Breaking it Down: Network and Database Security

By Paul Volk

Completed for: Tekdesk
Course Supervisor: Sharon Beaucage-Johnson
Course Code: FRSC 4890Y
Term: Fall-Winter 2011-2012
Trent Centre for Community-Based Education

Project ID: 4218

Call Number:

Acknowledgements

I would like to thank Sharon Beaucage-Johnson of the Trent University Forensics department and Marjorie McDonald of the Trent Centre for Community-Based Education for providing this amazing opportunity to research a project that reflects my own interests.

I would also like to thank Adrianne Schutt and Tekdesk as a whole for allowing me every opportunity to dive deeper into the aspects of this research topic in both the conversations we had and the interests that we share.

Keywords

Cloud computing: using a network of host computers to store data over the internet rather than storing the information on the work site.

Cracker: someone who gains unauthorized access to computers or networks for personal gain.

Encryption: the act of converting plain text that can be read by the average person into code unreadable to anyone but the parties who possess the encryption key to decode the code.

Exploit: a piece of software or set of commands which are used to take advantage of an error or a bug in a program or computer system.

Fuzzing: the technique of testing a piece of software by bombarding it with large amounts of random data in hopes of uncovering an error or bug.

Hacker: a very skilful computer programmer or user who gains unauthorized access to computer systems and data.

Hash: data that has been converted into a character string that is unique to that set of data.

Local Area Network (LAN): a small network usually used for computers that are in close proximity to each other such as in an office setting.

Man-in-the-Middle: a type of attack where the attackers computer sits in between the two communicating parties (plays both the host and the client) so that all sent or received information goes through their computer first.

Penetration Testing or Pentesting: the act of checking how secure a computer system is by simulating an attack by a hacker or cracker.

Rainbow Table: a table of pre-computed hashes that are used to convert a password hash back into plaintext form.

Sniffing: the act of monitoring the data sent and received between computer systems.

Social Engineering: the act of manipulating people into divulging information that is sensitive or which can be used in later social engineering attempts to gain sensitive information (i.e. To get bank numbers, passwords or answers to security questions)

SQL Injection: the injection of foreign code, usually via an exploit, into an SQL database in order to gain access to the information it contains

Secure Sockets Layer (SSL): Secure Sockets Layer is the most common method of encryption used on websites that transfer sensitive information, such as email or banking sites.

Virtual Private Network (VPN): Creates a Virtual Private Network to communicating over an encrypted channel or gateway between the two parties mimicking a local area network.

Traceroute: a software tool to trace a packet of data sent from a computer around a network. Traceroutes can be used to map out network structure and useful entities connected to the network such as printers, servers, or routers.

Abstract

Working with the help of Tekdesk in Peterborough Ontario, the purpose of this project was to explore the different threats and security concerns of small businesses and non-profits. The research was done via an analysis of literature on various security concerns pertaining directly to networks and databases. A security audit was also performed on a small, local non-profit organization to compare a real world case to the literature and see how well a small organization stacked up to what was suggested in the literature. A guide was created which outlines what the literature suggests along with additional information and suggestions derived from the security audit on the small, local non-profit organization.

Table of Contents

Introduction

Purpose

Tekdesk is a non-profit IT company whose goal is to provide support and solutions in a broad range of technological fields to other non-profit and small organizations. To aid in this goal, Tekdesk has been equipped with a workspace and computer lab in the basement of the Peterborough Public Library. These resources enable Tekdesk to research and develop solutions for common problems that are encountered with the use of technology in any business or personal setting. Once developed, the resources can be utilized in effective knowledge transfer, whether it is through small classes, boardroom presentations or distance education online.

This is Tekdesk's third venture with a community-based research student and also a third time with a forensics student. The two previous students have helped by developing literature reviews and legal paper analysis for the Trillium Foundation funded Internet Safety project. The Internet Safety project strives to provide education on the dangers of the Internet. This curriculum provides education to users about the technology they come into contact with every day. The end goal of the project is to provide education and improve user awareness of technology safety practices. User awareness is arguably one of the greatest security concerns with the use of any technology. In this phase of development, Tekdesk expressed interest in the future applications and offerings of the project. A need has been identified in smaller organizations and businesses that don't have the resources or personnel to investigate, implement, and test new hardware, software solutions as well as the ability to educate users of their respected client base.

Solutions to this need will be explored in three distinct parts. The first part is a literature review from various authorities on computer security to gain an understanding of current requirements and checks that are common practice in organizations which use various technologies. The second part is an internal security audit of a small, local non-profit organization. The organization selected for the audit is a model organization for Tekdesk's target market. The organization has a small staff, no designated IT personal, and an aging technology infrastructure. The audit, completed with industry employed tools, can be transformed by Tekdesk into a future service offering in addition to the user education portion of the Internet Safety project. The last part is the development of a manual/factsheet, compiled from research in the first part and the experiences from the second part. This guide will be something that can be supplied to those smaller organizations as a starting point to help them effectively and securely implement new and existing technological solutions.

Relevant Forensic Issues

In the current business climate, computers are slowly becoming increasingly used for operational tasks, whether that is communication through email, donations to a charity on a website, or tracking tasks and/or customers in a database. With this new reliance on technology come new legal risks. These risks have manifested in the recent news media. Underground and outlaw groups have taken advantage of unsecure computer systems to wreak havoc organizations and the people interacting with these organizations in a very public manner. As a result, there is an ever increasing need for organizations to understand their

relative risk level for these breaches and to better educate companies and users on the approach which these attackers take.

This understanding helps the organizations in a number of ways. First, they have a better grasp on how secure their stored data is with their currently implemented technology. Furthermore they can test and improve upon current setups and implementations. The testing helps organizations two fold. Firstly, the organization improves the security of their systems and the data that is stored on all of their systems. Secondly, the organization also becomes aware of how an attacker may potentially approach their systems in preparation for an attack. Armed with this knowledge, they will be able to mitigate damage and produce helpful evidence in the event that an attack is ever successful.

In the current IT security field there has been a shift toward needing an approach to stop attacks and breaches by assuming a breach already exists and mitigating damage as much as possible. It is often said in the field that it isn't a question of whether you are going to encounter a breach, but rather when and how badly that attack or breach will be. Educating the organizations on this fact is crucial.

Methodology

This research project was split into two distinct research components and a compiling of this research into a deliverable that can be used as a checklist or manual for small organizations with no IT personnel.

The first research step was examination of the literature on current and emerging technologies and their security implications. This was done through the use of Trent University's online journal databases, use of publications which Tekdesk subscribes to (such as SC Magazine and Hacker Quarterly), and the use of white papers that could be accessed on various websites that specialized in computer security (such as Symantec, Rapid7, and Sophos). Additional information and white papers were taken from media sources made available through conferences and online webinars (SC Webinars and presentations from SecTor). For a legal background specific attention was given to PIPEDIA legislation. This legislation gives specific guidelines, which organizations must follow when storing personal information on computer systems.

The second research part undertaken was the audit of a small, local non-profit organization. Within the security auditing industry there are a number of standard methodologies that are used. For this audit I opted to use a modified version of the penetration testing execution standard (PTES). (1) The PTES consists of seven steps:

i) Pre-engagement interaction

ii) Intelligence gathering

iii) Threat modeling

iv) Vulnerability analysis

v) Exploitation

vi) Post-exploitation

vii) Reporting

The modified version of the PTES used removed steps (v) and (vi). The reason for this was to accomplish tasks within allotted time restraints and to mitigate any risk of taking the computer systems down accidently. Steps (i) and (ii) where undertaken at the same time during the audit. A meeting with a senior staff member of the small, local non-profit organization was arranged to go over what the audit would entail and how it would go. Step (ii) was accomplished via a series of questions regarding his organization's computer security, and specific areas he wished be tested. The data was used to research various ways to exploit the system and which areas could be used the most effectively to take advantage of the systems, thereby accomplishing step (iii). This research was compiled into an overview of possible attack vectors that would be investigated. Step (iv) had a few different means of execution. The use of industry standard tools was utilized for vulnerability analysis of the current computer terminals and the network infrastructure. Rapid7's Nexpose vulnerability scanner and Tenable Security's Nessus vulnerability scanner were used for an automated investigation of the machine's vulnerabilities and possible exploits (2)(3). Nmap was used for quick information gathering on the computers and devices present on the network(4), and BackTrack 5 R2 (an open source Linux operating system) was used for information gathering on the network as well as testing security bypassing methods on the computer terminals themselves (5).

The scans were run three times through each program (Nmap first, Nexpose, and then Nessus) to get better accuracy in detecting possible vulnerabilities. These scans where all stored in a

database on the testing computer so that reports could be generated at a later time, when executing step (vii) of the PTES method. The scan results indicated vulnerabilities and possible exploits. Exploit databases and a high-level search of white papers were used to determine how to maximize exploitation of the identified vulnerabilities found on the computer systems. The sites utilized for these searches included Remote-Exploit, Exploit-DB by Offensive Security, and PacketStorm. This research was also transferred and stored along with the scan data for later compilation during step (vii) of the PTES method.

Vulnerability analysis of other areas was accomplished through interviewing various consultants who were responsible in part for different aspects of technology utilized at the small, local non-profit organization including but not limited to email, web sites, and mobile devices.

In the final step on the modified PTES method used for the audit, reports were generated from the programs utilize. These reports include a brief overview of each vulnerability, its relative risk level, whether there is a public exploit available to take advantage of it, and what computer(s) it effects on the network. In addition to this report, a translation and risk assessment based on extra research was provided to the senior staff memeber. A report on risk from information gained from the interviews with the consultants was also provided.

Consolidation into a factsheet was achieved by documenting the experience of using industry tools with the PTES method in a real world scenario, and combining it with a summary of the literature and current legislation. This allows the factsheet/manual to be both based in the literature and law, while also using knowledge obtained from a real world case.

