2019-2020 Information Technology Committee

AGENDA

Meeting Date: Monday, March 16, 2020

Meeting Time: 2:00 – 3:00 pm.

Meeting Location: Zoom Meeting

- **Call to Order**
- **Roll Call**
- **Approval of Minutes of** *February 17, 2020* and *March 2, 2020*.
- **Announcements and Recognition of Guests**
  - Invited Chris Vakhordjian from Information Security Office. Between this meeting and last, Chris provided some additional information on the planned phase-out of IMAP and POP
    - See the attached pdf: ISO Response on IMAP, POP and E-mail forwarding.pdf
    - Additionally, he emailed the information below:

      FBI Warns of BEC Attacks Abusing Microsoft Office 365, Google G Suite

      BleepingComputer, 6 Mar 2020: The FBI warned private industry partners of threat actors abusing Microsoft Office 365 and Google G Suite as part of Business Email Compromise (BEC) attacks. "The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds," the FBI said in a Private Industry Notification (PIN) from March 3. "Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling over $2.1 billion in actual losses from BEC scams targeting Microsoft Office 365 and Google G Suite." The cybercriminals move to cloud-based email services matches organizations' migration to the same services from on-premises email systems. Targets are redirected to the phishing kits used as part of these BEC attacks via large scale phishing campaigns, with the phishing kits being email service-aware and capable of detecting the "service associated with each set of compromised credentials." "Upon compromising victim email accounts, cybercriminals analyze the content to look for evidence of financial transactions," the FBI explains. The scammers will then impersonate employees of the now-compromised organizations or their business partners, attempting to redirect payments between them to bank accounts under the attackers'

control. The FBI issued a number of defense recommendations IT admins can implement on their networks to prevent BEC attacks:
• Prohibit automatic forwarding of email to external addresses.
• Add an email banner to messages coming from outside your organization.
• Prohibit legacy email protocols such as POP, IMAP, and SMTP that can be used to circumvent multi-factor authentication.
• Ensure mailbox logon and settings changes are logged and retained for at least 90 days.
• Enable alerts for suspicious activity such as foreign logins.
• Enable security features that block malicious email such as anti-phishing and anti-spoofing policies.
• Configure Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent spoofing and to validate email.
• Disable legacy account authentication.
End users can also take these measures to defend against BEC scammers:
• Enable multi-factor authentication for all email accounts.
• Verify all payment changes and transactions in-person or via a known telephone number.
• Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

The FBI recommends BEC scam victims to file a complaint regardless of the amount they lost at BEC.IC3.gov.

- Regarding the March 2 discussion of retiree information for Knights Email account creation and use, JP forwarded a link to a succinct knowledge article put together by UCF IT. It covers some of the more common questions related to retiree email. He indicated that all feedback is welcome, and that in addition to the link below, the article is easily accessible by searching "retiree" or "retired" at it.ucf.edu in the "Search the Knowledge Base" box. Link: https://ucf.service-now.com/ucfit?id=kb_article&sys_id=8ec66d481b2b8c505cd6b912cd4bcbc1

- **Old Business**
  - Continue discussion of issues regarding support for desktop Linux other than email (documented and published access solutions to all campus services, like printing, wireless, wired, and email; user support for desktop Linux).
  - Support for research computing (cloud CPU services, cloud document services, continuity of research computing over funding gaps, STOKES financial model, research group system support).
  - Mission of the Committee and how we can function more efficiently (items carried over from last academic year)

        - Description of the committee is available on Faculty Senate page: http://facultysenate.ucf.edu/committees/IT_committee.asp

- **New Business**
    - Discuss Draft Resolution 2019-2020-X Linux Access to IT Services

- **Other Business**
    - Upcoming meetings:
        - Mar. 19 Faculty Senate
        - Mar. 30 IT committee meeting
        - Apr. 2 Steering committee meeting (Last of this academic year)
        - Apr. 13 IT committee meeting
        - Apr. 16 Faculty Senate (First of next academic year)
        - Apr. 27 IT committee meeting (Last of this academic year)

- **Adjournment**

UCF Faculty Senate
Information Technology Committee

Minutes of **February 17, 2020**
Business Administration I, room 230A

Melanie Guldi, chair, called the meeting to order at 2:06 pm. The roll was called orally.

In Attendance: Thad Anderson, Anya Andrews, Dawn Eckhoff, James Gallo, Sandra Galura, Steffen Guenzel, Melanie Guldi (Senate Liaison), Joseph Harrington (Steering Liason), Athena Hoeppner, Pieter Kik, Viatchelslav Kokoouline, Heath Martin, Matthew Nobles, Michael Sink (ex officio).

