Breaches emphasize need for scanning, encryption

March 17 2009

Recent news reports indicate a computer containing confidential information about the helicopter that transports President Barack Obama was breached by a computer in Iran. In January, Heartland Payment Systems, a company that provides credit and debit card, payroll and related processing services to more than 250,000 business locations nationwide, announced it had a data breach that potentially exposed credit card numbers, expiration dates and other data. The Heartland breach includes about 700 Penn State purchasing cards, which are in the process of being replaced.

The Identity Theft Resource Center, a nonprofit organization dedicated exclusively to the understanding and prevention of identity theft, said that 656 security breaches had been reported by the end of 2008, reflecting an increase of 47 percent over the 2007 total. As of March 17, the resource center already reported 110 breaches for 2009, potentially exposing close to 1.3 million records containing personally identifying information such as Social Security and credit card numbers.

As the nationwide problem of identity theft continues to evolve and grow, Penn State is not immune. Malicious software, downloaded by unsuspecting employees who click on messages containing links to fake greeting cards or other seemingly harmless sites, has compromised computer networks at University Park and other campuses.

"We cannot stress enough the importance of not clicking on links in e-mail if you do not know for sure who sent the e-mail to you," said Kathy

Kimball, senior director of ITS Security Operations and Services. "The most common of these e-mails state that a friend sent you an e-card, and you need to click on the link to view it. When you click on the link, you're redirected to a Web site that downloads malicious software onto your computer without your knowledge, opening up security breaches that can affect every computer on the network to which your computer is connected."

Gary Langsdale, University risk officer, reports that since October of last year, his office has received reports of a number of potential privacy breaches, most of which are related to an employee inadvertently clicking on one of those malicious e-mail links.

One such breach happened at Penn State Harrisburg in December. A University computer containing personally identifying information, including Social Security numbers, of continuing education students was discovered to have been infected with malicious software that had been inadvertently downloaded from the Internet. The computer contained information for 557 continuing education students, along with roughly 50 student IDs from another university. The continuing education students work for five different Harrisburg-area employers.

"We're in the process of notifying those who may be affected," said Langsdale. "At this time we have no knowledge that this information was accessed by unauthorized individuals. Our goal is to alert anyone who may be affected and arm them with information and steps to take to lessen their risk of identity theft -- even if that theft is only a remote possibility."

Another breach involving the unintentional download of malicious software compromised a Penn State computer in the Office of Physical Plant at University Park in February. "Again, we do not have any information to indicate that sensitive information was accessed by

unauthorized individuals, but we are in the process of notifying those who may be affected."

Those whose personally identifying information may have been compromised were sent a letter informing them of the breach. The letter included a brochure containing information from the Federal Trade Commission and the Pennsylvania Attorney General's Web sites about how to prevent identity theft, including placing a fraud alert through the credit reporting organizations.

"These breaches could have been prevented and they certainly illustrate the importance of the University's security and privacy initiatives," said Kevin Morooney, vice provost for Information Technology. "Our information environment is under attack several times a second each and every day, so we need to respond with increased efforts to protect privacy. And as a research university, we need to make sure that what we do is as unobtrusive as it can be to scholarship."

The security and privacy initiatives include the location and protection of personally identifiable information on University-owned computers and full-disc encryption to protect laptops that are stolen or lost. The first phase of the initiative, which began in fall 2008, is focused on scanning University-owned equipment in University facilities. The reviews will be exclusively limited to looking for numerical codes that resemble Social Security, credit card and bank routing numbers, as well as the presence of malicious software that might enable the compromise of sensitive data. Reviews will be accomplished with the full knowledge of everyone involved and file content, such as teaching materials, research materials, financial information, letters of recommendation and personnel files, will remain untouched.

Reviews will be accomplished with the full knowledge of everyone involved and file content, such as teaching materials, research materials,

financial information, letters of recommendation and personnel files, will remain untouched, according to Kimball.

"We want to emphasize the scanning effort is not designed to highlight personal files or other material aside from the numerical patterns we have just described," Kimball said. "The ITS Security Operations and Services team has already been able to help many units at Penn State go through the review for sensitive data and we can report that the process has gone very well. In fact, it has resulted in a reduction of unprotected, personally identifiable information on Penn State networks."

Provided by Pennsylvania State University (news : web)