Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Now’s the time to rethink Active Directory security

Guido Grillenmeier, Semperis

Winding back the clock 21 years to the turn of the millennium would be a strange experience, given the world we live in today. Even putting the Covid-19 pandemic and its still-unfolding impacts to one side, life has changed a tremendous amount in the past two decades.

In the year 2000, Spotify, Facebook, Instagram and Uber didn’t exist, while Netflix (remember subscription-based DVD and CD rentals?) and Amazon were brand new. The Internet was still somewhat novel and the iPhone wouldn’t emerge for another seven years. The list could go on, but the point is that technological development in the world of IT has accelerated exponentially in the past 20 years or so.

Despite this evolution, one foundational innovation has prevailed, largely unchanged, throughout this period.

Pain point

Back in the 1990s, directories were a major administrative IT pain point for businesses. The working world was supported by a series of small directories that made sharing key data and files a tricky and laborious task. To access shared files, users would have to log into each individual file system, with various credentials, software and applications required.

With the introduction of Windows NT in the mid-1990s, Microsoft already helped many companies to adopt the ‘domain’ concept, allowing multiple systems to be joined together in a circle of trust, effectively reducing the segmentation of user identities into separate directories. But while Windows NT allowed Microsoft to successfully enter corporate datacentres, the inherent scalability limitations of Windows NT domains meant that multiple domain directories needed to be built and managed in different geographies with trusts between them to share access for the various users of a company. This became increasingly challenging as not only businesses but also their IT systems would jump onto the globalisation bandwagon.

Enter Microsoft Active Directory (AD) – which was at the time a revolutionary technology – originally released with the Windows 2000 server operating system, and one that continues to support much of the hyperconnected world of work that we inhabit in the modern era.

“It was in many ways ground-breaking. Global companies could scale their directories, no longer having to rely on many, small and hard-to-manage domains”

It was in many ways ground-breaking. Global companies could scale their directories, no longer having to rely on many, small and hard-to-manage domains. Indeed, there were other directories fighting to offer the same benefits for corporations. Novell eDirectory, for example, was widely used. Yet Microsoft AD prevailed above all others for one core reason – it was open.

Open or secure?

‘Open’, in the case of directory services, means ‘readable by anyone’, which is still the default in any AD configuration today, at least for the authenticated user – i.e., any user that is logged in to a computer with his or her AD account. Novell chose the more secure path with eDirectory, requiring administrators to specifically grant read permissions to every section required for users and applications, adding an operational hurdle to on-board and integrate new applications. This openness – which was Microsoft Active Directory’s biggest strength 21
years ago – has, however, since become its most concerning weakness.

At launch it was highly acclaimed because of its ability to integrate easily with applications and provide single sign-on across a complete business environment, thereby reducing the hassle of password management and directory management with broad-reaching authentication. It is because of this openness and ease of integration that AD remains a foundational piece of infrastructure for 90% of businesses. Indeed, it is used on such a broad scale that most business applications today do not even have their own directory, instead relying on the user to be Windows authenticated.

Yet this openness has also created vulnerabilities.

**Unconstrained delegation**

Take specific Kerberos features, for example. Kerberos is a computer network authentication protocol that works on a ticketing structure to allow nodes communicating over corporate networks to provide their identity to one another in a secure manner. It was a highly safe protocol for its time, which the meaning of its name emphasised: In Greek mythology, Kerberos is a three-headed dog that guards the gates of the Underworld to prevent the dead from leaving.

One special capability that Kerberos offered was that of delegation, which worked to ensure that a user accessing an application on one system would only be able to access specifically shared information (often a file, or specific data in a database) with that application on another system while preventing access to other data. From a technical perspective, this was achieved by the user being impersonated by the application while it accessed the other service on the user’s behalf. The app – or rather the server hosting the app – was ‘delegated’ to use someone else’s Kerberos authentication – ie, it was granted the right to forward the user’s Kerberos ticket to another system as if the user was directly accessing that other system. With the introduction of AD in 2000, it was possible to configure Kerberos delegation only in an ‘unconstrained’ way, meaning that the application was able to pass on the user’s Kerberos ticket to any other system.

Today, this has been rendered obsolete by much more secure and seamless ways of sharing data. But unconstrained delegation settings are still prevalent on a significant number of systems, often because the potential impact is not understood by the operators of AD or the owners of the specific server object chosen to be configured this way. Today’s hackers can use this to impersonate any given AD user on any other machine.

Combine this with the knowledge that a hacker can use any unprivileged AD account to read almost all attributes and objects in AD, including their permissions, allowing them to find computer accounts in any domain of an AD forest that are configured with unconstrained delegation, and you get an idea of why the default AD openness has become a vulnerability.

