



The Internet – A Dangerous Place

The Problem:

The internet has become a valuable tool for business. We all use it daily for purchasing from vendors, selling our own products, research, news, and more. But the internet is becoming increasingly dangerous, and has the very real potential to damage our businesses if we are not taking the proper precautions. The problem is getting worse every year. According to Panda Labs, more malware was created last year than all previous years combined.

This is no longer a bunch of hackers trying to impress each other with how many PC's they can crack, crash, or take over. The majority of activities are by sophisticated and organized cybercriminal groups that are out to make money at your expense. They want to steal your passwords, credit card information, social security numbers, banking info, anything they can resell for a profit. And, they want to do it in a fashion where you are not even aware that you have been compromised until it is far too late.

Even if you do not believe you have any data on your computers that anyone would want, you are still a target. These criminals are also looking to take over PC's for their own purposes to attack websites, distribute spam, and access your email lists of friends, customers, and business associates. It is estimated that these "taken over" computers, called Bots, number in the millions worldwide. And once your site has been infected in this manner, you will often lose your ability to send legitimate emails because the various anti-Spam services and agencies will black list you as a spammer and refuse any Emails you send until the problem is corrected.

Malware is the generic term for all types of malicious software threats including viruses, phishing, Trojans, root kits, bots, key logging, intrusive adware, DoS attacks, email as a vehicle for delivering undesired content and more. Most intrusions are due to accessing infected websites, Email attachments or click-thrus, or OS and application vulnerabilities. These attacks are become much more

sophisticated, using polymorphic and mutating code that is impossible to detect by signature based Anti-Virus programs. A new and increasing area of concern is Smart Phones, PDA's and other mobile devices. The number of attacks on these types of devices has increased sharply in the last year with specific malwares targeting Android, Windows CE and other mobile device OS's. This can not only cause you personal headaches, but can provide a back door into your business network depending on your environment.

Most companies have some level of internet security in place. Almost all have desktop Anti-Virus, and the majority of those centrally manage the update process. Most companies have some sort of firewall. Many companies use internet content filtering or rely on policy. Most of us have been forced to deal with Email spam, either thru Anti-Spam software, or a service. But, what is required in today's environment is a comprehensive set of policies. Ignoring just one area is like leaving one hole in your boat. We have had more than one client that felt they were completely protected. In a recent situation, a client was getting malware from websites even though they had internet content filtering in place to block access to those websites. It turned out that employees were accessing a nearby Wi-Fi hotspot to bypass the content filtering. In a similar situation, a client was getting re-infected by laptops that were being used both inside and outside the network.

What can be done?

Patch your software - Vulnerabilities are constantly being discovered in programs that can leave your systems open to attack. Not only in operating systems, but in programs like Flash, Adobe, Java, and others. When these Vulnerabilities are discovered, the software vendors move quickly to produce a patch to correct the problem. Unfortunately, the criminal element also moves quickly to develop programs and attack methods to take advantage of these vulnerabilities. It is important to keep on top of the patches to make sure you are protected before the hackers get around to you.

Perimeter defense – It is better to stop a threat from entering your network at all than to rely on your PC based antivirus to catch everything. Many companies have SAN, NAS, Process Control computers, and other devices that can act as carriers for viruses, even if they are not particularly vulnerable themselves. By implementing a firewall, antivirus protection, and intrusion prevention and detection at the perimeter of your network, preferably with a different brand of Antivirus software, you are increasing your chances of keeping Malware out of your network.

A good Firewall – Not all firewalls are created equal. Many lesser firewalls are packet filtering devices which means they accept or reject based solely on the address of the incoming traffic. Since IP addresses can be spoofed, and the widespread use of Bots allow Malware to be forwarded from apparently innocent servers, these devices are not able to stop disguised attacks. In comparison, a firewall that is capable of stateful inspection actually looks into the packet content to determine whether the data is harmful. In addition, this class of firewall is able to recognize Brute Force (IP flooding) attacks and automatically block the offending IP's. A good firewall will also provide reporting that is a valuable tool in administering your Internet connections.

