CAL POLY

IT Services

tech.calpoly.edu

Information Security Workgroup
Oct 7, 2020
Zoom Session

Present:

Doug Lomsdalen, ITS
Troy Weipert, A&F
Robert Crockett, CENG
Richard Cavaletto, CAFES
Bill Hendricks, CAFES
Debra Valencia-Laver, CLA
Craig Nelson, UD
Rick Salomon, Student Affairs
Trish Brock, ORED
Kyle Gustafson, ITS
Jon Vazquez, ITS
Craig Schultz, ITS

Lynne Harrington, Academic Affairs
Arthur Heubner, CSM
Joe Emenaker, OCOB
Jarrod Plevel, CAFES
James Mwangi, CAED
Jarrod Plevel, CAFES
Kelly Sebastian, Office of the President
David S. Bains, CPC
Brian Gautry, CPC
Sarah Jones, ITS
Gary McCrillis, ITS

Absent:

Kristy Cutter, OCOB
Jeff Nadel, CENG

Derek Gragson, CSM

I. **2020 Annual Risk Self-Assessment (ARSA) Overview**

We closed the ARSA process on June 26th, since then the Information Security team has been reviewing the data collected and comparing it with the source

a. Provided an overview of ARSA 2020 Findings, to include a discussion several discrepancies we identified.
b. There was positive growth in use of Enterprise Security Tools, we will work with each group to shrink the gap.

II. **Enabling Multi-factor Authentication (MFA) Campus-Wide**

Update: Cal Poly is enabling MFA campus-wide at the person level. When individuals log in via SSO, starting December 9th, it will be mandated. We're adding this extra layer of security to protect critical Cal Poly data and resources.

a. Person types impacted:
   i. Faculty / Staff / Students (admitted, current, recent) / Affiliates
   ii. Out of Scope: Department accounts and Emeritus
b. Timeline:
   i. October 25th: Enabling MFA for all individuals who have a device enrolled
   ii. December 9th (change): MFA will be mandatory
c. Full communication blitz: ITS is working Cal Poly Human Resources, Academic Personnel, Student Affairs and other communication vectors to spread the word.

III. Qualys Vulnerability Management

This summer our Information Security Office Intern tackled revamping the Vulnerability Management platform Qualys. Qualys checks servers, computers and other devices for vulnerabilities and identifies patches needed to remediate. We're moving to Qualys cloud agents to improve visibility.

a. Worked with CITC to get the cloud agents deployed and developed a dynamic tagging hierarchy.
b. Seeking each college/division actively use Qualys by maintaining the inventory and remediate vulnerable hosts.

IV. KeyServer

We continue to improve KeysServer data.

a. Added Apple "purchase date" and "warranty expiration" to data views.
b. Added "college/division" and "location type" to asset views
c. Improved report generation speeds.
d. We appreciate everyone's help getting the KeyServer agents deployed.

V. Security Tidbits

a. Information Security Audit 2020
   i. Cal Poly ITS has been notified the CSU Chancellor's Office Audit team will be conducting an Information Security audit.
   ii. Timeline to be determined; preliminary meet and greet is October 12th.
   iii. We will be asked to meet with a variety of decentralized IT teams.

b. Remote Work Environment
   i. Best practice is to have Faculty and Staff using state-owned devices from home to log into the VPN on a regular bases to ensure devices are getting required security patches.
   ii. We have handful of devices that are in need of patching.
   iii. Faculty and Staff Guide for Remote Work knowledge base article.

c. Splunk
   i. The Information Security Office had a Splunk Enterprise Security assessment, provided details on how we can optimize our data and shared best practices.
   ii. We've started windows server logs, thank you to A&F for their assistance in getting their logs forwarded to our Splunk instance.
   iii. We're working on views that would be useful to IT personnel on campus, more to come (e.g., alerts, performance monitoring).

d. WAF Reverse Proxy
   i. WAF: Web Application Firewall. The WAF inspects web traffic to campus web servers/applications and blocks malicious traffic.
   ii. This will allow us to provide website security without installing a Signal Sciences WAF agent (which are costly)
   iii. We're looking for early adopters in November.

VI. Action Items

ISCs: Please assign the role of Qualys Vulnerability Management “rep” to review respective reports regularly and remediate alerts.

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

VII. Next Meeting

a. January 6, 2020, 1:10 pm – 2:00 pm, Bldg 02 / Room 024 or via Zoom