Dealing with Computer Crime

Being the victim of a computer security incident is an unpleasant and stressful experience. In the spirit of first aid, these guidelines aim to provide assistance until expert help arrives.

First steps

The steps taken immediately after the incident is discovered will greatly affect the chances of a successful outcome, whether that outcome is the prosecution for a criminal offence or just the restoration of a compromised system to secure service. The initial aims in either case must be to prevent further damage to the system and to ensure the preservation of any evidence it may contain.

When dealing with any incident it is vital throughout the process to keep written notes of what actions are taken. These should be sufficiently detailed to allow an independent person to achieve the same results. Each page of notes should be signed and dated. These notes help to avoid confusion and will be required as evidence if a case comes to court.

The computer system involved in the incident should be isolated as soon as possible. Nobody should touch it, enter any commands or use the mouse. If the system is networked its connection should be physically removed after making a written note of which network sockets on the computer and wall were connected. At this point you should seek expert help from your local computer security staff, an Incident Response Team run by your organisation or network, or the police. They need to be provided with all relevant information about the incident and their advice should be followed.

If the computer is switched on, then you can collect some basic information at this stage. Make a note of what is visible on the screen. Ideally, take photographs of the screen and computer to record the display and the state of the equipment. If the computer is displaying a clock, make a note of how far it differs from the correct time, but do not change it. If it is likely to be some time before an investigation can start then it may be best to power the system down to stop further change: do not perform a software shutdown, but simply pull the power cable out of the back of the machine. This may leave file systems in an inconsistent state, but is likely to destroy less evidence than the cleaning up which is done as part of the shutdown process.

Once the computer has been isolated there are inevitable competing demands, whether to return it to service or to investigate the incident. If possible, the best solution is to replace the system with another, leaving the original for calm investigation. However there is no point in restoring a service that is as insecure as the original. At the very least the new system should be fully secured, its configuration checked and all passwords changed. For serious crimes, you have no option but to report them and allow the police to investigate.

Caring for the evidence

Evidence on magnetic disk is hard to deal with since it is easy to make accidental changes. Even running an apparently harmless command like 'dir' will alter the access times on many files and directories. This is likely to cause confusion even in local investigations and can be disastrous in court where each action may be used to cast doubt on the accuracy of the evidence. If at all possible, any investigation should be done on a copy of the original system. The police use special copying devices that duplicate even the arrangement of files on a hard disk. If these are not available then the UNIX 'dd' command can be used to image the raw disk device while preserving timestamps. Do not boot the system from its hard disk. A floppy disk version of Linux can be used to take disk images from any PC-based system.

There may well be other useful information about the incident that may be collected with less risk of damage. This includes documentation for the computer and information from its owner. Passwords and details of any recent changes may be requested, but must not be taken from the machine itself. Log files from other systems, particularly those on a network, may well contain useful information and secure copies of these should be taken. Logs from routers, firewalls, proxies, mail or web servers can give a picture of activity by other systems. Past backups from the system can be extremely useful in determining the time and extent of any changes. Until the investigation is completed, relevant backup media should be placed in a secure location and not reused.

ACPO principles

The Association of chief Police Officers (ACPO) publishes the guidance it gives to policemen on dealing with computer based evidence [1]. The following principles are a useful reminder to anyone involved in investigating incidents:

- No action taken by police or their agents should change data held on a computer or other media that may subsequently be relied upon in court;
- In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and give evidence explaining the relevance and the implications of their actions;
- An audit trail or other record of all processes applied to computer based evidence should be created and preserved and an independent third party should be able to examine those processes and achieve the same result.

For more information

The London Internet Exchange (LINX) publishes best current practice guides [2] dealing with many types of computer misuse

Computer Incident Response Teams usually have good contacts with law enforcement agencies and may publish specific guidance for their customers. Janet CSIRT [3] is the Incident Response Team provided by Janet as one of the services on the Janet network. Details and specific information on dealing with security incidents can be found on their website [3]

ACPO's Good Practice Guide for computer Based Electronic Evidence [1] is available online

---