Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Applied Principles of Defense-in-Depth: A Parents Perspective

This paper will seek to shift the paradigm of the traditional information security model as it applies to business and employees to a more personal model of home and family. Though the digital landscape is significantly different in the business world, the information warfare against your home assets are just as real and the attack vectors are, in most cases, even more profound. Additionally it will demonstrate how the defense in depth principals apply and can be implemented to make both your home network and family mo...

Copyright SANS Institute

Author Retains Full Rights

AD

PARADIGM SHIFT

Applied Principles of Defense-in-Depth:
A Parents Perspective.

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Tom Miles
July 26, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents:

Abstract
A Strange New World…
- A brief internet history
- Learning and discovery, exploring this vast new territory

The Dark Side
- The Internet and the new economy
- Social engineering and exploitation
- Illegal activity and inappropriate content

Defense in Depth
- Defense in Depth (DiD) defined
- The basics a framework to keep our family safe

The Security Policy
- House rules – The basic security policy

Security Awareness
- Security starts with knowledge
- Training activities and ideas for home users

Vulnerability Control
- Locking it down – Securing your systems and software
- Access Control and Least privilege basics
- Password management

Auditing
- Where to start…
- Following the bread crumbs

Conclusion
- Being a good internet citizen – sharing the information security responsibility

Appendices
- Appendix A – Security Awareness Resources
- Appendix B – Security Tools

References
List of Figures

© SANS Institute 2004, Author retains full rights.

Abstract:
This paper will seek to shift the paradigm of the traditional information security model as it applies to business and employees to a more personal model of home and family. Though the digital landscape is significantly different in the business world, the information warfare against your home assets are just as real and the attack vectors are, in most cases, even more profound. Additionally it will demonstrate how the defense in depth principals apply and can be implemented to make both your home network and family more safe and secure.

The topic of information security is extremely broad and complex. This whitepaper will help parents and individuals sort through the immense amounts of information giving specific insight into identifying problems, implementing solutions and providing valuable resources to supplement and expand upon the information covered here.

© SANS Institute 2004, Author retains full rights.

A Strange New World…

A brief history of the internet

Originally know as ARAPNET, the internet as we know it today started out in the 1950's to late 1960's as a collaborative research and academic network to ensure America's superiority in science and technology. Connecting US Military organizations and dozens of academic institutions the ARAPNET project thrived and expanded until the early 1980's. The 80's brought a continual wave of innovation and new ideas. With these new innovations, newly formed regional networks began connecting world wide. During the late 1980's, improvements in communications, networking protocols and the establishment of many internet standards ushered in an explosion of new network connected host systems, and by the turn of the decade more than 100,000 systems were interconnected. The momentum that was gained in the 80's accelerated further during the early 90's as ARAPNET was decommissioned and the World Wide Web (WWW) was born. During the 1990's the number of computers connected to the internet and the World Wide Web continued to grow at an incredible rate as hundreds of thousands of organizations, countries, and commercial entities came online. Fueled by economic promise, academic collaboration, and global information sharing the internet continues to grow, bringing faster connectivity, increased user interactivity as well as the opportunity for unscrupulous individuals to exploit and take advantage of the millions of users and entities that are connected to this global network.

Learning and discovery, exploring this vast new territory

Today more than 600 million users leverage the power of the internet to conduct business, play games, discover new things, and communicate with each other all over the world. The millions and millions of web pages that now populate the internet serve up information on virtually every topic imaginable. Day and night, for work or play, the internet is a one stop shop making it an ideal place for learning and sharing ideas.

In the United States as well as many other modern countries, virtually all public schools are connected to the internet. According to the National Center for Education Statistics (NCES), the ratio of students to instructional computers with internet access in public schools continues to drop year after year and in 2000 that ratio was 7 to 1. [1] (National Center for Education Statistics – Internet Access in Public Schools and classrooms: 1994-2000)

Educational facilities today are joining together in academic sharing communities to leverage economies of scale allowing them to access books and research information real-time that would have been too costly or impossible to share two decades ago. Both public and private schools are able to access educational resources not only in text but in a broad range of rich media such as sound, video, interactive slide shows, etc. The sensory rich environments are driving scientific research and innovation as researchers globally can share information

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

real-time and react to lab or study conditions changing on the other side of the globe.

