Issues in Information Systems
Volume 22, Issue 3, pp. 107-113, 2021

DOI: https://doi.org/10.48009/3_iis_2021_120-126

Enterprise network security from cloud computing perspective

Katherine Rongstad, *University of Wisconsin – Eau Claire, Rongstkr9975@uwec.edu*
Ruidong Zhang, *University of Wisconsin – Eau Claire, Zhangr@uwec.edu*

Abstract

This paper explains why Active Directory is becoming the core of enterprise security, and how identity management moving from on-premises Active Directory to Azure Active Directory is encouraging IT professionals to redesign their IT infrastructure. This paper is partly based on online research that is drawn from Attosol Technologies and Cyware Social resources. A case study was also conducted to further understand key concepts related to enterprise security.

Keywords: Active directory, Azure active directory, enterprise security

Introduction

Active Directory was developed by Microsoft to manage domain networks. It is the avenue by which users, customers, partners, the internet of things (IoT) and other devices authenticate to a system and obtain the ability to move within that system (What is Active Directory Security and why is it so important?, 2019).

Azure Active Directory, or Azure AD, is Microsoft's cloud-based identity and access management service which allows employees to sign in and access resources such as Office 365, the Azure portal, and thousands of other external software as service applications online as well as internal applications and intranet.

The main threats include ransomware, phishing, viruses, hackers, email spam, and even social engineering today which are targeting the people of the organization. These breaches happen through the use of default security settings, weak passwords, privileged access to non-essential employees, lack of timely patches on the AD servers, and unreported or unauthorized access are a few examples (Understanding and Defending Against Active Directory Threats, 2019). Further data related to the cybercrime and cybersecurity statistics can be seen online on the Comparitech website located in the reference page (Zaharia, 2020 Edition).

The people are the greatest asset that an organization can obtain and through the people is also where the greatest security concerns arise. Computers are the avenue that give way for cyber security attacks to come through by either having holes in the firewalls, the design of the network, or by human doing. The strength of the internal network and all data infrastructure is made stronger by the people planning it, designing it, securing it, and working with it every day. The network administrators, help-desk employees, CIOs, and even those who do not control the technology, but their job involves it, have a responsibility to be aware of the danger. It is up to those as Information Technology Professionals to build a system and mitigate the threats so that when the system is tested, it can withstand intentional and unintentional attacks. In the following best practices section, you will find ways to help prepare your system for Active Directory security and whole system security management.

The paper is organized into two sections. The first section regarding why Active Directory is the key to implementing successful security within a company. The second section takes a futuristic viewpoint on recognizing the extended benefits of Azure AD and how moving identity management to the cloud, at least by a hybrid approach, is beneficial for today's businesses. This is a topic that all Information Technology individuals should uphold as important and influential in order to experience the full power of having a well-managed identity directory.

Azure Active Directory

Azure AD is not on-premises Active Directory. They both are identity stores and that is the extent of the cross over. Both use completely different protocols for authentication as Windows Server Active Directory was not designed for web-based applications. In opposition, Azure AD was designed to support web-based services. Azure AD does not have the same group policy and GU structure for organization as Active Directory currently holds. Instead, in Azure your organization will be a tenant where the IT administrator may manage all the users with their passwords, permissions, user data, and more in groups instead of an OU structure. To begin moving towards a hybrid identity or someday a complete cloud management of the enterprise, the company must begin by organizing their current Active Directory. If AD is not stable, organized, and systematic, the transition will not be easy to pursue.

