Global Information Assurance Certification Paper

Securing my organisation
By Martin Spence. GSEC Paper 20th July 2004.

Contents

Abstract

2004 saw myself undertake a SANS Security Essentials Course. At that time I was a (Microsoft) Systems Administrator for a small / medium enterprise. What I will cover in my paper is what happened when I returned from SANS. I will list 10 areas which I have identified as areas of concern, how I identified these areas and also how I addressed these areas of concern and what my solutions were.

At the time of finishing my SANS course, my organisation had just recently migrated all client workstations to **Windows XP** (with the exception of some laptops). Our single domain infrastructure ran under a mix of **Windows 2000** and **Windows 2003** servers. Our company's firewalls and routers security were handled by a third party IT Security Company and, as such, are not covered in this document.

Before

The organisation I worked for was a small and young enterprise. It had experienced phenomenal growth since its inception but as a result, IT had never had either a security policy nor a Risk and Threat Analysis done. This clearly was a matter of concern and urgency yet immediately gave me something to focus on. It was my aim, and eventual task, to implement a security policy and to assess and address any highlighted security concerns.

I was keen to put into practise what I had learned at SANS. My first step was to brief my IT director and my CEO with my intentions of setting up a security policy for our organisation as well as identifying our threats and risks. I explained that I felt internal security was severely lacking and that staff awareness would have to be raised before we could fully implement a security policy.

The Key areas of concern I had identified to the organisation were as follows:-

1. **Passwords**. I was aware of a somewhat lacking password policy in that there wasn't one. Users were forced to change passwords every year but there was no complexity or history applied to these passwords. Additionally I would frequently come face to face with peoples passwords on a sticky note attached to their computer…
2. **Remote Users**. Whilst I was comfortable with our CITRIX server being secure from unauthorised access, I was not comfortable with the integrity of remote user's pc. A remote user's pc was usually in the family home and therefore, very worryingly, out of the control of the IT dept.
3. **Roaming Users Laptops**. It appeared that functionality was the only goal in the set ups of the roaming users laptops. Windows 95 and windows 98 were the operating system with dial up connections.
4. **All Office Users were members of Local Administrators.** I firmly believed having users as local administrators was a potential security risk.
5. **Admin passwords the same all over.** One password for admin accounts everywhere; switches, servers, everything.

6. **IT staff using Domain Administrator Account.** Who was doing what to what – I had no idea.
7. **No security auditing on servers.** Printing, file access, file modification, deleted files were all going unrecorded.
8. **Spyware, Malware and Virus defences.** Although there was a virus solution in place, I felt that the current one was inadequate and out-of date patches / versions existed.
9. **Patching Procedure.** As a small IT team, patching would sometimes be missed. A new solution to the current system would have to be found.
10. **Regular Security Reviews.** Security and logs would need to be examined on a regular basis.

It has to be noted that this was a company that had grown from 10 people to 240 within a couple of years and still retained a friendly, family-like atmosphere. I knew that without addressing these areas of concern, the company was leaving itself wide open to an opportunist or an accident. Additionally IT needed to protect itself as well as individual members of staff. A security policy was needed as were measures to address the above points.

During

Firstly I sent out a questionnaire to every member of staff relating to security. The purpose of this was two-fold; firstly to raise the profile of security as an issue within the company and, secondly, to gauge the IT security knowledge of staff.

I've attached the questionnaire in Appendices1 but it was clear to see that a lot of users were not technically minded nor security minded. Around 80% had home pcs and half of them did not have, what I would class, good security provision (anti-virus, firewall, good secure Operating System such as Windows 2000 onwards). To start to educate the users I held several lunchtime seminars (around 30 minutes) for a small group of about 30 people at a time. I ran through a PowerPoint presentation explaining about how a home computer connects to the internet, security defences such as firewalls, anti-virus software, Spyware and Malware detection software and of course keeping the pc up-to-date with patches. After this presentation, I would have questions and answer sessions about home pcs and security trying to give as much free advice as I could although I did tell a lot of internet users that they should really be investing in a good operating system and definitely a firewall and anti-virus solution. I was actually amazed at how many people told me that their pc was infected with a virus or that they had virus software but never kept it up to date.

