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.

The Weakest Link...This Is Not a Game!

Since the beginning of recorded time, history has proven that man has oftentimes recorded "his or her" version of whatever event was taking place at a particular time. As a result of these individual interpretations, history has many times been altered to suit the wants, needs or desires of the beholder. Enter the age of the computer and you will find that nothing has changed. Research has proven that "human nature" has altered very little since the introduction of computers in the workplace and private use. The detach...

Copyright SANS Institute
Author Retains Full Rights

AD

THE WEAKEST LINK….THIS IS NOT A GAME!
By Jack_Daniels_GSEC-Retake
Version 1.2e

Since the beginning of recorded time, history has proven that man has oftentimes recorded "his or her" version of whatever event was taking place at a particular time. As a result of these individual interpretations, history has many times been altered to suit the wants, needs or desires of the beholder. Enter the age of the computer and you will find that nothing has changed. Research has proven that "human nature" has altered very little since the introduction of computers in the workplace and private use. The detached attitude that most users have towards computers, as far as security is concerned, is to hand that responsibility to either Computer Security and/ or the Network Administrator. The complacent user is extremely common in all phases of our workplace and as a result now becomes "THE WEAKEST LINK".
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO46063,00.html

The complacency mentioned above has now become our major liability. Until our own computer, either in the workplace or at home, has been attacked, we remain inactive and docile. What used to be coined as a "day to day" changes in our modern technology and now come down to "minute to minute" attacks which are creating immense losses to major companies as well as at-home pc users. Most people wouldn't dream of driving their car to the city and leaving the keys in the ignition with the doors unlocked, but don't think anything about sitting at their desk and opening their "mail", only to find that one piece was an attack and has wiped out their computer and infected many others as a result.

The question is not "IF" you are ever attacked and infected, the question is "WHEN". On this note, the subject of firewalls comes into play. Once again, the Weakest Link believes that the safety and well being of their data of which they have so willingly typed into the computer is safe and totally impenetrable. Firewalls, like computers, come in all different sizes and values. It is now possible to purchase a comprehensive firewall for around $2,000. That's not to say that a company could still spend up to $60,000 for a more sophisticated product. A second line of defense is Anti-Virus software with automatic update. But then again, keep in mind, that every company is still vulnerable to inside saboteurs such as disgruntled employees and such.

Education is still the strongest asset to begin the decline of a hackers attack. If upper management has become more informed as to the seriousness of these attacks and passes this on to lower management who then parlays this over to the workforce of the company, then the cost of the firewalls would then be offset by the fact that the company would not be as vulnerable to attacks and thus not have their computers shut down and as a result lose business, which in many cases has proven to be in the millions of dollars. For example, the high-profile attacks on the major technology players such as Yahoo and Microsoft have since alerted every company to the potential danger of doing business over the Internet. Unfortunately, many companies have since discovered that an attack can create an immediate loss of revenue, productivity loss, potential long-term loss of customers or competitive position and possible legal exposure-whether in the form of lawsuits or fines from government regulatory agencies.

Speaking of government, presently, "The Weakest Link" is probably not even aware of the many laws that are presently before our Congress and Senate on both the state and federal levels in an effort to try to bring these security breakers to justice. Unfortunately, most of our government officials are also "weak linkers" as a result of their own lack of knowledge, and this means that the laws they are trying to hard to pass will also contain "holes" and misinformation and will merely add more paper to the already full volumes of laws in our land.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

If there isn't an overall understanding and reinforcement of these issues, employee practices concerning security can be extremely lax. Scenario-based training can help employees learn how to respond in certain situations, but education must go hand-in-hand with good business policies. Your business needs a policy that says very strongly: "NEVER give out your password, even when you know for a fact who the person is on the other line." Many security experts have reported that many breaches in security were caused by employee naiveté or the "it can't happen to me" attitude. All it takes is one employee to decide not to use the proper procedures set up by management and the system is either shut down completely, data becomes manipulated or oftentimes stolen.

Among hackers' strategies is something called "Social Engineering", which does not involve sophisticated programming skills, but is based entirely upon the weakest link (human weaknesses). There is no software or hardware solution to manage this phenomena. A hacker can pick up the phone and pose as security, giving the staff member a problem and ask for his or her password or computer setup. Email viruses are spread by the human element of curiosity. This happens so often, that businesses are now reluctant to admit how many times they are hit. Social Engineering can also be used by management and Security Administrators to educate the user. Thus, the same tool the hacker's use can be reversed and utilized to educate the public.

