ALTIMETRIK®

Trusted Cloud:

Windows Azure-Security Assessment Compliance

Table of Contents

Introduction 2

Identifying and understanding your attack surface 3

Reconnaissance of Azure tenant 5

Exploring Azure Enumeration 5

Understanding user enumeration, authentication, and password attacks on Azure 6

- Password Attacks 7
- Password Spraying 7
- Methods Used by Attackers 7
- Defending Against Password Spraying Attacks 7

Lateral movement after compromise 8

Understanding the Azure Subscription Hierarchy 9

- Organizations 9
- Subscriptions 9
- Resource Groups & Resources 9
- Roles 9

Understanding Resource-Specific Issues in Cloud Computing 10

- Serverless Environment Variables 10
- Azure Functions – Serverless Apps in Azure 10
- Instance Metadata Service 10
  - Securing User Attributes and Service Principals in Azure AD 11
  - Searching for Credentials in Description or Comment Fields 11
  - Azure Service Principal Hijacking 12
  - Securing User Attributes and Service Principals in Azure AD 12
  - Searching for Credentials in Description or Comment Fields 12
  - Azure Service Principal Hijacking 12

Securing Your Azure and Active Directory Environment 13

The Growing Cost of Data Breaches for Businesses 15

- The Financial Impact of Data Breaches 15
- Data Breach Mitigation Strategies 15

Conclusion 16

Introduction

Azure Security Assessment and Active Directory security testing is the practice of simulating a cyber-attack on a computer system, network, or web application to test its defenses and identify vulnerabilities that an attacker could exploit. In the context of Microsoft Azure cloud computing services, penetration testing can be a valuable tool for ensuring the security of your cloud-based and hybrid assets. There are several key considerations to keep in mind when planning and conducting a penetration test of your Azure environment.

1. **Scope:** The first step in any Azure Cloud security assessment or Active Directory security test is to define the scope of the specific systems and assets that will be included in the test. This may include specific Azure services, such as virtual machines, storage accounts, and web applications, as well as any on-premises systems that are connected to the Azure environment. It is important to define the scope clearly, as this will help to ensure that the test is focused and efficient and that all relevant systems are included.

2. **Permission:** Before conducting a penetration test of your Azure environment, it is essential to obtain the necessary permissions including non-disclosure agreements (NDAs). This may include getting approval from your organization's security team and any relevant legal or regulatory authorities. It is also important to inform any third-party service providers or customers whose systems may be affected by the test.

3. **Testing Methodology:** There are several different approaches to conducting a penetration test, including manual testing, automated testing, and a combination of the two. It is important to choose the methodology that is most appropriate for your organization's needs and resources and to ensure that the testing is comprehensive.

4. **Reporting:** After the penetration test is completed, it is important to provide a detailed report outlining the test results, including any vulnerabilities identified and recommendations for remediation. This report should be shared with relevant stakeholders, including the security team, IT staff, and any third-party service providers or customers whose systems were included in the test.

5. **Remediation:** Once the results of the penetration test have been reported, it is important to take steps to remediate any vulnerabilities that were identified. This may involve implementing security patches, updating software, or revising security policies and procedures. It is also important to periodically re-test the environment to ensure that all vulnerabilities have been properly addressed.

In summary, penetration testing is a crucial tool for ensuring the security of your Microsoft Azure cloud computing services and environment. By following best practices and taking a systematic approach, you can identify and mitigate vulnerabilities, and protect your

organization's assets from potential cyber-attacks.

Identifying and understanding your attack surface

Knowing your attack surface is critical for your organization. An attack surface is the sum of all potential points of entry that can be exploited by a malicious actor. It includes both external and internal resources, APIs, and user-based systems like Microsoft 365. Identifying these points of vulnerability helps organizations protect their digital assets from cyberattacks and other malicious activity. In this whitepaper, we will explore

External Resources (Unauthenticated)

