Global Information Assurance Certification Paper

Argentina: Preparing for a Security Violation

By Raymond Hoffman
September 11, 2002
For GIAC GSEC practical version 1.4b

INTRODUCTION: Argentina has recently been in the news, from spectacular court rulings to famous hackers. If there is very little justice, what can a small or medium-size company do for the eventuality of a computer crime? Regardless whether the company is Argentine or is international with an Argentine presence, fundamental is knowing the legal situation in Argentina, preparing the once-unprotected network, and knowing how to respond to a security violation. Being presented here are the three hopes. Justice. Security. Recovery.

On the 20th of March, 2002[1], a Federal Court of Argentina ruled[2] that a group of hackers, by not violated any existing laws, could not be penalized for their illegitimate alteration of the home page of the Supreme Court. This ironic decision reveals how legal sanctions have been lacking.

To start with, filing a charge, according to the Federal Police[3] here in Argentina, requires incident(s) of threat, trespass, theft and/or damage. In it you must be able to document the threat, to demonstrate the unauthorized entry, to show what was taken and/or to show the before and after of the damage.

Yet, only a handful of cases has been brought before the courts.

In speaking with the Federal Prosecutors[4] here in Argentina, they related to me three points:

1. Inadequate laws, failing to take technological advances into account.
2. Inadequate investments by companies to protect their information and data processing.
3. Additional training for judges and lawyers for increasing the understanding of the technological issues.

The Legal Environment in Argentina

In the Argentine Congress, the House of Deputies has recently approved the Information Crime Bill[5], spearheaded by Deputies Fontdevila[6] and Stolbizer[7]. The Senate has yet to approve it. In it are five fundamental parts.

Unauthorized Access: *"… prison (will be applied to) the person who knowingly and illegitimately gain access by any means to an information system or data without obtaining permission from the owner or by exceeding the limits of the conferred authority." And "… (A greater term of) prison to the perpetrator should he*

reveal, divulge or commercialize the information illegitimately accessed."[1]

Information Espionage: *"… prison (will be applied to) the person who intercepts, interferes or gains access to an information system or data in order to obtain data of an unauthorized form, violating the confidence or secrecy of the information of the said system."* And *"… double the sentence of the perpetrator should he reveal, divulge or commercialize the information illegitimately accessed."*

It must be noted that the mere fact of an unauthorized access or interference is sufficient.

Information Damage or Sabotage: *"… prison (will be applied to) the person who maliciously destroys, renders useless, modifies, deletes or makes inaccessible or by any mode and by any means hinders the normal operation of an information system or data."*

Information Piracy: *"… prison (will be applied to) the person who unduly appropriates, unloads or makes use of the information contained in an information system."*

Information Fraud: *"…prison (will be applied to) the person who, in the mood of making a profit and availing himself either ruse or deceit, harms another person's property (intellectually or otherwise) through the utilization of an information system, whether it be modifying data, be introducing false or true data or whatever strange element, that dodges the security procedures of the system."*

Further dispositions include: suspension of discharge of public duties to the perpetrator should he be a public official in carrying out his functions; greater penalties should he be the one responsible for the custody, operation, maintenance or the security of an informational file, registration, system or data. Also prison is applied to the person who delivers to another, distributes, sells or makes public any equipment of any nature or computer program destined to facilitate the commission of these crimes.

It is noteworthy that in all cases neither fines nor monetary damages are defined against the perpetrator.

So, being a penal code rather than a civil code, in the eventuality of a computer crime the victim might not be able to recover the losses. The civil code still remains old. This accents the point of the Federal Prosecutor that companies should realize the cost of implementing security as an investment of prevention.

Implementing the security

[1] All translations are by the author and are not intended to be complete nor accurate.

The first investment is the employment of a responsible person, given clear duties and being properly trained. The second is the implementation of corporate-wide security policies, which gives that responsible person the authority to implement and administrate those policies. Given the legal vacuum described above, the company should describe the conditions and the penalties that they would apply to employees found violating the security policy.

