LAN Domain Network Security Best Practices
An integrated approach to securing Company Co. Inc. LLC’s network

Written and Approved By:
Geoff Lacy, Tim Fielder, Matthew Demmler and Jim Thavisay

Company Co. Inc. LLC
Updated: 3/29/2012
# Table of Contents

Best Practices ......................................................................................................................... 2

Physical Security ....................................................................................................................... 2
  Equipment ................................................................................................................................. 2
    Authorized Equipment ........................................................................................................... 2
    Authorized Personnel ............................................................................................................ 2
    Logging and Monitoring ....................................................................................................... 2

Logical ....................................................................................................................................... 2
  Firewall ................................................................................................................................... 2
  Intrusion Detection and Prevention Systems ............................................................................ 3

Access Control List Configuration ............................................................................................. 4
  Allow ....................................................................................................................................... 4
  Deny-All .................................................................................................................................. 4

Network Architecture ................................................................................................................. 4
  Layered Security ..................................................................................................................... 4
    Perimeter Security ................................................................................................................ 4
    Network Security ................................................................................................................... 4
    Host Security ........................................................................................................................ 4
    Application Security ............................................................................................................. 5
    Data Security ........................................................................................................................ 5

Redundancy .................................................................................................................................. 5

Labeling ...................................................................................................................................... 5

Documentation .............................................................................................................................. 5

Segregation ................................................................................................................................... 5

Audits .......................................................................................................................................... 5

Updates ....................................................................................................................................... 5

Back-ups ..................................................................................................................................... 5
Best Practices
Company Co. Inc. LLC LAN Domain Network Security Best Practices is comprised for network administrators to integrate a safe and secure network environment for employee personnel, visitors, and clienteles. Network security is vital to the preservation of and responsibilities of our mission. This document provides employees with best practice principals to physical and logical infrastructures.

Physical Security
LAN Domain contains network devices allow logical data to flow within our infrastructure. It is our responsibility to ensure the efficiency, reliability, and security of the network. This section describes best security practices to ensure physical equipment is not jeopardized, and does not contain malicious applications.

Equipment

Authorized Equipment
All equipment must be approved and authorized for implementation and configuration within the network architecture

Regular audit and inventory of equipment must be conducted

Network equipment includes, but is not limited to the following: access points, routers, switches, cables, computers, and various network components

Authorized Personnel
1. Only authorized personnel are allowed to administer and configure networking equipment
2. Any changes must be approved and configured by authorized personnel

Logging and Monitoring
All equipment are logged and monitored in real-time. All component information is to be stored and review to analyze and assess for nefarious activity.

Logical

Firewall
Firewalls are the first line of defense for your network and should be treated as such. These are a list of best practices that one should follow for maintaining and enforcing a strong firewall policy.

1. Do not assume your firewall is the only security you need. This naivety will be exploited.
2. Deny all traffic by default and only enable the ports and protocols needed for the services being offered.
3. Make sure the security rule set on the firewall remains consistent with CCI's information security policy.
4. The firewall rules are NOT the same as your internal security policy. This should be noted and remembered despite it not being a formal "practice"

5. Try to maximize CPU cycles and network throughput. This can be achieved by
   A. Running AV, content filtering, VPN, DHCP, authentication software on other dedicated systems appropriately placed behind or in front of the firewall. They will usually be behind.
   B. Remove unneeded or redundant rules
   C. If firewall logging is going to be managed, then make sure it is managed thoroughly and professionally. If not, then disabling logging will allow you to free up some clock cycles.

6. Make sure the user ID of the firewall is its own unique ID. Follow the policy of least privileged and do not have your firewall run as root or administrator

7. Make sure the default firewall administrator or root password is changed before connecting it to the public internet. This should be a no-brainer.

8. Packet filtering is not adequate by itself. Implement stateful inspection, proxies, and application level inspection where possible.

