

Canaudit Perspective

September 2005
Volume 6, Issue 9

Topics of Interest:

- Capturing “THE DEAL” Information
- Web Mail Systems can be Compromised
- Securing the Virtual Private Network is a must
- Remote Desktop Access can result in Security Breaches
- Network Segmentation is a must
- Who is looking over your shoulder?
- Let’s not forget Wireless Networks
- Surveillance Devices need to be Identified and Neutralized
- Dumpster Diving & Social Engineering still works
- Network Security is a must

Mergers and Acquisitions: The Need for Enhanced IT Security



Gordon Smith

Everyone is aware of the legal requirements for public companies to restrict knowledge of a pending merger or acquisition. In this article, I want to focus on the information security requirements, from the first hint of a deal up to the actual marrying of the two organizations. The issues identified in this article are based on the network security and penetration results of Canaudit’s recent audits. All but two networks failed our tests this year. It appears that American organizations have not successfully protected their information assets and that confidential communications are not confidential. To ensure that a corporate combination is successful, the initial communications and subsequent discussions must be private. The Internet, mail and networks, as well as the servers and workstations within the network must be secure from those seeking to gain financial advantage before the merger and from disgruntled employees and contractors after the merger.

Capturing “THE DEAL” Information

There are many ways that a person can gain access (from an IT perspective) to information of a pending deal. The greatest weakness in corporate communication is email and web mail. Emails are often sent unencrypted through the Internet. With the right tools and techniques, it may be possible to intercept emails. The most effective control is to encrypt the email using an encryption product such as PGP. PGP interfaces with Microsoft Outlook and Exchange, making it a simple matter to encrypt any outbound email. It is also possible to encrypt email transmissions using other techniques such as creating an encrypted communication path using Secure Socket Layer.

Before reading an email, it must be decrypted. Again, this is a simple click-of-a-button process. A common flaw with encrypted email is failing to properly secure the decrypted version. Email is often decrypted then saved in an unencrypted file. My solution for this is to use an encrypted file system. Confidential information can be stored in this protected section of a hard drive, with access only by individuals who are authorized to view or modify the data and who use security token or biometrics (finger print or iris scan) to confirm that they are who they claim to be.

Web Mail Systems can be Compromised

Web mail also poses a significant threat. Many of our clients use web mail but do not properly protect it. When the user wants to log in from home or a hotel room, they log in to the network using their normal account and password, which can be easily compromised. On our audits, we use special tools to identify the poorly secured Windows machines within the network. In some cases, only one or two poorly secured machines will give us the information we need to gain control of the Windows domain or Active Directory. With this access, it is a simple matter to download

and crack everyone's password. Once the password cracking is complete, a "spy" can simply log into the web mail application using the CFO's account and password. Now they can view his or her email as easily as the CFO can. They can even send messages from the CFO to virtually anyone, anywhere. These appear to be authentic messages as the messages are actually sent from the corporate email application.

Securing the Virtual Private Network is a must

Some of our clients use a Virtual Private Network (VPN) to create a secure remote connection to the internal network. While this may seem acceptable, this is not necessarily a truly secure connection, as many VPN web mail applications use a software client on the user's machine. This software is freely available and can usually be downloaded from the software provider's web site. The use of a simple account name or password as the primary means of authentication will permit anyone who gains access to the password files as mentioned above, to gain access to the VPN. The control we suggest is to use two-factor authentication; the use of a security token, a certificate of authentication or biometrics, in addition to the account and password. With this technology, it will be very difficult indeed for an intruder to successfully masquerade as a valid user.

Remote Desktop Access can Result in Security Breaches

Another way to glean information is to use existing poorly secured software to gain access. Virtual Network Computing (referred to as VNC) is often used by help desk staff and administrators to provide remote support to clients. Most implementations of this product rely on a simple password. Software tools such as NBTEnum enable the capture of the encrypted VNC password. The encryption algorithm is very weak, enabling the encrypted password to be cracked in seconds. Windows Terminal Services can also be used for remote support. In most implementations any domain administrator or attacker who gains domain administrator rights can view desktops running Windows Terminal Services. As long as your machine is powered on, VNC and Windows Terminal Services can be used to gain access to your machine or view your files. "Locking" the computer only stops a passerby from sitting down at your workstation. It does not stop a skilled hacker who gains domain access from compromising a machine that is powered on.

