MID-MO ShowMe IT Summit

COLUMBIA, MISSOURI

WELCOME!

aws

MID-MO ShowMe IT Summit
COLUMBIA, MISSOURI

Cloudy with a chance of....

BREACH

Top Seven Misconfigurations

- “Not my responsibility”
- Giving too much access
- Failing to use built in data security controls
- Failing to monitor critical activity
- Failing to use network security groups properly
- Ignoring when resources are being used
- Allowing configuration drift

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE36QLE

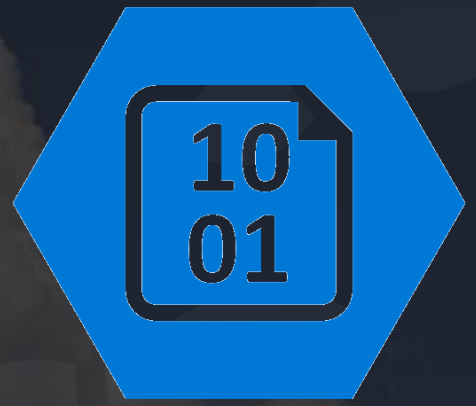
What is involved with testing the Azure Cloud environment?

- Allowed testing
- Public Storage
- Roles and Permissions
- SQL DBs
- Key Vaults
- App Registrations
- Azure AD

Azure

Public Storage

A public storage account is created with your subscription



- Misconfigured to allow anonymous access
- Watch for permissions/least privilege
- RBAC

Key Vaults

- Limit access to IP addresses
- RBAC and Access policies/privileged access
- Watch for leaks in code!

Roles and Permissions

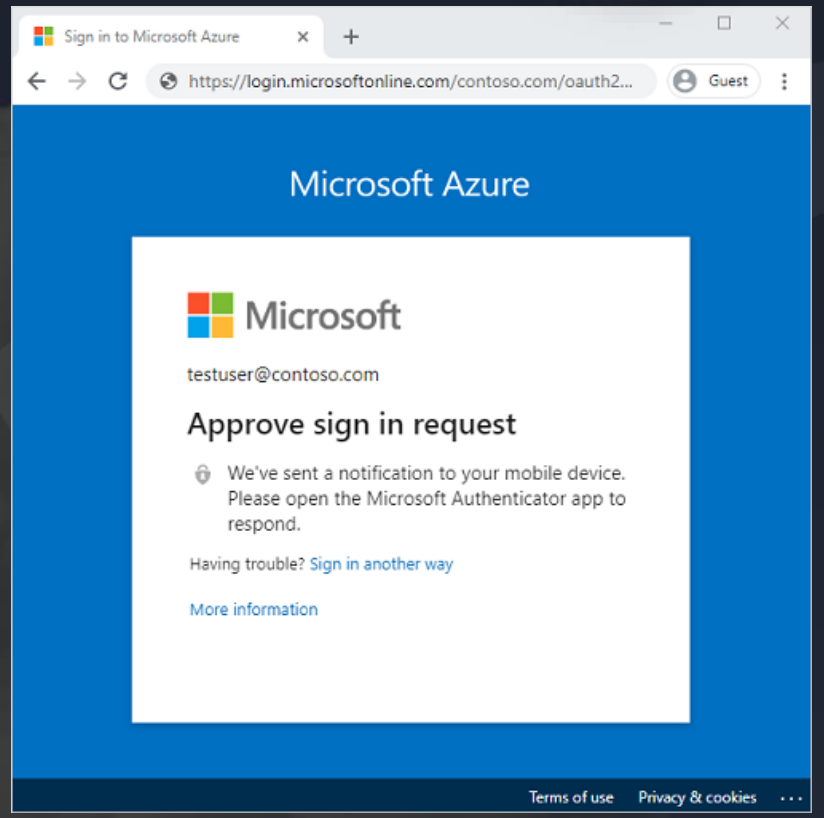
Too much access can be given, allowing for attackers to escalate privileges

- Role Based Access Control
- Conditional Policies
- Custom Policies

Multi Factor Authentication

Something you know, something you have…

- Attackers have no access/no possession
- AD Account Lockout
- Mitigates password guessing/bruteforce/spraying



SQL DBs

Connection strings can be misconfigured

Standard

```
Server=tcp:myserver.database.windows.net,1433; Database=myDataBase; User ID=mylogin@myserver; Password=myPassword;
Trusted_Connection=False; Encrypt=True;
```

Use 'mylogin@myserver' for the User ID parameter.

Azure SQL Database

- Misconfigured to allow anonymous access
- Watch for permissions/least privilege
- RBAC

Tools We Can Use

- PowerZure
- Azurite Explorer
- MicroBurst
- Stormspotter
- EvilGinx
- SkyArk
- ROADTools
- Trevorspray

Azure

It’s Demo Time!