Policy and Education:

Educating the public is not just a computer-based training course and classroom instruction, but an all-out constant reminder of vigilant security practices utilizing regular e-mail messages, screen banners, poster-of-the-month programs, mouse pads and bookmarks. This message has to be imbedded into each employee as to the awareness and the seriousness of it on every level of business. Even if we began today in training employees, it would still take years to have everyone understand that each person who operates a computer connected to the Internet is vulnerable to several different kinds of invasion.

To combat the latest threats, companies are beginning to use a number of approaches in building their awareness for security. For example, a web-based awareness course that addresses handling passwords, viruses and other critical topics as well as a clearinghouse for hoaxes and the latest real viruses. Maybe a weekly email bulletin of the latest hoaxes and viruses. This will go along way to elevate user panic from hoaxes that could cause a "Denial of service". Point user to a creditable web site like: http://hoaxbusters.ciac.org/

Even when a company has a good security awareness program, many employees really don't think it important enough to give it their full attention. To add to the problems, employees frequently don't realize they have a critical role to play. "The attitude still largely within the rank and file is, "Well, somebody is taking care of security for me. This is when training of management is especially critical. Because if management can explain the "why" of it and make it understood that one employee does make a difference and let them see how easy it is to break a weak password, then the company has no other choice – they must have the appropriate level of training to do the job in the most productive way possible.

The following article might be useful when you are trying to get management bye-in:

A recent survey commissioned by Camelot and eWeek and conducted by Digital Research indicates that authorized users, such as employees, contractors and Consultants, commit the majority of security breaches at companies. Companies are placing greater emphasis on IT security issues by increasing internal IT network Security budgets. Survey results include: The top two reported security breaches come from within the company's network: 57% of

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

respondents cited users accessing resources they shouldn't be entitled to as a cause of network security breaches 43% of respondents indicated security breaches were caused by user accounts left open after an employee has left the company IT security budgets are on the rise: Nearly half of the companies surveyed are increasing the budget for network security software and hardware. One in three companies have an annual budget specifically allocated to maintain and/or upgrade a network security system. Of those companies, 40% have an annual budget of at least $100,000 for network security systems. Close to half of the respondents plan to upgrade their network security system. "Although this survey validates that companies are taking steps toward establishing network security systems, the need to focus resources to maintain network security policies inside their companies remains unyielding," said Carolyn Adams, Research Director, eWEEK. "Unless companies proactively secure areas of weaknesses within their networks, these statistics will increase indefinitely". The results of this survey are based on 548 online surveys completed by business and IT decision makers. A sample of this size is considered accurate to plus or minus 4.2 percentage points at the 95% confidence level.
By Peter Fricke, CommWeb.com
Jun 19, 2001 (10:07 AM)
URL: http://www.commweb.com/article/COM20010619S0002

Finally, a security awareness policy should be constantly vigilant after the initial training in making sure that all employees continue to maintain the level of security they were taught when they were hired. The Computer Security Institute based in San Francisco estimates that up to 80 percent of computer attacks come from insiders. This places companies in the position that information, passwords or computer setups are not only restricted to the outside, but to the inside as well. Security Policy templates are a good starting point when laying out your security policy. There are many sources for the templates, one of which can be found at:
http://www.sans.org/newlook/resources/policies/policies.htm
Security experts say you can make your training program more effective by following these steps:
1. Get top management on board.
Without management behind you, you have no credibility, no protection, and no enforcement or funding to carryout any security policy you may have in mind or have developed already. Before approaching management with your security ideas, you should get you ducks in line as far as a rough security policy that management can add to and later presented to other departments for their input, which will insure the feasibility of the plan in relation to the business your in. Maybe your company had a recent hacker incident that you can use as a door opener or better put, an eye opener for management. If you have never been attacked, then you can show what happened to other businesses that got hit by attackers and what the cost was as far as loss of business due to a "Denial of Service" or compromised trade secrets. A good resource when talking to accounting types is the CSI/FBI Computer Crime survey which besides showing the type of computer crimes but also the financial loss of each. If funding is a problem due to budget constraints, you might want to have a security plan that can be implemented in stages. Training cost can be lowered by just training the network administrator and then he/she can train the workforce. Another example would be to have a lunch time session where a group of employees have lunch together while they are shown a slide presentation; maybe management bought the lunch for them.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

