RESOURCE CENTER

Five Best Practices for Enterprise Password Management

Learn the best practices for enterprise password management in this white paper.

Get the full interactive view at https://bitwarden.com/ja-jp/resources/five-best-practices-for-password-management-white-paper/

bitwarden

組織がセキュリティの優先順位を高め続ける一方で、その努力の重要な部分は、ベストプラクティスについて一般ユーザーを教育し、権限を与えることである。Yubico 2019 State of Password and Security Authentication Security BehaviorsReportから、これらの統計のいくつかを考えてみよう：

- 回答者の3人に2人が同僚とパスワードを共有している
- 参加者の51%が、個人アカウントとビジネスアカウントでパスワードを再利用していると回答した。
- 57%がフィッシング詐欺に遭った後もパスワードを変更しなかったと回答している。

企業に変化をもたらすには、セキュリティとITのチームがベストプラクティスについて従業員を教育する必要がある。パスワード管理に関して、パスワード衛生を奨励する最も簡単な方法の1つは、職場全体にパスワード管理ソリューションを導入することです。ここでは、採用すべきベストプラクティスをいくつか紹介しよう。

1.パスワード管理ソリューションの活用

一日を通して、ほとんどの人がパスワードを必要とする様々なサイトを訪れる。ユニークで十分に強力なパスワード（またはパスフレーズ）を数多く記憶することは、事実上不可能である。パスワード・マネージャーは、異なるサイト間でのパスワードの使用を簡素化し、ユーザーをより安全に保つ。世の中には、しっかりしたパスワード・マネージャーがいくつもある。クロスプラットフォームで動作し、個人向けに無料または非常に安価でサービスを提供するものを優先する。ほとんどのパスワード・マネージャーの機能も、年々拡張されている。

2.組織全体に簡単に導入できるツールを選ぶ。

パスワード・マネージャーは、初心者から上級者まで、あらゆるレベルのユーザーにとって使いやすいものでなければならない。大規模または分散した従業員ベースを考慮する場合、アプリケーションはユーザーが直感的に使用でき、導入が容易でなければならない。例えば、Bitwardenクラウドを選んでも、セルフホストインスタンスをデプロイしても、Bitwardenの立ち上げと運用は簡単です。また、Bitwarden Directory Connectorは、Azure、Active Directory、Google、Oktaなど、現在最も広く使用されているディレクトリサービスと連携し、Bitwardenのユーザーをチームや従業員と同期させることができます。

3.パスワードを変更するのは、情報漏えいの可能性があるときだけにしてください。

パスワードを3ヶ月ごとに変更する時代は終わった。今は、危険にさらされていると思われる場合にのみ変更するべきだ。米国立標準技術研究所（NIST）は、パスワードを頻繁に変更することを推奨していない。これは実際に、時間の経過とともにパスワードが弱くなる可能性のある行動につながる。パスワードが漏洩したかどうかは、クレジットカードの不正使用など目に見える証拠を参照するか、パスワードが漏洩したかどうかを判別できるツール（パスワード・マネージャーなど）を使用することで判断できます。

4.強固でユニークなパスワードを使用する。

オンラインで利用するすべてのサービスに、強力でユニークなパスワードを使用することで、データ漏洩の影響を最小限に抑えることができます。強力なパスワードとは、必ずしも一般的な単語や名前に特殊文字や数字を加えることではなく、パスワードのエントロピー、つまりランダム性を高めることを意味する。強力なパスワードを作るための簡単な戦術のひとつは、パスフレーズを使うことだ。パスフレーズとは、一見無関係に見える単語やフレーズを組み合わせたもので、ユーザーにとっては記憶に残りやすいが、そうでなければ攻撃者に推測されにくいものである。パスフレーズは高いエントロピーを持つと同時に、覚えやすい。

5.可能な限り二要素認証を有効にする。

二要素認証（2FA）が消費者向けサイトやビジネスサイトで一般的になりつつある今、優れたパスワード・マネージャーには、この機能を拡張する方法が含まれているはずだ。2FAを使用すると、マスターパスワードを入力する以外に別のトークンを入力する必要があるため、アカウントのセキュリティが向上します。たとえ誰かがあなたのマスターパスワードを発見したとしても、追加トークンにアクセスしなければ、パスワード・マネージャーにログインすることはできない。パスワード・マネージャーを始めたい方は、こちらから無料のBitwardenアカウントにサインアップできます。