GUIDELINES FOR THE PROPER USE OF SELF-MANAGED PCs AND SERVERS

adopted by the Head of Digital Solutions Service and IT Infrastructure with determination no.04/2024 on February 28th, 2024

Premises and purposes

As part of the FBK Security Project carried out by the Digital Solutions and IT Infrastructure Service in collaboration with the Cybersecurity Centre and following interviews with a sample of researchers to strengthen the security of FBK networks and systems, these "Guidelines for the proper use of self-managed PCs and Servers" have been elaborated, inspired by major national and international standards (such as AGID and IEC 62443) but are also designed to be practical and low-impact in terms of overhead.

These Guidelines, subject to specific and mandatory training sessions, in order to explain in detail the techniques to manage the systems in the best way, reducing the risks to the maximum, **will come into force from February 28th 2024** and must be **attended by all System Administrators of the Foundation**, as defined in art. 12 of the Privacy Regulation, be they PC and/or Server Administrators.

The System Administrator accepts the responsibility for the consequent civil and criminal liability and ensures the implementation of appropriate technical and organizational measures in order to meet the requirements of the GDPR and guarantee the subject's data rights protection and the one FBK is Data Controller of. The aim of these Guidelines is in fact to support the System Administrator in ensuring that the current FBK level of data security is maintained and not decreased.

These Guidelines are composed by:

- Procedure to obtain the qualification for the autonomous management of information tools provided by FBK and assume the role of FBK System Administrator;
- Guidelines for self-managed PCs;
- Guidelines for self-managed Server systems.

Procedure to obtain the qualification for the autonomous management of IT tools provided by FBK and to assume the role of FBK System Administrator

To take on the role of System Administrator it is essential to belong to the Digital Solutions Service and IT Infrastructure (for centrally managed systems) or to the organizational research articulations (for systems managed by research and/or for exclusive scientific research purposes). It is also **mandatory to complete the preparatory and periodic training activity** made available by the Foundation on the FBK Academy platform, in Italian with English subtitles and material. These are **online courses available from April 1st, 2024** that you can follow starting from a few days after you have requested registration.

Specifically, to become a System Administrator of a PC, attendance to the course "Secure PC Self-Management", while to become a Server System Administrator, attendance to the course "Secure Self-Management of Servers" is mandatory. To manage one or more PCs and one or more Servers, attendance of both courses is mandatory. In addition, **all those currently acting as Server System Administrators are required to enroll in the new course and pass the learning test by the end of June 2024**.

The applicant's direct supervisor and the FBK System Administrator (Head of Digital Solutions and IT Infrastructure Service) authorize the self-management of the tool through the participation approval to the compulsory courses.

GUIDELINES FOR SELF-MANAGED PCs

1. CONTINUOUS VULNERABILITY ASSESSMENT AND CORRECTION
    a. Automatically and quickly install software security patches and updates for both the operating system and applications.
        i. Configure devices to automatically and continuously perform operating system and application security updates.
        ii. However, regularly check the availability of new security updates on official channels.
        iii. Verify that the vulnerabilities revealed by the scans have been resolved either by means of patches or by implementing appropriate countermeasures.
        iv. In the event of new vulnerabilities, consider substitute measures, for example using alternative tools to those currently vulnerable, if patches are not immediately available or if the distribution times are not compatible with the risks.

2. APPROPRIATE USE OF ADMINISTRATOR PRIVILEGES
    a. Use administrative users only to carry out operations that require privileges, recording each access performed.
    b. Prevent weak credentials from being used for users, especially administrative ones.
    c. Ensure complete distinction between privileged and non-privileged administrator users, which must correspond to different credentials.
    d. Anonymous administrative users, such as "root" in UNIX or "Administrator" in Windows, must be used only for emergency situations and the related credentials must be managed in such a way as to ensure the accountability of those who use them.
    e. Store credentials to ensure availability and confidentiality using, for example, a password manager.
    f. If public and private keys or passkeys are used for authentication, it is recommended that the private key is adequately protected (with appropriate permissions and a password request each time the private key is used) and is never shared or communicated to others.

3. DEFENSES AGAINST MALWARE
    a. Install tools to detect the presence and block the execution of malware. These tools must be updated automatically.
    b. Activate the existing firewall systems.
        i. Use filtering tools that operate across the entire network traffic flow to prevent malicious code from reaching your PC.
        ii. Use anti-malware tools that exploit, in addition to signatures, detection techniques based on behavioral anomalies.
4. SAFETY COPIES
    a. It is recommended to use tools that allow you to not have work data on the PC, especially sensitive data, for example FBK's Google or Microsoft drives for data, browser for reading mail, etc.
    b. If this is not possible and there is work data on the PC, it is mandatory to:
        i. periodically make a backup copy of the information strictly necessary to avoid data loss;
        ii. encrypt your PC disk.

GUIDELINES FOR SELF-MANAGED SERVER SYSTEMS

1. DEVICE AND SOFTWARE INVENTORY
    a. Implement an inventory of active resources, updating it when new devices are connected to the network.
        i. Manage the resource inventory of all systems connected to the network and the network devices themselves, recording the IP address, machine names, system function, and the administrator responsible for the resource.
        ii. Qualify systems connected to the network through the analysis of their traffic.
    b. Maintain an inventory of software installed on Servers, such as recording software name, version, manufacturer, available licenses, installation date, license expiration date, license status, etc.
        i. Perform regular scans on your systems to detect the presence of unauthorized software.

