CAMPUS TECHNOLOGY

HOW TO PROTECT STUDENTS AND STAFF AGAINST PHISHING ATTACKS

The tools and methods for dramatically reducing cybersecurity problems on your campus are readily available. You just have to use them.

SPONSORED BY okta

Verizon's annual "Data Breach Investigations Report" always makes for a gripping read. Security practitioners who study the threats profiled in its pages will be better positioned to defend against them. But in the 11 years the company has been collecting and consolidating data from numerous contributors to develop its findings, one aspect hasn't changed. The two biggest threats leading to data breaches are compromised credentials, obtained through stolen or weak passwords, allowing the wrong people to pose as others.

Take this example. In March 2018 the U.S. Justice Department indicted nine Iranian hackers who, at the behest of their government, performed phishing scams on 100,000 American professors at 144 U.S.-based colleges and universities (as well as 176 schools in 21 other countries). Over the course of several years, the hackers were able to get into the email accounts of thousands of faculty members, enabling them to steal 31 terabytes of intellectual property worth an estimated $3.4 billion dollars. How were some of the most brilliant people in the world tricked? Spear phishing emails sent to the victims indicated that the sender had read an article published recently by the professor and expressed interest in several other articles. The sender would provide links to those additional articles. If the victim clicked on certain links, he or she would be directed to a malicious domain named in a way to be "confusingly similar" to the authentic domain of the recipient's institution, and it would contain a webpage designed to be a login for the victim's own university. When the victim entered the login credentials, they were seized by the hackers.

More recently, University of Buffalo officials are mopping up from a cyber break-in involving 28 faculty, 1,800 students and 862 alumni. Their login information was stolen after they visited a website and logged in using their institutional credentials. The university's advice to those users: Change your user name and password and don't use your school login information "for external services or websites."

Is it any wonder that for the third year in a row the top IT issue among Educause member institutions is information security -- or that identity and access management, single sign-on and multifactor authentication are showing up on institutional security program roadmaps everywhere?

Keeping out the wrong people will go a long way in protecting your institution's information. This report offers a straightforward process for doing that. What's required is setting up three layers of protection: confirming that users are who they say they are, figuring out what's known about them, and making sure they have access to the right applications and resources and no more.

Who You Are

Let's examine the first layer. How do you make sure users are who they say they are? Through their credentials, of course. Yet, you know the truth: Passwords by themselves no longer suffice. On the user side, people suffer from password fatigue. They have so many needs during the day to use passwords, they get truly idiosyncratic about how to manage them: through recycling, caching, writing them on sticky notes, and choosing flimsy variations every time they're asked to update them. On the criminal side, passwords can be guessed, stolen, sniffed, intercepted and brute-force cracked. They're a "notoriously weak form of authentication," as one RAND report put it, because they can be compromised at any point in the authentication process.

Many institutions have turned to single-sign-on (SSO) as an antidote to password fatigue and multi-factor authentication (MFA) as a surefire way to authenticate the user. SSO provides a streamlined route for user access to the appropriate online services or resources

Two-Factor vs. Multifactor

Two-factor authentication (2FA) most often couples something you have with something you know. You use it any time you head to the ATM machine. You supply your debit card (what you have) and your PIN (what you know). Variations on that could include something you "are," such as a typing cadence, fingerprint or retinal scan. If users are logging into an online service and don't see their personally selected security image on the login page, that's a first indicator to warn them that they may be being phished. Multifactor authentication just piles on from there. An example of MFA would be the use of the smartcard, the PIN and other elements, such as a physical token, a security code pushed to your phone or biometrics. If a user were to go to a nefarious website and enter credentials, the criminal wouldn't be able to access anything because the password on its own wouldn't be sufficient.

— no matter whether it's one application or a hundred. And MFA offers a Mission Impossible-caliber set of proofpoints that enables the user to demonstrate identity beyond a single password.

SSO has found some pickup in higher ed — about 40 percent, according to one source. This was due in large part to the introduction of Shibboleth, a project of Internet2 begun nearly two decades ago that focused on a federated approach to helping universities share resources and research across institutional boundaries. But even now fewer than 450 institutions are ID providers for the open source project. What's holding back other schools from participating? As Jim Faut, cloud enterprise architect for identity management company Okta, explains, "Shibboleth is fine and full-featured. But it's also complex to configure and an on-premise-only solution. You have to have specialized expertise to run and operate that environment."

