Quest

Managing the Insider Threat with Active Directory Security

The anatomy of an insider threat, and securing Active Directory against it

by Alvaro Vitta, principal solutions consultant, Quest

INTRODUCTION

"You mean this was an inside job?"

Ever since the first story about crime and the people who try to solve it, there has been that moment when somebody uncovers a piece of evidence that an insider was involved. The characters exchange shocked, wary glances as one of them says, "You mean this was an inside job?"

Unfortunately, glances and questions like those are becoming a standard feature of investigations into almost every data breach. Upon discovering that someone has illegitimately accessed data on the network, IT managers initially believe (hope, really) that the threat came from outside. But as recent, headline-grabbing data breaches demonstrate, a lapse in internal security — whether accidental or malicious — often makes the attack possible in spite of robust external security.

This paper focuses on Microsoft Active Directory (AD) as a prime target for attackers because of AD's importance in authentication and authorization for all users. Readers will see how a typical insider threat unfolds and take away Active Directory security best practices that minimize the risk of the insider threat to the availability, confidentiality and integrity of AD.

INSIDER THREATS AND THEIR IMPACT ON BUSINESS

Many businesses believe that insider threats — in which employees, former employees, contractors or valid users obtain unauthorized access to an organization's network and the resources connected to it — can cause as much damage as externally initiated attacks.[1] Attention centers on current and former employees, but service providers and business partners play a growing role in committing or facilitating cybercrimes.

[1] "US cybercrime: Rising risks, reduced readiness — Key findings from the 2014 US State of Cybercrime Survey," PwC, May 2014, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf

About 95 million, or one fifth, of AD accounts are under attack every day.[4]

The financial cost of a data breach from an insider attack, including the time and money to restore security to systems, is considerable. About one fifth of companies believe that the cost could exceed $5 million, but more than half of companies candidly admit that they have no idea how high or low to estimate their potential losses from an insider attack.[2]

The scenarios and human stories surrounding insider attacks reflect those of all crimes:

- Cross-border economic espionage
- Well-planned conspiracies to steal trade secrets
- Disgruntled former employees with broad network privileges
- Disaffected employees using credentials that a supervisor shared in confidence
- Username and password of a supplier company's representative stolen in phishing attack
- Authorized users finding and copying credit card data, then selling it on the black market

The broader cost of a data breach committed by insiders includes the loss of confidential information, harm to reputation and disruption of critical systems.[3]

INSIDER THREATS AND ACTIVE DIRECTORY

More than 90 percent of the world's large companies use AD, totaling some 500 million active account users.

About 95 million, or one fifth, of those accounts are under attack every day.[4]

Organizations use AD to provide authentication and authorization for employees, contractors, partners and customers. Through AD they also grant access to Windows-based network resources like shares and files, databases, email servers, some on-premises applications and cloud-based applications. Without AD, they lose Exchange, collaboration, real-time communications, SharePoint, SQL Server databases, web servers and other resources few companies can do without.

Hardened external security is no guarantee of AD security, because the biggest threats to AD security are the internal ones, and more than half of insider misuse involves abuse of privileges.[5] That extends to accidental or malicious misuse of AD permissions, elevated accounts and sensitive groups that can weaken security protocols and lead to unauthorized access to sensitive Windows-based data.

Unauthorized access to AD is like having a stolen key card: Once attackers are inside the building, they can take the elevator, wander through offices, open desks and look through drawers. With so many accounts under unrelenting attack from within and without, the insider threat to AD is clear and present.

IS IT DIFFICULT TO SECURE ACTIVE DIRECTORY?

AD is made to be secure, but as in the analogy of the key card, security breaks down when elevated access is in the wrong hands.

Consider three main areas IT administrators have to contend with:

Lack of automation

- Access controls should be continually assessed and remediated, but there is no automated process for it in AD.
- Continual implementation and testing of full disaster recovery processes would guard against prolonged downtime and data loss in AD, but AD does not natively provide an automated way to test and implement a full AD disaster recovery scenario across all domain controllers (DCs).

[2] *"Insider Threats and the Need for Fast and Directed Response," SANS Institute, April 2015,* https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

[3] *"Managing insider threats," PwC, February 2015,* http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/managing-insider-threats.pdf

[4] *John Fontana, "Active Directory czar rallies industry for better security, identity," ZDNet, June 9, 2015,* http://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/

[5] "*2015 Data Breach Investigations Report," Verizon, April 2015,* https://msisac.cisecurity.org/resources/reports/documents/rp_data-breach-investigation-report-2015_en_xg.pdf

- When unauthorized AD access or actions are detected, there is no way to automatically prevent or remediate them, and no way for stale credentials to self-clean.
- Without built-in, automated change controls in AD, companies are subject to accidental, unauthorized access and costly outages.

