AZURE DAY

Admin Odyssey: Navigating towards more secure Azure AD Admin Accounts

Pietro Visentin @ Moresi.com

Thanks to

Microsoft

avanade

4wardPRO
AN IMPRESOFT COMPANY

altitudo

BC Soft
consulenza sistemi informativi

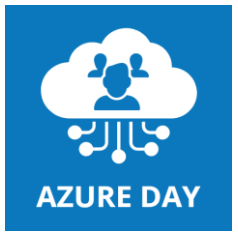
LOBRA

Reti
Società Benefit

UNIKEY
Bringing IT knowledge to the people

stickermule

Packt›



AZURE DAY

WhoAmI

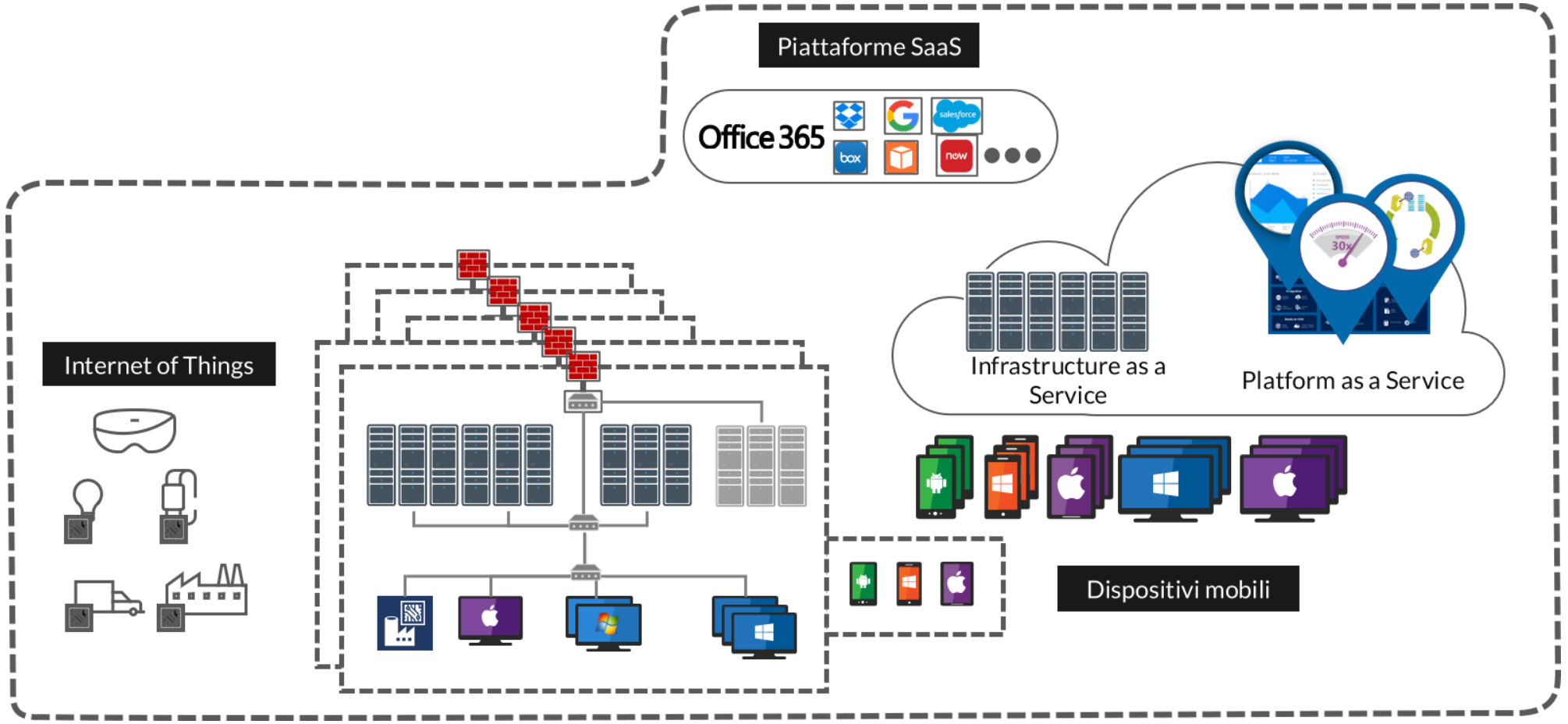
Pietro Visentin

Head of Security @ Moresi.com

Azvise.com

AZURE DAY

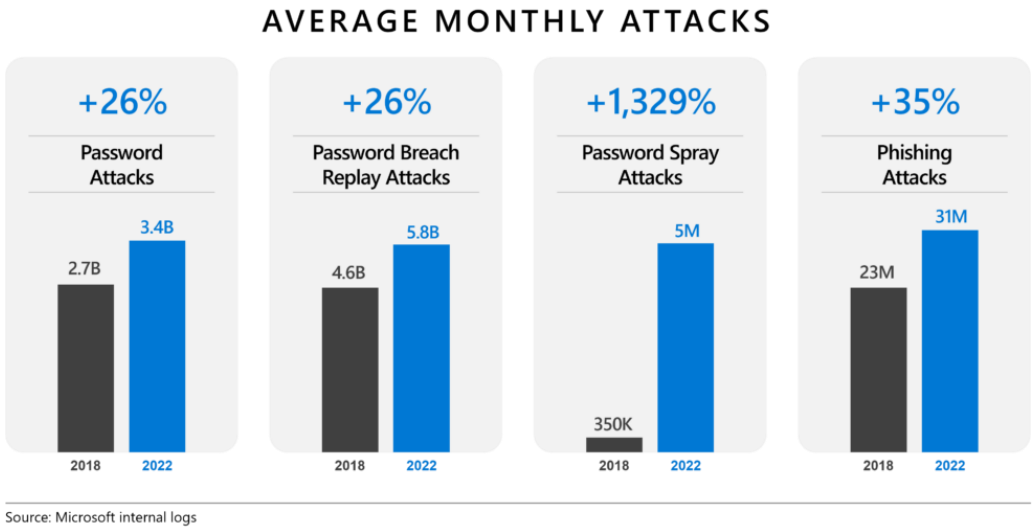
Le identità come focus



AZURE DAY

MFA per tutti

- Molti admin sono ancora senza MFA.
