Norme d'uso
per sistemi operativi Linux

V 1.4

Attuazione della Circolare AgID 18/04/2017, n. 2/2017
“Misure minime di sicurezza ICT per le pubbliche amministrazioni
(Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)”
GU Serie Generale n.103 del 05-05-2017

Livello Minimo

Introduction

This guide reports procedures, actions and configurations aiming to implement the requirements of AGID (*Agenzia per l'Italia Digitale*) guideline 18/04/2017, n. 2/2017 ("Minimum ICT security requirements for public administrations" (Prime Minister's directive August 1st 2015)", published in Italian–"*Gazzetta Ufficiale*" – General Series no 103 – 2017-05-05, for devices using Microsoft Windows operating system. We limit the analysis to minimum level of security required by the guideline, i.e. the minimal set of security measures that MUST be adopted by any public administration office.

Indications below reported aim to fulfil requirements expressed by AGID directive, not replacing, but rather integrating what is already indicated by *Commissione Calcolo e Reti (CCR)*:

Disciplinare per l'uso delle risorse informatiche–Regulation for the Use of INFN Information Technology Resources (CD 23/02/2007);

Carta della Sicurezza Informatica - Charter of IT security (CD 23/02/2007);

Windows base (20/12/2005)

Windows advanced (20/12/2005)

Servizi Centralizzati - Centralized services (20/12/2005)

Gestione Incidenti - Incident management (20/12/2005)

Sicurezza della LAN - LAN security (19/12/2005)

available here (some of them in Italian only):

- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica,
- https://web.infn.it/CCR/index.php/it/sito-utenti-del-calcolo/sicurezza-informatica/56-progetti-dei-gruppi-di-lavoro/documentazione-progetti/81-documenti-progetto-harmony

In particular this guide is an update and an extension of "Windows base (20/12/2005)" "Windows advanced (20/12/2005)" documents and, according with the guideline requirements, is addressed mainly to users having system administrator access level.

Guideline requirements related to minimum security level is reported in **Appendice A**.

Every single security measure will be referred with the related identifying number ABSC ID (Agid Basic Security Control(s) Id Number).

Systems administrator's duties

Procedures, actions and configurations targeted for implementation of AgID guideline, minimum level of security, will be indicated with the following keywords and included in a box (with a gray background in case of measures required by multiuser systems).

IT'S MANDATORY,

[IT] MUST/[THEY] MUST,

[IT] MUST NOT/[THEY] MUST NOT.

Fulfillment of these measures is a system administrators' duty.

Measures not marked with above indicated keywords are suggestions to increase the security level, although not explicitly recommended by the minimum level of security of the Guideline.

Operating system installation and configuration

In order to protect operating systems with standard and secure configurations [ABSC ID 3.1.1, 3.2.1] it is suggested to coordinate the installation and configuration of GNU/Linux operating systems with the "Computing Services" (CS) staff, following the methods and procedures they promote, beside those reported in this guide.

Preinstalled systems and systems whose configuration is not well known, should not be connected to the network.

Where physical access to the system is not protected, it is suggested to

- Protect BIOS access with a password,
- Disable from BIOS the boot choices from usb, floppy and CD,
- Set a password in the *boot loader* (for instance **grub**).

Installation

When it's not possible to use a semi-automated installation procedure provided by CS, only images downloaded from *official* repositories, or images provided by the CS **MUST** be used. In both cases, image authenticity MUST be validated comparing image checksum with the one reported in the repository.

When preconfigured virtual images, *containers* or *dockers* are used, the administrative credentials **MUST** be modified before connecting the system to the network [ABSC ID 5.3.1].[1]

When the installation image is not provided by CS, it **MUST** be stored *offline* (for instance on a CD or DVD [ABSC ID 3.3.1]).

1 For instance disabling the network interface and connecting to the virtual console of the system with administrator privileges.

Only stable and maintained versions have to be installed, avoiding test versions or versions no longer supported. It is a good practice to always perform a minimal installation. Only the software strictly necessary to provide the service should be installed.

In case of a server running centralized services, **IT'S MANDATORY** to compile and keep updated a list of software used and related versions. [ABSC ID 2.1.1].

According with statements of "Disciplinare per l'uso delle risorse informatiche" - "Regulation for the Use of INFN Information Technology Resources" concerning network configurations, IP addresses **MUST** be assigned by CS, either statically or via dhcp.

Configuration and first boot

The passwords of all administrator accounts:

- **MUST** have an adequate strength (for instance at least 14 characters) [ABSC ID 5.7.1],
- **MUST** be replaced with reasonable frequency (*password aging*) [ABSC ID 5.7.3],
- **MUST NOT** be reused within a short period of time (*password history*) [ABSC ID 5.7.4].

root login must be allowed only from the *virtual console* (tty*). Other types of access (including **ssh**) **MUST** be disabled [ABSC ID 5.10.3].

Never use trivial passwords, or passwords containing words reported in the dictionary of any language.

