International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

The Researcher Faces Data Security: Risks and Protection

Vicky Kajeje, Ir Sylvain Sibita, Muhindo Syauswa, H. Ciraba

Abstract: ***In this publication, we are presenting the dangers to which the researcher is exposed daily, through the data he manipulates (harvesting, analysis, processing and publication ...) What types of risks and attacks Is exposed; How to remedy them (remedies and solutions) and what precautions should be taken in the future.***

Keywords: data, virus, researcher, security

1. Introduction

A datum (data): Information, elementary description of a reality, it may be a measure, an observation.

A computer virus: program written in order to spread slyly and quickly to other computers. It more or less seriously disrupts the functioning of the infected computer. It can spread through any means of exchanging digital data such as the Internet, and in particular via e-mail messages or their attachments.

The Researcher: or man of science; Means a person whose profession consists in carrying out scientific research. It is difficult to define the profession of researcher as the fields of research are diversified and involve important differences in the practice of this profession.

Computer security: Computer security generally consists in ensuring that the hardware or software resources of an organization are used only within the framework provided.

A set of procedures or techniques in place to protect personal or corporate data;

Computer security is based on 5 fundamental principles namely:

- Integrity, that is, ensuring that the data is what is believed to be;
- Confidentiality of ensuring that only authorized persons have access to the resources exchanged;
- Availability, to maintain the proper functioning of the information system;
- Non-repudiation, to ensure that a transaction can't be denied;
- Authentication, to ensure that only authorized persons has access to resources.

We are in the contemporary era where we observe a lot of innovations especially on the technical level; Indeed, with the evolution of new information and communication technologies (ICTs), the whole world is undergoing a major revolution in many fields (Medicine, Army, Geology, Mechanics, Aviation, Architecture, Volcanology, etc.). A researcher, who lives his research on a daily basis, is also called upon to conform to the new mutations that are observed, he is obliged, for example, to use the computer tool well, especially since ¾ of the new equipment It is called to use are accompanied by software to allow the collection and interpretation of data.

That is why we felt it was essential to say something about data protection in the context of research.

A) Primary objectives:

- Make the Researcher aware of the importance of data protection.
- Know what an attack, how it spread and how to eradicate it.

Some definitions:

- Virus: small computer program, located in the body of another, which when executed loads into memory and executes the instructions that its author has programmed.
- Program capable of detecting the presence of viruses on a PC, and if possible, disinfect it.
- Virus eradication is used to describe the procedure for cleaning the computer.
- "Any computer program capable of infecting another program by modifying it so that it can in turn reproduce itself" (CPA: auto-propagable code)
- There are Resident Terminate and Stay resident viruses (TSRs), load into the computer's RAM to infect the executable files launched by the user.
- There are also non-resident viruses, which infect the programs present on the hard disk, as soon as they are executed.
- Viruses are not classified according to their degree of nuisance, but according to their mode of spread & infection.

The following types can be distinguished:

• Worms: are viruses capable of spreading through a network.
• Trojan horses: (Troyans) virus to create a flaw in a system. They are used more by "hackers"

Brief history of the Trojan horse

The Greeks, unable to penetrate into the fortifications of the city (TROIE), had the idea of giving as a gift an enormous wooden horse as an offering to the city, abandoning the siege.

The Trojans appreciated this offering and brought it back to the walls of the city. The Horse was filled with hidden soldiers who hurried out of it at night to open the gates of the city and allow access to the rest of the army.

Polymorphic viruses (several forms)

Some virus creators thought of giving them the ability to automatically change their appearance, like the chameleon, by giving them the ability to camouflage their signature.

Retrovirus: or "flibustier virus", a virus with the ability to modify antivirus signatures to make them inoperative.

Boot sector virus: infects the boot sector of the hard disk (MBR: master boot record)

Macro viruses or trans-applicative viruses

These viruses typically infect macros in micro-soft Office documents (Word & Excel)

Common script, which can be inserted in most documents containing macros, this is VBScript.

Currently, most visual basic scripts are broadcast by e-mail.

Mutant viruses:

In reality, most viruses are clones or "mutant viruses", ie viruses that have been rewritten by other users to modify their behavior or signature.

When there are several versions, we speak of variants of a virus, this one becomes difficult to locate since the Antivirus editors must add these new signatures to their databases.

Adware: loaded program on our computers and managing the display of advertisements. They do not collect or transmit information.

Spyware: any software introduced on a device that uses a user's Internet connection or any other means or medium without his knowledge or without his explicit and informed permission to collect data.