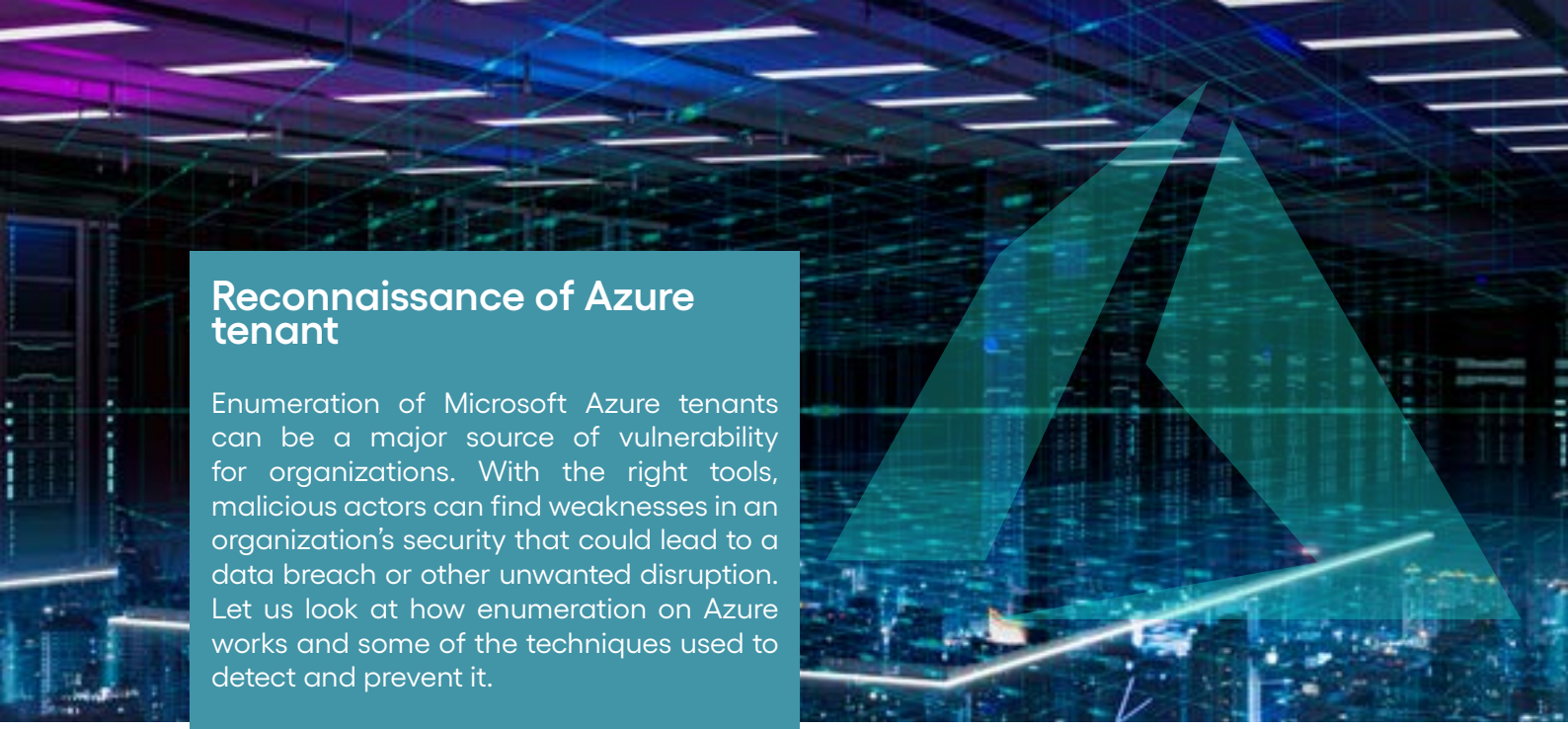
External resources are available to anyone with internet access, regardless of authentication status. These include public websites, mobile applications, and cloud services that can be accessed without authentication or authorization. Attackers often target these resources to gain access to valuable data or disrupt service delivery. To minimize the risk posed by external resources, it is important to patch known vulnerabilities promptly and implement effective countermeasures such as two-factor authentication and encryption.

Internal Resources & APIs (Authenticated)

Internal resources are those that require authentication before they can be accessed, such as cloud services hosted on Azure Resource Manager or internal server infrastructure. Additionally, attackers may use compromised credentials to gain access to sensitive data via APIs or other authenticated interfaces. To prevent unauthorized access, organizations should maintain a comprehensive inventory of internal resources and regularly audit their security settings for any misconfigurations or vulnerabilities that could be exploited by attackers. Additionally, organizations should deploy multi-factor authentication across all internal systems and use intrusion detection systems (IDS) to monitor network traffic for suspicious activity.

The Microsoft 365 Platform

Microsoft 365 is a widely used platform offering productivity applications such as Outlook, SharePoint, Teams, etc., which require users to log in with username/password credentials to access them fully. As with any other system requiring authentication, attackers may try to gain unauthorized access using stolen credentials or social engineering techniques such as phishing attacks. Organizations should take steps such as enabling two-factor authentication for all accounts and deploying anti-phishing solutions to reduce the risk posed by Microsoft 365 users being targeted by attackers looking for vulnerable accounts. Also, it is recommended you leverage a security operations center (SOC) with a Microsoft Sentinel deployment. Sentinel is useful for uncovering sophisticated threats with decisive response and intelligence, comprehensive security information, and event management (SIEM) for proactive threat detection, investigation, and responses. This allows your organization to ticket and track these vulnerabilities to completion. Knowing your attack surface is essential for CISOs (Chief Information Security Officer) who want to protect their business's digital assets from malicious actors looking for vulnerable points of entry into their networks or databases. From external unauthenticated resources like public websites and mobile apps, internal authenticated resources like cloud services hosted on Azure Resource Manager or internal server infrastructure, and even user-based systems like Microsoft 365 identifying these points of vulnerability helps organizations implement effective security measures so they can remain secure against cyberattacks and other malicious activity. Investing in the right tools and technologies now will ensure your organization remains secure now and into the future



Reconnaissance of Azure tenant

Enumeration of Microsoft Azure tenants can be a major source of vulnerability for organizations. With the right tools, malicious actors can find weaknesses in an organization's security that could lead to a data breach or other unwanted disruption. Let us look at how enumeration on Azure works and some of the techniques used to detect and prevent it.

Initially, an attacker may use the following links to identify Microsoft 365 usage:

```
https://login.microsoftonline.com/getuserrealm.srf?login=username@company.com&xml=1 (Tenant - federation / managed - ADFS link, etc.)
```

```
https://login.microsoftonline.com/[targetdomain]/v2.0/well-known/OpenID-configuration (Tenant ID)
```

Exploring Azure Enumeration

User enumeration is a technique used by hackers to determine if a given user exists in an environment. This type of attack is commonly used as part of a larger attack campaign, such as password spraying or account takeover. On Microsoft Azure, user enumeration can be performed by accessing the OAuth2 token endpoint found at:

```
https://login.microsoft.com/common/oauth2/token
```

And attempting to authenticate with a known username and password combination.

