



**Information
Technology
Security**

March 2010
Paul Rainbow CPA, CIA, CISA
IT Auditor/Consultant
paul.rainbow@mossadams.com

MOSS-ADAMS_{LLP}



The Current IT Security Environment

Today's IT Security environment is very complex and constantly changing. Although the technical aspects of the attacks change daily, the basic concepts and controls to prevent them remain fundamentally unchanged.

Agenda

- General IT security trends
- Financial Institution specific trends
- Review controls that can address these threats and ways to audit and monitor these areas
- Incident Response (Time Permitting)

3

SANS Top 10 Security Trends

1. Mobile Devices – Laptops
2. Mobile Devices – PDA/Smart Phones
3. Government Action (Regulation)
4. Targeted Attacks – Government and Commercial
5. Targeted Attacks – Cell Phones
6. Targeted Attacks - Voice over IP (VoIP)
7. Attack Techniques – Spyware
8. Attack Techniques – 0-Day Vulnerabilities
9. Attack Techniques – Rootkits
10. Defensive Strategies – Network Access Controls Sophistication

4

Mobile Devices

Laptops

- Large increase in use as prices drop and the workforce becomes more mobile
- Loss of data from theft (high value target)
- Encryption may become mandatory (especially for systems containing customer or patient data)

PDA/Smart Phones

- Increase of use by both individuals and employees
- Increase in theft due to value of hardware
- Increased volume of valuable data storage (which will also push the increase in theft)

5

Government Action

- Additional increase in legislation over the protection of customer information
- Changes in the state imposed data breach notification requirements
- Harsher penalties for the loss of sensitive personal information

6

Attack Targets

Attacks will be much more targeted

- Government agencies will be targeted
- Military contractors will be targeted
- Businesses with valuable customer information (Financial Institutions!)

Cell Phones

- Becoming more powerful tools (with full-featured operating systems)
- Cell phone worms will jump over wireless data networks

VoIP

- Technology was deployed quickly before fully understanding the security concerns

7

Attack Techniques

Spyware

- Can be a very profitable business
- Is being developed and distributed all over the world

0-Day Vulnerabilities

- Outbreaks result in thousands of infected PCs worldwide
- Some security researchers use exploits they find before selling them to vendors like TippingPoint

Rootkits

- Used to develop Botnets
- Hide the attackers presence
- Almost impossible to remove without a completely new install of the entire operating system

8

Defensive Strategies

- Network Access Controls will become much more sophisticated
- Internal networks will protect themselves from systems connecting from the outside
- Networks will evaluate new systems with deeper analysis, searching for traces of malicious code before allowing them on the network

9

Top Security Threats for Financial Institutions

1. Organized Crime
2. Authentication
3. Malware
4. Telephone Fraud
5. Insiders
6. Mobile Devices
7. Social Media
8. SQL Attacks

(based on the Dec 21, 2009 Article "Top 8 Security Threats of 2010" by Linda McGlasson)

10

Organized Crime (1)

- Significant increases in Organized Crime's involvement in attacks on Financial Institutions in recent years
- Many criminal organizations are now hiring and grooming hackers and technology professionals in order to expand and advance their abilities to perpetrate more complex and advanced fraud

11

Organized Crime (2)

- There are significant challenges to dealing with Organized Crime
- Many crime organizations are run out of eastern European countries
- Trying to recover funds or get information in a foreign country can be almost impossible

12

Organized Crime & Online Banking (1)

We have seen a significant increase in the attacks on financial institutions via online banking.

- Criminals are using trojans and keystroke loggers to obtain users online banking credentials
- Those credentials are then used to access online accounts and use ACH or wires to transfer funds

13

Organized Crime & Online Banking (2)

- Funds are transferred to intermediaries here in the U.S. before being transferred to other countries
- These “intermediates” are recruited via local ads in newspapers and online as “work from home” opportunities
- These individuals are tasked with receiving the money, keeping a small portion for their work, and transferring the rest out of country
- Often times they are naïve and do not understand that they are committing crimes

14

Organized Crime & Online Banking (3)

It is almost impossible to prevent this type of fraud because the criminals have valid user credentials. What are you doing to control the risk in this area?

One thing that can be done is to evaluate your online banking agreements to ensure that the user's obligation to secure their account credentials is stated and that they will incur liability for funds lost based on their negligence.

15

Sample wording for online banking (1)

Your access code (password) and online banking user ID are issued to you for security purposes. The access code and online banking user ID are confidential and should not be disclosed to third parties. ***You are responsible for safekeeping your online banking user ID and access code. You agree not to disclose or otherwise make your online banking user ID or access code available to anyone not authorized to sign on your accounts. If you authorize anyone to use your access code, their authority shall continue until you expressly revoke such authority by notifying us.*** If you fail to maintain the security of your online banking user ID or access code and we suffer a loss, we may terminate your online banking account services immediately.

