



IFDA
International foodservice
distributors association



Systems Security

Welcome

#706 8:00am-9:00am
Tuesday, October 9th, 2007





Systems Security - Agenda

- Intro/Video
- Risks
- Authentication
- Wireless

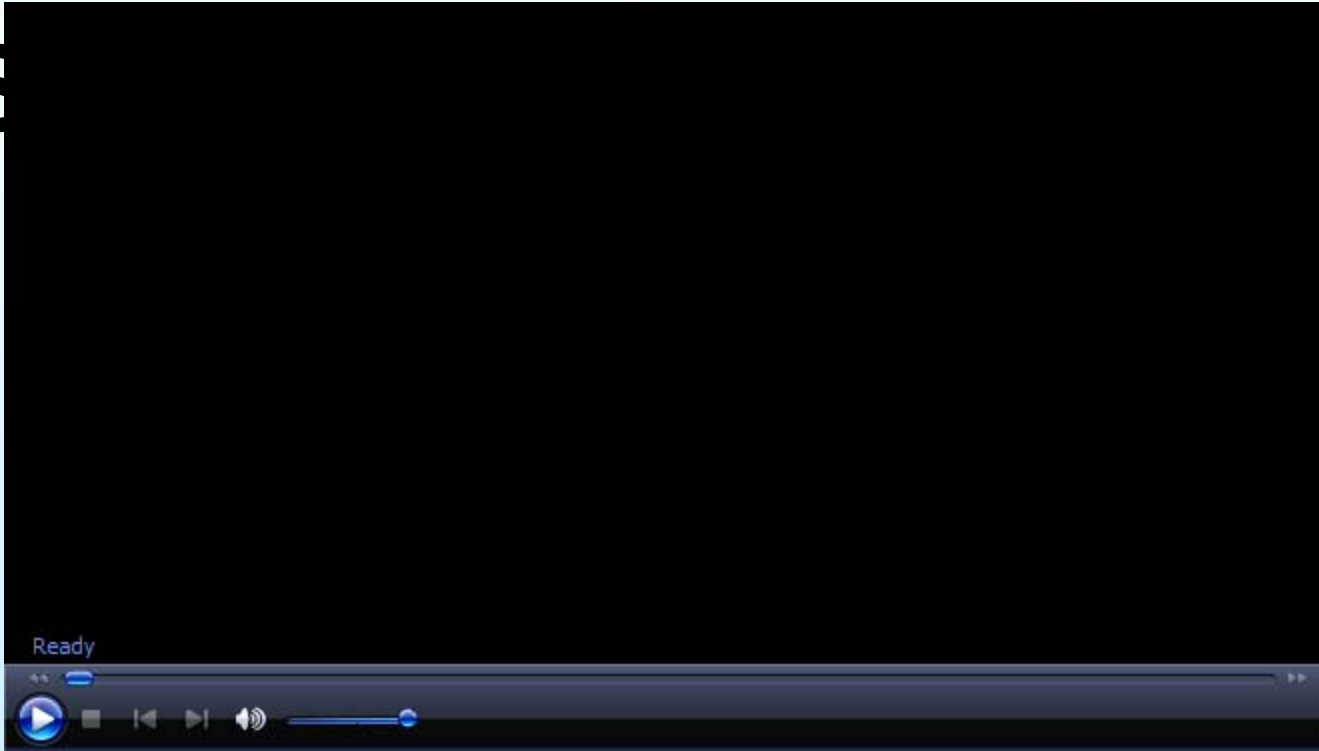
- Plan
- Implement
- Manage

- Recap
- Open





IFDA
International foodservice
distributors association





IFDA
International foodservice
distributors association



Systems Security – Risks

- Physical security
- Network connections
- Scam's - manipulating people
- Operating System patches - Instant messaging security holes
- USB devices – Mobile devices
- Document Shredding
- Employee transition

- Company Image / Reputation / Identity
- Compliance – (SOX, HIPPA, Auditors)
- Systems and Applications availability (Servers, Hosts, client computers, etc.)
- Systems Performance





IFDA
International foodservice
distributors association



Systems Security – Authentication

- User/Password - At Minimum have a Policy that...
- 3 strikes (deny device and disable)
- Strong passwords, with combination alphanumeric, not previously used, etc.
- No Post It's
- Specifically deny "common or shared" userids
- Set clear expectations for employee's and consequences for divulging their authentication means
- Invest in or implement a SINGLE sign-on solution
- Biometrics, Smart Cards, Tokens (hardware random generator), Kerberos





Systems Security – Wireless

CNN.COM's TOP TECHNOLOGY BREAKTHROUGHS (Top 25 in the last 25 years, from 2005)

- 1) Wireless world
- 5) Computers
- 9) Processors
- 10) Digital storage
- 12) Fiber optics
- 16) Biometrics
- 19) Batteries





Systems Security – Wireless

- No Default(s)
- Only use WPA(2)
- WEP is easily compromised
- Next generation is 802.1x
- Do NOT broadcast SSID – unless you have a Guest network on separate Lan/Vlan
- Wireless intrusion detection - put something in place to catch unauthorized access (controller, stand alone tools)
- Rogue Access Point - (controller, stand alone tools) - bridge to your wired network
- Do not fear the wireless – invest in NEW products