Results

Onsite server vs. Cloud based services

With the increase of upkeep and maintenance costs of hardware and software, businesses are seeking out cost effective solutions to minimize network downtime. The problem surrounds the resources needed to keep these types of systems running. Hardware must be maintained, software needs to be up to date, and of course the system need to be installed properly to ensure it is working to its fullest potential. This is what is known as an onsite computer system. The computers, networks and the server are all contained in-house and onsite with this type of system (6). As a result, all network security issues are the responsibility of the organization. Installation of this type of system requires the skills of an IT specialist. This can cause a huge overhead cost that is scalable across how large the company is. The solution to these high cost issues is one that isn't new to the IT world.

The use of super computers in universities, especially in the computer sciences departments, are a huge asset to research and a must for computational math. However the cost of these units have caused schools to look for cheaper alternatives. One such alternative is a number of lesser powered computers connected by a network to split and process data (7). This was arguably an equal, if not a better, choice then buying a super computer because you can add and remove computing power as needed.

Cloud services are built on the idea of adding a number of smaller storage units in a network that can be used for storing data. Much like the advantages for a super computer, cloud services can also increase in space by just adding additional, smaller computers (8). Cloud services, most commonly called cloud storage, is considered to be virtually unlimited in nature

as you can just keep adding computers to increase the capacity. The remaining problems of staffing IT specialists to keep up on the maintenance needs are handled by these cloud services as they are maintained by the companies renting the cloud storage space. Cloud services boast the ability to decrease company costs by off-loading IT management onto them, and also allowing secure remote access to files anywhere there's an internet connection (9).

Long term viability

The longevity goal of any system that is implemented for a business is to last the longest time possible, without the need for upgrading. In a perfect world, a company would install a system and it would run from that time on and never need to be upgraded. However this is a dream that will probably never be realized. When examining the literature it is quite amazing how technology has grown by leaps and bound in the past couple years. Technological advancements seem to be happening at an exponential rate and show no sign of slowing anytime soon. For onsite servers and computer systems, this means that as there is an ever increasing demand for computing power and storage space. The server located onsite must be upgraded to keep up with the demand. This requires staff to perform the upgrade and will also cause downtime when upgrading and can cause information stored on the system to be inaccessible. Cloud services on the other hand claim to eliminate this down time with the ability to continually cycle through computer systems. One can illustrate this point as follows; there are five computers all shared and storing your company's data, and were installed one after the other in one year intervals. At year five the fifth computer would be brand new while the first would be five years old. At this point it would be easy to swap out this five year old

computer for a new one. When this swap is done, the cloud service providers argue that there is little to no downtime with your data and after the switch is complete your system has a better running efficiency with a new and updated machine (10). This can then theoretically be done to all the old and aging computers, switching them to new and updated systems on a regular basis. This, argue the cloud service providers, means that you always have systems that are capable of running the latest applications and storing your critical data (6, 9).

Password security protocols

Accessing a computer, or data stored on a computer, typically means inputting data so that the computer can verify your identify. The common tools used today for this identification are passwords in some form or another. With the use of passwords as a type of identification, some tips and suggestions from security experts around the world can help use make use of this simple tool. Because it is often just a simple login screen that stands between a potential attacker and the data, it is important to investigate what security professionals say are the best ways you can make that screen as secure as possible. The literature suggestions a combination and balance of a number of factors to ensure strong passwords. Of all the factors, length of the password is probably one of the most important things to pay attention to. As with any combination type password, the length plays an important role in how secure it is. The longer a password is the harder it is to break. The length also goes hand in hand with the character set that is used for the password. The larger the character set the harder it is to break the password. Most security professionals suggest that you use at least eight characters that have a combination of upper and lowercase letters, numbers, and symbols such as '!', '@', '$' etc. At a

minimum of 8 characters, using only upper and lower case letters there are 852 combinations. As you can imagine, adding a couple more characters or including symbols only increase the number of possible combinations a large amount (11, 12).

Another factor that will increase the security of passwords is the complexity of the password. The security rating of a password decreases when it contains words that can be found in a dictionary or that have some personal attachment to the user. Unfortunately, it can be hard to remember a password. It is tempting pick something that is easy to remember or has some kind of personal attachment like an address, birthdate, or phone number. The literature suggests that these types of passwords should be avoided at all costs. Instead it suggests picking something that is more random in nature, that will be hard to guess, and that doesn't contain any words that could be found in the dictionary. Based off of this suggestion, many companies opt for very long and randomized strings of characters as passwords with an understanding that these will be the most secure (12).

A balance of the above factors makes for the strongest passwords. Focusing too much on one factor can lead to a lesser security rating instead of a higher one.

Inevitably passwords are forgotten or need to be changed for one reason or another. When picking a new password the above considerations should be taken into account. It is suggested that you should also pick a password that is quite different from the previous password. Sometimes employees who are forced to change their passwords on a regular basis will just add a number, date or character to their existing password. This can make a secure password into a free pass for a potential attacker. Hand in hand with what you change your password to goes the frequency with which you change your password. The suggestion from the security

professionals is to change your password as often as you possibly can. The more often you completely change your password the more secure it is and the more secure your systems will be as a result (12, 13, 14).

