Cyber Exploits: Improving Defenses Against Penetration Attempts

Mark Burnette, CPA, CISA, CISSP, CISM, CGEIT, CRISC, QSA
LBMC Security & Risk Services
Today’s Agenda

• Planning a Cyber Defense Strategy
  – How should I start?

• 5 Frequent Attack Targets/Vectors
  – What should I consider?
  – Countermeasures & Defenses

• Summing It Up
  – Wait, what? One more time!
Planning A Cyber Defense Strategy

In order to implement proper defenses, you must:

• Identify the potential targets (asset inventory)
  – Data (PII, PHI, CHD, intellectual property, etc.)
  – Systems (End user PC’s, servers, etc.)

• Assess the risk to each target
  – Consider effectiveness of existing controls
  – Likelihood X Impact = Risk

• Evaluate the organization’s risk appetite
  – Many factors can impact risk acceptance or mitigation

• Manage risk to an acceptable level
  – Deploy defenses to address the biggest risks
  – Fully eliminating risk is unreasonable in most cases
Identify The Target(s)

• Create or update an inventory of systems and data
  – Seek to know tomorrow what you don’t know today

• Ensure sensitive data and critical systems are properly labeled
  – Consider any compliance obligations (HIPAA, PCI, etc.)
  – This helps users and operators understand their obligations
Assess The Risks

• There are many risk assessment methodologies available to help with this

• Most important: Do something!
  – Ignorance is not an acceptable defense
  – Ambivalence can be a warning sign

• Consider your weaknesses
  – Controls can offset some risk exposure

Here’s a look at some common weaknesses/exploits, and how to defend against them....
The Evolution of Attacks

• Today’s threats have evolved as defenses have evolved
  – Firewalls and operating systems are more secure
  – Many organizations have basic protections in place
  – Many targets of attack have moved outside the traditional network perimeter

• Many hacking tools are freely available

• Hackers have unlimited time to execute an attack

• If the “low hanging fruit” isn’t easily accessible, they try new vectors
Weakness 1: Endpoint Attacks

• O/S patching is better, but still often lacking
  – Windows XP
  – Inadequate asset management (remember that asset inventory?)

• Third party software is often overlooked by IT departments, presenting an attack vector
  – Adobe Reader
  – Java (Active Content)
  – Internet Browsers (Chrome, Firefox, IE, etc.)

• The attacker may deliver a malicious payload or entice a user to visit a website
  – Code runs with the user’s privileges
  – Website can install a “hook” onto the target computer
  – Windows computers may provide password hash
While nothing can be done to completely prevent these types of attacks, there are several things that can reduce an organization’s susceptibility, including:

- Spam filter, with sensitivity turned up
- Strong “egress” filters on the network
- Up to date anti-virus/malware on EVERY endpoint
- Network intrusion prevention capabilities (with threat intelligence)
- Remove local administrator rights on workstations
- Require IT admins to use separate accounts for supporting servers
- Security awareness training for all personnel

Two-factor authentication is one of the most effective defenses against remote user account attacks.
Weakness 2: Application Based Attacks

As organizations have gotten better at hardening networks and operating systems, attackers have turned to applications for new attack vectors

- Error handling
- Cross-site scripting
- Buffer overflows
- SQL Injection
Application Security Countermeasures

- Develop application coding standards that include security considerations
  - OWASP, SafeCode Principles, security API
- Integrate secure coding requirements into SDLC
- Include security checks/testing in QA process
  - Peer reviews if necessary
- Train developers in secure coding techniques
- Hold third party developers accountable for secure coding techniques
  - Contract provisions, independent validation reports
- Conduct routine application security testing and remediate
  - Dynamic
  - Static
Weakness 3: Third Party Security

• Third parties are a very common vector of attack and vulnerability
  – They do not necessarily enforce the same level of security on your data that you do
  – Many third party agreements are codified between business people with minimal security acumen or awareness

