The ultimate network security checklist

brought to you by

GFI Software™

Introduction

If you're tasked with network security, either because you work on the IT security team, or perhaps you are the entire IT team by yourself, here is a simple list you can follow, broken down by category, which includes some tips and tricks for getting the job done.

This is a document to provide you with the areas of information security you should focus on, along with specific settings or recommended practices that will help you to secure your environment against threats from within and without. Using this checklist as a starting point, and working with the rest of your IT team, your management, human resources, and your legal counsel, you will be able to create the ultimate network security checklist for your specific environment. That's an important distinction; no two networks are exactly the same, and business requirements, regulatory and contractual obligations, local laws, and other factors will all have an influence on your company's specific network security checklist, so don't think all your work is done. You'll need to tweak this to suit your own environment, but rest assured the heavy lifting is done!

We'll break this list down into broad categories for your ease of reference. Some of the breakdowns may seem arbitrary, but you have to draw lines and break paragraphs at some point, and this is where we drew ours.

1. User Accounts

Let's face it. Users are the weakest link in any network security scenario. But since they are also the reason we have IT and more to the point…a job…we need to make sure we take care of them and they take care of us. That's why they come first on this list.

Training

Before a user ever gets a network account, they need training on what to do, what not to do, and how to go about protecting themselves and the network. This needs to be done first, and repeatedly, with at least an annual review and update.

Unique accounts

No shared accounts…ever! Make sure every user gets a unique account that can be attributed only to them. Make sure they know the penalty for revealing their credentials to another is death by tickling.

Separation between normal user and privileged user accounts

This goes more for the sysadmins reading this than end users, so do as we say and not as you do…make sure you log on with a regular account, and only authenticate with your privileged

account when you need to do admin work. Otherwise, you never know when you might accidentally click something that runs with those elevated privileges.

Multifactor authentication

If you look at every major hack that has hit the news in the past couple of years, from TJ Max to Target to Premera to the Office of Personnel Management…one thing could have prevented them all. Two factor authentication. Every one of those hacks started with compromised credentials which were simply username and password. The most annoying of all these is that OPM was supposed to already be using 2FA, but wasn't. Of course, neither was most of the government. That has finally changed, but it's a little late for the millions of people whose personal information was stolen.

Up to date information

Keep the data current in your system. Make sure contact details, job titles, managers, etc. are all updated whenever there is a change so that if you do need to look something up on a user, you have what you need, and not their phone number from seven years ago when they were first hired.

Review of group memberships when roles change

Given least privilege, it needs to be standard operating procedure to review and revise group memberships and other access privileges when a user changes jobs. If their new role does not require access to resources that their old role gave them, remove that access.

No sharing of accounts between test and production, or between any two external services.

This one is critical. If you have multiple environments it may be very tempting to share credential specifics between them. That makes it much more likely that compromise can occur, especially if the lab or UAT environment doesn't have the same security measures as production does, or that the hack of one external service could reveal your credentials that could then be used to log onto other services. Pop quiz…is your username and password for Facebook the same as for Twitter? If you answered yes, you're doing it wrong.

Disable stale accounts. Delete the really old ones.

Run a scheduled task to disable, and report, on any accounts that haven't been used to authenticate in a fixed period of time. I think two weeks is good, but most would say 30 days. Have another run at least once a month that identifies accounts that have been disabled for 90 days, and deletes them. Old accounts can be 'resurrected' to provide access, through social engineering or oopses. Don't be a victim.

2. Policies

The best laid plans of mice and men oft go awry, and nowhere can this happen more quickly than where you try to implement network security without a plan, in the form of policies. Policies need to be created, socialized, approved by management, and made official to hold any weight in the environment, and should be used as the ultimate reference when making security decisions. As an example, we all know that sharing passwords is bad, but until we can

point to the company policy that says it is bad, we cannot hold our users to account should they share a password with another. Here's a short list of the policies every company with more than two employees should have to help secure their network.

- Acceptable Use Policy
- Internet Access Policy
- Email and Communications Policy
- Network Security Policy
- Remote Access Policy
- BYOD Policy
- Encryption Policy
- Privacy Policy

A great resource for policy starter files and templates is the SANS Institute at http://www.sans.org.

