Global Information Assurance Certification Paper

Ernestine Poling
SANS Security Essentials GSEC Practical Assignment Version 1.3

Centralization of Account Provisioning:

Improving the Present and Planning for the Future

Introduction

Account Provisioning is defined as generation and maintenance of user accounts for platform and application access. This paper defines the reasons that centralization of account provisioning can improve security. It will outline the steps to be taken to develop and maintain centralized security within a Security Administration team:

1. Define the purpose of the Security Administration team
2. Identify Data and System "Owners" and Form Partnership
3. Define Risks
4. Review/Define Account Security Policy
5. Audit

and will briefly discuss how, once established, it can be used to aid in a future implementation of commercial account provisioning solutions.

Why centralization?

How does a new employee obtain access to applications and platforms in your organization? How long does it take to obtain this access? How confident are you that the access given to the employee is appropriate for the performance of his/her duties? What safeguards are in place to ensure that access is removed when the employee separates from the organization? Is access audited to ensure that it is appropriate and necessary for the employee's current position? How easy will it be for you to comply with governmental regulations? Do you have a way to audit the access requests? Are you following best practices for managing your information assets?

Unfortunately, application and platform access is often the most overlooked piece of the security puzzle. Companies employ perimeter defenses, may conform to the Center for Internet Security's (CIS) Benchmark security configuration[1], maintain up-to-date antivirus software, develop disaster recovery procedures, and even maintain a secure physical environment but often overlook this vital area of security.

In lieu of centralized security administration, systems access provisioning is usually divided among many groups including: network and systems administrators, developers, DBAs, and even end users. Although these teams do have an involvement with security, granting user access to systems is often a low priority, employees on the teams usually do not have security training, and procedures for granting access is not standardized and as a result is usually lax. Centralization can enable these teams to concentrate on *their* areas of competence and provide for standardization of security policy within a trained Security Administration team.

In her ZDNet News guest commentary, Eli Primrose-Smith states that "Companies must take a total enterprise approach" to integrate IT activities "into a holistic corporate security solution[2]." Centralization of account provisioning is one part of the enterprise approach, ensuring that security policies are uniform throughout the organization.

Step 1: Define the Purpose of the Security Administration team

The first step in developing a Security Administration is to define the purpose and scope of the Security Administration team. From that definition, a mission statement can be developed. For the purposes of this paper, the statement is defined as:

> The mission of the Security Administration team is
>
> - to manage access to all computing systems and applications within the organization and
> - to ensure that employees are given timely access to the information and systems *required* to successfully perform their jobs
> - while safeguarding the data and systems resources of the organization in accordance with the organization's security policy.

This mission statement should be broad enough to cover account provisioning as well as auditing. Auditing of systems access and event logs should be an integral part of the organization's security program.

Step 2: Identify Data and System "Owners" and Form Partnership[3]

It is necessary to determine the data and systems owners because information security cannot be defined unilaterally. These owners will ultimately partner with the Security Administration team in analyzing risks, approving the policy, and later in review of access levels. For example, the Human Resources function owns the data within the HR application and an owner or owners should be identified from the function, with the knowledge and authority to help define systems access policies. This should be done for all applications and systems. Data owners include not just the obvious – the functional (or business) owners such as Human Resources, Finance Department, Marketing Department – but also systems administrators, Internal Auditing and Legal.

The Internal Auditing function is responsible for ensuring the resources of the organization are used in a safe manner and with ensuring that proper safeguards are in place to protect the resources. Internal Auditing can also assist in the determination of appropriate separation of duties. For example, an employee should not have the ability to both pay bills and reconcile the bank statement. If the Finance Department approves giving both of these abilities to the same

person, Security Administration has a responsibility to ask for a review of the request from Internal Auditing.

The Legal Department is responsible for ensuring compliance with governmental regulations such as the Health Insurance Portability Act (HIPAA) or Gramm-Leach_Bliley (GLB) as well as ensuring that the organization's security policy and practices do not needlessly expose the organization to possible lawsuits.[4]

The Security Administration team may be thought of as the "hands" of the data owners. Recognizing that they are the proxy owners of the data and systems, it is important to develop a line of communication with the actual owners. Without communication, it is not possible to build a partnership and establish trust between the teams. Without partnership, the Security Administration team will be unable to develop a good security model because they need the expertise of the data owners.

Lastly, to ensure that systems access is centralized in the Security Administration team, it is important to ensure that data owners with rights to assign systems access do not give that access to anyone. For example, systems administrators of an NT domain obviously have sufficient rights to create accounts but will defer to the Security Administration team. Although communication and building a partner relationship with the data owners can help ensure that control remains within the Security Administration team, periodic audits of accounts are necessary to ensure that accounts are not created by others.

Step 3: Define Risks

Once the data and systems owners are identified, the Security Administration team should begin the risks analysis. This analysis should be reviewed by the data owners and is the precursor to developing the team's security policy.

