

Securing Active Directory against common attacks

Organizational security is a complicated thing – not just because of the technical aspects. It requires bringing together members of various teams to value security in the same way. It means exposing common misconceptions, like; *a firewall is enough, individual devices are secure, and hackers aren't interested in our data.* Before it can work, it will entail a better understanding of your IT infrastructure.

Organizational security begins with Active Directory

At the heart of your organization's computers, users, and IT infrastructure, you will find *Active Directory*. Used to mirror the corporate structure of a business, Active Directory houses sensitive data for more than [90%](#) of all organizations. On any given workday, users with active accounts collectively authenticate up to [10 billion times](#).

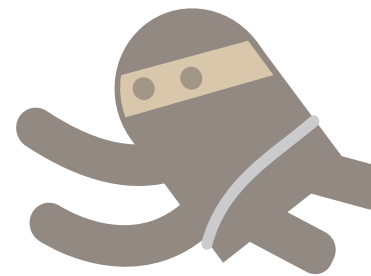
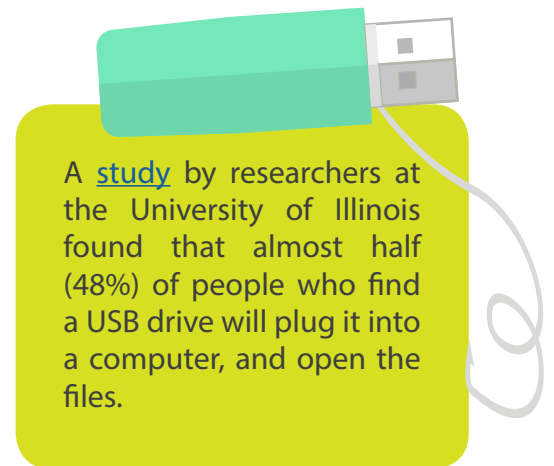
While Active Directory is designed with security in mind, its possession of the crown jewels makes it an attractive target for hackers. Their strategy is methodical – find a vulnerability, it could be as simple as [USB baiting](#), a social engineering technique accomplished by planting USB sticks with malicious content at places where users of the target network/system are likely to find them. When access to a workstation is obtained, use a publicly available tool (the same ones available to penetration testers) to move laterally from one compromised machine to another. Escalate privileges to gain administration rights (even with basic access, attackers can escalate privileges and obtain administrator access in less than [72](#) hours), and finally, steal data!

As attacks get more sophisticated, thanks to automated tools, poor Active Directory hygiene can put your organization at risk. The best practices provided below address security vulnerabilities in your organization, and serve as barriers for attackers.

Starting with the weakest link

You are only as secure as your weakest link. End users continue to be a primary target for attackers. While they no longer fall for letters from a Nigerian prince, they are finding it harder to avoid today's advanced attacks. The public availability of their personal information (thanks to social media), enables social engineers to better target and entice users to click malicious links, or download harmful software.

Most employees want to do the right thing, and a security awareness training program is a step in the right direction. The program should be completed by all new employees, and followed up with periodic training on an annual basis. Moreover, if your organization is bound to compliance standards, the training should be designed with those requirements in mind. The topics should help users identify potential threats, such as phishing, and social engineering, as well as the steps to take when something seems suspicious.



[91%](#) of cyberattacks begin with a spear phishing email

Assume breach

Hoping for the best, and preparing for the worst. *Assume breach* is a relatively new approach to security in response to today's threat landscape. IT perimeters are weakened as laptops, tablets, and smartphones, and bring your own device (BYOD) have taken over the workforce. Every organization needs to assume attackers can get in or they have already gotten in – it's not a question of *if*, but how long. Hackers are not always interested in gathering data within a day, instead they could monitor data over a period of time. Interestingly, the mean number of days that an attacker resides within a victim's network before detection is [200+](#) days.

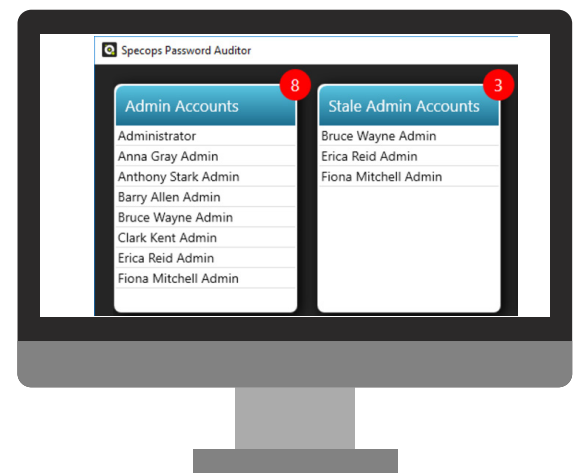
Do not assume the network or neighboring systems are secure. A zero trust position entails applying additional controls around Active Directory. A real-time monitoring system along with alerting is an important part of early detection. Cataloguing past activity will provide an easy comparison of current state and past state. Interestingly, [66%](#) of breach victims had sufficient evidence within their logs to discover the breach. Finally, regular password changes can help protect your system from users who tend to reuse passwords – if their password is compromised elsewhere.