These spy programs collect information about the user of the PC on which they are installed in order to send them to the company that distributes them to enable them to profile users (profiling).

Ex: traceability of URLs of sites visited. (A Uniform Resource Locator (URL) is a universal naming format for designating a resource on the Internet)

- Analysis of purchases made on the Net.
- Personal information
- Information - bank payment
- Tapping keywords entered in search engines.

Spam: spam (spam, spam) are unsolicited emails, usually for advertising purposes and whose addresses of recipients have been retrieved on the internet.

They often arrive with fake sender addresses. The solution is to use an anti spam software, or add the e-mail in the spam list or both.

C) Data can be lost in different ways, such as:

- ✓ Misuse or misuse of the computer
- ✓ Theft of the computer
- ✓ Fire
- ✓ floods
- ✓ Viruses for an unprotected PC
- ✓ Excessive temperature
- ✓ Excess Moisture
- ✓ Accidents
- ✓ Wear or aging of the equipment (damaged hard disk)
- ✓ Inappropriate cuts in electric current.
- ✓ The irresponsibility of the user
- ✓ Poor packaging (after a move, for example)
- ✓ Etc.

2. Eradication Methods

The best protection for your computer is yourself!

- Nothing can happen to you if you did not want it!!
- To eradicate viruses, programs are called **antivirus.**
- Antivirus: a program capable of detecting the presence of viruses on a workstation and, to the extent possible, disinfecting it.
- Virus eradication is used to describe the procedure for cleaning the computer.

Eradicating a virus means:

- Delete the code for the virus in the infected file.
- Delete the infected file;
- Quarantine the infected file (i.e. isolate the file in a place where it cannot be executed.

N.B: Each virus is characterized by its viral signature.

Some Means for Securing Data

We talk about the eradication of viruses to designate the procedure for cleaning the computer.

Anti viruses rely on this signature specific to each virus to detect them; it is git of the method of search for signature (scanning).

- In some antivirus programs are called "firewall or firewall"

These are programs that filter incoming and outgoing communications from your computer.

- Ex: - Firewall for windows
- Alarm Zone
- Tiny personal firewall

- Install a password manager to replace passwords regularly.
- Install a Licensed Operating System, not pirated copies.
- Security vulnerabilities must be detected:

1. Software Vulnerabilities:

The vulnerabilities of the software are introduced by errors in the Operating system or in the application code. New vulnerabilities are still common; that's why big companies like Microsoft, Apple and other operating system producers produce patches and updates every day.

2. Hardware Vulnerabilities:

Hardware vulnerabilities are often caused by hardware design flaws. The RAM, for example, consists essentially of capacitors installed close together. It was discovered that due to proximity, continuous changes applied to one of the capacitors could affect the surrounding capacitors.

Hardware vulnerabilities are device-specific and are typically exploited for compromising attempts. While exploits on hardware are more common in highly targeted attacks, classic malware protection and physical security provide sufficient protection for the ordinary user.

Some Practical Advice:

- Have a Personal Computer (PC, laptop preferably)
- Have a removable backup disk (external disk or flash disk ...)
- Avoid multi-user (several users) of your laptop.
- The computer being your tool of work, to shelter it of the children, or other curious.
- Avoid lending your Laptop to anyone; It will save you trouble or inconvenience with your friends or colleagues.
- Install only useful programs because there are others that can carry viruses.
- Take care to save data on multiple media at once (DVD, external Disk, data server (network), tape back up, memory card, external hard disk ...)
- Avoid flash drive traffic from outside.
- Save data electronically and hard (printed versions) if possible.
- Etc.

3. Conclusion

The Entry of the Computer and Computer Tools into the world of research is a revolution in the 21st century; The computer is increasingly successful; It makes available to the researcher many means, tools (Internet, index, electronic texts, dictionaries, search engines ...) that make

the search easy and allows to achieve the expected results in record time.

This is why the Contemporary Researcher cannot escape from it.

It is necessary to use prudence and know-how to shelter the data (its research) in order to bring to the benefit of the world (community, nation, universities, and region) the results to which it has led (publications).

References

[1] ITE course (IT Essentials), Academy CISCO, ITIG / Goma, unpublished 2015.
[2] CCNA 1 and 2 courses (ver 5.0), Academy CISCO, ITIG / Goma, unpublished 2016
[3] The CNIL Guides, The security of personal data, 2010 edition
[4] Introduction to Cybercrime, Cisco, 2016.
[5] Optimize your hard drive, Key4IT, 2014.
[6] Website: www.commentçamarche.com
[7] Encarta, 2009 Edition