SECURITY SECURITY II: Security Policy Account for Computer Security Account Policies

In the previous section I introduced common methods to protect an organization's computer. In the next part, I will present the specific methods in order, from the process of setting up the system, operating the system based on the safety policies from basic to the advance skills that the Admin Security should care about. to apply to building information security processes for organizations ...

HOW TO PROTECT THE COMPUTERS OF AN ORGANIZATION

Part 2: Account Security Policy for Computer (Security Account Policies)

In the previous section I introduced common methods to protect an organization's computer. In the next part, I will present the specific methods in order, from the process of setting up the system, operating the system based on the safety policies from basic to the advance skills that the Admin Security should care about. to apply to building information security processes for organizations. In this presentation, I would like to mention account security (account security) and how to create a secure account to deal with very popular and effective attacks with the help of witchcraft tools .

Poor account policies and account creation methods are the easiest way for an attacker, so other forms of security are applied to the system such as anti-maleware tools (preventing viruses, worms, spyware, ad-ware .), deploying defense system Network (Firewall) will not have any significant effect, because Admin is too indifferent in how to create an account and create account creation policy containing many risks. .

It is required to identify policies to create strong passwords and to create account security strategies applied to information security of organizations.

A. How to create and manage a secure Account

The following factors will show us how to create and manage Accounts safely

1. Account must be protected with a complex password (password length, password complexity).

2. Account holders are only allowed to access necessary information and services (without lack of authority and cannot be left over).

3. Account encryption in Internet transactions (including transactions in the Local Area Network)

4. Store accounts securely (certain databases store accounts that must be placed on secure and encrypted systems)

5. Train employees, those who directly use Computer security to avoid leakage (attacker can take advantage of the relationship with employees or pretend technical department to support troubleshooting system remotely to exploit), guide how to change the password when necessary and absolutely avoid recording the account on stick-notes and indiscriminate cockroaches on Monitor or Keyboard .), Lock right at Computer when not in use, By default on computers, there is usually an automatic policy to lock the computer after a period of no use, to help employees who forget to avoid elementary security errors (this error is like leaving the house without locking door)

6. Account creators and managers (especially system ***accounts*** - ***System accounts*** , and active accounts, controlling services - for ***service accounts***) for the entire organization are those who are considered **SAFE ABSOLUTELY** .

7. Disable unused temporary accounts, delete unused accounts.

8. Avoid sharing the same Password for multiple accounts

9. Locking the account after a number of times the user log-on failed the system.

10. Some system and service administration accounts may not be allowed, remote location log-on is not allowed, because these systems and services are very important and usually only allowed to be checked Control from inside (internal Network), if there is a need for administrator and remote support Security Admin still easily change the policy to meet the needs.

11. The admin security when logging on to the server should only use an account with low authority, when it is necessary to administer or operate the service, it is recommended to use the ***System*** or ***Service*** account (eg Microsoft Windows supports command *run as* through *run as service* to independently administer system components, services without having to log-on to the original machine with an admin account). This helps us to avoid dangerous programs that have entered the computer running with admin rights, when Computer's real administrators get into trouble.

12. Patch all system holes to prevent 'escalating privilege' attacks (start entering the system with a normal account and then escalate to the highest right)

13. The above are the most intuitive parts that Admin Security needs to visualize when designing security policies (account security policies). One of the system protection policies needs to be carefully reviewed, but it is usually easy to neglect or even overlook, the fact that most roads enter the system through the Credentials exploit (available through believe account), attacker grasp this vulnerabilities, so take

advantage of exploitation very effectively.

B. Analyze and design safety policies for accounts.

Analyze risks and identify threats to accounts :

The Account for a User determines the actions that the User can perform.

The classification of accounts will indicate different levels of protection.

Account type

Reliability

For example

External users

Low

User accesses Web server (anonymous user), business partners .

Internal staff

Medium

Contract staff, official staff .

Administrator group

High

System administration rights, services, organizational data .

Accounts on the system will receive 2 basic rights :

1. **User rights** : A type of privilege that a User is allowed by the system to perform special actions (eg: Right to Backup Files and Folders, change system time, system shutdown .).

2. On Windows you can type command ***secpol.msc*** at RUN, to open ***Local Security Settings local policies User rights assignment*** is the place where the system ***rights*** are set.

3. Permissions: Controlled by the system's ***DACLs (Discretionary access control lists)*** , allowed to access files / folders or Active Directory objects (in Domain) (eg User A is entitled to Read / Modify for with *C: Data* Folder, User B is Full Control for *Business* OU .).

4. Note in the allocation of Permission for the account, should put the account into the Group to easily control, avoid the decentralization of personal rights to a certain account. This enhances account control, because as the number of system accounts (Local or Domain) increases, this organization makes it more secure and easy to control.

Loopholes from Account can create an opportunity for an attacker :

Password:

1. The password is too weak (the password length is too short, the characters are simple, take the date of birth, the names of movies, place names, famous characters, set the password).

2. Use the same password for multiple accounts. The password is randomly assigned to Monitor / Keyboard, or save the password to an unprotected text file.

3. Share your system password for colleagues .

Privilege allocation:

1. Issuing Administrator privileges for Users.

2. System services do not use Service account.

3. Issuing User right is not required for the account.

Account usage :

1. Log-on to the machine with the Administrators account when performing common tasks.

2. Create user accounts that allow administrative rights to other accounts. Activate accounts that are no longer used (for example, employees who have retired, accounts still circulated on the system .)

Designing a password generation policy to ensure security for Account :

1. The policy of creating a password for security is one of the main factors to protect your account. This policy includes the following key elements:

2. Maximum password age: Maximum expiry date of the password before the user has to change the password. Changing your password periodically will increase your account security.

3. The minimum password time must be used before changing the minimum password age. Admin can set this time for a few days, before allowing the user to change their password.

4. Execute password history: The number of times different passwords must be used, before returning to the old password. The higher the number of Password history, the greater the security.

5. Minimum password length must be set. The longer it is, the safer.

6. The password must meet the complex requirements: not only in length but also in the complexity of the password set characters (for example, you can see the difference between the *password* and *P @ ssW0rd).*

7. When using a complex password, care:

8. Do not use first and last names

9. Contains at least 6 characters

10. You can mix uppercase, (A.Z) often (a.z), and special characters such as:! **@ # $% ^ & * ()**

11. Account lockout: Account will be locked for a certain period of time, if after some time log-on fails on the system. The purpose of this policy is to prevent brute force attacks on accounts to detect passwords.

The above are the core issues in creating and managing Account so that it is safe to meet the strict requirements of the organization's information security policy and for the Security Admin to think about this issue. should be negligent or indifferent, because this is the first 'entry' that attackers always prioritize in exploring and exploiting weaknesses of the system.

Article posted:

How to secure an organization's computers - **Part I**

New Horizons VietNam (New Horizons Computer Learning Centers)
Ho Viet Ha
Instructor Team Leader

Email: hvha@newhorizons.com.vn