PROTECT YOUR ORGANIZATION BY SAFEGUARDING YOUR PRIVILEGED ACCESS

JEAN-PAUL VAN RAVENSBERG

INTRODUCTION

SAFEGUARDING YOUR PRIVILEGED ACCESS

- Jean-Paul van Ravensberg, Azure Solutions Architect & Engineer
- 5 years in consultancy @ Avanade
- Experience with Azure Services, Automation and Security
- Holds various certifications, TOGAF & Azure Solutions Architect most recent
- Blog: Cloudenius.com – Twitter: @Cloudenius

Mention the following in a Tweet to get retweeted:

#DutchSecMeetup + @Cloudenius + @Maarten_Goet + @AvanadeNL

CLOUDENIUS

AGENDA

SAFEGUARDING YOUR PRIVILEGED ACCESS

- Risks & impact we are seeing today
- Impact of a recent cyber attack
- What can be done
  - Non-Technical Solutions
  - Technical Solutions
    - Microsoft
    - 3rd Party

CLOUDENIUS

WHICH RISKS ARE WE SEEING TODAY?

PRIVILEGED ACCOUNT MISUSE

- The lack of organizational awareness to invest in security
- The lack of user/admin awareness of their privileges
- Careless use of passwords can lead to unsafe privileged accounts
- Accounts not linked to a user and “No Named” accounts like service accounts are mostly not controlled by policies such as a password policy
- Too many highly privileged accounts
- Privileges are not separated/tiered into multiple accounts/environments

IMPACT

RECENT CYBER ATTACK: LOCKERGOGA

RANSOMWARE

- Ransomware targets several large multinationals – not widespread
- **Destructive**: Encrypts files blazingly fast, disables network interface, changes local user account passwords and logs users off. Users are completely locked out, servers are unusable
- Executable was **digitally signed**, verified & **undetected** at VirusTotal (0 engines out of 67). Result: no protection when using signature-based AV-software
- Cannot replicate itself around a network - no C&C or (DNS) Traffic

- Attackers must have had remote access to move laterally & get administrative permissions on other machines (and domain?)

Source: DoublePulsar.com

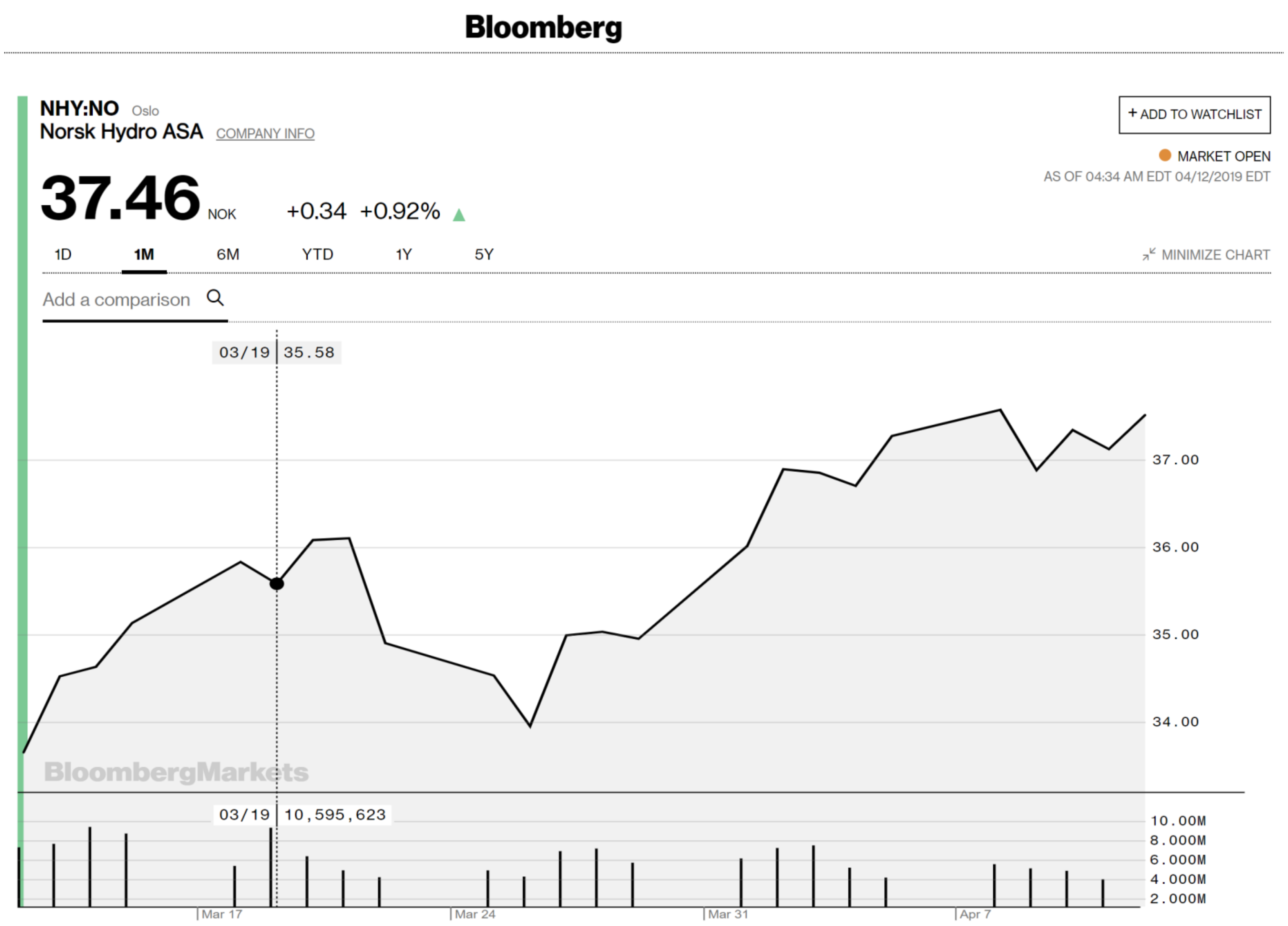
RECENT TARGET: HYDRO (19TH OF MARCH 2019)