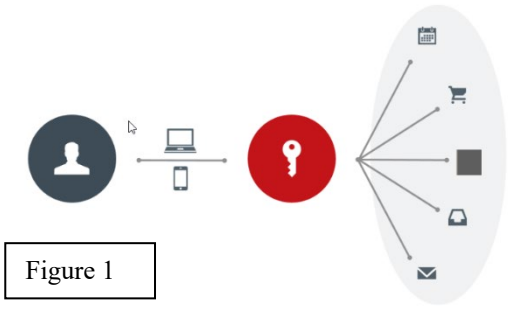

Figure 1

Figure 1 on the left illustrates the power of using Azure AD authentication which allows for one account to authenticate that user's many accounts, systems, and more. Further information on this will be described in the Simplified Access paragraph below. One hybrid approach is Azure AD Connect where Active Directory is still locally based on-premises while also syncing with the cloud. Azure AD does have the power to run your whole system from the cloud, but many companies are beginning with a hybrid identity. Azure AD Connect gives companies the options on how they want their accounts identities and passwords to be authorized by one of three methods: password hash synchronization (PHS), pass-through authentication (PTA), or Federation (AD FS). ADFS allows your on-premises Active Directory to control the authentication without having to use the password hashing needed with password sync. Pass-through authentication is used to validate users' passwords right against the on-premises AD. Federation integration is used to implement the ADFS structure which needs ADFS servers deployed and gives IT professionals management capabilities. Synchronization is allowed through the ability to create users, groups, and other objects that sync between on-prem users and that they match the groups in the cloud. Synchronization can also include password hashing. One final feature is health monitoring where Azure AD Connect Health allows you to oversee this process in the Azure portal.

The power of Azure AD can be harnessed with single sign on (SSO) as it allows one account to access all their many approved applications. Microsoft sees that the more accounts people are required to have, the more likely there is to be a security breach with weak passwords. There are many benefits of Azure AD, but this paper discusses the main reasons below.

Benefits of Putting AD in Cloud

High Availability

Availability is the uptime or the accessibility of Azure AD and other software as a service provision. This access can occur from your authenticated account anywhere. Azure AD stays highly available by routing across 28 data centers in different locations across the globe. Alex Simons states that, "Azure AD is a high availability, geo-redundant, multi-tenanted, multi-tiered cloud service that has delivered 99.99% uptime for over a year now" (Simons, 2018). This is a benefit because some software applications still go down for updates and changes today, but Microsoft's management applications, servers, and everything they offer in the support of every business is a stable foundation of almost constant uptime. One way that they continue their high availability is by the number of servers and how they partition each other by having a primary and secondary location of reading and writing. More information on this process can be found on Microsoft's website (What is the Azure Active Directory Architecture?, 2019).

Simplified Access

Users can be more productive by having a common, single identity with one account to access both cloud and on-premises resources such as the intranet, department specific software, and Office 365 (Outlook, Word, Powerpoint, Excel) to name a few. This not only makes it easier for most active users of the system in the company, but from a management perspective, this creates one location for the overseeing of your company as well. A comment made by John O'Neill Sr. in a Redmond magazine webinar on Azure AD Updates was about if a business' software, print server, and/or Enterprise Resource Planning system were located in the cloud, you do not have to worry about where you or the resources are. Azure AD and cloud-technology in general allow you to simply use the resource at any time in any place.

The single sign-on mentioned earlier can be included under simplified access. By allowing single sign-on to connect a user to all their applications, this would benefit them in accomplishing their job faster by removing the need to gain access with multiple different accounts. One would believe that having multiple accounts would be more secure, but most leaders know that allowing one person to only remember one strong password is easier than them having to remember multiple strong passwords. When people are required to have multiple strong passwords, usually this is only a slight variation or the same exact password for all accounts.

A final benefit of simplified access stems from application proxies. They eliminate the need to change the network infrastructure or use VPNs to access work or on-premise applications because they are now published on Microsoft servers which allows secure remote access (Benefits of Azure Active Directory, 2017). Your applications can be converted to work like any other software as a service application over the internet. Application proxies allow for secure communication and easier access.

Self Service Features

Azure AD and other features continue to be developed for a seamless user interface from administrators to the users. Apart of the benefits of self-service also includes password management which allows users in your organization to reset their forgotten passwords and update them on their own automatically. This allows the technology departments to save time on those automated system tasks. The newest updates to the Azure AD portal used by administrators included user experience updates to the My Apps Portal, Workspace, and the Edge phone app to name a few besides the Azure AD Portal itself. This is a benefit because currently Microsoft is putting great effort into developing Azure AD since it is the future. This

can be compared to less time spent on Office 2019, a one-time purchase application, versus Office 365, the newest and most up-to-date cloud-based version.