Minutes: Motions and second made to approve the minutes of the February 3, 2020 meeting. The minutes, with one spelling correction, were approved.

Chair Announcements:

- The chair announced some information provided by JP Peters regarding IMAP, and POP protocols and a link that goes into each protocol and Microsoft's timeline for deprecating it (https://techcommunity.microsoft.com/t5/exchange-team-blog/improving-security-together/ba-p/805892
- The chair introduced invited guest Chris Vakhordjian from Information Security Office.

Old Business

- Next, we tabled our discussion of the Mission of the IT committee, which we would like to discuss next time.

New Business

- We discussed Data Security, Cloud Storage, and Data Classification Policy (new but continued topic from 9/30 meeting) https://policies.ucf.edu/documents/4-008.pdf
    - Chris Vakhordjian provided a brief overview including emphasizing that the key issues are: compliance requirements, and that security issues are complex, complicated, and present many challenges. He also indicated that there is ongoing work regarding a data matrix to help users better understand how each type of data is classified and that policy 4-008 is being updated (see policy link referenced above). One issue that they are including in their discussions of the policy update is federal Controlled Unclassified Information (CUI) categories (see https://www.archives.gov/cui/registry/category-list). Matt Nobles suggested there is a difference between "Disallowed" versus "Unsupported" and this should be better understood. He also raised the point that the researcher is in charge of the integrity of the data. There was some discussion as to whether this is an individual (researcher) responsibility or an institutional responsibility. Next, there was some discussion about what kind of Personally Identifiable Information (PII) can be shared on the cloud.
    - Joseph Harrington asked why UCF is not actively considering Google Drive. Michael Sink indicated that other institutions are moving toward Onedrive and Office365 (USF). Athena Hoeppner informed the committee that the state (Florida's) library consortia uses Google Drive extensively. Michael Sink asked how many cloud storage vendors is "enough"? Committee voiced that one is probably too few, but acknowledged Chris Vakhordjian's point that adding additional cloud storage vendors increases the resources

necessary to provide adequate data security. One issue raised by multiple members of the committee is that Onedrive is difficult to use in several ways and that collaborators not at UCF are not able to access Onedrive as easily as they can access other services like Google Drive or Dropbox, where only an email is required. Chris Vakhordjian indicated that it is easy and that one can share a folder via email. He asked what kind of issues we have. Dawn Eckhoff indicated that earlier this academic year the College of Nursing had transitioned over to Onedrive and it has worked out really well. She also indicated that they collaborate with other institutions (that use Onedrive) and this has not presented issues, even with the use of the Teams feature in Onedrive. Athena indicated that it is hard to set up multiple access of multiple folders especially in the case when who is on which team varies frequently.

- Chris Vakhordjian suggested it might be a good idea to have an overview of how to do things using Onedrive as some of the issues raised seem to be addressable within this cloud service.
- We discussed resource requirements in more detail. Melanie Guldi asked what fraction of faculty are actively using Onedrive and asked if Michael Sink or Chirs Vakhordjian would know how to determine this. Joseph Harrington asked how many Full Time Equivalent faculty are needed to support Ondrive. He also indicated that Google doesn't offer or require user support and that users generally find answers in online forums.
- The conversation shifted to **Linux**- Chris Vakhordjian indicated that there is a Onedrive client that can be used on a Linux system.

Other Business

- None

ADJOURNMENT

The meeting adjourned at 2:59 pm.

UCF Faculty Senate
Information Technology Committee

Minutes of **March 2, 2020**
Business Administration I, room 230A

Melanie Guldi, chair, called the meeting to order at 2:05 pm. The roll was called orally.

In Attendance: Anya Andrews, Lee Dotson, Steffen Guenzel, Melanie Guldi (Senate Liaison), Joseph Harrington (Steering Liason), Athena Hoeppner, Viatchelslav Kokoouline, Matthew Nobles, JP Peters (ex officio).

Minutes: We did not reach quorum, so we did not vote to approve the minutes from our February 17, 2020 meeting.

Chair Announcements:

- The chair introduced invited guest Chris Vakhordjian from Information Security Office. He provided additional clarification regarding the planned phase-out of IMAP/POP due to Multi-factor authentication (MFA). He indicated that OAoth.net is a possible alternative.