LOCKERGOGA

- Hydro – a large Norwegian aluminum and renewable energy company
- 35.000 employees where asked to disconnect from the network and start manual production
- Transparency & communication
- Using Office 365, users where still able to work from other or non-compromised machines
- Backups where getting restored while no ransom was paid (per source)
- Financial impact: USD $35-41 million for the first week

Source: DoublePulsar.com et al.

HYDRO STOCK



Bloomberg

NHY:NO Oslo

Norsk Hydro ASA COMPANY INFO

MARKET OPEN

AS OF 04:34 AM EDT 04/12/2019 EDT

37.46 NOK +0.34 +0.92% ▲

CLOUDENIUS

WHAT CAN BE DONE?

MANY PARTS TO THE SOLUTION

CLOUDENIUS

NON-TECHNICAL SOLUTIONS

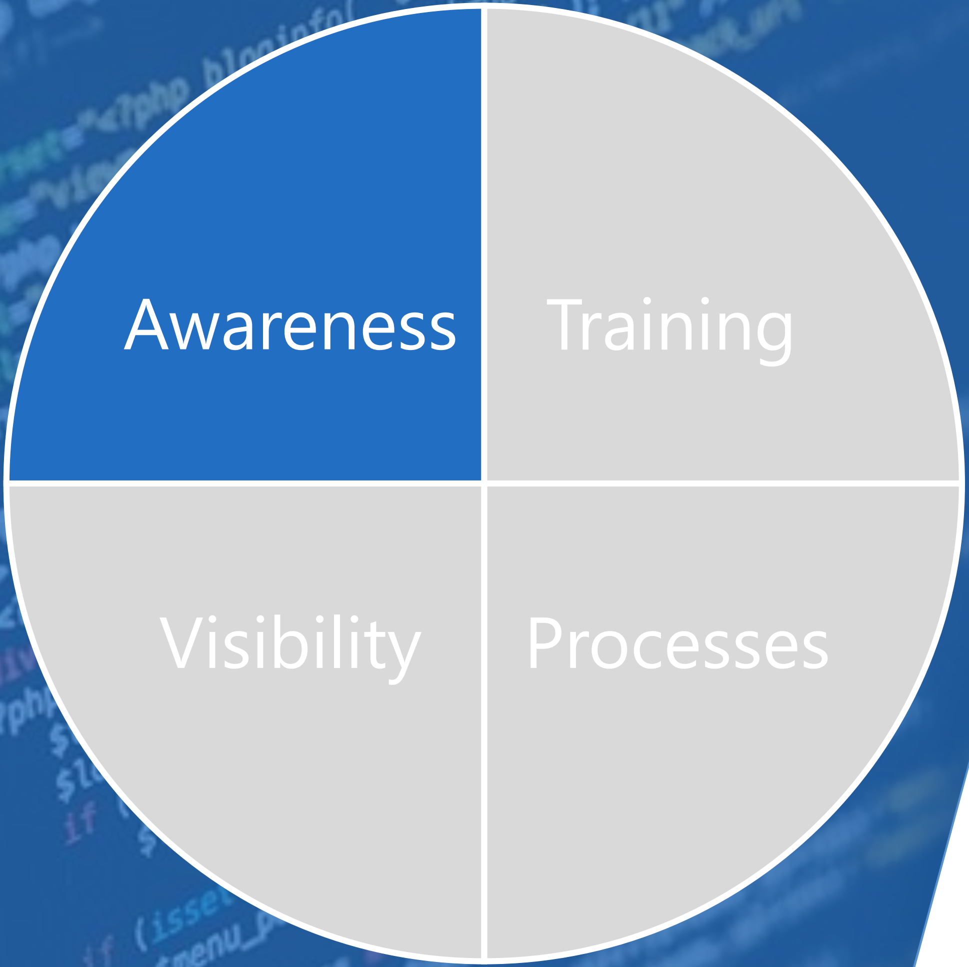
Awareness

Training

Visibility

Processes

NON-TECHNICAL SOLUTIONS



Awareness

Training

Visibility

Processes

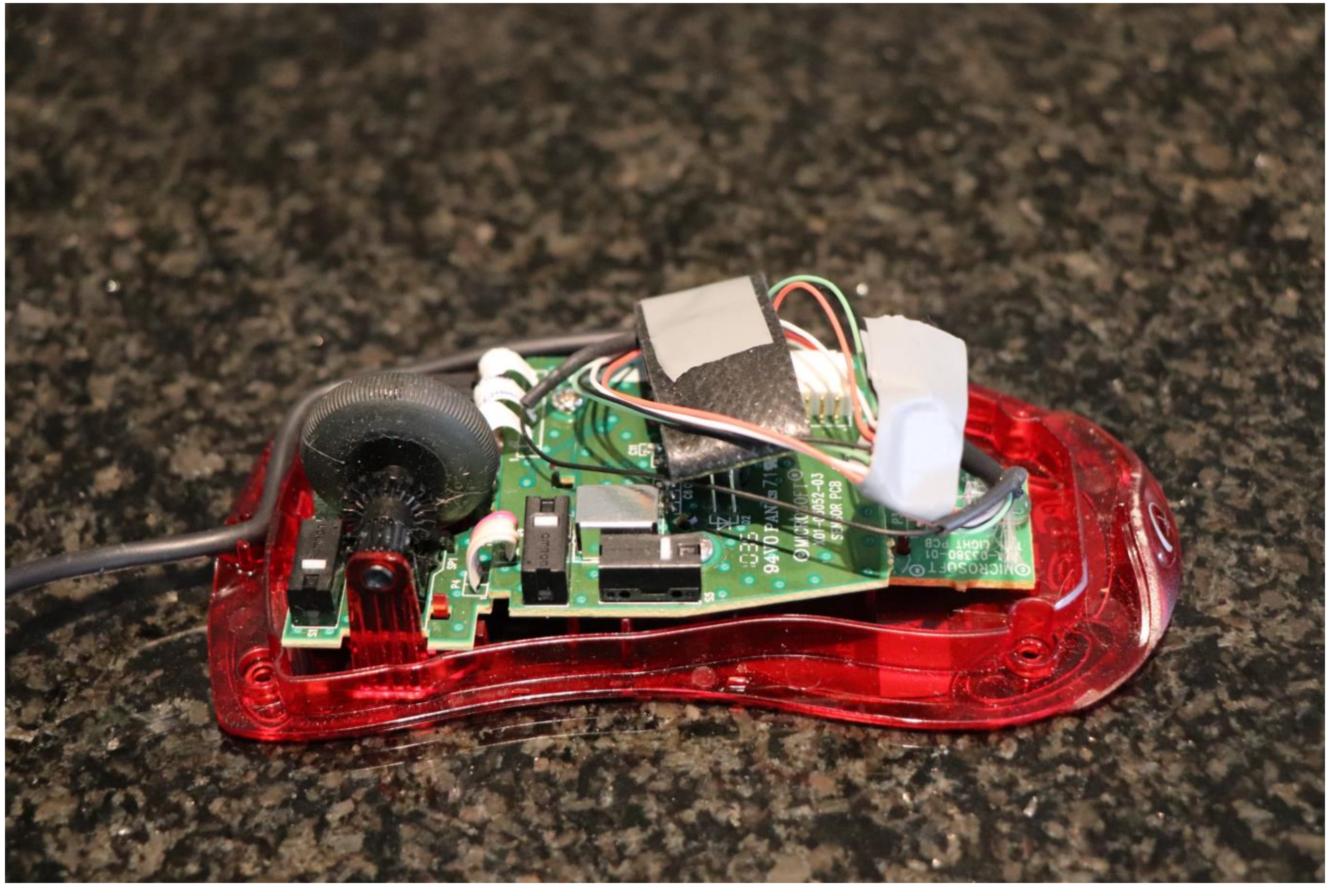
AWARENESS

PRIVILEGED ACCOUNT MISUSE

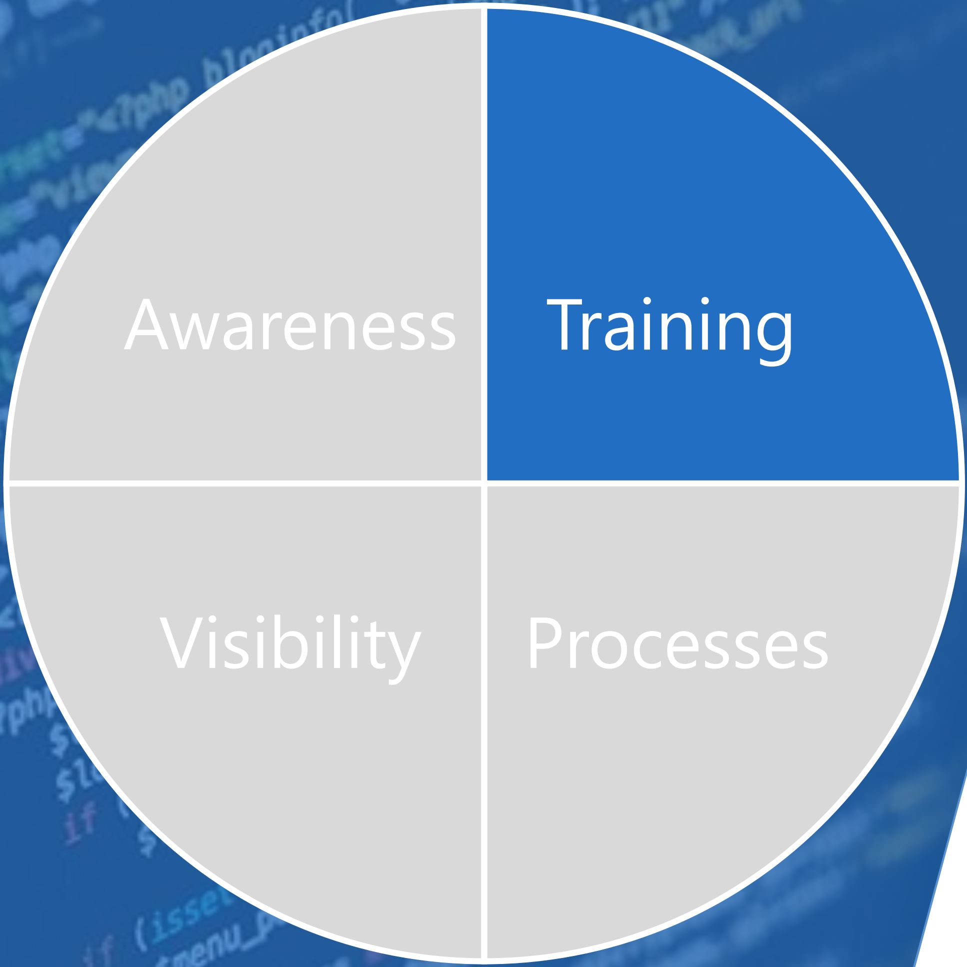
- Involve users & admins into security decisions - show the importance instead of focusing too much on compliance
- A user plugging in a rogue USB device (or peripherals) or opening a phishing email can be enough for an attack to happen.
