Global Information Assurance Certification Paper

Managing Administrative Authority

GIAC Security Essentials Certification Practical, Version 1.4b

By: Peter Hoff
March 19, 2004

Abstract

Change can quickly create vulnerabilities close to the core of an organization's technical infrastructure. One of those vulnerabilities is the administrator. Therefore, management of the administrators is a requirement when developing an effective Information Security program. However, this task is given little thought in many organizations. From the perspective of Information Security, growth of the information technology infrastructure can leave a sour taste in the mouths of auditors and security professionals' alike. Examples of common pitfalls are a lack of dual controls for administrators, over zealous implementation of administrative privileges or a lack of procedural controls to name a few.

This document is a roadmap to improving the controls over administrative privileges and providing a program for enhancing administrative awareness of security. Although this is one specialized area of the security infrastructure, the steps below will substantially add to a defense in depth. Hopefully, this document will expand one's perspective of the security holes that exist with administrators. The result should provide assistance in developing a program that will improve overall security and increase manageability of the administrative privileges.

Background

Looking back upon the history of Information Technology, the Administrator has been revered as the know-all of technology. When discussions of security arise, they are generally focused upon securing the systems and infrastructures from the outside world. The other concern is to protect the internal systems from rogue internal employees. Obviously, without those controls technology would probably not exist. But there is another area of concern.

Various surveys continue to indicate that internal threats account for more than half of the security concerns within the corporate world. Internal threats can come from anywhere such as a human resources employee modifying personal records, corporate espionage or even identity theft. In the case of internal administrators, the threat is much greater because they have access to systems and applications throughout the IT infrastructure. However, the threat is not only what actions the administrators take, but also the threats outside of the organization that can effect what actions they take. Professional hackers can and have been successful in gaining administrative user credentials through Trojan horses and numerous other viruses. Without segmentation of administrative privileges there is nothing that protects from the inadvertent or unknown catastrophes.

The fact remains, many times the administrative users are not as stable and trustworthy as management would hope. If it were, the prisons would be empty and we would not need agencies with computer crime units such as the FBI, CIA, state and local law enforcement.

Key Objectives

1. Identify a program that limits administrative privileges for users with administrative requirements to only those systems and information that is required to complete job-related tasks.
2. Segregate administrative access according to function, process and system in order to eliminate conflicts of interest and enable dual controls.
3. Identify controls that will persuade administrative users to remain honest.

Identifying the Risks

As a general rule, access should never extend beyond the minimum requirements to complete a task. This can be referred to as the Principle of Least Access. This is a simple concept when applying to users in segmented job categories. The personnel department only has access to their files and the databases that house the personnel records, and to take it a step further, they even limit access to certain areas within the database. Also for good measure, there is an audit trail for everything that occurs within their personnel database. The problem lies with the fact that the administrator has access to the entire system, application front end and the database with all of its information. In addition, the administrator probably has access to the payroll system also. This can very quickly create a conflict of interest. If an administrator has access to both the personnel system and the payroll systems, they can create a fictitious employee and pay them a salary. In an organization that utilizes temp employees frequently, this would be very difficult to catch.

So why should the restrictions for the administrative users be any different? The answer is fairly complicated. As stated earlier, there is a history of IT administrators locking down the environment for everyone else. Administrators are accustomed to meeting tight deadlines and getting the job done. In most cases there's little time set aside to lock down the administrative privileges. Reasonably speaking most administrators are also responsible for identifying the project plans and timelines, which explains why time is not set aside to identify conflicts of interest and security holes pertaining to their access. Besides, from the administrators perspective "they're not a security problem, they can be trusted. They setup the systems in the first place." The subject of locking down and segregating the administrative privileges can be difficult. Most small to medium-sized companies have no controls in place to implement security as part of the System Development Life Cycle (SDLC).

Make Security a Priority from Day 1

The very first step in accomplishing an effective security program for your administrative users is in the posture of the organizational policies. Begin by communicating the desired culture through well-written policies and follow up with management's enforcement and support of those policies. Policies provide a roadmap for how the organization expects the administrator to complete their tasks and a reasonable definition of acceptable behavior and ethics. This will be an on-going process due to

growth and change. According to CIO, Dave Swartz of George Washington University, "Policy is a great vehicle, of course you have to be ready to enforce the policy, and that's the problem." [1] Enforcement of the policies can be difficult without consistent support of their directives and an unforgiving adherence to the goals of those policies.

