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.

Who Wants To Be A Weakest Link?

This paper emphasizes the need to convey good security practices throughout an organization, because the "weakest link" can be located anywhere along a company's "chain." Possible weak links are discussed and an attempt is made to explain the need for preemptive education via "what-ifs." An assumption is made that employees are interested in keeping their jobs. The main "what-if" has to do with the loss (or downgrade) of positions held by the company's security weakest links. Another "what if" involves the possible los...

Copyright SANS Institute
Author Retains Full Rights

AD

Who Wants To Be A Weakest Link?

SANS Security Essentials GSEC Practical Assignment V. 1.3
March 7, 2002
Russell T. Hany

Abstract

This paper emphasizes the need to convey good security practices throughout an organization, because the "weakest link" can be located anywhere along a company's "chain." Possible weak links are discussed and an attempt is made to explain the need for preemptive education via "what-ifs." An assumption is made that employees are interested in keeping their jobs. The main "what-if" has to do with the loss (or downgrade) of positions held by the company's security weakest links. Another "what-if" involves the possible loss of the all-important dollar. It can, unfortunately, be concluded that no matter how hard security experts within a company try, they cannot fix all the weak links in a chain, but continued multi-directed efforts must be maintained to strengthen them as much as possible.

The Stage

You've worked countless hours to put together a very secure network for your company. From the CEO down, you and your staff have been given every resource needed to put everything in place that you could possibly have. The CEO's Executive Committee is now very confident that your company's systems and information is locked down – it was expensive but they are confident that the impenetrable security was worth it. But then something happened…

In this, obviously, fictional company (what CEO is ever going to give a security department a blank check?) things that aren't so fictional crept into the well-designed and very expensive security structure. The Weakest Link Syndrome started showing up in places it was expected, and in some that it wasn't. Real-life companies need to look into ways to prevent both hypothetical and actual weakest link situations. Simply looking into the problem, however, won't be good enough. Strengthening the weakest link before it breaks is a crucial security step.

If, however, that link breaks before it is strengthened, how will that link feel once he/she is identified? A long list of people will most probably come up with some unpleasant experiences for the unfortunate employee (ex-employee). If each and every employee is

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

forewarned of possible negative experiences happening to them, those weak links might actually attempt to strengthen themselves.

A slightly unpleasant experience might be in store for an employee that mistakenly downloads a minor virus, but what would happen if that mistakenly downloaded file turns out to be something else - something a bit more far-reaching?

What do you think might have happened to the employee who was responsible for a recent hacking that involved the personal data of "former president Jimmy Carter, activist actors Warren Beatty and Robert Redford, and Internet gurus Vint Cerf and Larry Lessig?"[1]
(http://story.news.yahoo.com/news?tmpl=story&cid=75&u=/nf/20020227/tc_nf/16544)
That breach was achieved through poorly configured proxy servers, but who's to say that it couldn't have happened through mistakenly downloaded malicious code? Conscientious employees take steps to avoid obvious security breachs that could result in the loss of customers' personal data, but do employees realized that innocent looking downloads might have far reaching impact? If you can convey that concern to them, it might just be a way to have the weak links strengthen themselves…

Where is that darn Weakest Link?

Finding and fixing the weakest link in a security "chain" is a never-ending process. As soon as one link is fixed, another one (or more) becomes the weakest. A security team can look for obvious weaknesses, but the chain will never hold up to the stress that will no doubt be placed on it in the computer-intense 21st Century unless the links have some sort of self-awareness. People who understand that really bad things can happen due to carelessness and oversight are strong links in security chains, and the obvious goal is to have all the links strong. That requires the knowledge to be thoroughly spread.

Many chains have snapped in the past, and some have held up. By understanding and dissemination of previous lessons learned to others, we can strengthen our company steel. Let's take a look at some areas where our "chains" can be strengthened and how that strengthening might be achieved.

The User Link

Users are tough links to strengthen because there are so many of them – and so many bad things that they can do. Even if you could prevent every user from committing SANS Institute's list of five worst end user mistakes (each of which can turn a good employee into a weak link), [2] (http://www.sans.org/mistakes.htm)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Failing to install anti-virus, keep its signatures up to date, and apply it to all files.
2. Opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources.
3. Failing to install security patches-especially for Microsoft Office, Microsoft Internet Explorer, and Netscape.
4. Not making and testing backups.
5. Using a modem while connected through a local area network.

they will still find other methods to weaken the chain. It's a challenge, but getting users to think "security thoughts" has got to be your ultimate goal.

