ABSTRACT

As Armstrong Atlantic State University prepares to enter the wireless world during the 2006-07 academic year, it is important that those connecting to the university’s network use notebook computers that are free from viruses and malware. In order to help secure the network, Information Technology students were given practical experience by organizing and performing virus and malware scans on student notebook computers. As an incentive to participate, students were provided flash memory jump drives containing various security programs to be installed and executed on their computers. These were purchased as part of an AASU Teaching and Learning Grant approved by the university in November, 2005. This paper describes this important project, its outcomes, and future pedagogical implications.

Keywords: Information Security; Information Security Education; Information Security Awareness Programs; Design.

2. THE PROJECT

In October 2005, this project was submitted to the Faculty Development Committee of AASU for consideration to be awarded a Teaching and Learning Grant. It was conceived to mitigate the threat of viruses transmitted into the AASU network from notebook computers, to make students more aware of the dangers of using an unprotected computer, and to give Information Technology students practical experience in creating and implementing an Information Security awareness campaign. The committee approved the project (AASU project # 727173) to be funded in the amount of $1697.00. The funds were used to purchase flash memory jump drives given to students as an incentive to participate, and to pay two students majoring in IT up to $200 each to assist with the design and implementation of the project, instruct the student participants in security best practices, and collect the data. The IT student assistants were enrolled in the first cohort of AASU’s Information Security course, ITEC 3100. Each 256 MB USB flash memory drive was loaded with a variety of free anti-virus, spyware removal, and security software. This allowed the students to become aware of the dangers of using an unprotected computer, and to give them practical experience by organizing and performing virus and malware scans. Each participant’s notebook computer was scanned for viruses and malware and then infect the network when they log back on.” [3]

To alleviate these threats, students should not only be made aware of them, but should have their notebook computers scanned for viruses and malware and be taught the best practices for maintaining the integrity of their computers.

1. INTRODUCTION

As more and more students at Armstrong Atlantic State University (AASU) use their own notebook computers to connect the Internet, they and the university run increased risks of exposure to dangerous viruses and spyware. Coupled with the wireless network that will be implemented on campus in the 2006-07 academic year, the threat of the university’s network being compromised by a notebook computer looms even larger. Indeed, “the threats against wireless networks reflect the variety of users on the network.” Unlike a corporation, which represents “a single point of trust for their employees,” the university environment lends itself to many different users on the network using a wide variety of notebook computers, not all of which will be “clean.” It

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Information Security Curriculum Development (InfoSecCD) Conference '06, September 22-23, 2006, Kennesaw, GA, USA.
Copyright 2006 ACM 1-####-####-####/06.. $5.00
3. EXPECTED OUTCOMES - ANTICIPATED IMPROVEMENT IN TEACHING AND LEARNING

There were two target populations of this project: the IT students performing the analysis and the student participants who had their laptops analyzed. It was expected that the project would provide a benefit to university by ensuring that their computers were “clean”, free from viruses and malware. It was also expected that the project would improve information security awareness on campus. The project achieved both expected outcomes. Students who submitted their notebook computers for analysis had viruses and spyware removed from their computers, and were instructed in the proper execution of the security software given to them, how to create strong passwords, and how to perform Microsoft security updates on their computer. Interest in the scan sessions has not waned since the last session was held on March 29, 2006. Weeks after that session (as recently as May 24, 2006), I was still receiving phone calls and e-mails from students asking when the next virus/malware removal session will be held.

Two students from my ITEC 3100 course were selected to prepare and execute the scan sessions. Both were paid the stipends in the budget approved by the AASU Faculty Development Committee. It was expected that the practical experience gained would include the ability to identify and assess risk, plan and conduct a security awareness program, work with different security technologies, and instruct students in various security best practices, thus translating the theory of the classroom into action.

4. THE PROCESS

The design of the project was documented in memos, e-mails, and MS Project Gantt charts. I performed the initial tasks immediately after the project was approved. These included scoping out the project in a Gantt chart and selecting the student assistants.

By early February, 2006, the two student assistants were selected from my Information Security class. They were selected on the basis of their technical expertise and interest in the project. Various tasks were listed and then assigned to both assistants at our first meeting on February 10. In order to keep the project on schedule, the tasks were entered into MS Project, which simulated a real work environment by giving them a method to ensure that every task was included and completed on time. Both students supplied ideas about advertising, including promotional advertisements and procuring student giveaways. Based on their academic and work schedules, several dates were chosen for the scans and a location was selected.

