Social Media Security Best Practices

Kurt Garbars, Certified Information Systems Security Professional

GSA Senior Agency Information Security Officer

May 24, 2012

Topics

- Public social media sites (e.g. Facebook)
  - Threats
  - Agency best security practices
- Publically accessible Gov social media sites (e.g. Gov blogs, wikis)
  - Threats
  - Agency best security practices
- Government “internal” social media sites (e.g. Salesforce Chatter)
  - Threats
  - Agency best security practices

Top Threats (public sites)

- Site is compromised with malware
  - Malicious links
  - Malicious files
- Sensitive information is posted
  - Personal information
    - PII (e.g. birthday, address, etc)
    - Vacation times
    - Embarrassing photos or posts
  - Government information that should not be shared
    - Locations (e.g. military)
    - Contract or budget information
    - Building drawings or plans

Agency best security practices (public sites)

- Annual user training
  - –Don’t click on unknown links or requests to download SW updates
  - –Be careful what you post (about yourself, your job, etc)
  - –Assume all your information is public even if you think only your “friends” can see it (privacy settings seem to mysteriously change all the time)
- Secure agency’s computers
  - –NO admin rights on end user workstations
  - –Up to date patching (especially Java, Adobe Flash, Adobe Reader)
  - –Latest hardened /secured browsers (e.g. GPOs/whitelisting extensions)
  - –Application whitelisting (e.g. Windows Applocker, Bit9)
  - –DEP/ASLR (Data Execution Prevention/Address Space Layout Randomization)
  - –Host firewalls/HIPs/File reputation SW

Agency best security practices (cont'd)

- Secure/Monitor agency's networks for malware
  - Examine netflow data for connections to "bad" IPs
  - Examine DNS entries for connections to "bad" URLs
  - Examine IDS/IPS log data for "bad traffic"
  - Implement application layer firewall (e.g. Palo Alto)
  - Use Security Incident and Event Management (SIEM) to correlate and analyze compromises
  - Work with US-CERT in obtaining threat data

Top Threats (pub gov sites)

- Site has been compromised with malware
  - Malicious links
  - Malicious files
- Malicious or derogatory postings by public
- Sensitive information is inadvertently posted

Agency best security practices (pub gov sites)

- Secure government website
  - Monitor for bad uploaded files (antivirus)
  - Application layer web filtering to prevent attacks
  - Harden web site IAW security hardening guides
  - Scan web site for vulnerabilities (e.g. WebInspect)
  - Perform penetration testing of site
  - Source code reviews
- Monitor site for inappropriate postings
  - Postings by public
  - Postings of sensitive data
  - Have website facilitator review all postings before allowing online (only really works for the most sensitive sites)
- Train government employees on what can and can't be posted

Top Threats (Gov “internal” sites)

- Sensitive information is shared with either too many people, the wrong people, or external people

Agency best security practices (Gov “internal” sites)

- Set up strong policies/procedures on posting and sharing information
  - Rules of behavior for group owners
  - Especially for use with external partners
  - Monitor postings and access control lists
  - Enforce 2-factor authentication as required
- Train government employees on what can and can’t be posted, shared, etc.