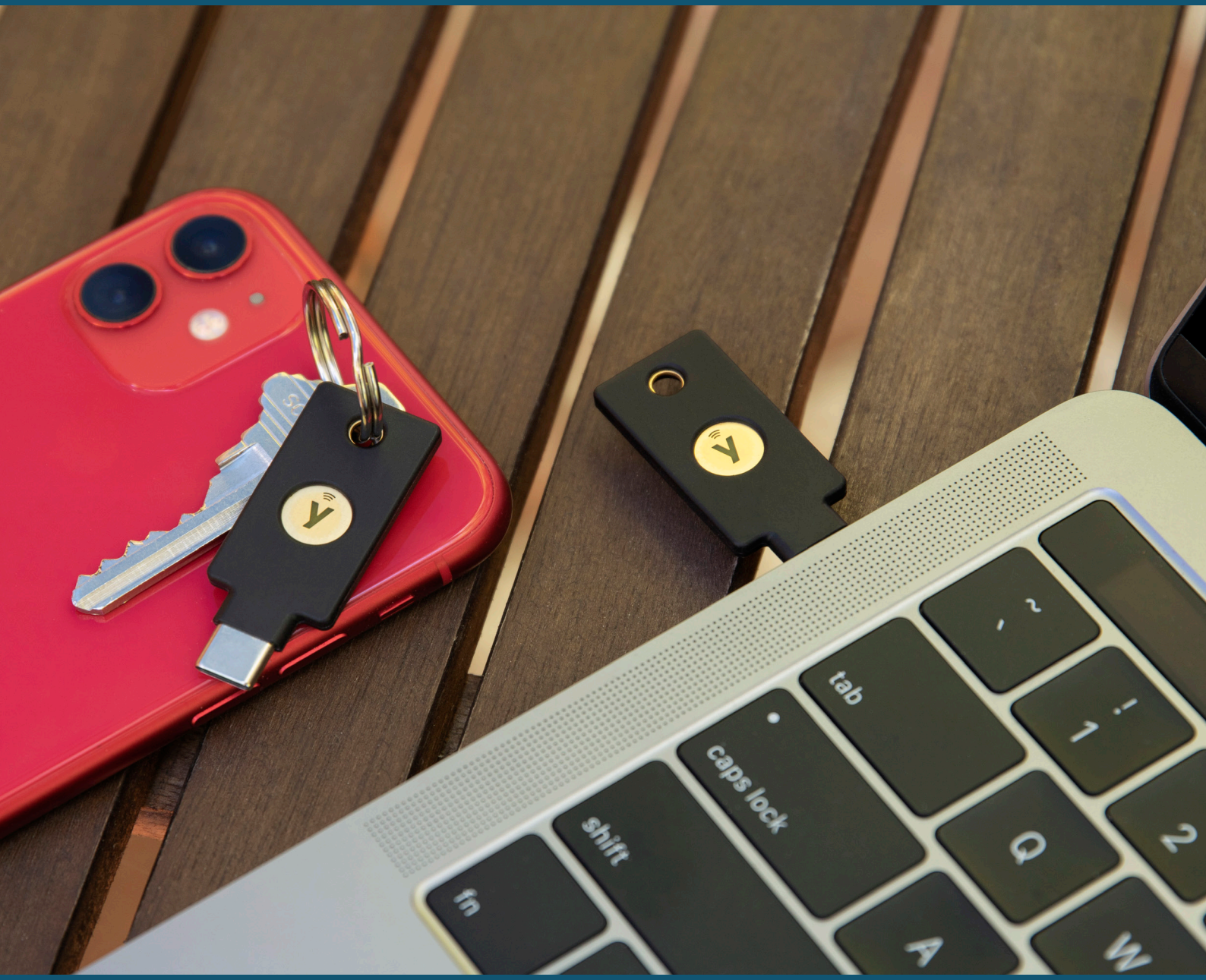

公共部門におけるサイバーセキュリティの強化：

州および地方自治体がハードウェアセキュリティキーを使用してアカウント乗っ取りに対処する方法

サイバーセキュリティは、政府機関にとってかつてないほど重要になっています。 2019年、政府は6,843件のセキュリティインシデントに対応し、そのうち346件の確認されたデータ開示が含まれていました。[1] これらのインシデントは、政府の攻撃対象領域を増やすソフトウェアのインストールから、クレデンシャルの紛失または盗難まで、さまざまな理由で発生します。

