2017 Skyport Systems Active Directory Assessment Findings

SKYPORT SYSTEMS

Over 90% of all organizations use Active Directory (AD) for user authentication and authorization.

AD controls users' access to data, applications, computers, storage, and the network in both the enterprise and the cloud, making it one of the most sensitive applications in the enterprise.

Because of its ubiquity, cyber attackers often target AD installations. According to a 2016 Verizon report, 63 percent of confirmed data breaches involved stolen or compromised privileged credentials and compromised domain controllers. Successful attacks against AD domain controllers or domain administrator credentials can be devastating because the blast radius reaches nearly every system.

The likelihood and impact of AD compromise

IT departments continuously patch AD vulnerabilities, and risk management teams use models to prioritize which issues to address based on the likelihood and potential impact of an attack.

Despite this, attackers can, and do, find a way into the enterprise using attack techniques such as email phishing, malicious web content, rogue USB sticks, and exposed, unpatched systems. Once they have access to one workstation, they can then use publicly available tools to move from the first compromised machine to others, gradually elevating their privileges until they control an administrative account or a domain controller. Many attack tools that penetration testers use are publicly available, and cybercriminals can readily access these tools, too, on sites such as GitHub. This method of break-in is common because it's simple and often successful.

Professional penetration testers consistently point out that it takes very little effort to find and exploit AD vulnerabilities while remaining undetected. AD tops the rankings for both likelihood and impact and is the leading contender for applications that you need to safeguard.

The Four Pillars of Defense

AD security experts advocate these four pillars to protect against cyberattacks

1. **Implement AD hygiene** by limiting who has domain admin privileges, preventing low-security tasks from being done from high-security accounts, configuring secure password policies, frequent patching, and strictly limiting admin group membership.

2. **Make admin workstations secure** to prevent credential theft and misuse. To prevent infecting domain controllers (DCs) with malware, you can implement secure administrative workstations (SAWs) for managing DCs and require multi-factor authentication to access these workstations.

3. **Protect DCs** against insider and external threats. Place your DCs behind firewalls, with continuous protocol and event inspection to detect and prevent attacks. Lock down inappropriate ports and protocols, and do ongoing verification of clean source.

4. **Build an isolated admin forest** if you have a large or complex enterprise. Reserve the forest for privileged accounts that access AD and related management tools, including patch management, backup, and domain management. The admin forest should be isolated and secure.

Where and how these defenses break down

Over the last year, Skyport Systems conducted AD security assessments based on the four pillars of defense with large and small organizations. Each assessment was an extensive evaluation of the organization’s current AD implementation, and included 100 questions related to the health of the organization’s AD infrastructure.

Here are our key lessons learned from these assessments, along with operational implications for reducing risk within organizations.

1 **Implement AD Hygiene**

2 **Make admin workstations secure**

3 **Protect DCs**

4 **Build an isolated admin forest**

Key Lessons Learned

Implementing AD hygiene

Most organizations focus primarily on implementing AD hygiene. The organizations that we assessed achieved the highest maturity score in this area. However, there are still significant gaps. Over 50% of the enterprises assessed allow administrators to use the same account to configure AD as they use for everything else. This means, when logged in as an admin, everything that you do has elevated rights, including opening attachments and downloading from the web, which are avenues for malware.

Over
50%
of the enterprises
allow admins
to use the
same account

Making admin workstations secure

Microsoft recommends implementing secure administrative workstations (SAWs) for management of AD. Malware, once installed on an administrative workstation, enables the attacker to take over all of the admin's privileges. However, less than 10% of customers assessed have implemented a SAW.

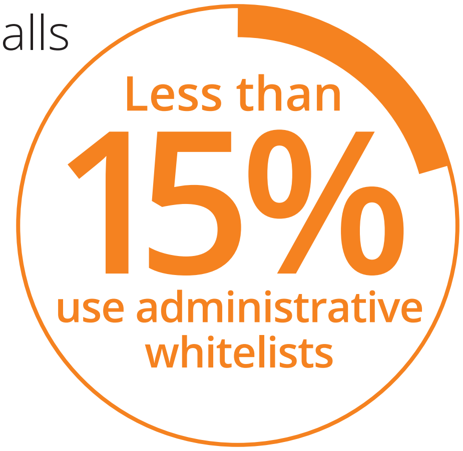
Less than 10% of customers have implemented a SAW

The assessment data also showed that fewer than 25% of customers use multi-factor authentication (MFA) for AD administrator accounts. This means that a compromised password can lead to the ability to access all your sensitive systems.

Fewer than 25% of customers use multi-factor authentication

Protecting DCs against insider and external threats

It is best practice to severely limit the systems that are permitted to alter the AD configuration (for example, through host-based firewalls and whitelisting of administrator accounts). The data showed that almost no enterprises implemented host-based firewalls for the DCs, and less than 15% use administrative whitelists.



In addition, one of the more common techniques used to compromise AD is theft of golden tickets. However, the enterprises assessed generally had little to no ability to see and stop these attacks.

Building an isolated admin forest

Microsoft has recommendations for building an Enhanced Security Administrative Environment (ESAE), but virtually no mid-market enterprises appear to be aware of, or effectively implement, these guidelines.

0%
Use admin forests

Summary

It seems that most organizations are at significant risk for security breaches related to AD. AD and the privileged credentials stored in it are highly vulnerable.

Not long ago, it required skills and patience to identify and exploit AD vulnerabilities. Today, attacks are weaponized in tools that are effective, free, and widely available. Bad actors are using these tools to automate attacks, using many attack techniques to find ways into the enterprise.

Once attackers have access to one workstation, they can easily move from the first compromised machine to other machines and accounts in the enterprise, gradually elevating their privileges until they control an administrative account or a domain controller.

Our findings show that most organizations lack sufficient rigor related to administrative workstations and communications. Also, few organizations sufficiently isolate and protect their domain controllers. These problems may help to explain why credential compromise has become such a common area for security breaches.

You can protect the AD infrastructure in your organization by:

1. **Raising awareness for AD within your organization:** AD is used to authorize access to nearly every piece of the IT infrastructure—users, data, applications, computers, storage and the network. AD’s reach even extends into services and systems in the cloud.

2. **Evaluating current defenses and comparing them to modern best practices and technologies:** The pace of AD attack tool development has surpassed automated defense countermeasures, and many tools can quickly become outdated.

3. **Establishing benchmarks:** While there is a wealth of guidance and best practice recommendations available, it is difficult to figure out where to start or what will make the biggest impact in securing AD.

Secure your Active Directory Now

Through complementary Active Directory assessments, Skyport helps organizations evaluate current safeguards, compare them to best practices, identify gaps and develop a phased plan to improve protections.

How secure is your Active Directory infrastructure? Contact Skyport today.

www.skyportsystems.com

SKYPORT
SYSTEMS
280 Hope Street
Mountain View, California 94041
855.999.4SKY
www.skyportsystems.com

©2017 Skyport Systems, Inc. All rights reserved. Skyport Systems and SkySecure are trademarks or registered trademarks of Skyport Systems, Inc. in the United States and other countries. All other trademarks are property of their respective owners. Skyport Systems assumes no responsibility for any inaccuracies in this document. Skyport Systems reserves the right to change, modify, transfer, or otherwise revise this publication without notice.