I made a point of making up free CDs for users to take away with Zone Labs' firewall Zone Alarm, Search and Destroy's Anti-Spyware program Spybot as well as virus removal tools from Symantec for the latest batch of viruses such as Netsky, Beagle and Sobig. I did also recommend that users order a copy of Norton's Internet Security as it's a suite of applications and a one-stop shop for updating the firewall and anti-virus program as some users really like their life as simple as possible. It also

became apparent that some users thought the whole patching process very tedious. Again Norton's Internet Security would ease the problem with automatic updates. I drafted a "securing your home pc" guide and put that onto our company intranet.

I received positive feedback from staff and I felt this had been a worthwhile exercise. Having successfully raised awareness of security within the company I was then ready to proceed to tackling the first of my areas of concern - passwords!

1. Passwords

Microsoft has created a list which is called "The Immutable Laws of Security". Law #5 states that, "Weak passwords trump strong security". [1] They go on to describe passwords as a security perimeter. As I had mentioned earlier I was shocked to discover post-it notes on monitors with passwords written on them. Things really were a bit lax around here I thought and my security perimeter was about as secure as a no-entry sign.

One day I went into my company's car-park and noted down the license plate numbers of the cars in the spaces that said 'Reserved for' and then the names of important people and my companies name. Then I went and tried to log in as those users with the license plate numbers as passwords. I was able to gain access to 3 accounts. This was quite worrying as its usually important people who have their own car-parking spaces and important people usually have access to important data. This was the case at my company. Additionally, all these people had Citrix remote access with their usernames.

Just to speed up my impending heart-attack, I also noticed that everyone's SMTP address was the same as their NT log-on names. I really was getting quite worried at this point. All the intelligence I had gathered so far had been free and easy.

Time to step up a gear I thought and inserted my trusty SANS cd into one of our domain controllers. Firing up L0phtCrack I noticed that a Brute Force attack was unavailable in the trial version but the dictionary attack and variant was available. I spent around an hour updating the dictionary with local and cultural words such as soccer teams, pop stars and movie titles. I then ran L0phtcrack to see what it would come back with. Within 10 minutes it had ran through the entire domain and retrieved around 75% of user account passwords. Additionally it also highlighted passwords under 8 characters and blank passwords too. It was time to reach for the aspirin. At least 20 passwords were users own name! It looked like my No-Entry sign just fell off the wall.

I took my findings and came up with the following Company Wide recommendations:-

a) Passwords Policy to be created as part of security policy
b) Password complexity enforced
c) Password minimum length set to 10 characters
d) Password History set to at least 8
e) Password Age set to 3 months.

With my findings and recommendations I then sought management approval. It is worth mentioning at this point that I had received written permission from the CEO to

run a copy of L0phtcrack. I am also glad to mention that my recommendations were accepted and rolled out with immediate effect.

2. Remote User's Pcs

Whilst we had control of user accounts and connections to our **CITRIX** server, there was no control whatsoever over remote user's pcs. We had 15 licenses for more senior members of management and I noted that them or rather their pcs were next on my hit list. You may remember when Microsoft source code was stolen **2**. That successful attack, "according to reports", was down to a hacker targeting a Microsoft employee's home pc via an **Outlook** vulnerability which in turn installed a back-door program. With the Microsoft employee's pc under control, access was in turn gained to Microsoft's network.

I had the senior members of management bring their home computers in so I could audit them. I was particularly worried about a Trojan Horse or a Key Logger infection, particularly as some of these pcs were running **windows 98** or **ME** edition, as this would compromise our **Citrix** server. Additionally an attacker could target these home computers and gain details from it about **Citrix**, recreate a **CITRIX** session to our server and start performing dictionary and Brute Force attacks.