Let's look at some of those policies and determine more precisely what should be incorporated within, what this administrator is commissioned. The economic situation of a typical Argentine company is considered by referring to inexpensive, sometimes free, solutions. The company should really determine the value of their information assets and determine whether to implement more appropriate, expensive solutions.

A nice brief[8] can be found on http://www.nipc.gov/warnings/computertips.htm . Also, at http://www.microsoft.com/security/articles/steps_default.asp Microsoft has issued a report called "7 Steps to Personal Computing Security"[9], which is quite applicable to small businesses.

Limiting Network Access

Start off by limiting network access through a firewall, established between the private network and the Internet. An inexpensive, yet effective way is to use an old computer 386/486/Pentium processor with Linux installed. Complete instructions can be found at http://www.linuxjournal.com/article.php?sid=3546[10], with diagrams. A quick summary is as follows:

1. Install a distribution of Linux with minimum services plus IPCHAINS.
2. Set up the default rule on the Firewall to deny all incoming connections.
3. Use private IP numbers on the private network and ensure the Firewall is configured for masquerading.
4. Implement logging for capturing, and thus documenting questionable accesses, among other things.

Enforce the use of the firewall by disabling or, better yet, removing all modems from the computers. This can be done by removing the modem drivers and removing the internal modem card or external modem. In case of an onboard modem (part of the motherboard), it will be necessary to disable it through a jumper on the board or through the BIOS configuration (refer to the motherboard manual).

Anti-virus Detection

Next, install an anti-virus program on all machines. They come in three flavors: manual, scheduled or real-time scanning. Manual scanning is usually done when there is a suspicion of a virus infection. Scheduled scanning is strongly recommended – its drawback is determining the best time when the machine is

on but not in heavy use. Real-time scanning does its check on selected types of files at the moment of use. Its drawback is that it can slow down a computer and/or interfere with certain applications. Some real-time scanning programs will also scan email for incoming/outgoing viruses.

As long the drawbacks do not apply, best is to find a solution that provides all possibilities. By the way, it is not recommended to mix different brands on the same machine – conflicts can and do occur between them. Although excellent commercial programs can be found[11], free programs can also be found. For example, the AVG 6.0 Free Edition[12] can be found at http://www.grisoft.com/html/us_downl.htm as a general solution and Trend has its Housecall[13] online manual scanner at http://housecall.antivirus.com/ .

Recovery and Backup

Before going any further, be ready to recover each and every computer. The boot up diskette is needed in the eventuality of an unbootable computer. At times, an emergency repair diskette (also sometimes referred to a rescue disk) can be made for the particular system. In addition to the installation materials provided with the operating system, one can check http://www.bootdisk.com for making boot disks[14].

Recovery also includes having backups available. Rather than having backups done individually on each machine, prepare another machine with sufficient disk space to be a file server. This equipment should have backup peripherals such as tape, zip or another disk or even access to offline services. Make sure that the backups are routinely done and tested. Do not overlook that special applications such as accounting and database often require special backup and have their own procedures. Backups should contain at least the critical data. Sometimes a complete backup is required, including the programs and operating system. Schedule the backups in accordance with the frequency of change in the data/programs. This may very well be daily and therefore done after hours.

Although Windows has a backup program as part of its suite of tools, there are many available, from sophisticated commercialized software to shareware, for example, the Rapid Backup[15] at http://www.mlin.net/RapidBackup.shtml

Security Patches and Software Updates

Essential, too, is maintaining all of the machines updated with security patches. Before doing any update, be sure to close all applications and any antivirus protection that may be running. Also be sure to have a complete backup available. Critical patches for Windows and Internet Explorer can be found at Microsoft's Windows Update[16] located at http://windowsupdate.microsoft.com/ , clicking on the Product Updates. Scanning for needed critical patches will begin. The scan for critical patches for the more recent versions of Microsoft Office[17] can

be found at http://office.microsoft.com/ProductUpdates/default.aspx . Downloads for other Microsoft products[18] can be found at http://www.microsoft.com/downloads/search.asp? .

