10

Foolproof Initiatives to Boost Your Network Security

David Piscitello
Core Competence, Inc.
dave@corecom.com
http://hhi.corecom.com
http://www.corecom.com

What we will discuss...

- **Ten practical guidelines you can put into place today to protect your network and critical data**

Top 10 security initiatives

1. Adopt a risk management methodology
2. Layer your security measures
3. Compartmentalize your network and data
4. Implement stronger authentication
5. Implement admission and endpoint controls
6. Improve the granularity of your access controls
7. Develop a secure software methodology
8. Be proactive with security
9. Develop an "attack anticipation" mentality
10. Ensure information integrity, privacy, availability

Hey, you talked about some of these already!

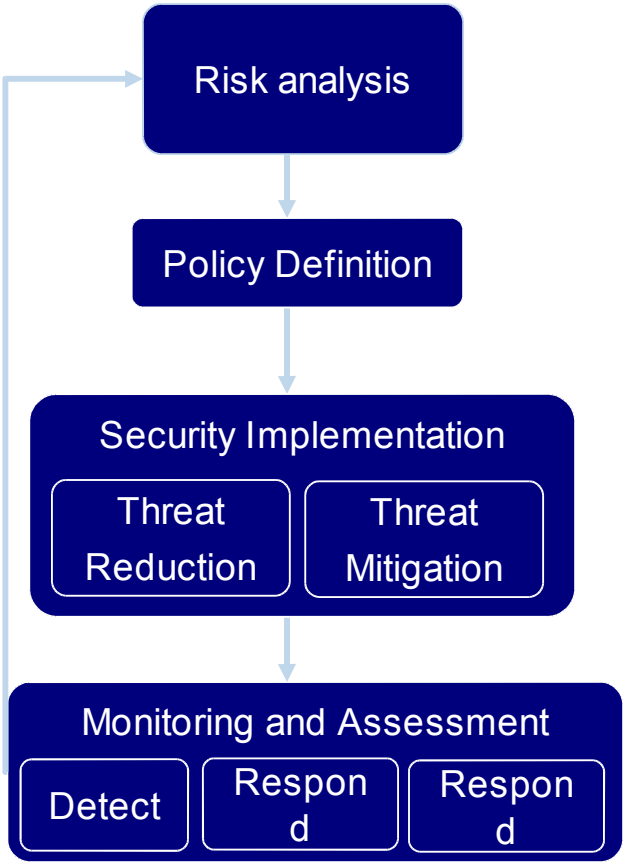
Repetition is the key to learning something deeply…

1. Adopt a risk management methodology

- "Change is the only constant." - Arthur Schopenhauer
- "Change goes undocumented until after an incident." - Dave Piscitello
- What changes?
  - User population, constituencies, business relationships, applications change (frequently)
  - Network and applications configurations
  - Policies and process
  - New attack vectors and vulnerabilities are announced "daily"
- Adopt continuous risk assessment and management to maintain a security profile

A systematic approach to IP security

- **Many companies have implemented IP security measures and processes**
  - **How do you know whether critical business resources are protected?**
  - **How do you know whether your implementation is sufficient?**
- **If adequate today, will it remain that way tomorrow?**
  - **Networks are dynamic**
  - **Secure networks require continued vigilance**
- **A systematic approach can help you to avoid oversights**
  - **Reduce risk to acceptable levels, in accordance with business needs**



New age risk assessment considerations

- **Accelerated timeframes**
  - **Haste-to-production is a leading cause of poor coding and configuration error**
  - **Is "first to market" worth being the first attacked?**
- **Evolving threat environment and model**
  - **Attacker profile is changing (example: spyware)**
  - **Social engineering increasing (example: phishing)**
  - **Little time to close attack windows of opportunity**
  - **Education is more critical than ever**

2. Layer your security measures

- **Firewalls and IDS are not substitutes for host security**
  - **Defense begins at Internet access and continues all the way to the asset**
- **Harden hosts that support your services**
  - **Tighten administrative controls to eliminate the most commonly exploited *NIX & Windows threats**
  - **Only run what's absolutely required**
  - **Keep number of "administrators" small**
  - **Add "wrapper", file, Web, and OS security software**

Layered defenses

- **Layer your anti-malware measures**
  - **At servers, clients: Up-to-date virus, spyware defenses, anti-spam**
  - **At security gateways**
    - **Content inspection**
    - **Malware blocking**
  - **At the firewall or (and) VPN security gateway**
    - **Block spam, undesirable and suspicious file types and sites**
    - **Proxies rule!**

3. Compartmentalize your network

- **Would you put a screen door on a submarine? Compartmentalize and reinforce security measures**
  - **Separate client subnets from servers**
  - **Separate public-facing servers from intranet servers**
  - **Create separate subnets for infrastructure servers**
  - **Use inter-departmental, server and personal firewalls**
  - **Move firewalls closer to assets**
  - **Terminate VPN tunnels closer to assets**