Who should have privileges?

If you frequent IT forums and blogs, you are already familiar with this guidance. Administrator privileges should only be granted to users performing tasks that span across Active Directory domains, or activities that require elevated permissions. To ensure accountability and move beyond a single point of failure, each administrator should have their own admin account – as opposed to a shared generic account with full rights. Furthermore, each administrator should have a separate user account, for day-to-day activities. For maximum security, a physical machine locked down to access only the internal server should be used for administrator tasks. For low level activities, a virtual machine inside the physical machine can be granted outside access, without access to the host operating system that contains the elevated access.

Finally, watch out for any stale admin accounts as they can be used to access resources without being noticed. Our free tool, [Specops Password Auditor](#), identifies stale admin accounts by reading the *lastLogonTimestamp*.

One way of handling administrator privileges is through delegation. Custom delegation groups should be in place to set privileges at the lowest level required for their responsibility. For example, common helpdesk tasks, such as unlocking accounts, and resetting passwords, do not require full control over an Organizational Unit.



Inside-out

Employees, contractors, service providers, and other insiders are in an opportune position to compromise data. While the term *insider threats* often implies a deliberate wrongdoing, it can also encompass users that are careless or unaware of organizational security policies. Regardless of intent, there are some effective measures for stopping this threat.

End-user training is an obvious start. Employees need to know what security policies are in place, and why. Next, you need a process for de-provisioning users that begins with immediate IT notification of any user changes. IT will have to disable/delete the relevant account, and remove the user from all groups and distribution lists. Temporary staff, contractors, interns, and visitors should have accounts with expiration dates. If temporary access to sensitive groups is required, you can assign temporary group memberships with automatic start and end dates.

Get physical!

Digital based security is the hot-topic, but you still need a physical security policy. Depending on your organization, this can range from locks, access cards, and surveillance to equipment and device security. Remember, no amount of digital security can help if an intruder can get their hands on your server. Lock up the server room and ensure that only the right personnel can get in. Do not forget vulnerable devices, such as unused laptops, and even printers, which can be used to make copies of recently printed documents.

Authentication

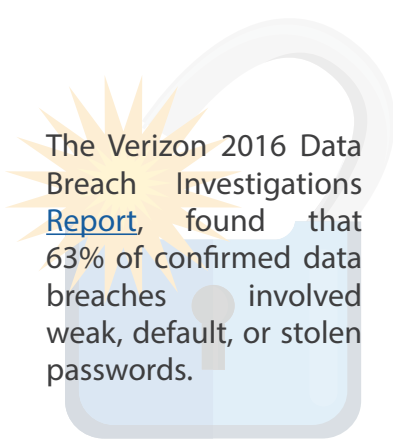
User authentication usually relies on a single factor – the password. Many of the recent data breaches were the direct result of compromised passwords. Users have to deal with more and more passwords, the average number of accounts per internet user is predicted to be a whopping [207](#) by 2020, but we still have not gotten any better at making them harder to crack.

With password attacks so powerful and prevalent, you need to consider existing password policies alongside a user-friendly authentication system. The best practices outlined below are a great place to start:



Turn on MFA

Use multi-factor authentication everywhere you can, especially for privileged users or when accessing critical system such as self-service password reset. [Specops uReset](#) requires users to authenticate with multiple identity services - ranging from identities they established themselves (e.g. social media) to ones that turn a smart phone into a high-trust identification device.



The Verizon 2016 Data Breach Investigations [Report](#), found that 63% of confirmed data breaches involved weak, default, or stolen passwords.



Encourage length and randomness

Size matters, and longer is stronger. Shorter, passwords are prone to brute-force attacks. Longer passwords are mathematically stronger. Passphrases, a combination of words that are meaningless together, are easier to remember and harder to crack.



Ban common passwords

As long as people continue using common/predictable passwords, dictionary attacks will continue to work. Attackers can use multiple dictionaries including foreign words, phonetic patterns, and lists from data breaches such as LinkedIn, Gawker, and Adobe. With the right tools in place, such as [Specops Password Policy](#), any dictionary list can be banned from being used in the organization.

Next steps

Active Directory security is a moving target, and while the periodic security audit will ensure that it is being properly managed, keeping an eye on daily changes is just as important. The best practices outlined in this document are certainly a good place to start if organizational security is keeping you up at night. For a graphical overview, we recommend our [7 Common Mistakes SysAdmins Make](#) Infographic. For a more proactive approach, we recommend taking advantage of free tools such as [Specops Password Auditor](#) that can scan your Active Directory and detect security-related weaknesses, specifically related to password policies.

ABOUT SPECOPS

Specops Software develops unique password management and desktop management products based on Microsoft technology. We build on top of Active Directory and Group Policy with innovative, simple, and cost-efficient solutions for organizations around the world.

specopssoft.com/blog