お客様成功事例

教育

デューク大学

米国の私立大学が導入した柔軟で信頼できる多要素ソリューション

課題

デューク大学は、米国ノースカロライナ州ダーラムにある私立の研究機関で、学部生と大学院生を合わせると約 1 万 4850 名の学生が在籍しています。

メリーランド大学で発生したハッキング事件ではその侵害コストが約 3,500 万ドルに達すると見積もられるなど、いくつかの高等教育機関におけるデータ侵害が注目を集める中、デューク大学は、重要な戦略の 1 つとして、学生、教員、および職員に対して二要素認証ソリューションを提供することが必要であると判断しました。

ソリューション

デューク大学の最高情報セキュリティ責任者兼 ID 管理責任者である Richard Biever 氏は、トークンを使用するレガシーベンダーを含め、同大学が 2010 年から二要素認証ソリューションを調査していたと述べています。そして、これらのソリューションには非常に多くのオーバーヘッドと管理作業が伴うため、シームレスな認証エクスペリエンスを必要とするエンドユーザにとっては複雑すぎると感じていました。

デューク大学は、同大学のコミュニティ全体の役に立つだけでなく、IT 管理者の負担が増えることのない、さまざまな認証方式に対応した柔軟なソリューションを必要としていました。これについて、Richard 氏は次のように述べています。「教員、職員、学生にとって使いやすい多要素ソリューションが必要でした。大学のシステムには、それぞれの行動やニーズもまったく異なる 5 万 4000 人を超えるユーザがアクセスします。大学のシステムに対するユーザの認証方法を選択できるソリューションが必要だったのです」。

> **Duo は柔軟であることが実証され、さまざまなテクノロジーと連携されています」**
>
> **Richard Biever 氏**
> 最高情報セキュリティ責任者兼 ID 管理責任者

フィッシング攻撃を機にデューク大学は大規模グループに Duo を導入

デューク大学は、多要素認証テクノロジーとして Duo を選択し、そのテストとして 600 ユーザの小規模なパイロットを実施しました。しかし 2015 年に教員の給与振り込み口座を標的とするフィッシング攻撃が発生し、その取り組みを加速することになりました。このとき標的になった 600 人の教員のうち 12 人がフィッシング攻撃にだまされ、10 人の給与が攻撃者の銀行口座に送金されてしまったのです。

フィッシング攻撃は高等教育機関だけがターゲットになるわけではありませんが、大学に対するこの種の攻撃がメディアで取り上げられる機会が増加しています。また Anthem 保険のフィッシング被害では、全米の主要な大学の教員、職員、学生を含む多数の顧客がデータが漏洩しました。

デューク大学の対策

デューク大学のセキュリティチームはこのインシデントを重視し、侵害された可能性があるアカウントの検出を強化するとともに、すべての教員と職員に多要素サービスを提供することを決定しました。デューク大学の学長から教員と職員宛てに発信されたメッセージでは、職員向けセルフサービスポータルへのアクセスに多要素認証を設定しない限り、給与振り込みが完全に保証されない可能性があることを通達しました。このメッセージが送付された直後に、6,000 人の教員と職員が Duo の二要素認証ソリューションに登録しました。

主要な IT スタッフは、全員が最初に実施された 600 ユーザのパイロット プログラムのなかで多要素ソリューションに登録されていました。そのなかの 1 人は、IT チームが管理しているシステムにアクセスするための手順を増やしたくないという意見を述べていました。しかし有名なフィッシング攻撃が発生した後、その IT 管理者は Richard 氏を訪ね、それまでとは異なる考えを示しました。「彼はフィッシング攻撃の後に考えを変え、実際に『このサービスがあってよかった』と言ったのです」。

多くの IT 部門とセキュリティ部門が心配していることを、Richard 氏とそのチームは検討する必要がありました。それは、多要素ソリューションを展開するための戦略と、このようなフィッシング攻撃にだまされないようにエンドユーザを教育する方法です。前者に関しては、デューク大学では、多要素認証の必要なサービスをエンドユーザとアプリケーションオーナーが決定できるようにしました。このような多面的なアプローチを採用することで、エンドユーザは保護したいものを自分で柔軟に選択でき、学部と学科は多要素認証を必要とする特定のアプリケーションを指定できます。また機密性の高いデータを含むサービスやアプリケーションを使用する場合、エンドユーザには多要素認証が必要となります。

デューク大学のチームは、非常に積極的に教育と普及に取り組んでおり、ほぼ毎週各学部を訪ねて多要素認証を啓蒙し、それが重要である理由を説明し、サービスの登録方法と効果的な使用方法を指導しています。エンドユーザは認証プロセスがどれだけシームレスであるのかを直接体験できるため、Duo はトレーニングの簡素化に貢献しています。

これについて、Richard 氏は次のように述べています。「Duo は柔軟であることが実証され、さまざまなテクノロジーと連携されています。VMware のような主要なインフラストラクチャ テクノロジーをはじめ、Shibboleth、リモートデスクトップ、SSH、VPN サービスといったリモート アクセス テクノロジーや SSO テクノロジーなどの既存の認証インフラストラクチャに Duo を組み込むことができました。どのテクノロジーと統合できるのか、コミュニティがどのように利用できるのかという点における柔軟性が、多要素認証戦略のパートナーとして Duo を導入するうえでの重要なポイントとなりました」。

Duo のユニファイド アクセス セキュリティ (UAS) で、すべてのユーザ、デバイス、およびアプリケーションを保護できます。

信頼できるユーザ

高度な二要素認証でユーザを確認し、ユーザアクセスポリシーを適用してアプリケーションへのアクセスを制限できます。

信頼できるデバイス

Duo により、ログイン時に従業員が所有するデバイスを含むすべてのデバイスのセキュリティ正常性がチェックされます。デバイスのリスクに基づいてアクセスポリシーをカスタマイズできます。

すべてのアプリケーション

ユーザと管理者の両方をサポートする Duo のセキュアなシングルサインオン (SSO) でクラウドとオンプレミスのアプリケーションを保護し、アクセスを簡素化できます。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp