Netsurion™

CYBER SECURITY BOOT CAMP 101

Cyber Security Boot Camp 101

Published in 2016 by Netsurion

On the web: www.netsurion.com

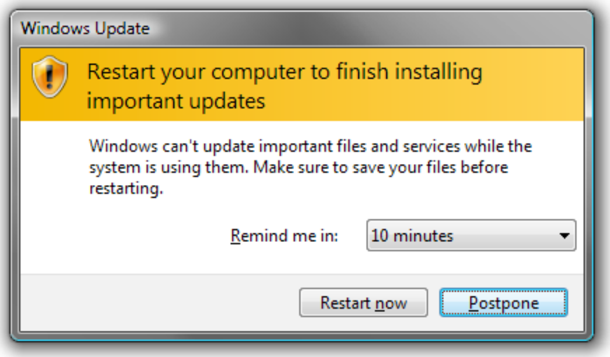
CONTENTS

In this eBook, we will explore some of the basic ways that businesses of all sizes can keep their computer systems safer. While it is impossible to say that a system can never be breached, if you deploy some basic steps to help protect your system and your data, then you are far less likely to experience a breach.

In the first article, we will discuss system and application patching. The second article continues to explore some of the basic ways that businesses of all sizes can keep their computer systems safer, including use of anti-virus protection. In the third article, we will discuss basic computer safety, including programs, ports, and services. The fourth article focuses on data and ways to keep track of where sensitive data resides and where it is going. In the fifth and final article, we will go over the use of remote-access software and what you need to look for to remain secure.

THE VIRTUES OF ONGOING PATCH UPDATES

A patch is a piece of software designed to update a computer program or its supporting data in order to fix or improve security vulnerabilities. Patching can improve the usability and performance of a machine.



Windows Update

Restart your computer to finish installing important updates

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in: 10 minutes

Are you keeping up with regular computer operating patches and the programs that run on it? Many of the breaches that make the news (and those that don't make headlines) are caused by reactive patches that a vendor deployed in response to a threat. When vendor-issued patches aren't supported or used properly, they can be impacted by holes in the software, also known as zero-day vulnerabilities.

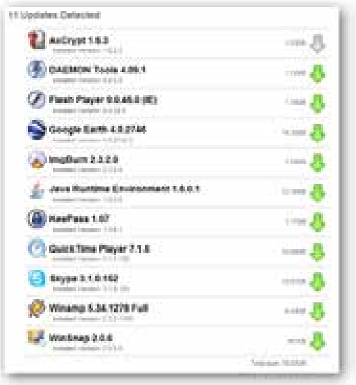
If you buy a new computer (PC) from a local computer retailer, chances are you have had to update it with a lot of patches soon after taking it out of the box. These updates come out typically on a monthly basis, and they should be allowed to download to your system and be applied. In larger companies where there are hundreds or thousands of computers to update, there will most likely be a commercial patching solution used that can download the update files once and then apply them to all the systems that need them on a rolling basis.

Don’t delay: allow patches to be applied that day.

There are times in which patches want to update your system and then reboot, and the timing may not have aligned with your plans. It is ok to postpone the application of patches until later in your day or when you are shutting down the computer, but you should never delay more than needed. Should you not be able to follow the same-day rule, then my advice is to not go more than 48 hours after the patches are available to get them applied.

What is being referred to above is mostly the operating systems patches, but what about third-party programs such as Adobe, Java, Flash, etc.? These too need to be updated often, and even though it may be annoying to see a pop-up on your screen notifying you of available updates, you should always take the time to apply the latest patches/updates to keep your system protected. Even if you don’t use a particular program, but it is installed on your computer, you should keep that up-to-date as well so it cannot be exploited.

There are even free utilities such as Update Checker from FileHippo that can run as a separate program and check your computer to see what available updates exist for you. According to FileHippo, “The Update Checker will scan your computer for installed software, check the versions, and then send this information to FileHippo.com to see if



11 Updates Detected

AxCrypt 1.6.3
DAEMON Tools 4.09.1
Flash Player 9.0.45.0 (IE)
Google Earth 4.0.2746
ImgBurn 2.3.2.0
Java Runtime Environment 1.6.0.1
KeePass 1.07
QuickTime Player 7.1.6
Skype 3.1.0.152
Winamp 5.34.1278 Full
WinSnap 2.0.6

Update Checker, a free software client from FileHippo, can scan your computer's installed software for available updates for you to download.