The "Inflexible Bastard" security policy

- Keep the allowed inbound services list short
- Limit user access to only known and approved Internet applications
  - Block everything else and wait for the phone to ring
  - Ask "What's the business value?"
    "Show me the policy!"
    "If it's not in the policy, who's signing off?"
    before enabling a service
- "That which is not expressly permitted is prohibited" has and will always be The Right Choice

4. Implement stronger authentication

- If you must use password-based authentication, impose complexity and frequent change policies
- Security tokens are mature and enterprise ready
- PKI is enterprise-ready
  - Inter-enterprise still a tough deployment
- Biometrics
  - The Patriot Act is accelerating the "drive to commodity"
- Consider combinations of authentication methods
  - Two or more of "something you know, you have, you are…"

5. Implement admission and endpoint controls

- **Endpoint security is as important as firewalls and VPNs**
  - **Of what value is a secured tunnel when one endpoint is compromised to anyone but the attacker?**
  - **Scan before connect, admission control, and EPC are must-haves**
- **Promising vendor and industry initiatives:**
  - **Network Admission Control (NAC, Cisco)**
  - **Network Access Protection (NAP, Microsoft)**
  - **Industry-standard access control frameworks (e.g., 802.1X)**

Admission control: Virtual customs and immigration

- Permit or deny network access to endpoint devices based upon compliance to security policy
  - AV software version, engine and signature file verification
  - OS type, patch and hot fix installation verification
  - Other security program presence, integrity, and configuration (e.g., PFW, VPN, IDS, anti-spyware)
- Ability to quarantine non-compliant endpoints
  - Permit access to a restricted area for remediation

Endpoint control

- **Endpoint control assumes that**
  - **User may access the company network from any system**
  - **IT may not be able to install resident admission control software (temporary agents may be used instead)**
- **Goal: Leave no trace on endpoint following logoff**
  - **No cached credentials**
  - **No leaks of network topology information**
  - **No record of (internal) hyperlinks visited**
  - **No temporary, spooled and cached data files**
  - **No local copies of company-sensitive information**

Additional EPC objectives

- Restrict applications from uncontrolled systems
  - E.g., prohibit use of FTP from non-work systems
- Restrict application command from uncontrolled systems
  - E.g., prohibit FTP GET operation from non-work systems
- Protect organization from compromise via uncontrolled systems by
  - Quarantining or limiting access when endpoint does not warrant full trust
  - Employing identity information in authorization decisions

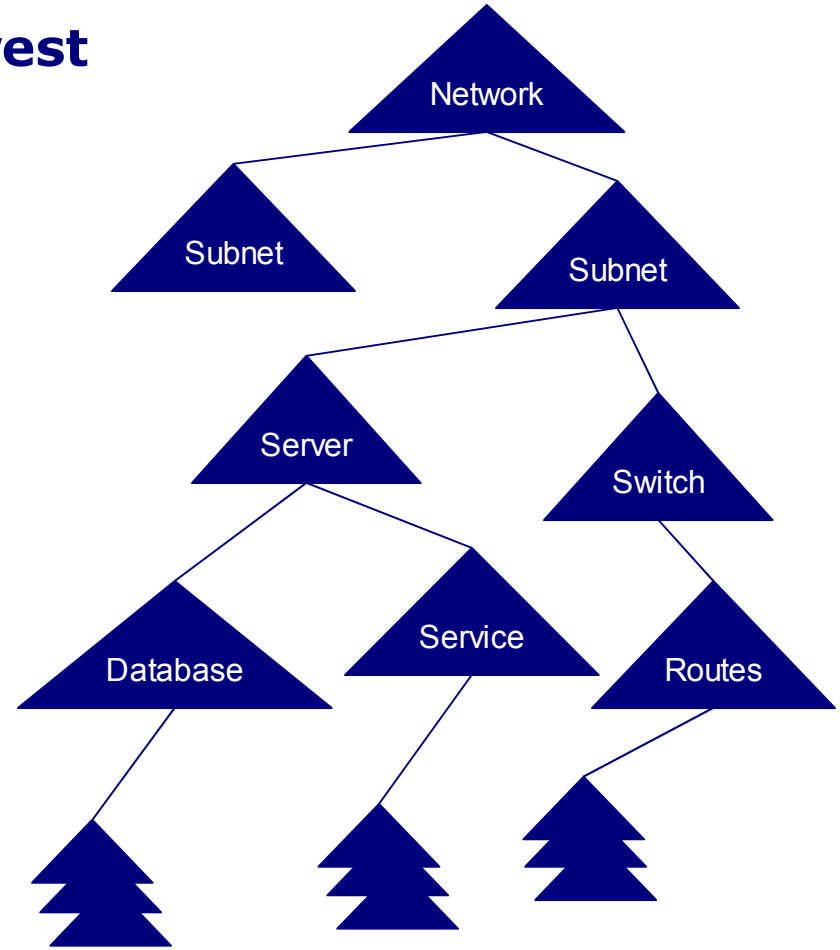
6. Improve granularity of access controls