Additionally, you may be able to enumerate users via OneDrive enumeration or by scraping LinkedIn for usernames and other information

Data in Public Azure Blobs

Microsoft Azure Storage is like Amazon S3 when it comes to data storage solutions; blob storage holds unstructured data such as images or documents that are publicly accessible via access policies set up by administrators (for example, read-only access). The URLs for these blobs are usually predictable and follow this format- "storage-account-name. blob. core. windows .net*" where "storage-account-name" can usually be found easily via search engines or social media sites like LinkedIn. As organizations continue to rely heavily on cloud services for their operations, they need to understand the potential vulnerabilities associated with those services so that they can mitigate any risks before they become disasters waiting to happen. Enumeration on Microsoft Azure is just one example of these kinds of risks—with the right tools and techniques, attackers can easily find weaknesses in an organization's security posture and exploit them for their gain unless proper defenses are in place. By understanding what methods malicious actors use when performing enumeration attacks and utilizing detection and prevention methods accordingly, organizations will be better prepared against any potential threats they may face in the future.

how to identify an organization's attack surface and best practices for mitigating risk.

Understanding user enumeration, authentication, and password attacks on Azure

Authentication is a critical aspect of any secure system. Without proper authentication, malicious actors can gain access to sensitive data and wreak havoc on your cloud infrastructure. Let us discuss the distinct types of authentications available and how password attacks can occur. We will also highlight the importance of properly securing authentication points and how your organization can defend against potential attacks.

Authentication is the process of verifying that someone is who they say they are. There are several diverse types of authentications available, including usernames and passwords, API (Application Programming Interface) keys, certificates, secrets, and more. It is important to understand the differences between these types so you can make sure your authentication settings are as secure as possible.

For instance, service accounts or those that authenticate with certificates may require multi-factor settings for added security. Additionally, it is important to be aware that occasionally developers post keys publicly in code repositories which could leave your cloud infrastructure vulnerable to attack.

Password Attacks

Password attacks are one of the most common methods used by malicious actors to gain access to cloud infrastructure. A password attack typically involves attempting to guess or crack a user's password by using brute force or dictionary attacks. These attacks are especially dangerous because they often go undetected until it is too late. To prevent these types of attacks from taking place, it is important to find all potential authentication points used within your organization and secure them accordingly with strong passwords or other forms of authentication such as two-factor authorization (2FA). Authentication is an essential part of any security system and should not be taken lightly. With the right knowledge, malicious actors can use various methods such as password attacks to gain access to sensitive data stored in the cloud environment and cause irreparable damage. As a CISO, it is important for you to understand the several types of authentications available and how best to secure them against potential threats. Finding all potential authentication points used within your organization is a key first step in protecting yourself against these kinds of attacks.

Password Spraying

Password spraying is an attack technique used to target an organization's users by trying one password for every user, avoiding account lockouts. While most systems have some sort of lockout policy (for example, 5 attempts in 30 mins results in a lockout), attackers are now attempting to authenticate as each username one time every 30 minutes so that no accounts are locked out. This technique is becoming increasingly popular among criminals due to its high success rate. Let us explore this attack method in more detail and how your organization can protect itself from it.

Methods Used by Attackers

Attackers commonly use passwords such as "Summer2023," "Spring2022," "Winter2022," or "Fall2022" when attempting password spraying attacks on organizations. There is even a script available online that logs if the user is valid if MFA is enabled if the tenant exists, if the account is locked or disabled, or if the password is expired. It also allows attackers to easily automate their tasks with minimum effort.

Defending Against Password Spraying Attacks

Fortunately, there are steps organizations can take to protect themselves from these types of attacks. Microsoft provides two tools that help defend against password spraying attacks: Azure Password Protection and Azure Smart Lockout. Azure Password Protection prevents users from picking passwords with certain words like the season, company name, etc., while Azure Smart Lockout locks out authentication attempts whenever brute-force or spray attempts are detected. Also, organizations should ensure they are using strong passwords and constantly changing them and implementing multi-factor authentication (MFA) where possible. According to Microsoft "More than 99.9% of these identity-related attacks are stopped by using multifactor authentication (MFA) and blocking legacy authentication."

Password spraying has become an increasingly popular attack technique used by criminals due to its high success rate. Organizations need to be aware of this attack method and take the necessary steps to protect themselves from it; otherwise, they will risk being victims to this type of attack.

Lateral movement after compromise

Once an attacker has compromised a system, they will often attempt to move laterally within the environment to gain access to additional systems and data. We continue to discuss some of the factors that need to be considered when performing lateral movement after the initial compromise. There are a few key questions that need to be answered when assessing lateral movement options after the initial compromise: What does the attacker have access to? What roles do they have? Is MFA enabled? What can they access (web applications, API, database storage, etc.)? Who are the system administrators? Are they able to escalate to an administrator? Are any security protections in place (ATP, Smart Lockout, Sentinel, Guard Duty, etc.)?

Answering these questions will help identify avenues for lateral movement. For example, if they have access to a low-privileged user account but MFA is not enabled, they may be able to brute force their way into other accounts. Alternatively, if the attacker has admin access to a web application, they may be able to exploit a vulnerability in the application to gain access to sensitive data. Once potential lateral movement paths have been identified, it is important to test them thoroughly before taking any irreversible actions. This can be done by setting up a lab environment that mimics the production environment as closely as possible. This will allow you to safely test different lateral movement defensive techniques without jeopardizing the production systems.

Lateral movement after an initial compromise is a critical phase of an attack and needs to be carefully planned and executed to avoid detection and minimize damage. By answering key questions and thoroughly testing potential paths in a lab environment, attackers can increase their chances of success while minimizing the risk of being caught.

