーザ本人である"ことを示す要素(チューリングテストや指紋あるいは他のバイオメトリック要素)

上記のうち 1 つの要素を複数回使うことは要件を満たさない．例えば，出身地とペットの名前のように「ユーザが知っている」2 つの要素を要求するだけでは多要素認証とは見なせない．

III. なぜ多要素なのか？

サイバー犯罪者はユーザアカウントへの不正アクセスを得ることに大変意欲的である．サービス提供事業者のセキュリティログを見たことがある人は誰でも，インターネットに接続されたシステムが定常的に不正アクセスを得る目的を持った者からの包囲攻撃に晒されていることを知っている．パスワードをアカウント乗っ取りの大惨事に対する唯一の防御メカニズムとして使用していることがしばしばあるが，パスワードのみでは脆い防御しか与えない．

多要素認証はアカウントの防御強度を大きく改善する能力を秘めている．真の多要素認証の利用は最近目立つアカウント指向の攻撃のリスクを劇的に低減し得る．多要素認証をオプションとして提供する大手企業の数は増えているが，残念なことに多くの他の企業はいかなる多要素認証オプションも全く提供していない．また，全てのユーザに多要素認証を課している企業は事実上存在しない．

この状況を変えるべき時が来ている．

IV. M^{3}AAWG 推奨

- M^{3}AAWG は，過去にアカウント侵害で大きな被害を受けた，ないし，今後高い確率でアカウント侵害を受ける恐れがあるサービスにおいて，全てのサービス提供事業者が全てのユーザに対するオプションとして多要素認証を提供することを推奨する．
- M^{3}AAWG は，経理部門のスタッフ，会社の上級役員，オンラインの有名人など，高い価値を持ち，人々の注目を集めやすく，一般的に標的にされやすいユーザに対して多要素認証を必須とすることを推奨する．
- M^{3}AAWG はシステム管理者，ネットワーク技術者，データベース管理者，セキュリティチームのメンバ，財務用アカウントにアクセスできるスタッフや他の重要ユーザ等のように，特権を持つユーザに対して多要素認証を必須とすることを推奨する．

これらの推奨は特定のテクノロジーを指定するものではない．ある環境に良く適合するテクノロジーでも異なる環境ではほとんど適合しないかもしれない．それ故，M^{3}AAWG は特定の多要素認証製品や提供事業者の利用を推奨するものではない．

V. 多要素の実装上の考慮事項

多要素のオプションを考える際にサービス提供事業者は以下の実装上の考慮事項に留意すべきである.

- 多要素認証の実装を成功させるには, 通常, 経営層の支援と技術チームからの熱烈なサポートを要する. もし組織の経営陣と技術チームが多要素認証のアイデアを支持しなければ, それは実装されないだろう.
- 商用ソリューションであるかオープンソースソリューションであるかに関わらず, 必要になる資金を確認せよ. 多要素認証の実装は, たとえそれが「無料の」オープンソースソリューションを使ったものであっても, 費用は不要にはならない. しかしながら, 実装にかかる費用と, 止むことのないアカウント侵害や他の同様なインシデントに対応するために会社が失っている費用を秤にかけることには価値がある.
- 多要素認証ソリューションの候補を評価する際には, 簡単に使えることを最優先に考慮せよ. もし多要素認証ソリューションが使いづらいものであった場合, それは使われないだろう.
- 通常時の使いやすさについて考えるのに加えて, 例外的な状況についても考えよ. それは, 多要素認証が通らなくなったり, 要素を失ったユーザを技術チームがどう扱うか? ということである. ユーザは緊急用バックアップコードを持ち運べるか? ユーザはハードトークンとスマートフォン上で動くバックアップのソフトトークンの両方を登録しておけるか?
- 少なくとも何人かのユーザが彼らのアカウントをセキュアに保つことの重要性を軽く見ることに対して備えよ. これらのユーザを教育し, たとえ一般のアカウントであっても防御の重要性を理解できるようにすることが必要になる. 現実には, 一般のアカウントであってもその侵害が攻撃者の能力を劇的に増加させ, 最終的に特権アクセスを取られる可能性がある.
- 技術チームがサポートする全てのプラットフォームについて考えよ. ラップトップ PC を使うユーザもいれば, タブレットやスマートフォンを使うユーザもいるだろう. 多要素認証ソリューションが全ての一般的プラットフォームで動作することを確認せよ.

VI. 結論

M^3AAWG は, サービス提供事業者に対し, 業界他社が多要素認証を実装するのを待つことなく行動を起こすよう強く推奨する. 普及に必要な数（クリティカルマス）の機関がリーダーシップの役割を果たし, 業界の同業者のための事例を作る必要がある --- そうしないとデッドロックが発生する可能性がある.

さらに,「完璧への探求」をするソリューションが意味のある進歩を脱線させることがないようにし, 代わりに「リスクの最小化」を考えよ. 完璧ではないかもしれないが, それだけで普通のパスワードよりはるかに優れているたくさんのソリューションが利用可能である.

M^{3}AAWG が公開している全てのベストプラクティスと同様, この文書の更新については M^{3}AAWG Web サイト(www.m3aawg.org)をチェックして下さい.