Security Advisory Committee – Update on Activities & Meeting Minutes
Co-Chairs: Wayne Donald & Mary Dunker

November 17, 2009

A new committee member, Tim Tutt, has joined the committee representing the student body at Virginia Tech.

Since the last committee meeting in April, 2009 there have been several activities and implementations to help in addressing the areas of concern identified at the last meeting.

Awareness/Education

1. The IT Security Office (ITSO) is working on a solution to provide online security modules (for both general awareness and compliance issues). A decision will be made before the end of this calendar year and the plan is for some modules to be in place before July, 2010.
2. Participation continues in the Faculty Development Institute (FDI) as well as in various orientations for faculty, staff and students. The ITSO also participated in several large undergraduate classes early in the semester reaching over 5000 students.
    a. It was also suggested that the IT Security Office might check on what is being done with some of the professional development efforts at Tech. Perhaps something can be incorporated into their process.
3. General awareness has continued for the university community with the use of ads for the online version of Collegiate Times during the month of October (National Security Awareness month). There will be another emphasis starting this week (for people leaving for Thanksgiving) and the week of December 7 for the holiday break.
4. A one day seminar was offered in October and attended by over 80 individuals – seminar was entitled "Defense against the Dark Arts." Monte Elkins conducted the training and covered several topics related to hacking techniques.
    a. The IT Security Office will look at offering a SANS class in the Spring but because of budget constraints it will most likely be a "short" class or an online (distant learning) offering.
5. The security web site (http://security.vt.edu) has been redesigned and some new features added (including a link for the committee: http://www.security.vt.edu/it_security_subcom.html).
    a. Developed a new site gateway dedicated to cyber security issues. Review the link at http://www.security.vt.edu/cyber_security/index.html.
6. The IT Security Office prepared awareness materials and provided them for download from their web site. The download materials include awareness posters and desktop background images for computer labs and individual machines. Awareness videos are also linked form our website.
    a. Distributed awareness mouse pads to students thru collaboration with Software Distribution (on the Torgersen bridge).
7. The IT Security Office has established a presence on social networking. The IT Security Office now is on Twitter, Facebook, and YouTube. Those sites will be linked from the University Relations site and the IT Security site in the near future.
8. Randy Marchany and Nick Pachis will be offering a one day class for new system administrators in early January (prior to students returning).
    a. Marc DeBonis is available to assist with instruction or consulting on Active Directory in the new system administrator class.

b. Plans are to have another offering in the Spring or early Summer. If you have any specific topics of interest, it's suggested to send them to Randy Marchany.

There continues to be an effort to implement a "required" verification process that will be put forth for all Virginia Tech employees. The verification process is to ensure anyone working with sensitive data has a secure operating environment.

Access Security

1. Although not "directly" associated with access security as this committee might consider, there is a joint effort starting between the Information Technology organization and Administrative Services. A committee will be meeting to identity areas that need to be reviewed and considered for further initiatives. This is an effort to determine how physical security and cyber security might converge on providing a more overall secure environment for Virginia Tech.
    a. This effort should bring to light more attention to provisioning and de-provisioning, as well as the various electronic identities individuals have at Virginia Tech.
2. Identity Management Services (IMS) recently de-provisioned 1279 former employees – anyone that had no other (significant) affiliations except "former employee" and had been a former employee for 2 years or longer. PID/email/Hokies de-provisioning is currently a partially automated and partially manual process.
    a. In conjunction with this effort, IMS prepared a short document for Human Resources describing IMS's processes regarding the PID/email of employees separating from VT.
3. Alumni email is being de-provisioned via the cutover to Google email. There are approximately 60,000 alumni email accounts that will be converted to Google email. IMS is "pushing" 10,000 accounts per week, beginning the week of November 16.
4. A meeting was recently held to start defining an automated process for de-provisioning Hokies/Exchange accounts in conjunction with the Active Directory (AD) Admin project through the Microsoft Implementation Group (MIG).
    a. The AD Admin project involves using an updated Microsoft infrastructure to replace the Hokies self-service (HSS), OU Admin, and Identity Management Service's MMC interface to Active Directory. The first priority is HSS, but work is being done on de-provisioning Hokies Active Directory accounts. A question was asked about time lines and it is estimated the AD Account de-provisioning can be ready this summer, 2010.

Secure Enterprises

The specific concern in this area seems to be on the various documents required by departments (the Continuity of Operations Plan (COOP), a Risk Assessment (RA), and a Disaster Recovery Plan (DRP). Since the last meeting departments have also been requested to prepare an Emergency Action Plan (EAP). There will be discussions in the near future with Emergency Management personnel to determine

1. What the university (and we assume each department) will be required to have,
2. who will provide the template(s) and instructions, and
    a. It was noted that there should be an "online" form/application for the COOPs in place by March, 2010. This will come from the Administrative Services area.
3. what area(s) will be required to "account" for everything being in place.

Other Initiatives

1. Secure Enterprise Technology Initiatives (SETI) has been leading an effort to develop a Standard for use of Personal Digital Identities that can be implemented for the university community.
    a. The Standard for Use of Personal Digital Identities has been drafted. The standard is intended to give sponsors a methodology for selecting authentication credentials that provide an appropriate level of trust in the digital identity of the person accessing a service, function, or application. In addition to the PID, Hokies ID, and Oracle ID, central IT now supports guest accounts and personal digital certificates (PDC) for authentication. A level of assurance (LOA) is associated with the credential, based on the degree of confidence that the credential is being used by the person to whom it was issued. The standard was distributed to the group, and they were encouraged to provide feedback.
    b. IT is strongly encouraging people to use CAS rather than ED-Auth LDAP authentication because CAS is more secure. At some point in the future, LDAP authentication using ED-Auth will be restricted. The version of CAS now in production can be used for authorization information such as affiliations and group membership. CAS also passes the LOA (a number from 1-5) in the SAML payload so an application can know what type of credential was used to authenticate to the application. CAS supports PID and PDC today, but in the future will support guest account login.
    c. It was suggested that having a document available to help application administrators understand what has to be done would be very helpful.
    d. Although there is no stated migration plan, IT would like to begin having applications utilize the CAS features, and begin to purge a dependence on LDAP and ED-ID. It was suggested that perhaps some date needs to be determined (with an appropriate timeline) and users notified of what actions need to take place.
2. The IT Security Office will be assuming responsibility for the Rights Management Services (RMS) that will allow for the encryption of documents in shared folders on the NAS.
3. The IT Security Office is working with Network Infrastructure & Services to develop/implement an open source intrusion detection system.

Additional items for discussion and consideration:

After discussion of the items above, individuals were asked if they had anything to bring up for information or future discussion.

- The student representative brought up the issue of using the student name and identification (ID) number for various things on campus. For example, some areas distribute materials that contain name and the full student ID number, and there is a very lax environment in exposing that information. Also, some areas on campus that retain sensitive information on students only require the name and ID number to give out that information. It seems to ID number is starting to become as critical as the social security number was previously, and perhaps we need to look at how it is indeed being used.

- There was some discussion about departments on campus purchasing the commercial product called Identity Finder to examine systems for sensitive data. There have been discussions about a possible site license but it has really been cost prohibitive. However the IT Security Office will contact the vendor and see what procurement options might be offered.