The student assistants were assigned to write a liability waiver to protect the university and a privacy policy to protect the participants; a list of approved practices to be distributed to the participants at the evaluation sessions; a list of statistics to be collected and survey questions that the participants would answer; and a list of software to be loaded on the flash memory drives. The software would then be copied onto the participant computers and executed. Unable to come up with a satisfactory liability waiver, I contacted Dr. Michael Whitman of Kennesaw State University, and he was kind enough to provide similar documents used for the same purpose by KSU’s ISSA chapter. We altered them accordingly for our purposes and for AASU. This effort taught the assistants the importance of including strong, detailed policies as an element of any information security plan. Designing the various elements of the plan gave them realistic experience in systems design, necessary for the installation of an information system of any size.

The assistants came up with several different free anti-virus, anti-spyware, and firewall software selections to be loaded on the flash memory drives, provided to the participants, and used during the sessions. We decided on the Grisoft AVG Free anti-virus software, the Lavasoft Adaware SE and Spybot spyware removal tools, and the Jetico Personal Firewall. Working with the various software packages helped the student assistants determine which programs would be easy to install and simple for the student participants to understand and use. A key element of their decision was future ease of use by the participants, for once the software was installed on the their laptops, it would be their responsibility to continue to execute the programs in order to keep their computers secure. Due to the more complex features of the Jetico Personal Firewall, they decided not to include it in the set of software to be installed. After the final decision was made, I purchased the first 25 flash memory jump drives, and the team loaded them with the anti-virus/spyware removal software.

Advertising is an important component of any information security awareness program. The student assistants came up with the advertising plan: create eye-catching flyers and place them all over campus. Conveniently, the husband of one of the assistants is an art teacher, and he produced several original drawings for advertising flyers. We selected two of them, both students refined them, made numerous copies, and posted them in every building on campus, including on-campus student housing. I contacted the secretary to the vice-president, and she e-mailed the flyers to all faculty members so they could promote the sessions in their classes. In addition, I e-mailed each faculty member in the School of Computing so they could also announce the sessions to their Computer Science and Information Technology students.

Each element of the preparation, design, and implementation of the diagnostic scan project enabled the student assistants to put classroom theory into practice. From deciding on scan dates to creating and distributing the advertising to determining the software to be used, the process provided them with invaluable experience in the creation and execution of an information security awareness program.

5. IMPLEMENTATION, EVALUATION, AND FINDINGS

The scan sessions were held on March 6, March 8, and March 29, 2006. All three were two hour sessions. Twenty-five student notebook computers were evaluated during these sessions.

Upon arrival, each student was required to fill out the waiver of liability, which included supplying the following information: computer model; operating system; processor type and speed; RAM size; and any existing security software. Each student was given the flash memory drive containing the security software. The student assistants and I loaded the security software onto the participant’s notebook PC from the flash memory drive. In each case, if a participant had up-to-date antivirus or anti-spyware
software, we used the programs already on their PC to perform the scans and recorded the results. Otherwise, we used the programs that we gave them.

It was not enough to perform the virus/malware scans. Data on mobile devices such as notebook computers must be protected, and the student assistants taught the participants various different ways of doing this. These included: instruction in the utilization of “strong passwords containing alpha-numeric characters that are at least eight characters long and are unique”; [2] instruction in how to update their anti-virus software; and instruction in the use of a mobile firewall.

5.1 Findings of the anti-virus scans
Each student’s PC came loaded with various different anti-virus programs. As expected, the most popular pre-loaded programs were Symantec’s Norton products and McAfee’s products. Ten PCs had various Norton products loaded, including Norton AntiVirus, SystemWorks, and Internet Security. Five PCs had McAfee products, the most popular being McAfee’s VirusScan. While most students were knowledgeable about the use of their anti-virus software, four indicated that they rarely check the results of their virus scans and two others who used Norton products had let their virus definition subscriptions expire. The students with expired subscriptions had no choice but to use the free AVG anti-virus software we provided.

Nearly all of the computers we were able to successfully scan did not contain any viruses, and based on the date/time stamp of their most recent scan, it appeared that their owners had set their computers to automatically perform the scans on a regular basis. Of those that we were able to successfully scan, over 1,400,000 files were scanned, and only 13 viruses were discovered. All of the viruses that were detected were successfully deleted.

