Integrating Security into Your Corporate Infrastructure

December 13, 2001

Matthew K. Miller, CISSP, GIAC
Manager, Security Services
RedSiren Technologies

Who is RedSiren?

- We are a MSSP
- Managed Security Service Provider
- 24 x 7 Monitoring and Management of:
  - Information Systems
  - Firewalls
  - Intrusion Detection
- Security Professional Services

Our Goal is to help you secure your corporate infrastructure.
Phase 1
Security Policy

✓ What are you protecting? From whom?
✓ Must encompass major areas including:
  ✓ Appropriate Use Statement
  ✓ Equipment Usage
  ✓ Email
  ✓ Internet Usage
  ✓ Passwords
  ✓ Firewall Policy
  ✓ Disaster Recovery
  ✓ Incident Response
✓ Must be signed by upper management AND enforceable!
Phase 1
Hints

✓ Conduct a Security Assessment
✓ Risk Assessment – OCTAVESM
  ✓ Critical Assets, Threats, Countermeasures
✓ Vulnerability Scans – benchmark
✓ Policy Creation
  ✓ Cross-functional team
✓ Concise Overarching Policy (3 - 6 pages)
✓ Referenced Procedures
✓ Supporting Standards and Guidelines
✓ Enforcement
  ✓ Signed consent from users
  ✓ Initial and recurring training
  ✓ Known and consistent consequences

Phase 2
Security Architecture

✓ Security Program Organization
  ✓ Roles and Responsibilities
  ✓ Steering Groups
  ✓ Reaction Teams
    ✓ Disaster Recovery
    ✓ Incident Response
    ✓ Audit / Assessment
✓ Personnel
  ✓ Training
  ✓ Support
  ✓ Managed (Security) Service Provider?
✓ Upper Management Support
  ✓ Or else it won’t work…
Phase 2
Hints

- Steering Groups
  - Integrating Security and Business
  - Not just IT!
- Response Teams
  - Prepare ahead of time
  - Checklist Driven (react in crisis)
  - Practice Practice Practice
- Budgeting
  - Training
    - SANS, CERT, ASCAC, DEFCON, ...

Phase 3
Network Planning

- Review results from Phase 1
  - The “What”
- Design infrastructure to support the “what” – use the CIA!
  - Confidentiality
  - Integrity
  - Availability
- Don’t forget the maintainability...
Phase 3
Hints

✓ Budget
  ✓ Use the Risk Analysis to focus $$$
  ✓ Justification is difficult – LOI vs. ROI
✓ Personnel
  ✓ Training
  ✓ Support
✓ Steering Group Approval

Phase 4
Firewall Management

✓ Phase 1, 2, and 3 outputs
✓ So, what is a firewall??
✓ Prevents intruders from entering network
✓ Enforces security policy on your network
✓ Use to connect two untrusted networks
✓ Okay, I installed one. I’m done?
  ✓ Log Monitoring
  ✓ Maintain Patch Level
  ✓ Change Control
Phase 4
Hints

✓ Choose a firewall that supports Phase 1
  ✓ Software vs. Hardware Based
  ✓ Vendor??
✓ Supportability
  ✓ Log Reviews require expertise
    ✓ Preludes to attack
    ✓ Auditing of user activity
    ✓ Evidence
✓ Updates / Upgrades
  ✓ www.cert.org
  ✓ www.sans.org
  ✓ Vendor’s Site
✓ Change Control
  ✓ Steering Group

Phase 5
Intrusion Detection

✓ “But I have a firewall ...”
✓ What is Intrusion Detection??
  ✓ A means of detecting an intrusion (duh!)
  ✓ Examines traffic for suspicious or malicious activity
✓ Sends alerts when activity is discovered
  ✓ Is anyone listening?
  ✓ Ok, do they know what to do?
✓ This is not a preventative mechanism
  ✓ Well… that’s not entirely true
Phase 5
Hints

✓ Network vs. Host Based IDS
  ✓ Network: What’s going on within my network? (Sniffer on steroids)
  ✓ Host: Once someone has compromised a server (Server Activity Analyzer)
✓ Placement
  ✓ Refer back to Phase 3
  ✓ Depends on your strategy and patience
✓ Maintenance
  ✓ Updates, Upgrades, Signatures, … (oh my!)
✓ Cool features! But…
  ✓ Potential for self inflicted D.O.S.
  ✓ Baselining Baselining Baselining

Phase 6
24 x 7

✓ What are a “black hat’s” hours?
  ✓ a) 9 – 5
  ✓ b) 5 – 9
  ✓ c) all the above
✓ The Internet never closes
✓ Support for Phases 4 and 5
✓ Murphy’s Law (remember her?)
✓ Other options to D.I.Y. ?
Phase 6
Hints

✓ Very costly for 24 x 7 in-house
✓ Managed Security Service Providers
  ✓ Expertise
  ✓ Certifications and Training
✓ Confidentiality
  ✓ Encrypted communications
✓ Integrity
  ✓ Secure storage
✓ Availability
  ✓ Redundancy
✓ Why not ask if they practice what they preach?!

Phase 7
Planned Response

✓ There are no 100% security solutions
✓ You will always assume some level of risk
  ✓ Remember Phase 1?
✓ What happens when there is a Murphy’s Day?
  ✓ Remember Phase 2?
✓ Disaster Recovery, Incident Response …
✓ How will you react in a crisis?
✓ Once again: Practice Practice Practice
Phase 7
Hints

✓ Recognize the 20-80 / 80-20 rule
✓ Upper management empowerment of teams
  ✓ Time is of the essence
✓ Clearly defined roles and responsibilities
✓ Step-by-step checklists
✓ Practice Practice Practice!!!

On-Going Actions

✓ Businesses and Networks are dynamic
  ✓ Adding new functionality may open
    new vulnerabilities
✓ Periodic Assessments and Audits to ensure:
  ✓ security policy is executed
  ✓ regulatory compliance is maintained
✓ And repeat the continuum process
SECURITY WELLNESS CONTINUUM

RedSiren Technologies
Corporate Headquarters
650 Smithfield Street
Pittsburgh PA 15222
www.redsiren.com