HACKER COMBAT
COMMUNITY

HUMAN FACTOR

HUMAN FACTOR IN CYBER SECURITY: OVERVIEW

HACKER COMBAT

Human Factor in Cyber Security: Overview

Human errors are circumstances in which planned actions, decisions or behaviors reduce — or have the potential to reduce — quality, safety and security.

Human factors in cyber security are often the cause for security breaches. Here are some solutions to reduce risk and build a threat prevention strategy

A company can spend all the funds it wants on the latest cyber security technology, like firewalls, threat detection, artificial intelligence, and machine learning tools, but there is one security risk that can't be blocked from entering the company networks: **the employee.**

INTRO

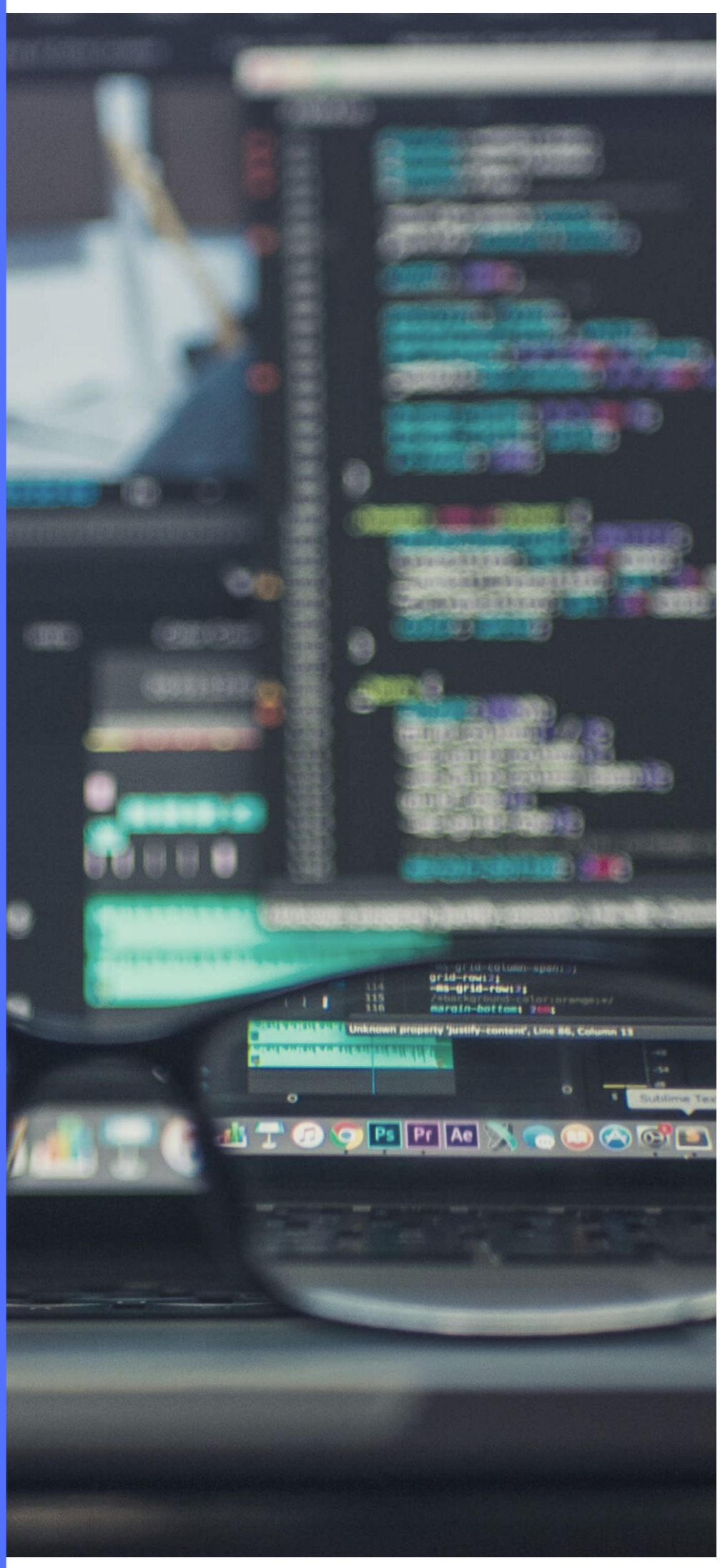
The implementation of adequate computer security measures requires contemplating technical, organizational and legal aspects, however, in many cases very little attention is paid to the importance of the human factor in computer security.