3. Provisioning Servers

Willie Sutton, a notorious American criminal, when asked why he robbed banks, answered "because that's where the money is." If you could ask a hacker why s/he breaks into servers they would probably reply with a similar answer "because that's where the data is." In today's society, data is a fungible commodity that is easy to sell or trade, and your servers are where most of your company's most valuable data resides. Here's some tips for securing those servers against all enemies, both foreign and domestic. Create a server deployment checklist, and make sure all of the following are on the list, and that each server you deploy complies 100% before it goes into production.

Server list

Maintain a server list (SharePoint is a great place for this) that details all the servers on your network. At a minimum it should include all the name, purpose, ip.addr, date of service, service tag (if physical,) rack location or default host, operating system, and responsible person. We'll talk about some other things that can be stored on this server list down below, but don't try to put too much onto this list; it's most effective if it can be used without side to side scrolling. Any additional documentation can be linked to or attached. We want this server list to be a quick reference that is easy to update and maintain, so that you do. Include in this list when the physical hardware goes out of warranty, and when the operating system goes into extended support, so you can track and plan for hardware replacement and operating system upgrades or server replacements.

Responsible party

Each server must have a responsible party; the person or team who knows what the server is for, and is responsible for ensuring it is kept up to date, and can investigate any anomalies associated with that server. Make sure to update this when people change roles.

Naming conventions

Naming conventions may seem like a strange thing to tie to security, but being able to quickly identify a server is critical when you spot some strange traffic, and if an incident is in progress, every second saved counts.

Network Configuration

Ensure that all network configurations are done properly, including static ip.addr assignments, DNS servers, WINS servers, whether or not to register a particular interface, binding order, and disabling services on DMZ, OOB management, or backup networks. Make sure to disable any interfaces that aren't being used so they don't grab an ip.addr or register their APIPA address in DNS if they do get connected to a live Ethernet port by mistake.

IPAM

All servers should be assigned static IP addresses, and that data needs to be maintained in your IP Address Management tool (even if that's just an Excel spreadsheet.) When strange traffic is detected, its vital to have an up to date an authoritative reference for each ip.addr on your network. Windows Server 2012 R2 includes IPAM services.

Patching

Every server deployed needs to be fully patched as soon as the operating system is installed, and added to your patch management application immediately.

Antivirus

All servers need to run antivirus software and report to the central management console. Scanning exceptions need to be documented in the server list so that if an outbreak is suspected, those directories can be manually checked.

Host intrusion prevention/firewall

If you use host intrusion prevention, you need to ensure that it is configured according to your standards, and reports up to the management console. Software firewalls need to be configured to permit the required traffic for your network, including remote access, logging and monitoring, and other services.

Remote access

Pick one remote access solution, and stick with it. I recommend the built-in terminal services for Windows clients, and SSH for everything else, but you may prefer to remote your Windows boxes with PCAnywhere, RAdmin, or any one of the other remote access applications for management. Whichever one you choose, choose one and make it the standard.

UPS and power saving

Make sure all servers are connected to a UPS, and if you don't use a generator, make sure they have the agent needed to gracefully shut down before the batteries are depleted. While you don't want servers to hibernate, consider spinning down disks during periods of low activity (like after hours) to save electricity.

Domain joined

Unless there's a really good reason not to, such as application issues or because it's in the DMZ, all Windows servers should be domain joined, and all non-Windows servers should use LDAP to authenticate users against Active Directory. You get centralized management, and a single user account store for all your users.

Administrator account renamed and password set

Rename the local administrator account, and make sure you set (and document) a strong password. It's not a foolproof approach, but nothing in security is. We're layering things here.

Local group memberships set and permissions assigned

Make any appropriate assignments using domain groups when possible, and set permissions using domain groups too. Only resort to local groups when there is no other choice, and avoid local accounts.

Correct OU with appropriate policies

Different servers have different requirements, and Active Directory Group Policies are just the thing to administer those settings. Create as many OUs as you need to accommodate the different servers, and set as much as possible using a GPO instead of the local security policy.

Confirm it is reporting to management consoles

No matter what you use to administer and monitor your servers, make sure they all report in (or can be polled by) before putting a server into production. Never let this be one of the things you forget to get back to.

Unnecessary services disabled

If a server doesn't need to run a particular service, disable it. You'll save memory and CPU, and it's one less way bad guys will have to get it. But don't just disable something because you don't know what it does. Confirm what you are doing and be sure that you double-check when configuring new applications that may need a service.