MFA is a different matter. In contrast to fairly broad adoption of SSO, leading institutions are still getting up to speed on MFA. If it's so great, why doesn't MFA, which has been mandated for federal agency use by a Homeland Security directive, abound in higher education too? That same RAND report mentioned earlier offers a few clues. One is a lack of sector peer pressure. Healthcare, the federal government and financial services, where MFA abounds, face stringent regulation that force them to take what they have at stake more seriously, it seems, than other industries. Another is budgetary consideration. MFA is usually part of a broader security plan that may also include closer monitoring, new intrusion detection systems, closure of unneeded communications ports, pulling back on administrative privileges or access from certain locations or machines, and the improvement of physical security. Once the budget is spent in those areas, MFA may be put on the backburner until the next funding year.

What isn't an issue is user resistance, the RAND survey found. Users want MFA once they know what it is. User pushback doesn't exist. And, for the record, once MFA is in place, no organization goes back to old ways of doing authentication.

Frequently, the same organization will deploy SSO across the board to its users to facilitate stronger password practices and provide MFA to a subset of individuals who access particularly sensitive data, such as those working in financial areas, health-related units and research teams or for those who possess administrative rights on the campus network.

Joyseulay / Shutterstock.com

"Being able to do automated provisioning and deprovisioning of applications to users is a big advantage security-wise for an organization," says John Lally, education lead at Okta

What's Known about You and What You Have Access To

The second layer of protection in campus security is figuring out what's known about the user -- both the roles played and the groups he or she is part of. Those will determine who gets past the third layer: what applications and data access are allowed. Most of higher ed has implemented some kind of access management program to automate those basic activities.

The best access management applications, however, cover all of the complex stages of the user lifecycle, from first provisioning through authentication, authorization, and eventual deprovisioning.

There are several aspects to this lifecycle. One is affiliation. As a community Wiki on Internet2 lays out, that can be "formal" (possessed by staff members, researchers and students, for example) or "casual" (for people whose

institutional affiliation is "transitory" or "periodic," such as alumni, library users and external vendors). Frequently, those affiliations are stacked on top of each other; a staff member might be an alumnus; a student might be staff. And they go through transitions: A student becomes a student worker then a staff member and alumnus then a retiree. At each stage, the roles evolve and so should the access. When the HR department or the registrar or some other unit has officially declared in its system that somebody has left the college, the access management application should pick up that detail and instantly turn off access to network resources.

"Being able to do automated provisioning and deprovisioning of applications to users is a big advantage security-wise for an organization," says John Lally, education lead at Okta. At the same time, he adds, it's an optimizer for the IT organization, because it "reduces on a per-person basis the amount of time it takes to provision each one of the applications they may need to access."

Jumpstarting Your Security Response

The cover story for the April 2018 issue of IEEE's Computer Society journal examined cybersecurity vulnerability trends, a topic the authors have taken up regularly since January 2009. Among the discoveries made in an analysis of data from the U.S. National Vulnerability Database: Even though applications are becoming more "complex," well-documented implementation errors such as buffer overflow and other buffer-related faults are the major source of vulnerabilities, accounting for about two-thirds of the total. In other words, the article advises, cybersecurity vulnerabilities can be reduced simply by applying "tools and methods that are readily available."

You couldn't hope for better news. The technology solutions for SSO, MFA and lifecycle management exist. Your job is to make good choices and put them in place.

What should you look for? Here are five tips for choosing wisely.

1. Pick cloud-ready. Colleges and universities are undergoing a great upheaval in IT. Where software-as-a-service solutions are available, they're more likely to seriously consider them over on-premise programs for all the benefits inherent in cloud adoption. But nobody moves instantly. Look for an SSO system, such as Okta's, that lets users access on-premise and cloud applications to avoid the problem of dueling login portals.

2. Consider your user base... As you're rolling out MFA, you need to match your users with the solution, says Faut. That includes "rolling out the factor," whether that is physical tokens,

Training Your Students

Increasingly, colleges and universities are working with industry partners to give students a taste of real-world problem solving through hackathons. Frequently, these all-nighters are focused on creating apps for use by the campus community itself. Other times, it's purely intended to inspire innovative thinking. As an example, Amazon and Okta recently sponsored a 24-hour hackathon at the UCLA Career Center that invited participants to create applications that would tie into Alexa. Participating teams used Okta to secure their creations with authentication, authorization and user management.

Teams were judged based on the quality of their ideas, their implementation and best potential for impact. Top winners received cash prizes and major bragging rights. Recalls Jim Faut, who attended as a solution architect to help participants with their security implementations, "We had some very compelling ideas that came out of that. The students seemed to pick up the technology quickly and readily to build those into their apps."