- MFA will not solve all your authentication issues. Users can still be phished (MitM) or without awareness the user can accidentally click on “yes”. (Remember the UAC prompts?)

MAARTEN’S WEAPONIZED MOUSE

“HEY, CAN I BORROW YOUR MOUSE FOR ONE SEC?”



Source: https://medium.com/@maarten.goet



Awareness

Training

Visibility

Processes

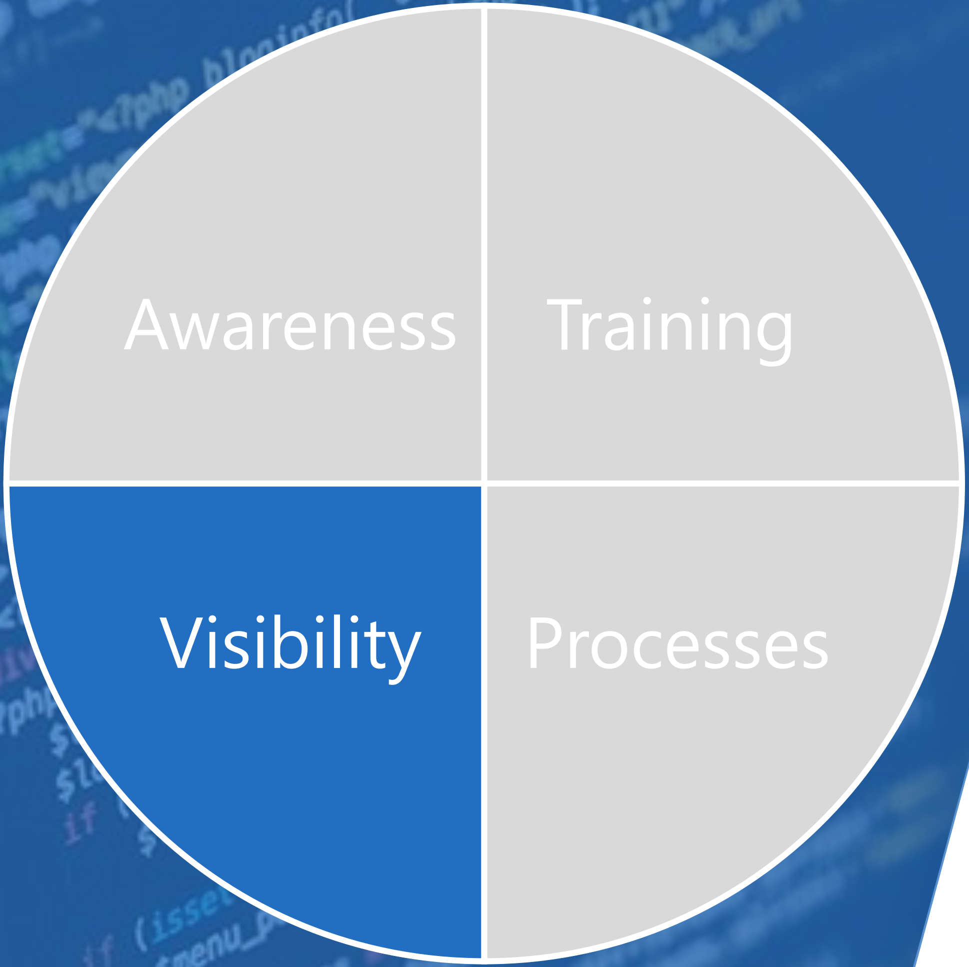
NON-TECHNICAL SOLUTIONS

TRAINING

PRIVILEGED ACCOUNT MISUSE

- Train personnel with anti-phishing campaigns & pay close attention to user with privileged access like local admin or extensive application permissions
- Explain to users what a security measure like MFA is, why it is important and what they need to do when prompted without logging in

