SECUREPURDUE NEWS
www.purdue.edu/securepurdue

January 2009
Volume 4, Issue 1

All the news that's secure to print.

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Happy New Year!! The New Year brings an opportunity for predictions and resolutions. In that spirit, I want to make a few predictions in the security area and suggest a few resolutions for your consideration.

In 2009 cybercrime will continue to grow. Past history has shown it to be a low risk, high value endeavor and there is no reason to believe this won't continue. In fact, in difficult economic times worldwide, cybercrime will become even more attractive. Talented people will find themselves in difficult situations and the risk/value proposition of cybercrime will just become too attractive. This means that, not only will the level of activity increase, but also the level of creativity will increase.

In 2009 cybercrime will continue to be big business. It will be all about the money. In some countries, these "businesses" will function with the endorsement of political leaders. These groups will have employees, set goals, have paid vacations, celebrate with office parties, and support the local economy.

In 2009, traditional defenses involving networks, operating systems, and applications will continue to become more available. Vendors will become more creative and there will be new products to try to address new threats. The fact will remain, however, that technology alone will not be able to solve the problem of cyber security. 90-95% of the "incidents" will still involve an end-user intentionally installing some malware or users freely giving up their password. Creative methods will continue to work on gullible users who don't understand the risk.

Sadly, 2009 will not bring any significant improvements in either new laws or policies or enforcement in the areas of cybercrime. The multi-jurisdictional issues will continue to be the key impediment to addressing this issue. Additionally, governmental energy and focus will be completely consumed with addressing more pressing issues.

Not a very pretty picture but I don't believe the situation is hopeless and that brings me to the opportunity for some New Year's Resolutions. The most important thing each of us can do is accept that cyber security isn't a problem that belongs to someone else to solve. Security is everyone's business.

Let's resolve we will not believe that every piece of e-mail suggesting to "Just click here ..." represents something in our best interest. Let's be suspicious and think before we click.

Let's resolve to check in with http://www.purdue.edu/securePurdue at least once a month to check on current cyber security news and threats.

Let's resolve to attend at least 2 sessions during October Cyber Security Awareness activities to review the threats that face us and the actions we can take.

Let's resolve that we will do everything possible to protect the critical information that our fellow Boilermakers have entrusted to us. We must handle it as if it were our own information.

We will need to work hard in 2009 to keep pace with the threats. If we are successful, we can hope that 2009 will be about the same as 2008. If we don't continue to work hard, 2009 could be a much worse year than 2008.

As always, thanks for reading and be careful out there.

In this issue

Filelocker: New Secure File Transfer Program for Purdue Staff and Faculty

Filelocker is a program created by IT Networks & Security (ITNS). Purdue faculty and staff can use Filelocker to conveniently and securely share files with other people on campus. With Filelocker, you can share large files easily, without having to worry about single e-mail message size quotas. In order to access the Filelocker application, you must login in with your Purdue Career Account and password.
Filelocker allows a person to upload a number of files into the web-based application. Then, users can set permissions to share the file with another faculty or staff member at the University. Files can also be shared with other people outside of the Purdue community by sharing files via a URL link, which is protected by a pass phrase. Files that are shared via the Filelocker application are encrypted during transfer and can also be stored encrypted.

Currently, the sever storage per person is set to 750 MB. Once a user has exceeded his or her storage allotment, existing files will need to be removed before new files can be uploaded.

Files transferred between employees or with others outside the university using Filelocker are only available for seven days.

Filelocker is not a file storage application. The primary purpose of Filelocker is to provide a safe and secure means to transfer files between employees in a manner that conforms to the University's Data Handling Guidelines for Electronically Transmitted Information.

Filelocker has also been used in the University's IT Incident Response handling process to share virus-infected files for research and analysis.

Filelocker is not a file storage application. The primary purpose of Filelocker is to provide a safe and secure means to transfer files between employees....

Use of the Filelocker tool is subject to Purdue University's IT Resource Acceptable Use Policy. Copyrighted materials may not be shared via Filelocker without permission of the copyright owner.

The Filelocker application went live on January 5, 2009.

In order to access the Filelocker application, you must login with your Purdue Career account and password. Use your career account login at: https://filelocker.itns.purdue.edu

The ITaP Knowledge Base has help on using this new software. To find articles detailing how to use Filelocker, go to: http://help.itap.purdue.edu/search.php?s=filelocker

SPOTLIGHT

Network Operations Security Center (NOSC)

Security Services has been working on the creation and implementation of a Network Operations Security Center (NOSC) located in Young and lead by Eric McCarty. The goal of the NOSC is to create a tier 2-3 support group that will monitor and take ownership of networking and security incidents, and prioritize and resolve these incidents in a timely manner.

