Virginia Tech's Subcommittee for IT Security

Meeting Details

- Date and Time: February 5, 2014, 3:30pm to 4:30pm
- Location: IT Security Office, 1300 Torgersen Hall

Attendees

- Randy Marchany
- Mary Dunker
- Al Cooper
- Dale Pokorski
- Sandy Power
- Karen Herrington
- Malcolm Beckett
- Dominik Borkowski
- Jerrad Miers
- Brett Besag
- Allen Campbell
- Annie Wong

Meeting Support

- Richard Sparrow

Agenda

A formal agenda was set by Mary Dunker and Randy Marchany prior to the meeting. Agenda Items included:

- Agenda bashing
- SANS-EDU: Auditing Networks, Perimeters, and Systems
- Restricted/Limited Access Project (RLAN) Status
- PID Password Expiration Notices
- Update to Personal Digital Certificates
- Open Discussion

Discussion of the SANS-EDU: Auditing Networks, Perimeters, and Systems

Randy Marchany discussed a SANS training opportunity that the IT Security Office was organizing for March 10-15th. He talked about the training, intended audience, and cost.

Discussion of RLAN Status

Randy Marchany discussed the progress of the Restricted/Limited Access Network (RLAN). He gave an overview of the projects status and intended purpose.

PID Password Expiration Notices

Mary Dunker discussed password expiration notices with the group. Several members of the group indicated that communication of pending password expirations were beneficial for their users. Brett Besag did not think the communication should include links. Brett felt that some of his users found it difficult to distinguish between legitimate VT communications and phishing email. Brett suggested that communications should direct users to my.vt.edu to change thier passowords. Karen Herrington stated that my.vt.edu was capable of facilitating password changes for PID, Hokies, and Oracle. The group indicated that the links inside of my.vt.edu needed to be more visiable.

Dale Pokorski and Al Cooper indicated that users are often confused about which accounts they have and that the email communication should help describe the accounts. The group also indicated that users sometimes are unclear about the difference between PID, Hokies, and Oracle accounts.

Dale Pokorski questioned why the PID or Hokies credential could not be used for wireless. Mary Dunker explained that the PID credential could not be used because the wireless implementation would introduce a security risk, giving access to the PID password outside the Enterprise Directory control.

Dale Pokorski indicated a need to be able to check the password expiration status of her users in an effort to reduce work disruption. She indicated a need for a tool that would show her users status. Karen Herrington mentioned that the password expiration attribute would be available. Mary Dunker discussed the challenge of authorizing individuals to only view their users' information and limiting access to attributes based on the principle of least access needed.

MultiFactor Authentication

Randy stated that the use of multifactor authentication is expected to increase and that several multifactor solutions were being examined. Malcolm Beckett indicated that his group was had examined YubiKey, Mary Dunker indicated that the e-Token was available, and Karen Herrington indicated that VASCO OTP was being used.

Karen Herrington indicated that approximately 300 users with elevated Oracle privileges would receive VASCO OTP (One Time Passwords) devices in an effort to further secure Oracle accounts. Several members of the group indicated that they would like advance notification of their users who may receive the OTP device. There was concern that the devices may become lost if they are infrequently used.

Many and the group indicated support for increased use of multifactor to help reduce the risk and impact of credential compromises. Dominik Borkowski mentioned that OTP is effectively delivered via mobile devices and SMS messages. Mary asked the group to share possible use cases.

Update on Personal Certificates

Mary Dunker updated the committee on personal certificates. She stated that work was being done to have the certificates globally trusted and that a certificate authority for software certificates was being created. The software certificates could be used to encrypt email and encrypt documents. The software certificates could also be used for authentication.

Open Discussion

Some topics were submitted by Subcommittee members for discussion.

Increase in Brute Force Attacks

Randy Marchany stated that the IT Security Office has seen an increase in brute force password guessing attacks on Virginia Tech systems. He stressed the importance of strong passwords and firewall settings for services like RDP.

Awareness Training

Brett Besag commented on the techsupport listserv discussion about Securing the Human awareness training. He stated a concern that awareness efforts were too simple and would be of little value to his users. He stated that the needed to be "short and hard hitting." Many of the group members indicated that Securing the Human adequately covers awareness material.

The benefits and challenges of a mandatory awareness program were discussed. Many of the group felt that mandatory training would be beneficial. Dale Pokorski indicated that a top down approach that was enforceable was needed. Jerrad Miers indicated that removal of network access may be an appropriate enforcement mechanism. Al Cooper indicated that an awareness training process tied to password resets should cover pressing topics and should be limited to 15 minutes. The consensus of the group was that pushback would be likely to mandatory training but could be beneficial if it was enforced.

Communications

Brett Besag discussed his concern that communications from central IT were too technical for his users. He gave an example of a recent email communication that discussed a hard drive failure that may have caused phone messages to be lost. Dale Pokorski stated that she often rewrites messages to make the message more appropriate for her users. Karen Herrington indicated this was a common challenge and that improvement might be needed.

Discovering a User's PID

Brett Besag indicated that he had a challenge discovering a user's PID in an effort to help them. Allen Campbell indicated that Banner access may help discover a user's PID if they know the ID number.

Proxy Development

Dominik Borkowski indicated that he once understood the IT Security Office was developing a web proxy to be used by the university community. He indicated a strong desire to use such a system in his area. Richard Sparrow stated that the IT Security Office did not have the project on their roadmap.

Log Monitoring

Allen Campbell discussed the challenges of log monitoring. He indicated that he thought log monitoring was a challenge for many departments across the university and asked what other committee members were doing. Malcolm Beckett stated the that his area was implementing Kiwi to archive the logs. Dominik stated that his group relied on syslog to send the logs to an external system for archiving.

Allen also indicated that he thought there was a need for a common system to process logs that could be analysed by IT Security Office personal. Mary Dunker indicated that some central IT departments were using Splunk, and some analysis was being done for Windows.

Digital Signing

Group discussion regarding certificates led to discussion about projects that could facilitate digital signing and workflow. Dale indicated a desire to see more digital signing incorporated in items like leave reports. Dale also indicated that she thought that the timeclock system was difficult.

Allen Campbell shared information about projects that were intended to leverage digital signing and workflows. He updated the group on the wage/timekeeping project and the travel reimbursement system project.

Action Items

- Send draft password expiration email languge to group
- Update subcommittee website with new members