NON-TECHNICAL SOLUTIONS



Awareness

Training

Visibility

Processes

"LACK OF VISIBILITY AND AWARENESS OF ALL OF THE PRIVILEGED ACCOUNTS, ASSETS, AND CREDENTIALS ACROSS AN ENTERPRISE STANDS AS ONE PERVASIVE STUMBLING BLOCK FOR COMPANIES IN EFFECTIVELY MANAGING PRIVILEGES" (BEYONDTRUST)

CLOUDENIUS

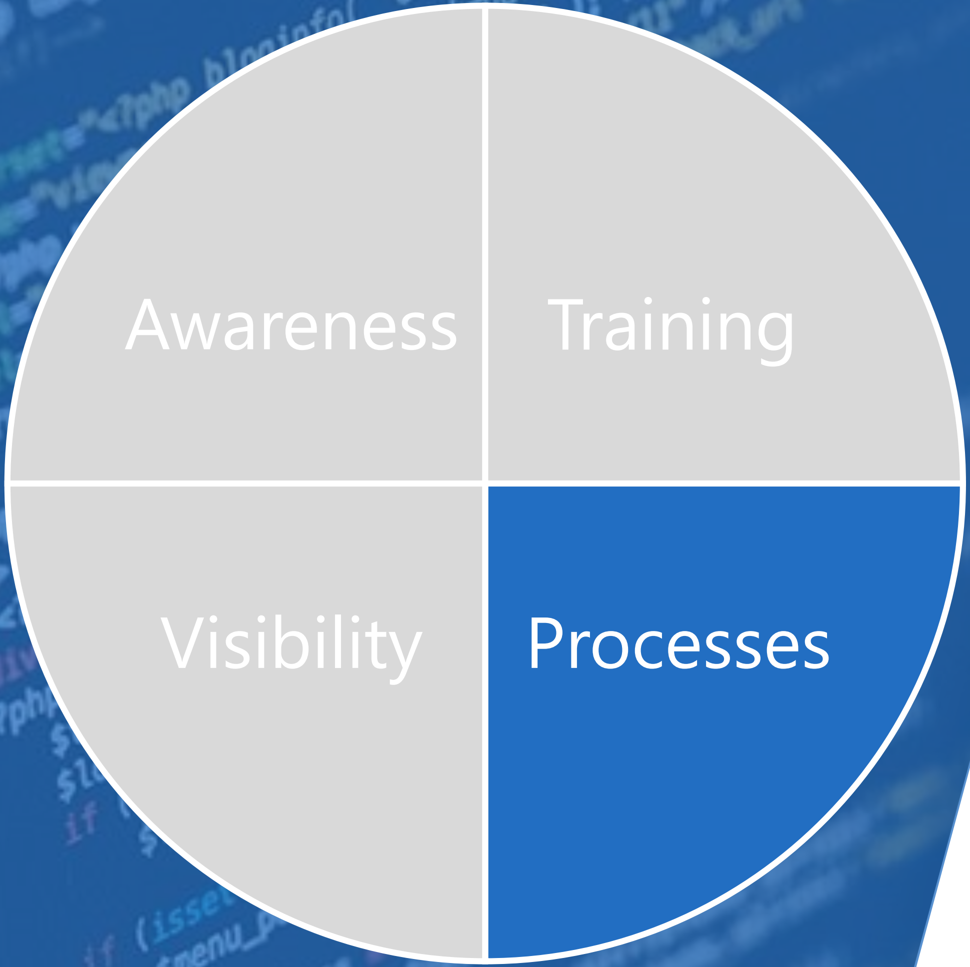
"GEBREK AAN ZICHTBAARHEID VAN ALLE PRIVILEGED ACCOUNTS, ASSETS EN CREDENTIALS BINNEN EEN ORGANISATIE VORMEN EEN STRUIKELBLOK VOOR ORGANISATIES DIE EFFECTIEF PRIVILEGES WILLEN BEHEREN" (BEYONDTRUST)

CLOUDENIUS

VISIBILITY

PRIVILEGED ACCOUNT MISUSE

- Make these privileged accounts, assets, and credentials visible by providing a safe place to store & control them
- Give users and administrators insights in the permissions that they have



NON-TECHNICAL SOLUTIONS

CLOUDENIUS

PROCESSES

PRIVILEGED ACCOUNT MISUSE

- Establish an identity governance process
- Link user accounts to admin accounts
- Security ≠ Bad end user experience
- Ensure permissions or roles can be requested easy & fast

TECHNICAL SOLUTIONS

CLOUDENIUS

PRIVILEGED IDENTITY & ACCESS MANAGEMENT (IAM)

REDUCE THE ATTACK SURFACE

- **Privileged Identity Management (PIM)**
  - Defines how admins have access to privileges (e.g. with an admin account)
- **Privileged Access Management (PAM)**
  - Controls which permissions an admin has within a specific system (e.g. restart a service)
  - PAM is no. 1 on the Top 10 Security Projects for CISOs according to Gartner
- **PIM & PAM are used interchangeably – don’t get confused**
  - Even Gartner & Forrester refer to it differently

