Securing Active Directory: An Overview of Best Practices

Published: April 2013

The threat of compromise to IT infrastructures from external attack is rapidly growing and evolving. The Active Directory environment is often the target for these attacks. This article details steps that your organization can take to protect its Active Directory environment. For more on strategies described here, see the comprehensive document: Best Practices for Securing Active Directory.

Introduction

Potential compromises to computing infrastructures have existed as long as computers. Moreover, as computer technology has evolved, so too has the sophistication of the attack techniques.

During the past decade, an increasing number of public and private organizations, of all sizes, in all parts of the world, have been compromised in ways that have changed the threat landscape significantly. The motivations behind these attacks range from hacktivism (attacks motivated by activist positions) to theft of intellectual property.

At the heart of any IT environment is the Active Directory® infrastructure that provides access control for servers and applications. Against this backdrop, Microsoft® IT has developed a set of best practices to help other enterprises protect their Active Directory environments.

This article provides a short overview of four interrelated strategies that Microsoft IT uses to protect its Active Directory environment, including:

- Identifying vulnerabilities
- Reducing its Active Directory attack surface
- Monitoring for signs of compromise
- Developing a long-term security plan

To learn more about the best practices that support these strategies, refer to "Best Practices for Securing Active Directory."

Identifying Vulnerabilities

Most IT security breaches start with the compromise of only one or two computers within an infrastructure. Beyond these entry points, the progress of the breach can spread quickly. Conversely, it can be slowed or stopped as quickly, depending upon the actions of an IT department to mitigate risk in key areas.

By understanding and circumventing the vulnerabilities that hackers leverage to gain access initially to its IT infrastructure, an organization can prevent them from using that access to propagate the compromise across additional systems, which eventually can target Active Directory and domain controllers to obtain complete control of the organization’s Active Directory Domain Services (AD DS) forests.
Protect and Update Software
Malware protection is an obvious but important area of focus for protecting infrastructure. Microsoft IT ensures that antivirus and antimalware applications are deployed and updated properly throughout its environment, and monitors all attempts by users to disable or remove these applications.

As part of these operations, Microsoft IT regularly checks the environment for gaps in patching by using a patch-management system for all Windows® operating systems and Microsoft applications.

Software products that exceed their useful life also can pose a compromise threat. As Microsoft IT plugs the gaps in its malware and virus deployments, it also works to identify operating systems and applications that are outdated. As a rule, Microsoft IT eliminates legacy systems and applications by identifying and cataloguing them, and then determining whether to upgrade or replace the application or host.

Custom development in an IT organization is another potential area of exposure. Microsoft IT takes care to implement secure development practices, particularly for its Internet-facing applications.

Fix Faulty Configurations
Errors in configuration also can create vulnerabilities. An IT organization can fix these faults by identifying configurations that introduce risk into the environment, regardless of whether they are on domain controllers, operating systems, or Active Directory, or within applications, and then finding solutions to improve the configurations.

Microsoft IT has established several best practices for improving potentially faulty configurations, including that it:

- Secures all privileged accounts and groups by using proper configuration settings and techniques.
- Avoids disabling security features on users’ computers.
- Avoids granting excessive rights and permissions to accounts (particularly service accounts).
- Avoids using identical local credentials across systems, and does not permit the installation of unauthorized applications and utilities that create vulnerabilities.
- Eliminates permanent membership in highly privileged groups.
- Eliminates unnecessary applications and utilities on domain controllers.
- Does not allow downloads of Internet content and freeware utilities on the domain controllers.

Reducing the Active Directory Attack Surface
This set of best practices outlines the steps to take within Active Directory to reduce its attack surface, which is the portions of the software that allow unauthorized operation by design. This can include user-input fields, protocols, interfaces, and services.
Manage Privileged Accounts and Groups

Active Directory supports the principle of least privilege in assigning rights and permissions. By this principle, regular user accounts have access to read most directory data, but can change only a limited set. Privileged accounts (and accounts added to privileged groups) can perform specific tasks, but only those that are relevant to their duties.

Close management of privileged accounts and groups is an important part of reducing the attack surface in Active Directory. For Microsoft IT, the first step is to reduce the highly privileged accounts that require access for day-to-day administration. Microsoft IT then can secure the privileged groups and accounts, and implement secure administrative practices and systems. Lastly, Microsoft IT ensures that its environment’s administrative users continue to use the principle of least privilege to reduce the accounts that are have rights and permissions that exceed what it necessary to perform daily operations.

Leverage Built-In Features

Active Directory features multiple built-in technologies that Microsoft IT uses to help protect its environment. These include:

- **AdminSDHolder.** Microsoft IT uses AdminSDHolder to ensure consistent enforcement of the permissions on protected accounts and groups, regardless of the location of the protected groups and accounts in the domain.

- **Security Descriptor Propagator (SDProp).** Microsoft IT uses SDProp to compare the permissions on the domain’s AdminSDHolder object with the permissions on the domain’s protected accounts and groups, and to reset the permissions if they do not match.

- **Role-based access controls (RBACs).** Microsoft IT uses RBACs to group users and provide access to resources based on business rules.

