Information Security Workgroup
Jan 6, 2021
Zoom Session

Present:	Troy Weipert, A&F	Lynne Harrington, AA & EMIS
	Kelly Sebastian, Office of the President	Robert Crockett, CENG
	Kristy Cutter, OCOB	Joe Emenaker, OCOB
	Bill Hendricks, CAFES	Jarrod Plevel, CAFES
	Arthur Heubner, CSM	James Mwangi, CAED
	Josh Machamer, CLA	David S. Bains, CPC
	Craig Nelson, UD	Trish Brock, R-EDGE
	Joan Pedersen	Doug Lomsdalen, ITS
	Sarah Jones, ITS	Kyle Gustafson, ITS
	Jon Vazquez, ITS	Gary McCrillis, ITS
Absent:	Rick Salomon, Student Affairs	Derek Gragson, CSM

I. Enabling Multi-factor Authentication (MFA) Campus-Wide

We enabled MFA, on web-based applications, on December 9, 2020. We currently have 38.9K users enrolled in Duo. It was a big project and turned out very successful due in part to everyone's help in getting users enrolled in Duo and keeping them update on the project's progress.

a. Up Next:
   i. Enable Bring Your Own Token (targeting February 2021)
   ii. Emeritus (TBD)
   iii. Department Accounts (TBD)

b. Helpful guides for "remember me"
   i. Remember Me: https://calpoly.atlassian.net/wiki/spaces/CPKB/pages/708215005/Enable+Remember+Me+for+a+Duo+Device.
   ii. More info about Macs and iOS:
      1. https://calpoly.atlassian.net/wiki/spaces/CPKB/pages/797966477/Can+t+Enable+Remember+Me+in+Duo
      2. https://calpoly.atlassian.net/wiki/spaces/CPKB/pages/893091876/Can+t+Access+Duo+on+My+iPhone+or+Mac

II. CSU CO InfoSec Audit Update

The information security audit is still ongoing; the CSU is reviewing all of the data they collected during the "field-work" phase. We received feedback from the national guard unit tasked to scan our network, systems and websites; we will create a project to remediate the issues they identified.

III. Qualys Vulnerability Management

Qualys is an application that checks servers, computers and other devices for vulnerabilities and identifies patches needed. The audit significantly disrupted our plans to provide training to Division and College IT reps. We understand centralization will impact how we rollout the training and will take this into account.

IV. CSU Incident

A CSU university suffered a disruptive breach, significantly disrupting operations by impacting their Domain Controllers/Active Directory. The end game of the malicious actors was to obtain sensitive data to hold for ransom.

The CSU Chancellor's Office has directed each campus to assess and enhance five primary areas. The ITS Information Security Office is reaching out to areas for assistance with Active Directory assessments. The broad focus areas are:

a. Active Directory
b. Securing Network and Remote Access
c. Domain Controller and System Hardening
d. System Logging and Monitoring Tools
e. User Account Security

V. Security Tidbits – Upcoming Projects

a. Information Security Audit Remediation
   The CSU CO auditors have provided periodic check-ins with the security team. So far, there haven't been too many surprises. We'll work together to address some of the findings. Since our meeting, January 22nd has been set as our out-brief with the audit team. We will provide a recap at our April meeting.

b. Email Security
   MFA is configured to protect our web-based applications; unfortunately, there are a handful of legacy email protocols that allow unauthenticated access. Microsoft has scheduled the retiring of these protocols the second half of 2021, we'll be tracking this and ensuring users are notified of the changes.

c. Segment Tech Park Network
   For years, the tenants of the Tech Park have been on the Cal Poly network; this project with segment them in their own area of the network and they will not be able to affect any of our Cal Poly network resources.

d. WAF Reverse Proxy
   Our WAF project was stalled this past quarter due to the Security Audit. Our office plans to resume migrating organizations who want to put their web presence behind our WAF. In 2020, the WAF stopped 4 million attacks against our Drupal environment.

VI. Action Items

ISO: Provide guidance on how the role of an ISC will change with regards to centralization.

ISCs: Contact Kyle G if interested in being an early adopter of our WAF Reverse Proxy.

VII. Next Meeting

a. April 8, 2021, 1:10 pm – 2:00 pm, via Zoom