Visit FileHippo >

there are any newer releases. These updates are then neatly displayed in your browser for you to download." The Update Checker works on any PC running Windows 8, 7, Vista, XP, 2012, 2008, 2003, 2000, ME, or 98. I have found this utility particularly useful for keeping applications like Skype, Google Earth, etc. up-to-date.

What happens if you don't apply patches?

If you leave your systems unpatched, then hackers or software exploits may use holes in older versions of software to find a way to get into your computer and/or steal your data. Hackers could also use these software weaknesses in unpatched software to gain information about you and your web activities in order to scam you later via email or phone. Perhaps the worst example is the rise of Ransomware, in which the contents of your hard drive are locked until you pay a ransom to the hackers.

Keep in mind that a compromised system may hurt not only that one system. If you use your computer on a network that includes other computers, your issue could impact them as well. If you use a laptop at home and it gets compromised, then you bring the laptop to work, that issue could follow you to your workplace and affect the other computers on the corporate network.

In summary

It is a best practice to keep your system up-to-date at all times. Be sure to turn on any automatic updates that are available to your operating system. If you need to use a utility to scan your computer for third-party applications that may need updates, be sure to find one you can trust, like the Update Checker noted above, and use it regularly.

ANTI-VIRUS PROTECTION MADE SIMPLE

While it is impossible to say that a system can never be breached, if you are not doing some of the basics to help protect your system and your data, then you are more likely to experience a breach.

A computer virus is a type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its own source code) or infecting other computer programs by modifying them. Infecting computer programs can include data files or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. The term "virus" is also commonly, but erroneously, used to refer to other types of malware.[1]

More than 317 million pieces of malware (computer viruses or other malicious software) were created in 2014 alone[2]. That's more than 1 million new threats released each day on average.

Viruses only target Windows-based computers, right?

While Windows-based systems may be a much easier target for many virus writers, over the past few years there has been more news in the press and

[1] Wikipedia
[2] Symantec

on security blogs about viruses being designed specifically for Apple devices running the latest IOS operation system.

Why do viruses get written and distributed?

There are probably many answers to this question. The simple truth is that they are designed by those looking to do bad things to others by taking their systems offline or by stealing data. Viruses can be designed by nations looking to attack their enemies, or by those that want revenge on their employers, or those that have done them wrong in school, and even within their circle in social media.

> In 2015, there were 38 percent more security incidents detected than in 2014.
>
> – "The Global State of Information Security Survey 2016" | PWC

How do you protect yourself against computer viruses?

The best defense against computer viruses is a solid anti-virus product. While it may be tempting to download a free product simply because it is free and got good reviews, be careful. You know what they say: You "get what you pay for". When it comes to good solid anti-virus protection, it will most likely cost you a little money and be well worth the investment.

What about the anti-virus product I got when I bought the computer?

If you bought your computer from a local retailer, it most likely came with a trial edition of some commercial anti-virus solution. These trials are usually time limited, such as a 90, 120, or a one-year subscription. During that trial, these solutions are fine, but if you do not renew the subscription, you are leaving your computer potentially unprotected and open to be compromised.

What is a good anti-virus product?

This is a loaded question, as many people are as passionate about anti-virus companies as they are about religion or politics. I personally like products that are easy to use and that don't slow my system down too much when they are on. Recently I have turned to products that can be managed from the cloud, such as Sophos Cloud Protection, but I also like products from TrendMicro and Webroot too.

Another thing to mention about anti-virus software is that it's only good if it is enabled and up-to-date. What I mean by this is if you have five computers at home or in your office, all five need to have anti-virus installed, and they all need to be up-to-date.

When I say they need to be enabled, I have performed several audits in the past in which a client had anti-virus software, but certain key features were not enabled or disabled due to the fear that by enabling them it may slow down the computer.

I have a built-in anti-virus product as part of Windows – isn't that enough?