SNMP configured

If you are going to use SNMP, make sure you configure your community strings, and restrict management access to your known systems.

Agents installed

Backup agents, logging agents, management agents; whatever software you use to manage your network, make sure all appropriate agents are installed before the server is considered complete.

Backups

If it's worth building, it's worth backing up. No production data should ever get onto a server until it is being backed up.

Restores

And no backup should be trusted until you confirm it can be restored.

Vulnerability scan

If you really think the server is ready to go, and everything else on the list has been checked off, there's one more thing to do; scan it. Run a full vulnerability scan against each server before it goes into production to make sure nothing has been missed, and then ensure it is added to your regularly scheduled scans.

Signed into production

Someone other than the person who built the server should spot check it to be sure it's good to go, before it's signed into production. By "signing" it, that user is saying they confirmed the server meets your company's security requirements and is ready for whatever the world can throw at it. That person is also the second pair of eyes, so you are much less likely to find that something got missed.

4. Deploying workstations

Making sure that the workstations are secure is just as important as with your servers. In some cases it's even more so, since your servers benefit from the physical security of your datacenter, while workstations are frequently laptops sitting on table tops in coffee shops while your users grab another latte. Don't overlook the importance of making sure your workstations are as secure as possible.

Workstation list

Keep a list of all workstations, just like the server list, that includes who the workstation was issued to and when its lease is up or it's reached the end of its depreciation schedule. Don't forget those service tags!

Assigned user

Track where your workstations are by making sure that each user user's issued hardware is kept up to date.

Naming conventions

It's very helpful when looking at logs if a workstation is named for the user who has it. That makes it much easier to track down when something looks strange in the logs.

Network Configuration

You probably will assign IP addresses using DHCP, but you will want to make sure your scopes are correct, and use a GPO to assign any internal DNS zones that should be searched when resolving flat names.

Patching

Since your users are logged on and running programs on your workstations, and accessing the Internet, they are at much higher risk than servers, so patching is even more important. Make sure all workstations are fully up to date before they are deployed, update your master image frequently, and ensure that all workstations are being updated by your patch management system.

Antivirus

Here's how to handle workstation antivirus. 100% coverage of all workstations. Workstations check a central server for updates at least every six hours, and can download them from the vendor when they cannot reach your central server. All workstations report status to the central server, and you can push updates when needed. Easy.

Host intrusion prevention/firewall

Consider using a host intrusion prevention or personal firewall product to provide more defense for your workstations, especially when they are laptops that frequently connect outside the corporate network. Make sure that the configuration does not interfere with your management tasks, like pushing antivirus updates, checking logs, auditing software, etc.

Remote access

Much like servers, pick one remote access method and stick with it, banning all others. The more ways to get into a workstation, the more ways an attacker can attempt to exploit the machine. The built-in Remote Desktop service that comes with Windows is my preference, but if you prefer another, disable RDP. Ensure that only authorized users can access the workstation remotely, and that they must use their unique credential, instead of some common admin/password combination.

Power saving

Consider deploying power saving settings through GPO to help extend the life of your hardware, and save on the utility bill. Make sure that you have Wake-On-LAN compatible network cards so you can deploy patches after hours if necessary.

Domain joined

All workstations should be domain joined so you can centrally administer them with unique credentials.

Administrator account renamed and password set

Rename the local administrator account and set a strong password on that account that is unique per machine. Trust me, one of these days you will have no choice but to give some travelling user the local admin account, and if that is the same across all machines, you will then have to reset them all. Use a script to create random passwords, and store them securely where they can be retrieved in an emergency. It seems like a lot of work up front, but it will save you time and effort down the road. If you must use a domain account to remote into a machine, use one that ONLY has permissions to workstations so that no attacker can run a Pass The Hash attack on you and use those creds to get onto servers.

Local group memberships set and permissions assigned

Set appropriate memberships in either local administrators or power users for each workstation.

Correct OU with appropriate policies

Organize your workstations in Organizational Units and manage them with Group Policy as much as possible to ensure consistent management and configuration.

Confirm its reporting to management consoles

Validate that each workstation reports to your antivirus, patch management, and any other consoles before you turn it over to the user, and then audit frequently to ensure all workstations report in.

Backups/ Restores

You probably won't perform regular full backups of your workstations, but consider folder redirection or Internet based backups to protect critical user data.