IFDA
International foodservice
distributors association



Systems Security – Plan

- Define your policy - new hire and ongoing - setting expectation from day 1
- Physical security
- Network diagram including “applications”
- What to secure (Physical/premise, servers/hosts, clients/nodes, applications, switches, routers, vpn, e-mail server, ftp, web, laptops, wireless, SAN/NAS (Storage), communications/phone/VoIP, archived records/images, HTTPS)
- When a theft/loss/breach occurs, what are the steps and expectations ?
- Do developers or admins have access to production data ?
- Who authorizes file/applications permissions ?
- Hire 3rd party to test/break in - NOT the same company who created the solution
- Vendors, trusted parties/partners and their "contractors" - SEE E-MAIL





IFDA
International foodservice
distributors association



Systems Security – Plan

"This email is to inform you that Hal Smith has left ACME Networking Management, Inc. and is no longer authorized to access your system as a representative of our company, effective Oct 04, 2007. As a Network Engineer of ACME, they had remote access to networks by way of a common user name and password that ACME had created on your systems. This password will be changed to protect your networks from unauthorized access and this change will be completed on Oct 04, 2007. Please refer to the attached Client Remote Management Password Policy for full details of this policy. It is our intention to keep you informed about changes that affect the security of your network. If you have questions or concerns, please contact me at 888-484-ACME x200."





Systems Security – Implement

- Commitment, education, budget (awareness)
- Quantify business impact
- Design solution
- Align IT with business value
- Implement





Systems Security – Manage

- OS Patches, especially windows, virus definitions/recipe's, - Including mobile devices (Treo/Palm, PDA's, Blackberry's, etc.)
- Create security steering committee (IT Mgmt, Security admin, Risk Officer, HR, Controller/CFO) - review security user log(s) and application
- IDS/IPS (intrusion detection & prevention - in firewall products) force the viewing of those logs and store
- Cannot live in a set and forget environment
- Hold administrators & Security positions accountable with weekly/monthly/quarterly activities
- Remember MOST breaches occur from within





Systems Security – Recap

- Commit / Budget – Not just one time - .01%-.03% to sales
- Educate – Make it part of your culture
- Plan
- Implement
- Manage
- Test
- People, People, People (Internal Customers, Senior Executives/Management, IT Staff)
- Handout - Mistakes People Make that Lead to Security Breaches





IFDA
international foodservice
distributors association



Systems Security – Open

- Question & Answer





IFDA
International foodservice
distributors association



Systems Security

Thank You! Have a great session
at the
2007 Distribution Conference!





IFDA
International foodservice
distributors association



Systems Security – References

<http://www.sans.org/resources/mistakes.php>

<http://www.cnn.com/2005/TECH/04/01/cnn25.top.technology/>

http://eval.symantec.com/mktginfo/enterprise/other_resources/ent-it_risk_management_report_02-2007.en-us.pdf

<http://www.informationweek.com/showArticle.jhtml?articleID=197005446>

http://www.sans.org/reading_room/whitepapers/wireless/171.php

<http://www.esecuritytogo.com/>





Mistakes People Make that Lead to Security Breaches

(<http://www.sans.org/resources/mistakes.php>)

Technological holes account for a great number of the successful break-ins, but people do their share, as well. Here are the SANS Institute's lists of silly things people do that enable attackers to succeed.

The Five Worst Security Mistakes End Users Make

1. Failing to install anti-virus, keep its signatures up to date, and apply it to all files.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.
3. Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, Firefox, and Netscape.
4. Not making and testing backups.
5. Being connected to more than one network such as wireless and a physical Ethernet or using a modem while connected through a local area network.

The Seven Worst Security Mistakes Senior Executives Make

1. Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job.
2. Failing to understand the relationship of information security to the business problem-they understand physical security but do not see the consequences of poor information security.
3. Failing to deal with the operational aspects of security: making a few fixes and then not allowing the follow through necessary to ensure the problems stay fixed
4. Relying primarily on a firewall.
5. Failing to realize how much money their information and organizational reputations are worth.
6. Authorizing reactive, short-term fixes so problems re-emerge rapidly.
7. Pretending the problem will go away if they ignore it.

2007 Distribution Conference Expo
Workshop Session #706: Systems Security
Tuesday, October 9th, 2007, 8:00am – 9:00am
Speaker, Joseph Wood, Chief Information Officer, Nicholas & Company, Inc.



The Ten Worst Security Mistakes Information Technology People Make

1. Connecting systems to the Internet before hardening them.
2. Connecting test systems to the Internet with default accounts/passwords
3. Failing to update systems when security holes are found.
4. Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
5. Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
6. Failing to maintain and test backups.
7. Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices
8. Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing.
9. Failing to implement or update virus detection software
10. Failing to educate users on what to look for and what to do when they see a potential security problem.

And a bonus, number 11: Allowing untrained, uncertified people to take responsibility for securing important systems.