The short answer is probably not. While the product that is built into Windows is better than nothing, various tests done by industry experts have proven that other products provide more comprehensive protection, which is very important in today's world of ever-changing threats.

What else can I do?

Another piece of advice I can offer against the dangers of viruses and emerging threats such as Ransomware is: Backup your data.

> $209 million was paid to ransomware criminals from Jan. – Mar. 2016.
>
> — CNN

Backup your data to a cloud-based or external storage location and keep it disconnected from your computer unless you need to connect it. For example, using an online storage provider such as Carbonite is great – you can back up your data and it is stored with them in the cloud. If your computer is infected with a virus, you can have your computer reformatted, and then when it is clean and ready to be used again, you can get your files from the cloud storage location and continue your use. Obviously, backing up infected files will not help you recover them clean when needed, so it's best to keep several versions of backup jobs from your computer so you can go "back in time" as needed to get files restored that are clean and virus-free.

In summary

It is a best practice to use a good anti-virus product and to keep it up-to-date at all times. Using anti-virus software doesn't mean that a virus cannot get into your computer, but without good virus protection, you are simply asking for trouble.

BASIC COMPUTER SAFETY: PROGRAMS, PORTS, AND SERVICES

While it is impossible to say that a system can never be breached, if you are not doing some of the basics to help protect your system and your data, then you are more likely to experience a breach.

Installed program pitfalls.

Many computer users are unaware of the various programs that may be running on their computer.

Whether it's that they installed the program months or years ago and have now forgotten it was there, or maybe it's that they know about the program but they don't use it regularly. It could also be that they use the program every day but they don't know enough about computers to know how it works and whether or not it is leaving their system open to hackers and malware.

If you are unsure of what programs are installed on your computer, take a look. If you use a Windows-based system, navigate to the Control Panel and look under Programs and Features to see a list of programs that are currently installed on

⚠

Before you uninstall programs, be sure to have a good backup of your PC.

your system. Caution – before you proceed – be sure you have a good backup of your PC – just in case.

The Control Panel is a good place to check for unknown or unwanted programs that can be uninstalled, but be careful, some of the things listed here are utilities and drivers that make your PC work – so if you accidentally remove those items, you could make your PC not work any longer.

What do I look for exactly?

A good piece of advice is to sort this list by the date that it was installed and examine the list from the most recently installed items to those installed a long time ago.

Look for programs that just appear strange to you, such as printer drivers for printers you don't have connected to your PC, or coupon printers that you don't recall installing, or other applications that make absolutely no sense to you.

> The median number of days that attackers stay dormant within a network before detection is over 200.
>
> – "Microsoft Advanced Threat Analytics" | Microsoft

The other thing to focus on when reviewing this list are applications that you may have once installed for a reason but no longer use or need. If you don't need to use them, remove them. This will save space on your hard drive and will help you as we progress through the review of the remaining items in this article.

If you decide to uninstall some programs, you should reboot your system after you are done.

What about ports?

When we discuss ports, we are discussing TCP and UDP ports. In the internet protocol suite, a port is an endpoint of communication in an operating system. While the term is also used for hardware devices, in software it is a logical construct that identifies a specific process or a type of network service.[3]

Why do I care about ports?

Knowing what ports are open and listening for traffic to/from your PC is a big part of computer security. For example, if you happen to be running an FTP server on your PC but don't know it, you could be exposing holes on your PC that others (hackers) could use to get into your system to steal data.

You can use the NETSTAT command to quickly see all the used and listening ports on your computer. This article on Speed Guide explains this method.

Visit Speed Guide >

One way to find out what ports your computer is on is to use your PC's NETSTAT command. If you are comfortable with computers and want a more comprehensive test that you can run on your own, using the Network Mapper (NMAP) utility is a favorite choice for many.

Using the NMAP utility will not only tell you what ports are open on a system, but the utility will also try to determine the operating system of the device that is tested. This utility is a great way to inventory all the devices on your home or corporate network as well (if used on a corporate network, be sure you have permission to use it before you start scanning the network).

