CoALS Technology Security Committee
June 16th, 2021
1:00 p.m.

Attendance:

Members			
Kerry Pickens - Chair (Manager Policy & Compliance)	X Tim Ramsey X (Associate Director of IT)	_ name (Title)	Keith Wicker (Information Security Officer)
Gene Curtiss (Manager Systems & Infrastructure)	Barry Stratta (Manager Software & Applications)	Sushant Patil (Security Analyst – Security & Risk)	Michael R. Foggitt (System Administrator II)
_ name (Title)	_ name (Title)	_ name (Title)	_ name (Title)

Also in Attendance:

Minutes

Item 1: **Approval of Minutes**
Description: Review and approval of minutes from 5-19-2021 meeting.

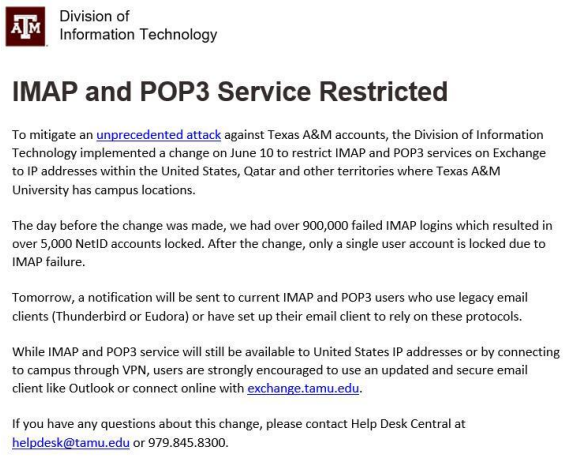
Item 2: **Governance Committee Reports (5 mins)**
Description: Note relevant information from available reports as applicable

A. TAMU ITEC – N/A
B. AgriLife Computer Advisory Team – N/A
C. CoALS Council of Department Heads – N/A
D. Ag riLife Technology Leadership Council
E. AIT Enterprise Technology Committee (ETC)
F. AIT Technology Security Committee (ETC)

- Business and Technology conference in Austin called InnoTech now open to public. Have great speakers in regard to security
  - https://www.innotechaustin.com/

G. AIT Technology Compliance Committee (TCC)

Item 3: **Lessons Learned (10 mins)**
Description: As applicable from recent activities

- Vulnerability Scans-
  - Multiple issues all related to software updates (Linux OS and PHP versions) for the same host (turns out machine can be decommissioned)
  - Multiple vulnerabilities linked to outdated Apache versions on remote servers
- TAMU Division of IT has mitigated increased password-spraying attempts on accounts by restricting IMAP and POP3 services on Exchange to IP addresses within the US, Qatar and other campus locations.
  - Around 900,000 failed IMAP log ins led to 5,000 accounts locked
  - For more information see: https://threatpost.com/imap-attacks-compromise-accounts/142824/
  - 
Division of
Information Technology

IMAP and POP3 Service Restricted

To mitigate an unprecedented attack against Texas A&M accounts, the Division of Information Technology implemented a change on June 10 to restrict IMAP and POP3 services on Exchange to IP addresses within the United States, Qatar and other territories where Texas A&M University has campus locations.

The day before the change was made, we had over 900,000 failed IMAP logins which resulted in over 5,000 NetID accounts locked. After the change, only a single user account is locked due to IMAP failure.

Tomorrow, a notification will be sent to current IMAP and POP3 users who use legacy email clients (Thunderbird or Eudora) or have set up their email client to rely on these protocols.

While IMAP and POP3 service will still be available to United States IP addresses or by connecting to campus through VPN, users are strongly encouraged to use an updated and secure email client like Outlook or connect online with exchange.tamu.edu.

If you have any questions about this change, please contact Help Desk Central at helpdesk@tamu.edu or 979.845.8300.

Item 4: **New Business / Special Topics (15 mins)**
Presenter: Kerry Pickens
Description: Annual Risk Assessment

- Phase I RAIL inventory completed
- Phase II assessment
  - IT Professionals RSAM assessments due July 30 in RSAM tool – Should get emails from TAMU IT requesting that you do your RSAM assessments assigned to you, can schedule a meeting with Kerry/Sushant to help answer questions
  - Non IT Professionals assessments are from August 16th to Sept 30. Bailey Teter is sending out an email campaign to increase compliance. Needs updated list of emails to contact.

Description: Policy review by IRPSC will impact updates to AgriLife IT Policy

- Business Contingency by changing terminology "mission critical" to "moderate or high impact" to match terminology in TAC 202.
- Changes to policy implementation steps for Contingency Plan Testing, Information System Backup, Incident Monitoring, Risk Assessment

Kerry to present to Agrilifle Compliance Committee Meeting on June 29.
Federal Conflicts of Interest and Foreign Components – big issue for Researchers and will talk about Research Computing group
https://grants.nih.gov/grants/guide/notice-files/NOT-OD-19-114.html

Item 5: **Action Item Summary**
Description: List of action items, assignee, objective, due date.

A. Business Continuity Plan and DR Plan to include policy revisions
B. Meetings with DH to review security programs – ENTO and HORT
C. Presentation to AgriLife Compliance Committee

Item 6: **Close**
Description: Adjourn meeting on time noting actions and conclusions of meeting.
Next meeting: 3rd Wednesday of May at 1 p.m.