

SECURITY UPDATE

Presentation to the Academic
Leadership Council
December 8, 2008

Outline

- ▣ Security a Chief IT Concern
- ▣ The Evolving Threat Environment
- ▣ Where to from here?

Top 10 Information Technology Concerns

- ▣ Security is listed as the highest IT concern (of the Top Ten) by the Educause Current Issues Committee
 - EDUCAUSE is a nonprofit association with more than 2,200 college, university and educational organization members. Its mission is to advance higher education by promoting the intelligent use of information technology

Why? The Threat Has Moved Well Beyond That of a Few Years Ago

- All you have to do is browse the web...
 - Infection can occur through legitimate Web sites
 - Automated computer takeover and control mechanisms are gaining sophistication and can "hide"
 - You don't have to do anything for your machine to become infected

Source: "Emerging Cyber Threats Report for 2009", Georgia Tech Internet Security Center (GTISC), October 15, 2008

Moving Target

- 1998
 - Simple probes, email viruses
 - Until late in the year attacks did not have a sophisticated command and control method
- 2008
 - Old favorites are still there but much more refined (targeted email phishing schemes, devious probes)
 - Joined by web browsing and web server attacks
 - Automated attacks now have complex command and control structures associated. Sometimes thousands of machines involved

Corresponding Statistics

- 75 percent of malicious Web sites are legitimate sites that have been compromised. This represents an almost 50 percent increase over the previous six-month period
- 60 percent of the top 100 most popular Web sites have either hosted or been involved in malicious activity in the first half of 2008
- 46 percent of data-stealing attacks are conducted over the Web

Source: Websense

More "Interesting" Attack Statistics

- ▣ 66% involved data the victim did not know was on the system
- ▣ 75% of breaches were not discovered
- ▣ 85% of breaches were the result of opportunistic attacks
- ▣ 87% were considered avoidable

Source: Verizon

Effect

- ▣ Because even well protected systems may be infected via simple web browsing, Penn State needs to:
 - Protect personally identifiable Information
 - Embrace safer web browsing practice--browsing with the least computer privileges possible

Where to From Here?

- ▣ IPAS Working Group preliminary reports due soon
- ▣ Data Classification and Security Standards - Review in Process
- ▣ Encryption - Working on finalizing password reset methods
- ▣ Scanning Update:
 - Continuing to work with units that desire scans
 - Percentage of systems scanned that have verifiable SSN, credit card or bank account numbers remains high (~51%)


