Cyber Security Update

Recent Events in the Wild

and

How Can We Prepare?

Bob Cowles

August, 2011
DOE Labs Hacked!

- ORNL off the Internet for nearly 2 weeks – extensive remediation efforts put into place.
- JLab went off the Internet on June 30. Rebuilt infrastructure and desktops. Offline for two weeks.
- PNNL went off the Internet on July 1. Like Jlab, offline for two weeks.
What Happened?

- Attackers found vulnerabilities
  - Phishing
  - Unpatched web application
  - Unpatched desktop application
- Used architectural “feature” to take control of the infrastructure
- The feature is common across operating systems in wide use at SLAC
What Were They After?

- Currently, lots of groups are looking for documents; many corporations and government entities are under attack
- Same group attacked PNNL and JLab
- ORNL attack might have been different
- Possible help that SLAC is not a “.gov” site

“Every year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies.”

DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE
Could It Happen At SLAC? – YES!

- Vulnerable web applications
- Widespread use of elevated privileges
- Unpatched systems and applications
  - Even centrally managed systems have over 1000 unique applications that need to be kept up-to-date
- Differently managed systems
  - Various flavors of Linux (Fedora, Ubuntu, Debian)
  - Macs (600+ on-site with no official support)
    - Major vulns in past 3 years Mac: 1,151; Win 1,325
  - Laptops (especially Linux and Macs)
  - Smartphones and tablets
- Lab culture –
  - Cyber security is not my problem
  - My system is too critical to be scanned / patched
  - The border firewall protects my system
  - “I use antivirus” or “I have a Mac”, so I’m safe
What Would We Have To Do?

• Segregate computing resources (re-architect entire network)
  – Infrastructure, Business, Controls, PPS
  – Multiple scientific subnets (to control lateral movement of attackers)
• Rebuild all affected servers and desktops
• Recovery operations only after “cleaning” verified successful
  – Safety systems
  – Dependencies
  – Mission importance
  – Critical projects
• Review/remove privileges
  – admin, root, sudo
  – No one outside of infrastructure services has admin privileges
• Change ALL passwords (internal and external users)
• Redesign and lock down remote access
Protections (Current)

- Blocking “bad” sites using “federated model”
  - Attacking IP addresses shared between DOE labs
- Vulnerability scanning (expanding to more systems)
- Extensive patching (systems and 3rd party applications)
- AntiVirus alerts and additional AntiVirus scanning (about 50/month – 200-300 hours of lost time)
- Training (new employee/manager, annual)
- Lots of time-consuming, manual processes
Protections (In process)

- Web proxy – help to block bad sites and malware (hope to reduce AV time lost)
- Alerts from log analysis to give earl(ier) warning of attack in progress
- More training to heighten awareness of the ever-changing attack vectors
- Increased emphasis on patching to catch up and stay current in the future
Protections (To Do)

• Define recovery plan including data classification
• Policy (and implementation) on removing elevated rights
• Re-architecture of network with appropriate boundaries / levels of access
• Perform current web application assessment plus incorporate security into application design and test
• Develop and implement appropriate controls on non-centrally managed systems (incl. internal, visitor, home)
• Macintosh support
• Lifecycle budgeting and planning
• Mobile devices (policy and implementation)
What You Can Do Now

• No web browsing or email (or external devices) when logged in with admin rights

• Remote access
  – Reconsider the balance between convenience and safety
    • Unmanaged home computers
    • Smartphones / tablets with unknown other applications
  – Institute safeguards to limit potential damage

• Start thinking about the priority and steps for recovery and continuing operation when a cyber attack occurs
  – What’s critical/important/wait for later?
  – What are the dependencies?
The New World of Risk Management

- DOE now describes a Risk Management Framework for cyber security – incorporated into the Contractor Assurance System
- Cyber Security can provide suggestions and help management to understand threats
- Management (at all levels) must determine appropriate protections (balancing cost & benefit) and accept the residual risk
Information Security Prayer

Grant me the **serenity** to accept people who will **not** secure their systems;

The **courage** to face them when they blame me for their problems; and

The **wisdom** to go out drinking afterwards.