

Security Auditing and Security Design

Karl Fox and Ron Kellogg
Lithik Systems, Inc.

What is an Internal Auditor Required to Know?

- You must be able to demonstrate that your IT systems comply with FFIEC guidelines
 - Monitoring—If something goes bump in the night, will someone be notified?
 - Defense in depth—Multiple layers of protection defend against even persistent attackers
 - Good passwords—Passwords don't have to be hard! Learn how!
 - Patches—Missing patches are the #1 vulnerability exploited by hackers
 - Architecture—Networks are not usually designed for either security or compliance
 - Good inventory—This is the foundation of any automated security system
 - Reporting—Compliance requires regular documentation of all the above

The Hacker Economy

- Hackers are now an entire worldwide black market economy unto themselves
 - Technology specialization
 - Product development, including research, development and testing
 - Online hacker stores and eBay-like markets
 - Dynamic, stratified, distributed, scalable, efficient and highly effective

Malware Trends

- The U. S. Secret Service reports that, although insider attacks are up 26% over last year, 96.5% of all stolen customer records occurred through external attacks*
- 95% were attributable to malware
- 80% involved malware explicitly designed to provide remote access to the hacker

* Source: Verizon *2010 Data Breach Investigations Report*

Drive-by Downloads

- Hacker penetrates a legitimate web site and installs an exploit script
 - The Google Anti-Malware Team recently found *3 million* such sites
- Hackers exploit search engines to position hacked sites high in search results
- Exploit scripts “exploit” vulnerabilities (often published vulnerabilities) in
 - Apple QuickTime Player
 - Adobe Flash Player
 - Adobe Reader
 - RealPlayer
 - WinZip
 - Specific browsers
- Browsing to such a web site *using a vulnerable web browser* automatically installs malicious software on your computer

Defenses Against Drive-by Downloads

- Modern web browsers include malware-blockers
 - Blacklist-based
 - Most infected web sites only stay infected for a day or two
- Most attacks target published vulnerabilities
 - *Keep your systems patched!*
- HIPS (Host Intrusion Prevention System) features of anti-virus systems can help block drive-by downloads
- Web whitelisting can be highly effective against such attacks
- Web proxy filtering can be highly effective against such attacks
- Software whitelisting is 100% effective against such attacks

Obstacles to Good Security Architecture

- Malware strategy is advancing faster than best practices defensive strategy
- Changing your network architecture can be
 - Highly disruptive
 - Expensive
 - *A huge job!*
- The security industry loves the Band-Aid approach
 - *Buy a box, feel secure*
- Most IT professionals *and most IT security professionals* are still solving yesterday's problems using yesterday's solutions

Little Known Facts of the IT Security Trade

- Bigger is not always better— Big 8 type companies seldom provide a quality security audit
- Good IT audits come only from people and companies who specialize in IT security and have done many audits
- Don't use the same audit firm more than two years in a row
- A pen test is not an audit
- Good passwords are *easy*—if you know how
- Most security problems can be corrected quickly, easily and cheaply
- Simple and relatively inexpensive architectural changes can *drastically* improve your security

A Simplified Proxy-Based Security Architecture

- Route all inbound e-mail through a filtering service
- Route all outbound web traffic through an authenticating, filtering web proxy
 - *Now all outbound traffic goes to predictable destinations*
- Configure your firewall to allow traffic to all your predictable destinations
 - E-mail and web proxies
 - Anti-virus updates, software updates
 - DNS, NTP, FTP, banking applications
- Block all outbound TCP, UDP and ICMP traffic to *all other destinations* and ***ALARM ON ALL VIOLATIONS***

What To Expect From Your IT Provider

- A spirit of cooperation—no territorialism or turf protecting
- Forward thinking about future improvements in architecture, software, and security equipment
- A monitoring and reporting system managing critical aspects of network security, including
 - Missing patches for Windows, Office and third party applications
 - Anti-virus status, including infections and coverage
 - Policy violations detected by the monitoring system or the firewall
 - Firewall configuration, including globally allowed outbound ports

The Future

- Cloud computing—It's not ready for you yet, but it *will* be
 - All servers, desktops and applications run on computers in a secure data center
 - Customer Premise Equipment includes thin clients, printers and network equipment
 - A mail and web proxy based security architecture protects against malware
 - Dynamically created (short lived) Windows desktop instantiations are “malware shedding”
 - Disaster recovery and backups are completely automated
 - Last mile bandwidth requirements are lower and more predictable
 - Support for a wide variety of mobile devices is automatic and simple

<http://www.lithik.com/blog>

Karl Fox <karl@lithik.com>

Ron Kellogg <rkellogg@lithik.com>

614-890-0026