Some potential risks are:

- Unauthorized requests
- Inappropriate requests
- Account obsolescence
- Inactive accounts
- Temporary or contractor accounts
- Test accounts
- Physical Security
- Confidentiality
- Requests to access another employee's account(s)
- Passwords
- Lack of system timeouts

Risks should be listed and periodically reviewed in order to develop appropriate policies for all known or perceived situations.

Step 4: Review/Define Account Security Policy

With the risks defined, the Security Administration team should consult with the owners to define the departmental policies and procedures to mitigate these risks. A sample of policies that address the risks identified above is shown in the table below. Note that most of the policies are broad in scope and are intended as examples from which to define your specific policies.

- Unauthorized requests

  All requests for systems access must be submitted to the Security Administration team by the employee's manager (approved requester).

  Requests from an approved requester for access to certain sensitive systems (these should be named) must be submitted to the data owner for approval and/or identification of appropriate level of access

- Inappropriate requests

  The level of access granted to each employee is based upon their job title and predefined "normal" systems access. (Security Administration must work with data owners to define this "role based" security.)

  Requests from an approved requester for access other than that which is considered normal will always be submitted to the data owner for approval.

  Requests for "generic" or "unowned" accounts (such as one account for a department or facility) will require a stated business case and review by the Security Administration manager, the data owner and Internal Auditing.

- Account Obsolescence

  Security Administration is responsible for timely deletion of all systems access for separated employees. (NOTE: In some instances, it may be necessary to inactivate an account instead of physically deleting it. The home share of a separated associate and/or e-mail account may be required to maintain business continuity or for legal reasons.)

  Security Administration is responsible for changing systems access for an employee who changes jobs or locations.

  Security Administration is responsible for auditing accounts on all systems and applications to ensure compliance with policy.

- Inactive Accounts

  Security Administration is responsible for auditing login dates to determine if an account is inactive. If an account has been inactive for six months, it will be removed from the system.

- Temporary or Contractor accounts

  If temporaries and contractors are not maintained in the HR system the accounts are to be set up to expire after 90 days. Extensions of these accounts should be for no more than 90 days per extension. Managers of these employees are to notify the Security Administration team as soon as the end of employment is known.

- Test Accounts

  All requests for test accounts must include a business case for creation and must be submitted by the department to the Security Administration manager and will be subject to review by the data owners and Internal Auditing.

  Any test accounts that are created will have an expiration date and must comply with password policies.

- Physical Security

  The Security Administration team must ensure that their workstations are either logged off the network or are locked when they are unattended.

  Team members with laptops may not leave them on their desk when leaving work for the day or weekend unless secured with a lock or cable to a solid object or locked in a cabinet.

  When removing a laptop from work, care must be taken not to leave the laptop in open view in their car or otherwise unattended.

  Security Administration will ensure that all confidential electronic documents remain within the control of the team and do not go to outside parties other than data owners or authorized approvers.

  Any paper copies of electronic documents are to be kept in a locked cabinet or, when no longer required, must be shredded.

- Confidentiality

  All Security Administration team members must sign a confidentiality agreement.

- Requests for access to another employee's accounts

  Access to another employee's accounts is prohibited except as provided below:

  In the event of an employee's separation, the employee's manager may submit a request to the Security Administration manager for access to the separated employee's files and e-mail for the purposes of ensuring business continuity.

  Requests for access to an employee's accounts who has not separated from the organization must be submitted to the Security Administration manager and will then be reviewed by the Legal Department and/or Internal Auditing.

- Passwords

  Where possible, password policy on systems must require a combination of letters, numbers, and special characters and be at least eight characters in length (password lengths may vary in length depending on the organization but all should contain a combination of characters and numbers and may also include upper and lower case).

  Where possible, all passwords should have expiration dates.

- Lack of system timeouts

  Where possible, system timeouts will be employed to ensure that users are logged out of applications and systems after a period of inactivity.

Once the security policy is defined, "role based" access privileges should be determined. A discussion of how to implement role based access privileges is beyond the scope of this document. Simply put, role based access privileges can be defined at a high level as a set of applications or platforms to which a group of employees should have access, or an "organizational role." This model also plays a part in developing security within applications and platforms. Where possible within the platforms and applications, "access roles" should be used to assign rights to resources and data.

For example, an HR Manager organizational role could include an e-mail account, a Windows NT logon, access to the HR application and access to the Financials application. In this example the access roles would be as follows:

- the Windows NT logon would include access to general HR folder on the file server through membership in the HR group as well as access to the HR Managers folder through the HRMgr group
- within the HR application, manager's access would be a combination of roles within the HR function-including the access role assigned to HR clerks which grants access to the functions and data required to perform their tasks and an additional access role with manager access to actions or features that are outside the job duties of the clerks
- access to budgeting within the Financials application would be assigned using the standard budgeting manager access role

Role based access privileges benefit the organization through elimination of user-specific access. Care must be taken not to develop too many roles or to develop overlapping roles. Overlapping roles can be eliminated by combining multiple roles as was described above for access within the HR application.