People represent the weakest link in computer security, unlike computers, people may not follow the instructions exactly as they were dictated, in addition, they may carry out actions that provoke a security hole in the network of the organization such as the installation of malicious software on your computer, disclosure of sensitive information to third parties, among others.

The main experts in IT security have already warned us in recent years about the need to consider the human factor as one of the most important and decisive when implementing a good information security management system.

HACKER COMBAT COMMUNITY

Implementation of a Computer Security Management System should consider the human factor as one of its key elements, contemplating aspects such as:



01 **Implementation of computer security measures**

02 **Adequate training and awareness of employees**

03 **Involvement of managers and team members**

04 **Approval of internal regulations on the use of computer tools in the organization**

05 **Any other measure of positive contribution**

Follow us

Visit

Hackercombat.com

Actions or good practices to be executed are:

PROPER USE OF EMAILS:

The way to ensure that the exchange of information is carried out properly and under the necessary protection is through the development of a policy that includes the means used in this activity. In this policy should be incorporated:

- The procedures defined to correctly manage the system.
- Use of electronic signature.
- Checks through controls that prevent unauthorized modifications, interpretations, duplicates or elimination of information.
- Inspections of protection against malicious code.
- Social engineering methodologies.

Rigorous Staff Selection

As established by ISO 27001, checklists have to be carried out before all the candidates for employment, contractors and third parties are present.

It must be found in accordance with current legislation and ethics, the checklist must take into account privacy, the protection of all personnel data and employment must be based on the following:

- The availability of satisfactory references on all attitudes, such as one of the personnel and another of the company.
- The verification of the candidate's Curriculum Vitae.
- Confirmation of academic and professional certification.
- The company has to consider making a much more detailed check over time, when a person accesses a job, with an initial contract, taking into account the resources needed to process the information and in particular it is about sensitive information, that is, financial information.

Rigorous staff selection (continuation):

The functions and obligations of each of the different people who have access to the data and services of the information system of an organization should be clearly defined at all times.

These measures affect the different groups that may have access to the services of the system and computer network of the organization:

- Administrator of the system and the computer network
- Application developers
- Technicians responsible for the maintenance of equipment and the computer network
- End users of the system
- Managers
- External personnel: service companies that have access to the computer resources of the organization.

Practical Standards

- Each team assigned to a job will be under the responsibility of one of the authorized users in the computer system of the organization.

- Before leaving the workstation team, either temporarily or at the end of your work shift, you must cancel all active sessions and connections with the corporate network servers.

- Use a password-protected screen saver. Lock the machine when moving away from it.

- Prevent other users from using their identity to access the computer system.

- Do not insert CD-ROMs, USB or other means without prior checking that they do not contain any risks.

- The configuration of the equipment will not be changed nor will it be attempted to solve possible operational problems. In this case, the person in charge of the maintenance of the equipment must be informed immediately.

Practical Standards (continuation)

- Only the corporate tools will be used, being prohibited the installation of any software in the computers of the company that has not been expressly authorized.

- Discs and documents with sensitive information should be kept under lock and key.

- In the case of printers, make sure there are no printed documents in the output tray that contain protected data or other sensitive information.

- Should be informed of any incident that could affect the security of the computer network or the normal operation of the system.

- The computer equipment and means of the organization can not be taken out of the organization without the corresponding authorization of those responsible.

- Access to the Internet will only be limited to professional purposes.

Confidentiality Agreements

A confidentiality agreement or non-disclosure agreement is a legal contract between at least two entities to share confidential material or knowledge for certain purposes. This includes the following:

- Inclusion of security within contractual responsibilities.
- All the terms and conditions of the worker must reflect the company's policy in addition to clarifying the following terms:
- All employees, contractors and third parties who have been granted access to sensitive information must sign a confidentiality agreement, as they can not disclose the access to information processing facilities.
- The responsibilities and rights of subcontractors, for example in relation to all legislation on the protection of personal data.
- The responsibilities of the classification of information and asset management that are associated with the Information Security Management Systems and the services that are used by the worker or the subcontracted company.
- The responsibilities of the workers or third parties necessary to maneuver with the information that the companies receive.
- All responsibilities on the part of the company to inform the staff, which includes information used by the work carried out by the organization.
- The responsibilities extend beyond the hypotheses established by the organization and that are outside the normal working period.
- The actions taken if the worker or contractor does not comply with all the requirements established for the Information Security of the organization.

PARTNER WITH US

LET'S GROW YOUR BUSINESS

Together!

Sign Up Link Given In the Comments!

HACKER COMBAT
COMMUNITY

Follow us!

Find us Online