NMAP is a free and open source utility for network discovery and security auditing, which is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

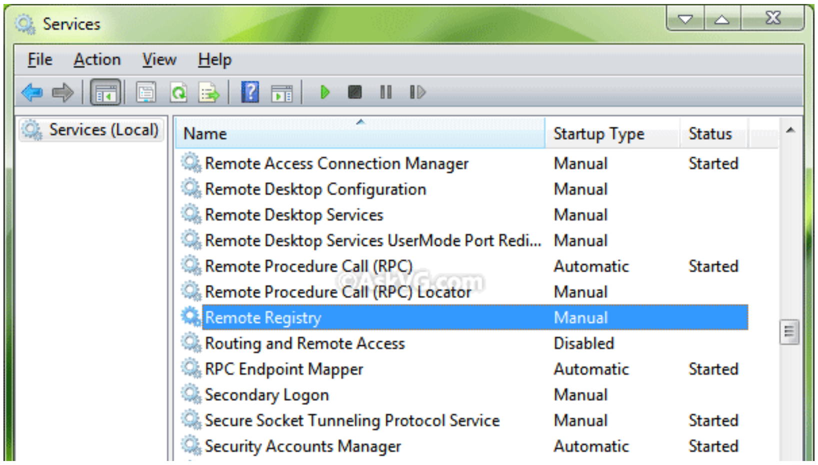
Visit NMAP >

What about services?

Services go along with programs that are installed on your computer, and by reviewing what services are running, you can learn a lot about your system and potentially speed things up a bit too.

[3] Wikipedia

To review services on a Windows-based system, go to Computer Management and click the Services link. From there you will see a list of services and their statuses (running or not running), along with information about the service (usually) and the user account that the service runs under.



Name	Startup Type	Status
Remote Access Connection Manager	Manual	Started
Remote Desktop Configuration	Manual	
Remote Desktop Services	Manual	
Remote Desktop Services UserMode Port Redi...	Manual	
Remote Procedure Call (RPC)	Automatic	Started
Remote Procedure Call (RPC) Locator	Manual	
Remote Registry	Manual	
Routing and Remote Access	Disabled	
RPC Endpoint Mapper	Automatic	Started
Secondary Logon	Manual	
Secure Socket Tunneling Protocol Service	Manual	Started
Security Accounts Manager	Automatic	Started

Before disabling any running services, be sure you know what you are disabling. From this screen you can also disable certain services from reloading the next time you start your computer, and by doing so, you may speed up the overall performance of your system. Be careful though, as with programs, these services may be needed to run your computer, so be sure you know what you are disabling before you do it.

In summary

It is a best practice to know what programs are installed on your computer and to uninstall the ones that you don't need anymore. It's also good to know what ports and services are running on your PC. Doing all of the steps above doesn't mean that a virus or a hacker cannot get into your computer, but by checking your system periodically for things that just look weird, you are potentially saving yourself from the perils of cybercrime

KEEPING TABS ON YOUR CORPORATE DATA

It's a common phrase used in the IT community that "you can't secure what you can't manage", or another way to think of this is that you cannot secure what you don't even know exists on your network. In order to tackle the task of securing your company data, you have to know that it exists in the first place. Many corporate users don't realize where they may be putting their data, and many corporate network administrators and executives may not realize where their employees may be putting the data that runs their company.

First things first: do an inventory check.

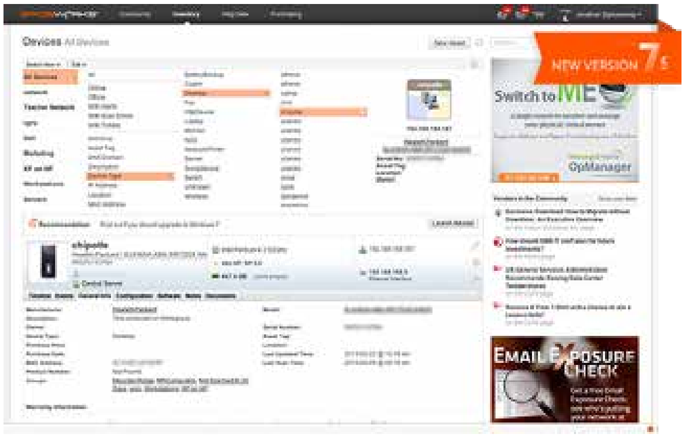
To get started, I recommend that you take inventory of what PCs, servers, laptops, tablets, and phones are on your network and able to connect to your shared drives, email, and other systems. If you already have an inventory, chances are it may reside in a spreadsheet or other document, and if it is a little outdated or not complete, it's time to do it again. Ideally you should have a system in place that is doing automatic inventory, and keeping a central database up-to-date with any new devices or changes to the systems that are being monitored. Before you do any type of inventory of corporate-owned devices, be sure that you have permission (in writing) first before you start. You should never scan any system that you do not own or have approval to scan.