If there are no policies or policy enforcement, over time a culture will develop that is not necessarily conducive to a strong security model. Administrators and users alike will create what they believe is acceptable security practices. As an example, a user may call the help desk to inquire why they can't get into their e-mail. The help desk takes the call and opens an incident for an administrator to look into the problem. While the employee is at lunch, the administrator with uninhibited privileges opens the users e-mail to make sure that everything is working properly. While this is taking place, he "accidentally" reads a confidential email pertaining to the demise of one of his peers. The outcome of this example can go anywhere with a little imagination. However, these types of incidents are very common and it is due to the culture. The administrative culture can easily exclude themselves from the most basic security and privacy issues. This is a pitfall of always allowing full permissions; many times administrators take it upon themselves to create a culture. Once the culture is established they may take it personally when access is restricted. Restricting the administrators is a delicate process that can be implemented through careful communications and a little training. Just remember, changing the culture is much more difficult than establishing the culture from the beginning.

Some Suggestions for Administrative Policies

1. The Administrative User policy should be based upon the principle of least privilege, which states that users may only be given the access privileges required to perform their job functions, and no more. This can be a fairly difficult task since many applications and operating systems will not support granular permissions. However, this is the time to introduce the concept and the standards behind assigning access privileges. Reasonable effort should be made to assign only those privileges that are required. Later within this document there will be some discussion in applying the concept to the production environments and ways to smooth the implementation phases.

2. Identify by policy what is appropriate and inappropriate behavior with administrative privileges. Identify and define privacy expectations for the administrative users. This is also an opportunity to toss in some ethical behavior statements. You may also want to disallow administrative privileged accounts to be used for personal, non-administrative tasks such as Internet surfing, checking internal e-mail accounts or updating personal files.

3. Identify by policy that it is inappropriate to utilize service account ID's for administrative tasks outside the documented and authorized functions of that service

[1] Scalet, Sarah D., Dr. Crime's Terminal of Doom and Other Tales of Betrayal, Sabotage & Skullduggery. CIO Magazine. June 1, 2002. http://www.cio.com/archive/060102/doom.html

ID. (e.g. The Backup user ID should never be used by another user to view files on a server. It should only be used as an automated login for backup purposes.)

4. Policy should declare that the organization will at all times make every effort to reduce potential conflicts of interest based upon access permissions or assigned tasks. This should include requirements for segmentation of duties. For instance, network administrators responsible for maintaining the routers, switches and phone systems probably should be segmented from administrative privileges on the application servers.

5. Develop policy requirements and guidelines for senior management when there is inappropriate use of administrative user ID's and privileges. This is intended as a means for consistent standards to handling security violations. Senior management must support and enforce the policies they have developed and approved in order to have an effective security program.

Clearly Document Administrative Responsibilities

Once the policies pertaining to the Administrative Users are defined, it is time to evaluate the duties and responsibilities for each administrative user. This step is primarily to map an administrative title or position with a formal job description that reflects their true access permission requirements. Depending upon the size of the organization and the staff responsibilities, the job descriptions may be very broad. However, they should be specific enough to identify security requirements.

Identify a Security Model

Identify a security model for the management of administrative users. There may already be a specific security model in place for your organization. In many cases the security model in use is probably a mix of multiple models. Depending upon the size of the organization, there may only be one or two administrators. An organization may be forced to accept the risks inherent with one overall administrator. Nevertheless, a model must be chosen.

There are several schools of thought on the subject. For purposes of this document, three generally accepted security models will be addressed: Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). [2]

Mandatory Access Control

MAC bases its structure on the premise that everyone and everything can fit into well-defined groups of access privileges. In most cases it is hard coded into the application

[2] National Institute of Standards and Technology. "An Introduction to Role Based Access Control". NIST/ITL Bulletin. December 1995. http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html

or operating system and is very difficult to modify its structure. Because of this, organizations that use MAC may have only one department to manage security. MAC is not flexible enough to spread out over various areas. This is a shortfall due to regular changes that occur to user permissions or attributes.

