Help! I've Been Hacked... Now What?

ASME Technical SIG 1/9/07

David Strom

(310) 857-6867,
david@strom.com

Webinar outline

- What about my desktops?
- Liability for personal data leaks
- Learning from my mistakes
- What kinds of information logs do I need?
- Where do I go for help?

My background

- IT trade magazine and Web site editor for 20 years
- IT manager at the dawn of the PC era in the 1980s
- Test and write about hundreds of PC, networking and Internet products
- Articles in the NY Times and IT trades
- Podcaster, blogger, and professional speaker

Security is hard

- More blended threats to your networks
- More guest workers and outsiders that need to be inside your security perimeter
- Greater reliance on Internet-facing applications and hosted services
- Windows still a patching nightmare
- More complex compliance regulations

Fear #1: My desktops!

- Your perimeter is porous
- Every PC needs an operating personal firewall and AV
- What about your guest workers?
- Do you know what is running across your network?

It is so easy to secure XP – NOT!

-install latest patches, and enable Windows Update
-disable file and print sharing, disable DCOM
-turn off several Windows services
-use autoruns and msconfig to disable more stuff
-disable extension hiding and file sharing in Explorer
-secure IE, then install and use Firefox & noscript plugin
-install a firewall
-install antivirus, antispyware, and Security Task Manager
-install a new hosts file to block ads and malicious sites
-create and always use an unprivileged account
-if my kids will be using the computer, then use Microsoft's Software Restriction Policies

(from SANS Internet Storm Center diary 10/17/07)

And Vista isn't much better

- Disable User Account Control
- Disable Driver Signing
- Fix screen blanking behaviors
- Throw away most of the Aero stuff, too

Fear #2: I am liable for any data leaks

- HIPAA: Identify security breaches
- SOX: Capture and audit events
- PCI: Preserve privacy and prevent ID theft
- FRCP: Widened definition of eDiscovery
- Europe and elsewhere have their own ones, too!

Fear #3: How can I learn from my mistakes

- Buy the right kinds of IDS and firewalls, and understand their setup and logs
- Know your limitations, and when to **outsource** your security
- Know when Cisco and Juniper don't have all the answers and what else to pick
- Examine a breach and understand what went wrong and what data leaked out

What happened?

- Hacker stole data
- Some systems were compromised, or had obvious passwords
- Inside job or disgruntled employee
- Denial is not an option!

Do a vulnerability analysis

- Look at desktops, servers, and networks as an entity
- Look carefully at what people have access to which computing resources
- Look at entry/egress points of your network, if you can find any of them
- Stop trying to defend the perimeter!

Hindsight is an incredible tool

- Create chains of custody and business operation rules about your network before your auditors tell you
- Audit your ACLs and then severely limit the access rights of your users to the smallest set possible
- Use logging tools to periodically monitor who (and when) has access to your network's crown jewels

Fear #4: I can't log everything

- First, understand that logs fall into three functional areas:
  - collection
  - data repositories
  - how you do your analysis
- Should you focus on real-time alerts or long-term archives?
- Your chain of custody requirements also determine your needs

Log managers vs. Security Info Managers

- SIMs: Event correlation and analysis for real-time threat resolution and monitoring
- SIMs: Codifying business rules, notification of events
- LMs: Archival and eDiscovery purposes
- LMs: After-the-fact investigations supporting litigation

You need a common, enterprise-wide log repository

- One place where all logging data lives
- Resist the temptation to DIY and patch together something on your own
- Home grown scripts end up being more costly and are difficult to maintain

Where can I go for more help?

- Owasp.org “Web Goat”
- SANS institute for general training
- Johnny.IHackStuff.com
- Google hacking
- SPIdynamics.com's Web Inspect site scanning tool
- Nessus Vulnerability Scanner from Tenable Network Security
- My white paper for Breach Security on SQL Injection

Wise words to end

- Don’t treat security as Yet Another IT Project
- Try to balance security with functionality and realistic staffing
- Lawyers can be your friends, if you let them
- Start with small steps and work out from the core

Thank you!

- David Strom
- (310) 857-6867
- David@strom.com
- http://strominator.com