Many organizations will have some sort of database or system that requires users to log on, apart from their workstations. These systems, if they require a password, will need to store the passwords of all the users to match them and grant authorizations. When storing passwords, extra precautions should be taken as an insecurely stored password table can be the difference between a major or minor data breach. With many high profile breaches in the news, the common theme for most is that the companies who have their password tables stolen have stored them, for the most part, in plain text. This means the passwords are stored in a format that can be read by a person, without any kind of encryption. Security professionals suggest changing these passwords into hashes which are strings of seemingly random characters calculated through a mathematical formula that aren't easily read by a person. It is worth mentioning that most hashes are only one way converted, meaning that once a string is converted, the resulting hash can't be converted back to decode the password. The way this works is that the password table will have a set of hashes in it. When the user enters a password it will be converted into a hash using the same formula as the one to create the password table. The hash resulting from the user's entry is then compared to the one in the table and if it matches they are granted access to the system (15).

Day to day access to information

Whenever a worker uses a computer they will always need access to some information. This may be as simple as just access to the internet or as complex as access to an internal database of customers or clients. The problem in security occurs when you are letting workers or other people have access to information on your systems that they don't need or shouldn't have. Take the example of a summer student or part-time intern, whose job it is to do research or a literature review for a newly proposed project. Depending on the specifics of the proposed project, it could be argued that these temporary workers wouldn't need access to your customer and client databases. The solution to this problem suggested by security professionals is to give various privileges to different users depending on how much access they need to your internal systems. These different privileged users not only help protect access to private data but can also stop threats that may take down or affect the stability and security of your systems. These threats include malware such as viruses, Trojans, and spyware, but also could include user downloaded programs that would allow the user to have access to the systems from a remote location other than the office (16). Likewise, there is also the suggestion to protect private things behind yet another user password login so that you can control access to this sensitive information. This adds another barrier between a potential attacker and your private data. The suggestions above are ones that are said to be gaining momentum in the corporate world because of the growing threat of corporate espionage. In the growing competitive climate it is common to hear about companies hiring people to get jobs with their competitors just to siphon off privileged information. Though this isn't as common with the smaller companies, security professionals are of the opinion that it is only a matter of time till it

reaches these companies too. These internal threats are among the most detrimental seeing as the private data is usually handed to these individuals through granted access in logins and other access to the data (17).

External protection

Though arguably not the largest threat against the integrity of your company, external threats aren't something that should be taken lightly when examining your company's security. With the recent rash of external breaches to many big companies and organizations such as Sony, RSA, HBGary, and NASA, there has been a real push among security professionals to secure systems from outside remote access. One of the first considerations that should be taken into account is who is setting up your system. A competent IT professional can setup a very secure system that is properly configured. Though someone you know may have the knowledge to setup a computer and offer to set your system up at a really low cost it isn't a good idea to have them setup the system that you will be storing private client and customer data on.

Once the system has been setup there are a few different programs that you can install to make the network even more secure. Two necessities that security professionals suggest are anti-virus protection and a firewall. Anti-virus protection will help to stop incoming threats that may make their way through your email of from employees who download or use removable media, such as USB sticks, on outside computers (18). A firewall protects your systems two-fold. It is responsible for monitoring and directing the traffic to and from the computer. Usually if you have a firewall installed a message will pop up when a program requires access to the Internet. Most times this message will tell you what the program is trying to access and/or where the

program is trying to access. This information can be really useful, especially if you happen to get a virus that masquerades as a legitimate program. You will be able to see that it wants to communicate with a location that isn't necessarily needed and you can block it. The second way a firewall works is by blocking traffic that wants to come into your computer and network. You can think of it as a gate keeper. With this in mind let's examine how a firewall works from the outside. The way a computer communicates with the outside world is through things called ports. These ports allow information to be passed to and from the computer to the outside world. These ports are like doorways. On a computer with no firewall some of these doorways are always open. The port that deals with delivering website content for example is almost always, if not always open to send and receive data. When an attacker comes to the door he can just walk right on through or say he is a webpage and get through the door. The other type of port on a computer without a firewall is one that is closed. A closed port won't let any traffic through unless the user says to or the information is of a specific type. One example is a port that is only designated for email. It will only let email through and is closed unless the user has set it up. When an attacker comes to this door they knock and the computer responds identifying the port along with the information it needs to be opened. This can be good in one respect because the computer doesn't just let the attacker walk in like with the open website port but the computer has also given out information that could be used by the attacker to fake the type of information so the computer will open up. A computer with a firewall installed will act a little differently. First off it closes all the ports unless the user specifically tells it to leave them open. When the attacker comes to the firewalled port and knocks, the computer says nothing. It gives out no information at all. It doesn't even acknowledge that the computer is

online. This tends to foil many attackers from getting in from the outside as they get no useful information back (19, 20).

The last factor to keep in mind that many companies overlook is physical access to computers or workstations. It isn't that far of a stretch for someone to come in off of the streets and pose as a worker or maintenance person to gain access to the computers to get information out of them. One common practice that security professionals and researchers have noticed is that people won't lock or logout of their computers when they go to the washroom or out to lunch. They figure, to save time when they come back they will just leave the computer fully logged in. The problem with this is that someone can come by and within seconds use your computer to do something bad, or use your privileges to get access to information that they wouldn't otherwise be able to get access to (21, 22).