I had already gained budgetary approval to upgrade any pcs. Any pc that was unable to be upgraded to **XP** would be replaced. I upgraded the pcs to run **XP Home Edition** and installed **Norton's Internet Security** whose anti-virus program would handle scripts and emails as well as email attachments. I'd also set up each pc with user accounts as I deemed this to be more secure than user's being administrators of their machines. I had also set up automatic updates for both Windows and Norton's. This was all documented and added to the security policy which was taking form.

Before commencement, however, I had run a full virus scan and a Spyware scan including **BHO Demon** so I could check that there were no infections, nor that Internet Explorer had been hijacked. Sadly a number of machines had been compromised with numerous mass-mailing viruses but luckily there were neither Trojans Horse programs or key loggers.

3. Roaming Users Laptops

A lot of members of staff would work off-site quite frequently. Our company had 8 IBM ThinkPad 600s running Windows 95 utilising Dial-In access to our **Citrix** server and no firewalls! As these laptops were a few years old I did not have any trouble getting management to approve replacements, now IBM ThinkPad X40 with wireless (802.11b). Again with **Norton's Internet Security Professional** running on top of **Windows XP Professional**, I invoked Windows file encryption as well as putting BIOS locks on power-up and hard disk. I had setup all networking connections and then installed Norton's firewall; I then configured a local group policy locking as much down as I could for the roaming user accounts.

At this point I created a roaming user policy requiring each roaming user to

read and sign before taking their laptop away. I'd updated the policy to include:-

a) The laptops were for acceptable company uses only
b) No Software will be installed unless by a member of IT
c) Any Loss, Damage or Theft must be reported to I.T. immediately.
d) No unauthorised use by anyone other than custodian of the laptops.
e) No confidential data must be retained on the laptop

Due to budgetary constraints I was unable to procure a third-party utility for hard disk encryption at the BIOS level; if this had been the case then I would have amended the policy so that confidential data could be stored on the laptop. I did make recommendations that this is one area I would like to focus on after I completed my first ten tasks and it will be shortly up for management review and hopefully approval. This would have given me another layer of protection for our roaming users, particularly in the case of theft or loss. I was concerned that, if one of the laptops as is, were to fall into the wrong hands, the hard drive could be removed, installed into another laptop, and eventually compromised.

In America in 1999 over 1 billion dollars of computers were stolen **3.** Also listed in the article is a comparison with some Fortune 1000 companies losing over 45 billion dollars due to, as the article puts it, "loss of proprietary information". We were giving our roaming users' $1,000 dollar laptops but they could be downloading confidential data worth a lot, lot more onto those laptops.

4. Office Users were members of Local Administrators.

I had identified two applications, requiring local administrator access to some files, which were heavily used throughout the office. I was quite alarmed at having so many local administrators and, whilst we had already rolled out a restricted desktop via group policy, I would have liked to remove the local administrator membership from user's accounts. By changing file permissions on the files requiring access by the application on users' pcs, I was able to get both applications functioning correctly whilst the pc was logged in under a more restricted user account.

5. Admin passwords the same all over.

As I mentioned earlier, my organisation had grown very quickly from a small company. As a result, a great deal of administrator passwords shared the same password. This had also been the same password since the company started. Obviously it was unreasonable and hypocritical of us to enforce a password policy on users without this applying to IT never mind the security implications.

Firstly I audited all pieces of equipment with administrator accounts. I was able to gather servers, switches, printers / print servers and photocopiers. Again I arranged a meeting of the IT department, both Systems Administrators and Developers to discuss our Password Policy.

We agreed that no different piece of equipment or system should share the same password. We had drawn up a several complex passwords for differing devices. We also included in our IT password policy the need for review every 6 months. We had decided on 6 months as we felt that this would suit our needs best. Personally I would have chosen 3 months but we needed to achieve the right balance between security and manpower requirements.