各機関が発生しているセキュリティ脅威に対処していくにつれて、インフラストラクチャとプロセスの最新化、ハイブリッドワーカーの支援と実現、接続とアクセスのセキュリティ保護など、直面するビジネスニーズも進化していきます。

IDとアクセスの管理は、包括的なサイバーセキュリティ戦略にとって極めて重要です。パスワードがフィッシング攻撃やアカウント乗っ取りに対して効果的ではない場合、効果的なものと比べて保護が不十分になります。そのため、政府機関はデジタルトランスフォーメーションへの取り組みを推進する際に、アクセス制御や認証を強化する多要素認証(MFA)ソリューションを採用しています。ただし、一部のMFAツールでは、未だセキュリティの欠陥が残っています。たとえば、プッシュ通知、SMS、OTPなどのモバイルベースの認証システムは、マルウェア、中間者攻撃、SIMスワップの影響を受けやすくなっています。さらに、これらのタイプのモバイルソリューションは、ユーザーを苛立たせる可能性があります。

リモートワークは、フィッシング攻撃やアカウント乗っ取りなどのセキュリティリスクを高める可能性があります。

フィッシング攻撃やアカウント乗っ取りなどのサイバー脅威に対抗するために、いくつかの州および地方の政府機関は、ハードウェアセキュリティキーを使用した強力なMFAの導入に取り組んでいます。ワンタッチ認証デバイスのユーザーは、コンピューターや携帯電話にそのキーを挿すことで、重要なシステムやアプリケーションに安全にアクセスできます。州や地方自治体はすでにこれらのキーを使用しており、リモートワーク環境でのリスクを軽減、ファーストレスポンダーの機密データへの高速アクセスの提供、選挙インフラストラクチャのセキュリティ保護、共有ワークステーションを含むコンピューティングデバイス上の機密データの保護、特権ユーザーやエアギャップネットワークへの安全なアクセスの提供、市民向けの迅速で安全なデジタルサービスを提供をしています。サクラメント市はリモートワークをより安全にし、ワシントン州は選挙インフラストラクチャの保護にこのソリューションを活用しています。カリフォルニア州ミッションビエホ市は、非常事態の際でも事業を継続するために使用しています。

公共部門はセキュリティ体制の強化に取り組んでおり、ハードウェアセキュリティキーを使用した強力なMFAを採用することで、州、市、郡の政府はセキュリティやユーザーエクスペリエンスを損なうことなく敏捷性を高め、これらの組織がより応答性の高いサービスを提供し、従業員のニーズを適切に満たすことができるようにしています。

サクラメント：より安全なリモートワークインフラストラクチャの構築

新型コロナウイルスによりリモートワーク環境が大幅に拡大したため、政府機関は急激に増えたセキュリティの脆弱性に直面しています。

「コロナウイルスが発生する前は、誰もが同じ場所で作業していたため、ユーザーアクセスを保護する方法に自信を持っていました」と、YubicoのソリューションエンジニアであるCody Hussey氏は述べています。Yubicoは、州および地方自治体がセキュリティを向上させるのに役立つハードウェア認証キーを製造しています。「現在、一部の職員は自宅で仕事をしているので、緩和策を変更する必要があります。」

リモートワークにより、セキュリティで保護されていない可能性のある家庭向けWiFiネットワークを使用している職員が、新たなセキュリティリスクにさらされる可能性があります。リモート職員が仮想プライベートネットワーク(VPN)を使用している場合でも、無許可の個人用デバイスやアプリをこのネットワークに接続することで、その機関のセキュリティが危険にさらされる場合もあります。

認証セキュリティを強化するために、サクラメント市は、フィッシング攻撃やアカウント乗っ取りから保護することを目的とした、Yubicoのハードウェアセキュリティキーベースの強力なMFAソリューションであるYubiKeyを導入しました。これまで、市は職員の認証にモバイルベースの音声およびテキストOTPを使用していました。しかし、すべての職員が政府支給のモバイルデバイスを所有しているわけではないため、さらに多くの職員がリモートで作業しなければならなくなった途端にこのアプローチは困難になりましたとサクラメントのシステムエンジニア長であるCurtis Chiuu氏は述べています。

