CAL POLY
Information Technology Services

Information Security Workgroup

Meeting Notes

July 2, 2019
Education, Building 02, Room 024 at 2:00 – 3:00pm

Present:	Doug Lomsdalen, ITS	Jon Vazquez, ITS
	Alison Robinson, ITS	Kathryn Hammer, ITS
	Arthur Huebner, CSM	Kristy Cutter, OCOB
	Craig Nelson, UD	Kyle Gustafson, ITS
	Dave Mason, AA	Rick Salomon, SA
	Debra Valencia-Laver, CLA	Troy Weipert, A&F
	Derek Gragson, COSM	Joe Emenaker, OCOB
	Eumi Sprague, CPC	
	Jarrod Plevel, CAFES	

I. Annual Risk Self-Assessment

Doug L. shared that the Annual Risk Self-Assessment (ARSA) was promptly kicked off following last quarter's ISC meeting. We made a couple of big changes in how data was collected (e.g., ARSA Questionnaire via a survey in Eramba and the Workstation Survey through SurveyGizmo). Overall, I'm very happy with the process (all questionnaires but a couple & 40% response rate to workstation survey). As with anything new, we will review lessons learned from this year's process and be happy to accept any feedback you may have for us.

Our goal is to have reports available before 2019 Fall Quarter kicks off.

II. OS/Security End-of-Life Updates

We continue to monitor progress being made on reducing the number of operating systems being updated across the campus. We currently have less than 195 days before Win7/Server 2008/R2 and SQL2008 reach end-of-life.

ITS prepared a summary of locations (by college / division) where the older operating systems (Microsoft/Apple) are being used. We used this opportunity to highlight a couple of other items:

- Major browser support for TLS 1.0 and 1.1 ends January 2020; upgrading the cipher suite is relatively easy but has a big impact on end-users (communication during this change will be paramount).
- Redhat/CentOS 6.X will reach end-of-life on November 20, 2020

III. Security Logging Project

ITS has been logging data for ages, but the data is stored in disparate locations. This project will centralize all logging sources into a single Logging Account in AWS. The project starts next week, July

8th. The ISO team along with key log owners within ITS Operations will work together to identify the data and programmatically ship it to the cloud.

Centralization of our logging source data will benefit campus by facilitating better/pro-active monitoring for malicious activity. Alerting will be set up so as to better position us to take timely action.

IV. End-Point Protection - Sophos

Since June 1st, Sophos Endpoint Protection software has been available for colleges and divisions to download / install. The recommendation, due to the level of hand-on required for Macs, is to wait for JAMF rollout by ITS. Over 1200 devices on campus have been upgraded to Sophos; we still have about 5000 to go by the end of September.

Kyle is hosting CITC training in Bldg 2 / Rm 24: July 18 @ 10am and July 19 @ 10am

Personal home use version of Sophos is available for download, visit the ITS website for details on how to redeem "My Free Sophos Home License." An individual can protect up to 10 devices in their home. If users experience issues with the Home Use product, please reach out to InfoSec@calpoly.edu.

V. Office 365 Email - Security

Since our last meeting, ITS migrated email from on-premise Cisco IronPort device to 100% utilization of Microsoft O365 and their Advanced Threat Protection layer of defense.

As expected, we've seen an uptick in spam and phishing emails as the system re-learns and we work to bolster the rules that filter mail. We continue to see Phishing, Whaling and Job Offer/Scam emails.

ITS rolled out a Junk/Phishing Reporting button; when used by our customer base, this provides useful feedback to O365 and the Information Security Office the necessary header information to facilitate blocking malicious users and URLs.

Users can follow instructions at this ITS Knowledge Base article to find the button in their respective email client: Report Phishing and Spam

VI. Bluekeep Response

Approximately a month ago, the vulnerability Bluekeep was made public. Bluekeep exploits a vulnerability with Remote Desktop in Windows 7, Windows 2008/R2 and older operating systems.

Overall the response has been good in regard to patching impacted devices. Jon Vazquez will follow up with individuals over the course of the month. At the end of the month, July 31, the unpatched devices will be blocked from accessing the network until they get patched.