The Wild, Wild Internet

Cyber Security for Community Colleges

Mark Wilson, CISSP, ITIL, CBCP, CCM
Director of Information Risk Management
Is This the Current State of the Internet?
Security experts say that **OperationUSA**, a coordinated online attack against banking and government websites slated for May 7, is a serious threat. As a result, organizations should be upping their distributed-denial-of-service attack mitigation strategies to guard against the attacks, which are being coordinated by the hacktivist group Anonymous.
Current Statistics

Internet Users in the World by Geographic Regions - 2012 Q2

- Asia: 1,076.7 million
- Europe: 518.5 million
- North America: 273.8 million
- Latin America / Caribbean: 254.9 million
- Africa: 167.3 million
- Middle East: 90.0 million
- Oceania / Australia: 24.3 million

Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group
Current Statistics

World Internet Penetration Rates by Geographic Regions - 2012 Q2

<table>
<thead>
<tr>
<th>Region</th>
<th>Penetration Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>78.6%</td>
</tr>
<tr>
<td>Oceania / Australia</td>
<td>67.6%</td>
</tr>
<tr>
<td>Europe</td>
<td>63.2%</td>
</tr>
<tr>
<td>Latin America / Caribbean</td>
<td>42.9%</td>
</tr>
<tr>
<td>Middle East</td>
<td>40.2%</td>
</tr>
<tr>
<td>World, Avg.</td>
<td>34.3%</td>
</tr>
<tr>
<td>Asia</td>
<td>27.5%</td>
</tr>
<tr>
<td>Africa</td>
<td>15.6%</td>
</tr>
</tbody>
</table>

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,017,846,922 and 2,405,518,376 estimated Internet users on June 30, 2012.
Copyright © 2012, Miniwatts Marketing Group
The Current Threat Landscape

File statistics during last 7 days

- United States of America: 46.2%
- Norway: 18.3%
- Taiwan: 6.9%
- Germany: 9.2%
- Korea: 6.9%
- Canada: 5.5%
- Ukraine: 4.4%
- Russian Federation: 4.4%
- Other: 4.4%
The Current Threat Landscape

Submissions

- Files
- Unique files
- Unique files detected by one engine or more

The Current Threat Landscape

File types

Win32. EXE, PNG, Win32. DLL, Android, HTML, JPEG, ZIP, Text, PDF, RAR, GIF, Java Byte, XML, C, JAR, BitTorrent, Office, WAV, C++, Linux, MS Word, Email, MS Excel, GZIP, Flash, Windows, OGG, PHP.
Organizations on Average Hit Every Three Minutes with Malware
Google, Bing, Yahoo, etc…

Visible Web
Web pages search engines can crawl and index

Invisible Web
Databases
Password-Protected Websites
Federal, State, County & City Public Records
Intranets
Message Boards
Website Archives
Forums
Classified Advertisements
Online Library Catalogs
Etc.
The Darknet

Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

What is Tor?
Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor

Why Anonymity Matters
Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Get involved with Tor
Three Security Pillars

SECURITY – C.I.A.

CONFIDENTIALITY

INTEGRITY

AVAILABILITY
What is Security?

Security Transcends Technology

(ISC)²
International Information Systems Security Certification Consortium

Confidentiality
Integrity
Availability

Data & Services
High Level Security Controls

Physical
- Locks
- Lights
- Fences

Logical (technical)
- Firewall
- Passwords
- Motion Detectors

Administrative
- Policies
- Audits
- Training

Preventive – Detective – Corrective - Compensatory
High Level Security Controls

Preventive – Detective – Corrective - Compensatory
What’s Wrong with Security?

People, Process, and Technology
It’s Not Part of the Equation or Design

#1. It’s NOT fundamental

Security must be part of the fabric of our organizations

#2. It’s not important… enough

Risk < Reward
What’s it Cost?

2013 Annual Cost of Failed Trust Report: Threats & Attacks

The Ponemon Institute’s First Annual Cost of Trust Report reveals that failed key and certificate management threatens every global enterprise with potential cost exposure of almost U.S. $400M.

18% of enterprises expect to fall prey to attacks due to using weak, legacy cryptography over the next 2 years.
Deleting Information?

» Computers
  » Memory
  » Files

1011101000101111 in use
1011101000101111 deleted

» Backups
» Archives
» Cloud backups

…is it ever really gone?
…and we are still building computers this way!
OWASP Top 10

Open Web Application Security Project

» A1 Injection
» A2 Broken Authentication and Session Management
» A3 Cross-Site Scripting (XSS)
» A4 Insecure Direct Object References
» A5 Security Misconfiguration
» A6 Sensitive Data Exposure
» A7 Missing Function Level Access Control
» A8 Cross-Site Request Forgery (CSRF)
» A9 Using Known Vulnerable Components
» A10 Invalidated Redirects and Forwards
US-CERT is aware of an ongoing campaign targeting the content management software WordPress, a free and open source blogging tool and web publishing platform based on PHP and MySQL. All hosting providers offering WordPress for web content management are potentially targets. Hackers reportedly are utilizing over 90,000 servers to compromise websites’ administrator panels by exploiting hosts with “admin” as account name, and weak passwords which are being resolved through brute force attack methods.
National Institute of Standards and Technology

nvd.nist.gov

» National Vulnerabilities Database

» Resource Status

» NVD contains:
  » 56,016 CVE – Common Vulnerabilities & Exposures
  » 209 Checklists – (Security Checklists)
  » 245 US-CERT Alerts - (Computer Emergency Readiness Team)
  » 2,708 US-CERT Vulnerabilities Notes
  » 8,140 OVAL Queries (Open Vulnerability and Assessment Language)

» Last updated: 04/18/13

» CVE Publication rate:
  » 17 vulnerabilities / day
Cyber Intelligence Sharing and Protection Act

» Designed to encourage the public and private sectors to share cyber threat data in real time by removing some of the legal hurdles.

» Opponents of CISPA still say the law doesn’t go far enough to protect citizens’ private data, including emails and financial records, from being misused by law enforcement and by private companies mining data for business intelligence and marketing purposes.
What to Do Next?

Big Ideas:

» Everything changes at scale

» **Change** requires **Change**
What to Do Next?

1. Awareness: We will not be ignorant

2. Mindset: Security is NOT an option

3. Can’t be all things to all people
   » Focus on things that matter to your constituents
   » Consider trusted 3rd parties for the rest

...no risk free environments
Thank You
Questions?
Mark Wilson
mwilson@sikich.com

www.sikich.com