• Data that is stored “in the Internet” on service provider’s systems must be secured
  – Salesforce.com, Amazon AWS, Dropbox, Box.com, Sugar Sync, etc.
  – Users may be using these services today to store sensitive data

• Once data leaves your control, it is difficult to protect it

• Many regulations require companies to enforce security measures on third party providers
Third Party Security Countermeasures

• Create a policy governing the use of cloud-based services
  – ID & label sensitive data, and encrypt before uploading if possible
  – Train users to understand their responsibilities and acceptable use

• Develop and maintain an inventory of third party providers
  – Seek to know tomorrow what you don’t know today

• Where possible, use contract language to require adequate security measures be enforced by the service provider and include penalties for non-compliance
  – Require a security sign-off in project management process & legal review
  – Require third parties to provide or cooperate with a security assessment annually

• Periodically re-assess risks related to third party providers and adjust program accordingly
Weakness 4: Mobile Device Security

- The capabilities of today’s mobile devices and the lack of robust built-in protections makes them a common target
  - The issue is much greater than the device just being lost or stolen
  - Mobile devices are typically outside the network’s secure perimeter
- Sensitive data on the devices is the target
  - E-mail, accessible cloud services, “side loaded” data, or corporate apps may all have interesting data
- Current mobile device attacks are difficult to detect
- Users may be using devices not approved or provisioned by the company
  - OWA may allow connections
  - Users may sync sensitive data without organization’s knowledge
Three primary considerations for mobile devices:

• Security related to physical control of the device
  – Password/PIN, device lock, ability to wipe memory

• Security of the services used to transmit data to/from the device
  – Encryption of transmissions across networks
  – Patched servers

• Securely coded applications that are used on the device
  – Input sanitization checks within application
  – Use of standard API’s for mobile app development
  – Perform a security audit of any application that will be used to store, process, or transmit sensitive information
    • Dynamic and static testing
Mobile Device Countermeasures

• Create a mobile device security policy
  – Address stance on BYOD
  – Require PIN/password, encryption, device locking
  – Train users on their responsibilities

• Enforce restrictions on mobile device connections whenever possible
  – OWA lockdown
  – Create a separate wireless network for guests and devices
  – Maintain a list of approved mobile devices (hello, asset inventory!)
  – Third party software tools can also help enforce restrictions

• Restrict downloading of non-approved apps to devices that have sensitive data
  – Even App Store apps may steal data
Weakness 5: Passwords

- Passwords remain the most widely-used authentication mechanism to a private computer environment
- Provides user accountability
  - Proves that the user is who she says she is
  - Protects the user and the company
- Provides access to the company’s sensitive information
  - Authorization

As long as passwords are the primary method of authentication to an IT system, companies will struggle to effectively protect data.
Password Security Countermeasures

• Require regular password changes (at least every 90 days)
• Use at least 7 character minimum length
• Require strong passwords (letter, number, spec. char.)
  – Train users in good password selection techniques
  – Easy to remember, difficult to guess
  – Example of the perfect password: Y@ms,M0s
• Enforce account lockouts after 5 bad login attempts
• Change default passwords on all systems
• “Harden” computer systems using industry standards
  – Windows LANMAN authentication is easy to crack
• Educate users to use unique passwords for each online site
• When possible, use strong (multi-factor) authentication
How Can A Company Reduce Security Breaches?

- Identify, inventory, and label sensitive data and systems
  - Know what you have

- Develop and implement system hardening guidelines
  - Change default passwords, restrict running services
  - Patch ALL computer systems (Don’t forget third-party patches)

- Develop & implement robust security policies & standards
  - Secure coding standards

- Educate employees on security risks
  - Awareness training

- Monitor the environment
  - Intrusion detection, log review, FIM, etc.

- Periodically evaluate controls and security
  - Risk assessments, penetration testing, “current state” assessments
Thanks, and Stay Secure!

Mark Burnette, CPA, CISSP, CISM, CRISC, QSA
mburnette@lbmc.com
(615) 309-2447

www.lbmcsecurity.com