Legal obligations of database managers

When a company is storing private data of clients or customers there are some legal obligations that they must follow as set out by the Canadian government. All of these requirements are listed in the Personal Information Protection and Electronic Documents Act (PIPEDA). Though the act covers a multitude of different aspects pertaining to keeping electronic documents, sections pertaining to cloud services and data breaches were the ones that were concentrated on in this particular study. It was found that PIPEDA requires that the documents and information that is kept in databases or computer systems by companies must be kept private unless there is some sort of legal request to relinquish the data as would be the case of a Canadian search warrant (23).

With regard to obligation on the part of the database administrators or parent company to inform people who may have had their information taken in a breach or hack there is no legal obligation set out in PIPEDA. These companies do not legally have to inform you if your data is stolen or if there has been a successful breach in their computer systems (23).

Email

Email is something which is one of the staple points and a go-to communication tool of the business world today. Because of the ease of use, it is being utilized by many attackers to gain a way into a company and has been successful in gaining critical information from very prestigious security companies such as RSA (24). Many threats such as viruses or spyware will hitch a ride on email and can cause critical information to be disclosed. Security professionals have suggested a number of different things to help mitigate these threats. One is to implement software that reads through and scans email for content or context that looks as though it may have questionable intentions. Along with that, many ant-virus programs also now integrate an email scanner that will scan different things in the emails such as attachments or pictures that are contained in the body. These two things will help to lessen the risk posed by email threats to a point where most common threats will be caught (25).

Workstations

Workstations are one of the most vulnerable pieces of any company's network because of the direct interaction with the user, though they are normally not the target in an attack because

they often don't store any private data. A lot of the above suggestions go along with the idea protecting workstations and what little data may be stored on them. Security measures such as password selection, anti-virus software, and user differentiated privileges can really help to mitigate any risks that may be encountered. There are a few other suggestions that security professionals make that are commonly overlooked. One such security hole is bootable devices. The way computers are designed they normally start up the operating system from the hard drive. Usually this is the operating system where you have your files behind a username and password and if you don't know those you can't get in. Most computers have an option to boot an operating system off of a device other than the hard drive. In this way a potential attacker with physical access to the computer would be able to boot up into an operating system containing tools that could be used to dump the data off of the hard drive or get the passwords for the various user accounts that are present on the system. It's suggested that you disable this feature on workstations, especially if you are keeping any private data directly on them because the password won't protect the data (26).

Website

With any company or business it is critically important to have a website that effectively sells or draws attention to the services and/or products which you offer. Though a website brings in all new business it also brings with it all new security threats. The first step towards keeping your website secure is to make sure that your website is hosted on a service that is reputable and one that has a good track record with security. Cheaper web hosting services often don't keep their software and/or hardware up to date and can be easy targets for attackers. Along with

this also goes the type of data that you are going to be storing on your website. Some companies will store their databases or private client data on the website so that it can be accessed easily by the workers from home. In that case you should know where it is your data is being stored location wise and what the hosting company's policy is on how they handle and are responsible for this data (27).

You need to pay attention to how the website is designed and keep the content management system up to date. Many websites now are made using a content management system because it is an easy and graphical way for people to update and change their websites. Some of the more popular choices used include Wordpress, Joomla, and Drupal. These are software components and like any other software component they need to be kept up to date. If you don't keep them updated, serious security holes may go unpatched and you could find your website under attack (28).

The last thing that many security professionals mention to pay attention to is search functions that use databases on your website. If these search functions or databases aren't correctly designed they can lead to security holes that an outside attacker or malicious user could take advantage of. One of the most common flaws found in the search functions and databases is known as an SQL injection flaw. Like the name implies, this type of flaw will allow an attacker to inject a command of their choice into the programming code which the database designer has written. Often times the commands that are injected are ones that tell the computer to dump the database content and email it. If manipulated correctly the attacker may even be able to display login information or even bypass login screens altogether (29, 30).

Discussion

Onsite server vs. Cloud based services

Cloud services seem like a good way to go for companies and organizations that don't have the money to afford a dedicated server but there are some potentially major problems with this type of computer services.

One benefit is that it can spread the strain out that your systems would have to deal with otherwise. Instead of having everyone access the data from one computer, they take it from a number of computers. This can be very beneficial if you have a large number of users or clients that are trying to access information from your system. This also helps prevent against a security concern known as a denial of service (DoS) attack. In a DoS attack, the attacker uses a number of compromised computers under their control, known as zombies, to over whelm the host with requests. Instead of having to overload a single host the attacker now must get enough zombies to overwhelm a number of computers and this can be hard to accomplish depending on how many computers are in the cloud (31).

Though these security benefits, along with the decreased cost are good, other security concerns plague these services. One of the most readily identifiable problems with cloud systems is that you don't actually know where your data exactly is, as in its physical location on a set of servers. You know that your data is housed on servers that are under the control of a company but you don't know on what exact servers. This can be a huge problem if a server in their server farm goes down. If this happens you now have to figure out what data from your company, if any, was located on that particular server and you have to replace it from the backup that you hopefully have (32).