Old Business

- Joseph Harrington indicated that he is drafting a resolution regarding Linux and should have this ready to circulate for our next meeting.
- The committee engaged in a further discussion of IMAP/POP deprecation and Chris indicated he would email additional information after our meeting. He indicated that the key issue is how these protocols (IMAP/POP) interact with third party apps, which makes them difficult to manage.
- The committee asked about open source email clients/apps for Linux users. The issue was raised that Microsoft is a proprietary system and if they change the protocols that there is no guarantee that the open source clients/apps will continue to work.
    - Chris provided his opinion that Microsoft wouldn't change their interface drastically, because it would affect end user experience (such as checking email via smart phone).
    - Chris indicated he would do some research to see what the best plug-in (e.g for Thunderbird)
    - JP suggested it would be good to publish a knowledge base if a plug-in that works (for Linux) is identified.
        - One committee member indicated the OWL plug-in for Thunderbird works
- Our discussion then turned to retiree email.
    - The committee asked if one can forward @ucf email to @Knights
    - The committee noted that there is an information gap for retirees. The policies posted appear to be targeted for current students, not retirees. JP indicated that this could be addressed.
- We did not have time to discuss the mission of the committee.

New Business

- None

Other Business

- None

ADJOURNMENT

The meeting adjourned at 3:00 pm.

University of Central Florida

Information Security Office
infosec@ucf.edu

ISO Response on IMAP, POP and E-mail forwarding

E-mail is a critical service for all UCF faculty, staff, and students. Our campus community depends on email to communicate with one another and with the outside world. It is important to have the proper controls in place to protect the confidentiality, integrity and availability of this critical service. Current policies are in place for the purposes of maintaining the confidentially, integrity and availability of our email, mailbox content, our enterprise email system and its services. Current policies and technology controls are in place to prevent the spread of malware through email, to reduce phishing and spam traffic, and to promote secure access to email. These measures are also in place to protect our users and the university from identity impersonation or theft, breach or disclosure of confidential information, which may be protected by state and federal laws.

Disabling IMAP and POP:

Prior to exchange, during the GroupWise era, users had the ability to configure any email client they wish to connect to the GroupWise servers using IMAP or POP.

We discontinued the use of IMAP and POP (and SMTP) for the following security reasons and concerns:

- The E-mail client (e.g., Mozilla's Thunderbird, Apple mail, etc.)
    - Giving the users the freedom to choose their own email client of choice introduces the following questions and concerns:
        - How secure is the email client? How up-to-date is the email client? How does one insure the email client is updated?
            - An email client that is not up-to-date introduces risk of compromise and disclosure of information.
        - Does the email client save the users credentials in a secure way?
        - A third party email client would typically save the IMAP and POP passwords and would not prompt a user to enter credentials to access the email through the client. Therefore, users would not need to authenticate to retrieve their email, thus potentially violating our policies (Policy 400-2) and standards.
        - Third party email clients installed on uncontrolled or unmanaged computers introduces the undesirable effect of having ones email and email archives on unknown and unmanaged computers. The ability to locate and retrieve email and email archives are important for investigation and eDiscovery purpose, or when served with a public records request.

- The Protocol (IMAP, POP and SMTP)
    - IMAP and POP are only email retrieval protocols. To be able to send email the SMTP (Simple Mail Transport Protocol) protocol must be used with an email client.
    - All three protocols generally work under clear text transmission and did during the GroupWise era. In other words, communication using these protocols can

be in the clear and therefore susceptible to "wiretapping." There are many easily found tools to wiretap such network communications and clearly read the communication. Although it is possible to secure them using SSL/TLS (Secure Sockets Layer/Transport Layer Security) they would typically work without SSL, especially the SMTP protocol, allowing someone to both read the communication and the credentials used to authenticate the user to the email system. Limitation on the security and strength of the SSL encryption would allow one to once again wiretap the network, "strip" the SSL/TLS from the communication and read the communication in the clear.

- We would not be able to prevent a user from using insecure SMTP protocol to send email messages. In fact, if one's Internet Service Provider provides SMTP protocol on their network, users will be sending email inadvertently in the clear for others to eavesdrop and read the communication.
- Some Internet Service Provides (ISP) have turned off the SMTP protocol, due it's inherent security issues and due to its use for nefarious reasons, e.g., phishing, form their customer networks, therefore users could experience connectivity issues while on ISP networks.
    - In such cases, ISPs provide their own SMTP services for users, which typically allows sending email without proper protections, i.e., SSL/TLS.
- **In short, IMAP or POP do not offer a methodology to ensure devices connecting to UCF enterprise email servers are compliant with our policies**
- Reducing the footprint of the amount of protocols that are available to our enterprise email systems, reduces the attack vectors from the internet. Brute force attacks against these protocols would be proactively mitigated.
- Email protocols such as POP, IMAP, and SMTP will not work with multi-factor authentication (MFA) or circumvent them.

