

Network Security White Paper

The 7 Must-Do's of IT Security

Table of Contents

Executive Summary	3
IT Challenges	3
Must-Do #1 – Antivirus Software	4
Must-Do #2 - Antispam	4
Must-Do #3 – Patch Management	5
Must-Do #4 – System Logging (SYSLOG).....	5
Must-Do #5 – Off-Site, Encrypted Data Backups.....	6
Must-Do #6 – Security Audit	6
Must-Do #7 – Managed Firewall	7
Conclusion	8

The 7 Must-Do's of IT Security

Executive Summary

Are you doing all that you can to secure your network and to protect member data? Knowing what to do can be confusing. Opinions on what services and methods to secure your network can vary from vendor to vendor, as well as from examiner to examiner.

When all is said and done, there are seven principles to network security that every credit union should follow. These principles will provide the foundation on which a secure network can be developed.

But can you afford to do all seven steps? You can't afford not to.

IT Challenges

As a small credit union, you are asked to comply with the same network security principles as the larger credit unions. In addition, you may not employ an IT staff and adding additional tasks or workload to your existing staff is not possible.

In many cases, the follow seven must-do's can be installed and maintained with little IT assistance, or can be outsourced to a trusted network security vendor.

Must-Do #1 – Antivirus Software

It seems that network security and threat prevention all began with antivirus software years ago, yet many credit unions fail to implement and maintain adequate antivirus protection.

1. Every workstation and file server needs to have industry standard antivirus protection software installed on it. Industry standard would refer to vendors such as McAfee, Symantec, Norton, Kaspersky, or Trend Micro. “Freeware” products aren’t industry standard.
2. Annual support licenses need to be paid for to maintain current status of your antivirus software. Antivirus software is not a one-time purchase, but rather an active license.
3. Your antivirus software is only as good as the latest definition file. Make sure that all computers have the latest antivirus software. Most antivirus software licenses come with management software to assist in maintaining the software. Implement and use it.

Must-Do #2 - Antispam

Spam email is no longer a nuisance or inconvenience. The primary purpose of spam is to transport malware, Trojans, and other threats. An antispam service is required to help reduce the possibility of infection from spam email.

1. Reduce the amount of spam or junk email that arrives into your email inbox by implementing an antispam service.
2. Don’t be afraid of having that “important email” blocked. Antispam services allow you to review the email messages that are blocked. Frequent senders can be added to a “whitelist” so that their email messages will not be blocked in the future.
3. If you receive an email and you don’t know who the sender is, delete it.
4. Protect all of your email accounts. Many free on-line email services such as Google and Yahoo include antispam services.
5. For business, use a hosted or in-house antispam solution to scan all email before it gets to your email server or email client.
6. See Postini, GFI, SonicWALL, MailWise, or Symantec for quality products.

Must-Do #3 – Patch Management

Malware, Trojans, Worms, and other threats are designed to take advantage of known vulnerabilities within an operating system or software application. Patches are provided by software vendors to “seal up” these known vulnerabilities as they are discovered. Failure to apply patches will leave your computers at great risk of infection and exposure.

1. Using an auto-update service isn't good enough. You need to validate through reporting tools that all workstations and file servers have received the latest software patches that are available from all tier-one software vendors.
2. Microsoft appears to be the biggest culprit. But, they're not the only software vendors that deploy patches. Make sure that all programs and software on your computers are updated.
3. Subscribe to news services that announce or publish when software patches have become available. These alerts are available from all major software vendors.
4. Review reports about patches on web based news services. NetworkWorld news reports at www.networkworld.com/topics/patchmanagement.html is a good one.

Must-Do #4 – System Logging (SYSLOG)

All network devices that support the SNMP protocol create log files detailing activities within the device such as logins, file changes, firmware updates, etc. The collection of this data is important as a means of providing forensic information to be used in the event of a network breach.

1. File servers, routers, firewalls, and most network devices automatically create these system log (SYSLOG) files.
2. The data within SYSLOG's includes any and all changes made to the equipment as well as user actions within the network.
3. Too much time would be required to go to each device to capture the data. Use a SYSLOG reporting tool or service to automatically capture this data and to format it in a way that presents the information as readable and useful.
4. These data logs can be very large. Again, their real value is for forensics purposes.

Must-Do #5 – Off-Site, Encrypted Data Backups

Critical member data and operational data files should be stored only on file servers, and all file server data should be backed up incrementally throughout the day, or at a minimum, on a nightly basis.

1. Any type of tool used to backup data should be based on a system or service that is unattended. Systems that require user intervention never work.
2. Multiple retentions of all data backups should be created. This would include daily, weekly, monthly, and annual copies of all data. If using a tape based system to backup your data, keep all legacy hardware and software. Often, tape hardware and software is not “backward” compatible.
3. All data backups must be encrypted. 128-bit encryption is the current industry standard.
4. All data backups need to be transported to an off-site location. If using tapes, use a bonded courier for this service. Never take the data off-site yourself. Never take the data home!
5. Consider replacing your tape backup service with an electronic service like EVault. With EVault, your data is encrypted and then electronically transferred to an off-site, SAS70 compliant data vault. See www.evault.com for more information on their service.
6. Whatever process you use, test data restores and document the process. Perform testing of data restores on a very frequent basis.

Must-Do #6 – Security Audit

The network should be inspected by an independent security auditor who is familiar with auditing the types of network systems used by financial institutions. The inclusion of host (core) systems can provide a unique experience when auditing networks.

1. Perform network security audits on an annual basis, at the minimum.
2. Include “social engineering” and staff education in your security audit. Most network breaches are due to mistakes made by staff.
3. Review the audit with the auditor and clearly understand their recommendations. Many audit reports are very technical and can lead to frustration or inaction.
4. Listen to your auditor’s recommendations and be willing to make changes.

Must-Do #7 – Managed Firewall

A firewall is the primary and often the first line of defense against Internet based threats. Most efforts, time, and dollars should be spent at this entry-point to ensure network security.

1. Do you have a firewall, or is it a router? Many credit unions still have routers installed in place of a firewall. There is a difference.
2. Is your firewall more than 3-years old? If so, it is unlikely that it is able to protect against today's threats.
3. Modern firewall appliances are *dynamic*, not *static*. They receive software updates on a daily basis to protect your environment from the latest threats.
4. In addition to basic firewall service such as port configuration, a modern firewall appliance should also run software services such as intrusion detection, content filtering, gateway antivirus, and antispysware.
5. Make sure that you use a firewall or firewall service that provides detailed reports. Reports help to validate that the services are being performed.
6. Because of the critical nature of a firewall, it is best to outsource and to use a managed firewall service that ensures that your firewall is being maintained and managed on a 24/7 basis.

Conclusion

This list does not represent all tasks and services that should be done to protect a network environment. It only represents those tasks and services that should be done at a very minimum. Yet, though years of our work with credit unions and other financial institutions, we find that sometimes these basic steps towards network security are overlooked.

Btech is a managed security services provider that can help your credit union implement and maintain services to maintain your network security.

For more information on Btech solutions and services, visit www.btechonline.com or call 626-397-1045.