Not every security exposure can be taught to users through courses or e-mails. Unexpected security threats come about through day-to-day activities and must be recognized and dealt with as they occur (on the fly). An example of this would be the use of a photocopier. How many people run into a copying room and make a few copies of a report on their way to a meeting? The copies will only be handed out to a few people, and those people can be trusted with the content, so that information should remain secure, right? Well, no. The SECURITYsense website details some misconceptions that people have about computer security involving photocopiers:

(http://nsi.org/NSIProducts/SECURITYsense/Samples/2oct01.html)

> Today's copier/printers are actually sophisticated computers that are often connected to the company network and feature hard drives, which are used to save document data. This means a copier/printer's hard drive contains all manner of sensitive corporate information.
>
> About 1,100 IT and networking professionals the people usually in charge of managing printer/copiers responded to the survey. Perhaps the most troubling finding was that 77% of all respondents did not know their copier contains a hard drive.
>
> The most common security threat to printer/copiers is theft of the hard drive. But because the machines are part of the company network, they are also vulnerable to remote hackers, experts say.[3]

What might happen to the intern that runs off a few copies of a salary report at the last minute – instead of printing them on his sponsor's printer? Well, if nothing happens to the copier's hard drive he should be all right. But if something does happen… he is the weakest link – Good Bye.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Alan S. Horowitz has a list of security mistakes that point out some more potential weak links[4] http://www.computerworld.com/itresources/rcstory/0,4167,STO61986_KEY73,00.html?OpenDocument&~f: "**The not-so-subtle Post-it Note.**" So you spent hundreds of hours integrating all of your platforms so they can all be accessed with a single REALLY STRONG password, and you were able to get all of your users to sign off that they would use that hard to remember little monster… What if the Vice President's Secretary, Betty, writes his password down on a Post-it Note because she has to get into his e-mail when he's gone? Someone spots it on Betty's monitor and sends out some e-mail from the VP's account. Betty may have taken good dictation, but she is a weak link. She will be missed – Good Bye.

Horowitz reports an estimation of 15 – 20% of employees within an office supply manufacturer in Florida regularly use that method to remember their passwords. If employees in that company are advised that there might just be a really big farewell party for those who continue to weaken the security chain that way, the sticky pad memory might just come to an end. It would be even better if they can be made to understand WHY that was a bad idea – which would be a start in strengthening the high percentage of very weak links.

Some more mistakes on his list: "**We know better than you.**" Some users think they know that some security measures aren't really all that necessary, so they "do an end-run around you." A user "**leaving the machine on**" when he/she walks away from their desk is an obvious problem. No passwords needed, everything free for the taking, 'nuff said – Good Bye.

"**Laptops have legs.**" Unsecured, unattended, laptops can disappear quickly. Did you ever notice how laptops all pretty much look the same? Who's going to spot someone with a laptop and say, "Hey, that's Joe's computer! You go put it back." Nobody is going to spot something like that. Since they can't, Joe's should have some excitement added to his day when he gets back to his desk. "Hey, where's my computer? What am I going to do now?" Hopefully he has a box for his personal items. Good Bye Joe.

Joe's disappearance should serve as a message for anybody who hears about his little "experience." They will probably tend to lock down their laptops a little more rigorously – thereby strengthening the chain. Thanks for the life lesson Joe, but no thanks for the cleanup effort that will have to take place due to the compromise of everything he had access to – and maybe even things he didn't have access to…

Users who think that no matter what they do, they won't be shown the door should probably think again. Lisa Kelly reports that 90% of US companies reported some form of security breach in 2000 (via ePrivacy & Security Report) [5] http://www.vnunet.com/News/1116612. The cost of those breaches totaled up to $265 million. How much money do you think most employers are willing to lose on account of weak links? That might not be something most are interested in testing.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Administrator Link

The people who actually dole out the access to users are also common weak links. The goal of security administration is to give out only the access that is needed to only the people who need it. Anything above and beyond those end points qualifies as an unnecessary security risk.

The same goes for taking access away from those who don't need it. A real-life example of a costly blunder caused by not removing a user's access has to do with "revenge hacking." [6] http://nsi.org/NSIProducts/SECURITYsense/Samples/20jul01.html The day a "high-tech" employee got fired, he decided to delete hundreds of the company's electronic files and to send out false e-mail from the company. He was apparently a weak link that the company did part ways with, but with him out of the way the Administrator weak link was exposed. The fired employee's access should have been removed immediately. If the responsible Administrator knew of the firing and didn't take the proper steps, it might be time for his/her good-bye speech. If, however, Human Resources did not get the information to the Administrator in a timely fashion the story would be different. A system must be in place to quickly delete accesses to users who have been shown the door.