Spice Works IT Asset Management software can not only inventory all your devices, but manage them as well.

Visit Spice Works >

What do I use to do an inventory?

There are many products available to help you with IT inventorying. Some cost a little money and others cost a lot of money. What you choose is up to you and should match your particular requirements. However, there is a FREE solution called Spice Works that I have used for years that may help get you started. I have used this product in the past to help audit the local network that I am connected to, and I even use this product at home to keep my home network inventory up-to-date.



What should I audit using these tools?

What you ideally want to audit are the PCs, laptops, servers, tablets, phones, and other devices that are connected to your network. Then from there, using these tools you would want to audit the software that is installed on the devices. One of the features of the Spice Works tool is the ability to audit hardware, software, and even tell you the “health” of those devices. You can tell how much space is left on a hard drive, how much memory is installed on a device, and how much is in use, and I have even had the system tell me when the toner in my wireless printer was low so I could re-order it.

What about my data? How do I tell where it resides?

Now that you have a high-level overview of the devices on your network and what programs are installed on them, it’s time to move on to determining where your data resides. This can be difficult without specialized tools that can scan your devices for data files (such as documents, spreadsheets, databases, etc.) and those tools are typically grouped into a category called “Data Loss Prevention” or “DLP”. These can be very costly for the small/home office (SOHO) or small- to mid-size business (SMB) type of user, but for larger enterprises, they should be considered a requirement. Without a costly tool like DLP, you can take other steps to try and determine where data may reside.

Some steps to take include checking for:

- Devices on your network to determine if you see employees bringing in personally owned devices that you do not permit.
- Programs installed on corporate-owned devices that you do not permit, such as cloud-sharing products, personal email programs, or data encryption utilities that you do not control.
- Systems that are attaching to your corporate email system that you do not recognize or control. Devices such as phones and tablets can be used to store corporate data that you may prefer to not allow.
- Database products on devices since these local databases may conflict with corporate policy and may be used to store copies of sensitive data that you do not control or permit.
- Software products installed that you do not approve, or installations that exceed your allowed count of available licenses.
- Utilities such as FTP (File Transfer Protocol) programs that could be used to send large amounts of data to an external server that you do not control.
- Email communication to see what data is going out via email to recipients that it should not (or to your employee’s personal email accounts if you do not allow this).

Important Note: With any of the steps listed above, be sure you are authorized to complete these steps by your employer before doing these types of scans. Also ensure that you have the proper policies in place that lets your employees know that these types of audits will be done periodically, and that proper responses *and possibly sanctions may be applied if employees are found violating your established policies.*

What about USB sticks and external hard drives?

One of the most dangerous types of devices being used in corporate environments these days are USB sticks and external USB connected hard drives. While these devices can be just fine if they are provided by the company for employees to use, with encryption, the ones they buy on their own and bring in from home could have devastating consequences to your business if not managed properly. USB drives do not typically arrive with encryption on them, nor do they have anti-virus built in. If you do not block these devices, you should have a written policy in place that says that they must be checked and pre-approved for use before they are allowed to plug into your corporate-owned devices. Users can inadvertently bring in viruses from home on them, and they can also be used to copy sensitive corporate data and be brought home or lost in transit.

In Summary

While the steps above may not find all of the corporate data on the devices that are connected to your corporate network, it is a good start. Using the process above, you may end up finding personally owned devices on your network that you did not know were there, or you may even find data that you thought was better secured than it is. When you find things that do not meet the corporate standards for use and storage, you should take steps to fix the situation so that data is not allowed to continue to be out of your control.