Understanding the Azure Subscription Hierarchy

When it comes to IT security, the Azure subscription hierarchy is an important concept that all CISOs should understand. The Azure Subscription Hierarchy consists of organizations, subscriptions, resource groups, and roles. Let's explore these elements in more detail so that you can better protect your organization's resources on Azure.

Organizations

Organizations are typically created for billing use cases, and they contain multiple subscriptions. Note that licenses are not considered subscriptions; rather, they are separate from the subscription hierarchy and are used to provide access to certain features or services within a given subscription

Subscriptions

Subscriptions are grouped for billing purposes and can only be accessed by users with appropriate roles assigned to them. Each subscription can have distinct roles assigned to it, allowing various levels of access depending on who is using the subscription. For example, a user with "Owner" permissions would have full control over resources within the subscription while a user with "Reader" permissions would only be able to read attributes within the subscription

Resource Groups & Resources

Resource groups and resources help determine which subscription you are in when accessing Azure services. Each subscription has its informative name - e.g., Prod / Dev, etc. Multiple subscriptions can be held under the same Azure Active Directory (AAD) directory (tenant). Each subscription also has multiple resource groups associated with it which may contain various resources such as virtual machines, web apps, databases, etc.

Roles

Roles are specific permissions that grant users access to various Azure services and features within their respective subscriptions. There are four built-in Azure Subscription Roles - Owner (full control over resources), Contributor (all rights except changing permissions), Reader (only able to read attributes), and User Access Administrator (manage user access to Azure resources). Depending on what type of access you need for a particular service or feature on your organization's platform, you can assign one of these four roles accordingly.

Every organization needs to understand how the Azure Subscription Hierarchy works to effectively manage their organization's data and keep their IT assets secure in the cloud environment. Knowing how organizations link together with their associated subscriptions and resource groups allows you to properly configure role-based permissions so those who need access get it while those who do not stay locked out of certain areas of your system where they do not belong. With this knowledge at hand, you can ensure that your organization's data remains safe from malicious actors or unauthorized personnel who might otherwise gain access without proper authorization from management or yourself an IT security personnel responsible for safeguarding company assets in Microsoft's cloud platform environment

Understanding Resource-Specific Issues in Cloud Computing

As cloud computing becomes more widely adopted, CISOS needs to understand the resource-specific issues that come along with this technology. Here are some of the most common issues related to serverless environment variables and Azure functions. Let us focus on and discuss how instances can use the Metadata Service to orient themselves in a dynamic environment and the potential security risks associated with it.

Serverless Environment Variables

Serverless environment variables refer to secrets, such as credentials or connection strings that can be stored within source code or added as environment variables. Organizations need to be aware that plaintext values can be exposed if these secrets are not called from secure Key Vault locations. Also, reader-level access functions allow viewing of these values, which could lead to malicious actors accessing sensitive data.

Azure Functions – Serverless Apps in Azure

Azure functions are serverless apps hosted on Microsoft's cloud platform. This platform allows users to deploy serverless applications quickly and easily without having to build their infrastructure. While this provides many advantages, it also means that administrators should take extra steps to ensure that passwords are stored securely and not exposed in plain text. Additionally, they should ensure that only certain functions have access permissions, and all other connections are blocked off by unauthorized personnel.

Instance Metadata Service

Cloud servers need a way to orient themselves due to the dynamic nature of their environments. To address this issue, a "metadata" endpoint was created and hosted on a non-routable IP (Internet Protocol) address (169.254.169.254). This metadata endpoint contains access/secret keys used by AWS (Amazon Web Services) and IAM (Identity and Access Management) credentials which enable cloud services such as Amazon EC2 instances or AWS Lambda functions to communicate with each other securely. However, there is always the risk of malicious actors using SSRF (Server-Side Request Forgery) to

compromise or SSRF vulnerabilities to gain access to these credentials remotely. To prevent such occurrences, organizations should ensure that this endpoint is only reachable from the local host and that all external connections are blocked off by unauthorized personnel.

Cloud computing has become increasingly popular over recent years due to its scalability and cost savings benefits compared with traditional IT infrastructures. However, it comes with its own set of unique challenges related to resource-specific issues such as serverless environment variables and Azure functions. By understanding how cloud servers use instance metadata services, CISOs can take the necessary steps toward ensuring their organization's security. With proper planning, cloud computing can offer numerous advantages while still staying secure