MAC has been a method generally utilized by the government because it fits so well into their tight security classifications of information. User access is based upon clearance levels, such as secret or confidential, and the security assigned to the information or systems used. As defined in the POSIX.6 standard for MAC, users that are identified with a specific security classification cannot step above that clearance level, nor can a user with a higher level clearance escalate another users privileges to their level. [3]

Benefits of MAC

One of the most important aspects of MAC is that it removes all discretion. Once the security model is setup, security is based upon hard coded rules enforced by the system. The owner of the system, application or information is not allowed to complete security over-rides.

Discretionary Access Control

DAC is discretionary in that the administration of access is up to the owner of the system or information. This method is much more efficient in its control methods because user administration is spread out over numerous administrators that are the owners of the systems. This can be misleading since users within an organization rarely "own" the system or its information. For this purpose, the term owners identifies the primary administrators of the system or information.

This method can also be much less secure due to its discretionary nature. Not all administrators are created equal. Some may have a higher level of trust or possibly a misunderstanding of the permissions granted to users on their system, thus granting far too much permission to a single user.

As demonstrated earlier, the administrator of a human resources system may not be aware that an employee, whom they just provided access, is also allowed permissions into the payroll system by a different administrator. This scenario creates quite a conflict of interest. Generally speaking, this method of user administration is used in corporate environments because users do not need to wait long periods of time to be granted access into a system that is internal to their department.

[3] Barkley, John. NIST Special Publication 800-7. "Security in Open Systems - Mandatory Access Control" July 1994. http://csrc.nist.gov/publications/nistpubs/800-7/node36.html

Benefits of DAC

This is a great model for small organizations that have a very limited IT staff. It stands to reason why Microsoft had adopted this model as its primary means of securing networks for the NT platforms. The users themselves and the administrators share the responsibilities of security. Changes can occur swiftly and without too many controls to approve the change.

Role Based Access Control

The third security model as defined by the National Institute of Standards and Technology (NIST) is Role Based Access Control. RBAC is a fairly new security model for the administration of users. Its beginning goes back to 1992 with two individuals, David Ferraiolo and Rick Kuhn. They began looking for better ways to manage security that would support the growing number of IT systems. [4] Since then there has been many forums to identify a standard for RBAC. Numerous companies have already begun adoption of what they believe fits into the standard. Whether your environment is Novell, Microsoft or Unix based, there is a good chance that there is a way to adopt some form of RBAC.

There are five basic items that make up RBAC; 1) Role, 2) Permissions, 3) Operations, 4) Users and 5) Objects. Below are simplified definitions and their attributes:

Role
A role can be defined as a means for assigning relationships between users and the assigned permissions to conduct an operation against an object. A role is created as the focal point for managing the permissions for operations. Permissions are assigned to the role. However, a role cannot be utilized to authenticate to an object because it has no user attributes.

User
Users are defined for the identification and authentication. It is the descriptor for the individual user. Permissions are not directly applied to the user. Users are assigned to roles. Users can be assigned to multiple roles.

Objects
Objects are the systems, resources and information that can be accessed for a purpose. For example, an object could be a file, printer, server, scanner, directory, etc. Permissions are granted to roles in order to access the object.

[4] Secretariat: Information Technology Industry Council (ITI). “Role Based Access Control”. September 16, 2003. http://csrc.nist.gov/rbac/rbac-std-ncits.pdf

Permissions
Permissions are the attributes assigned to an object that identify specific operations that can be conducted on an object. Permissions are assigned to roles.

Operations
Operations are the tasks or functions that occur against the object by the user. For example, an operation may be changing passwords, backing up files or installing an application.

RBAC can be thought of as a modified mandatory access control method. It works from the pretense of predefined privileges, however provides a model that allows distributed administrative management model throughout an organization. For example, a role can be developed and applied to all managers for the privilege of maintaining password administration for their department. This is thought of as mandatory because it only grants privileges to complete a specific task within a very controlled set of users. However, each department manager can manage their own employees passwords. In this example the administrative task is distributed across the organization much like DAC, but the people responsible for managing passwords cannot actually assign that privilege to anyone else.

