Lepide

10 BEST PRACTICES FOR KEEPING ACTIVE DIRECTORY SECURE

A Whitepaper by Lepide

10 Best Practices for Keeping Active Directory Secure

Due to the increased regularly of attacks targeted at Active Directory, and the resulting increase in the stringency of regulatory compliance, we thought it best to prepare this list of 10 of the most important best practices for keeping AD secure.

Most of the attacks and cyber-security threats you are likely to face will come from within your organization.

Therefore, there is no one complete solution to keep AD secure. Your best bet is to combine a powerful auditing and monitoring solution with the below list of best practices. So, let's get started.

1. Limit Access to Domain Admin Groups

The Domain Admins group is like gold dust for a potential attacker. The reason being that members of this group have local admin rights on every domain joined system. This kind of power is exactly what hackers and malicious insiders are looking to exploit.

Once an attacker gains access to your network through a compromised computer or user account, they may look to move laterally through the network, attempting to compromise accounts with higher permissions, such as those members of Domain Admins groups. One way to slow this down is to limit the number of members to this group.

Most Admin groups, and even Microsoft themselves, recommend completely limiting the number of day-to-day user accounts in this group (with the one exception being the Domain Admin account – which we will get to later). If you need DA access at any point, you should temporarily assign permissions and revoke them the moment these permissions are no longer required.

So, the first step is to clean-up the number of accounts that you have in the DA group, which is easier said than done. It's quite a manual process and you will have to remove the accounts one by one. But don't be disheartened. Once you have a clean Domain Access Group, you can be confident you've taken the first step in securing your Active Directory.

2. Have Both a Standard and Admin Account

If you are in the privileged position of having an admin account, you should be using it with caution. Don't log in to do your day-to-day tasks with a privileged account (by which I mean an account with any sort of elevated permissions – local or domain admin, for example).

You should have a standard account for the everyday tasks that has no admin rights at all. That way, it makes it easier to operate on a policy of least privilege as the standard account can be used to access emails, browse the internet and do other general activities; leaving the Admin account for admin tasks only (such as creating a new Active Directory user).

3. Pay Attention to the Domain Administrator Account

By default, every domain will include an Admin account that will automatically be a part of the Domain Admins group. The use of this account should be limited to activities like domain setups and disaster recovery. The Admin account should not be used by multiple users as and when they require elevated permissions. Should a situation arise when elevated permissions are required, use of their own personal account if far preferable to allowing access through the Admin account.

In addition to restricting access to multiple users, the account should never really be used at all, except in emergency cases such as a disaster recovery. The password should be unbreakable and almost absurdly long/complex. No one should know what that password is, and it should be kept behind lock and key. We cannot stress enough the importance of ensuring that this account is secure.

4. Is the Local Administrator Account Required?

So, most system administrators will be aware of the Local Administrator Account; it's a fairly well-known account in Domain environments. However, there is some debate as to whether this account is required at all.

There are a number of issues associated with this account, mainly down to the fact that it is so well known and widely accepted. Firstly, the fact that most Sysadmins know about this account means that most attackers know about it to, making it a popular point of entry for attack. Even once you rename the account, the SID remains the same and attackers know this.

5. Introduce Passphrases

Obviously, the longer and more complex you make your AD passwords, the more secure they are going to be. But no one likes having to remember 20-character passwords with random special characters laced throughout. They are very difficult to remember, and this can lead to people writing down a physical copy of their passwords. Insider threats can arise when users get their hands on the passwords to privileged accounts, so let's not make it easy for them. Instead, one common method to get around this is to think not in terms of pass "word" but pass "phrase".

Hackers have at their disposal long lists of passwords that they can rattle off and you would be surprised at how many of us use passwords that are generic and easy to hack. Passphrases can be easier to remember,

as they are just two or more words that make a phrase memorable and specific to the user. They are harder for hackers to get a hold of, as long as the phrase itself is not generic.

Passwords should also be updated very regularly (once every 90 days at least) to ensure that even if you are the victim of an attack, it won't continue for prolonged periods of time.

6. Clean up Old and Unused Active Directory Users and Computer Accounts

A common method for attackers to try and breach into an organization's Active Directory through unused, "stale" accounts. If a user leaves the organization, a process should be put in place to ensure that his/her AD account is disabled. Having large numbers of unused accounts can lead to issues with reporting, the speed of group policy and also create a larger attack surface for potential hackers.

7. Scan, Patch and Use Up-to-Date Software

Microsoft quite often will build in defences against the latest cyber-security threats into the most up-to-date versions of its operating systems. Ensure that you and all other users in your organization are running the latest version of Windows OS. Those pesky Windows updates are there for a reason!

Similarly, attackers will be quick to exploit known vulnerabilities. Just as there are IT communities sharing tips on how to secure your IT infrastructure (such as SpiceWorks and TechNet) there are communities of attackers sharing tips on how to exploit weaknesses. One quick way to ensure that you are as secure as you can be is to perform regular scans using third-party tools to determine where your areas of weakness are and patch them immediately.

8. Implement Two-Factor Authentication

Two-factor authentication (2FA) is a great way to ensure that your account is as difficult to compromise as possible. A password is fairly easy to hack, but both a password and security key (for example) can make it near-impossible. Many sites are now using methods of 2FA to ensure that, even if a password was compromised, illegitimate access cannot take place. Vodafone, for example, require users to enter a unique code that is sent via SMS after the correct login details are provided. Only the user with access to the device will be able to complete the login.

Whilst there are examples of 2FA being fallible (see the Reddit breach this year) it is still far more secure than simply using a username and password. Let's take a phishing attack as another example. Say one of your users fell for a phishing attack in an email and entered their login information onto the attacker's site. The attacker would attempt to login using this information but would be blocked by the 2FA. Not only that, but if the 2FA was linked to the user's device, they would be notified that someone was trying to login to their account.

9. Monitor and Audit Active Directory Changes and Events

Ensuring that you are able to continuously and proactively audit active directory changes is a critical part of ensuring AD security. The native auditing settings that exist within Active Directory are hampered by the fact that they provide no real actionable insight. It's reactive, meaning that if you are trawling through raw logs, you're probably too late to prevent the damage an attack has done. You will also find it difficult to get the information you need to investigate a particular incident, as the native audit processes generate a lot of noise.

To solve this, it's best to look to third-party Active Directory Auditing Solutions that can automate much of the process and provide you with real time alerts and reports. The main things you should be looking out for are who has permissions to what and when have these permissions changed? Knowing the answers to these two questions will a long way to helping you establish that principle of least privilege.

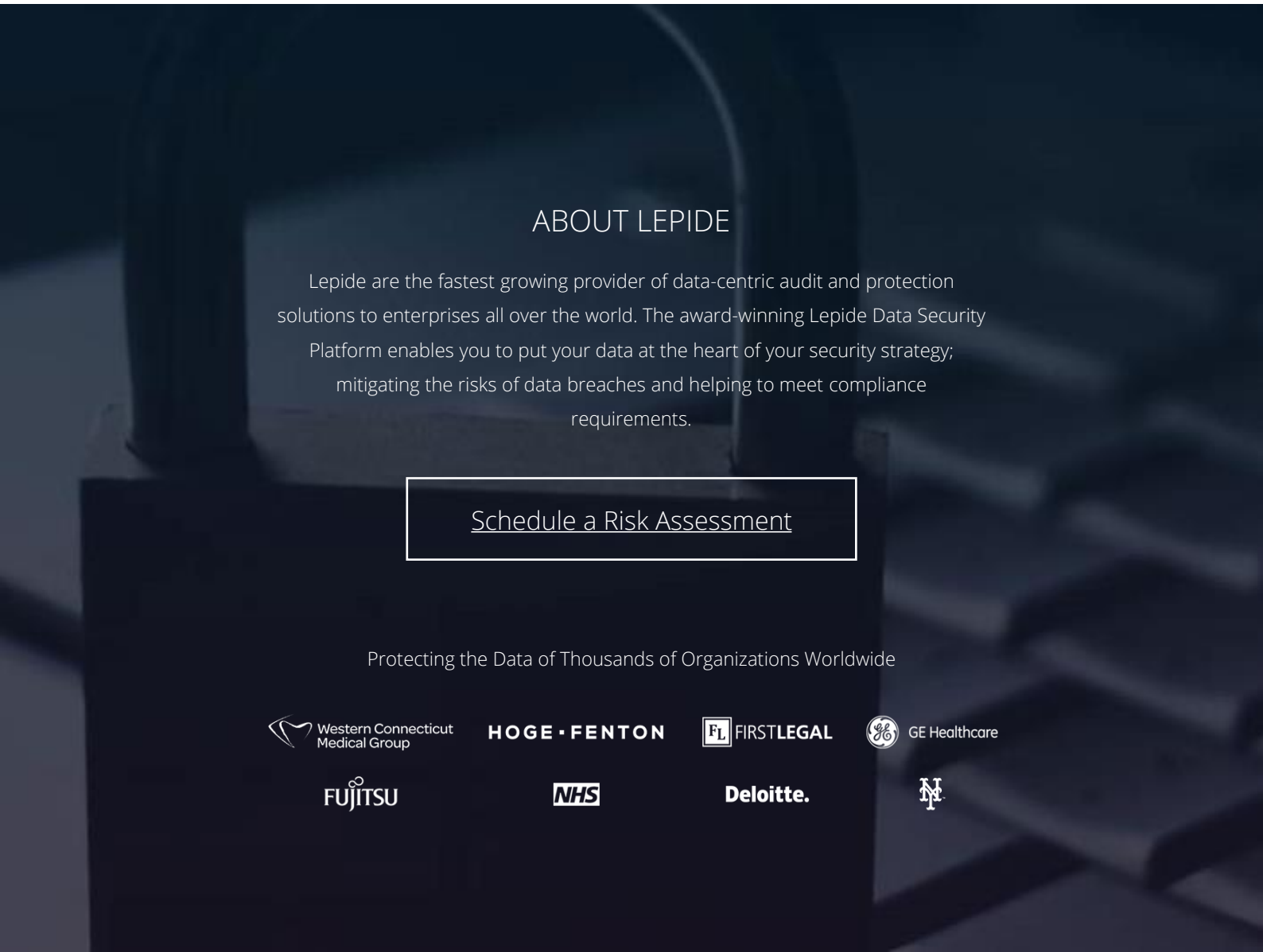
10. Plan for Compromise

Hope for the best, prepare for the worst.

If the worst happens and your organization suffers a huge data breach or ransomware attack, do you have a plan of action in place? Do you know who you need to notify in the event of a breach? Are you able to quickly determine the source of the breach and prevent further damage being caused?

All your users need to be aware of their responsibilities in the event of such incident. This includes creates a detailed incident response plan, complete with responsibilities, policies, procedures etc. Your users should be taken through this plan and drilled on how to respond in a worst-case scenario.

Passwords should also be updated very regularly (once every 90 days at least) to ensure that even if you are the victim of an attack, it won't continue for prolonged periods of time.



ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning Lepide Data Security Platform enables you to put your data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.

Schedule a Risk Assessment

Protecting the Data of Thousands of Organizations Worldwide

Western Connecticut Medical Group · HOGE · FENTON · FIRSTLEGAL · GE Healthcare · FUJITSU · NHS · Deloitte. · NYC