This scattered data isn't just a problem if one of the servers goes down but what happens if you want to move your private data stored through these services to another provider. You have to locate all your data scattered throughout the servers, back it up and move it. This can be a daunting task in and of its self however the problems don't just stop there. You now want to make sure your data is purged from the system because you don't want to leave private client information laying around on the server long after you have gone. And finding all of it to delete can be hard to do when it is scattered over a number of different servers and computer systems (32).

Along with these concerns you also have to depend on a third party company to secure and make sure that your data is stored properly and that it is being looked after. This can be a complicated issue especially if something happens with a breach or the cloud service provider isn't following proper legal guidelines. Who now holds the responsibility for the legal ramifications (33)?

For these reasons it seems as though an onsite server, though costly, is the most secure choice. With an onsite server option, you are in charge of all the security put into it. You can make it more secure or less secure based on your needs and what you are storing on it. This way you cut out the middle man that is there when using a cloud based service.

Password security protocols

The suggestions in the literature make perfect sense security wise but shouldn't be overdone. There is a level at which the maximum security for a password can be reached, but there are some trade-offs that can make it more or less secure.

It is rightly stated that both length and character set can greatly increase the security of a password. The longer the password is and the more sets of different characters means that there are more possible combinations that an attacker must go through to break a password. For this reason it is suggested that users set passwords that are fairly long and that include upper and lowercase letters, numbers, and symbols.

Complexity of the passwords can also play a large part in the security. Passwords that contain dictionary words should be avoided as it is very common for attackers to use dictionary based attacks to find the password. Personal identifiers in passwords should also be avoided at all costs. It is now fairly easy to modify or make dictionary files which contain personal information as passwords. There are a number of programs that are freely and legally available that will either ask you for information about the user which you are trying to attack (such as birthdate, pet's names, child's names etc.) or that you can point to a URL and it will scour and compile a dictionary file (34).

One problem found with the majority of the suggestions was that most made it seem like really long and random passwords were the most secure when this just isn't the case. This is even a common misconception among businesses and many laypeople. Though in theory these very long and randomized passwords seem to be more secure they are often very hard to remember. Because they are hard to remember, people will often write them down somewhere or store them on their computer in a location blatantly named something in relation to passwords. This defeats the purpose of the password if anyone who sits down at your desk can read the 24 random character password off the Post-It note under your keyboard.

The suggestion from the literature and security professionals to change your passwords on a frequent basis is a very good one. As suggested throughout, changing your password is a very good thing to do and will increase your security by multitudes. You can think of it from a few different aspects. Say the attacker is in the process of cracking your password. If you never change it then every moment passing is one moment closer to the time when the attacker will finally have your password but if you change it then the attacker would have to start the cracking process over again to fully test all the combinations. The second way to look at it is even in the worst case and your password is known by the attacker, the minute you change it, they are back to square one and need to crack it all over again. For these reasons it is of the utmost importance to change your passwords on a regular basis. And when changing them always pick a new one that hasn't been used before. Also make sure that separate passwords are used for separate things. Don't use the same password to login to your email, Facebook, and database because one of the first things an attacker tries once they have one password is to get into other accounts using the same password (35).

With the storage of passwords being a big gap that has allowed so many successful hacking attacks it is very surprising that there aren't better suggestions around the storage of passwords and user credentials. Much of the literature suggests storing passwords in encrypted or hashed form but this really only scratches the surface. It is true that hashes can only be converted one way (plaintext to hash) but with the prices of powerful computers falling and software being developed to take control of fast computing components such as the graphics card, it is surprising that single hashing is the suggested form of password storage. While single hashing (that is only creating a hash from plaintext) is much better than plaintext storage, a

password considered strong singly hashed could be cracked in as little as a day and would take a week or so at the most to run through all the possible combinations. A much better solution is multihashing. In multihashing you basically create a hash from the plaintext value, and then you create a second hash from the first one and so on. This can be done a multitude of times and each time you hash the value it becomes much more secure (36).

Day to day access to information

While the idea that giving out crippled user accounts will mitigate a lot of problems works in theory, when put into practice it has a tendency to fail miserably. Different levelled user accounts are one of the most used tools to stop people from wrecking computer systems. They are common place in schools, libraries, and anywhere else that lets you use a computer publicly. The thought is that is you aren't given privileges to install programs or modify settings then you can't mess the computer up. This assumption though is very wrong.

These settings may work for the people who don't know how to use a computer but even a mildly experienced person would be able to circumvent these restrictions. Take one of the most common restrictions placed on school computers, access to the command line terminal. Though the person may not be able to directly launch one from the start menu there are a number of ways that someone can get around this. One would be to create a small script that runs a command that is faulty. The program will open up a command line terminal try to execute the command, fail, and then sit there open and ready to use. From here the user can access critical system files on the hard drive that are normally out of reach and the user can even look at and kill any monitoring programs such as firewalls, anti-virus, or internet censoring

programs. It would also allow the user to access different parts of the network and dump private data from that computer or possibly from other locations on the network (37).

Likewise, the comments about it protecting from viruses and other malware is a bit off. Some very basic viruses and malware it may be able to protect from but many of the new and more advanced malware have built in functions to bypass this kind of thing in much the same way as a user can. This renders the computer as vulnerable as it was if the user account hadn't been locked down (37).