"A DISCOVERY GAP BETWEEN WHAT ACCESS HAS BEEN GRANTED AND WHAT USERS ARE ACTUALLY DOING HAS MADE IT DIFFICULT TO UNDERSTAND SECURITY RISKS AND HAS PLAGUED IAM FOR YEARS" (CSO, 2016)

CLOUDENIUS

"EEN GAT TUSSEN DE TOEGANG DIE IS TOEGEWEZEN EN WAT GEBRUIKERS FEITELIJK NODIG HEBBEN HEEFT HET LASTIG GEMAAKT OM SECURITY RISICO'S TE BEGRIJPEN"
(CSO, 2016)

CLOUDENIUS

PIM & PAM

REDUCE THE ATTACK SURFACE

- Reduce the risk of administrative privilege misuse
- Lower the attack surface
- Mitigate the risk of excessive, unnecessary, or misused access rights
- Provide **just enough** privileges **just-in-time**.
  - Just Enough Administration
  - Just-in-Time Administration

WHICH SOLUTIONS ARE AVAILABLE TO MITIGATE THE RISK

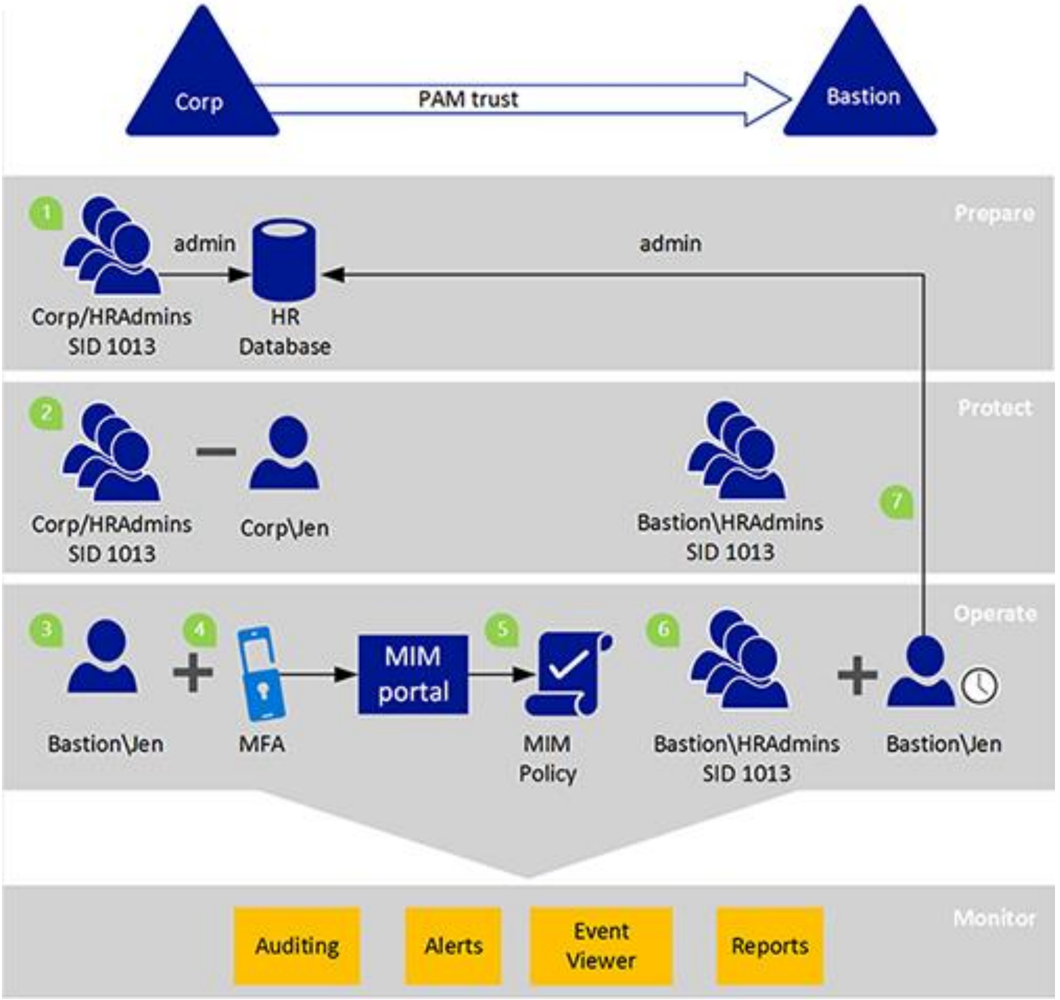
- Available for cloud & on-premises solutions
- Traditional datacenters – top 3 products by Gartner
  - Centrify
  - BeyondTrust
  - CyberArk
  - Microsoft Identity Manager
- Azure Cloud
  - Azure AD PIM