It is suggested to perform the following steps at first boot:

Si consiglia di eseguire le seguenti operazioni al primo avvio:

- make sure that the OS package management system checks package signatures using **gpg**, such to reduce possibilities to install suspicious packages.
- close all the services that are not necessary and make sure they do not start at boot time; in particular for laptops disable the *bluetooth service* and activate it only when necessary;
- when not needed remove the following users: adm, ftp, games, gopher, halt, lp, mail, news, operator, shutdown, userdel, uucp;
- when not needed remove the following groups: adm, dip, games, groupdel, lp, mail, news, uucp;
- disable the special accounts (for instance bin) necessary for the proper behavior of the system modifying the *shell* in /etc/passwd in /bin/false;

- make sure that the boot of the system in *single-user* mode is allowed only after the root password is inserted; this is very important if the system is not located in a controlled area and can be physically accessed by unauthorized people;
- set the proper rules so that services can be accessed only from the desired addresses, using *iptables* or *tcp_wrapper* (/etc/hosts.allow and /etc/hosts.deny files);
- use PAM libraries to control the access to services and resources of specific users;

Filesystem sharing: nfs

NFS filesystem is based on *UID* and *GID* of the remote user and for this reason is not a secure service by itself. It is recommended to use it only when really necessary. It has then to be configured with at least the following restrictions:

- do not use *wildcards* in **`/etc/exports;`**
- do not allow **root** access (if possible)[2];
- mount the filesystem in read-only mode (if possible)[3];
- export the filesystem only to the hosts that need it;
- check the situation with the showmount command with -e and –a options;
- if the filesystem is inserted in the **`/etc/fstab`** file, use the nosuid option;
- if possible use *iptables* to filter 111 and 2049 udp and tcp ports;
- add the *portmapper* service to the ones controlled by *iptables* or, otherwise, use tcp_wrapper;

Remote Access to the system

Remote access to the system **MUST** be done using only secure protocols, for instance using software like **ssh**, **scp**, and so on [ABSC ID 3.4.1].

In order to simplify authentication and authorization mechanisms some services and applications allow to configure remote machines as "trusted", so that it is possible to directly access the service or application, even in a batch mode. Such a configuration should be in general avoided.

2 The request is difficult to implement in many scenarios. Anyway it is important to evaluate its feasibility to improve the protection against ransomware (Reveton, CryptoLocker, WannaCry, …).

3 Also in this case the request is difficult to satisfy, but it could reduce the ransomware damages.

In the case such a configuration is used it is suggested to:

Se è necessario utilizzarle si consiglia di:

- use iptables or **tcp_wrappers** (/etc/hosts.allow and /etc/hosts.deny files);
- reduce to the minimum strictly necessary the number of machines allowed to login without authorization, and never allow it from outside the LAN;

First backup

When the installation and configuration is done, a full backup of the system MUST be performed, so that system can be recovered if compromised [ABSC ID 3.2.2]. This backup MUST be stored *offline* [ABSC ID 3.3.1], for instance on CD or DVD.

Specific software, as *clonezilla*, can be used on this purpose. Or, simply, dd + gzip.

Maintenance

System update

The system must be kept constantly updated. Security patches **MUST** be applied as soon as they are released [ABSC ID 4.8.2]. It's recommended to enable automatic updates (for instance using *cron*) both for operating system and installed software [ABSC ID 4.5.1].

If the system has critical services that could be potentially broken by automatic updates, those **MUST** be notified and performed interactively at the earliest opportunity. In this case priority MUST be assigned to the actions for vulnerability fixing according with the associated risk. In particular top priority **MUST** be given to patches fixing severe vulnerabilities. [ABSC ID 4.8.2].

If the system is subject to significant variations (i.e. new services added) **IT'S MANDATORY** to agree with the CS a security scan to highlight potential new vulnerabilities introduced [ABSC ID 4.1.1]. If the scan finds new vulnerabilities, actions **MUST** be taken to fix the vulnerabilities, or if not possible, the accepted risk **MUST** be documented [ABSC ID 4.7.1] and communicated to CS.

Accounts and credentials audit

It is suggested to periodically check user accounts and passwords with specific programs (for instance **John The Ripper**).

Users Management

Administration privileges **MUST** be granted only to users having adequate skills that need, for operational purposes, to change systems' configuration [ABSC ID 5.5.1].

IT'S MANDATORY to maintain a registry of all administrative accounts ensuring that each of them is formally authorized [ABSC ID 5.2.1].

Administrative accounts **MUST** be used only for administrative, not-ordinary tasks. Any administrative access MUST be recorded. [ABSC ID 5.1.2]. Fot that reason **IT'S MANDATORY** to always use *sudo* to execute administration commands [ABSC ID 5.1.2].

Administrators' privileged credentials **MUST** be clearly distinguished from non-privileged ones, which MUST correspond to different credentials [ABSC ID 5.10.1]. In other words, if a user is also an administrator, he/she MUST have two accounts, but only one of them will be member of administrators group (*sudoers*) and will be enabled for administrative tasks.

All accounts, and administrative ones in particular, **MUST** be nominal and clearly associated to one physical person (no shared accounts) [ABSC ID 5.10.2]

It is always suggested, when possible, to make use of **sudo** in order to reduce the risk of performing wrong operations on the system.