Obtain Approval of Policy

After the policy has been written, it should be reviewed with the data owners who have helped to define it, to ensure that it meets their expectations. At that time they should sign off on the policy and recommend adoption.

Once the data owners have recommended adoption of the policy, it should be submitted to Security Administration's function head, the CSO (if the organization has one), and Executive Management according to your organization's practices. During the approval process, revisions may need to be made and if made may involve sending the policy back to previous approvers.

Once approved, the policy should be published so all employees can review it. Although the policy "belongs" to the Security Administration team, it impacts all employees so should be posted in a public place (such as the organization's Intranet).

Step 5: Auditing

In addition to the normal audits performed by both an Internal Auditing staff and external auditors, the Security Administration team should perform their own audits. These audits should be a part of the daily routine and should consist of compliance to policy, review to determined orphaned or inactive/unused accounts, and review of event logs. Auditing should also include periodic review of security policies and rules to ensure that they comply with current requirements. Periodic review of roles should be undertaken with the assistance of the data owners.

Account Provisioning Solutions

A benefit of centralizing account provisioning within one team is that the organization will be better able to know the costs involved with the process. It will become apparent that staffing levels will need to increase due to more applications and platforms that must be managed as well as mergers and acquisitions. However, staffing levels often do not keep pace. This results in delays in obtaining access, delays in removing access, and human error. Most likely prioritization will be given to granting access and less to removal. There may be little or no time for auditing. Companies can continue to hire more administrators, but there is a better solution.

An account provisioning solution can relieve the administrators of most the account provisioning process. It can include workflow to manage access requests and approvals that in a manual process often produce delays. When deployed with good policies and rules, service levels are improved, security holes are closed, administrative costs are reduced, and the organization's potential legal liabilities may be reduced. When combined with a meta directory, the result is a total identity management package that will allow the organization to leverage an existing HR system to create a single trusted data source. Add single sign-on to the mix and one of the biggest weakness in password-based security is greatly improved-that of managing multiple accounts and remembering the passwords associated with them.

Conclusion

Centralization of systems access responsibilities benefits the organization by providing increased security over its information resources through a trained and clearly-focused team. This increased security is realized through

- Separation of duties so that systems administrators, DBAs, and others can concentrate on their areas of expertise
- Cross-functional communication to ensure that security is developed appropriately
- A single policy or standard in place for systems access procurement
- Demonstrable compliance with best practices

In addition to increased security, centralization benefits the end users because they will receive more timely access to systems and they only need to remember one department to contact for systems access requests.

Training of the Security Administration team is *essential*. This training should include more than just "security" training but should also include a working knowledge of the systems and applications to which the team provides access.

Centralization can be a step toward account provisioning solutions and single sign on. If looked at closely, account provisioning is centralization at its utmost. Defined policies and rules ensure compliance with security policy and provisioning is accomplished through one source. The guidelines within this paper will ensure that the organization is well-positioned to implement these solutions because the business process, security policies, and roles have been defined. In other words, the homework will have already been started.

List of References

[1] *The Center for Internet Security Home Page.* URL: http://www.cisecurity.org/ (24 March 2002).

[2] Primrose-Smith, Eli. "Facing the new corporate security rules." *ZDNet News* 8 March 2002. URL: http://zdnet.com.com/2100-1107-855323.html (24 March 2002).

[3] Kolb, Garry. "Melding Security & Customer Service." *The Encyclopedia of Computer Security Papers.* 5 November 2001. URL: http://www.itsecurity.com/papers/garykolb.htm (24 March 2002).

[4] Scalet, Sarah D. and Berinato, Scott. "The ABCs of Security." *CIO Security* 20 February 2002. URL: http://www.cio.com/security/edit/security_abc.html#keys (24 March 2002).

"10 Tips for Creating A Network Security Policy." *eWeek.* 22 October, 2001 URL: http://www.eweek.com/article/0,3658,a=16846,00.asp (24 March 2002).

"Business Security Tips." *techtv Cybercrime.* 27 July 2001. URL: http://www.techtv.com/cybercrime/internetfraud/story/0,23008,2127598,00.html (24 March 2002).

"Improving Security." *ID-SYNCH.* http://idsynch.com/about/security_prob.html (24 March 2002).

"ITL Bulletin: Risk Management Guidance for Information Technology Systems." *National Institute of Standards and Technology (NIST) Computer Security Resource Center.* February 2002. URL: http://csrc.nist.gov/publications/nistbul/02-02.pdf (24 March 2002).

"Mistakes People Make that Lead to Security Breaches." *SANS Institute Resources.* 23 October, 2001. URL : http://www.sans.org/mistakes.htm (24 March 2002).

Swanson, Marianne. "Guide for Developing Security Plans for Information Technology Systems." *National Institute of Standards and Technology (NIST) Computer Security Resource Center.* December 1998. URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF (24 March 2002).

"Top Ten Tips for Preventing Cyber Sabotage." *Access360 Home Page.* URL: http://access360.com/pdf/topten_cybersabotage.pdf (24 March 2002).