Azure for Students

Overview on Azure and their services (kinda ranked after use-cases)

1. Compute: VMs (IaaS), Container Instances (virtualised Applicationenvironments), App Service, Functions

2. Networking (VPN,...)

3. Storage

4. Mobile services (apps,...)

5. Databases

6. Web (Web apps, ...)

7. IoT (manage all IoT assets, ...)

8. BigData (cluster services, ...)

9. AI services and Machine Learning

10. DevOps

Notes

- CA from my static website: Microsoft Azure TLS Issuing CA 01

- Easy to differentiate between VM and Containers: VM virtualise the hardware, containers the OS

- `azurewebsites.net`, `azurestaticapps.net` as domain ending

- Static and web apps can be set up with the help of Git
  → learning something via Git Accounts?

- Possibilities to secure Azure: SecurityCenter, Sentinel,

To be checked out:

https://sonraisecurity.com/blog/attackers-find-aws-s3-bucket-with-17m-users/

Most common mistakes with Azure

- **Misconfiguration of Roles & Administration:** [1] [2] [3]

  making everyone as (co-)administrator in the Azure subscription. Team members often times remove or delete the Azure components, which creates lot of impact on overall application and ruins the stability of the environment. Members also unknowingly keep on provisioning Azure resources for research and evaluation purpose which causes a huge expenditure. Data Storage Access Misconfig: a user can set permissions that expose data to the entire internet in "Azure Storage" **(try to do that!)**

  → provide users only with the amount of permission they need to do their job! RBAC (Role Based Access Control) or ARM (Azure Resource Manager) or MFA (Multi-Factor auth.)

- **Choosing incorrect specifications (of Azure VM) & not securing access points** [1] [4]

  All aspects like overall user load, nature of the application and geography of the users must be considered by enterprises and individuals hosting their applications, before designing the infrastructure. Not securing access points to the clouds, allowing users to access the VM from any machine, anywhere.

- **Billing of over usage** [1]

  They keep running their Azure instances, even if they are not in use or when purpose is served.

  → keep resources in off-state or delete them once you no longer need them.

- **Weak, mismanaged Passwords:** [2] [4]

  Improper password management and bad password habits. Microsoft reports 10 million username/password pair attacks per day.

- **Misconfig/not enabling of Security/Managing Controls:** [2]

  Failed to turn on the logging feature. Necessary to permit access visibility but also to see who is accessing and managing the subscription. Failing to enable Azures security center and its native security tools (**check this out!**)

  TODO: subnets should not be assigned to a public IP that could open unwanted ports. (Network Security Groups (NSGs)) NSGs control access by permitting or denying network traffic via communication between different workloads on a vNET, network connectivity from on-site environment into Azure, or direct internet connection.

- **Lack of Oversight / Security Monitoring:** [2] [3]

  Missing ongoing management and security (often times just in the beginning and then not covered anymore) Security vulnerabilities result when Azure users don't

---

[1] https://blog.e-zest.com/here-are-10-most-common-mistakes-while-managing-azure-cloud

[2] https://www.lightstream.tech/top-5-azure-mistakes-your-security-team-is-making/

[3] https://www.viacode.com/most-common-azure-security-problems/

[4] https://techgyo.com/5-common-microsoft-azure-security-mistake

understand what they are responsible for and the tools and services Azure provides to help them.

Shared Responsibility Model for Security in the Cloud			
On-Premises (for reference)	**IaaS** (infrastructure-as-a-service)	**PaaS** (platform-as-a-service)	**SaaS** (software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

☐ Customer Responsibility ☐ Cloud Provider Responsibility [5]

- **Cloud misconfiguration:** [3]
  Especially the misconfiguration of databases and object storage services. (linked there - https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf)

- **Not encrypting data at rest:** [3]
  blobs are encrypted by default, but VM disks are not, creating vuln. User have to enable disk encryption on their own (for free!).

- **Not managing patches correctly:** [4]
  Not applying a patch at all or do it only half the way.

- **Not testing security or taking it for granted:** [4] [1]
  Users should use penetration testers (microsoft has a policy governing such tests). Even though Microsoft secures the platform, it can't protect against e.g. weak passwords

- **Not opting for Microsoft support option** [1]
  To save costs, companies try to avoid the support when purchasing the Azure subscription. But it can happen, that even a high skilled employer isn't able to e.g. shut down a VM. The support however can do this. If enterprises have not chosen the appropriate support option then there might be a huge impact.

- **McAfee Report** [5]
  More and more files contain sensitive information and too many are publicly accessible. Enterprise organizations have an average of 14 misconfigured IaaS/PaaS instances.

---

[5]https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf

Azure Key Vault

Search for `.vault.azure.net` websites (e.g. Dorking: `site:*.vault.azure.net/`)
→ no results, aren't listed...

Resolve the key vault uri (`https://super-secure-keyvault.vault.azure.net/`, `https://aiskeyrun.vault.azure.net`)
→ runs on `51.116.154.67` and `ASN 8075`

Azures SecurityCenter