16

Sample wording for online banking (2)

Any person having access to your online banking user ID and access code will be able to access your accounts through the online banking service and perform all transactions, including reviewing account information and making transfers to other accounts and to other persons. ***You agree that we will not be responsible for any loss incurred as the result of any person becoming aware of your online banking user ID or access code. You are responsible for all transfers, bill payments, or other transactions authorized by you or by any person who accessed your account due to your negligence.*** Additionally, you are responsible for any transactions by persons you authorize to use your account(s).

17

Authentication

- Regulatory requirements have boosted the use of multi-factor authentication
- This has led to the aggressive attack of authentication by more technical means
- Hackers are now using Trojan kits to enable them to use the customer's browser to collect authentication credentials or send money in real time

18

Malware

- Malware infection was 10 times higher in 2009 than 2008
- Fraudsters are using social networks and social engineering to spread their malware
- The malware is becoming higher quality
- Malware development is being funded by organized crime groups

19

Telephone Fraud

- As financial institutions enhance their online security, the criminals are changing their avenue of attack
- Information collected through trojan programs or through social engineering (phishing, spear phishing, or smishing) is used
- Criminals are outsourcing the actual calls to Russia and often times use Caller ID spoofing to help the fraud to appear more genuine

20



Insider Threat

- The struggling economy may cause an increase in internal fraud due to financial pressure and desperation
- Employees not receiving raises or bonuses
- Terminated employees (or other disgruntled staff)
- Contractors, seasonal, or part time workers

21



Mobile Banking

- Greater numbers of institutions offering mobile banking to customers
- Greater use of smart phones and mobile devices
- Mobile banking moving from just checking balances to actual account control and transactional abilities
- Cell phones being targeted for worms and viruses

22



Social Media

- Easy way for criminals to gather intimate details about customers to use in fraud
- Easy way to send malware or trojans to a large group of people from a “trusted” friend
- New frontier for phishing and social engineering attacks

23



SQL Attacks

- The largest data breach on record was SQL Injection (Heartland Payment Systems)
- Websites are becoming a target for criminals to gain access to systems and collect customer data
- The web browser is becoming the favored attack vector as well as attack tool
- With fewer operating system vulnerabilities, attack are moving to applications and the web

24

Top 20 Critical Controls (1)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs

(based on SANS Twenty Critical Controls for Effective Cyber Defense)

25

Top 20 Critical Controls (2)

7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services

26

Top 20 Critical Controls (3)

14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

27

Inventory of Authorized and Unauthorized Devices

- Deploy an automated asset inventory discovery tool and use it to build a preliminary asset inventory of systems connected to the enterprise network.
- Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine names, purpose of each system, an asset owner responsible for each device, and the department associated with each device.
- Ensure that network inventory monitoring tools are operational and continuously monitoring, keeping the asset inventory up to date on a real-time basis.

28

Inventory of Authorized and Unauthorized Devices - Testing

To evaluate the effectiveness of automated asset inventory tools, periodically attach several hardened computer systems not already included in asset inventories to the network and measure the delay before each device connection is disabled or the installers confronted.

29

Inventory of Authorized and Unauthorized Software

- Devise a list of authorized software that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses.
- Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level.

30

Inventory of Authorized and Unauthorized Software - Testing

To evaluate the effectiveness of automated software inventory tools, periodically install several software updates and new packages on hardened control machines in the network and measure the delay before the software inventory indicates the changes. Such updates should be chosen for the control machines so that they do not negatively impact production systems on the network.

31

Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

- System images must have documented security settings that are tested before deployment, approved by an agency change control board, and registered with a central image library for the agency or multiple agencies.
- Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system.
- Any deviations from the standard build or updates to the standard build should be documented and approved in a change management system.

32



Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers - Testing

At least once per month, run assessment programs on a varying sample of systems to measure the number that are and are not configured according to the secure configuration guidelines.

33



Boundary Defense

- Organizations should deny communications with known malicious IP addresses (blacklists) or limit access to trusted sites (whitelists).
- Define a network architecture that clearly separates internal systems from DMZ systems and extranet systems.
- Organizations should devise internal network segmentation schemes to limit traffic to only those services needed for business use across the internal network.
- Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

34

Boundary Defense - Testing

Periodically, test packets from blocked source IP addresses should be sent into the network to verify that they are not transmitted through network perimeters. Lists of bad addresses (unroutable or otherwise unused IP addresses) are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.