The scan of other common applications can be found at CNET's free Catchup Service[19] site http://catchup.cnet.com/ . Don't forget to check the vendors of special applications on a regular basis. Subscribing to mailing lists of the vendors and/or security groups should help staying on top of it all. To subscribe to Microsoft Security Notification Service[20], send a blank email to securbas@microsoft.com . Also, don't forget to register all your software – frequently registrations grant access to updates and their notifications.

In the course of checking all of the applications installed, some applications or services may no longer be needed. If so, uninstall them, thus eliminating possible security vulnerabilities.

Passwords

Securing each machine is essential. If a computer has Windows 95 or 98 or Millennium, passwords must be implemented on the BIOS level. Regrettably, these versions of Windows do not have much security.

On the other hand, Windows NT or 2000 or XP can participate on a domain. If a domain was established, there is a centralized administration of accounts for each user. Otherwise, each machine will have its own administration of users allowed to use that machine. In either case, the preferred file system is NTFS, rather than the FAT(32). NTFS will extend the control of users down to folders and files. With such control and logging through events, the activities of all users can be tracked – their signing in and out and their use of various resources. More on this is discussed as one of "Ten Data Security Tips for Your PC Systems"[21] at http://www.smallbiztechtalk.com/news/archives/tips110501-ht1.htm

Passwords should be prepared by each user very carefully. Even more so for the powerful administrator account. Speaking about the administrator account, the person designated as the administrator should use a regular user account when doing regular tasks. He should use the administrator account only for administrative tasks. This is to prevent a (possibly bad) process from effecting changes on a broader scale than anticipated.

It is through the password that a user is authenticated. If it is too easy to guess, someone else can impersonate that user. Also, as a password may become known to others, users should get in the habit of regularly changing their password. There are guidelines[22] such as at http://www.microsoft.com/security/articles/password.asp on how to make passwords difficult to guess. The administrator should establish more clearly the requirements. For example, the password should be no less than 7 characters in

total using numbers and letters with the letters in both upper and lowercase. Names and words are to be avoided. For more critical accounts, passwords should incorporate special characters, such as underlines, asterisks, dashes and so on.

Nonetheless, there is one account that should be disabled. The guest account, even with the minimum permissions, has been involved with various hacks and therefore should be disabled.

Internet Practices

At http://www.microsoft.com/security/articles/assess.asp Microsoft has a nice checklist[23] on Internet access. It may seem obvious but still worth stressing: if the connection to the Internet is not needed all the time, disconnect it. This may include shutting down the firewall, like overnight.

Users should be using distinct passwords for the different services and sites. This way if one password becomes known, only one service becomes exposed.

Caution users who are navigating by Internet against downloading and installing programs and plug-ins of questionable quality or source. The company may wish to limit this activity to an authorized list of programs and their sources. In such case, the administrator should have the authority to uninstall any unauthorized programs and plug-ins.

Email is probably the most difficult realm to control. Users should be trained to not open, preferably deleting, any messages with attachments that fall in any of the following conditions:

- The originator is unknown.
- The attachment is not expected.
- The attachment is an executable or a script.

The company may wish to have configured email client programs to deny attachments that are executables or scripts. In this way a bad judgment call on the third condition can be eliminated.

Also, email client programs may have other settings. Check with the manufacturer of the program. For example, Microsoft has posted for its various versions of Outlook and Outlook Express[24] at http://www.microsoft.com/security/articles/settings.asp .

The Eventful Incident

Regardless of the preparation as described above, still there may be security violations. Possibly the most frequent will be virus infections.

There are often tattletale signs. These signs should not be confused with the

signs calling for maintenance. Running manually the antivirus program is a given.

Let's take as an example that the computer is running much slower. Perhaps all that is needed is a defragmentation of the hard disk. Yet, perhaps there is a process running that is causing this problem. For a Windows 95 computer, Microsoft provides a Windows Process Watcher[25] at http://www.microsoft.com/windows95/downloads/contents/wutoys/w95kerneltoy/ . This unsupported tool has been found to work also with Windows 98. With this tool, all the processes in the computer and their processor use can be seen. Windows NT/2000 has its own Task Manager. Still, these tools will reveal not all surreptitious activities.