Secure Access

Whether you have Active Directory on site or have migrated to a hybrid identity, secure access is easily within reach for your systems. A few features that help achieve this secure access while using the cloud resources include multi-factor authentication, conditional access, privileged identity management, and dynamic groups.

A Case Study

A mid-west university has taken advantage of implementing multi-factor authentication with the use of single sign on. This is used in a variety of related applications from educational to resources to health or fitness websites. Users are directed to the single sign on university logon page. Beyond that page, Duo Security Application is used to confirm authentication a second time. One further development references the Powerful Capabilities section as discussed above. The university uses Azure AD Connect which is the hybrid authentication approach the combines on-premises Active Directory with the capabilities of Azure AD.

Collaboration

This is similar to the shared collaboration between users on Word documents and other projects within the student level except this is within the management console in Azure AD where Microsoft offers Azure AD B2B and Azure AD B2C. B2B says, "corporates can add partners to their project groups and share the information internally without worrying about their identity existence" (Benefits of Azure Active Directory, 2017). With B2C this is for applications used by customers which allows Azure AD to take care of identity management for you, so all you need to accomplish is the creation of the shared application.

Reporting

Similar to the real-time auditing of Active Directory that was mentioned in the first part of this document, Azure Active Directory already allows for easy to use reporting without a third party where security and activity reports are accessible from the portal by administrators. Overviews are available of the possibly compromised user accounts and attempts made to access by non-legitimate owners of those accounts (Benefits of Azure Active Directory, 2017). Cloud application discovery is another reporting avenue to see which applications are not under IT control but are continuing to be used. With this whole management system, when functioning effectively, the whole business system can be operated under the wing of Azure AD as their identity management.

Current Best Practices in Securing AD

Privileged Access Management

This practice involves first controlling the use of who has access to Active Directory, and what branches they have access to within AD. There must be proper control of who has access to what in Active Directory, with giving the privileges only to those who are needed for the proper job roles. A whole team or department does not need access to AD even if only one person needs access to it for their specific job role. Be diligent when access is granted and to what level. Privilege should not be easily granted off what

only your client is saying they need it for. As an Information Technology Professional, one needs to listen to colleagues and clients alike when discerning what type of access, they should have. Identity and access management is something that every organization needs to take seriously. Recognize that your privileged users/accounts have a higher risk than standard user accounts and guest user accounts. Only give those who are an integral part of managing Active Directory access.

This topic of access management not only affects Active Directory users but also makes an impact on access control to other business systems, applications, and networks within the company. Office 365 changes cost depending on the different licenses that you as an enterprise give your employees. Not all employees should receive the license with access to every desktop Microsoft application if they barely use it. This would be an extreme cost compared to if you adapted the Office licenses to what each department or even more specifically for the employee needs.

Separate Administrators and User roles

One way to better control Active Directory access management as discussed above, is by using privileged credentials or in other words, separate accounts that have differentiated access than normal accounts. These accounts have separate usernames and passwords to login into your domain with. This comes in the form of power users, super users, domain users, and more. A username example for the difference is domain\jksmith or domain\pu_jksmith. Same employee but access controls are limited to only pu_jksmith as the power user account.

Without the separation a lack of system unawareness could arise (Privileged Access Management, 2020). If forgotten privileged accounts continue to free float on the network these could be an in for many threats in cyber security. System awareness needs to be controlled. Many security concerns can be eased when you have confidence you are in control of who accesses your network and what they have access to. Regular deletions should be running to delete unneeded accounts.

Real-time Auditing

Real-time Windows auditing and alerting should be an understandable and consistently ran report. Auditing the system is a useful tool because you can visually see the unauthorized access attempts to your system through Active Directory. Through group policies, when new computers, servers, and accounts are created, they all are a part of the automatic auditing. There are multiple companies offering tools to link with your system to see the data in easier to understand graphics such as Lepide, Solar Winds, and more.