MICROSOFT SOLUTIONS

CLOUDENIUS

ON-PREMISES: MICROSOFT IDENTITY MANAGER

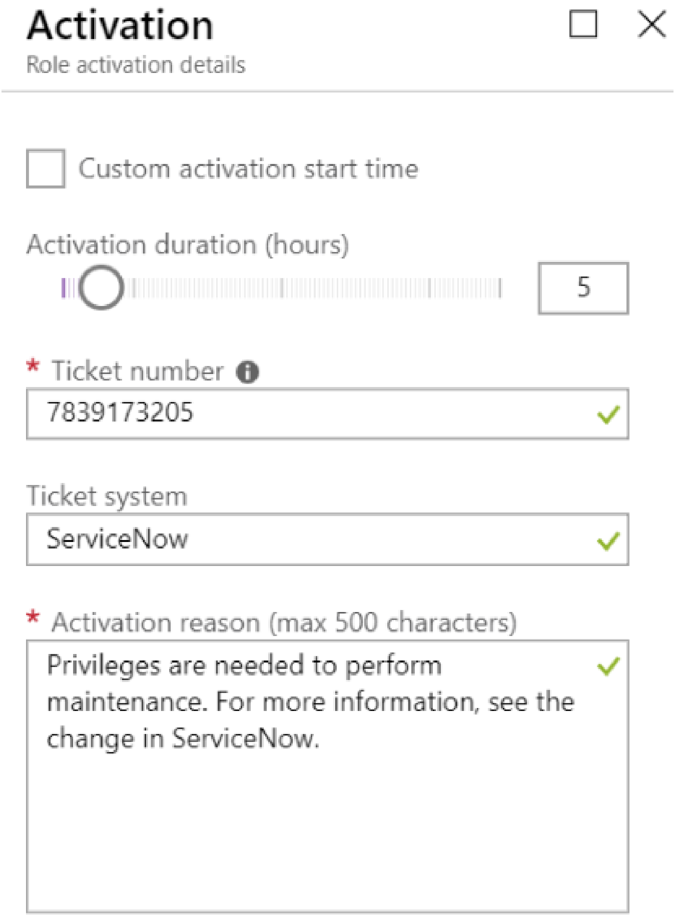
- One major benefit: creates a temporary user in a Bastion AD-forest
- Included with Azure AD Premium P1/P2
- Dependency on SharePoint Server



CLOUDENIUS

MICROSOFT CLOUD SOLUTIONS: AZURE AD PIM

- Get in control of administrative privileges
  - Nobody needs to be fulltime (Global) Administrator
- Get insights in privilege requests by using audits and reports
- User can request administrative privileges (e.g. Global Administrator) which will be assigned for a limited period of time after approval
- No Just-Enough-Administration (JEA) – JIT only
- Only works in Azure, extendible to e.g. Intune (as long as they use Azure AD Roles)
- Requires either AAD Premium P2, EM+S E5 or M365 M5



Activation

Role activation details

□ Custom activation start time

Activation duration (hours)

5

* Ticket number

7839173205 ✓

Ticket system

ServiceNow ✓

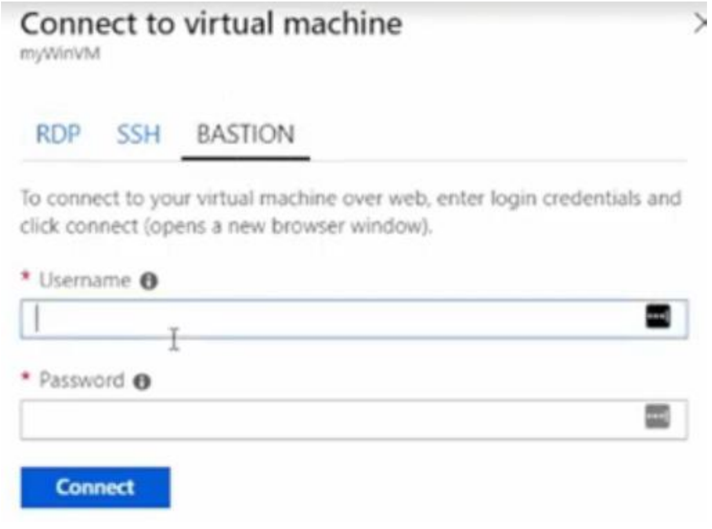
* Activation reason (max 500 characters)

Privileges are needed to perform maintenance. For more information, see the change in ServiceNow. ✓

CLOUDENIUS

COMING SOON: AZURE BASTION

- Public Preview - Public information released on the 14th of June on YouTube
- Connect to Azure VMs over RDP/SSH through Bastion, without a public IP address
- Responsive & fast connection through browser