In my opinion, poorly secured VNC should be eradicated from the network. To reduce the damage that can be done from an attacker, we strongly suggest that the executive network be segmented from the corporate network (using a firewall, router or switch that is properly filtered). We also suggest executives have their own Windows domain or Active Directory container that is administered by one or two trusted and bonded administrators. The executive PCs should have encrypted hard drives or segments of the hard drive should be encrypted so that sensitive information can be stored in a protected manner. If information needs to be viewed by various executives, then an encrypted shared drive should be set up and access granted on a proven need-to-know basis. All machines that access the shared drive should be within the segmented executive network or using a VPN with two-factor authentication to connect to the shared drive.

Network Segmentation is a must

One of the questions that often arise in conjunction with a separate executive network is "Who should use the executive network?" There are two answers to this question. The first is for normal business operations, excluding mergers and acquisitions. I believe that the first group to be included should be the executives and their assistants. I also believe that the legal, internal audit and some of the HR staff who have access to sensitive information should be included in the segmented executive network. The employees and contractors working in these areas have access to very sensitive information. Lawyers have access to confidential documents that are subject to client-attorney privilege. Auditors have documentation that identifies security flaws in the control structures, as well as documentation on the business applications themselves. These areas need separate encrypted shared drives within the Executive VPN.

The second answer to the question relates to the Mergers and Acquisition staff and consultants themselves. We believe that these people should have their own highly protected and secured network segment. Again, their email should be encrypted and they should have a separate encrypted shared drive. This group should be on their own VPN. To deter the chance of information leakage, file transfers and emails between this VPN and the outside world should be monitored. Any unusual activity should be investigated.

Who is looking over your shoulder?

Another source of information leakage are blackberries (handheld devices used to send and receive email). Let's look first at the major security issue. Many of our clients have blackberry servers within their network. This by itself is not an issue. The security concern I have is from default accounts and passwords. On several occasions, we have identified an administrative account called bberry with a password of bberry. In most cases this gave us administrative access to the blackberry server. By downloading and cracking the password file off this server, we were then able to glean an account that gave us domain administrator rights. I also observed another blackberry issue on airplanes. It is surprising the number of people who read their emails while they are flying. They do not understand that there are prying eyes sitting beside and behind them. The same hold true for those who do email on their laptops or read briefs and other documents while flying or in Internet cafes, bars or restaurants. Oh, let's also not forget cell phone conversations in public places or prior to and after landing. Some people do not exercise common sense when using phones.

Let's not forget Wireless Networks

Home networks can also be a good source of unauthorized information. The first issue is with wireless networks. Many executives like to be able to use their laptop anywhere in the house. They set up a simple wireless network, often without technical support and hence without proper security. Since they are using a "secure VPN," they think they are fine. That may be true for communications between their laptop and the corporate network, but it is not true for communications between other PC's and peripherals on the household network. Often they transmit documents to the printer or transfer files through the network from the corporate laptop to their personal computer. If this is done using a wireless network, then a person with a wireless device and software may be able to pick up their transmissions. One of my senior staff members was once able to pick up a wireless signal more than a mile away using a special antenna.

Surveillance Devices need to be Identified and Neutralized

Our clients are often surprised at the beginning of our audits when we perform a "bug" sweep of the room our team will use. Most organizations do not perform regular bug sweeps of the executive and the M&A team's facilities. A competitor or even a suitor sure would love to glean information about the deal and any potential roadblocks facing them, as well as determine who is on board and who is not. Often in M&A meetings, tempers flair and people get excited. What better for a potential buyer or seller to know than what hot buttons exist and who they have to entice to win the deal? Conversely, a competitor will learn how to best squelch a deal if they gain access to this type of information.