How about an Administrator who decides to save some time by giving all temporary employees from one company the same ID and password? Can you smell the weakness of this link? SANS described one such incident:
http://rr.sans.org/encryption/war_stories.php

> The customer realized that it could save money by hiring temporary workers in the shipping department. The system administrator realized that she could save time and money by re-using the same account login and password for all the temporary workers. Last of all, one of the previous temporary workers had realized that with the shipping clerk away at lunch between noon and 1 pm and the unchanged shipping clerk's account login and password, he could send his friends a new laser printer every week.[7]

Knowing exactly who should get what access is a tough thing to do, but giving out the same Ids and passwords to many different people? Good Bye!

The Manager Link

Managers, while not always physically generating security problems, can definitely always be involved amongst the mental weak links. Greg Shipley relates a story about a small company (i.e.: the Management of the company) that didn't feel it was a target for

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

hacking. They had nothing to do with credit cards or national security (that's the only thing hackers are interested in, right?), so they should be nice and safe. That company found that all of its servers had been very violated. This is a good example that security through obscurity is a myth.
http://www.networkcomputing.com/1204/1204colshipley.html

> The folks at that small organization now face four options: Investigate every file on their systems and attempt to identify all possible Trojans, which translates into months of difficult work. Rebuild every machine from scratch and change every password on the entire network. Permanently disconnect from the Internet, eliminate dial-up access and hope the intruders weren't internal. Or continue operations and pray the problems and potential time bombs won't resurface. [8]

If the manager who decided the company wasn't a target is still in the building, he or she had better be wearing a disguise and taking some security classes. My guess is that mistake won't be made again, but what might the next one be?

A fear of what might happen could be the best way to educate the weakest managerial links, but most of them are fairly secure in their positions. They probably won't relate very well to the "Good Bye" threat. The loss of the almighty dollar should be a much better incentive to the upper crust. Maybe the story of an easily preventable loss of $100,000 would make some unsuspecting managerial weak links straighten up a little?

NSI reported a story about an unhappy former employee of SkyNetWEB Ltd. [9] (http://nsi.org/NSIProducts/SECURITYsense/Samples/1aug01.html) Using his supervisor's password to access the company's web-hosting network; he was successful in shutting down one of his ex-company's biggest clients. A manager's changing (or not giving out his password in the first place) could have saved the company $100,000… Hmm? If it's not Good Bye, it should at least be GULP.

Not all managerial mistakes are as easily preventable as not giving out passwords, but simple supervision can comes in handy too. Denial Of Services (DOS) has become known as a very common and devastating internet attack. It can occur internally as well. The source of a recent DOS was hiring practices and lack of supervision. [10]
http://rr.sans.org/encryption/war_stories.php

A cable company had branched out into the internet provider/web hosting services. They decided to use local college students for labor. As time went by the company kept running out of data storage space, so they continued to buy more. They figured their business was going really well. What the management failed to notice was that the college student employees were storing all sorts of MP3 music files and they themselves were eating up all the storage space. The actual customers were unable to store all of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

their data when they needed to. While this might lead to some Good Byes to the college students, the managers should have been focused a little closer on the problem.

Others may use the lesson learned by those unfortunate managers as an example of the wide range of 21st Century problems that can occur. It is a good reminder that many things simply cannot be predicted and taken care of through security checklists. Brains must always be used. The demonstrated threat of dollars lost will hopefully pump more blood through the upper management cranial units.

While the previous examples of strange security blunders are good examples that managers should always try to think outside of the security "box," it is still necessary to remind them of what sort of security measures are inside the "box." Orthus has put together a list of top ten security mistakes made by managers.[11]
http://www.orthus.com/health_mistakes.html

1. Fail to establish solid policies and procedures.
2. Pretend that the problem will go away.
3. Authorize reactive, short-term fixes so problems re-emerge rapidly.
4. Fail to realize how much money their information and organizational reputations are worth.
5. Rely primarily on a firewall.
6. Communicate to employees their security responsibilities.
7. Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow-through necessary to ensure that problems stay fixed.
8. Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
9. Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.
10. Fail to understand that security is a process not a product.

Each of the ten mistakes is important, but depending on what sorts of services are offered by a company their priorities may differ. The goal to get managers to understand and avoid the identified pitfalls is a nasty challenge that will probably never totally go away, but continued effort must be made. The fear factor is a good tactic to start with, but it won't always work. Other methods aimed at educating all of the weak links are suggested later in this paper.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Weak Hacker Link

It is nice to know that weak links can also occur on the other side. Bad guys also make mistakes, and I recommend that they not be educated to prevent future mistakes. The FBI is on the trail of some of the September 11 terrorists who made some security mistakes. [12] http://nsi.org/NSIProducts/SECURITYsense/Samples/15oct01.html They apparently accessed the internet from public libraries thinking they would keep their anonymity using such a public method. Well, that train of thought might just work into a double whammy for them. Not only may they be identified through their online chats and e-mail exchanges, but also anything else they did on those machines may be traced. If they did any research on future terrorist plans, it might not be too secret any more. When their "upper management" finds out what they did, the Good Bye they receive might just be a little bit worse than losing their jobs… That would be a darn shame, wouldn't it?