Internet content filtering – Using Internet content filtering provides a number of big benefits. Non business websites have a much higher chance of being infected, particularly ones with lots of click-on ads. Sites like Facebook, MySpace, Twitter, and even LinkedIn are becoming notorious for Malware and social engineering (using these sites to find out more about you to guess passwords, impersonate you to coworkers, customers, and vendors, and more.)

According to the U.S Dept of Commerce, 30-40% of Internet use at the workplace is not related to business, 70% of all Internet adult site traffic occurs during the 9-5 workday, and 37% of workers surveyed say they surf the Web constantly at work. Besides the obvious loss of productivity, the bandwidth usage of personal surfing is disproportionately large. Consumer based websites tend to be much larger in bandwidth usage, and streaming media such as live sports and other broadcasts, internet radio, live weather radar, YouTube videos, etc. can take up a shocking amount of your total bandwidth. Finally, companies need to protect themselves against legal liabilities. There have been many lawsuits by employees against their companies for being subjected to objectionable content seen on a coworkers PC, circulated via email, or inserted by virus. Many of these lawsuits are being won by the employee if their company cannot demonstrate that they are taking sufficient precautions via policy and controls to prevent this from occurring.

Email controls - While in the last year, Email spam is actually down a bit, it is still a huge problem. 95% of all email is spam. Just the time consumed in managing spam is considerable, not to mention that email is still a primary method for delivering malware to your network. Most companies do not allow certain attachments such as Zip files or executables, but all types of attachments can be suspect, even pictures. It is important to have the ability to automatically scan emails and attachments, and to have a good anti-Spam process whether it is a software or service.

VPN – If you have remote offices, or employees accessing your network from home or remotely, it is important to secure that connection. VPN (Virtual Private Network) is basically an encryption that prevents interception, diversion, or eavesdropping of that connection. It also extends the policies and controls of your network to that remote user. It is important to note that VPN itself does not prevent Malware resident on the remote device from spreading to your network. Most good Firewalls or security gateways provide both site to site and individual VPN capabilities.

Mobile and Remote devices – This is becoming an increasingly complex issue. Whether it is remote desktops, laptops, smart phones, PDAs, or other mobile device, the commonality is these devices can and do access unsecured internet and networks as well as yours. This can provide an undesired conduit into your network for a number of Malware types. There are specific security methods that can be put into place for this, but it is dependent on your environment.

Back Doors – As mentioned earlier, one of the most common ways your network security can be circumvented is by accessing local Wi-Fi hotspots. It is a good practice to use a Wi-Fi scanner or laptop on a regular basis to see what signals you can pick up at various areas of your facility, and to monitor the use of wireless capable devices that are attached to your network. Additionally, if you provide wireless capabilities within your network, it is very important that you lock it down securely, so that unauthorized persons sitting in your parking lot, or a few doors down cannot gain access. Takeover programs such as Himachi, PC anywhere, etc. are other back door situations as they bypass content filtering and perimeter security. Use of these types of programs should be closely monitored.

Security Policy – Even with all possible controls in place on your network, it is essential to have a comprehensive and specific security policy in place. This should outline what the acceptable uses of your business computers are, address common situations, such as what to do when you get one of those fake virus messages or how to handle Nigerian emails that want to pay us big to launder money for them, etc. You should set specific policies regarding passwords, loading non authorized software, and file copying to removable devices. Basically, the security policy should cover all aspects what is allowed and not allowed on your network. It is important for those of us in IT to remember that computer users are generally not computer professionals, and what may be second nature to us needs to be spelled out clearly for everyone using our networks.

Being computer professionals, most of you are very aware of the security issues with the Internet. But, it can be difficult to get mindshare, or budget from non-IT executives to deal with these threats. Yet, the consequences can be far more

damaging than a server failure or software crash. The purpose of this whitepaper is to increase awareness among those that are not already familiar with the problem, so feel free to pass this along to the appropriate individuals within your organization.

No matter what size company you are, you are at risk. There is a lot you can do yourselves, but if you have questions, want help, or recommendations, call us. CPS Technology Solutions has been helping small to medium sized businesses with Network performance, reliability and security for over 28 years. We can help you come up with common sense solutions that fit your company and budget.

Robert B. Kennedy
President
CPS Technology Solutions
bk@cpsts.com
763-278-9660