Another tattletale sign is a sudden increase in network activity by/to the machine in question. The easiest way is to look at the back of the computer – most network cards (where the network cable is connected) have a traffic indicator that blinks. Sometimes, disconnecting the cable from the network card will help find what is causing the traffic.

A third sign is the sudden loss of disk space. Again, the normal maintenance of cleaning out temporary files and emptying the Recycle Can may be all that is necessary. Otherwise, find the large files (through the Find, specifying recent files with a size of over so much) and the directory(ies) with a lot of files (through the Explorer, sorted by date, checking the quantity through the properties of the recent directories.)

These are not the only signs. The user, and hopefully the administrator, should have the awareness when the computer is not behaving quite correctly.

Here are some guidelines from the "The Emergency Action Card"[26] in handling suspected security violations.

Do Not Panic

It is actually incredible how often things are not like what they first look. Keeping composure will help a lot, saving face later on if proven wrong.

A good technique is to take notes. Not only will it help to clear your mind, these notes can be used as a reference to the incident, even as evidence later on.

Find out what happened. At this stage nothing should be changed or deleted.

At all times avoid finger pointing. Rather, focus and remember that every moment does count. Business must be brought back to normality.

Communication

At this point all communication should not be done through computers. Rather, use the phone or fax, or even better, do it in person.

As soon as possible inform the appropriate management of the incident. Do keep it brief and to the point. Unless asked, don't speculate.

At the same time, avoid talking too much with other people. It is better to be asking them what happened than sharing what one thinks or knows. Encourage them to also limit their conversations.

With the management's consent the Federal Police may be called, either for consultation or for filing charges. They can be reached at:

> Telephone: (54-11) 4370-5899
> Division of Informational Intelligence
> Cavía 3350
> C1425DDJ Buenos Aires

Control the Spread of the Problem

Determine whether the problem is being aggravated or spread by being connected to the network. If so, the computer(s) in question may be disconnected from the network. Naturally, the management will make the final decision.

Full Backup

As soon as possible, make a complete backup.

There is a fast way if the computer can be taken off the network and be shut down. There are two good reasons for not doing this. First, essential operations may be shut down. Second, the computer may have trouble rebooting or have malicious programs starting as a result of the reboot. On the other hand, rebooting the computer with a boot diskette is clean – no files on the hard disk are being used and all files can be copied easily. To do this fast and clean backup, shut down the computer and install a spare hard disk as a secondary. Start up the computer using a boot diskette and copy all the folders and files of the primary to the secondary using DOS's *xcopy* command. Be sure to specify the parameters of *xcopy* to include empty folders, copy the attributes and continue even if there are errors.

An excellent way to copy the entire disk is through a ghosting program like Norton Ghost (http://www.symantec.com/sabu/ghost/ghost_personal/). Because ghosting can backup the entire hard disk, not just the folders and files, more detail is available for forensic analysis.

If the computer is not to be taken off the network, then do the backup over the

network to a media that is new and unused. This may be to tape, zip or the spare hard disk installed elsewhere on the network.

Repair the Problem

This is where concentration and analysis come in. Of course, practice and experience helps. The administrator should have already been encouraged to know his systems.

All the various logs should be inspected for pertinent evidence as to what may have happened. Perhaps there was a hacking attempt (unauthorized access) revealed in the firewall and event logs. In this case tighten up the permissions and change passwords that were abused.

Compare previous backups with the actual to determine what files have changed. Perhaps there were cracking attempts (unauthorized change of information).

Earlier backups may be needed to get the system back up and running. Be sure to take good and detailed notes.

Bring the Computer Back Up

This is not the moment to say, "A job well done!" even if it seems well deserved.

Rather, verify that the problem is not recurring or occurring elsewhere. Monitor the computer and check other computers. It is possible that the notes will be quite useful for restoring them quickly.

Also, this is a good time for everyone who was involved in this incident (the managers, the technicians, the administrator) to sit down and review the entire incident. This will be where the notes will come most handy. The tone of the meeting should be calm and reflective.

What just passed was a bad incident and, understandably, nobody will want a repeat of it.