2. Tie the training to the mission of the Agency/ Company.
The training should show what the company does and how this could be compromised by hackers.
3. Develop a comprehensive program. A good security program should involve a mix of computer-based training and classroom instruction, as well as ongoing awareness efforts such as posters, flyers and regular e-mail messages. Maybe consider hiring an outside consultant with expertise in the security field. SANS might be a good choice.
4. Teach the "whys" as well as the "hows" of security. Employees are much more likely to follow security rules if they understand the consequences of not following them. This is where management backing is important and enforcement will be carried out according to policy that management has signed up to.
5. Offer role-based training. Beyond the fundamentals, managers and Web developers need more in-depth security training than clerks and human resources personnel. Technical staff will require more in-depth detail in security training and management training would focus on cost affectedness of the security policy. The rank in file would only need general information on security threats and teach them to be aware of thing that might not look normal with there computer systems.
6. Account for the different types of employment environments, including in the home, in the field and in foreign countries, as well as at contractors' locations. Company work being done on computers at home, in the field and foreign countries are probably the most vulnerable and security training has to be geared for this type of environment, which should include education on personal firewalls and anti-virus protection as well as cautions on media carried to work. Also if traveling to a foreign country, you cannot have a 128bit browser on your system and your laptop can be confiscated along with any company data on the laptop. A possible precaution with foreign laptops is to have some spare laptops configured for foreign use and only these laptops can be used abroad.
7. Make the training dynamic. Training needs should be constantly monitored and content refreshed on a regular basis. It's apparent by reading most security bulletins that as soon as you find vulnerability and patch it, another pops up soon afterwards, and so, any security training will have to be dynamic. To schedule training every 6 months might not appropriate for the present hacker traffic and maybe you need a 3-month schedule that is just an update type of training.
8. Train individuals as needed. If new employees arrive after a security-awareness course has been held, don't wait until next year's course to bring them up-to-date. You could have a security training tape made that is updated each time you have new training and this tape would be required viewing for all new employees.
9. Always follow up. Employee practices must be monitored using audits or system controls, and their awareness of security measures should be reinforced on a regular basis. All employee machines should be setup by authorized company technicians who will ensure that all security patches, scripts and controls are installed prior to employee use. Employee machines should be audited periodically for security settings, to be sure employee have not changed the settings. Make it a requirement for computer accounts to be renewed each year based on a security test given to all computer users.
BY Heather Hayes, " Security Training Checklist"
June 18, 2001
Federal Computer Week
Comments and conclusions were added to the above checklist.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx1-06-18-01.asp
Backup of company data is an important part of the "Security Policy". This backup not only refers to the company data servers but also data accumulated by each employee and stored locally on their workstation. Employees must be made conscience of the fact that the data they produce is company data and most often is sensitive data and has to be backed up. The backup process must be made automatic and transparent to the user, when it comes to the data on their systems, and it would be a mistake to assume the user would back the data up. A requirement of the automatic backup of user data would be that all apps that produce data will be stored in one folder, and the folder name would be the same on all users machines. Off-site archiving of tapes is essential, along with periodical restore tests of older archive tapes.

Conclusion

Your perimeter may consist of a Firewall, Anti-Virus and maybe an Intrusion Detection system like "Tripwire", all of which must be tuned constantly for the latest threats and for the most part they will hold the perimeter secure. Your employees have the ability to bypass the Perimeter everyday just by coming to work, and here lies the greatest challenge. They can bring just about any virus right past the perimeter in the form of a Floppy Disk, Jaz or Zip cartridge, ReadWriteCD, and not to be overlooked the "Palm Pilot", which just recently found to carry a virus. Most anti-virus scanning programs will cover these devices but Palm Pilot scans require special options added to your anti-virus software, which was just recently made available to look for Palm Trojans. More employees are using their home computers to do office work and security policy as well as education should address this situation by requiring Personal Firewalls and Anti-Virus software. It would be cost effective in the long run for the Company to supply these necessary tools for home system protection. Remember some of the tools that you as an administrator are using for vulnerability checking are actually hacker tools and you need management backing before using them, or you might find yourself out on a limb with possible legal repercussions. Even if access from home is through a VLAN tunnel, which is very secure, you have to consider where the home system has been before the VLAN connection, and possibly picked up a Trojan while on their regular ISP. Research has shown that the majority of successful attacks are done on a few well-known vulnerabilities that were not patched early on or forgotten about. The single most important thing an administrator can do is to keep the patches updated. Some of the reasons for not applying the patches in a timely manner is that the administrator is busy doing regular duties and preventive maintenance,
or the fact that you just can't apply a patch and hope it is compatible with the applications running on your system. A good example of checking what patches are needed, would be a system that I use on our IIS Server, where I run a program called "Update Expert"(St. Bernard Software), http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
which checks my system for patches and will list what patches are needed, however it does not tell you which ones are most dangerous, so I check with SANS to see what patches are really needed. Security awareness is everyone's job and if you develop a complacent attitude, then maybe someday that job will not be there anymore because of a hacker. There is some similarity to the game show "The Weakest Link", and that if you turn out to be the Weakest Link in your company, Security Policy dictates that you leave. Finally, the recent "Code Red " worm attack once again shows that the human element cannot afford to be complacent about attacks, the community acted together and acted fast. It looks like we are coming around to the fact that attacks real and more prevalent than ever before and we are becoming more alert to our 'Weakest Link".