In the worst case, the intruder could gain access to such a system and furthermore find that your domain controllers still have the printer service (spoiler) running. The printer service is by default always turned on, on any Windows server – it should be disabled by IT administrators on any server that doesn’t need it, but many fail to do so. In our scenario, a hacker can then invoke a domain controller to authenticate to the computer with the unconstrained delegation and use the so-called printer bug to invoke an authentication request from the domain controller to the captured computer. Although there is nothing to print, through this process a threat actor can secure a domain controller’s Kerberos ticket and will thus have compromised your AD domain and forest.

Constrained delegation is a little more secure, but it’s still attackable.

**Opportunity for threat actors**

There are more examples of how the three-headed dog has lost some of its protective strength over time. More and more attack vectors against it were found and documented publicly, thus allowing cyber criminals to use them during their attack path against AD.

Another good example comes from service principal names (SPN), this being the way in which a Kerberos client uniquely identifies an instance of a service for a given Kerberos target computer (eg, a SQL database) and also helps to locate the related service account (eg, the SQL service account), which is used by the service itself to authenticate to AD.

“Security researchers have found SPNs themselves being easily attackable through information that they pass on during the Kerberos authentication to the service – namely the hash of the password of the service account itself”

This mechanism allows users to leverage Kerberos for authentication to a SQL database rather than authenticating with the less-secure NTLM protocol and has become the standard for integrating AD authentication for SQL implementations in most companies. The downside is that security researchers have found SPNs themselves being easily attackable through information that they pass on during the Kerberos authentication to the service – namely the hash of the password of the service account itself – even if the requestor does not proceed to authenticate to the service. That hash is now subject to offline cracking attempts, which a variety of publicly available tools, such as John the Ripper, are happy to help with.

Due to AD’s openness, an intruder is easily able to find privileged SPNs in the environment (think of an SPN attached to a domain admin account), creating another easy attack vector capable of being manipulated to provide high privileges and full visibility. This combination of control and visibility can be incredibly dangerous. When you have the highest permissions, you have full control and can take down a business and request ran-
som. But you’re also able to use it for reconnaissance prior to this.

“What are the privileged accounts? What are the vulnerabilities that I can go after?” For threat actors, Active Directory acts like a map, highlighting points of weakness in the environment. Once in your network, a hacker will use AD to seek out and target your important data, extract it, encrypt it and demand ransom from you. And many businesses are simply not prepared for such an eventuality.

It creates a conflict. Do you have proper back-ups to recover your whole business – including your Active Directory – quickly without paying a ransom? For many the answer is no – they are forced to pay the ransom and the hackers move on to another similarly unprepared target, creating a vicious cycle.

The SolarWinds example

So, how often is AD leveraged in such a way by threat actors? The SolarWinds breach, aka Solorigate, stands as one of the most infamous recent examples, where AD was instrumental in a large-scale supply chain attack that affected tens of thousands of high-profile organisations, including US governmental bodies.

SolarWinds itself is a leading global provider of IT solutions, its network management tool Orion being a leading software that these organisations used to secure, sustain and protect their own networks. In the SolarWinds attack, hackers managed to successfully inject a trojan into the Orion software, this then having been spread via a periodic download mechanism that the company’s customers had installed. Having begun as early as March 2020, this state-sponsored attack and its trojan were not found until December that year.

It was a highly malicious attack that affected countless Fortune 500 companies and vitally important governmental bodies in the US. But how was such a powerful supply chain attack allowed to happen? This is where AD and on-premise leaks come in.

SolarWinds had set up a federation service between its own on-premise directory services and the cloud, where it managed its Orion software code. In such a setup, the cloud puts full trust in the federation service to correctly prove a user’s identity, allowing you to log onto it with your on-premise identity, often coupled with a third-party multi-factor authentication (MFA) solution. By signing on this way and receiving a properly signed federation token, your cloud provider trusts you with the authentication and will then authorise authenticated users by providing them with access to the requested cloud resources.

“The cloud puts full trust in the federation service to correctly prove a user’s identity, allowing you to log onto it with your on-premise identity, often coupled with a third-party multi-factor authentication (MFA) solution”

In the case of the SolarWinds attack, the intruders were able to use this federation to their advantage for stealthy access to the Orion source code hosted in the cloud by stealing the token signing certificate. It was the first of its kind to be known to have used a golden secure access markup language (SAML) attack. Federation happens via protocols such as SAML, used to pass on a security token to that trusting party. But how did the intruder get this token signing certificate?

We come back to where the breach occurred: the token signing certificate was secured by the service account for AD federation services, which is hosted like any other account in the on-premise AD. Once the threat actors gained access to the on-premise AD and the AD FS service account, they had a way of reading the certificate and using it to create their own SAML token to gain access to the SolarWinds cloud resources. As a result, the chain of events shows that Active Directory security was one of the key weaknesses on the attack path of this major breach. Indeed, it is a prime example of a company having believed that its cloud systems were secure when they were not, owing to AD and its on-premises reliance.