- Portable devices with email clients using IMAP, POP and SMTP
    - Smartphones and portable devices, when configured using IMAP or POP, have the ability to retrieve/download email close to real-time without user interaction. This introduces the same security concerns and issues mentioned above under unmanaged third-party email clients, and IMAP/POP/SMTP protocol weakness, etc.
    - Since the nature of these protocols are to download email messages, an unmanaged device configured using IMAP and/or POP introduces the risk for disclosure of potentially confidential information.
    - Using solely IMAP or POP protocols, smartphones and portable devices, cannot be secured administratively or provide the accountability that these devices are secured. With these protocols in use, there are no technological capabilities for forcing a password on portable devices, thus to comply with university policy 4-007, or the capability to remote wipe a device in the event of device theft or loss.
    - **The inability to execute a remote wipe or force access password on a portable device, places the university at risk for disclosure of personal, sensitive or proprietary information.**
        - This risk is eliminated with the use of Microsoft Exchange synchronization Services

Forwarding of email to webmail (e.g., Gmail, Live, AOL, Yahoo, etc.):

Prior to exchange, users had the ability to place mass forwarding rules in GroupWise to forward all their emails to unknown webmail locations.

The ability to mass forward emails should be disabled to mitigate any issues with delivery and accessibility of critical email communication from the university, to mitigate the potential of disclosure of confidential information, and avoid the commingling of personal and business email and the ramifications in the event of an investigation, public records request or a subpoena. This restriction does not mean denying the ability to forward email, but rather setting up a rule to forward all email received to an external, non-UCF, email system.

- Webmail (e.g., Gmail, Live, AOL, Yahoo, etc.)
  - Allowing to forward email introduces the same security concerns and issues mentioned above under third parity email clients and the protocols used to retrieve those emails from webmail
    - Email ending up on webmail systems, such as Gmail, Live, etc. would allow users to use unmanaged email clients with insecure protocols, such as IMAP, POP and SMTP, and possibly from insecure networks, such as wireless or shared networks in apartments and hotels.
  - Privacy concerns have been raised about webmail as users are storing large amounts of personal information. This raises some concerns and questions:
    - Do all webmail providers use the same privacy polices?
    - How does each provider secure user's information?
    - Do webmail providers scour around users email for purpose of targeted advertisement?
    - Do webmail providers comply with privacy and confidentially requirements outlined by federal regulations, such as FERPA, HIPAA, PCI, etc.?
    - Does the webmail provide have a legally binding agreement with UCF?
  - webmail providers retain control over the individual's email while providing email services and storage functions on an individual's account
    - Storage location is hosted and controlled by the webmail provider. The individual does not "have" their email but only has "access" to it and that access is under the sole control of the webmail provider.
    - This becomes a problem when users lose their email account through hacking or malice and are unable to retrieve the only copies of their stored email.

In closing, these measures are intended to enhance the security of our enterprise communication systems, to mitigate exposure of personal or propriety information protected by laws or contract, and to mitigate identity theft or impersonation via email.

Resolution 2019-2020-X Linux Access to IT Services

Whereas,

Linux is among the best operating systems for teaching students to control computers, both for programming and for operating-system-level tasks,

Linux is free of charge and runs on a wide variety of hardware, enabling low- and no-cost, license-free computing for anyone,

Reducing the cost of education, both for UCF and for our students, is a high priority in the university,

, therefore

BE IT RESOLVED that all IT services that faculty, staff, or students are required to use or that are reasonably necessary for success in their respective roles be based on broadly accepted internet standards. Specifically, for email, these include the Post Office Protocol, version 3 (POP3) or later, and the Internet Message Access Protocol (IMAP). For shared filesystems, this includes the Common Internet File System (CIFS). For printing, this includes the Internet Printing Protocol (IPP).

UCF IT shall promulgate on its web site and by other means the standards, servers, port numbers, and other settings required for self-supporting users of any operating system to connect their computers to campus services.

UCF IT may additionally choose to recommend and support specific client software for specific operating systems, and not to support other software, based on a combination of campus demand and support load and impact.

For users of confidential data, UCF IT may establish restrictions and required training to ensure that such data are not inadvertently disclosed.