HOW TO HARDEN ACCESS TO YOUR CLOUD INFRASTRUCTURE AND RESOURCES

VLADIMIR STEFANOVIĆ

WHO AM I

- Vladimir Stefanović
- System Engineer @SuperAdmins
- Technical Trainer @ATC
- MCSA, MCSE, MCT, IAMCT Regional Lead, Speaker
- Azure UG Serbia leader
- stefanovic.vladimir@hotmail.com
- www.tech-trainer.info
- https://github.com/Wladinho/Presentations

WHAT IS A GOAL OF HARDENING?

- Your infrastracture and resources are more resistant
- Your client is happier
- You will sleep better
- In case of emergency, you have more time to react

WHAT NEED TO BE HARDENED?

- Access to tenant
  - *User management & Password Policy*
  - *MFA (Multi-factor Authentication)*
  - *Conditional Access*
- Resources
  - *IAM (Identity Access Management)*
- Network Access
  - *NSG (Network Security Group)*
  - *Firewall*

TENANT (CLOUP APP) ACCESS

- User management & Password Policy
  - *Try to avoid so many Global Admins*
- MFA (Multi-factor Authentication)
  - *Force „critical“ users and Global Admins to use MFA*
  - *Easy to configure, not expensive*
- Conditional Access
  - *Buy licenses and play* ☺

RESOURCES AND NETWORK ACCESS

- IAM (Identity Access Management)
  - *Role Based Access Control*
  - *Carefully select appropriate role*
  - *Can be configured on many „levels“*
- Backup
- Backup Again
- Network Access can be protected with
  - *NSG (Network Security Group)*
  - *Firewall*

DEMO