Another similar concern is the widespread use of video conferencing. We are used to seeing this equipment in most conference rooms. Often the microphones and cameras can be activated remotely from another site. If you are using a conference room with video conferencing facilities, ensure that the machines are unplugged from the electrical outlets. This is a simple yet very prudent precaution. Something less obvious is a team member who has his or her laptop on in the conference room. They could be transmitting the meeting to the competitor or simply just recording on the presentation for later use or sale using readily available software. For this reason, we suggest that the people in the room not be permitted to use the Internet. All laptops and devices in the meeting room and those used in the M&A process should have monitoring software installed on them (without the user's knowledge). If anyone is tempted to sell information or accept a bribe, then your security folks should be able to detect them early in the game.

Dumpster Diving and Social Engineering still works

Let's not forget the paper records. "Dumpster diving" has been updated to the 21st century. One trick is to rent a truck and show up in the uniform of your document destruction or shredding firm. These people can then load your sensitive documents into the truck and drive away with them. Even if you have a shredder, it is now possible for most shredded documents to be recovered. The FBI perfected these techniques years ago and use document recovery procedures in some of their corporate forensics investigations. If they can do it, so can "consultants" hired by your competitor.

Let's not forget the couriers such as UPS, FEDEX and DHL. What procedures are in place to ensure that the person who picks up your confidential packages is really from the courier? Is it possible that it is an imposter who has the right uniform? Most people give packages to couriers without any thought. You might want to drive particularly confidential documents to a drop-off center or street drop-box yourself. Make sure that you vary the time and the drop location every day to avoid someone monitoring your habits.

Network Security is a must

The last major area I would like to cover is network security. Based on the results of our audits, most corporate networks are not secure. At the earliest indication that a deal is in the works, a full network penetration test or vulnerability assessment should be performed to identify security issues. Using our philosophy, a specially trained team, such as the Canaudit Security Squadron, should rigorously, yet safely, test the corporate Internet presence, dial-in and other external connections, as well as the internal network. They should also test for wireless both at company locations and near the homes of corporate executives and merger team members. Needless to say, vulnerabilities will be discovered. These vulnerabilities should be corrected and then the network should be retested. To ensure that the network remains secure, regular network security procedures should be implemented to scour the network looking for vulnerabilities.

Once "the deal" is announced, some of your employees may be concerned about their future with the company. Network, database and server administrators are known for putting backdoors onto their systems. They are worried that someone will inadvertently change the environment or disable their account. Should this happen, they use a back door or trust relationship from another machine to gain access. If any of these people will be leaving the company, then additional security measures are required. The backdoors and trust relationships will have to be identified and removed. Strong change management will need to be in place to ensure that unauthorized modifications are not placed on the systems or in the databases. People may be physically removed from the premises, but they may still be able to remotely access the network for malicious purposes after they are terminated.

Normal users can also do a lot of damage to company records or simply take copies of confidential formulae, customer or vendor records, or simply insert erroneous data into the applications. Clearly a strong IT security function is required. They will need to be constantly reviewing the systems to ensure that they remain secure, applications to ensure that data is not needlessly altered or deleted, and network traffic to ensure that copies of company records are not transmitted through the firewall to a home PC or a competitor.

Conclusion

I have just scratched the surface in this article. People can be very ingenious when there is money to be made or their jobs are at stake. IT security is a critical part of any merger or acquisition. It will require funding and possibly some additional staff or contractors. Keeping the pending deal private until it is publicly announced is essential. The risks of premature disclosure to one or two people are serious enough as premature public disclosure can have serious legal and financial ramifications.

The comments in this article are mine and mine alone. Nothing makes an author happier than to receive comments from the reader. Positive comments stroke our egos and negative comments serve to make us better. Please email any comments you may have to Gordon@canaudit.com.

Gordon Smith
President, CEO