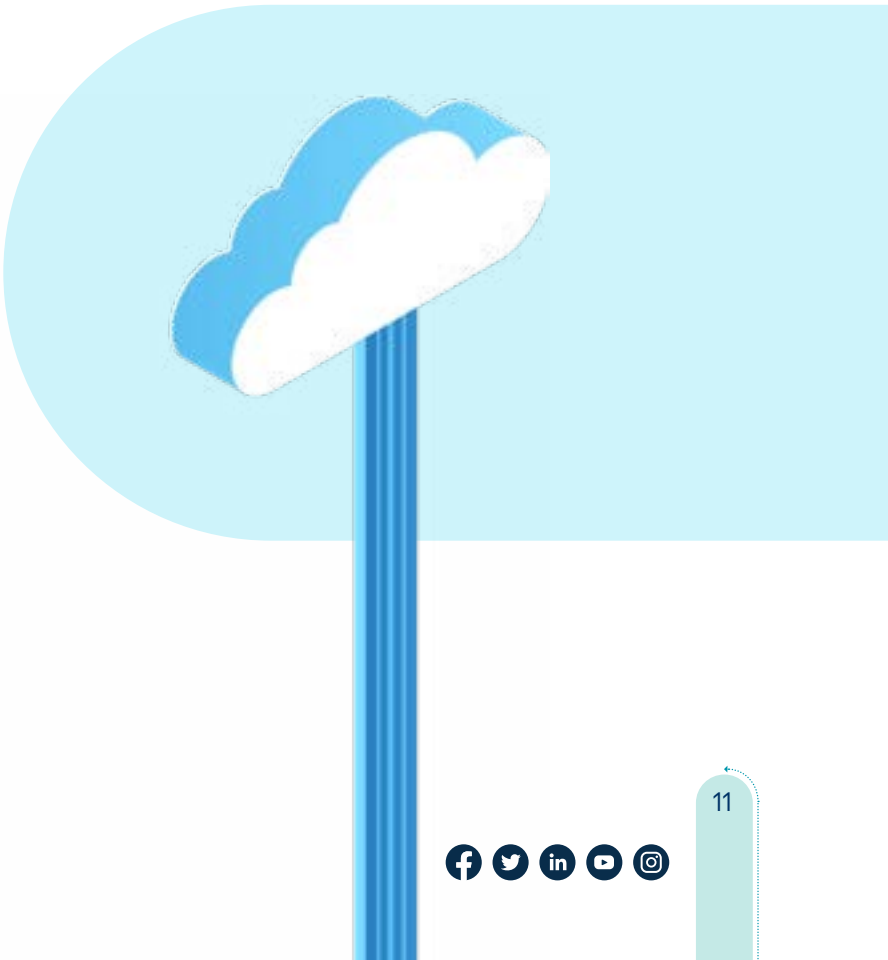
Securing User Attributes and Service Principals in Azure AD (Active Directory)
It is especially important to secure user attributes and service principles in Azure AD. Let us examine two key aspects of this process: searching for credentials in description or comment fields and preventing the hijacking of Azure service principles.

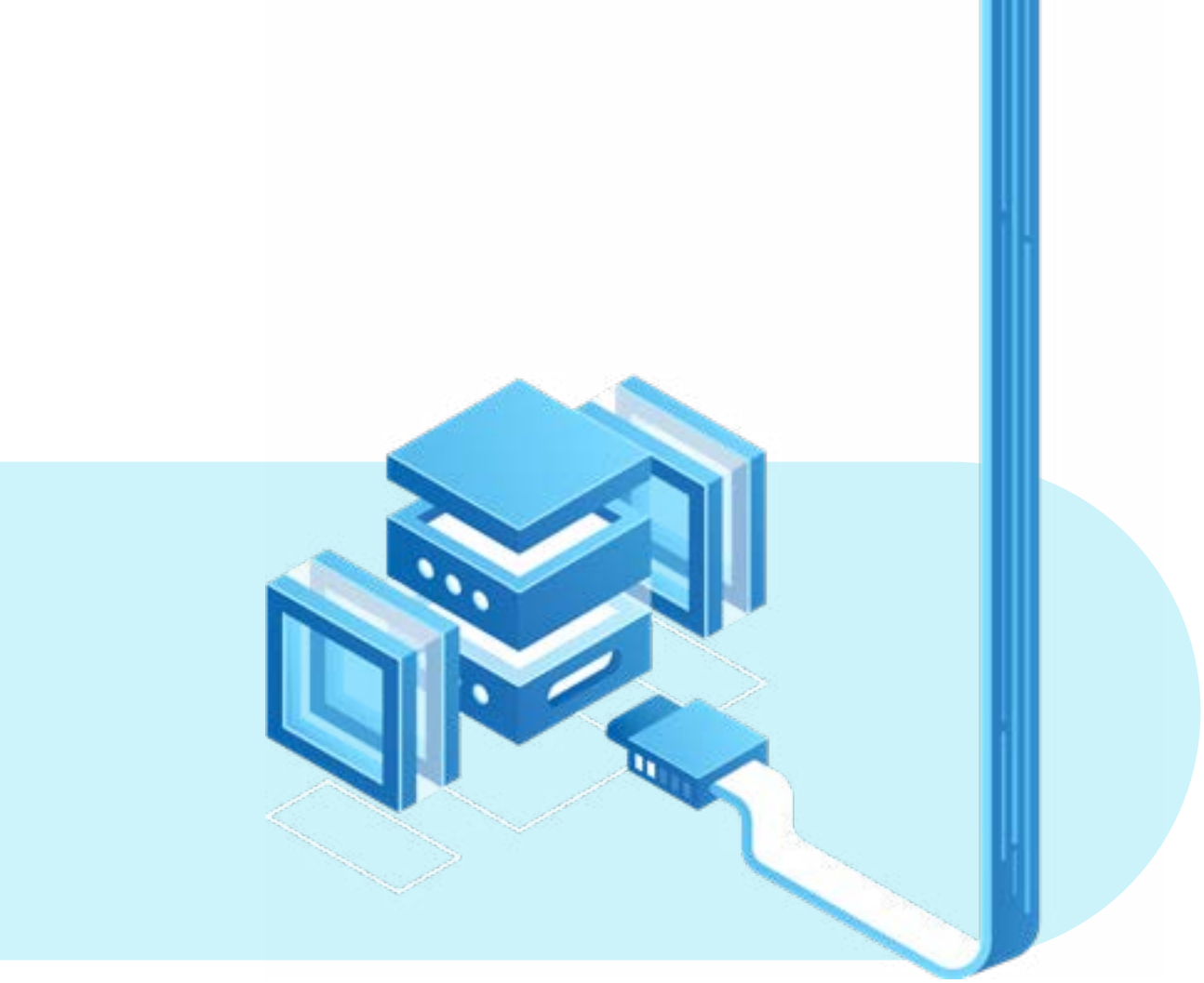
Searching for Credentials in Description or Comment Fields