Access Management in Action

When California's San Jose State University IT leaders wanted to simplify how users log into web services, they searched for a single sign-on solution that could "support a lot of different applications, be transparent to users and integrate with SJSU's existing system of record for identity management." IT was also hoping to reduce help desk calls and give support staff visibility into where users were at in their authentication process when problems cropped up. Plus, the university hoped to choose a "large player" in the identity realm so they could count on a steady supply of enhancements and new features.

The school chose a combination of Okta's Single Sign-on and Universal Directory. After a set of modest tests, the university took a giant step by integrating Okta with its existing SSO, Shibboleth. As Joel Johnson, IT director for web and campus applications, explains, "We let applications think they're authenticating with Shibboleth, but it just does an authentication relay to Okta. Okta then tells Shibboleth it's OK to grant access." Now he advises other institutions to be more "aggressive" with their move to SSO. "It's easy to move, easy to configure, and you'll get to the end state of single sign-on pretty quickly."

email or the use of push codes on a smartphone. That phase requires having a good understanding of what kind of technology your users have access to and then communicating with them as they're getting up to speed with the use of MFA. "Finding the right match there will make the experience as good as possible," he suggests.

3...Then prioritize what's most important to them. As you're planning your provisioning of better security mechanisms, look at applications and use, advises Faut. Go after the programs everybody on campus is dependent on and then "trickle down to the ones less used." In parallel with working on broadly used applications, consider the important ones, such as finance and the student information system, "to make sure the right administrative people are getting access to those immediately."

4. Simplify working with existing infrastructure and adding new applications. Legacy technology running SAML, Open ID Connect or WS-Fed can't be ignored. Likewise, each time somebody introduces a new application on campus, it needs to be incorporated into the SSO and MFA fold. Choose a provider that knows how to do integrations with the software you're using. As an example, Okta's Integration Network includes 5,500 pre-built integrations or "connectors" that work with both cloud and on-premise programs, including the most popular ones for higher ed: Office 365, G Suite, Box, AWS, Blackboard, Canvas, Ellucian and others.

5. Remember your in-house application development. Universities creating their own mobile apps, for example, should be able to use SDKs to build in identity and access control. As Lally notes, "baking access management into apps" through the use of APIs means the developers "don't have to be concerned with it. They can focus on the user experience." Okta, for example, maintains a website where developers can subscribe to a free instance of the Okta identity platform "that will allow them to get their application up and running very easily."

It's time to modernize your approach to authentication, authorization and user management for the services and apps you rely on. If you've lived with the same cobbled-together security tools for years, maybe it's time to figure out how you'll maintain them in an era of cloud and mobility. The "tools and methods" you need to accomplish that are readily available.

Access Management in Action

South Australia-based Flinders University sought a more efficient way to manage the identities of its 26,000 students and 2,500 staff members not just for the sake of addressing budget pressures but also to give them the "best possible user experience," according to Aaron Finnis, associate director of information security and governance. The university wanted to reduce the number of password recovery requests, gain easy integration with existing systems and new cloud services, onboard and offboard large numbers of users and improve security monitoring practices.

Okta was the university's choice. After a whip-fast implementation (launch came 22 days after the start of the project), users have a single login for accessing all of their many applications and resetting passwords on their own. To bolster the security profile for a specific group of users, the university is also rolling out Okta's Adaptive MFA. And with Lifecycle Management, Flinders is streamlining the provisioning and deprovisioning of access to apps as the user's role within the institution changes. Says Finnis, "Okta has helped us create an identity cycle that is both simple and seamless."

Okta Products

In the latest version of Gartner's "Magic Quadrant for Access Management, Worldwide," Okta was named a "Leader"(for the second year running). Among the handful of other companies included in that quadrant, Okta placed highest in "ability to execute." Here are the solutions that draw institutional and enterprise customers to Okta:

Adaptive MFA: A cloud-based program for implementing different kinds of authentication factors, including security questions, passwords, SMS or voice, verified push, physical tokens and biometrics.

Lifecycle Management: A cloud-based technology for providing automated provisioning and deprovisioning of users throughout their relationship with the institution.

Single Sign-On: A cloud-based tool for allowing end users to access all of their applications on the network and online, with real-time security reporting and two-factor authentication.

Universal Directory: A cloud-based directory for storing and managing user identities, devices and passwords and setting up and enforcing identity access management policies; UD works with its own data and data maintained in Active Directory and LDAP, among other directory services.

For more information, please visit www.okta.com/education.
Or contact us at info@okta.com | 1-888-722-7871

okta