AD Backup & Recovery

A crashed Active Directory can pause business processes when all applications on your network need access control to function. An example of this was from a Redmond magazine webinar where they discussed the shipping company Maersk. In a ransomware attack, cyber criminals accessed their network and erased Active Directory except for one domain controlled that was offline because of a power outage during the attack. It still took 9 days to get AD up and running with access to those last drives.

With the backup of Active Directory and sync with Azure AD Connect, Active Directory can be recovered much faster today with the proper mitigations which will be discussed further on below in the benefits of moving Active Directory to the cloud. Your companies AD backup configuration should be kept updated and the disaster recovery process must be practiced for faster recovery. If there is an actual breach to Active Directory, all domain controllers should be able to be restarted from the last secure version. Remote locations of servers should also have physical safeguards where the hardware is not at

risk. If you have a cloud provider managing servers with AD data on them, make sure it is under secure management (Understanding and Defending Against Active Directory Threats, 2019).

Identify & Patch Vulnerabilities

Finding problem areas and fixing or patching these vulnerabilities must be a priority because you do not know when that specific hole, or a combination of them will be the problem you wished you had mitigated for. If there is a delay in the patching, the hole could be forgotten or pushed off too long for the help your system needs. All patches or maintenance processes should be fast and automated as seamlessly as possible for the critical systems and others following it, so that when problems arise there is less left to human error. Also, be diligent in the removing of unused servers, software, or data that is not needed. The more knowledge there is of how the system runs and works with all other pieces, the better the whole Information Technology team can control the flow of people through Active Directory and the rest of your company's essential information.

Conclusion

It is important to know that on-premises Active Directory is still the base of many organizations today, yet those seeking to advance have transitioned to a hybrid system such as what the University of Wisconsin-Eau Claire is using with Azure AD Connect. With the continual change of technology, every level of security must continue to adapt and evolve as the threats within the online realm continue to grow. This is alongside the people's reliance on the public network for not only personal and work devices, but also home, appliances, and their livelihoods as these pieces are now ingrained into the internet of things. Our accounts and passwords make up our identity in the online world which need to be protected as much as our social security or personal identity. Identity management is a topic that must be taken seriously by the enterprises entrusted to best serve the people, their company, and the economy. As the internet continues to eliminate the barriers of connection, all must ruthlessly pursue a secure directory of their users. Data shall be secured and protected, so that threats have no foothold to find. This process starts by securing your users accounts and effectively managing the movement of users within your network and outside as well.

Active Directory and Azure AD are applied in this essay because they are Microsoft's popular domain management systems which many organizations use. Even if Microsoft does not stay at the top in the coming years, these benefits and security concerns will continue to be relevant in the Information Technology industry.

References

Benefits of Azure Active Directory. (2017, December 27). Retrieved from Attosol Technologies: https://www.attosol.com/benefits-of-azure-active-directory/

Privileged Access Management. (2020). Retrieved from Beyond Trust: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Simons, A. (2018, September 6). *Azure AD: Under the hood of our geo-redundant, highly available, distributed cloud directory*. Retrieved from Microsoft: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/azure-ad-under-the-hood-of-our-geo-redundant-highly-available/ba-p/243762

Understanding and Defending Against Active Directory Threats. (2019, October 15). Retrieved from Cyware Social: https://cyware.com/news/understanding-and-defending-against-active-directory-threats-5310a39f

What is Active Directory Security and why is it so important? (2019, January 21). Retrieved from NS TECH: https://tech.newstatesman.com/sponsored-by-quest-software/active-directory-security

What is Active Directory? (2019, July 31). Retrieved from Microsoft: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis#:~:text=Azure%20Active%20Directory%20(Azure%20AD,in%20and%20access%20resources%20in%3A&text=Internal%20resources%2C%20such%20as%20apps,developed%20by%20your%20own

What is Azure AD Connect? (2020, January 8). Retrieved from Microsoft: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

What is the Azure Active Directory Architecture? (2019, April 23). Retrieved from Microsoft: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-architecture

Zaharia, A. (2020 Edition, April 22). *Terrifying Cybercrime and Cybersecurity Statistics & Trends*. Retrieved from Comparitech: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/