TitanHQ™

Complete Network Security Checklist

Make sure your network and organization are secure against threats internally and externally

The Key Cyber Threats Threatening the Working from Home Movement

This checklist gives you the tips and tricks needed to get you started and guides you to the areas of IT security you need to focus on.

1. Policies / Rules

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

2. Provisioning Servers

In today's society, data is a valuable commodity that's easy to sell or trade, and your servers are where most of your company's most valuable data resides. Here are some tips for securing those servers against all threats. 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 - A quick reference that is easy to update and maintain

Maintain a server list that details all the servers on your network - including name, purpose, ip.addr, date of service, service tag (if physical), rack location or default host, operating system, and responsible person.

Responsible party per server

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.

Naming Convention

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, 00B management, or backup networks.

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, it's vital to have an up-to-date and authoritative reference for each ip. addr on your network.

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.

Anti-virus

All servers need to run antivirus software and report to the central management console. Scanned 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, that 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.

2. Provisioning Servers

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 reporting to managment 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.

Disable unneccesary services

If a server doesn't need to run a particular service, disable it. You'll save memory and CPU.

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 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.

3. Deploying workstations

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's issued hardware is kept up-to-date.

Naming Convention

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'll probably 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.

Anti-virus

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.

Remote Access

Like servers, pick one remote access method and stick to it, banning all others. The more ways to get into a workstation, the more ways an attacker can attempt to exploit the machine. 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 & password set

Use a script to create random passwords, and store them securely where they can be retrieved in an emergency scheduled scans.

Local Group memberships set & 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 managment 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.

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, TrueCrypt, or hardware encryption, make is 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.

TitanHQ™

Complete Network Security Checklist

Make sure your network and organization are secure against threats internally and externally

4. 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 Manage¬ment (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 / Stores

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.

Switchs

- Server
- Network Switch
- Printer
- PC
- ADSL modem

VLANs

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

Promiscous devices & 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.

Firewalls

1) Explicit Permits, implicit denies
'Deny All' should be the default posture on all access lists - inbound and outbound.

2) Logging & Alerts
Log all violations and investigate alerts promptly.

Routers & Routing protocol

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

5. Vulnerability Scanning

Weekly external scan scheduled

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

Differences 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 schedules 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.

6. 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; ensure that any tape transported offsite, whether through a service or by an employee, is encrypted to protect data against accidental loss.

Restricted access to tapes, Backup Operaters Group

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 admin group.

Restores Completed 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.

7. Remote Access

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.

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

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

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.

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

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

8. Wireless Networking

SSID

Use an SSID that cannot be easily associated with your company, and suppress the broadcast of that SSID. Both aren't 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.

Encryption

Use the strongest encryption type you can, preferably WPA2 Enterprise. Never use WEP. If you have barcode 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.

Authentication

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

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.

TitanHQ™

Complete Network Security Checklist

Make sure your network and organization are secure against threats internally and externally

9. Email

- Use a multi-layered protection approach: don't rely only on your mail servers filtering capabilities, also add a third party dedicated solution to filter your mail and help your users and your company protected.
- Deploy an email filtering solution that can filter both inbound and outbound messages to protect your users and your customers.
- Ensure that your edge devices will reject directory harvest attempts.
- Deploy mail filtering software that protects users from the full range of email threats, including malware, phishing, and spam.

10. Internet Access

OTG (On The Go) protection

Protect your users when they are not in the office with 'On The Go' solutions that can help filter traffic on their laptops and identify when they are in the office and need to use the office filtering solution.

Internet Security

Use internet filters when possible to protect your users and business from malicious websites. Ransomware is one of the most devastating type of cyber attacks right now. Provide your users with secure Internet access by implementing an Internet monitoring solution.

Encryption

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 users are tempted to violate policy.

11. File shares

Remove the everyone and authenticated user groups

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".

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.

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.

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.

12. Loq 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 manually. 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.

13. 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. Security is not an easy thing and is a very sensitive and complex area, so don't try to do it all by yourself. There are lots of excellent, experienced managed service providers and security experts available that have the knowledge you need to help you protect your business.