「職員が私物の電話を業務に使用することを強制できないため、別のソリューションを考え出す必要がありました」とChiuu氏は言います。

サクラメントは以前、重要なインフラストラクチャにアクセスする必要のある少数のリモート職員や、政府支給のモバイルデバイスにアクセスできないフィールドワーカー用にハードウェアベースのMFAにより、デバイスベースの認証がなくなり、個人デバイス利用(BYOD)に関連する返還費用も削減されます。各職員は、共有ワークステーションのデータを保護するのにも役立つ自分専用のキーも取得します。YubiKeyのようなハードウェアベースの強力なMFAソリューション は、OTP、SmartCard、最新のFIDO U2F、FIDO2/WebAuthn認証プロトコルなどの複数の認証プロトコルを単一のセキュリティキーでサポートすることができ、ユーザーがさまざまなオンラインサービスに安全で便利にアクセスできるようになり、フィッシング攻撃やアカウント乗っ取りに対するセキュリティが強化されます。サクラメントのような政府組織がハイブリッドワーク環境に移行するには、これらすべての機能が重要になります。

ワシントン州：重要な選挙インフラストラクチャの保護

各機関は選挙に関するセキュリティの脆弱性に直面しています。ソフトウェアベースおよびSMSベースのMFAソリューションにより、実際に選挙機関への攻撃が増加し、それにより選挙機関はマルウェア、フィッシング攻撃、およびその他のセキュリティ脅威の影響をより受けやすくなる可能性があります。

ハードウェアセキュリティキーベースのMFAソリューションを採用すると、選挙機関が有権者登録システム、電子投票簿、その他の重要な選挙インフラストラクチャにアクセスする必要がある選挙スタッフおよび季節労働者に個々のハードウェアセキュリティキーを配布できるため、攻撃対象領域を縮小できます。ユーザーはユーザー名とパスワードを入力し、このキーをコンピューターのUSBポートに挿入し、キーのボタンをタッチすることで認証プロセスを完了することができます。モバイル経由でログインしている場合は、MFAプロバイダーのモバイルアプリを使用してデバイスを登録できます。登録後、NFC対応のモバイルデバイスに対してキーをタップするだけで、認証してログインできます。[2]

ワシントン州はYubiKeyを採用した際に、これらすべてのメリットを実現しました。季節労働者を含む選挙スタッフが公的業務に個人のデバイスを使用することに懸念を抱いていたため、州知事たちはモバイルベースのMFAソリューションを使用したくない考えであったことをワシントンの選挙局長であるLori Augino氏が述べています。

ワシントンでは、同日投票を促進し、州内39郡の選挙システムを統合する新しい州選挙管理システムであるVoteWAを立ち上げた際に、YubiKeyを使い始めました。この州では今まで、許可リストに記載された承認されたIPアドレス、強力なパスワード、およびユーザー権限を使用していました。キーベースのMFAを活用してセキュリティ層を追加したとAugino氏は言います。また、これにより選挙スタッフ用に政府支給のモバイルデバイスを購入するコストも削減できます。

「電話認証とは対照的な、YubiKeyが好きです」とAugino氏は言います。「私たちのシステムには、州や郡が提供する携帯電話を所有していないユーザーがたくさんいます。そのようなユーザーが機関やオフィスの業務に自分の個人用デバイスを使用することはまったく望んでいません。YubiKeyは、まさに、ここワシントン州で私たちが選んだ使いやすい多要素認証であり、望んでいた追加のセキュリティニーズを達成しました。」

ハードウェアベースのセキュリティは、選挙機関にいくつかの利点をもたらします。[1]つは、モバイル認証システムよりも優れたセキュリティを提供することです。セキュリティキーは、デバイス上のプロンプトでの90%の防止率、二次メールでの79%の防止率、SMSコードでの76%の防止率と比較して、アカウント乗っ取りを100%阻止します。[3] ハードウェアソリューションもバッテリーやネットワークへの接続の必要なしに機能します。た、NIST、FIDO、その他の業界標準のセキュリティおよび政府のコンプライアンス要件を満たしています。

「最新の脅威の手口、技術、慣行に対抗するためには、MFAによるセキュリティ体制と認証を向上させる必要があります」とAugino氏は言います。「このような重要なシステムにアクセスするために不可欠なものです。これなしでは運用できません。」

ミッションビエホ：デジタルサービスのセキュリティ強化

より多くの政府機関が市民にデジタルサービスを提供しており、非常事態の際に事業継続性を確保する上で重要な役割を担っています。

ミッションビエホ市はデジタルサービスを取り入れており、これにより市民が苦情を報告したり、さまざまな部門にサービスリクエストを送信したり、バーチャル会議に参加したり、オンラインで市の記録にアクセスすることができます。[4] この市では、タイムリーな更新を提供し、市民が公安問題を報告できるようにする独自のモバイルアプリであるMV Lifeアプリも採用しています。[5] このようなデジタルサービスでは、市民のデータの収集とバックエンドでの確認が含まれています。つまり、職員はオフィスにいる場合でもリモートで作業している場合でも、システムに安全にアクセスできる必要があります。

