

The Cnaudit Perspective

September 2004
Volume 5, Issue 7

Simplicity is the key to defeating corporate security

Written by: Gordon E. Smith - President, CEO



In this article, I'm going to take another look at the threats facing our networks. To date, cyber terrorism, while a significant risk, has not occurred on a broad basis. Thank goodness for that as many corporate networks are not prepared for a serious cyber event. We are getting better. External connections, such as modems are better controlled. Firewalls are more effective today than they were several years ago. Even wireless networks, which just last year were very poorly secured, are much stronger. My premise in writing this editorial is that improved controls can actually lead to poor security. While this may not seem possible at first glance, by emphasizing one form of security and or relying on specific security controls, we are susceptible to measures that bypass those controls.

By securing some assets, we expose other assets

As water always tries to find its way to the lowest area, it will climb hills by forming ponds and lakes on its journey to the ocean. Cyber criminals and terrorists will also seek out methods that may not seem efficient to attack the least protected assets, even if they have to build detours around your controls to achieve their objective. As organizations make their external network boundaries stronger, they often ignore the internal network. I frequently hear that corporations have hardened the outside of the network; therefore the risk to vital IT assets is mitigated. This is overly simplistic. Once controls are strengthened in one area, the threat dynamics change. Building a control in one place may expose a machine in another place. Let's review several examples from our recent audits.

Implementing security controls can create additional exposures

Physical security remains weak in most American companies. Yes, they have increased the number of guards. They may have security cameras and other devices, yet with all of these additional controls, our social engineering still works. We succeeded in every physical security test we attempted this year. In one case, we simply waved to the guards and drove in with other employees. In several other cases we used fake IDs to get past the security guards. We made our security cards from hotel room cards, imprinting our pictures and the target organization's logo carefully onto the face of the card. By claiming to be from a small remote location and using our real names, we defeated sophisticated security systems. If we can do this, then the disgruntled employee or terrorist can do it!

In several recent classes, we had fake badges made and couriered to our location overnight to demonstrate just how easy it is to defeat card entry systems. In one case, when I could not get through the person trap, I waved my fake badge at the guard. He let me through as there was a long line behind me (as there always is when employees are entering the building at the start of the day). Cards sometimes fail and the guards are in the habit of buzzing people through. In one case, I was stopped and had to show my drivers license. Since the fake badge had my real name on it, my official ID agreed with it. Yes, I had to show government picture ID, but I still got in. Once in, it is a simple matter to find a conference room, plug into the network, start a sniffer and glean the community strings and other data needed to compromise the network. Some organizations feel they are safe because they are using intrusion detection software to detect foreign devices. We defeat this in most cases by walking up to a printer, pressing menu, and printing out the configuration data. Then we unplug the printer from the network, change our IP and MAC addresses to that of the printer and we are in. By keeping a low profile, we glean additional information needed to get onto the domain controllers and servers.

Network incidents are often inside jobs

Recently I read an article that mentioned what most of us already know. Most network incidents occur from the inside. That spurred me into thinking about the changes in Corporate America. In the good old days, employees did most of the technical work in information technology. These employees performed the database administration, network management, operations, security, help desk and development. To lower costs, many organizations started outsourcing. (My opinions on outsourcing are very well known – see IT Outsourcing, Placing our Nation at Risk http://www.canaudit.com/Perspectives/Volume4_Issue9.pdf). Now that organizations have outsourced critical IT functions, they have lost the ability to control their security. Third party firms, both national and international, are free to hire whomever they want to perform the work being outsourced. Yes, the staff may have to be technically competent. But, can we be sure that every single person hired by the outsourcer has been subjected to a detailed background check? Could a cyber criminal or terrorist be given the keys to the corporation because of poor hiring practices at the outsourcer? I say the answer is definitely - YES! While there may be a contractual obligation for an outsourcer to perform background checks etc, I have yet to see a client that audits this well. They rely on the contract rather than testing the controls.

To be fair, I can't just pick on outsourcers as we also have to look at contractors. Many organizations do not have procedures to ensure that contractors are properly vetted. Your HR department will normally do a good job of scrutinizing new employees, catching those with undesirable backgrounds before they are hired. Yet these same organizations will bring in consultants; give them access to the network, yet never do a background check on them. To be fair, some companies are now requesting background checks of contractors. But this is still the exception rather than the rule. I believe that the failure to properly vet the credentials of consultants needlessly exposes an organization to cyber crime and electronic fraud.