An added bonus I found when carrying this out, was that there had been several devices such as one switch, a couple of print servers and all our photocopiers with blank admin passwords. I was able to set this according to our new policy and agreed passwords. Additionally whilst doing the audit I identified a number of firmware updates, particularly with our switches, and these were upgraded accordingly.

We had identified the need for a password review but as this was giving us the benefit of a firmware review, our security policies were not only having the effect of tightening security, it was also helping our infrastructure run more smoothly and efficiently. This in-turn was helping me justify further security recommendations and improvements.

6. IT staff using Domain Administrator Account

As part of my security focus, I had identified that all members of IT were using the domain administrator account. Additionally all members of IT were members of Domain Administrators. I had already consulted my team members over the creation of IT's password policy and I was going to amend it to take into account the Domain Administrator Account and membership.

My first course of action was, during an IT meeting, to show my colleagues the simple procedure of being able to 'run as' Administrators. I suggested we try a pilot trial of a month with myself and one of our developers trying to work with a more restricted user account. We still retained the administrator password for whenever we needed the administrator privileges as we were both no longer members of Domain Admins.

After a month we extended the trial to the whole team. It has now moved to becoming standard practise and has been written into the security policy. An added benefit is that auditing can show exactly who has been changing or accessing Active Directory. Except I discovered that auditing was not utilised much!

Auditing had been cut back somewhat from the standard default settings during a somewhat frenzied Kerberos troubleshooting session. Much of the auditing information had been removed and not switched back on. This was a big area for concern which lead me to my next task.

7. No security auditing on servers.

I become somewhat aggressive with regard to security auditing. Going through each of our servers one by one, I implemented full auditing on everything. As my organisation held highly confidential information, I had decided to implement object access on every document and folder, whether a success or a failure. I also heavily increased the size of all event logs. This would make further problem-diagnosing problematic, having to shift through more information, but really this was more of an inconvenience given the protection that the IT department and the company would receive in return for increased auditing.

Now I had created a policy for auditing we, as a department, decided that all event logs from all servers be backed up and archived every month.

8. Spyware, Malware and Virus defences.

My organisation already had a virus defence program. This consisted on McAfee VirusScan 4.51 on user's desktops. I had no trouble gaining funding for a new virus defence system and policy. I was able to get a new version of VirusScan, version 7.10 Enterprise with the addition of McAfee Protection Pilot. This version had been updated to include Worms, Viruses, Spyware, Trojans and all sorts of malicious software. Protection Pilot enabled me to set up a dedicated console which could give me an entire snapshot of the network. I could see the state of Virus Scan on every single computer, when a pc had last updated its definitions, when a full scan was last run, how many infections were found etc. It was a really useful piece of technology.

Our organisation already used MessageLabs (www.messagelabs.com) for email filtering. All our viruses must therefore becoming via the internet or via media bought into the building. I enabled on-access scanning in VirusScan which would scan every file as soon as it was accessed, or saved. Secondly I also scheduled full system scans at 8.00am, 12.45pm and at 6.00pm. Some other excellent features of Protection Pilot combined with Virus Scan 7.1 was that I was able to specify how much processor capacity was to be used on each scan, I could schedule scans or updates on client workstations at any time and change client workstation settings. Again I had introduced another security system with additional support overhead savings.

I was also able to run reports on the state of the company's Windows network and get a graphical picture of our Anti-Virus defence almost instantly.

As another layer of Mal-Ware defence, I installed Spybot Search and Destroy and BHO Demon onto clients PCs. Besides viruses, Spyware and Malware was getting to be a real problem.

9. Patching Procedure.

Although great emphasis was based upon patching, it was occasionally missed due to absences or holidays. Client workstations were set to automatically update, but the facility was removed on all our production servers. As a result it was agreed that each member or IT would take turns to do a short weekend shift performing server patching. Cover was always arranged and now servers are upgraded every week.