Human/organization/business factors

- When employees transfer between business units, most organizations apply deficient processes to off-board them. Instead, administrators leave the users with elevated authority — accumulated from previous job requirements — that they will no longer need.
- AD administrators cannot be prevented from accessing sensitive Windows resources.
- Data fidelity and company naming standards in AD are hard to enforce, which makes it hard to categorize access, review entitlements and audit assets.
- As a matter of business convenience and trust, it is common for employees, contractors and business partners to know and share one another's privileged AD credentials.

Limitations of AD

- Lack of security context delays detection of data breaches.
- AD does not allow organizations to fully enforce a true, least-privileged user account (LUA), which results in users with higher privileges and more access than they need to perform their job. For example, if an administrator wanted to delegate the ability in AD for help desk employee JSmith to move user objects from the Planning organizational unit (OU) to the Engineering OU, the admin would have to grant JSmith the right to delete any user object from the Planning OU and write to the Planning OU. That encompasses considerably more permissions than JSmith needed (and that the admin really wanted to grant) to execute the move and greatly increases the organization's exposure to risk.

Traditional tools for security information and event management (SIEM) are bound by limitations on native log auditing. For example, the native audit log indicates that a Group Policy Object (GPO) was modified, but does not record which settings were changed or their values before and after the change.

Thus, securing AD is an ongoing balancing act between granting users the rights they need to do their job and keeping them — even domain administrators — out of security groups that can access sensitive databases, folders and files containing human resource or credit card information or health records.

ANATOMY OF AN INSIDER ATTACK AGAINST ACTIVE DIRECTORY

Consider this fictitious story describing how an insider threat caused by weak security controls can affect AD.

As the end of support for Windows Server 2003 approaches, a medical products retailer named Acme hires JSmith under a four-week contract to help upgrade its environment to Windows Server 2012. PBrown, the AD administrator at Acme, adds JSmith to the domain administrator group.

On Friday of JSmith's second week, Acme terminates the contract, but nobody tells PBrown to remove JSmith from the administrator group. The following Monday, PBrown finds out that JSmith is no longer working for Acme and removes the contractor from the administrator group.

The following steps describe what happens over the weekend.

1. Creating a bogus account

Unhappy that Acme terminated his contract prematurely, JSmith looks for ways — including illicit ones — to make up the income he had counted on earning. From a friend, he learns of a black-market site where he can make quick money selling credit card data.

JSmith logs in to Acme's network from home using his administrator credentials and creates a new administrator account for himself. To keep the creation of the new account from attracting attention, he calls it corpsvcbk1, following Acme's naming convention for backup service accounts. He counts on being able to use corpsvcbk1 in case Acme removes or resets the password on his original admin account.

> Securing AD is an ongoing balancing act between granting users the rights they need to do their job and keeping them out of security groups that can access sensitive resources.

To keep the creation of the new account from attracting attention, he follows Acme's naming convention for backup service accounts.

2. Obtaining Domain Admin privileges

JSmith notices a group called CorpOperations, which is a member of the Domain Admins Group. He creates a new account in the group and calls it corpsvcbk1. He then covers his tracks by adding it to the nested CorpOperations group, which gives him indirect Domain Admin privileges without raising alerts. (Acme's generic monitoring system is configured to monitor only direct changes to the Domain Admins group.)

3. Accessing the file servers

JSmith locates the SQL Servers and file servers where Acme stores credit card data and personally identifiable information (PII).

He modifies the GPO that prevents administrators from logging on to certain database and file servers, then he logs on locally to SQL1 and FSRV1. He adds his corpsvcbk1 account to the local administrator group on SQL1 and assigns to it the system administrator role in SQL Server.

Looking around, he finds the unencrypted credit card database and exports all of its records across the remote connection onto his laptop.

On FSRV1, he locates the files that contain PII. Again covering his tracks, he adds his admin account to a nested group called FinanceOps, a member of the built-in administrators group on FSRV1. In the Accounts Receivable folder, he finds the file Customer_PII.xlsx. To access the file, he adds his admin account to the Accounts Receivable group; that prevents his account from showing in the access control list, yet still gives him full rights to the file. He opens the file, ensures it's the one he wants and copies it to a mapped network drive on his laptop.

4. Setting up eavesdropping

Next, JSmith modifies a Registry key that lowers LmCompatibilityLevel and session security enough for him to install malware that eavesdrops as SQL1 and FSRV1 pass credentials between them. That will allow him to decipher additional credentials in the future as admins authenticate so that, even if Acme deletes his bogus corpsvcbk1 account, he can continue stealing more credit card data.