35

Maintenance, Monitoring, and Analysis of Audit Logs

- Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis.
- System administrators and security personnel should devise profiles of common events from given systems, so that they can tune detection to focus on unusual activity and avoid false positives.
- All remote access to an internal network, whether through VPN, dial-up, or other mechanism, should be logged verbosely.
- Operating systems should be configured to log access control events associated with a user attempting to access a resource without the appropriate permissions.

36

Maintenance, Monitoring, and Analysis of Audit Logs - Testing

Organizations should periodically test the audit analysis process by creating controlled, benign events in logs and monitoring devices and measuring the amount of time that passes before the events are discovered and action is taken. Ensure that a trusted person is in place to coordinate activities between the incident response team and the personnel conducting such tests.

37

Critical Logs to Review

- 1. Attempts to Gain Access through Existing Accounts**
- 2. Failed File or Resource Access Attempts**
- 3. Unauthorized Changes to Users, Groups and Services**
- 4. Systems Most Vulnerable to Attack**
- 5. Suspicious or Unauthorized Network Traffic Patterns**

(from SANS Top 5 Essential Log Reports)

38

Controlled Use of Administrative Privileges (1)

- Before deploying any new devices in a networked environment, organizations should change all default passwords to a difficult-to-guess value.
- Organizations should configure all administrative-level accounts to require regular password changes on a 30, 60, or 90 day interval.
- Organizations should ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis.

39

Controlled Use of Administrative Privileges (2)

- Through policy and user awareness, organizations should require that administrators establish unique, different passwords for their administrator accounts and their non-administrative accounts.
- Organizations should configure operating systems so that passwords cannot be reused within a certain time frame.
- Passwords for all systems should be stored in a hashed or encrypted format.
- Organizations should ensure that administrator accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet.

40

Controlled Use of Administrative Privileges (3)

- Organizations should configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators group.
- All administrative access, including domain administrative access, should utilize two-factor authentication.
- Administrators should be required to access a system remotely using a fully logged and non-administrative account. Then, once logged in to the machine without admin privileges, the administrator should transition to administrative privileges using tools such as “sudo” on Linux or “runas” on Windows

41

Controlled Use of Administrative Privileges - Testing

Organizations should implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

- Built-in operating system features can extract lists of accounts with superuser privileges, both locally on individual systems and on overall domain controllers.
- To verify that users with high privileged accounts do not use such accounts for day-to-day web surfing and e-mail reading, security personnel could periodically gather a list of running processes in an attempt to determine whether any browsers or e-mail readers are running with high privileges.

42

Dumpsec

Tool for obtaining detailed information from Domain Controllers regarding policies, users, groups, rights, and services.

The IT Audit group at Moss Adams has done additional scripting to further enhance the use of this product and obtain easy to use reports that contain the critical data needed for reviewing users and security policies in Windows environments

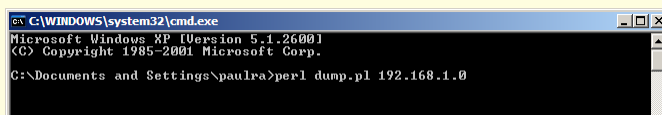
43

Dumpsec Execution

- The program can be run from the command line of any system that has domain administrator rights. You can run it based on the name of the domain controller or IP address.



```
ev C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\paulra>perl dump.pl DomainController1
```

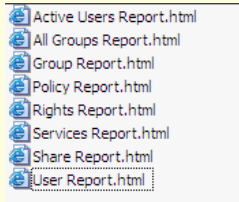


```
ev C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\paulra>perl dump.pl 192.168.1.0
```

44

Dumpsec Report List

- The scripted Dumpsec creates the list of html reports listed below:



45

Group Report

The Group Report provides a list of users that have high level privileges (Administrators, Domain Administrators, etc).

Group Report			
Generated on: 10/13/2009 10:00:28 AM			
<i>This report shows all high profile groups on all servers.</i>			
Group	Comment	User Name	Server
Account Operators	Members can administer domain user and group accounts	IT Admin GG	
Administrators	Administrators have complete and unrestricted access to the computer/domain		

46

Policy Report

The Policy Report provides the main security policies and their current settings for the network

Policy Report	
Generated on: 10/13/2009 10:00:28 AM	
<i>This report shows all policies on all servers.</i>	
Policies	Server
Account Policies	11
Min password len: 8 chars	11
Max password age: 60 days	11
Min password age: 5 days	11
Password history: 10 passwords	11
Do not force logoff when logon hours expire	11
Lockout after 3 bad logon attempts	11
Reset bad logon count after 300 minutes	11
Lockout duration: 10080 minutes	11

