



OFFICERS:

Chairperson:

Joe Sommers 2007
City of Muskego
(262) 679-4150
jsommers@ci.muskego.wi.us

Vice Chairperson:

Tim Ullman 2008
Door County
(920) 746-2304
tullman@co.door.wi.us

Treasurer:

Marie Panko 2007
City of Wisconsin Rapids
(715) 421-8222
mpanko@wirapids.org

Secretary:

Todd Demers 2007
Polk County
(715) 485-9220
toddd@co.polk.wi.us

BOARD MEMBERS:

Sue Schaefer 2008
City of New Berlin
(262) 797-2440
sschaefer@newberlin.org

Howard Mezera 2006
Calumet County
(920) 849-1456
howard@co.calumet.wi.us

Mark Beveridge 2006
City of Fond du Lac
(920) 322-3602
mbeveridge@ci.fond-du-lac.wi.us

Mike McGinnis 2006
Washington County
(262) 335-4486
mike.mcginis@co.washington.wi.us

Allen Mundt 2008
Waukesha County
(262) 970-4757
amundt@waukeshacounty.gov

TO: GIPAW MEMBERSHIP

DATE: 5/2/2006

RE: 4/20/2006 Spring General Meeting Minutes

A meeting of the Governmental Information Processing Association of Wisconsin – Spring General Meeting was held at the Grand Seasons Motel in Waupaca, Wisconsin.

8:30-9:00AM REGISTRATION

9:00AM:

Joe Sommers officiated the meeting and introduced our guest presenters. Joe also discussed Survey and “wapig05” is the password to go to survey on gipaw website. Time was taken to recognize the newcomers.

Managed Intrusion Detection for Networks:

Mirage Networks Appliance from AT&T

Mike Hoff – presenter – ATT Channel Director for Mirage Networks - Net Access Control applications - Controls what is allowed on networks -- 24/7/365 Server - IDS Firewalls,

Curtis Miner – Chicago branch of Mirage –

- Mike talked about security issues – holes in overall security
 - o Company started with pen tests on government systems
 - o Developed first IDS - Wheel Group in the 90's
 - o Mirage is out of Austin TX for 3 Years
 - o Only company who ever partnered with ATT / SBC

Defending Networks and the Interior of the networks

- Mobile computing is a major threat for bringing in infected computers onto your network.
- VPN is another threat to networks – don't know what is really on the other end
- Wireless is still the greatest threat

Discussed Voice Over IP (VoIP)

- 44% of network hacks are being successful from the INSIDE of our networks
- A DayZero attack is an attack that is released that has not been identified by our anti-virus / intruder detection systems.
- We need a network security system that is not O/S specific
- **We need to monitor outside computers / vendors connecting to our network**
- **We need to monitor smart cards or thumb drives being used by our employees**

- **Disable AutoRun on the CD Devices**
- **Disable Computer Management Console from all users except Admins**
- **Train all users on Policy and enforcement**
- Mirage works like this
 - o Discover
 - o Detect (HyperDetection)
 - Early Warning System
 - Hackers need to scan networks before setting up shop
 - Mirage takes unused IP Addressed in network and using them as a imitation network – virtual decoy that allow hackers to talk to / synchronize with
 - Snare hackers by allowing a connection to be made but we put this communication on-hold
 - The time of hold is 4 minutes but is repeated forever
 - During this time Admins needs to decide a plan to counter this attack
 - o Deceive (Snaring)
 - o Cloaking / Quarantined) is our Defense
 - We push this attack off of our network until we are ready to address
 - This pushes the hacker off of our network
 - Protection will always be focused to the network, before we consider endpoints
 - All traffic from infected PC is sent to the CounterPoint and examined

SB C has recommended Mirage Networks for most comprehensive appliance
Data storage for compliance purposes: Sarbanes Oxley, HIPAA, GLBA and SAS 70

Cost of using Mirage = .50 per hour x 24hours per day x 365 days per year = \$4380
****** Mirage is \$7000 and \$2000 for install ******

10:05AM – 10:30AM BREAK

10:30AM

Enterprise Information Security for IT Managers

Exceed Security Systems

Enterprise Information Security - Threats and Risk Mitigation

Cory Michal – Presenter cmichal@exceedsecurity.com

Exceed Security
(877) 249-7481

Exceed Security Systems

- Mitigate Risk of ORG Info Tech usage
- Achieve Regulatory Compliance
 - o Assure Compliance with industry and Government Regulations
 - o HIPAA – Health Care
 - o GLBA - Financial
 - o SOX - Public Trading Companies
 - o FISMA – Federal Government
 - o State Information Disclosure Notification – California SB 1386 – Wisconsin SB 164
 - o Data Trust and Accountability Act - Federal Attempt to make this law to have businesses notifying customer when their accounts have been compromised
 - o PCI Standards – MasterCard and Visa
- Confidentiality, Integrity, Availability (C.I.A.)
- Threat, Vulnerability (weak spot in security mechanism), Safeguard (patch)
- Average Yearly Loss \$85,919
- Percentage of companies who reported being Attacked = 78%
- Trojans = Theft of Services, Drone Army Member, Pay Per Click Fraud, Brazilian Dialer
- Worms = Exploit a vulnerability on a system and then begin propagating to other systems
- Viruses = Cause malfunctions and problems with software
- Network Insider Abuse
 - o Average Yearly Loss \$21,905
 - o Percentage of companies who reported being Attacked = 49%
 - o Need to prevent where users can go on the Internet
- DoS Attacks