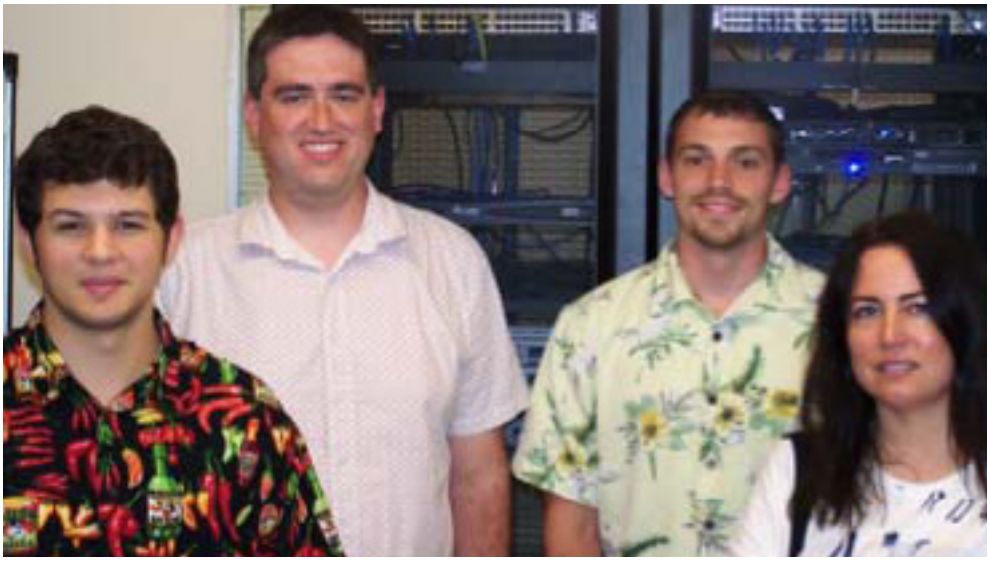
They manage the network applications and equipment to ensure patches and upgrades are performed routinely. This Center will also look for certain network and security conditions which may require special attention in order to avoid impact upon the performance of the Purdue University network.

The NOSC analyzes network and security issues before or as they occur, to minimize the scope and impact on Purdue resources. For instance, by analyzing network traffic, we can determine if a user on Purdue's network has been infected with malicious code and then attempt to prevent data loss.

The support hours are from 8:00 a.m. to Midnight Monday through Friday. The second shift started September 2nd, 2008. They have currently taken over approximately 65% of the security operations tasks and implemented a more robust network monitoring and notification system.

The NOSC will begin phase 2, which is the network handoff piece, in the near future. Within one year of starting the network handoff, the NOSC team will be able to handle 95% of all network incidents. Thanks are due to both the Security and Networking teams in helping the NOSC move forward.

By merging the operations of both Security and Networking and having a centralized focus on these tasks, it will allow for greater efficiency in handling incidents and projects. Moreover, this synergy will allow engineers to focus on development of the next generation of networks and security.



Brett Davis, Anthony Paladino, Brad Graves, and Cynthia Welch

Don't Just Click It!

Click It or Ticket is the most successful seat belt enforcement campaign ever. We want to create an equally successful campaign to caution people from clicking on URL links in e-mails or Instant Messages (IM) or e-greeting messages sent to you from a friend. Clicking on links in an e-mail or IM can take you to a fraudulent web site in an attempt to steal your personal information. Just don't do it!

MILESTONES

CISO Awarded 2008 ISE North America Information Security Executive of the Year Award

Scott Ksander, executive director of IT Networks and Security and Chief Information Security Officer for Purdue University, was awarded the 2008 Information Security Executive of the Year Award, Academic Category on November 17, 2008, in Washington, D.C.

The Information Security Executive (ISE) of the Year Award Program Series™ recognizes individuals and project teams who have demonstrated outstanding leadership in the field of information security, in the United States, Canada, United Kingdom, and Ireland. The ISE Executive of the Year Award honors exemplary achievement and excellence in the management of enterprise-wide Internet and network security. To learn more about the award, visit: http://www.infosecaward.com/northAmerica/northamerica_aboutAward.php

Ksander was nominated for the award by his colleagues in ITNS for his efforts in the SecurePurdue initiative and was one of 3 higher education nominees for the award. "Receiving this award is a great privilege and a tremendous acknowledgement of the success of the entire SecurePurdue team," Ksander said.

Ksander has more than 33 years experience in information technology and over 20 years experience at Purdue in information technology and information security.

Ksander has held the Executive Director for IT Networks, Security, and Chief Information Security Officer position since early 2007. In this position, Ksander is responsible for the data and voice networks, video, and information security functions for Purdue University. Ksander also holds an appointment as an Assistant Professor in the College of Technology where he contributes to the Computer Forensic program and was recently named as an Associate Member of the American Academy of Forensic Sciences and is one of 30 founding members of its new Digital and Multi-Media section.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

Filelocker login URL
- *https://filelocker.itns.purdue.edu*

Login with your Purdue Career account and password.

ITaP Knowledge Base Articles on Filelocker
- http://help.itap.purdue.edu/search.php?s=filelocker