IT Security at WSU: Program and Threat Overview

Computing & Information Technology

2014
Today’s Topics

- 21st Century IT security threats
- Repercussions
- Wayne State’s IT security program
- How can you help?
21st Century IT security threats

- Email Phishing and Spear-Phishing and Whaling
- Social Engineering
- Distributed Denial of Service (DDoS) attacks
- DNS hijacking
- Botnets
- Hacks
- Advanced Persistent Threats (APT)
- SQL injections
- Wired and wireless network sniffing
- New vectors being developed and exploited regularly
Security breaches happen

- University of Maryland; servers compromised in early 2014 resulting in >309,000 student and employee records being exposed
- Indiana University; IT security error in early 2014 results in >146,000 student records being exposed
- University of North Dakota; servers hacked in early 2014 results in >291,000 records being exposed
- Evernote hacked; almost 50 million passwords reset after security breach in 2013
- Educause hacked; all passwords needed to be changed in 2013
- Twitter hacked; 250,000 accounts affected in 2013
- New York Times hacked; criminals had long-term access to documents – discovered in 2013
- LinkedIn hacked; 6 million passwords obtained and published online in 2012
- South Carolina taxpayer server hacked; 3.6 million Social Security numbers compromised in 2012
Security breaches are expensive

- University of Maryland 2014 - $2 million. Servers compromised resulting in >309,000 records being exposed.

- Idaho State University 2011 - $400,000. Patient information was vulnerable for at least 10 months because a firewall protecting a server was disabled.

- Massachusetts Eye and Ear Infirmary - $1.5 million. Triggered by a laptop theft that affected about 3,500 patients.

- The Alaska Department of Health and Social Services - $1.7 million. Theft of a stolen unencrypted storage device that allegedly contained data on about 500 Medicaid beneficiaries.

Wayne State is targeted

- Spear-phishing attack results in dozens of WSU login credentials being divulged – within hours, international hackers hijack duped employees’ payroll direct deposits. Money unrecoverable.

- Spear-phishing attack results in dozens of WSU login credentials being divulged – within hours, hackers in South Africa login to TravelWayne and attempt to buy airline tickets.

- On a weekly basis, Wayne State email accounts are compromised as a result of phishing attacks. Accounts are hijacked and used to send more phishing and SPAM barrages.

- On an average day, **millions** of security probes from China and Russia are turned away by WSU’s firewall.
We need you to help secure WSU!
How you can help

- Be vigilant! Security threats are real, frequent and multi-vectored
- Password and PIN protect computers, tablets and mobile phones
- Don’t open suspicious emails or visit suspicious websites
- Use WSU-SECURE Wi-Fi when on campus; use VPN when off-campus
- **Never share your password** or confidential information, especially via email
- Employ firewall, antivirus/antispyware software on your personal computers and servers. Install Microsoft, Adobe, Java patches in a timely way.
- Limit administrative privileges on PC’s
- **Report suspicious events** (via security.wayne.edu)
- Read WSU IT security communiqués
- Stay in touch with your IT support – **we’re here to help!**
Phish Tank and other resources at WSU

Visit security.wayne.edu for:

- IT policies and standards
- C&IT security news feeds
- Broadcast Message Alerts

**Email Phish: "Emergency Notice"** April 23, 2013

Wayne State University has been the recipient of a new email phishing campaign, with numerous staff, faculty, and students reporting the following malicious email being delivered to them. Please review this message and be aware that it is NOT LEGITIMATE and was not sent by Wayne State University. All persons are advised to delete this message immediately if they receive it, and to NOT click on any of the links contained within.

Please note the following characteristics of this latest Phishing attempt:

- The sender's address is NOT from wayne.edu;
- Poor capitalization;
- Different mismatching font sizes;
- Asking you to visit a link that DOES NOT end with wayne.edu;
- Asking you for your login information.

![Phishing Email Example](URL to http://oleans.php5.cz)
How you can help

- Read and adhere to WSU’s Confidential Information Policy
  - computing.wayne.edu/confidential
- **Confidential Information Includes**
  - Social Security number
  - Credit card numbers
  - Bank account numbers
  - Any student information that is not included in the public directory
  - Health information
  - AccessID and password
How your Department can help

- Protecting FERPA information is your responsibility!
- Do not store any confidential information you do not NEED on departmental personal computers, external/removable media and servers
- Departmental personal computers and servers must be properly maintained and administered
- Password protect and encrypt confidential data
- Be aware of Federal technology export control regulations
- Ask for C&IT or external vendor security reviews of existing and new department software systems or servers
C&IT security services

Information Security Officer
- Oversight of divisional security operations
- Monthly cross-division security work group meetings
- IT security incident response plan in-place and exercised
- Regular communications, awareness, online training

Network Security
- Network Firewalls – perimeter, datacenter, server rooms
- Network behavior analytics – Qradar
- VPN network access from remote sites
- Regular Nessus scans for known security vulnerabilities on all computers and servers
- External penetration testing for enterprise systems
C&IT security services

DeskTech
- Antivirus/antispyware/firewall on PC’s and servers
- Full-Disk Encryption for DeskTech Windows computers using Bit Locker
- Administrative privilege role limitations on PC’s

Identity and Access Management
- Complex and expiring passwords
- Creating and maintaining application security profiles
- Deprovisioning access for former employees
Vice Presidents, Deans, and the CIO must write and co-sign letters to every person whose records were potentially exposed – help keep Wayne State, your boss, you and me out of the media spotlight!
Questions?