Visit us at: www.gipaw.org

- Average Yearly Loss \$36,922
- Percentage of companies who reported being Attacked = 31%
- Extortion Schemes – Mob attempt to force companies to pay for protection
- Targeted System Penetration
 - Average Yearly Loss \$7,719g
 - Percentage of companies who reported being Attacked = 17%
 - Cashing out Credit Cards
 - Attacking to find SSL numbers, Credit Cards Info, Confidential Corp Info
- Wireless Network Abuse
 - Average Yearly Loss \$4,501
 - Percentage of companies who reported being Attacked = 19%
 - Stealing bandwidth
 - Sit on the street outside of business
 - Web encryption takes only about 45 minutes to break
- Sensitive Information Exposure
 - Trade Secret
 - Intellectual Property
 - Business Plans
 - Contract Bids
 - Lost BackUp tapes
 - Average Yearly Loss \$152,356
 - Percentage of companies who reported being Attacked = 32%
- Financial Fraud
 - Average Yearly Loss \$50,294
 - Percentage of companies who reported being Attacked = 8%
 - PINs are being stored in a BLOCK File – hackers use a White Card with Account # and PIN on ATM
- ChoicePoint
 - 145,000 accounts stolen
- Luxor Casino
 - Locked for 3 hours
- Bank of America
 - Lost Backup Tapes

Largest numbers of compromise

- Viruses
- Unauthorized access
- Theft of Proprietary Information

Sample: `.php?id = ' (scripting language)`

Do NOT allow web access to Servers with sensitive data

Check Web Applications, because they do not get secured properly and point to Active Directory

Turn off SSH access to sensitive servers

Database passwords should never be the same as user network password

Monitor your IDS system and have alerts sent to you

Governments are targets, because of our client information

FrontPage Extensions are a common vulnerability

TESTS:

- Pen tests
- External Network Security Assessment
- Internal Network Security Assessment
- Org Info Security Assessment

IAM = Information Security Assessment Methodology

- Management
- Technical
- Informational

OSSTM = Open Source Security Testing Methodology

INFO SEC TOOLS

- Nessus, SAINT, Retina, Qualys

3rd Party Assessments

Certified and Accredited?
Experienced?
Specialist in Info Security?
Know what you are getting
Look for methodologies being used by vendor

Need an I.T. Security Policy

Basic Rules, guidelines, and definitions for everyone on network

Need staff to read log files – set policy?

Need to monitor firewalls – stop TCP traffic on Port 23

On Firewalls, block everything and then open only what is needed

Never install firewalls and leave it in “plug-and-play”

Have an outside assessment done

IDS

Compare traffic
Monitor logs
Decipher what is being attacked

IPS Intruder Prevention Systems - will close ports that it thinks is a threat

Manage Security Services

Let someone else worry about this
Monitors logs 24/7/365
Automatic firewall and IDS updates

Virus, Worm, Malware Protection

96% of companies use some sort

SPAM

Fishing attacks
SpamAssassin is a good tool
Barracuda
Can outsource to ISP

Two (2) Factor Authentication

Operates on the “Something you know” and “something you have” philosophy
Excellent option for securing remote access (VPNs)
Price is dropping

Management and Monitoring!! A MUST

Know what is going on in your network
Only 16% of attempted hacks go to authorities

Here is what to do:

- Security Assessment
- Risk Mitigation
- Management
- Repeat annual or bi-annual

NOON: LUNCH

1:00PM STATE OF WISCONSIN REPORT

1:30PM GIPAW MEMBER ROUND TABLE

Round Table Discussion

Wireless Mesh Network

Concern on security from Mobile Computers in Squad Cars

Concerns about the sheer bandwidth for WiFi operations

Visit us at: www.gipaw.org

Attempting to eliminating Meter Reading
Wireless units for Water Departments in municipality
Joe asked if we wanted this as a topic for July Meeting?

Managing Assets

SMS was used by three (3) counties and dumped
Performance was heavy, and configuration as very hard

Another product called Desktop Standards Tools – Claims to be very good
Desktop Standards is a snap-in with / for Active Directory
Also can be configured through Group Policies
<http://www.desktopstandards.com>
Cost is about \$12 per unit and very easy to use

Another product is call Desktop Authority – Door County
It is like Novell Zen Works on steroids

Al Mundt asked about a good BOT and / or Trojan scanner

2:15PM ADJOURN

Next GIPAW Board of Directors Meeting - Friday, May 12, 2006 - Waupaca WI

END OF REPORT FOR THE APRIL 20, 2006 GIPAW GENERAL SPRING MEETING.