Local encryption

There is no excuse for letting any laptop or portable drive out of the physical confines of the office without encryption in place to protect confidential data. Whether you use Bitlocker, third party software, or hardware encryption, make it mandatory that all drives are encrypted.

Vulnerability scan

Perform regular vulnerability scans of a random sample of your workstations to help ensure your workstations are up to date.

5. Network equipment

Your network infrastructure is easy to overlook, but also critical to secure and maintain. We'll start with some recommendations for all network equipment, and then look at some platform specific recommendations.

Network hardware list

Maintain a network hardware list that is similar to your server list, and includes device name and type, location, serial number, service tag, and responsible party.

Network Configuration

Have a standard configuration for each type of device to help maintain consistency and ease management.

IPAM

Assign static IP addresses to all management interfaces, add A records to DNS, and track everything in an IP Address Management (IPAM) solution.

Patching

Network hardware runs an operating system too, we just call it firmware. Keep up to date on patches and security updates for your hardware.

Remote access

Use the most secure remote access method your platform offers. For most, that should be SSH version 2. Disable telnet and SSH 1, and make sure you set strong passwords on both the remote and local (serial or console) connections.

Unique credentials

Use TACACS+ or other remote management solution so that authorized users authenticate with unique credentials.

SNMP configured

If you are going to use SNMP, change the default community strings and set authorized management stations. If you aren't, turn it off.

Backups/Restores

Make sure you take regular backups of your configurations whenever you make a change, and that you confirm you can restore them.

Vulnerability scan

Include all your network gear in your regular vulnerability scans to catch any holes that crop up over time.

VLANs

Use VLANs to segregate traffic types, like workstations, servers, out of band management, backups, etc.

Promiscuous devices and hubs

Set port restrictions so that users cannot run promiscuous mode devices or connect hubs or unmanaged switches without prior authorization.

Disabled ports

Ports that are not assigned to specific devices should be disabled, or set to a default guest network that cannot access the internal network. This prevents outside devices being able to jack in to your internal network from empty offices or unused cubicles.

Explicit permits, implicit denies

Deny all should be the default posture on all access lists, inbound and outbound.

Logging and alerts

Log all violations and investigate alerts promptly.

Routing protocols

Use only secure routing protocols that use authentication, and only accept updates from known peers on your borders.

6. Vulnerability scanning

Weekly external scans scheduled

Configure your vulnerability scanning application to scan all of your external address space weekly.

Diffs compared weekly

Validate any differences from one week to the next against your change control procedures to make sure no one has enabled an unapproved service or connected a rogue host.

Internal scans scheduled monthly

Perform monthly internal scans to help ensure that no rogue or unmanaged devices are on the network, and that everything is up to date on patches.

7. Backups

Tape rotation established

Make sure you have a tape rotation established that tracks the location, purpose, and age of all tapes. Never repurpose tapes that were used to backup highly sensitive data for less secure purposes.

Old tapes destroyed

When a tape has reached its end of life, destroy it to ensure no data can be recovered from it.

Secure offsite storage

If you are going to store tapes offsite, use a reputable courier service that offers secure storage.

Encryption

Even reputable courier services have lost tapes, so ensure that any tape transported offsite, whether through a service or by an employee, is encrypted to protect data against accidental loss.

Restores confirmed regularly

Backups are worthless if they cannot be restored. Verify your backups at least once a month by performing test restores to ensure your data is safe.

Restricted access to tapes, backup operators groups

Backup tapes contain all data, and the backup operators can bypass file level security in Windows so they can actually back up all data. Secure the physical access to tapes, and restrict membership in the backup operators group just like you do to the domain admins group.

8. Remote Access

Only approved users and methods

Set up and maintain an approved method for remote access, and grant permissions to any user who should be able to connect remotely, and then ensure your company policy prohibits other methods.

Two factor authentication

Consider using two factor authentication, like tokens, smart cards, certificates, or SMS solutions, to further secure remote access.

No split tunneling

Protect your travelling users who may be on insecure wireless networks by tunneling all their traffic through the VPN instead of enabling split tunneling.

Internal name resolution

If you are going to do split tunneling, enforce internal name resolution only to further protect users when on insecure networks.

Account lockouts

Set strong account lockout policies and investigate any accounts that are locked out to ensure attackers cannot use your remote access method as a way to break into your network.