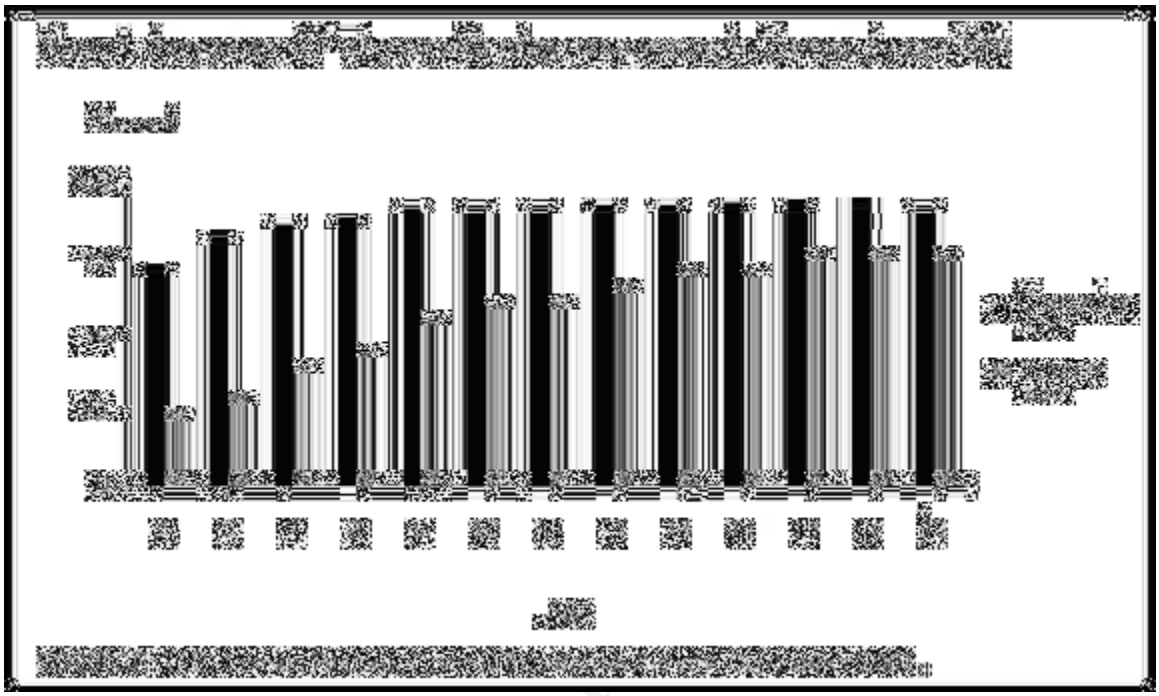

Figure 1 NCES research study 2001

Additional NCES research also noted that, about 90 percent of children and adolescents ages 5–17 (47 million persons) use computers, and about 59 percent (31 million persons) use the Internet. Among those statistics, about 25 percent of 5 year-olds use the Internet, and this number rises to over 50 percent by age 9 and to at least 75 percent by ages 15–17. [2] (National Center for Education Statistics - Computer and Internet Use by Children and Adolescents in 2001)

Because of the vast amount of information that the internet makes available, children are one of the fastest growing groups of online users.

Recent industry research conducted by Jupiter Research, suggest that 57% of kids age 11 and under will be online by 2007. Digital Marketing Services concluded in their survey of more than 2000 kids ages 7-12 that nearly half (46%) go online at least four times a week and nearly 20% go online every day.

"Today's kids are becoming increasingly sophisticated about the online medium. It's not surprising that we are seeing kids adopt the Internet most strongly as a vehicle for fun and games. These survey findings indicate that kids are incorporating the Internet into the parts of their lives that are most important to them - playtime and school." said Malcolm Bird, AOL Senior Vice President and General Manager of Kids and Teens.[3] (America Online/Digital Marketing Services – Press Release 2003)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Among the most popular online activities for kids include:

- Communicating with other children via e-mail, instant messaging, or chat.
- Researching school assignments and doing homework.
- Playing games
- Entertainment – listening to music and watching videos.

According to most kids, learning, communicating with each other and sharing ideas are the most important aspects of being online.

There is no doubt that the internet is a value tool available to parents and children to foster education. Improvement in personal computers, software and the development of ubiquitous connectivity will allow for even richer content and more interactive learning experiences.

The Dark Side

The internet and the new economy

It is easy to understand the numerous benefits of the internet and how it can be used to improve research and idea sharing. But, like any other technology, it must be used appropriately for those benefits to be obtained. Sir Isaac Newton stated in his third law, "For every action, there is an equal and opposite reaction." The internet is no exception. For all the positive and wonderful uses of the internet, there is a dark side as well. A shadowy realm disguised by the anonymity of the internet that breeds misdeeds and ill intent. Everyday, online users are besieged by cyber attacks, targeting their computer systems, their personal data, their identity, etc. For children, this is a perilous situation that can have a disastrous outcome.

Amid all the interactivity, millions of web pages, and countless online users, the seedy underbelly of the internet is teaming with hackers, thieves and scam artist proliferating all manner of illegal activity, organized crime, fraud, and questionable – if not inappropriate and detrimental content.

Louis Freeh, the Director of the FBI stated before a Senate committee on appropriations on Cyber crime in 2000 that “Twelve years ago the "Morris Worm" paralyzed half of the Internet, yet so few of us were connected at that time that the impact on our society was minimal. Since then, the Internet has grown from a tool primarily in the realm of academia and the defense/intelligence communities, to a global electronic network that touches nearly every aspect of everyday life at the workplace and in our homes. There were over 100 million Internet users in the United States in 1999. That number is projected to reach 177 million in the United States and 502 million worldwide by the end of 2003. Electronic commerce has emerged as a new sector of the American economy, accounting for over $100 billion in sales during 1999, more than double the amount in 1998. By 2003, electronic commerce is projected to exceed $1 trillion. The recent

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

denial of service attacks on leading elements of the electronic economic sector, including Yahoo!, Amazon.com, Ebay, E*Trade, and others, had dramatic and immediate impact on many Americans." [4] (FBI Press Room – Congressional Statement 2000 on Cybercrime) His statement goes on to note that the Melissa virus a year earlier caused an estimated $80 million dollars in damages.

As cyber crime continues to grow and corporations spend millions of dollars in counter measures, home users are left exposed making them easy prey, Seldom having the resources to combat the increasing sophistication of the cyber criminal and their attempts to exploit their marks. The challenge is that home users are left with the daunting task of securing their home systems and protecting themselves, their families and their data. This problem is further compounded by the digital divide that exists between parents and their children, as children often are more technologically savvy than their parents. The recent advances in computer technology that is allowing our children to discover new things and learn about other cultures is also leaving them vulnerable to exploitation and harm by online predators. Parents must teach their children at a young age about the many dangers lurking about the internet and constantly monitor their children's activity to ensure their safety.