- **Privileged Identity Management.** Microsoft IT uses Privileged Identity Management to provide mechanisms by which accounts receive temporary rights and permissions to perform build or break-fix functions, rather than leaving privileges attached to accounts permanently.

Utilize Other Reduction Tactics

Microsoft IT follows additional best practices to reduce its attack surface, including:

- **Ensuring domain controller physical security.** Of all systems in an IT infrastructure, Active Directory domain controllers generally require the most stringent protection from physical access. Microsoft IT ensures the physical security of domain controllers by installing them in dedicated secure racks or cages that are separate from the general server population. Additionally, it configures its domain controllers with Trusted Platform Module (TPM) chips, and protects volumes in the domain controller servers using BitLocker® Drive Encryption.

- **Implementing secure administrative hosts.** Secure administrative hosts are workstations or servers that are configured specifically for creating secure platforms from which privileged accounts can perform administrative tasks in Active Directory or on domain controllers, domain-joined systems, and applications that are running on domain-joined systems. Microsoft IT has developed detailed best practices for account configuration, physical security, operating systems versions and
configurations, patch management, and configuration management on secure administrative hosts. To learn more about these best practices, refer to "Best Practices for Securing Active Directory."

- **Using access control.** Microsoft IT routinely implements robust authentication controls, such as multifactor authentication (smart cards) and certificate-based authentication mechanisms.

**Monitoring for Signs of Compromise**

As part of the daily operations in its IT environment, Microsoft IT uses a robust security information and event management system to identify events on Windows-based systems that may indicate an active attack.

As a best practice, other enterprises can employ similar monitoring systems. When implementing monitoring policies, Microsoft IT ensures that each policy includes:

- Traditional and advanced audit policies, including effective configuration of audit subcategories in Windows Vista® or newer operating systems.

- Detailed, comprehensive lists of objects and systems to audit.

- A list of events to monitor to help detect compromise attempts.

As mentioned previously, faulty configurations can play a key role in spreading the progress of a malicious incursion into an IT environment. To prevent further escalation of attacks from penetration to complete compromise, Microsoft IT identifies configurations that introduce risk in its IT systems, and then determines ways to improve those configurations.

**Developing a Long-Term Security Plan**

Passive monitoring is not enough to maintain an environment securely. Effective security planning for Active Directory requires actively planning for compromise.

An IT organization will know it has achieved maturity in its Active Directory security when it is able to stop break-fixing all of its current security holes and start planning for the road ahead. By utilizing the principles in this article, an organization can plan its long-term IT security strategy in view of the current threat landscape, as well as lessons the organization has learned from experiences, and knowledge of the organization’s future.

**Identify, Segregate, and Secure**

To develop an effective and efficient Active Directory security plan that will serve its long-term needs, Microsoft IT follows a logical and repeatable cadence. First, it identifies the users, applications, and systems that are most critical for its stability and operations, with respect not only to the IT infrastructure, but also to the entire business that the infrastructure supports. Then, Microsoft IT focuses on segregating and securing these critical assets, regardless of whether they are intellectual property, people, or systems.

In some cases, Microsoft IT can segregate and secure assets in an existing AD DS environment. However, in other instances, it chooses to implement small, separate Active Directory cells that establish a secure boundary around critical assets, and then monitors those assets more stringently than less-critical components.

The exercise of isolating critical assets also helps to maintain a more secure environment by combining business and IT information to construct a detailed picture of a normal operational...
By knowing what is normal for its organization, Microsoft IT is more likely to notice abnormalities that may indicate attacks.

**Use Creative Destruction**

*Creative destruction* is an IT term that describes the mechanisms by which an organization can eliminate legacy applications and systems by replacing them with new solutions.

Microsoft IT applies this concept to Active Directory security planning by harnessing the significant benefits and expediencies to securing entire IT environments that resulted from the advent of server and application virtualization. By deploying in the cloud, Microsoft IT reduces its attack surface strategically by eliminating legacy systems and applications that presented vulnerabilities previously that attackers could leverage.

**Develop Comprehensive Protection Strategies**

To shore up long-term exposure to compromise, an organization must have a comprehensive strategy for protecting both its computing infrastructure and its intellectual property. The more that the organization’s strategy focuses on deterring compromise, the stronger its overall plan will be for protecting its IT assets.

To keep long-term planning on track, Microsoft IT uses the following best practices when prioritizing the following security activities:

- Isolating legacy systems and applications to reduce threat exposure, and utilizing creative destruction to follow migration plans that limit risk.
- Simplifying security for end users by implementing controls that are transparent and principles that are easy for the users to understand and follow.
- Utilizing security best practices for Active Directory to develop all custom Internet-facing applications.
- Ensuring that applications and operating systems are up to date, and implement a thorough strategy for patch management.

**Conclusion**

No IT infrastructure is immune from attack. That is an unpleasant fact in today’s cyber world. However, if an organization implements appropriate policies, processes, and controls to protect key segments of an organization’s computing infrastructure, it may be able to prevent escalation of attacks, from penetration to complete compromise.

To read more about the best practices for securing Active Directory environments, see the detailed technical document "Best Practices for Securing Active Directory."
For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Order Centre at (800) 933-4750. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase

© 2013 Microsoft Corporation. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, Active Directory, BitLocker, Windows, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.