Now imagine that your company is going to outsource your job. If you have advance notice, what would you do? Float your resume? Seek another position within the company? Take early retirement? These are all options. But what happens to an underperformer whose skills are outdated and has work or home related stress? The bill collectors are at the door and the spouse is leaving and taking the children. This is the worst case scenario for a disgruntled employee. If someone offered this poor soul \$50,000 for a copy of your organization's proprietary client information, would they sell it? You betcha!

Companies must be ever vigilant to identify potential disgruntled employees. In addition, if outsourcing or staff reductions are necessary, then they must be kept secret until after security measures have been implemented to protect your information assets. We worked for clients on several occasions who wanted us to test their security prior to acquiring a new subsidiary, outsourcing or a major downsizing. This is prudent and cost effective. As the old adage goes "An ounce of prevention is worth a pound of cure".

New technologies create new exposures

While external security is improving, there are some new holes opening up. Let's look at web mail. Some corporations have implemented two factor authentication for external web mail connections. Meanwhile, many other organizations continue to rely on the old account and password, in clear text, to access web mail from a home computer, hotel business center or airline club machine. While this is convenient, it does open up a major hole. Many users prefer to synchronize their passwords. As a result, the web mail password may be the same as the internal domain password used by the employee when logging in at the office. If a cyber criminal could compromise the domain password file, then they would have access to some, many or in the worst case, all web mail users. This would enable them to see confidential information including self help passwords generated by internal systems such as PeopleSoft. Imagine a disgruntled employee who logs in as the Vice President of HR and sends an email to all employees. The message could be that it has been a good year and everyone is getting a 15% one time cash bonus. Another stunt would be to send a message to all employees on the Wednesday before Thanksgiving stating that the company has been bought out and all employees should report immediately to the auditorium to receive their final pay and termination documentation. These pranks can be very expensive to an organization, both in terms of lost productivity and poor security.

Another entry point is the home wireless network. Wireless devices can be purchased at Best Buy for less than \$50. Now we have to worry about the wireless household and the effect it has on our employee connectivity. Several vendors have created wireless print servers and other devices that make it easy to share devices within the home. Home devices usually do not have firewalls or updated anti-virus software. In addition, they may be infested with spyware or other nasty software. Encryption is normally not used and it is likely that the home machines are not up to vendor patch level.

These factors, when combined, make it easy for a cyber criminal to gain access to the home network. They may sit down the street in a van, connect to the wireless network, and use an exploit such as DCOM to gain access. Or, they may simply run a program such as CIS to find accounts without passwords or passwords equal to the account name. The bottom line is that executives with poorly secured home networks create additional risks, including disclosure of confidential information and potentially causing a corporate network breach through their personal home computers.

Improved Window server security forces the cyber criminal to try harder

In the last year, we have observed a noticeable improvement in Windows server security. That said, workstations and some of the less important servers may not be properly patched or secured. The cyber criminal will attack these less critical machines, harvest and crack the password file and then use the cracked passwords to gain access to the domain controller. Recently we had a client that moved to Active Directory. Unfortunately, they forgot to disable the domain controllers. We were able to harvest the password files from the domain controllers and use the cracked passwords to penetrate Active Directory.

Speaking of cracking passwords, we are very proud of our new Rainbow Crack dictionary. In the old days (last year) special characters imbedding within passwords made it very time consuming to crack passwords. It has taken many months to compile our dictionary, but we now have a crack ratio of 99.8 percent. This means that the time to crack almost any Windows LANMAN password is now measured in hours instead of days and weeks. We will reach the 100% mark in another month or two as our computers continue to calculate the permutations necessary to crack any Windows LANMAN password. For years, the audit and security professions have prompted users to select complex passwords. With Rainbow Crack, which is freely available on the Internet, organizations must get rid of the LANMAN password hash because it is susceptible to Rainbow Crack. This cannot be accomplished until all of an organization's old Windows NT, 98, 95 and ME machines are replaced with Windows 2000, XP or Server 2003. Another option, which I prefer, is to use two factor authentication or biometrics to log in. Two factor authentication uses a token (such as SecurID) in addition to the account and password. Biometrics are not only cheaper now than several years ago, but the false negatives have been greatly reduced. If you want to foil the cyber criminal, then it is time to move forward with stronger authentication techniques.

The mainframe is now an easy target

The bastion of control, the mainframe is likely to be attacked. There are several factors that created this situation. The first is that many of the people who actually understand Z/OS or OS/390 and RACF are now retired or outsourced. Secondly, the mainframe has not been on the audit radar. Many organizations have not performed a full technical review of the mainframe operating system in years. Our mainframe specialist at Canaudit is quite adept at gaining access to the machine, stealing OPERATIONS, SPECIAL or AUDIT access and then creating his own empowered account. If he can do it, you can bet that a disgruntled employee with the required skill set could do it as well. It is essential that your security specialists completely secure the Authorized Program environment. That includes protection for the libraries. Access should be strictly limited to several trusted staff members. Also, change controls must be in place to prevent someone from placing malicious code into a library.