Over the next few sections, we will discuss many of the possible dangers that parents and kids face and how they can be avoided. There is no silver bullet that will make everything safe or kid proof but, with a little planning and diligence, you can substantially lessen the threats to yourself, your home systems, and your family.

Social engineering and exploitation

Social Engineering can be defined as the manipulation of the natural human tendency to trust one another. This manipulation and deception is used to gain information from the trusting party that can later be used to exploit the trusting party, their system or their personal information. Social engineering tactics have been used for many centuries both in warfare, industry and by individuals who have sought to exploit others. Aaron Dolan articulates this well in his whitepaper on social engineering where he states: "Although a successful social engineering attack does not require a great deal of technical knowledge, using technology in conjunction with social engineering principals can be very effective." [5] (Aaron Dolan – Social Engineering)

Children are especially trusting and thus are particularly susceptible to social engineering efforts. Parents must teach their children not to give out personal information such as their name, their address, their phone number, or where they might go to school.

One technique used to gather information is the use of banners, popups and pop under advertisements. Although one could arguably say that banners and popups are not deceptive by design, there are however, many cases where these tools have been used as an attack vector both in social engineering

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

exploits as well as a carrier for malicious payloads. Because of the transparent nature of web technologies and the ability to mask certain content or functionality it can be difficult to teach and explain to children about these types of deceptions.

In a study published by Jakob Nielsen which focused on website usability for children ages 5 – 11 year old, Nielson found that in response to advertisements, "Children don't distinguish between ads and content. To them, it's all information. A grown-up user clicks on an ad banner maybe once a year, but children do it all the time. They see a banner with a Pokemon character and they think it's a game. They don't realize it takes them to a different site.... My main advice for parents is to sit down with their kids at the computer, teach them to recognize ads. A Disney character in an ad doesn't mean that you'll get a game or a cartoon - it just means that someone has rented the character to sell a product." [6] (Jakob Nielsen's Alertbox, April 14, 2002)

Another major concern is exploitation. Unfortunately, there are many individuals who use the internet to either directly or through social engineering tactics, sexually exploit children.

Most children are taught at a very early age not to talk to strangers, not to let them in the house, not to get into their car and the like. Many parents however, either do not realize the anonymous nature and interactivity that the internet makes available or are complacent regarding its use. Children are left to surf and interact with other online users as if they were watching television. Children are easily misled online because they have no way of visually or audibly verifying that the person they are interacting with on the other end is in fact who they say they are.

According to Department of Justice almost one in five (19%) of young internet users surveyed received an unwanted sexual solicitation in the past year. In those statistics one out of every thirty-three solicitations was aggressive involving offline contact or attempts or request for offline contact. Additionally almost one half (49%) of incidents were never reported to anyone. [7] (U.S. Department of Justice – Office of Juvenile Justice and Delinquency Prevention – Fact Sheet)

Illegal activity and inappropriate content

The internet is also home to enormous volumes of questionable content such as sexually explicit sites, racial hate and persecution sites, as well as many illegal activities such as online gambling, drug trade, software piracy and much more. The subject of illegal activity and what content is appropriate for the internet is a complex one that walks the tightrope of censorship and the right to free speech and capitalism. Some might argue that if the content is inappropriate that you should avoid the site containing that content. That is easier said than done. Many countries have very different moral and ethical standards. In many countries such as France, Japan, and much of Europe, nudity and sexuality are accepted as "the norm". It is very common in these areas of the world for children to be exposed to adult oriented material at a very young age.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Online criminals are using complex high-tech methods to lure unsuspecting or naive users to sites in an attempt to compromise their systems or otherwise exploit the users for their gain. Crafty web designers use automated scripting, and plain old fashion misdirection to mislead users into thinking that they are going to site A when they are in fact going to site B by using web addresses that are similar to the site intended. An example of this type of deception would be when a users makes the inadvertent typo; by typing www.ebays.com instead of www.ebay.com. More elaborate schemes copy entire sites so that unsuspecting users do not even know that they are not on the legitimate site they were trying to reach.

Another major threat conduit, which should be monitored, is e-mail and particularly unsolicited and potentially harmful e-mail known as spam. Some of the more common techniques for dealing with spam include creating filtering rules within your e-mail client that will delete or quarantine e-mail matching specific criteria or the use of spam blocking software that uses a continually updated database of filter rules, and detection algorithms to block potential spam messages. Besides being annoying, spam can contain sexual or inappropriate material as wells malicious payloads such as viruses, Trojan programs or potentially damaging code embedded directly into the e-mail message itself.

Parents should employ content filtering software such as Cyber Patrol, Net Nanny or similar software to enforce restrictions on children to any site the parent may deem inappropriate. Most of these software packages categorize sites based on criteria such as sexual content, gambling, drugs and alcohol, etc. and update their list of “filtered” sites frequently as illicit site are often changing URLs’ in an elaborate cat and mouse game trying to stay one step ahead of the authorities.

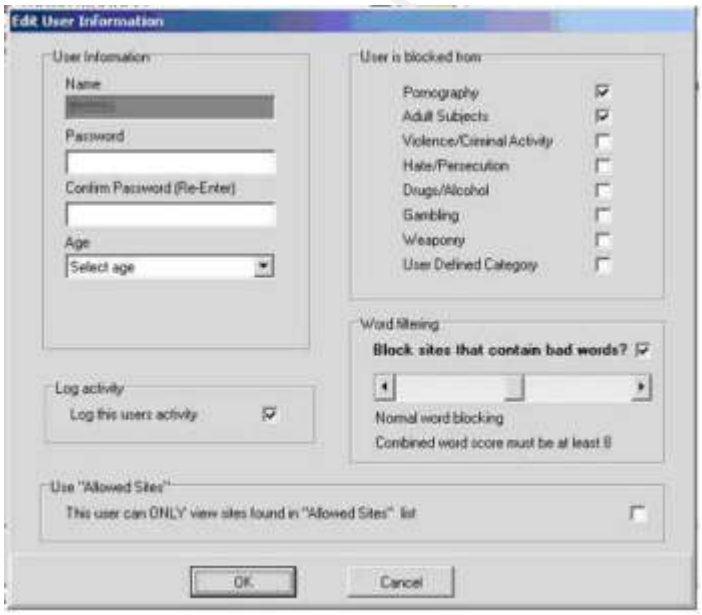

Figure 2 Filter options from We Blocker v2.1 by We-Web Corporation

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Parents may also find using software designed to block popup advertising and spam useful tools in protecting their systems and families from would be attackers. Many sites promoting pornographic material as well as online gambling use popup and pop under advertising techniques to trick users into visiting their sites by clicking on a innocuous interactive game.

The introduction of peer to peer file share in recent years such as Napster and Kazaa have fueled a wave of piracy with users swapping music, movies, software and many other copyrighted works. The speed with which these file sharing communities have grown have caused a backlash of litigation by industry association like the RIAA - Recording Industry Association of America seeking to shutdown such systems and prosecute it's member who have actively participated in trading or selling pirated goods. According to BSA - the Business Software Alliance in a study recently released with IDC research, 36% of all software installs globally in 2003 are pirated and accounted for a loss of approximately 29 billion dollars.[8] (BSA / IDC 2004 Global Piracy Study) Home users should be aware of the legality and risks of participating in such online communities and parents should monitor their children activity closely.

There are many other hazards that parents and children encounter each trip out on the information super highway. The rest of this paper will focus the principals of Defense in Depth and build upon that framework ways to demonstrate how this architecture can be adapted to the home computing envrionment.

Defense in Depth (DiD)

The principles of Defense in Depth (DiD) defined

Considering these staggering statistics and the continually mounting threats from viruses, spam and other activities, it is important to plan, monitor and act quickly to protect our families and our systems and make changes as needed to ensure this protection is constant, difficult to circumvent and resilient as attackers change focus and direction.

The principle of Defense in Depth teaches us not to put all our eggs in one basket and that no single defense strategy will protect our assets fully. Defense in Depth takes the approach of applying defensive counter measures in multiple layers one atop the other in an attempt improve the resiliency and overall strength of your security posture. Because the threats we confront come in many forms and from various sources, it is important that, should a particular security safety net fail, there is another layer of protection. The vital importance of these additional layers becomes apparent when newly discovered viruses or vulnerabilities are exploited. They serve not only to keep the asset safe but, in many instances act as a buffer, slowing down the threat or attacker until a resolution can be found or initiated and the damage from the attack can be cleaned up.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Another important point to remember is that we must learn from our mistakes and as part of our Defense in Depth strategy make adjustments to our defenses to ensure that the vulnerabilities that were exploited are fixed and that safety measures are put in place to keep the incident from happening again in the future. Cleaning a virus infected files is pointless if we do not update our virus protection software to block that virus strain in the future preventing re-infection.

The graphic below illustrates principles of Defense in Depth and how combining multiple strategies, we can create a strong foundation and secure framework with which to protect, monitor and maintain the safety of our systems and families.

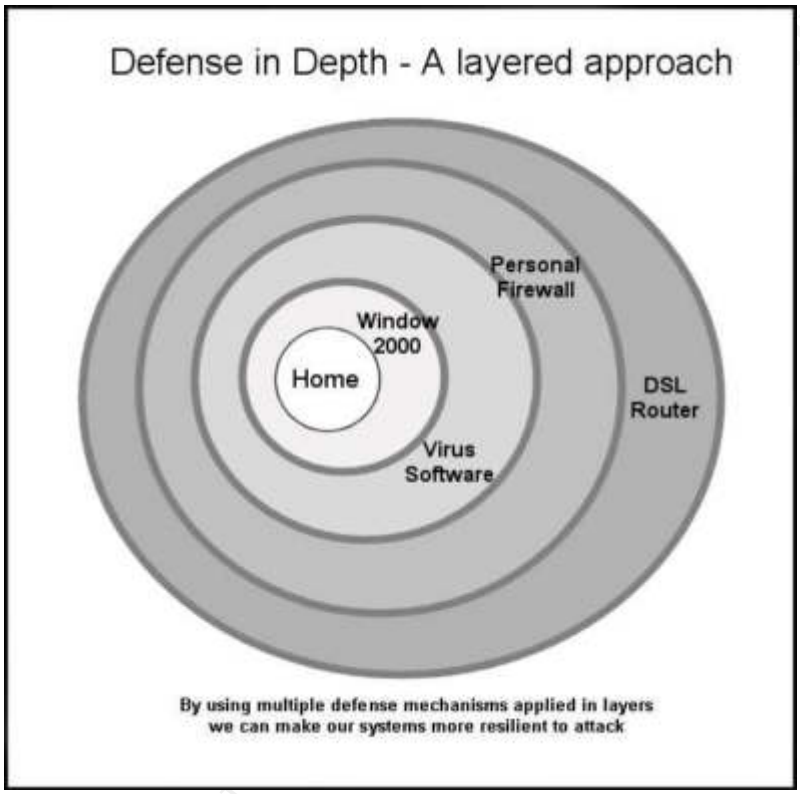

Figure 3 Depiction of multiple defensive layers

The Basic Framework – Keeping what's important safe.

In the next few sections we will discuss several of the key concepts that will help in securing your computer assets and family. As the saying goes, knowledge is power, and information security is no different. The better your understanding of what threats and vulnerabilities exist, and how best to protect against them, the better you will become at making your system more secure for you and your family. There is a vast array of knowledge and resources available both on the internet and through books that can help you to understand how computers work, and how they interact on the World Wide Web. Armed with a little knowledge and some common sense, you can make the target on your back (i.e., your data,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

computer or family) more difficult to reach, harder to exploit and more resilient to attack.

The Security Policy

House Rules – The basic security policy
The security policy is the cornerstone of your defensive strategy. It is a written document that defines both proper uses of the computer and online activity as well as consequences for improper use. The security policy establishes the processes needed to protect the systems and users (family members)

Some may argue that it is un-necessary in a home environment to document a written policy but, the fact is that if it is not in writing, then there is room for ambiguity and confusion on how resources should be safeguarded or properly used, and what to do in the event they are compromised.

Now that we have established the importance, what are some considerations when writing our basic home security policy? First of all, the security policy will describe what assets should be covered, who is responsible for ensuring that coverage and why the coverage is important. Let's look at three of these and then we will move on to the next topic of procedures which will cover how the assets will be secured, where and when.

What should be covered you ask? The policy should only define coverage of vulnerable components. For instance, it is not practical to define a policy regarding your computer monitor. Except for physical theft, your computer monitor is not a vulnerable component. The policy should go on to indicate who will be responsible for maintaining the countermeasures to protect each asset as well as a brief explanation of why each particular asset need be secured or the risk of not securing that asset would be "x".

An example of this might be:
"All computer data and systems will be protected with anti virus software. It is (Dads) responsibility to make sure that the virus software is updated with the latest patches. It is important that the data and systems be protect with anti-virus software to prevent loss of information (i.e. pictures, tax files, online banking files, etc.)"

As you can see the statement is simple and contains what component (*computer system and data*), who is responsible (*dad*) and what the consequences of not maintaining compliance with the policy are (*loss of data*). It is not important that the statements be formatted in any particular way or that it contain a lot of legalese. Notice also that the statement does not address specifics of how, when or where the statement will be fulfilled. This is where procedures come in.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Security policies provide guidelines on what, who and why. Procedures create more specific view of how those guidelines will be implemented. Let's write a sample procedure for our anti virus policy.

"The responsible party for managing the anti virus software (XYZ Anti Virus) will configure the software's auto update functionality to check the manufactures website each time the computer boots up. This person will also verify weekly that anti virus software is current and working correctly, as well as perform weekly scans of the computer system. All infected files will be either repaired or deleted."

Well that wasn't too difficult now was it? The key point is to set aside time to create your written policy, to ensure that everyone at home understands the importance and proper use of the computer and acceptable online behavior. Each member of the family should sign an acknowledgement stating that they understand the security policy as well demonstrate acceptable use of the system.

Security Awareness

Security starts with knowledge

Perhaps the weakest link in our security defenses is ourselves, the human factor. Whether it is our lack of technical knowledge or our ignorance of the unknown, we are the single biggest vulnerability. We compromise our security measures by doing things like picking simple passwords, or downloading potentially unsafe files, we give away important clues and information that makes us easy targets to viruses, hackers, and malicious perpetrators.

In order to correct problems like this, we must learn to be more cognizant of the ways in which we will be exploited and devise ways to thwart those attempts. We should challenge every assumption and re-think our current security habits to ensure they are adequate.

Security is a moving target because threats change constantly and as such, we must constantly learn and adapt. To start our learning journey, we need to re-think how we think about security. To do this, and swing things back in to balance we must first educate ourselves and then we must educate others around us, spouses, children, parents, neighbors, etc. Passing on our knowledge and helping others to become aware of the threats and security dangers that abound will help prevent us from being attacked or compromised.

Training activities and ideas for home users

It is again very important that we get everyone involved and that we share the information we learn. Children especially need guidance on safe computing so that they can become safe and productive online citizens. Talking with your families and keeping them informed on a regular basis not only keep security

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

awareness at a higher level but, will also prepare them to handle the many situations they might face.

Laying down ground rules in a security policy and having everyone in the home sign a safe computing contract that states that they will comply with the policies is a way of driving home the importance of these issues.

This whitepaper along with the many other reading room papers on the SANS website (www.sans.org) offer a great starting point on you mission to understand. To assist in teaching your children, many child friendly websites like (www.kidsdomain.com), (www.pbs.org) and (www.yahooligans.com) have plethora of information and interactive actives that parents can use with their children to help them learn about the various dangers online. The FirstGov for Kids website (www.kids.gov/k_computer.htm) is a great starting point for information and activities for children regarding internet safety and being a good online citizen. Role playing and practicing various situations with your children and how to respond to them will ensure you family knows what to do when they encounter a virus infected file, a tempting popup, or an online predator.

Appendix A has some helpful material and activities to help get you started talking with your children and family.

Vulnerability Control

Locking it down – securing your system and data

In this section we will attempt to cover some of the things that you can do to help make sure your system is more difficult to compromise.

Another cornerstone in your defensive posture is your operating system. It is vital that you choose and use a secure operating system such as Windows 2000 or Windows XP or even Linux. Why, you ask? Simple, these operating systems offer more advanced security mechanisms, such as secure file systems, file encryption, access control lists, etc than their predecessors. Operating systems such as Windows 95 or 98 were built on an insecure file system and lack many of these security features. Because of this it is more difficult to protect and secure these legacy operating systems.

Having a secure operating system in itself is not enough; we have to use it securely in order to reap the safety benefits that it offers. To begin, we must ensure that we have downloaded and installed the latest security patches and service packs. These updates which are released periodically, fix newly discovered security flaws and vulnerabilities in the operating system and continually make it's defenses stronger and safer. Additionally service packs may also include increased functionality and new software enhancements.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Access control and least privilege basics

Most modern secure operating systems use a hybrid security architecture that blends role base access control (RBAC) which allow each user their own secure profile with discretionary access control (DAC) which allows each user the ability to manage or delegate authority their files. Additionally, the security model of these systems use the principle of least privilege. What this means is that each user or process (program) should only have enough authority or privilege to do its function. In order to fulfill this requirement users are divided into groups, and then each group is given appropriate authority based on its function (RBAC). Each operating system by default comes with an administrative or master account that should only be used for system maintenance or software installation such as installing service packs or security fixes. All other users should have their own accounts for normal system use. This approach offers two things: from a user perspective the user has authority over their personal files or the ability to restrict or delegate authority to another user (DAC). Secondly, from an administrative perspective this allows for better system auditing and the ability to log who did what and when.

Figure 4 NTFS security dialog Windows 2000 by Microsoft Corp.

As we stated, each user or the administrative account, has the ability to restrict or grant authority to resources that they have authority to change. Sensitive information or data should be secured so that only the appropriate users have access to them. By doing this, you are practicing Defense in Depth and adding an additional layer of defense to your important data. To take this one step further, many operating systems make it possible to encrypt files making them unreadable to anyone who does not have sufficient privileges to access them even if they are copied or moved to another system. File encryption offers a

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

strong countermeasure against intruders attempting to look at your sensitive data but, it should be used wisely and the encryption key should be backed up to a secure and safe location. Poor planning or loss of your encryption key could mean that the data is lost or inaccessible forever.

File Encryption - cipher text

Normal Text hello

Cipher Text pgAAADP1wJU8OtQgiOPV9b+EyS6lz6acuGAKrm1
GEcl4eJJolT68cOb1H/o/PxZ8 nYls0UupT+0= =7mu0

Figure 5 Example of encrypted text

The next step in battening down the hatches on you system is to stop or uninstall any unnecessary or unused services and applications. Newer operating systems such as Windows 2003 help by configuring your system to be more secure initially. But, you should still double check. Windows 2000 for example installed many features by default that pose a significant security threat if left in their default state. Things like, unused communication protocols, www publishing services, default administrative shares, routing and remote access, CD auto-run, file and printer sharing etc. should be disable if not needed.

The whitepaper "Defense in Depth and the Home User: Securing the Home PC" by Shauna Munson [9] is an excellent reference on securing you home operating system.

Now that your operating system is configured it is important that you protect your system with at minimum a virus protection software but, it may be helpful to also install anti-spyware software such as Adaware from Lavasoft (www.lavasoftusa.com/software/adaware/) or Spybot Search & Destroy by Patrick Kolla (www.safer-networking.org) as well as a personal firewall to build additional defensive layers. These programs will actively monitor your system and its files to help prevent exploitation from viruses, Trojan applications, malicious content, and spyware which can not only damage your system but, could also expose your sensitive data as well as reveal personal information about you and your family. A firewall is an application that can filter and block undesired communications from attackers on the internet. Additionally, if you have a broadband internet connection such as DSL or cable it is also advisable to install a router which will provide another protective layer by creating a NAT or Network Address Translation zone to separate your home systems from the

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

internet connection. NAT zones make your internal systems virtually inaccessible to outside systems.

The diagram below shows a typical NAT zone.

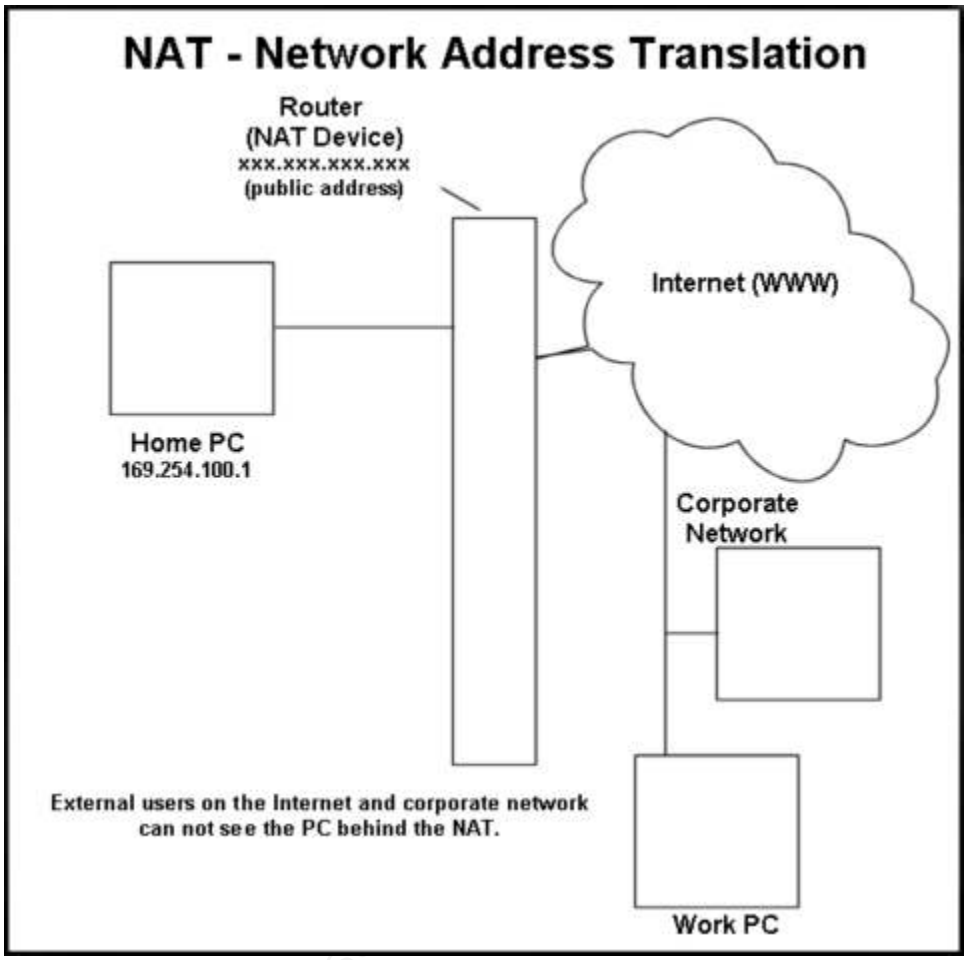

Figure 6 Depiction of NAT zone

Appendix B details many free or low cost tools that you can use including anti virus software, spy removal tools, and firewall applications to help you protect your system and personal data.

Password management

Using a good password and learning to create a strong password is another crucial piece to the overall security puzzle. You have put in place many layers of defense including a secure operating system, anti-virus and firewall applications, a router, but, all of that is useless if a would be attacker can easily guess your password and access all of your data or make changes to your configuration.

Humans, unlike machines like to simplify things to make them easier to remember especially passwords because we can potentially have a lot of them.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

One password for logon, one for the router, and one for the internet service provider, etc. For instance instead of creating a secure password like "Cx37!uu%D", we have a tendency to pick things that are familiar to us and easy to remember, like our favorite sports team or our birth date. We are always looking for ways to simplify things. The problem is that today's computers have enormous computing power that can manipulate data and do hundreds of millions of calculations every second. This makes figuring out simple passwords very easy and quick. Using social engineering techniques, an attacker could easily discover a simple password. So what should we do or not do when creating a password?

Password don'ts:
Do not use any word found in the dictionary
Do not use your logon ID or any part of your name in your password
Do not use sequential keystrokes such as "abcdef" or "123456"
Do not use names of pets, family members, favorite sports team etc.
Do not use birthdates of yourself or a family member
Do not write down your password

Password Dos:
Use 7 characters of more for password length
Use a mix of letters, numbers, and special characters like "agC$9u!q4"
Use a familiar phrase – "**I w**ent to **E**urope **l**ast **y**ear for **v**acation**!**" becomes "Iw2Ely4v!"

You should change your password frequently, at least every 90 days but, more often is more secure. You should also change your password immediately if you suspect that someone may know it or if the password is a default password. By following these simple rules you can create strong passwords that will many any attackers attempt much more difficult

Auditing

Where to start…
Auditing is an important step in the security life cycle. Auditing allows you to monitor users, system, and application activity for any suspicious anomaly or inappropriate use. The typical home user, particularly parents should become familiar with checking the system's event logs and the logs from your personal firewall, spyware, content filtering, and anti-virus applications. These logs may be vital for determining what has happened in the event of a security breach and may help in building better countermeasures to prevent future compromise. You should locate each of these logs and get a familiarity with them before an incident occurs so that you can react more quickly to those situations.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

So let's dive in and look at what some of these log files do and how they can be used to improve our security posture. The security log in Windows systems allows you see events regarding file or resource access. Events such as successful and unsuccessful logon or logoff, file or object access, etc, are logged here. Configuring object access auditing within the operating system on sensitive files for instance will allow you to see who or what is accessing or attempting to access your sensitive data.

The system and application logs display status messages from the operating system and the applications that are installed. The status message will show when an application is malfunctioning or not working at all, which may be an indicator that something has been compromised or the configuration modified.

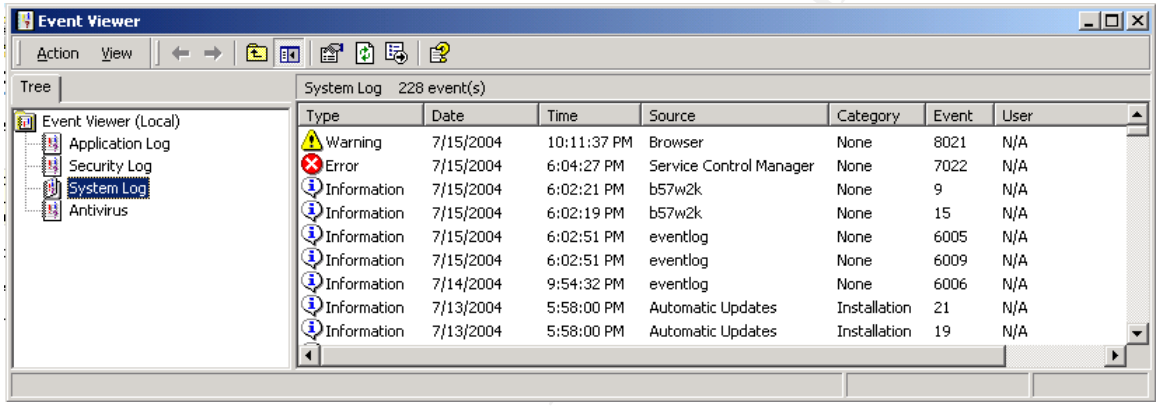

Figure 7 Event View – Windows 2000 by Microsoft Corp.

The log files on your spyware and anti-virus software will tell you what files may be infected and whether or not they may be recovered safely or may potentially need to be deleted permanently. It is important that you understand which files are compromised so that you do not inadvertently re-infect your system or possibly pass the file on to someone else and cause them system damage.