2. PROTECT HARDWARE AND SOFTWARE CONFIGURATIONS ON SERVERS
    a. Use standard secure configurations to protect operating systems.
        i. Standard secure configurations must match the hardened versions of the operating system and installed applications. The hardening procedure typically includes: deleting unnecessary accounts (including service accounts), disabling or deleting unnecessary services, applying patches, closing open and unused network ports.
    b. Define and employ a standard Server configuration.
        i. Use systems configuration management tools that allow you to restore standard configuration settings.
        ii. Any operating systems that are compromised must be restored using the standard configuration.
        iii. Changes to the standard configuration must be made according to change management procedures.
        iv. Regularly ensure the validation and updating of the installation images in their security configuration also taking into account the most recent vulnerabilities and attack vectors.
        v. The installation images must come from official sites and be validated with the procedures made available by the supplier.
    c. Perform all remote administration operations of Servers, network devices and similar equipment via protected connections aligned with the most recent security standards (e.g. AES, SHA256, TLS >=1.2, RSA keys of at least 2048 bits).
    d. Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered.
    e. Implement “logging” of Server operations.
        i. To support analytics, the reporting system must be able to show the history of configuration changes over time and identify who made each change.
    f. Use, when possible, “Infrastructure as code” solutions for the deployment of infrastructure and applications.

3. CONTINUOUS VULNERABILITY ASSESSMENT AND CORRECTION
    a. For each significant configuration change, perform a vulnerability search on all networked systems with automatic tools that provide each system administrator with reports indicating the most critical vulnerabilities.
    b. Periodically scan for vulnerabilities commensurate with the complexity of your infrastructure.
    c. Verify that logs record the activities of vulnerability scanning systems
    d. Bind the source of vulnerability scans to specific machines or IP addresses, ensuring that only authorized personnel have access to that interface and use it properly.

e. Ensure that the vulnerability scanning tools used are regularly updated with all relevant security vulnerabilities.
f. Sign up for a service that provides timely information about new threats and vulnerabilities, using them to update scan tasks.
g. After ensuring that patches do not cause problems or disruptions in production systems, for example by using a test environment, automatically and quickly install software security patches and updates for both the operating system and applications.
h. Verify that the vulnerabilities revealed by the scans have been resolved either by means of patches or by implementing appropriate countermeasures.
i. In the event of new vulnerabilities, consider alternative measures, for example blocking access from the outside, if patches are not immediately available or if the distribution times are not compatible with the risks.

4. APPROPRIATE USE OF ADMINISTRATOR PRIVILEGES
    a. Limit administrative privileges to only users who have the appropriate skills and operational need to modify the systems configuration.
    b. Use administrative users only to carry out operations that require privileges, recording each access performed.
    c. Assign to each administrative user only the privileges necessary to carry out the activities foreseen for it.
    d. Record the actions performed by an administrative user and detect any behavioral anomalies.
    e. Maintain the inventory of all administrative users, ensuring that each of them is duly and formally authorized, periodically checking their real need.
    f. Before connecting a new device to the network, replace the default administrator credentials with values consistent with those of the administrative users in use.
    g. Track failed login attempts with an administrative user in the logs.
    h. Use multi-factor authentication systems for all administrative access, including domain administration access. Multi-factor authentication can use various technologies, such as smart cards, digital certificates, one time passwords (OTPs), tokens, biometrics, password keys and other similar systems.
        i. When multi-factor authentication is not supported, use highly robust credentials (e.g. at least 14 characters) for administrative users.
    i. Prevent weak credentials from being used for administrative users.
    j. Ensure that administrative user credentials are replaced frequently enough where multi-factor authentication is not supported.
    k. Prevent credentials that have already been used from being reused in the short term (password history).
    l. Ensure complete distinction between privileged and non-privileged administrator users, which must correspond to different credentials.
    m. All users, in particular administrative ones, must be nominative and traceable to a single person, except for technical users connected to applications or services.
    n. Anonymous administrative users, such as "root" in UNIX or "Administrator" in Windows, must be used only for emergency situations and the related credentials must be managed in such a way as to ensure the accountability of those who use them.
    o. Store administrative credentials to ensure availability and confidentiality using, for example, a properly configured and periodically reviewed password manager.
    p. If keys are used for authentication, it is recommended that the private key is adequately protected (with the appropriate permissions and with a password request each time the private key is used).
5. DEFENSES AGAINST MALWARE
    a. Install tools on all systems to detect the presence and block the execution of malware. These tools must be updated automatically.
    b. Activate the firewall systems on the Servers.

i. Use filtering tools that operate across the entire network traffic flow to prevent malicious code from reaching hosts.
ii. Use anti-malware tools that exploit, in addition to signatures, detection techniques based on behavioral anomalies.

6. SAFETY COPIES
    a. Make a backup copy of the information strictly necessary for complete system recovery at least daily.
        i. To ensure a system's ability to recover from its backup, backup procedures must cover the operating system, software applications and data.
        ii. Make sure that the media containing at least one of the copies are not permanently accessible by the system to prevent attacks on it from also involving all its backup copies.