Regular review of audit logs

Perform regular reviews of your remote access audit logs and spot check with users if you see any unusual patters, like logons in the middle of the night, or during the day when the user is already in the office.

9. Wireless

In addition to the items in the network equipment list above, you want to ensure the following for your wireless networking.

SSID

Use an SSID that cannot be easily associated with your company, and suppress the broadcast of that SSID. Neither are particularly effective against someone who is seriously interested in your wireless network, but it does keep you off the radar of the casual war driver.

Authentication

Use 802.1x for authentication to your wireless network so only approved devices can connect.

Encryption

Use the strongest encryption type you can, preferable WPA2 Enterprise. Never use WEP. If you have bar code readers or other legacy devices that can only use WEP, set up a dedicated SSID for only those devices, and use a firewall so they can only connect to the central software over the required port, and nothing else on your internal network.

Guest Network

Use your wireless network to establish a guest network for visiting customers, vendors, etc. Do not permit connectivity from the guest network to the internal network, but allow for authorized users to use the guest network to connect to the Internet, and from there to VPN back into the internal network, if necessary.

BYOD

Create a "Bring Your Own Device" policy now, even if that policy is just to prohibit users from bringing their personal laptops, tablets, etc. into the office or connecting over the VPN.

10. Email

Inbound and outbound filtering

Deploy an email filtering solution that can filter both inbound and outbound messages to protect your users and your customers.

Directory Harvest prevention

Ensure that your edge devices will reject directory harvest attempts.

Antivirus/Antispam/Antiphishing

Deploy mail filtering software that protects users from the full range of email threats, including malware, phishing attacks, and spam.

11. Internet Access

Provide your users with secure Internet access by implement an Internet monitoring solution.

Filter lists

Use filter lists that support your company's acceptable use policy.

Malware scanning

Scan all content for malware, whether that is file downloads, streaming media, or simply scripts contained in web pages.

Bandwidth restrictions

Protect your business critical applications by deploying bandwidth restrictions, so users' access to the Internet doesn't adversely impact company functions like email, or the corporate website.

Port blocking

Block outbound traffic that could be used to go around the Internet monitoring solution so that if users are tempted to violate policy, they cannot. Remember, not every browser will honor GPO settings and not every app will process what's in a PAC or WPAD. You don't want any holes in your defences.

12. Fileshares

Here's where most of the good stuff sits, so making sure your secure your fileshares is extremely important.

Remove everyone and authenticated users

The default permissions are usually a little too permissive. Remove the Everyone group from legacy shares, and the authenticated users group from newer shares, and set more restrictive

permissions, even if that is only to "domain users." This will save you a ton of time should you ever have to set up a share with another entity.

Least privilege

Always assign permissions using the concept of "least privilege." "Need access" should translate to "read only" and "full control" should only ever be granted to admins.

Groups

Never assign permissions to individual users; only use domain groups. It's more scalable, easier to audit, and can carry over to new users or expanding departments much more easily than individual user permissions.

Avoid Deny Access

If you have a file system that tempts you to use "Deny Access" to fix a "problem" you are probably doing something wrong. Reconsider your directory structure and the higher level permissions, and move that special case file or directory somewhere else to avoid using Deny Access.

Auditing

If there is any sensitive data at all in there, turn on auditing and make sure the data owner reviews the logs regularly for any inappropriate access. Don't just audit failures, or changes. If the wrong user simply reads a file, bad things could happen.

13. Log correlation

If you have more servers than you can count without taking off your shoes, you have too many to manually check each one's logs by hand. Use a logging solution that gathers up the logs from all your servers so you can easily parse the logs for interesting events, and correlate logs when investigating events.

14. Time

Use a central form of time management within your organization for all systems including workstations, servers, and network gear. NTP can keep all systems in sync, and will make correlating logs much easier since the timestamps will all agree. Make sure all your VM hosts, your Active Directory PDC emulator, all of your network gear, your SEM, your video camera system, and your other physical security systems are all configured to use this same time source so that you know correlation between events will be accurate.

There is a lot of stuff to do to make sure your network is as secure as can be, so tackle this the same way you would eat an elephant…one bite at a time. Make 2016 the year you get your security house in order, and you will be well on your way to ensuring you won't be front page news in 2017.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States, UK, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

More information about GFI can be found at http://www.gfi.com.

GFI Software™

For a full list of GFI offices/contact details worldwide,

please visit: www.gfi.com/contact-us