List of References:

1. Gornstein, Marcelo H. Y otros. "103.570-IN Fed. Crim. y Corr." Secretaría de Jurisprudencia, Cámara Criminal y Correccional, Nro. 12, 2002/03/20
2. Leyden, John. "Argentine judges want law update after crackers walk free." The Register. May 13, 2002. URL: http://online.securityfocus.com/news/407
3. División de Inteligencia Informática, Policía Federal de Argentina, Cavía 3350, Buenos Aires, Argentina
4. Procuración General de la Nación, Avda. de Mayo 760, 4° Piso, Buenos Aires, Argentina
5. "Sesiones Ordinarias 2002 Orden del Día Nº 639." Cámara de Diputados de la Nación. July 25, 2002. URL: http://www1.hcdn.gov.ar/dependencias/cceinformatica/Órdenes_del_día/OD_639.html
6. Diputado Pablo Fontdevila, Presidente de la Comisión de Comunicaciones e Informática, Cámara de Diputados de la Nación, Buenos Aires, Argentina

[7] Diputada Margarita Rosa Stolbizer, Presidente de la Comisión de Legislación Penal, Cámara de Diputados de la Nación, Buenos Aires, Argentina

[8] National Infrastructure Protection Center. "Seven Simple Computer Security Tips for Small Business and Home Computer Users." URL: http://www.nipc.gov/warnings/computertips.htm

[9] Microsoft. "Security & Privacy for Home Users: 7 Steps to Personal Computing Security." April 2, 2002. URL: http://www.microsoft.com/security/articles/steps_default.asp

[10] Regan, Jeff. "An Introduction to Using Linux as a Multipurpose Firewall." Linux Journal. March 1, 2000. URL: http://www.linuxjournal.com/article.php?sid=3546

[11] Feinstein, Ken and Keizer, Gregg. "CNET's antivirus guide 2002." CNET Software. July 3, 2002. URL: http://www.cnet.com/software/0,10000,0-806174-8-20096702-1,00.html?tag=st.cn.sr1.ssr.

[12] "AVG 6.0 Anti-Virus System - AVG 6.0 Free Edition Download." Grisoft Inc. URL: http://www.grisoft.com/html/us_downl.htm

[13] "HouseCall." Trend Micro. URL: http://housecall.antivirus.com/

[14] Bootdisk.Com. "BootDisks - PC Support - Essential Utilities." URL: http://www.bootdisk.com

[15] Lin, Mike. "Rapid Backup." URL: http://www.mlin.net/RapidBackup.shtml

[16] Microsoft. "Microsoft Windows Update." URL: http://windowsupdate.microsoft.com/

[17] Microsoft. "Microsoft Office Product Updates." URL: http://office.microsoft.com/ProductUpdates/default.aspx

[18] Microsoft. "Download Center." URL: http://www.microsoft.com/downloads/search.asp?

[19] CNET. "CatchUp." URL: http://catchup.cnet.com/

[20] Microsoft TechNet. "Product Notification Security." URL: http://www.microsoft.com/technet/security/bulletin/notify.asp EMAIL: securbas@microsoft.com

[21] Feinbert, Joshua. "Ten Data Security Tips for Your PC Systems." Small Biz Tech Talk. URL: http://www.smallbiztechtalk.com/news/archives/tips110501-ht1.htm

[22] Microsoft. "Security & Privacy for Home Users Checklist: Create Strong Passwords." April 2, 2002. URL: http://www.microsoft.com/security/articles/password.asp

[23] Microsoft. "Security & Privacy for Home Users Checklist: Assess Your Risk." April 2, 2002. URL: http://www.microsoft.com/security/articles/assess.asp

[24] Microsoft. "Security & Privacy for Home Users Checklist: Check Your Settings." April 2, 2002. URL: http://www.microsoft.com/security/articles/settings.asp

[25] Microsoft. "Windows 95 Kernel Toys Set." November 14, 2000. URL: http://www.microsoft.com/windows95/downloads/contents/wutoys/w95kerneltoy/

[26] Northcutt, Stephen. "Computer Security Incident Handling: Step-by-Step." The SANS Institute. 1998. URL: http://www.sans.org/newlook/publications/incident_handling.htm