Other Methods of Strengthening Weak Links

Okay, you've heard the "Good Bye" threat several times and you're still not buying that it will work on everybody. Fine. Feel free to use some other types of methods (whatever it takes). A soon to be released book, "The 4th Edition of the Computer Security Handbook," [13] http://nativeintelligence.com/awareness/chap29-7.asp looks into several other tools that may be used to promote good security practices:

- Intranet and/or Internet
- Screen Savers
- Sign-on Screen Messages
- Posters
- Videos
- Trinkets and Give-aways
- Publications
- Surveys, Suggestion Programs, and Contests with Prizes and Awards
- Inspections and Audits
- Events, Conferences, Briefings, and Presentations

These methods promote more of a positive reinforcement type of incentive to employees in attempt to transfer security knowledge than the Good Bye threat does. The styles and sizes of individual companies are factors in determining what methods will work best. You must decide on your own how to convey the security message, but the most important thing to remember is that you MUST convey the message.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary

Weak security links can show up anywhere along a company's security chain. Steps can be taken to prepare, train, educate, and scare employees into safer and more secure practices, but people must also be trained to use their minds. Use whatever method(s) you can get users to think of the consequences of their actions. If you can get you users to understand that others in their positions have unwittingly caused all sorts of damage to their companies (and have paid the price for it), then maybe they will take steps to avoid similar situations happening to them. Even hypothetical situations can be used to convey the train of thought that should be used when dealing with computers in our day and age. A stitch in time saves… a big security mess.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

REFERENCES

[1] Lyman, Jay. "New York Times Hack Exposes High-Profile Data." 27 Feb 2002. URL:http://story.news.yahoo.com/news?tmpl=story&cid=75&u=/nf/20020227/tc_nf/16544 (6 Mar. 2002).

[2] "Mistakes People Make that Lead to Security Breaches." Updated 23 Oct. 2001. URL: http://www.sans.org/mistakes.htm. (2 Mar. 2002).

[3] "Did You Know the Photocopy Machine Poses a Security Risk?" National Security Institute, Inc. URL: http://nsi.org/NSIProducts/SECURITYsense/Samples/2oct01.html (2 Mar. 2002).

[4] Horowitz, Alan S.. "Top 10 Security Mistakes." 9 July 2001. URL: http://www.computerworld.com/itresources/rcstory/0,4167,STO61986_KEY73,00.html?OpenDocument&~f (2 Mar. 2002).

[5] Kelly, Lisa. "Security breaches soar in US." 19 Jan. 2001. URL: http://www.vnunet.com/News/1116612. (3 Mar. 2002).

[6] "'Revenge Hacking' Nets Jail Time for Employee." National Security Institute, Inc. http://nsi.org/NSIProducts/SECURITYsense/Samples/20jul01.html. (2 Mar. 2002).

[7] Seidl, Ronald. "Who's Really Logged On?" An Overview of Computer Security as Told Through War Stories. 26 July 2001. http://rr.sans.org/encryption/war_stories.php (2 Mar. 2002).

[8] Shipley, Greg. "The High Price of Vulnerability." Security Watch. 19 Feb. 2001. URL: http://www.networkcomputing.com/1204/1204colshipley.html (5 Mar. 2002).

[9] "Ex-Employee Arrested in Crippling of Computer Network." National Security Institute, Inc. URL: http://nsi.org/NSIProducts/SECURITYsense/Samples/1aug01.html (1 Mar. 2002).

[10] Seidl, Ronald. "Availability." An Overview of Computer Security as Told Through War Stories. 26 July 2001. URL: http://rr.sans.org/encryption/war_stories.php (5 Mar. 2002).

[11] "Ten Most Common Security Mistakes." Orthus Information Security Solutions. URL: http://www.orthus.com/health_mistakes.html (6 Mar. 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[12] "FBI Tracks Terrorists' Cyber-Footprints." Water Cooler Stories. National Security Institute, Inc. URL: http://nsi.org/NSIProducts/SECURITYsense/Samples/15oct01.html (6 Mar. 2002).

[13] Rudolph, K.; Numkin, Louis; Warshawsky, Gale; "Seurity Awareness." The upcoming 4th Edition of the Computer Security Handbook. URL: http://nativeintelligence.com/awareness/chap29-7.asp (3 March 2002).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 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**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**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**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**