Your firewall or router logs will show what ports and communication channels are being used by your system and it's applications as well as information on those services being accessed or requested from the outside. Many online service providers offer firewall, and virus protection as part of their service.

Following the bread crumbs

Parents should also be familiar with auditing their children's activity including where they might have been online. Parental control applications like Net Nanny, We Blocker, and Cyber Patrol offer content filtering options, extensive logging capabilities as well as functionality to limit online access to certain hours. These settings are customizable for each user so that younger children could have more stringent settings while young adults could be given greater latitude regarding the content they view or access online. If you do not use parental control software it is possible to examine clues as to where your child might have gone on the internet by checking both the internet history and user cookies

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

located in the temporary internet files of their user profile. Most internet browsers like Microsoft Internet Explorer have the capability of tracking online history but, this information is easily removed.

Conclusion

Being a good Internet citizen – sharing the security responsibility

There are many threats and vulnerabilities to our home systems and our families. In order to effectively protect these valuable resources, everyone needs to understand the rules and responsibly of using the computer and acceptable practices of being online. By defining a basic security policy and maintaining good security awareness among the entire family we can mitigate the largest single security threat; ourselves. We must re-thinking our environment, and be aware of the many risks that abound. By implementing the practices and principles of Defense in Depth, we can harden our computer systems, strengthen our knowledge and make our resource much harder to compromise or exploit. Parents must take an active role in their children's online activity and usage. By exploring this vast new world with them and helping them to spot the dangers that confront them, we can teach them to be good internet citizens and help keep them safe while online.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix A – Security Awareness Resources

Internet Safety Quizzes
http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=714

http://www.safekids.com/quiz/

http://www.safekids.com/quiz/

http://www.techcorps.org/resources/internetsafety/getnet.htm

Online Safety Pledges
http://www.safekids.com/contract_kid.htm

http://familyfun.go.com/parenting/learn/school/feature/famf0700safeweb/famf0700safeweb7.html

http://www.youthonline.ca/safety/parentspledge.html

Internet Safety Games
http://www.kidscom.com/games/isg/isg.html

http://disney.go.com/surfswell/index.html

http://www.netsmartz.org/kids/indexfl.html

http://www.msn.staysafeonline.com/default2.htm

Additional Learning Resources for Parents
http://www.wiredsafety.org/

http://www.media-awareness.ca/english/special_initiatives/games/index.cfm

www.cybertipline.com

http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/adults.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Appendix B – Security Tools

Anti-Virus tools:
Trend Micro - http://www.trendmicro.com/en/home/us/personal.htm

Anti Vir Personal Edition- http://www.free-av.com/

AVG Anti-Virus - http://www.grisoft.com/us/us_dwnl_free.php

F-Prot Antivirus – http://www.f-prot.com/download/home_user/

Avast! Home Edition – http://www.avast.com/

MicroWorld AV Utilities – http://www.mwti.net/antivirus/free_utilities.asp

BitDefender - http://www.bitdefender.com/index.php

Symantec - http://www.symantec.com/index.htm

Spyware tools:
Spyware Blaster – http://www.javacoolsoftware.com/spywareblaster.html

Spyware Guard – http://www.javacoolsoftware.com/spywareguard.html

Ewido Security Suite – http://www.ewido.net/en/

Abtrusion Protector – http://www.abtrusion.com/Downloads/appersonal.asp

Spybot Search & Destroy – http://www.safer-networking.org/en/index.html

Ad-aware Standard Edition – http://www.lavasoft.de/support/download/

Firewall Tools:
Kerio Personal Firewall – http://www.kerio.com/us/kpf_download.html

Agnitum Outpost – http://www.agnitum.com/download/outpost1.html

Look 'n' Stop Lite – http://www.looknstop.com/En/download.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

ZoneAlarm – http://www.zonelabs.com/

Sygate Personal Firewall - http://smb.sygate.com/products/spf/spf_ov.htm

References

1 National Center for Education Statistics – Internet Access in Public Schools and classrooms: 1994-2000 (http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2000086)

2 National Center for Education Statistics - Computer and Internet Use by Children and Adolescents in 2001 (http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2004014)

3 America Online/Digital Marketing Services – Press Release 2003 (http://media.aoltimewarner.com/media/newmedia/cb_press_view.cfm?release_num=55253423)

4 FBI Press Room – Congressional Statement 2000 on Cybercrime (http://www.securitymanagement.com/library/cybercrime0200.html)

5 Aaron Dolan – Social Engineering (www.sans.org/rr/catindex.php?cat_id=51)

6 Jakob Nielsen's Alertbox, April 14, 2002 (http://www.useit.com/alertbox/20020414.html)

7 U.S. Department of Justice – Office of Juvenile Justice and Delinquency Prevention – Fact Sheet (http://www.ncjrs.org/html/ojjdp/annualreport2000/chap6.html)

8 BSA / IDC 2004 Global Piracy Study (http://www.bsa.org/globalstudy)

9 Shauna Munson (www.giac.org/practical/GSEC/Shauna_Munson_GSEC.pdf)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of Figures

1 Figure 1 -- Percent of 5-17 year olds using computer or the Internet, by age: National Center for Education Statistics 2001

2 Filter options from We Blocker v2.1 by We-Web Corporation

3 Depiction of Defense in Depth layered approach

4 NTFS security dialog Windows 2000 by Microsoft Corp.

5 Example of encrypted text

6 Depiction of NAT zone

7 Event View – Windows 2000 by Microsoft Corp

© SANS Institute 2004, Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced