Polizia di Stato

A guide to safe computing

Let's dispel the myth that only important companies run the risk of being attacked over the internet. Indeed, people believe that the more a company is known the greater is **the chance of being attacked**.

We all presume that a well known company arouses people curiosity and that violating their systems would represent a coveted trophy. **This is only partly true** because an increasing number of attacks are being launched blind.

The term "blind" means that the victim is unknown to the hacker. These attacks are made using **special software tools,** which are capable of scanning entire domains looking for machines using specific operation systems and application software, possibly containing some known bugs.

The real attack is launched when these machines have been identified. It will be successful if the necessary patches (updating) have not been installed on the computer.

Since hundreds of bugs are discovered (and advertised) every day, no system administrator will consider his/her machine safe without **updating its software** frequently.

The only way to make our computers reasonably safe is a correct and constant application of a "security policy".

We have set out some **basic technical advice** below which can be usefully applied by every internet user and that any system administrators can share with the employees of their company in order to make them think over the issues of IT security.

Some of these tips are for those employees who are using a laptop computer containing some business data, with which they connect to the internet from home.

Use a firewall Use an antivirus software Do not open email attachments unless checked with an antivirus Do not run programs unless first examined with an antivirus Make back up copies Do not give out personal data in chat Choose a strong password and do not disclose it to anybody Use encryption software for confidential communications

Use a firewall Firewalls are tools, both hardware and software, that allow you to monitor the exchange of data between your computer/local network and the outside world.

They are programmed with a set of rules so as to inhibit, for example, data traffic coming from outside and directed towards pc ports often used for attempting intrusions. They also allow users to view the history of intrusion attempts, including the electronic address used by the hacker. Many firewall tools are available free of charge on the Internet.

Use an antivirus software and keep it updated The computer virus is nothing but a program that has the ability to self-replicate and, once written on the disks, to conduct a series of operations on the host PC, which can be more or less harmful: from displaying messages on-screen to encrypting the hard disk's contents, making it unreadable. Since new viruses are created every day and spread with great rapidity, thanks to the development of the Internet, it is essential not only to install a good antivirus on your PC, but also to update it frequently. Moreover, an antivirus software, if not updated regularly, could be even more dangerous than not having it at all. It could make us feel safer up to the point of failing to comply with the basic internet security rules.

Do not open email attachments unless checked with an antivirus The main vehicle for spreading viruses is the e-mail, or better e-mail attachments. Indeed, a virus can be transmitted only through executable files (files with extension .exe, .com, .drv and .dll) or containing a piece of code that is executed (e.g. Word documents containing macros).

Therefore, you cannot infect your computer by simply reading the text of an e-mail: you must run the infected file that could be attached to e-mail received.

It should also be noted that opening an attachment to an e-mail message only if you know the sender is not in itself sufficient to protect us from infection. In fact, some types of viruses steal the infected computer's e-mail addresses registered in the e-mail

client and send them e-mails on your behalf containing the virus in the attachment.

The recipients of such messages could open them (including the attachment) without using any precaution, because they know the sender. This explains how the virus "Melissa" was able to infect millions of computers! On the other hand, we cannot delete all the attachments we receive assuming they are infected!

It is therefore surely worthwhile spending a few seconds to save the attachment to a floppy disk and then parse it with an antivirus.

Finally, there are some programs that, when executed on your PC, have the ability of putting it under someone else's remote control. These programs can also be inside the files attached to e-mail messages and can be identified by a good antivirus.

Do not run programs unless first examined with an antivirus We have seen what is a virus and how it is transmitted. This applies, of course, not only to e-mail attachments but also to all executable files contained in floppy disks or CD ROMs. It is therefore advisable to check these files for viruses before running them.

Make back up copies Antivirus software dramatically reduces the risk of infection, but we should consider that, if an antivirus detects a virus, it is because there have been some victims already. This means that it could also happen that our antivirus software does not recognize a file as containing a virus, because it is outdated or because the virus is brand new. In this case, as a result of the infection, the data on our hard disk could get lost. In this unfortunate event it is of vital importance to have made a back up copy beforehand.

Do not give out personal data in chat During virtual conversations (chats) resist temptation to give out personal information to unknown chat participants.

This for two reasons: We do not know who is on the other side. Our data could be used to steal our passwords.

Choose a strong password and do not disclose it to anybody To create a secure password you should take the following steps:

The password should be the maximum length allowed by the system and at least six characters long. In fact, the programs used to crack passwords require a time that is directly proportional to the length of the password in order to be successful.

The password must not be a term contained in a dictionary, because there are programs that, supported by the machine's computing power, will try all the words in a dictionary.

The password should not contain lower or upper case only but both and possibly also alphanumeric symbols such as asterisks and dashes. In this way, password cracking programs must try every possible character combination, thus requiring a long time to find it out, especially if the password chosen is a long one.

The password should not be in any way related to the owner's private life. Therefore, it is advisable not to use the car registration number, the name of your favorite team, your name, date of birth etc., because the first attempts will be related to the private life of the password owner.

The password should not be written anywhere. What's the point of choosing an uncrackable password if you write it on a post-it left on the monitor or the mouse pad? To create a password easy to remember, you can use the so-called "pass phrase" composed by the first letter of each word that makes up a sentence. For example, from the phrase "Nel Mezzo Del Cammin Di Nostra Vita" ("Halfway through the journey of our life") we get the password NMDCDNV which, to be more difficult to guess, will be made up of both upper and lower cases: nmdcDNV.

It is advisable to use a different password for each application because, in the event it is discovered, the damage caused would be lower.

The default password, assigned by the systems the first time they are used, should be replaced immediately.

The password must be changed periodically.

Do not tell anyone your password! If there is a need to share it with anyone for any reason, you should change it as soon as possible.

Use encryption software for confidential communications When you send confidential data, you should use an encryption software that allows you to encrypt outgoing messages. In this way, the message intercepted would appear as an unintelligible set of characters without the key used to encrypt the document. There are several programs that offer this kind of protection which can be found on the Internet free of charge.

The suggestions in this article are certainly basic but if each of us followed these elementary "security measures" when using the Internet, there would be a significant reduction in computer crime and its consequences.

Happy surfing to all.

20/04/2011