yubico

アカウントの乗っ取りを防止し、ITコストを削減するGoogle社

2009年からGoogle社の社員を保護してきたYubiKey

ケーススタディ

Google

業界
テクノロジー

プロトコル
U2F

製品
あらゆるYubiKeyの
フォームファクター

デプロイメント
従業員

USB用U2F

Google社について

Google社は、世界の情報を整理してどこからでも活用できるようにする、という一つのミッションのもと、1998年に設立されました。それ以後、できるだけ多くの人々の生活を大きく向上させるサービスを開発することにフォーカスし続けたGoogle社は、今やフォーチュン50に名を連ねる国際企業となり、世界を代表するインターネット企業とみなされています。Google社のような革新的なテクノロジー企業の成長の鍵となるのは、機密情報へのオンラインアクセスを正当な社員や契約者に確実に限定することです。

アカウントの乗っ取りを阻止

2009年、Google社は従来型のセキュリティ機能を回避できる高度なサイバー攻撃の標的になっていました。そのような攻撃やアカウントの乗っ取りを効果的に阻止できる有効な2段階認証(2FA)の選択肢がなかったため、Google社はYubicoと密に協力し合ってYubiKeyの2段階認証技術を拡張し、公開鍵による暗号技術も導入し始めました。この協力を通じて、YubicoとGoogle社は単一のフィッシングに強いキーのコンセプトに基づいて強力な認証プロトコルを共同開発し、すべてのサービスを保護するようになりました。この作業が、後にFIDO Universal 2nd Factor (U2F)規格と呼ばれる、FIDOアライアンスが採用したオープンな規格に繋がります。

ユーザーの情報や秘密鍵をサービスプロバイダー間で共有することなく、一つのYubiKeyを使用して多数のオンライン・サービスを保護することができます。モバイルの接続性、携帯端末、モバイルアプリを選ぶことなく、また手作業によるコードの入力も不要です。

結果

Google社はワンタイム・パスワード(OTP)、TLS証明書、ICカードや他の認証方式を2年かけて評価した後、セキュリティや使いやすさに関する企業のニーズを最もよく満たせるのがFIDO U2F Security Keyであると結論づけました。そのすぐ後、Google社はYubiKeyの導入を拡大してすべてのスタッフや契約者のコンピューターやサーバーログインを保護するようになり、その数は現在、社員数50,000名を超えています。

ハードウェアベースの認証がビジネスに及ぼす影響を2年かけて評価したGoogle社の調査では、主に次のような重要なメリットが明らかになりました。

セキュリティ強化：社内アカウントをYubiKeyとFIDO U2Fだけで保護すれば、セキュリティが格段に向上することが判明しました。

社員の生産性の向上：社員がYubiKeyを使用すれば、SMSを介したワンタイム・パスワード(OTP)を使用する場合よりも大幅に（約50%）認証にかかる時間を削減することができました。YubiKeyを使用すれば、Google Authenticatorの場合よりも約4倍早くログインすることができました。このスピードを実現できるのは主に、ミリ秒レベルで実行されるワンタッチYubiKey認証のおかげです。

ケーススタディ

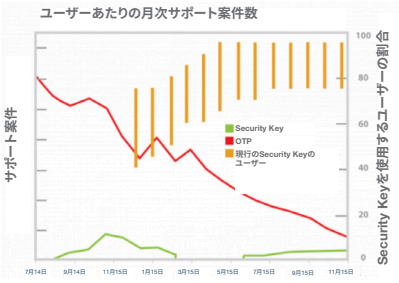
Google

業界
テクノロジー

プロトコル
U2F

製品
あらゆるYubiKeyの
フォームファクター

デプロイメント
従業員



サポートを削減： 認証のために電話を使う場合よりも使いやすく、堅牢な設計で、耐水性を持ち、壊れにくいのがYubiKeyです。またYubiKeyであれば、ユーザーのノートパソコン内に搭載するよう設計されたYubiKey Nano一つとキーチェーン用のYubiKey一つを使用するなどして、各社員に対して複数のバックアップを発行できるようになります。Google社は、サポートを求める電話を減らし（サポートの案件が92％減少）、年間のサポート・コストを数千時間削減することができました。さらに、推定される認証の失敗件数はゼロでした。

所有コストを削減： YubiKeyを使用すればセキュリティ、使いやすさ、ワークフローの効率が高まるため、Google社は各社員に複数のYubiKeyを与えながらも、全体のコストを削減することができました。

強力な2FAで社員や顧客を保護

今日、Google社はYubiKeyを使って社員を保護しているだけでなく、すべてのGoogleユーザーのためにYubiKeyとFIDO U2Fセキュリティキーのサポートを導入し、セキュリティを確保しています。Googleアカウントを持っているすべてのユーザーは YubiKeyによる強固な認証を利用し、高度なフィッシングを防止することができるようになっています。

フィッシングに対する強固な保護

ごく最近のことですが、Google社は2017年10月、ジャーナリスト、企業幹部、政治活動を行うチームのようなリスクが高いユーザーのためにAdvanced Protection Program (GAPP)を開始しました。このGAPPプログラムは、ハードウェアを使用するFIDO U2Fセキュリティキーを使って安全にログインすることを強制（任意ではなく）することで、Googleアカウントのユーザーの安全性をさらに高めるものです。Advanced Protectionは従来型の2段階認証よりも強力なフィッシングに対する保護を提供します。GAPPの参加者は、パスワードと物理的なセキュリティキー（つまり、YubiKey）を使ってアカウントにサインインすることが求められます。Google Authenticatorアプリ やSMS経由で送信されるコードなどのような他の2FAの認証方式はフィッシング可能なことが判明しているため、それらは機能しなくなります。

Adwordsの顧客を保護

Google社はまた、YubiKeyを使ってAdwordsアカウントを保護するメリットについても語っています。2016年、Google社はJellyfish社とiProspect社というデジタル・マーケティングの代理店2社が、YubiKeyを使ってAdwordsのアカウント、顧客、売上を保護している方法をブログで語っています。

モダンでスケーリング可能な認証

Google社は、革新と発明を中心に据えた、業界を牽引するテクノロジー企業です。現在はFIDO U2F規格と呼ばれている、強固な認証のためのオープンな規格を定義する際、欠かせない役割を担ったのが、Yubicoと協力しているGoogle社でした。現在、YubicoとGoogle社は10億を超えるGmailユーザーや50,000名以上のGoogle社の社員に対してフィッシングに強い強固な2段階認証を提供し、個人データを保護しつつ安全にインターネットを利用できるようにしています。大規模な導入を開始した後、セキュリティキーを使用してアカウントの乗っ取りが発生したという事案は確認されておらず、またユーザーの満足度も向上しています。

Google社、セキュリティ・エンジニアリング部門ディレクター、Mayank Upadhyay氏

「このトークンを使用することで、商業的に当時利用可能だったものを超えるレベルでセキュリティ水準を高めることができたと考えています。Googleのウェブブラウザである Chromeと連携するこのデバイスは、Googleの社員が日常的に行っているワークフローにシームレスに統合されています」

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301米国
844-205-6787（フリーダイヤル）
650-285-0088