The difficulty with RBAC is how to segment the duties and clearly define privileges that are useful to the organization without becoming too restrictive. As stated earlier within this document, segmentation of duties is the task overlooked, but the danger is over segmenting or creating roles that are too restrictive. Luckily, there are solutions on the horizon for defining specific roles at very granular tasks. The key then is testing those newly created roles. And hopefully those roles fall within the predefined job descriptions of the users they will be applied to.

Benefits of RBAC

These recommendations have many benefits including simplification in management of user access. Microsoft supports it as stated in the Security Administration Operations Guide [5] and by industry best practices identified by the National Industry for Standards and Technology (NIST).

While standards and cost are a concern, RBAC is designed to improve overall control of user administration. With that said, several recent studies indicate there is a cost savings. A survey was conducted by Research Triangle Institute (RTI) that seems to

[5] McPherson, Dave. "Role-Based Access Control for Multi-tier Applications Using Authorization Manager". 2004. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/athmanwp.asp

indicate a forty-five percent reduction in administrative overhead and overall improved employee productivity. [6]

The structure itself can be modified to fit nearly any medium to large-sized organization. For the sake of this document, I will continue to show how to improve management of administrative users through the use of RBAC. The main concern is to accurately identify administrative roles that can be documented for future management. In the long term, the principles and methods of user administration with RBAC can be extended to the remaining users within the organization. Conversely, various other models could be chosen. They will all need to follow similar steps to adequately segment the administrative privileges.

Applying the Security Model

Once your policies are in place and the organization has chosen a security model, the next step is implementation. For the sake of this document, the steps that follow will generally apply to an implementation of RBAC. However, they provide some interesting foresight into areas that should be addressed regardless of which security model is chosen.

Step 1:
Identify administrative roles. Listing the general functions and tasks that are implemented on a daily basis can help to identify roles. Do not eliminate functions or tasks because it is unknown how security would be applied. This is a brainstorming step to classify all of the operations that are completed by each administrative user. Be careful to avoid listing items that are too granular. This will make the job more difficult in the near future. The more granular the list, the more control; however, at the cost of efficiency.

Some examples could be Workstation Administrator. This role might be responsible for adding workstations to the network and managing applications on the users desktop, but would not allow server administration or administration of applications on servers.

Another example that is fairly granular, but could be justified, is Password Administration. The advantage of this role is to segment the duties from the server managers and allow a distributed approach for password administration. Departmental Managers could share in this administrative task for their specific areas. Thus reducing the workload on the helpdesk for password resets.

One more example that applies directly to administrative service accounts could be Backup Operator. This role is fairly self-explanatory, however removes the ability of other administrators from backing up and restoring information without authorization.

[6] Kropp, Brian & Gallaher, Michael. "CASE STUDY - ACCESS TO COST SAVINGS". Information Security Magazine. April 01, 2001. http://infosecuritymag.techtarget.com/articles/april01/cover.shtml

Step 2:
Evaluate several tools that assist in implementing your security model. For RBAC methods and software there are several possible choices: 1.) BV_Admin by Bindview. The advantage to this solution is its much more comprehensive for implementation into current Microsoft NT/2000 environments and will provide compatibility with newer versions of Microsoft server products. BV_Admin is also X.500, LDAP and Active Directory compatible, which will enable integration into third-party applications.[7] However, this is primarily a tool for segmentation of administrative tasks. Implementation of RBAC into the enterprise for all users is much more difficult and will require substantial integration efforts. 2.) If your organization is primarily Microsoft, upgrading to Server 2003 with Active Directory will also solve the problem. Microsoft Windows 2003 uses a utility called Authorization Manager (AU). AU introduces the use of objects called roles. This additional utility in conjunction with the use of roles enables the RBAC model. [8] 3.) Evaluate other freeware or third party products that possess the features and functionality that best fit the organization. For organizations that are primarily Unix there are some very good products that allow expansion from the use of Access Control Lists, ACL's. Free products available in this arena can be found at http://csrc.nist.gov/rbac/.

Step 3:
For RBAC, identify what roles will be created based upon the ability of the RBAC application to assign permissions and the chosen segmentation of duties. This requires substantial testing and coordination with management and administrative users. The bottom line, strong communications with technical staff and management is key. The changes that will take place may make the administrative staff uncomfortable or uneasy about their responsibilities. In fact, a few may not be able to cope with the idea that their duties are being segmented and their privileges reduced. Just remember, communications, communications, communications!