- Granting every user
  - Carté blanche access
  - To every asset of a trusted network
  - Based on successful (endpoint) authentication

  is A Bad Idea
- Additional controls should identify assets a user is authorized to access

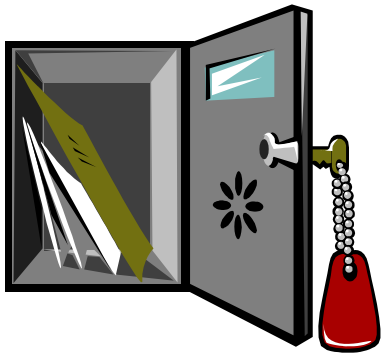
Authorization and granularity

- **Apply access controls at the lowest level of granularity possible**
  - **Networks**
  - **IP subnets**
  - **Servers**
  - **Network equipment**
  - **Computers**
  - **Applications and services**
  - **Users**
  - **File shares**
  - **Printers**
  - **(Removable) devices**
  - **Data objects (files, URLs)**



Managing trust

Admission control ➔ Authentication ➔ Authorization ➔ ➔ Exit control



Do I trust the endpoint device ?

Do I trust the user ?

Do I allow **this user** perform **this action** on **this datum**, from **this location** ?

Leave no evidence of user activity

7. Develop a secure application software methodology

- The majority of today's attacks target (Web) applications
- The majority of Web application developers know little about security
- Web application languages are recreational drugs
  - (They encourage experimentation)

Best practices

- Design applications to require fewest privileges possible
- Choose language and constructs wisely
- Subject all applications to rigorous review and audit during design and development
- Test, test, test…
- Contain and separate business and custom applications from each other, and from infrastructure applications

8. Be proactive with security

- Routinely scan networks, servers, and clients
  - How else can you know your "normal" state of operation?
  - Scan, identify, then mitigate new vulnerabilities
  - Review existing policy and implementation based on results
- Keep software current
  - Use standard builds/images, limit user self-administration
  - Know what's running on all servers, switches, clients
  - Apply patches following a formal verification process
    - Most incidents exploit known vulnerabilities

9. Adopt an attack anticipation mentality

- **Prevention is better than detection**
  - **Vaccines are better than antibiotics**
- **Build your network to be immune to attacks**
  - **Resistant networks will have less down time**

IDS and IPS

- Don’t be dazzled by the technology
- Intrusion detection is complementary security
  - Place IDS where it’s beneficial not intrusive
  - If you’re constantly adjusting alarms,
    you’re either a sweet target or it’s in the wrong place
- Intrusion prevention and rejection
  - Isn’t this what firewalls *do*? Did we need another name?
  - Blocking is evidence that your network is correctly inoculated
  - If you aren’t logging, how would you know this?

Predictive analysis

- **Stay informed**
  - **Will your press releases and advertisements be welcomed?**
  - **Will fallout from adverse political or social events affect you?**
  - **Have other organizations in your industry attracted determined intruders?**
- **Monitor any activity that might warn you of an imminent incident**
- **Take threats seriously**

Forewarned is forearmed

- Maximize your logging and auditing information
- Don’t just store logs, study them!
  - Logs are your blood tests and MRIs
  - Use analysis tools to interpret logs
- Look for deviations from normal activity
- Look for trends that have historical precedence
- Stay abreast of news that affects your industry sector
- Monitor mail lists that identify exploits and vulnerabilities

10. Ensure information integrity, confidentiality, availability

- **Integrity**
  - **File system and OS anti-tampering technology**
  - **Archival and retrieval process should include configuration data**
- **Confidentiality**
  - **File encryption, VPNs, encrypted archives**
- **Availability: A security metric?**
  - **Why do you think they call it denial of service?**
  - **Not only applicable to technology and services but people as well**

Methods for ensuring availability

- Use recovery processes that "restore to current state"
  - Installing an image of a hardened server does this; reinstalling the OS from OEM disks does not
  - It's the configuration, silly!
- Load balance to minimize lost service time
  - Distribute traffic load across multiple paths
  - Network equipment
  - Application servers and data centers

More availability measures

- **Redundancy and recovery measures**
  - **Imaging hardened servers and client installs**
  - **Hot and cold standby systems and equipment**
  - **Data and site mirroring and archiving**
  - **Uninterruptible power supplies**
- **Build in diversity to avoid single points of failure**
  - **Multiple and varied communications paths**
  - **Network equipment, application servers and**
  - **Critical infrastructure components (e.g. name and time servers)**

Conclusions

- You can only squeeze so many security initiatives into a budget
- Too many initiatives at once increases complexity
- Choose security initiatives that have a potential for immediate and measurable payoff – and you may land a bigger budget!