As illustrated, limiting user accounts doesn't really help stop attacks. The only thing it will really protect against is the user who doesn't really know their way around the computer. In that case and usually only that case, a limited user account would be something that could increase the security of your computer systems. For this reason, if there is information, such as a database of clients, that you wish to hide from a set of users, you are better off putting it behind another login screen.

External protection

External protection is of huge importance to any company. Protecting their data from outside attack is usually what is thought of when computer security is mentioned on any level. Suggestions to have programs like anti-virus are enormously important in keeping your computer systems safe from outside attacks. Not only do you need to have this kind of software but it also has to be installed, running, and up to date. A virus scanner that isn't up to date, while arguably better than no protection, can still lead to crippling security problems for your computer systems and network.

Along with anti-virus protection, a firewall is another must have in security software for any company. The internet traffic moderation which it does is an indispensable thing to have. It acts as a two way shield and will stop things going in and out of the internet that shouldn't be. It also allows you to see the traffic which you otherwise wouldn't have the ability to do. One of the best things about a firewall is that they tend to be very hard for attackers to get around, from both sides. This is best illustrated with the example of a computer who has a virus that is trying to transmit data back home to the attacker but it can't because the firewall is blocking it from talking to the outside world. For these reasons it tends to be one of the best pieces of software that you can invest in (19).

One of the only problems with these types of software is the messages that they cause to pop up. While the messages themselves aren't harmful, they can tend to be a bit complicated and technical in nature. Because of this, users often disregard them and click on whatever button gets rid of them. This can be a huge problem if you aren't dealing with the issue as it may be critical to the integrity of your stored data and the security of your computer systems. This is one of the reasons that education of the staff to report these types of popups should be done so that you can address problems in a timely manner. Depending on what software you opt for it may also be possible to set it to send an alert to someone when there is an issue so that if the person does just ignore it then there is a record of the problem and it can be addressed by someone who knows and can deal with it.

With regard to actual physical access to the terminals the only way to stop this threat is to train your staff to logout or lock their computers when they leave them unattended for any period of time. The magnitude of this threat again has a direct link with educating the user on what can

happen if they do leave their computers logged in while they leave to go photocopy something or while they go to the washroom (22, 21).

Legal obligations of database managers

PIPEDA is an interesting piece of legislation especially when it comes to using cloud based services. As stated earlier PIPEDA requires the administrators to follow Canadian law with regard to relinquishing private data of clients or customers. The problem comes about when the cloud service providers don't have their servers located in Canada. The servers and any information stored on them will be under the law of the land and this could breach Canadian privacy law. The perfect example of this is the US PATRIOT Act. If invoked, this piece of law allows the US government to seize anything that they deem to have connection to keeping the country safe without a warrant. This could include servers and computer that your private data may be stored on. If this happened, your company would be in breach of Canadian law and could be held criminally responsible. This is why it is critically important to know where your data is being stored and what legal obligations you have in storing that type of data. Smaller services that are used should also be taken into account. DropBox service for example bases all of its operations out of the Amazon E3 cloud computer networks which are located in the US. This means that if you store any private data through this service you would be in breach of obligations set forth by PIPEDA (23).

Email

With email there are a few problems that I have with the suggestions put forth by some security professionals. While I think it is good in theory to have software on your computer that reads through email and predicts whether it is of a good and legitimate intention I just feel this is another security concern. I would rather have no program reading or looking through my email because I really don't know what they program is reading, if it is storing anything, and what it is doing with any of the information gathered from this reading process. Furthermore these programs tend to be very hit or miss with their detection. Sometimes they get a little too carried away and will end up flagging emails that are genuine. Scanning of attachments makes a little more sense to me. Though the program may be looking at the file it isn't looking for context as to what is in the file, rather it is looking to see if there is any code that is present in the file and whether it is malicious in nature (25).

While having programs that will automatically identify threats that come through email are great, the biggest way to prevent problems with email is user education. Users should be educated not to click on attachments that look fishy, or links to sites they don't know or are from people they don't know and/or trust. This is the easiest and best way to prevent security problems that may arise from email. Teaching the users not to go into their junk mail folder and click on attachments from people they don't know on things that they don't know can save a lot of headaches and embarrassing network breaches as was the case with the RSA breach.

Workstations

Bootable media is usually one thing that both users and IT administrators usually overlook when they are thinking about security concerns to their systems. The reason for this is that they never really venture into the inner workings of the computers boot sequence and when they do they usually need to install a new version of software on the computer. The easiest way to stop this security concern is just to put a password for changing the bios settings instead of just disabling it. While disabling it will force the boot to go to the hard drive, it is possible to switch the order back by going into the bios and switching the boot order again. By putting a password on the bios, users who may be smart enough to try and use a USB stick to get the data off the hard drive won't be able to change the order of the boot so that their operating system on the USB stick is booted up before the one that is on the hard drive (26).

Websites

A reputable web hosting service can go a long way in the world of website administration. A company who is popular and up to par will usually have all of their things in order and be one that is less likely to encounter serious security or hardware/software problems. Another thing to keep in mind when choosing a web host is where the servers are located and what kind of data is being stored on the servers. Remember that if you are storing private data on the webspace it needs to be in line with the provisions of PIPEDA (23).

