We moved to the cloud

So, we don't have to worry about ransomware, right?

Markus.Lassfolk @truesec.se
Mikael.Nystrom @truesec.se

Misconfigurations have bigger impact

- Default settings allow access to the management interface from anywhere
- Building a VM in azure and allow 3389 from the world, is common and wrong
- Access keys gives a lot of access, from the entire world…
  - Storage blobs
  - Databases
  - Cloud services in general
- Security will not be stronger than the weakest partner
- Security is always an ongoing process…

Responsibility cannot be outsourced

- Moving resources to the cloud will not move responsibility of the solution
- VMs will not automatically be managed, it is still your responsibility
- The password of “Summer2023” will not be better if it is used in the Cloud
- If running on-prem, backup can be in the cloud, but the reversed?
- Security is possible, but maybe not the default

TRUESEC

What we see

- Identity Secure Score = 1.57%
- AD Sync – Syncs everything
- On-prem admins are synced to Azure AD as GA
- Weak password policy's on-prem, same in Azure
- Exposed VMs on port 3389 without white listening

Things to have in mind

- Make sure you have SLA’s that make sense when the disaster is a fact
  - “-Hi, it is Christmas evening, and we need to restore 45 VMs now, - Sure, give a minute”
- Make sure the the Incident Responders are allowed to do investigations
  - Otherwise, it will be hard to understand what happend, and prevent it from happening again”
- Make sure that your insurence is valid in all scenarios

What we see

- Exposed VMs on port 3389 without white listening
- MFA is configured for a group, but group is empty
- Azure AD Free is being used, or P1/P2 is used, but security functions are not enabled
- Number of Global Admins is to much
- PAWs or not being used

Backup in the cloud, is different

- Owner of storage?
- Does Global Admin have access to the backup?
- If breached, what will you get back?
- Time to restore?

Think again

“How many times have you experienced a product or a solution that is so secure that you have never needed to configure it…”

Protect the control plane

- Use ONLY delegation when managing
- Use privileged access workstations
- Use whitelisting/similar
- Review configuration yearly or more often
- Automate response
  - If someone adds a member to the GA role, you should be notified
- Reduce the attack surface for the Control Plane, it should only be possible to access from a limited number of computers and users

Protect identity

- Enable Password Management
- All user should use MFA, now
- Monitor access and watch out for abnormal behavior
    - "Hello Sir, it seems that you have done some impossible travel…"
- Enable user self service for MFA enrolment, and other security settings
- Use managed identities when possible
- Use Azure Key Vault

Assume the worst
-hope for something better

- How will you know that someone become Global Admin?, Now what?
- How will you know that data is being manipulated?, Now what…
- How will you restore all the VMs that was erased suddenly? Now what

Note...

“Remember, securing your cloud services is an ongoing process, and it’s important to stay up-to-date with the latest security measures.”

TRUESEC

Thank you

www.truesec.com   x.com/truesec   linkedin.com/company/truesec