ミッションビエホの情報技術担当ディレクターであるJackie Alexander氏は、この市は今まで認証に複雑なパスワード要件を使用していましたが、セキュリティ体制を強化するためにハードウェアセキュリティキーベースのMFAソリューションを採用することに決定しましたと述べています。

「ユーザートレーニングとパスワード制限が実施されているとしても、最新の重要システムへのアクセスを保護するには、ユーザー名とパスワードだけでは不十分です。悪意のある攻撃者は、パスワードスプレーまたはソーシャルエンジニアリングを使用してアクセスできます」と続けます。さらに市は「パスワードのハッキングが成功したとしても、2番目の保護層を通過しなければならない、第2の認証方法」を追加するハードウェアベースのセキュリティに取り掛かりました。

より多くの機関がSoftware-as-a-Service (SaaS) アプリケーションを採用するにつれて、ハードウェアセキュリティキーベースのMFAが特に重要になっています。

市は図書館やコミュニティセンターを含む、12の異なる場所にYubiKeyを使用したハードウェアセキュリティキーベースのMFAを導入しました。すべての部門がこのソリューションを使用してログインする必要があります。Alexander氏によると、YubiKeyは市が高いセキュリティ基準を満たすのに役立ち、さらに他のMFAソリューションと比較して費用対効果も高くなります。また、パスワードを頻繁に変更する必要がないため、職員にとってより手間の少ない操作となります。

より多くの政府機関がSoftware-as-a-Service (SaaS) アプリケーションを採用し、それらをネットワークに接続して市民にデジタルサービスを提供するようになると、ハードウェアセキュリティキーベースのMFAが特に重要になってきます。これはクラウドベースのシングルサインオンプロバイダーと組み合わせることができ、職員は仕事をするために必要なデジタルアプリケーションに合理的かつ安全にアクセスできるようになります。

「ユーザーアカウントに対する攻撃は何度か確認しましたが、成功していません」とAlexander氏は言います。「MFAを使用していない場合は、このソリューションを採用するための予算を用意する必要があります。MFAにより本当に必要な保護層が追加され、パスワードの悪用からの保護が可能になります。」

結論

今日の変化する状況において、政府は包括的なサイバーセキュリティ戦略を必要としています。これは、セキュリティ防御を強化するソフトウェアベースのソリューションのみに依存するものではありません。ハードウェアベースのセキュリティは、重要な政府システムを外部と内部の両方のセキュリティリスクから保護するために不可欠です。

政府は、サクラメント、ミッションビエホ、ワシントン州のように、ハードウェアセキュリティキーベースのMFAをセキュリティ戦略に組み込むことを検討する必要があります。それらの州や市の経験から、政府機関が物理デバイスのセキュリティに目を向けることで得られるメリットを示しています。

「二要素認証がないと、ネットワークと組織が脆弱なままになります」とミッションビエホのAlexander氏は言います。「このセキュリティ層を追加することは非常に重要です。これは、サイバーセキュリティの専門家が採用するべき多くの層のうちの1つです。これは最前線なのです。これを実施せずに、他の層から始めないでください。」

本書は、*Yubico*からの情報を使用して、*Government Technology Content Studio*によって開発および作成されました。

後注：

1. *Verizon 2020 Data Breach Investigation Report*
2. *https://www.yubico.com/products/yubikey-for-mobile/*
3. 概要「*Modernizing election security with the YubiKey*」
4. *https://cityofmissionviejo.org/services-guides/how-do-i*
5. *https://apps.apple.com/us/app/mv-life/id1173015105*

作成先：

government technology

Government Technologyは、テクノロジーを賢く利用することで、州および地方政府の問題を解決することを目的としています。Government Technologyは、州および地方の政府および教育のみに焦点を当てた、国内で唯一のメディアおよび調査会社であるe.Republicの一部門です。
www.govtech.com

作成先：

yubico

Yubicoは、企業や個人に対するアカウント乗っ取りを根絶します。YubiKey（世界一のハードウェアベースのセキュリティキー）は最も安全で、使いやすく、手頃な価格の多要素認証です。Yubicoは、最も重要な情報、アカウント、アプリケーションをセキュリティで保護することに関して、世界最大級の政府、テクノロジー企業、および金融機関からの信頼を得ています。詳細については、www.yubico.comをご覧ください。