There is nothing wrong with using a simplified content management system (CMS) when creating a website and this is probably one of the best ways to go security wise. Unless you have access to a web designer who is very up to date with the latest security issues that plague

the internet it is better to use a CMS that you can update as new security patches come out. The key with it though is to keep it up to date. If you fail to keep the CMS patched and up to date you may be leaving your site open to vulnerabilities that could affect the integrity of your website and threaten the image of your company or organization (28).

Search features and databases on websites tend to be particularly dangerous. For this reason it is suggested that you try to avoid them unless they are a crucial part of your web presence. Many companies and organizations need these types of things on their website and there are a few things you can do to protect yourself from attacks such as the SQL injection attack. The first thing is get a database programmer who is experienced and has a proven track record of supplying good products. A good database designer and programmer will be able to mitigate potential security threats as much as possible. Also make sure that where ever you have user input that access a database (login pages or search boxes) make sure that the function is sanitizing the user input. The way an SQL injection works is that the user can put SQL commands into the program. A function that sanitizes the input won't allow input that is also an SQL command. This is probably the easiest and most effective way of stopping SQL injection attacks. If the attacker can't manipulate the database then they are forced to look for a different way in (29, 30).

References

1) http://www.pentest-standard.org/index.php/Main_Page
2) http://www.rapid7.com/products/nexpose-community-edition.jsp
3) http://www.tenable.com/products/nessus
4) http://nmap.org/
5) http://www.backtrack-linux.org/backtrack/backtrack-5-release/
6) Han Y. On the Clouds: A New Way of Computing. Information Technology & Libraries, 2010; 29(2): 87-92
7) Kondo D, Taufer M, Brooks CL. Casanova H, Chien AA. Characterizing and evaluating desktop grids: an empirical study. Parallel and Distributed Processing Symposium, 2004; 26(30): 26
8) Foster I, Zhao Y, Raicu, I, Lu S. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, 2008; 12(16): 1-10
9) http://www.sitepoint.com/what-cloud-computing-can-mean-for-your-business/
10) http://www.journeytothecloud.com/cloud-computing/cloud-life-cycle-management-now-that-i-have-it-how-do-i-patch-it/
11) Summers WC, Bosworth E. Password policy: the good, the bad, and the ugly. WISICT '04 Proceedings of the winter international synposium on Information and communication technologies, 2004.
12) Shay R, Bhargav-Spantzel A, Bertino E. Password policy simulation and analysis. DIM '07 Proceedings of the 2007 ACM workshop on Digital identity management, 2007.
13) Jobusch DL, Oldehoeft AE. A survey of password mechanisms: Weaknesses and potential improvements. Computers & Security, 1989; 8(7): 587-604
14) Gehringer EF. Choosing passwords: security and human factors. Technology and Society, 2002. (ISTAS'02). 2002 International Symposium, 2002: 369-373
15) http://www.pixel2life.com/publish/tutorials/118/understanding_md5_password_encryption/
16) Stiegler M, Karp AH, Yee KP, Close T. Polaris: virus-safe computing for Windows XP. Communications of the ACM - Privacy and security in highly dynamic systems, 2006; 49(9)
17) Chan M. Corporate Espionage and Workplace Trust/Distrust. Journal of Business Ethics, 2003; 42(1): 45-58
18) http://openaccess.city.ac.uk/524/2/ISSRE11_AV_Diversity.pdf
19) http://www.leetupload.com/database/Misc/Papers/Asta%20la%20Vista/Firewall-Evolution-deep-packet-inspection.pdf
20) http://revistaie.ase.ro/content/44/25%20dodescu.pdf
21) http://www.wright.edu/rsp/Security/V1comput/Social.htm

22) http://www.sans.org/reading_room/whitepapers/engineering/threat-social-engineering-defense_1232
23) Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) http://laws-lois.justice.gc.ca/eng/acts/P-8.6/
24) http://www.rsa.com/node.aspx?id=3872
25) Heron, S. Technologies for spam detection. Network Security, 2009; 1: 11-15
26) Casini M, Prattichizzo D, Vicino A. Operating Remote Laboratories Through a Bootable Device. Industrial Electronics, IEEE Transactions 2007; 54(6): 3134-3140
27) http://www.ra.ethz.ch/CDstore/www2005/docs/p480.pdf
28) http://jstahl.org/archives/2007/02/18/open-source-cms-security-part-ii/
29) http://www1.cs.columbia.edu/~locasto/projects/candidacy/papers/boyd2004sqlrand.pdf
30) http://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf
31) http://www.infoworld.com/d/cloud-computing/can-cloud-computing-save-you-ddos-attacks-306
32) http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf
33) http://www.whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/
34) http://www.darknet.org.uk/2006/11/wyd-automated-password-profiling-tool/
35) http://www.symantec.com/connect/articles/ten-windows-password-myths
36) http://static.usenix.org/events/sec05/tech/full_papers/ross/ross_html/
37) Provos N, Friedl M, Honeyman P. Preventing privilege escalation. SSYM'03 Proceedings of the 12th conference on USENIX Security Symposium