When using an Azure system, it is common to find credentials stored in a description or comment field. To search for every Azure AD user field for passwords, you can use a one-liner command such as the following example:

```
$users = Get-MsolUser; foreach ($user in $users) {props = @();$user | Get-Member | foreach-object {$props+=$_.Name};foreach($prop in $props) (if($user.$prop -like "*password*")(Write-Output ("[*]" + $user.UserPrincalName + "[" + $prop + "]" + " : " + $user.$prop)}}}.
```

This will help you locate any existing passwords that have inadvertently been stored on your system.





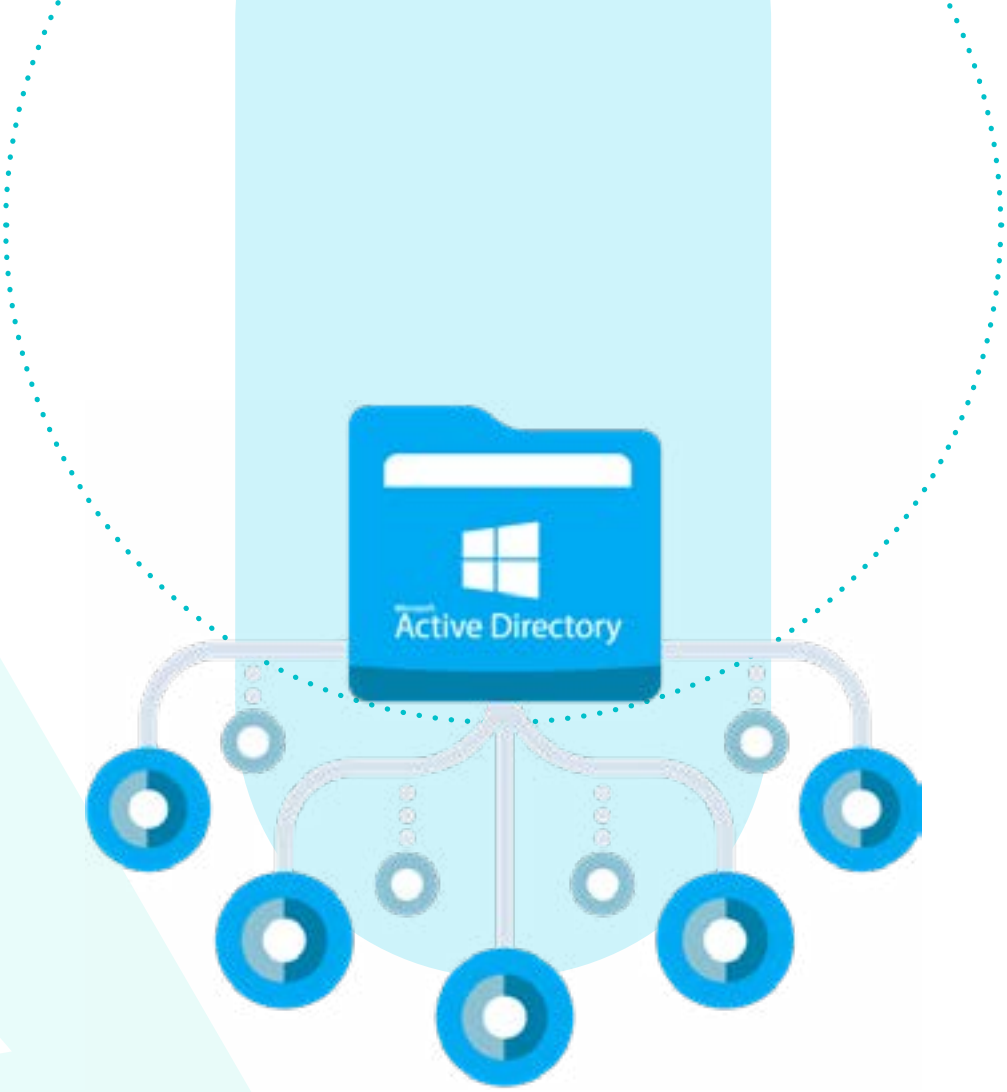
Azure Service Principal Hijacking

Another aspect of protecting user attributes and service principles is ensuring that there are no attempts at hijacking them. In an 0365 tenant, there are over 200 default service principles that can have varying levels of permissions through Microsoft Graph. As an Application Administrator, you should be aware of the potential risks associated with changing passwords or certificates for these service principles without taking proper security measures. It's also important to note that none of these service principles are visible through the Azure GUI portal—this can put your company at risk if someone were able to gain access to your system without authorization.

Securing user attributes and service principles within Azure AD requires vigilance and dedication from all members of a company's IT team. By taking steps such as searching for credentials in description or comment fields and preventing the hijacking of service principals, you can help ensure that sensitive information remains safe while still allowing users access to necessary applications and services on your system. With the right precautions put into place, your company can benefit from making full use of the features offered by Microsoft's cloud platform without compromising data security or privacy standards.

Securing User Attributes and Service Principals in Azure AD

In the modern age of cybersecurity, it is especially important to secure user attributes and service principles in Azure AD. With many companies gradually transitioning to cloud-based systems, they must take the necessary steps to protect their sensitive information stored in Azure. Let's examine two key aspects of this process: searching for credentials in description or comment fields and preventing the hijacking of Azure service principals.