5.2 Findings of the anti-spyware scans
Most students did not already have third-party anti-spyware software loaded on their PCs. Those that did were using Spybot or SpySweeper, and were knowledgeable about their operation. Students that weren’t using third-party software were using the default Microsoft Windows XP Service Pack 2 anti-spyware solution as a default. From our interviews, we discovered that many of the students using the Microsoft anti-spyware program had it configured when they purchased the computer and weren’t familiar with its features. Consequently, we installed Lavasoft’s Adaware SE program on nine PCs, and Spybot on three others and executed the software. Of over 928,000 files scanned, 1,518 spyware files were detected and all of them were deleted.

5.3 Windows Update
Each student’s PC was checked to determine if Windows Update was being run on a regular basis. Twelve students were running it on a daily basis, and four were running it at least weekly. Those students who were not running Windows Update on a regular basis were instructed on how to set up their PC to do so.

5.4 Participant Evaluations
Nearly all of the students found the virus/malware scan sessions to be of great assistance. Many not only suggested that the program be held again in the future, but that they would once again bring their PCs to be scanned and evaluated.

When asked “Did you find the services offered helpful?” every student responded in some form of “Yes.”

When asked “What other services could we offer to improve the security and usefulness of the AASU computing environment?” we received many different responses: “Offer services to on-campus apartments.” “Wireless connection info help”; “Maybe a guest speaker on Internet security.”

5.5 Student Assistant Evaluations
Since there were only two student assistants, a formal survey was not used to determine their evaluation of the project. Rather, I had them write their assessments. The most significant observations were: “there was so much to do during the scan sessions that we needed more student helpers” and that “creating and distributing the advertising helped me understand what goes on in an awareness campaign.” In addition, one of the assistants wrote that “as much as I know about software, deciding what software should be used helped me to think about what would be the best and easiest for non-technical students to use.”

Both student assistants enthusiastically responded that the program should be continued in the future, perhaps on a regular, once per semester basis.

6. RECOMMENDATIONS AND CONCLUSIONS
Overall, the program accomplished its goals of making the AASU student population aware of the need for securing their computer while providing the student assistants with practical experience in designing, planning, and executing a computer security awareness campaign that includes virus/malware scanning as its primary focus.

6.1 Recommendations
It is my intent to perform this program when ITEC 3100 is taught again during the Spring 2007 semester. Before this is done, several problems that were discovered need to be addressed and corrected.

We needed more student assistants, as there was just too much work to be done by two assistants and myself. The project was funded to provide stipends for two assistants. Using students who were being paid and students who were not might have caused conflict throughout the duration of the project. Another problem with using more student assistants was the “non-traditional” nature of AASU’s students, many of who work during the day and were not available for the sessions. Since future sessions will not involve student stipends, there will not be an issue of budgetary constraints vis-à-vis some student assistants being paid and others not being paid. The solution to not having enough assistants is that the entire Information Security (ITEC 3100) class should be involved, not just two student assistants. Working the students in shifts should alleviate the problem of scheduling “non-traditional” student assistants. If more students are needed to help, they can be recruited from the AASU Student Chapter of ACM. More assistants will also facilitate a more accurate recording of scan statistics and provide the student participants with additional one-on-one instruction.

Not enough time was given to thoroughly scan each student’s notebook computer. A normal virus scan will often run for an hour or more. The longest session was only two hours long. Provided that we have enough student assistants, we should schedule each session for a minimum of four hours, and perhaps
an entire school day. An increase in the number of student assistants should make it easier to offer longer sessions, thus allowing the student participants to leave their laptops with the scan team to ensure that all of the diagnostics are completed.

We used the university’s (faculty) dining room for the scan sessions. While the room provided ample enough space to accommodate all of the student participants, with only two network jacks, the location was not conducive to downloading updates to the software. Despite the difficulty of scheduling computer labs at AASU, the next time this program is conducted, it should be held in one of the School of Computing labs or the general student computer lab.

6.2 Conclusions
With the coming of a wireless network, computers at Armstrong Atlantic State University will be more vulnerable to viruses and malware if steps are not taken to make the general student population more aware of them and to mitigate these risks by ensuring that student notebook computers that access that network are free of these pests. Scanning only twenty-five notebook computers may not sound like a lot, but it raised the awareness of the student participants to the need for them to take ownership of the security of their computers. The advertisement and execution of future such sessions should raise the security awareness of all AASU students, even those who do not participate in the scans.

Pedagogically, the student assistants participated in the planning, creation, and execution of an Information Security Awareness Program, thus enabling them to transform textbook knowledge into practice. This project laid the foundation incorporating the planning and execution of future campus-wide virus/malware scans in the curriculum of our department’s course in Information Security.

7. REFERENCES