UNIVERSITY OF CALIFORNIA, DAVIS
AUDIT AND MANAGEMENT ADVISORY SERVICES

UC Davis Health
Multifactor Authentication
Audit & Management Advisory Services Project #24-07

February 2024

Fieldwork Performed by:
Yarazel Mejorado, Senior IT Auditor

Reviewed by:
Sarah Flower, IT Audit Manager

Approved by:
Ryan Dickson, Director

Multifactor Authentication
AMAS Project #24-07

MANAGEMENT SUMMARY

Background

As part of the fiscal year (FY) 2024 audit plan, Audit and Management Advisory Services (AMAS) performed an audit of multifactor authentication at UC Davis Health.

UC Davis Health adopted the use of Duo multifactor authentication services in 2018. In addition to a username and password, multifactor authentication provides a second layer of security by sending an additional approval request to a user's device (usually in the form of a push notification to a mobile phone) after the user enters their login credentials. Users may also opt for a phone call or text instead of receiving a push notification, and some users opt for tokens (a small piece of hardware that generates authentication codes) rather than using their mobile phone for multifactor authentication. This makes it more difficult for attackers to gain access to an account if they are only in possession of the user's credentials, but not the user's secondary authentication device.

Industry best practices have come to regard multifactor authentication as a compulsory element of a robust cybersecurity program. For example, NIST special publication 800-63B includes multifactor authentication as part of its digital identity guidelines. The UCOP systemwide IT policy "UC Account and Authentication Management Standard" states that accounts used to access Institutional Information or IT Resources classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 or higher must use multifactor authentication. The UC Davis Health policy "UCDH Account Type and Authentication Policy" further specifies that multifactor authentication must be used for all hosted and cloud applications, as well as for internally hosted applications that contain PHI, PII, or FERPA information and when accessed outside of the UC Davis Health internal network.

As of this report, there is an overall Duo adoption rate of nearly 100% for individual users. This statistic includes staff, faculty, students, and external users. We also noted that there is currently a Duo hardening project being performed to address potential security vulnerabilities raised during discussions with the Duo vendor as well as other UC health systems.

Purpose and Scope

The purpose of this audit was to evaluate the effectiveness of the implementation of multifactor authentication at UC Davis Health. Utilization of Duo at UC Davis campus was not included in the scope of this review. To accomplish these objectives, we interviewed relevant management and staff; reviewed relevant policies, procedures, Duo vendor documentation, and regulatory guidelines; reviewed Duo enrollment data and reporting; and assessed budgetary documentation.

The timeframe under review was January 2023 to November 2023.

Conclusion

We found that for individual users, there is a 99.9% adoption rate of Duo for UC Davis Health applications and a 99.5% adoption rate of Duo for Office365. Duo enrollment is mandatory, and frequent evaluation and user education campaigns by the Innovation Technology unit have led to improvements in usability.

We also found that approximately 40% of accounts classified as “departmental” do not have Duo multifactor authentication enabled, and applications that do not use Duo multifactor authentication are not in compliance with the UC Davis Health “Account Type and Authentication Policy” and the UC Davis Health “Cyber Safety Exception Policy”.

Observations, Recommendations, and Management Corrective Actions

A. Departmental Accounts

Many “departmental” accounts do not have Duo multifactor authentication enabled.

UCOP systemwide IT policy “UC Account and Authentication Management Standard” states that accounts used to access Institutional Information or IT Resources classified at Protection Level 3 or higher and IT Resources classified at Availability Level 3 or higher must use multifactor authentication. UC Davis Health “Account Type and Authentication Policy” also requires that multifactor authentication be used to protect logins for all hosted and cloud applications, as well as for internally hosted applications that contain PHI, PII, or FERPA information when accessed outside of the UC Davis Health internal network.

Multifactor authentication assumes that an account is accessible by a single user, and therefore a push notification can be authorized through a device under the control of that single user. “Departmental” accounts however may be accessed by multiple users because they serve a collaborative purpose such as for a shared inbox or calendar. There are 72 departmental accounts (40%) that do not have Duo enabled for Health applications and 73 departmental accounts (40.6%) that do not have Duo enabled for Office 365.

Through conversations with staff, we were able to verify that some of the accounts that do not have Duo enabled can be used to access data likely classified at Protection Level 3 or higher. Without multifactor authentication, attackers can gain access much more easily. This risk is compounded when accounts are shared amongst multiple people, where passwords are less likely to be rotated or stored securely.

Recommendation

Innovation Technology should review all departmental accounts to determine whether they are used by more than one person or can be used to access data classified at Protection Level 3 or higher. These accounts should be brought into compliance with the UC Davis Health “Account Type and Authentication Policy” and “Cyber Safety Exception Policy” where necessary.

Management Corrective Action

1) By September 1, 2024, Innovation Technology will review all departmental accounts and confirm that they comply with the UC Davis Health “Account Type and Authentication Policy” and “Cyber Safety Exception Policy” where necessary.

   Owner: Innovation Technology

B. Applications Excluded from Duo Multifactor Authentication

The applications not using Duo multifactor authentication do not comply with the UC Davis Health policies requiring multifactor authentication, exception documentation, and exception review.

The UC Davis Health "Account Type and Authentication Policy" requires that multifactor authentication be used for all hosted and cloud applications, as well as for internally hosted applications that contain PHI, PII, or FERPA information. Any exceptions to this policy must be submitted, reviewed, and approved at multiple levels of the organization per UC Davis Health's "Cyber Safety Exception Policy". However, there are applications in production that do not comply with either the multifactor authentication requirement in the Account Type and Authentication Policy or with the Cyber Safety Exception Policy. For example, ServiceNow[1] was set to bypass Duo and did not have an exception documented in accordance with the Cyber Safety Exception Policy. [2]

There are at least 80 applications enabled with Active Directory Federation Services (AD FS) in use at UC Davis Health that do not comply with the UC Davis Health Account Type and Authentication Policy because they do not use multifactor authentication. Where exceptions may be necessary, no exception rationale or compensating controls have been properly documented and no review process exists to determine whether the rationale is still relevant and necessary, as required by the Cyber Safety Exception Policy. Allowing applications in production without implementing multifactor authentication leaves the applications more vulnerable to malicious attacks.

Recommendations

Innovation Technology should implement multifactor authentication on all AD FS-enabled applications covered by the UC Davis Health Account Type and Authentication Policy. Any exceptions to this policy should be submitted, reviewed, and approved per UC Davis Health's Cyber Safety Exception Policy. A process to regularly review exceptions to the multifactor authentication requirement in the UC Davis Health Account Type and Authentication Policy should also be implemented.

Management Corrective Actions

1) By May 1, 2024, Innovation Technology will identify all AD FS-enabled applications that do not use multifactor authentication as required by the UC Davis Health Account Type and Authentication Policy.

   Owner: Innovation Technology

2) By September 1, 2024, Innovation Technology will implement multifactor authentication on all AD FS-enabled applications covered by the UC Davis

[1] ServiceNow is the enterprise cloud application used to automate and streamline IT and business unit operations at UC Davis Health. Management reports that multifactor authentication was activated for this application in November 2023.

[2] The UCDH Cyber Safety Exception Policy governs the Information Security policy exception process and details the requirements for submitting requests for exceptions to the policy.

Health Account Type and Authentication Policy, and where exceptions are necessary, complete the Cyber Safety Exception Policy process.

Owner: Innovation Technology

3) By September 1, 2024, Innovation Technology will establish a process to consistently document and review AD FS-enabled applications’ compliance with the multifactor authentication requirement in the UC Davis Health Account Type and Authentication Policy.

   Owner: Innovation Technology