Management of files with critical or relevant data

Access to files with particular requirement for privacy or confidentiality (data relevant for INFN) or containing critical information as personal certificates, private **ssh** keys, server certificates, gpg keys, and so on, **MUST** be stored using 600 (rw- --- ---) o 400 (r-- --- ---) permissions.

Malware prevention

IT'S MANDATORY to install an antivirus software (AV) [ABSC ID 8.1.1]. Automatic update of AV must be set, as well as automatic execution of anti-malware scan when a removable device is plugged in [ABSC ID 8.8.1].

Even if not directly affected by the malware, an antivirus software is useful also on GNU/Linux operating systems. The AV can limit the propagation of malwares to other systems running different OS, where they could produce damages.

IT'S MANDATORY to use a personal *firewall* like for instance iptables [ABSC ID 8.1.2].

IT'S MANDATORY to limit usage of external devices, limiting their usage only when strictly required from operational needs [ABSC ID 8.3.1].

IT'S MANDATORY to disable automatic execution of contents from external devices in the moment they are connected [ABSC ID 8.7.1].

IT'S MANDATORY to disable automatic execution of dynamic content (macro) included in file [ABSC ID 8.7.2].

IT'S MANDATORY to disable automatic opening of e-mail messages [ABSC ID 8.7.3]

IT'S MANDATORY to disable automatic preview of file contents [ABSC ID 8.7.4].

Safety copies

IT'S MANDATORY to make, at least weekly, a backup of the "information strictly needed for a full restore of the system" [ABSC ID 10.1.1].

In case of backup on cloud, or when it's not possible to ensure the complete confidentiality of the information contained in the backup by proper physical protection of supports, **IT'S MANDATORY** to encrypt the backup before its transmission [ABSC ID 10.3.1], making sure also that it's not permanently accessible through the network, avoiding that attacks to the system will involve also its safety copies [ABSC ID 10.4.1][4].

Enhance data protection with cryptography

For laptops, it's suggested usage of encrypted filesystems, to prevent access to data in case of loss. Encrypted filesystems are suggested also for those workstations with special privacy requirements.

Follow INFN indications on the kind of files that **MUST** be protected with encryption, making sure that encrypting keys are protected as well [ABSC ID: 13.1.1][5].

System compromission

4 The request allows to improve the protection against ransomware (Reveton, Cryptolocker, WannaCry, …).

5 See "**Management of files with critical or relevant data**".

If a system is compromised, CS **MUST** be contacted immediately, and recovery procedures MUST be agreed upon.

System recovery **MUST** be performed either from safety copies created when the system was installed and configured[6], or as a new installation[7] [ABSC ID 3.2.2]

Log files

It can be useful to maintain and periodically analyze log files in order to spot security issues and wrong system configurations.

It is suggested to properly configure the *logging level* of every host. Critical hosts will require to store more detailed log files and for a longer time.

It is suggested to keep a copy of log messages, when possible, on a different machine (remote logging).

Other recommendations

Never use setuid scripts. Always use sudo.

Install software that checks the filesystem integrity, like, for instance, *ossec*.

Disable the following services or filter the ports they use:

- echo (7/tcp and udp);
- systat (11/tcp);
- chargen (19/tcp and udp);
- rstat (udp);
- tftp (69/udp);
- rwall (udp);
- ruser (udp);
- discard (9/tcp e udp);
- daytime (13/tcp and udp);
- bootps (67/udp);
- finger (79/tcp);

6 See "**First Backup**".
7 See "**Installation**".

- sprayd (udp);
- pcnfsd (udp);
- netstat (15/tcp);
- who (513/udp).

Periodical checks:

- Verify that network interfaces (ethernet and wireless) are not in promiscuos mode;
- Verify that /dev/mem e /dev/kmem devices cannot be read by all the users;
- Verify that all the devices have root owner, excepts the terminals;
- Verify that the /dev directory does not contain regular files;
- Install a software that can check the file system integrity (File Integrity Monitoring), like *ossec*;
- Verify that there are not files with bits SUID/SGID enabled:

  ```
  find / -type f \( -perm -04000 –o –perm -02000 \) –exec ls –l {} \;
  ```

- Verify that there are not files with unusual names, like "..." (three points) or ".. " (point point space) or "..^G" (point point control-G):

  ```
  find / -name ".. " –print –xdev
  find / -name ".*" –print –xdev | cat -v
  ```

- Verify there are not files with write permissions to everybody:

  ```
  find / -type f \( -perm -2 –o –perm -20 \) –exec ls –lg {} \;
  find / -type d \( -perm -2 –o –perm -20 \) –exec ls –ldg {} \;
  ```

- Verify there are not files without a owner (except inside /dev directory):

  ```
  find / -nouser –o -nogroup
  ```

- Check if there are .rhosts files; if it is necessary to keep them verify they do not contain wildcards or comment lines;
- Verify the users' *umask* (root must have at least 0x22).

APPENDICES

Please refer to the AgID web page https://www.agid.gov.it/en/security/Minimum-ICT-security-measures-for-public-administrations for the minimum ICT security policies for public administrations.