THE PERILS OF USING REMOTE-ACCESS SOFTWARE

While software that can be installed on your PC and used to remotely connect can be very handy, it also comes with risks that may not be apparent at first.

Various products exist to allow you to access your computers remotely including TeamViewer, GoToMyPC, AAA PC Remote Control Software, and several others.

If not set up properly and securely, many of these products can leave your PC open to external hackers or malware that could potentially get into your PC without your knowledge, possibly stealing your data or doing damage to your system.

One of the main issues with any product like this is that many use a password to protect the remote capabilities, and some users choose to re-use passwords that they use for other systems including bank accounts, social media accounts, etc.

Most recently, there is a great deal of press about the issues at TeamViewer and GoToMyPC.

Teamviewer
Users Reporting
Unauthorized Access,
Hack Suspected

Read Article >

According to a recent CSO Magazine article, “Several TeamViewer users have reported unauthorized access over the last few days, leading some to suspect that the remote connection company has been hacked. The unauthorized access reports started showing up on Reddit around the same time that the company suffered possible DNS issues that triggered an outage lasting for several hours.”

What is not completely known yet is how this reported DNS outage for TeamViewer may have affected the users of the product (if at all), and if this incident is related at all to the reports from users having their information and accounts compromised.

And in a notice from GoToMyPC, the company said, “Unfortunately, the GoToMYPC service has been targeted by a very sophisticated password attack. To protect you, the security team recommended that we reset all customer passwords immediately. Effective immediately, you will be required to reset your GoToMYPC password before you can login again.”

The company also recommended implementing two-factor authentication. The details of the breach are unknown at this time.

How does something like this affect you?

If you use any remote-access software on your computer, you should immediately check the security as it pertains to how it is set up. First and foremost, if you no longer need to use the remote-access software, then remove it. If you are unsure if it has been set up securely or not, then remove it until you can consult with someone that can help you get it set up securely.

If you have to continue to use the remote-access features, then you should be sure that any passwords you may be using are unique and very strong, and that you are not using the same password for any other systems or accounts.

I don’t use remote access software at home, but it is used at my company – so how can I protect my company?

If your company uses remote access software for vendors or employees, it should be secured and restricted to only those users that absolutely need to use this method of connection. Remote capabilities should be reviewed at least annually to ensure that orphaned accounts do not remain.

Another thing that you can do to protect other users at your company and your corporate data is to ensure that you have a good firewall in place and that activity through your network is monitored for unusual activity. The last thing you need is to have a hacker or rogue employee with remote access to your network and private data without that activity being detected. Incidents like this should hopefully be shut down before any damage can be done.

In Summary

The bottom line is this: If you don’t need to have remote access software on your computer, then take it off and don’t use it. If you do have to use it, be sure that it is set up securely and that the activity for that program is somehow logged and monitored.

Managed network security firms such as Netsurion can help secure your company network and ensure that things like remote access software are not allowed through the firewall and, therefore, not able to be used as an access point into your computer and your company’s sensitive data. Netsurion can also monitor other activity that is allowed in and out of your network to help ensure that no suspicious issues are seen and not responded to.

ABOUT NETSURION

With Netsurion, distributed enterprises accelerate innovation while reducing complexity by combining network security, threat management, and compliance readiness into a single suite of managed services. Netsurion Connect is a powerful and practical WAN security platform with flexible co-management services to efficiently manage many branch locations and IoT applications. Netsurion Protect delivers enterprise-grade threat lifecycle management through a leading Security Information and Event Management (SIEM) platform that unifies machine learning, behavior analytics, and security orchestration. Netsurion Comply consists of regulation-specific solutions that streamline compliance management, so organizations are always audit-ready.

To stay ahead of current and emerging threats, Netsurion merged with EventTracker to combine enterprise-grade managed network security service with leading managed SIEM. Our service offering – SIEMphonic – is powered by EventTracker and helps deliver comprehensive security benefits to edge locations that normally would not have the means to leverage such a solution.

Netsurion has been providing network security services for almost 30 years. Today we secure locations for many national chains, as well as regional and local establishments. We serve any industry that accepts credit card payments, including retail, hospitality, healthcare, legal, and insurance.