Security Architecture
- Week 10 -

Perimeter Security
Week 10

• No class meeting this week
• Week 10 assignment:
  - Authenticating devices on the network
• Lecture: Perimeter Security
• Quiz
It is human nature to protect ourselves and the things we care about by building barriers to keep things out. In most corporations, perimeter security management still dominates efforts to protect corporate information assets.
Perimeter Security

• Very extensive topic
• Diversity, size and complexity of enterprise perimeters
• A number of basic concerns that should be addressed
• Checklist approach is required (SANS, ISACA)
Perimeter Security Topics

• Inventory of Devices
• Inventory of Software
• Secure Configurations
• Continuous Assessment
• Malware Defenses
• Application Software Security
• Wireless Access Control
• Data Recovery Capability
• Security Skills Assessment and Training
• Secure Configurations for Network Devices
Perimeter Security Topics - continued

• Control of Network Ports, Protocols, and Services
• Controlled Use of Administrative Privileges
• Boundary Defense
• Maintenance, Monitoring, and Analysis of Audit Logs
• Controlled Access Based on the Need to Know
• Account Monitoring and Control
• Data Protection
• Incident Response and Management
• Secure Network Engineering
• Penetration Tests and Red Team Exercises
Inventory of Devices

• Authorized Devices
• Unauthorized Devices
• Use of RADIUS Authorization
• BYOD
• Network Identity Services
Inventory of Software

• Authorized Software
• Unauthorized Software
• Use of Active Directory and ABAC systems
• BYOS (software/service) – email example
• Network Identity Services
Secure Configurations

- Firewalls
- Routers
- Switches
- Servers
- Client Computers
- Mobile and BYOD challenges
Continuous Assessment

- Threat Awareness
- Vulnerability Assessment
- Remediation Strategy
- Operationalization

- Repeat -
Malware Defenses

- Signature-based scanning
- Patching discipline
- Behavior based and predictive analysis
Application Software Security

• Software design and development standards
• Application-based access controls
• Patch management
• Application authentication (certificate authority management)
Wireless Access Control

• Current wireless standards
• Wireless encryption
• Physical security
• Virtual Private Networks
Data Recovery Capability

• Back-up and restore processes
• Resilient architectures
• Failover and warm site strategies
Security Skills Assessment and Training

- Human factor considerations (HR)
- Security awareness training, reminders
- Risks from employees and vendors
- Testing and monitoring (e.g. phish your staff)
Secure Configurations for Network Devices

- Firewalls
- Routers
- Switches
- Verify not default install and password
- Formal approval, tracking and inventory of config changes
Limitation and Control of Network Ports, Protocols, and Services

• Again ... Firewalls, Routers, Switches
• Verify not default install and password
• Limited permissions tracked by individual user
• Formal approval, tracking and inventory of config changes
Controlled Use of Administrative Privileges

- Servers
- Storage Devices
- Client Hardware (Windows policies, for instance)
- Centralized (small) administration group
- Formal change request processes
- Mandatory vacations
- Password maintenance and audit
Boundary Defense

- Firewalls (NAT, port restrictions)
- DMZ(s)
- Intrusion Detection System
- VPNs
Maintenance, Monitoring, and Analysis of Audit Logs

• Routine but essential
• Daily to yearly process
• Log retention policy
• Advanced analytics (machine learning)
Controlled Access
Based on the Need to Know

• Information Protection RISK function
• Formalization of data ownership
• Formal data access request processes
• Data access audit and revocation
Account Monitoring and Control

- User detail logging
- Audit and review
- Automatic expiration of privileges
- Centralized authority
Data Protection

• Access control
• Physical controls
• Anonymization (data masking)
• Encryption
• Access log maintenance and review
Incident Response and Management

- Risk identification
- Mitigation Planning
- Event response prioritization
- Event Response organization development SIEM tool implementation
- Active monitoring and analytics
Secure Network Engineering

• Security considerations in network design (DMZ, sub-netting, domain management)
• Cleanly executed and documented network
• Patch maintenance
• Ongoing review and improvement
Penetration Tests and Red Team Exercises

- Both internal and external resources
- Track outcomes, identify vulnerabilities
- Security improvement planning and tracking
- Participation in industry sponsored groups for best practices
Quiz