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

http://www.computerworld.com/cwi/story/0,1199,NAV47_STO41770,00.html
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59373,00.html
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58119,00.html
http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx2-06-18-01.asp
http://www.fcw.com/fcw/articles/2001/0618/sec-feat3bx1-06-18-01.asp
http://www.computerworld.com/community/security
http://www.commweb.com/article/COM20010619S0002
http://grc.com
http://www.commweb.com/article/COM20010619S0002
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
http://www.networkmagazine.com/article/NMG20010720S0002

© SANS Institute 2001, Author retains full rights.

Last Updated: May 6th, 2016

Upcoming SANS Training

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

SANS Stockholm 2016	Stockholm, SE	May 09, 2016 - May 14, 2016	Live Event
SANS Baltimore Spring 2016	Baltimore, MDUS	May 09, 2016 - May 14, 2016	Live Event
SANS Houston 2016	Houston, TXUS	May 09, 2016 - May 14, 2016	Live Event
SANS Melbourne 2016	Melbourne, AU	May 16, 2016 - May 21, 2016	Live Event
Beta 2 Cincinnati - ICS456	Covington, KYUS	May 16, 2016 - May 20, 2016	Live Event
Security Operations Center Summit & Training	Crystal City, VAUS	May 19, 2016 - May 26, 2016	Live Event
SANS SEC401 Luxembourg en francais	Luxembourg, LU	May 30, 2016 - Jun 04, 2016	Live Event
SANSFIRE 2016	Washington, DCUS	Jun 11, 2016 - Jun 18, 2016	Live Event
SANS Philippines 2016	Manila, PH	Jun 20, 2016 - Jun 25, 2016	Live Event
SANS Pen Test Berlin 2016	Berlin, DE	Jun 20, 2016 - Jun 25, 2016	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 23, 2016 - Jun 30, 2016	Live Event
SANS Salt Lake City 2016	Salt Lake City, UTUS	Jun 27, 2016 - Jul 02, 2016	Live Event
SANS Cyber Defence Canberra 2016	Canberra, AU	Jun 27, 2016 - Jul 09, 2016	Live Event
MGT433 at SANS London Summer 2016	London, GB	Jul 07, 2016 - Jul 08, 2016	Live Event
SANS London Summer 2016	London, GB	Jul 09, 2016 - Jul 18, 2016	Live Event
SANS Rocky Mountain 2016	Denver, COUS	Jul 11, 2016 - Jul 16, 2016	Live Event
SANS Delhi 2016	Delhi, IN	Jul 18, 2016 - Jul 30, 2016	Live Event
SANS San Antonio 2016	San Antonio, TXUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS Minneapolis 2016	Minneapolis, MNUS	Jul 18, 2016 - Jul 23, 2016	Live Event
SANS San Jose 2016	San Jose, CAUS	Jul 25, 2016 - Jul 30, 2016	Live Event
Industrial Control Systems Security Training	Houston, TXUS	Jul 25, 2016 - Jul 30, 2016	Live Event
SANS Boston 2016	Boston, MAUS	Aug 01, 2016 - Aug 06, 2016	Live Event
Security Awareness Summit & Training	San Francisco, CAUS	Aug 01, 2016 - Aug 10, 2016	Live Event
SANS Vienna	Vienna, AT	Aug 01, 2016 - Aug 06, 2016	Live Event
SANS Prague 2016	OnlineCZ	May 09, 2016 - May 14, 2016	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced