
Software QA/ Cyber Security Session Report

Brief on Cyber Security Event at JLab
Bob May, Deputy ESH&Q

Accelerator Safety Workshop 2011
Sept. 20- 22, 2011
Argonne National Lab

Cyber Security Event

- Primer
- Description of JLab Event and Timeline
- Follow-up steps
- Take-home lessons

Primer

- Cyber attacks typically result in loss of:
 - confidentiality
 - data integrity
 - availability of services
- E-mail phishing has highest success rate
 - you can access a large number of people relatively inexpensively
- Advertising
 - Sending out infected educational materials, CDs, memory sticks
- Zero-day vulnerabilities
 - Vulnerabilities that are unknown to the user or even the software developer

Description of Event and Time-line

- Attack
 - Mid-April: attack initiated across multiple DOE sites
 - May 24: two externally facing JLab web-servers compromised
 - Five weeks of recon by attackers
 - June 28: attackers return and elevate privileges
- Discovery and protection
 - June 30 AM: attack detected
 - June 30: blocked selected Internet traffic; enhance monitoring; launch analysis
 - July 1: block all internet access except e-mail
 - Safety and physical security systems not impacted; most on-site IT systems operational

Description of Event and Time-line, cont'd.

- Analysis and recovery
 - July 2: develop an understanding of initial event
 - July 2 & 3: turn a year-and-a-half of “shovel ready” security enhancement projects into a 5-8 day activity
 - July 3-5: launch recovery activities
 - July 6-15: created external website; created a new Windows Domain; changed all passwords; reissue “smart cards”; general internet access online
 - July 16-29: most web services online
- During all of this, the safety and physical security systems were not impacted; most on-site IT systems remained operational

Follow-up Steps

- Implemented additional cyber security enhancements during the 6-month shutdown
 - Least privilege administrative access (limited only to what you need)
 - Web access via a proxy with white list and dedicated terminal servers
 - Removed direct Internet access from operations computers
 - Highly segment networks: adds complexity
- Recent review of enhancements
 - Self-assessment to review changes
 - Two reviews by CSC (JSA Partner)

Take-home Lessons

- Guiding design principles:
 - Prevention has not worked for “connected systems”
 - No longer “how do we keep them from getting in” but assume there in and provide lots of opportunity for trip-up and detection
 - Focus on detection and eradication
 - Layered defense-in-depth (important stuff is buried beneath layers – adds hurdles for malware to trip on and be detected)
 - Disconnect or “air gap” certain systems (no direct access between Ops and Internet)
- Everyone wants security, ease of functionality, performance
 - Pick two!