Don't forget about the SVCs (supervisor calls). These can be used to by the cyber criminal or disgruntled employee to become authorized. While the number of SVC's has dwindled over time, most of our clients do not know what the existing SVC's do as they were installed by the vendor. This abdication of responsibility could result in a seriously compromised mainframe. We are also concerned about the number of people with sensitive privileges such as SPECIAL and OPERATIONS. These people can do whatever they want in the mainframe environment, bypassing controls in a flash. At some organizations, there are outsourcers or off shore consultants performing sensitive tasks using SPECIAL AND OPERATIONS. I believe this greatly increases the risk.

The proliferation of password synchronization (using PSYNC or another tool) also makes it easier to gain access to the mainframe. Once the passwords are cracked in the Windows environment, Brutus can be used to attack the mainframe on port 21 using the compromised accounts and passwords. When we do this during our security reviews we normally have over 50 accounts which we can use to gain access to the mainframe. Once we gain access, we usually escalate our capabilities to SPECIAL or OPERATIONS by exploiting holes in the security configuration. Remember that synchronizing passwords has a down side. Once one operating environment is penetrated, all other environments may be exposed.

The UNIX world also offers opportunities to breach security

In the UNIX and LINUX world there are many exploits which are available to the cyber criminal. Many HP-UX machines do not have shadow password files. As a result, anyone who gains access to the machine can easily harvest and crack the password files. Sun boxes are exposed to sadmin and integer overflow issues. The integer overflow in the SUN environment requires a two step approach to gain remote root access. We initially use the integer overflow exploit to log onto the sys account without a password. (Normally, one cannot log onto the sys account. That is what makes this exploit so dangerous). Once onto the machine as sys, the cyber criminal or terrorist could change the default profile (which the sys account can access) so that the root account can be logged into remotely. They then logoff and use the integer overflow to log on as root. The next step is to set up another root empowered account, then change default profile back to its original state so root cannot log in remotely. While the hacker is on the machine, they might as well harvest the password and shadow password files, then crack the passwords.

Watch out for the XEROX high speed printers. Some of these machines have an internal SUNSPARC machine and are susceptible to the integer overflow. Your network or security people may not even know this machine exists as they think of it as "only a printer." Once an "evil doer" gains access to this poorly secured printer, they can use it as a firebase to attack the network. They may also be able to change the data in the print queue. This is particularly sweet if your organization still prints checks.

UNIX boxes in general have a problem with world readable files. A cyber criminal, once onto a machine, could harvest the Oracle or DB2 database exports (also called backups) of your database. Once they have these, they can import them into a database instance they control. Your data is now their data. Periodically search for world readable files, then analyze and secure them. Also disable the finger service to make it more difficult for an attacker to enumerate valid accounts on the target machine.

The last item I would like to address is the use of waivers (also called exceptions or exclusions). These are often granted when a machine or application cannot conform to an organizations policies or practices. A waiver is granted by management to except these machines or applications from the policies. These waivers are normally intended to be temporary, yet experience shows that they may be in place for years. Remember what a waiver or exclusion means. **Your system cannot meet your own security standard. This makes the machine a perfect target to the cyber criminal!**

Everyone understands the need for strong external security. Testing perimeters must remain a high priority. External penetration tests should be conducted on a surprise basis up to four times a year. In addition to this testing, we need to strengthen internal security. Simply using intrusion detection or prevention software is not enough. A series of security reviews or audits are required to ensure that the network, operating systems (including the mainframe), database engines, and applications can withstand an attack if the perimeter is breached. In addition, given the current world situation, it is time to ramp up physical security and social engineering audits to determine if your organization has the controls necessary to protect your information assets and your staff.

The comments in this article are mine and mine only. I invite your comments (Gordon@canaudit.com) as they provide me with additional insight into the current level of security awareness. Also, if you need assistance in planning the required security reviews, you may contact me. "United we stand, divided we fall". By working together, we can create a strong security environment for your information assets.

While this article is copyright by Canaudit, you may forward it in electronic form to your associates. If you are not on our distribution list, please email charlene@canaudit.com. She will ensure you get future copies directly to your email address. For permission to reprint this article, please contact Jennifer@canaudit.com.



Gordon Smith, CEO