Securing Your Azure and Active Directory Environment

As businesses move more operations to the cloud, cybersecurity must be a top priority. This is especially true for organizations using Microsoft's Azure and Active Directory products. If these tools are not properly secured, it can lead to serious data breaches. To help keep your organization safe, Altimetrik & Microsoft recommend following the security best practices outlined below:

People: It is important to ensure that your team members have a strong foundation in cloud security principles. Educating them on the basics of cloud security will help them understand why certain measures are necessary and how they can keep their data safe. You should also make sure they know how to use the available technology to secure their environment, such as passwordless authentication or multi-factor authentication.

Process: Establishing clear processes for cloud security decisions ensures everyone involved knows who is responsible for what tasks and keeps things organized. This includes updating your incident response process for the cloud, so you know what steps need to be taken if an attack occurs. Additionally, you should create a system for tracking your organization's security posture over time so any changes can be quickly identified and addressed.

Technology: Integrating native firewalls and network security into your environment can provide an extra layer of defense against potential attackers. You should also consider integrating advanced threat detection solutions such as AI-driven monitoring systems like Sentinel or user behavior analytics platforms that can detect suspicious activity before it becomes a major issue. Finally, encrypting all sensitive data will help protect it from being accessed by unauthorized personnel.

everything is up to date and compliant with industry standards. Additionally, having advanced threat detection solutions in place will give you real-time visibility into any potential issues or malicious activity occurring within your environment.

Architecture: Altimetrik recommends you standardize on a single directory and use identity-based access control, as the program matures you'll start to realize how important a unified security strategy is, well-architected design, repeatable steps, single source of truth, security as code, following cloud architecture frameworks during design to eliminate poor design practices and provide best practices to help your architects, developers, administrators, and cloud practitioners who design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective

Securing Azure and Active Directory environments requires a comprehensive strategy that covers people, processes, technology, and threat protection measures such as auditing and detection solutions. By following these best practices, you will be well on your way toward keeping your organization's data safe from any potential threats or cyberattacks that may arise in the future. Microsoft is making security defaults available to everyone because managing security can be difficult. Identity-related attacks like password spray, replay, and phishing are common in today's environment. More than 99.9% of these identity-related attacks are stopped by using multifactor authentication (MFA) and blocking legacy authentication. The goal is to ensure that all organizations have at least a basic level of security enabled at no extra cost. Altimetrik highly recommends investing time into researching and implementing these strategies as soon as possible to ensure maximum safety for all your digital assets. In case you're still on the fence about your Azure security, continue reading for some recent analysis on the costs of a data breach and the impacts that can have on your business and reputation

The Growing Cost of Data Breaches for Businesses

As technology and infrastructure continue to evolve, data breaches become more and more common. Unfortunately, the cost of a data breach can be substantial for modern businesses of all sizes. According to IBM's latest Cost of a Data Breach report, in 2022 the average cost of a data breach globally reached an all-time high of $4.35 million. Businesses need to understand the potential financial repercussions that come with suffering a data breach and take measures to protect themselves.