9. Make sure to check packets for correct source and destination addresses to keep malicious traffic from flowing to/from your network.

10. Make sure your firewall is physically secured as well. Just because your firewall is technically a logical security device does not mean it is susceptible to physical security attacks.

11. Follow the K.I.S.S (Keep it simple stupid) principle. Make sure your firewall configuration is as simple as possible.

12. Be sure to have regular security tests against the firewall including any VPN endpoints it hosts.

13. Make sure the firewall's operating system and application software is up to date with the latest patches. It is highly recommended to subscribe to your firewall's vendor's security bulletins.

14. Use firewalls internally to segment networks and permit access control based upon business needs.

15. Implement a secure remote syslog server that makes log modification and manipulation more difficult for a malicious attacker.

16. Require remote hosts to run their own personal firewall/IPS.

17. Regularly backup the firewall rule-base and configuration files. These backups should be kept offsite in a secure location.

Intrusion Detection and Prevention Systems
Administrators shall administer the following practices:

1. Monitor and tune one IDS at a time
2. Block nefarious traffic process
3. Build rules to alert an administrator in the event of attempted and successful attacks
4. Logs shall be reviewed regularly
5. Audits will be conducted regularly
6. Placement of IDS and IPS will be in all computer systems and network devices
Access Control List Configuration

1. Create an access baseline
2. Automate user provision
3. Find the business case
4. Tie access controls to your environment
5. Segregate access using rules
6. apply the doctrine of least access
7. channel administrators
8. terminate accounts with extreme prejudice
9. control remote access, plus application and database

Allow
Only validated traffic shall be allowed to access internal network architecture.

Deny-All
A deny-all rule must be applied in all access control list rules.

Network Architecture
The network architecture poses as the foundation of Company Co. Inc. LLC’s data infrastructure. It handles all traffic of sensitive and non-sensitive data. We construe the highest quality of data transfer amongst our employees, vendors, and clients. To do so, we integrate these best practices as minimal contingencies throughout our infrastructure.

Layered Security
Layering security allows architectures the ability to secure each segment with appropriate mechanisms. Layers within the network will be classified as perimeter, network, host, application, and data. Provided below is a list of minimal security mechanisms to be used to authenticate valid users and deviate against nefarious activity.

Perimeter Security
- Firewall
- Anti-Virus
- Virtual Private Network

Network Security
- Intrusion Detection and Prevention Systems
- Vulnerability Management System
- Network Access Control
- Access Control/ User authentication

Host Security
- Host Intrusion Detection and Prevention Systems
- Host Vulnerability Analysis
- Network Access Control
- Anti-Virus
- Access Control/ User authentication

**Application Security**
- Sandbox
- Access Control/ User authentication
- Input Validation

**Data Security**
- Encryption
- Access Control/ User authentication

**Redundancy**
Network schemes must have redundancy to improve availability in the event of a natural disaster. The function of redundancy is to ensure all networks have no downtime. Network administrators will integrate mesh and hybrid networks in appropriate areas for complete mediation.

**Labeling**
All network cables and switches must contain labels. Labeling scheme must follow proprietary labeling scheme for identification of source, destination, and function.

**Documentation**
Documentation is an important in ensuring all cables, systems, and network devices have been approved, implemented, and configured appropriately. In addition, administrators will have the ability to identify possible vulnerabilities and improve the network.

**Segregation**
Internal networks must not be open to the public. Company networks must be classified by perimeter and evaluated to assess specific classification to segregate internal networks and sensitive data.

**Audits**
Informal audits will be approved and authorized by the Computer Information Security Officer. Audits may be performed with or without informing users at any time.

**Updates**
Updates and patching must be made on a regular-basis. Changes in specified times may be applied. Updates must be downloaded and tested prior to implementation on live networks. Updates must be integrated during downtime to ensure patching and updates have not been compromised.

**Back-ups**
All sensitive information must be backed up in secure areas for quality information assurance.