Step 4:
Assign roles to specific job descriptions. Each job description should be associated with specific operations that can be tied directly to a pre-defined set of administrative privileges and an associated job description. Assigned privileges should take into account whether there should be dual control over the system or data. Segregate administrative access according to function, process and system in order to enable dual controls. While identifying roles for administrative users, duties must be reviewed carefully in order to eliminate conflicts of interest.

[7] Hurwitz Group. "Management Controls: Security Impact of IT Administration". July 2001. http://www.bindview.com/downloads/public/whitePapers/ImpactofItAdministration.pdf

[8] McPherson, Dave. "Role-Based Access Control for Multi-tier Applications Using Authorization Manager". Microsoft Corporation. 2004. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/athmanwp.asp

Monitoring and Auditing

While establishing solid controls is a great start, defense in depth would be lacking without the proper monitoring and periodic reviews of administrative privileges. It goes without saying, auditing should always be turned on within systems that are deemed critical. This should include successes and failures of logins, user administration functions and changes in security-related configurations. The subject of monitoring and auditing could easily be an entire book, but it is important to remember this is a task that requires regular attention.

Training

Develop a security awareness-training program for IT Administrators. How can an organization expect to stay secure without training the people in the trenches? Just because the administrators know a lot more than the average user does not mean that they know what or how to secure the organization. Besides, these are the people that are more than likely going to catch the security vulnerabilities. Provide them with the tools to make your organization successful and secure. One great way is to send them to training that deal with the experiences of others. In fact, there are various training courses and seminars that provide hands-on experiences to improve overall understanding.

Communications

If it has not been mentioned enough earlier, there is a dire need for continued communications. Maybe the most effective ways to keep a healthy and honest workforce is to listen and communicate. Developing open channels and forums to discuss successes and failures can help to maintain a healthy work environment. Utilizing brainstorming sessions to get buy-in on new methods for securing the environment is one suggestion. Let the technical gurus in on discussions about security models and what the industry is doing. Sometimes the gurus are the ones left in the dark because they are so entrenched with the technical side of things. They can become part of the secure security culture if you let them.

Conclusion

We are very fortunate that most administrators that make it to the pinnacle of the technical world are good people. They care about their work and are interested in maintaining system uptime. Chances are, none of the administrative staff will ever knowingly cause damage to the organization. However, segmentation of administrative privileges protects from the inadvertent or unknown catastrophes. Through segmentation, the impact of security incidents can be minimized. That is really what this document is about. Identifying policies that help the administrators maintain security, segment duties and develop some controls to verify security. In the long run, administrative and user permissions alike will be more manageable.

References:

Barkley, John. NIST Special Publication 800-7. "Security in Open Systems - Mandatory Access Control" July 1994
http://csrc.nist.gov/publications/nistpubs/800-7/node36.html

Bianco, David. "Admins' "Dirty Little Secret"" Information Security Magazine. October 2003. Volume 6. Number 10. p. 55.

Ferraiolo, David and Kuhn, Richard. "Role-Based Access Controls". January 1995.
http://hissa.ncsl.nist.gov/rbac/paper/node2.html

Hurwitz Group. "Management Controls: Security Impact of IT Administration". July 2001.
http://www.bindview.com/downloads/public/whitePapers/ImpactofItAdministration.pdf.

Information Technology Industry Council (ITI) American National Standard for Information Technology. "Role Based Access Control". April 2004.
http://csrc.nist.gov/rbac/rbac-std-ncits.pdf

Kropp, Brian & Gallaher, Michael. "Case Study – Access to Cost Savings". Information Security Magazine. April 01, 2001.
http://infosecuritymag.techtarget.com/articles/april01/cover.shtml

Malik, Bill. "Information security policy: Answering to the board of directors". Computerworld. September 18, 2003.
http://www.computerworld.com/securitytopics/security/story/0,10801,84767,00.html

McPherson, Dave. "Role-Based Access Control for Multi-tier Applications Using Authorization Manager". Microsoft Corporation. 2004.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/security/athmanwp.asp

Microsoft. "Security Administration Operations Guide". April 2001.
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp

NIST/ITL. "An Introduction to Role Based Access Control". NIST/ITL Bulletin. December 1995. http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html