Connect to virtual machine
myWinVM

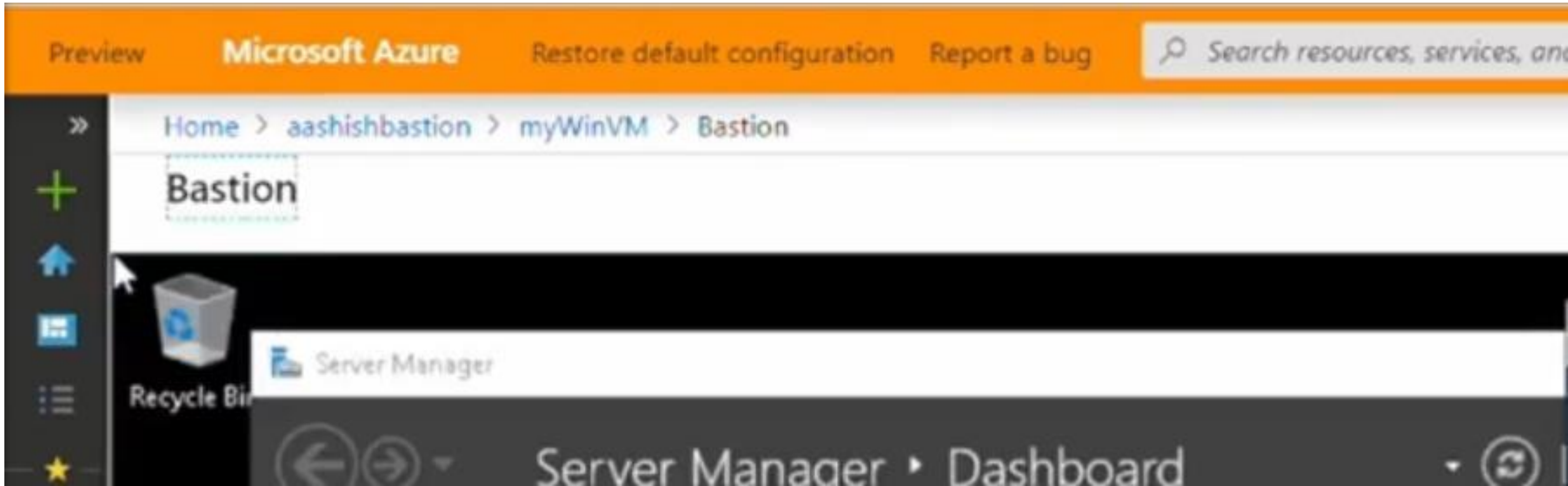
RDP SSH BASTION

To connect to your virtual machine over web, enter login credentials and click connect (opens a new browser window).

* Username

* Password

Connect



Preview
Microsoft Azure
Restore default configuration
Report a bug
Search resources, services, and
Home > aashishbastion > myWinVM > Bastion
Bastion
Recycle Bi
Server Manager
Server Manager • Dashboard

3RD PARTY

3RD PARTY - COMPONENTS

CENTRIFY, BEYONDTRUST, CYBERARK

- Self-Service portal to request privileges
- Privileges are given per role and time-bound
- Give insights in the use of privileges (Auditing & Reporting)
- Monitor, record & (sometimes) automatically stop sessions based on analytics
- Password vault with check-in/out, automatic password change, discovery of Windows/Linux accounts and integration with MSTSC/Putty
- SIEM integration like Splunk & workflow integration with ServiceNow

3RD PARTY - SUMMARY

CENTRIFY, BEYONDTRUST, CYBERARK

- There is no clear winner… They basically all do the same thing: providing the right amount of privileges at the right moment
- Difference: Using a web portal versus integrating with MSTSC/Putty
- Focus on the Machine Learning/AI capabilities of the product
- Ensure that the product integrates with the components you already have in your environment

OTHER TECHNICAL SOLUTIONS

CLOUDENIUS

REDUCE THE ATTACK SURFACE

RESTRICT & MANAGE ADMINISTRATIVE ACCESS

- Implement Microsoft LAPS to ensure that local all administrator accounts on workstations & servers have unique passwords across the AD domain.
- You will always have a (small set of) users that need or want administrative permissions. Limit this group to a minimum and implement tools like Avecto.

ASSUME BREACH

WHAT'S NEXT?

- Segregate your systems, identities & access into multiple Tiers with PAWs
- "Issue an administrator identity from a separate namespace or forest that cannot access the internet and is different from the user's information worker identity." - Microsoft

MULTIPLE TIERS/PASSWORDS & PASSWORDLESS?

- MSFT: “76 % of breaches start with **compromised passwords**”
- MSFT: “80 % of internal users are **passwordless**”
- Scenario with Windows Hello and Password Vault:
  - User: Logs in passwordless with Windows Hello (e.g. face recognition)
  - Server Admin: Uses Azure Bastion to login to servers on Azure with LAPS
  - Domain Admin: Uses Privileged Access Workstation/VM to work with DCs
  - Global Admin: Uses Azure AD PIM to request permissions Just-in-Time

Source: SiliconRepublic.com

CLOUDENIUS

HOW MUCH SECURITY IS ENOUGH?

CLOUDENIUS

WHERE TO START?

CLOUDENIUS

WHERE TO START

DEFINE LONG TERM & SHORT-TERM PLANS

- LAPS, MFA, Conditional Access should be a short-term plan
- A complete IAM strategy (except for Azure AD PIM) should be a long-term plan. Don’t underestimate the time needed to redefine processes, roles & responsibilities and sufficient training
- Gartner recommends to implement PAM on most valuable assets first

CALL TO ACTION

ASK YOURSELF THE FOLLOWING QUESTIONS

- Would my First Line Workers use Maarten's mouse?
- Are my password stored securely & visible?

  (Not limited to: routers/switches/servers/applications/vaults/backup servers)
- Are my administrators aware of their privileges?
- If the local administrator password is compromised, what would the impact be on other machines?

THANK YOU

WWW.CLOUDENIUS.COM

Q & A

Slides will be available at:
GitHub.com/MaartenGoet/MeetUp

THANK YOU

WWW.CLOUDENIUS.COM

Mention the following in a Tweet
to get retweeted:
#DutchSecMeetup + @Cloudenius
+ @Maarten_Goet + @AvanadeNL

Slides will be available at:
GitHub.com/MaartenGoet/MeetUp