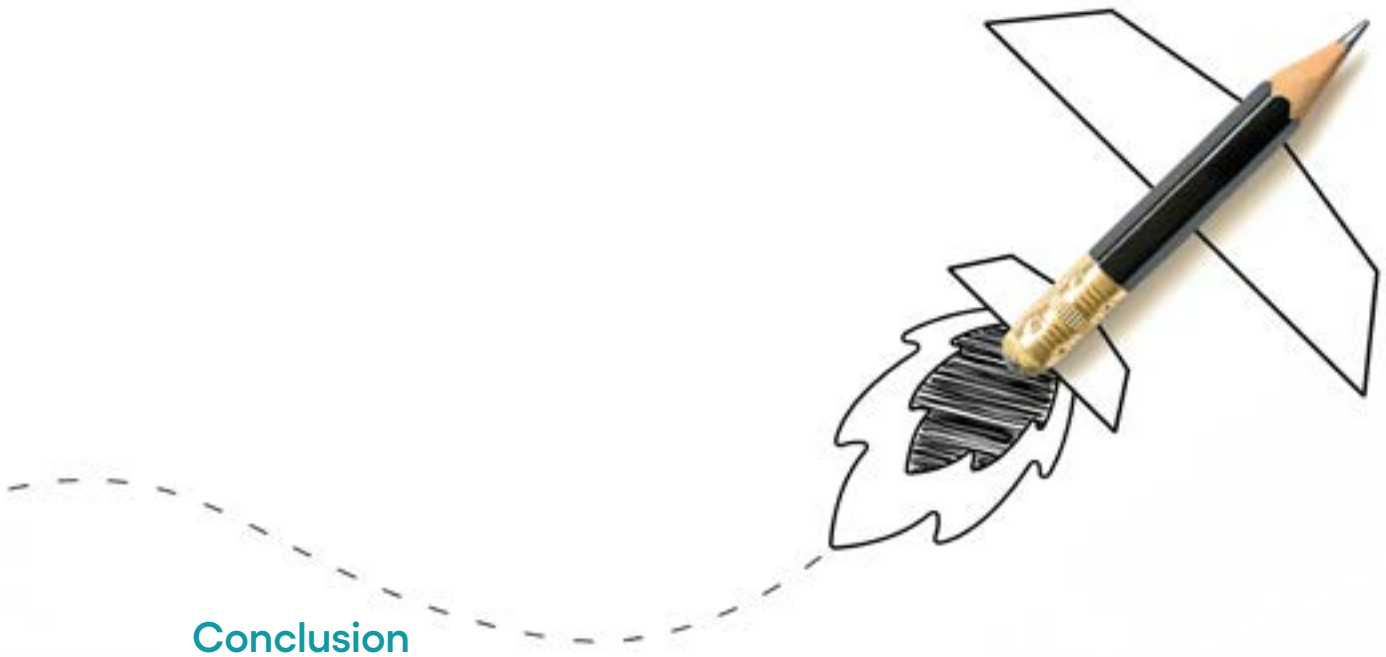
The Financial Impact of Data Breaches

First and foremost, organizations must recognize the significant financial implications associated with data breaches. According to Forbes, research conducted by the Ponemon Institute revealed that in 2019, the average total cost per breach was $3.54 million; this figure has only continued to rise since then. Furthermore, IBM's Cost of a Data Breach report found that on average companies lose nearly 1 million dollars within two weeks post-attack due to remediation costs as well as investigation and legal fees incurred from customers and regulators. Companies are also at risk for lost revenue due to decreased customer trust—IBM found that businesses typically lose between 3-4% of their customers following a breach. In addition, businesses must factor in fines from regulatory bodies such as GDPR or CCPA which can be quite costly depending on the nature of the incident (e.g., the type of data affected).

Data Breach Mitigation Strategies

Considering these potentially severe financial ramifications, organizations must have robust strategies in place for mitigating against and responding to incidents should they occur. CISOs should focus on implementing effective security protocols including training programs around cybersecurity best practices, investing in user authentication solutions (e.g., multi-factor authentication), regularly testing their systems against potential threats (e.g., penetration testing as a service - PTAAS), and ensuring their infrastructure is up to date with current security standards (e.g., keeping software patched). In addition, companies must have plans in place for responding quickly and efficiently if an incident were ever to occur so as not to limit any potential damage caused by delays or missteps during the response process.

The impact of a data breach can be huge – both financially and reputationally – for any organization regardless of its size or industry sector. It is therefore essential for CISOs to ensure their organizations are taking necessary steps towards protecting their systems from attack by implementing comprehensive cybersecurity protocols as well as developing strong incident response plans should an incident occur despite these precautions being taken... Doing so will help ensure your organization can reduce its risk exposure while minimizing any potential losses incurred from a security incident should one occur down the line.



Conclusion

Azure Security Assessment and Active Directory security testing is the practice of simulating a cyber-attack on a computer system, network, or web application to test its defenses and identify vulnerabilities that an attacker could exploit. In the context of Microsoft Azure cloud computing services, penetration testing can be a valuable tool for ensuring the security of your cloud-based and hybrid assets. There are several key considerations to keep in mind when planning and conducting a penetration test of your Azure environment.

1. It is important to define the scope of your penetration test clearly
2. Before conducting a penetration test of your Azure environment, it is essential to obtain the necessary permissions
3. It is important to choose the methodology that is most appropriate for your organization's needs and resources and to ensure that the testing is thorough. Altimetrik leverages the MITRE Attack Framework and OWASP testing guidelines along with offensive security and red team attack simulation methodology
4. After the penetration test has been completed, it is important to provide a detailed report outlining the results of the test, including any vulnerabilities that were identified and recommendations for remediation.
5. Take steps to remediate any vulnerabilities that were identified

In summary, penetration testing is an important tool for ensuring the security of your Azure environment. We covered a plethora of topics ranging from Altimetrik - Azure Security Testing, the process of identifying and understanding your attack surface, reconnaissance of Azure tenant, understanding user enumeration, authentication, and password attacks on Azure. Methods used by attackers and how organizations can defend against password spraying attacks, what to do in the event you detect lateral movement in your organization after compromise. Understanding the Azure subscription hierarchy, Organizations, Subscriptions, Resource Groups & Resources, Roles and understanding Resource-Specific issues in cloud computing. We dove into serverless environment variables, Azure functions, and the Instance Metadata Service. Securing User Attributes and Service Principals in Azure AD, searching for credentials in description or comment fields, Azure service principal hijacking, securing user attributes and service principals in Azure AD. Finally, we spoke about how you can secure your Azure and Active Directory environment, the growing cost of data breaches, the financial impact, and breach mitigation strategies. By following best practices and taking a systematic approach, you can identify and mitigate vulnerabilities, and protect your organization's assets from potential cyber-attacks.

About Author

Aladdin Elston

Aladdin is a vCISO | CBSP | CISSP | OSCP | CSM Cyber Security Leader who demonstrates experience leading cross-functional teams and is always customer-focused with a solid technical background with over 20 years of experience. He is currently involved in cybersecurity mentorship programs focused on diversity, has exceptional problem-solving skills working in a variety of roles, and is always excited to take on new, ambiguous projects. Using strong business judgment Aladdin has assessed the security of systems and infrastructures ranging in size from small to large including full enterprise networks, e-commerce web applications, and blockchain infrastructure. He has worked with several Fortune 500 companies and has been the spokesperson to senior management in identifying and articulating risks and developing mitigation strategies to manage the identified risks.

About Altimetrik

Altimetrik is a data and digital engineering services company focused on delivering business outcomes with an agile, product-oriented approach. Our digital business methodology provides a blueprint to develop, scale, and launch new products to market faster. Our team of 5,500+ practitioners with software, data, and cloud engineering skills help create a culture of innovation and agility that optimizes team performance, modernizes technology, and builds new business models. As a strategic partner and catalyst, Altimetrik quickly delivers results without disruption to the business.