While the cloud was separated, the trust between the vulnerable on-premises systems and the cloud provided access to the network, creating a bridge that the threat actors could use to intrude upon the company’s cloud resources.

Addressing the challenges

From a security perspective, AD is the source of many headaches. Microsoft has failed to invest into a security-related update for AD since 2016, even though this core identity system is still used by 90% of businesses today.

The easiest solution would be to eradicate AD, but that is simply not going to happen. It is a legacy solution, but it is not going to go away anytime soon with so many companies and hundreds of thousands line-of-business apps still reliant upon the technology. That said, it is not a lost cause and there are steps that companies can take to ensure that they protect themselves.

“You can begin to identify, understand and prioritise which vulnerabilities to address. It must be a holistic process that leaves no stone unturned in the way of achieving full preparedness”

Indeed, this is a process – the implementation of proper protection protocols beginning with the recognition and understanding of potential vulnerabilities. Conduct a brainstorming session and ask yourself, ‘what would happen if critical systems went down?’.

Companies can address outages by operating with dual datacentres, or a datacentre and cloud hybrid solution, yet they must go further than this and consider what might happen if a critical system like identity management becomes compromised.

Take the time to understand the dependencies to all your business apps. And explore the dependencies between...
When ransomware strikes, what’s your recovery plan?

Stephen Young, AssureStor

Preventing a ransomware attack requires a tiered approach utilising a defence-in-depth methodology. This incorporates user training, email filtering, virus detection, firewall configuration, edge security and activity monitoring, combined with an array of additional techniques where budget, resources and expertise allow.

However, at the point that a business is alerted to a ransomware attack, security has already been circumvented and the fate of crucial data is in the hands of cyber criminals. With extreme speed, servers and PCs and other devices connected to the network will experience encryption. The well-documented NotPetya attack at Maersk in 2017 saw 7,000 servers, 49,000 PCs and 150 DCs encrypted within seven minutes – every device connected to the network was encrypted, including backup systems. Recovery took nine days to implement and cost the business approximately $35m.

At best, after payment of a fee, an organisation’s data may be unencrypted, but there is still a chance that it has been released onto the dark web, generating more revenue from the attack. Even paying a ransom does not guarantee that any data will be unencrypted and there is a strong argument that it may encourage more demands. The worst-case scenario is that data is unrecoverable, gone for good. Regardless of the course taken, regulatory bodies like the ICO will penalise the business and reputational damage will further affect the organisation’s fortunes.

"Even paying a ransom does not guarantee that any data will be unencrypted and there is a strong argument that it may encourage more demands"

Absolute confidence in a recovery plan, with regular testing and comprehensive planning in anticipation of such a situation, gives a business the opportunity to conduct data forensics immediately. This will allow technical staff to determine the nature of the attack, when the firm was attacked, and what has been infected, encrypted or paralysed. Armed with this information it is possible to implement a recovery process factoring in these parameters, with a good chance that downtime will be reduced with minimal data loss, and presumably costs.

If planning for such an event has not been fully considered, it is unlikely that a business has been able to thoroughly test for an attack or outage of such significance, leaving the organisation exposed to extremely damaging outcomes. Testing is crucial and a positive outcome from disaster recovery (DR) tests is critical if a business is to be in a position to recover. Consider the purpose of a DR test: is it to establish that running a test can be accomplished, or is it to conclusively determine that the business can actually recover from a disaster?

Restoring from backup

A recovery position could be to revert to your backups, which may be based on tape, disk or a cloud service. With a successful backup to fall back on, you should be able to restore to a desired recovery point, replacing or removing your authentication process and the cloud. With a federation-based authentication system, you could end up in hot water very quickly.

Once you have understood these dependencies, you can begin to identify, understand and prioritise which vulnerabilities to address. It must be a holistic process that leaves no stone unturned in the way of achieving full preparedness. If a boat is leaking and you don’t have the equipment to fix a leak, then the boat will sink. Equally, if you only spot one of multiple holes that are leaking, the boat will still sink. It is vital that a company comprehensively understands all potential vulnerabilities to address them and prepare as necessary.

If nothing else, the SolarWinds attack serves as an important learning curve, demonstrating the catastrophic effects that might occur when an AD-based attack takes place. Given the growing and increasingly complex threat environment, it has never been more important to address AD-led vulnerabilities than it is today.

About the author

Guido Grillenmeier is chief technologist with Semperis. Based in Germany, he has been a Microsoft MVP for Directory Services for 12 years. He spent 20-plus years at HP/HPE as chief engineer. A frequent presenter at technology conferences and contributor to technical journals, Grillenmeier is the co-author of Microsoft Windows Security Fundamentals. He’s helped numerous customers secure their Active Directory environments, and supported their transition to Windows 10/m365 and Azure cloud services.