47

User Report

The User Report contains a number of lists that are critical to monitoring access to the network. They include:

- All user accounts that are active with passwords that cannot be changed
- All user accounts that are active and do not require a password
- All user accounts that are active and do not expire
- All user accounts that are currently disabled
- All user accounts that are active and have logon hour restrictions
- All user accounts that are active and have not been logged on to for more than 3 months

Password Can Be Changed Report			
Generated on: 10/13/2009 10:00:28 AM			
<i>This report shows all user accounts that are active with passwords that cannot be changed.</i>			
User Name	Full Name	Password Can Be Changed	Server
Account Analysis>Main	Account Analysis Maintenance - CA/OR/WA	No	G:\Dumpsec\users_...tsv

48

Controlled Access Based on Need to Know

- Organizations should establish a multi-level data identification/separation scheme (data separated into categories based on the impact of exposure of the data).
- Organizations should ensure that file shares have defined controls to specify that only “authenticated users” can access the share.
- Organizations should enforce detailed audit logging for access to non-public data and special authentication for sensitive data.

49

Controlled Access Based on Need to Know - Testing

Periodically, security or audit personnel should create a standard user account on file servers and other application servers in the organization. Then, while logged into that test account, authorized personnel should examine whether they can access files owned by other users on the system, as well as critical operating system and application software on the machine.

50

Account Monitoring and Control (1)

- Review all system accounts and disable any account that cannot be associated with a business process and business owner.
- Systems should automatically create a report on a daily basis that includes a list of locked out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire.
- Organizations should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.

51

Account Monitoring and Control (2)

- Organizations should regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
- Organizations should monitor account usage to determine dormant accounts that have not been used for a given period, such as 30 days, notifying the user or user's manager of the dormancy. After a longer period, such as 60 days, the account should be disabled.
- On a periodic basis, such as quarterly or at least annually, organizations should require that managers match active employees and contractors with each account belonging to their managed staff.

52

Account Monitoring and Control - Testing

A test account should be created, with very limited privileges so that it cannot access anything except public files on a system. No user should log into this test account. Any login activity to this test account should be investigated immediately. Automated software should check to ensure that the system generates a notice about such a test account after 30 days of non-use. Furthermore, an automated script should verify that the account has been disabled 60 days after the account was first created, notifying security personnel if the account has not been automatically disabled.

53

Malware Defenses

- Organizations should monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, anti-spyware, and host-based Intrusion Prevention System functionality.
- Organizations should employ anti-malware software and signature auto update features or have administrators manually push updates to all machines on a daily basis.
- Organizations should configure laptops, workstations, and servers so that they will not auto-run content from “thumb drives”, USB hard drives, CDs/DVDs, or other removable media.
- Organizations should configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

54

Malware Defenses - Testing

To verify that anti-malware solutions are running, organizations should periodically introduce a benign, non-spreading test case, such as the EICAR anti-virus test file, onto a system in the environment to ensure that it is detected by the antimalware system, and that the detection is reported to the enterprise anti-malware management system.

55

Wireless Device Control

- Organizations should ensure that each wireless device connected to the network matches an authorized configuration and security profile.
- Organizations should ensure that all wireless access points are manageable using enterprise management tools. Access points designed for home use often lack such enterprise management capabilities, and should therefore be avoided in enterprise environments.
- Network vulnerability scanning tools should be configured to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points.

56

Wireless Device Control - Testing

- Security personnel could periodically activate an isolated wireless access point, which has no physical or wireless connectivity to a production network. The team should determine whether the alerting system is triggered by the test access point, and record the amount of time such detection required.
- Additionally, the security team could periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organization mandates.

57

Data Loss Prevention

- Organizations should deploy approved hard drive encryption software to laptop machines that hold sensitive data.
- Network monitoring tools should analyze outbound traffic looking for a variety of anomalies, including large file transfers, and possibly the presence of certain keywords in the data traversing the network perimeter.
- Deploy an automated tool on network perimeters that monitors for certain Personally Identifiable Information (PII), keywords, and other document characteristics to determine attempts to transfer data in an unauthorized fashion.

58

Data Loss Prevention - Testing

Free tools are available that will attempt to obtain password hashes or reset the local administrator password (by booting from a CD) on a system. Hard drive encryption should prevent these tools from functioning properly and should not allow them obtain passwords (or even recognize that there is an operating system installed on the drive).

59

Thank You



Disclaimer

The material appearing in this presentation is for informational purposes only and is not legal or accounting advice. Communication of this information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although these materials may have been prepared by professionals, they should not be used as a substitute for professional services. If legal, accounting, or other professional advice is required, the services of a professional should be sought.