There are still instances where Microsoft releases critical updates very quickly. As part of the Systems Administrators responsibilities, they now have to check every morning. If it is found that a critical update is urgently required then a company wide email and Net Send message is sent out to every user advising that essential maintenance is required and that everyone has to log out over a certain period at lunchtimes. This had management approval and was now included into the security policy.

10. Regular Security Reviews.

Finally the last of my ten tasks was to instigate a weekly Monday morning Security review consisting of at least one Systems Administrator, one developer and the IT director. For this we would go through a summary of event logs, RAS logs and our ISA and IIS logs. Secondly we would discuss current security and identify areas where we could improve security. This is now a regular and very beneficial occurrence. Each week security is always on our agenda and is always being

addressed and improved. This will always be an on-going process but it is now part of our weekly tasks and thoroughly integrated into the IT department. Occasionally we also have our CEO sit in with us which helps greatly specifically from a non-technical perspective.

After

Since undertaking my SANS course, I was able to identify threats and their associated risks to my organisation's IT infrastructure. Not only was I able to identify these threats, I was also able to clearly demonstrate the threats by exploiting them. I was successfully able to present these threats to my management team and was given full backing and support to address the threats.

Whilst I am confident that I have enhanced the security procedures and, indeed, established a good, workable security policy for my company, I am well aware that this is an on-going process. Security must always be reviewed and adapted. Our company's policy is now a very accessible and dynamic document, receiving frequent updates yet always available on our company's intranet and is now included in the staff handbook too. By successfully raising the profile of security within the company, each member of staff is more vigilant and aware.

I have done my best to tighten security by addressing the 10 greatest risks I had identified to my company. Since doing so I have identified another 10 risks which I am in the process of addressing. I imagine that after I've finished doing that I will find another 10. I also have the benefit of my IT team mates, as well as work colleagues, working hard with me on security now – before security came after functionality (if at all) – now it is at the forefront of everything the IT department does at our company. To the rest of the company, it is something we all play a part in.

Appendices 1 - Security Questionnaire to Company Employees

Here is a copy of my short questionnaire initially sent out to all members of staff to raise the profile of security and to gauge their knowledge of IT security.

1. Who do you think is responsible for our Company's IT Security?

a) Department Managers
b) IT Department
c) Individual Users
d) A,B and C

2. How many of the following IT terms do you know and understand - Firewalls, Viruses, Key Loggers, Worms?

a) One
b) Two
c) Three or more
d) None.

3. What do you think makes a good basis for choosing a new password?

a) Your car's license plate number
b) Relative or Pet's name
c) A phrase consisting of several words, symbols and digits
d) Your last password with a new number on the end

4. Which statements do you agree with?

a) It is acceptable to give your password to your secretary or line manager
b) It is acceptable to give your password to your work colleague
c) It is acceptable to give your password to your IT department.
d) I would not give my password out to anyone.

5. Any other comments?

Appendices 2 – References

reference 1. Microsoft's Immutable Laws of Security URL :
http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx

Reference: 2. Thurrot, Paul,
"Microsoft Hack Attack Raises Serious Questions" October 31, 2000 URL :
http://www.winnetmag.com/Article/ArticleID/16025/16025.html

Reference: 3. Zbar, Jezz "Lessons in Laptop Security" march 26, 2001
http://security.itworld.com/4337/NWW010326zbar/page_1.html

Appendices 3 – Software Used

Windows XP, 2000 Server, 2003 Server, Windows 95, 98 & ME
www.microsoft.com

CITRIX
www.citrix.com

Zone Alarm
www.zonelabs.com

Spybot Search and Destroy
www.spybot.info

Nortons Internet Security
www.symantec.com

L0phtcrack
www.atstake.com

BHO Demon
www.definitivesolutions.com

McAfee VirusScan, Pilot Protection
www.nai.com

Last Updated: September 21st, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event