5. Cleaning up

JSmith removes his corpsvcbk1 account from admin groups, clears the logs (to erase evidence of his attack) and decides to keep malware in the network for future exploits.

Acme's security policies and security controls are insufficient to prevent this insider attack against Active Directory. JSmith's tactics ensure that it will take a long time for Acme to detect the data breach, by which time JSmith will likely have recovered his lost income and Acme will be in the throes of recovering from the data breach.

ACTIVE DIRECTORY SECURITY BEST PRACTICES

There is no slam-dunk approach to Active Directory security, but organizations can guard against insider threats to AD by following several guidelines:

1. Set account and group expirations for temporary access to sensitive groups.

a. Instead of permanent membership to sensitive groups, use temporal group memberships with automatic start date/time and end date/time.

b. Set account expiration dates when creating accounts for temporary staff such as contractors, interns and visitors.

2. Prevent unauthorized creation of accounts by defining a whitelist of authorized credentials permitted to perform this task. If someone who is not on the approved list creates a user account, the event triggers an email alert. It can also trigger remediation that disables the creator's account and/or the created account.

3. Monitor in real time not only direct changes (that can be tracked in native security logs) to privileged enterprise groups in AD, but also additions of nested members (that is, indirect membership to elevated AD groups), which Windows servers do not log.

4. Monitor the following enterprise groups for direct and nested membership changes:

   Administrators, Print Operators, Network Configuration Operators, DHCP Admins, Backup Operators, Incoming Forest Trust Builders, Account Operators, Cert Publishers, Group Policy Creator Owners, Domain Admins, Domain Controllers, Enterprise Admins, Server Operators, RAS and IAS Servers, Schema Admins

5. Monitor real-time changes to GPO settings in AD. The before and after values of these settings cannot be tracked in native logs, presenting a backdoor threat to AD.

6. Regardless of user permissions, prevent unauthorized changes to important enterprise groups and GPO settings by using a whitelist of authorized users. With a whitelist in place, even if attackers gain Admin rights from compromised credentials, their changes to memberships in privileged groups like Domain Admins and Enterprise Admins will be denied. The whitelist also applies to making changes to sensitive GPO settings like disabling or denying logon to important servers and weakening NTLM authentication.

7. Monitor in real time any suspicious activities like logons to sensitive servers after regular business hours and changes to sensitive registry keys like LmCompatibilityLevel. The latter is a backdoor tactic for lowering values used by the NTLM authentication protocol.

8. Audit permission changes and activities performed against databases and file servers (including files, shares and folders) containing sensitive data.

9. Continually review user access rights and privileges to sensitive groups and servers. Review SQL Server database permissions and NTFS permissions on AD and SQL file servers.

10. Enforce separation of duties to prevent, for example, contractors from becoming members of Domain Admin groups. Apply a least privilege access model for AD and Windows.

11. Implement an automated process for deprovisioning users that includes disabling/deleting accounts, removing accounts from all groups and distribution lists, removing remote VPN access, and automatically notifying HR, security and facilities management.

AD SECURITY AS PART OF OVERALL GRC STRATEGY

Active Directory security plays an important role in governance, risk management and compliance (GRC) as well.

AD security extends to the organization's ability to prove that it has proper controls for AD and for the entire Windows environment, including SharePoint, Exchange and SQL Server. Proving compliance means being able to report efficiently on AD-level details such as information on past and current privileged users; accounts of former employees and contractors; and configuration, update and patch status of servers. Tight AD security is an essential part of GRC and of careful preparation for an audit.

CONCLUSION

The insider threat to AD is real, pervasive and costly. The predominance of AD in enterprises around the globe makes it an appealing target for adversaries who can exploit technical limitations and human factors to launch data breaches from the inside out.

Monitoring logs of AD events is a start, but many insider threats take advantage of AD events that are not logged. Besides, the list of things to look for in a suspected attack is long and there is no automatic way to guard against all of them.

Whether accidental or malicious, insider threats are pernicious by nature. Organizations will continue balancing the need to let their system administrators perform tasks with some autonomy against the need to grant only the privileges required for those tasks. In the meantime, Active Directory security best practices are an important part of overall GRC strategy.

ABOUT THE AUTHOR

Alvaro Vitta is a principal solutions consultant specializing in security at Quest. He has been assessing, designing, testing and deploying security solutions for large enterprises in the private and public sector since 2000 in the areas of identity and access management (IAM), Active Directory security, and governance, risk and compliance (GRC). Alvaro holds industry certifications that include CISSP, CISSO, MCSE and ITIL.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.