- MFA sicuri (Authenticator) e blocco protocolli legacy
- Il 29% degli utenti su Microsoft 365 e Azure il mese scorso ha effettuato un login multifattoriale.
- Securing security info registration



AZURE DAY

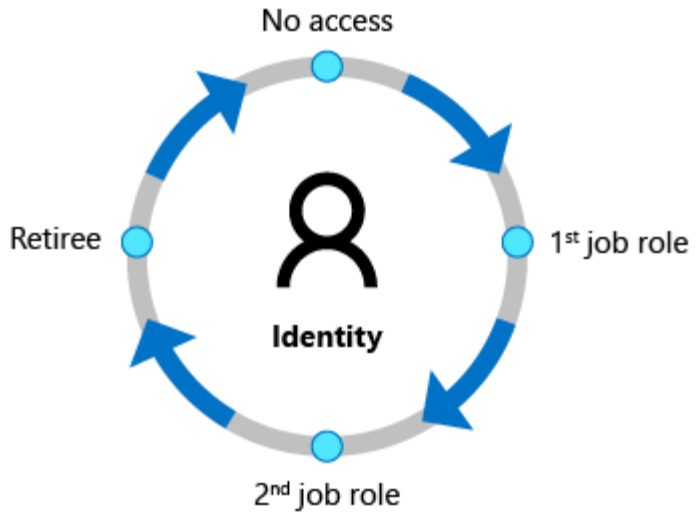
Passwordless per gli admin

- L’MFA non basta più
- Transizione a Passwordless
- Abilitare l’accesso solo da risorse conosciute e gestite

AZURE DAY

Who are your admins?

- Meno di 5 Global Admin
- Devono ancora avere permessi?
- Access Reviews
- Come primo check controllare:
  - Global Administrators
  - Privileged Role Administrators
  - Exchange Administrators
  - SharePoint Administrators



AZURE DAY

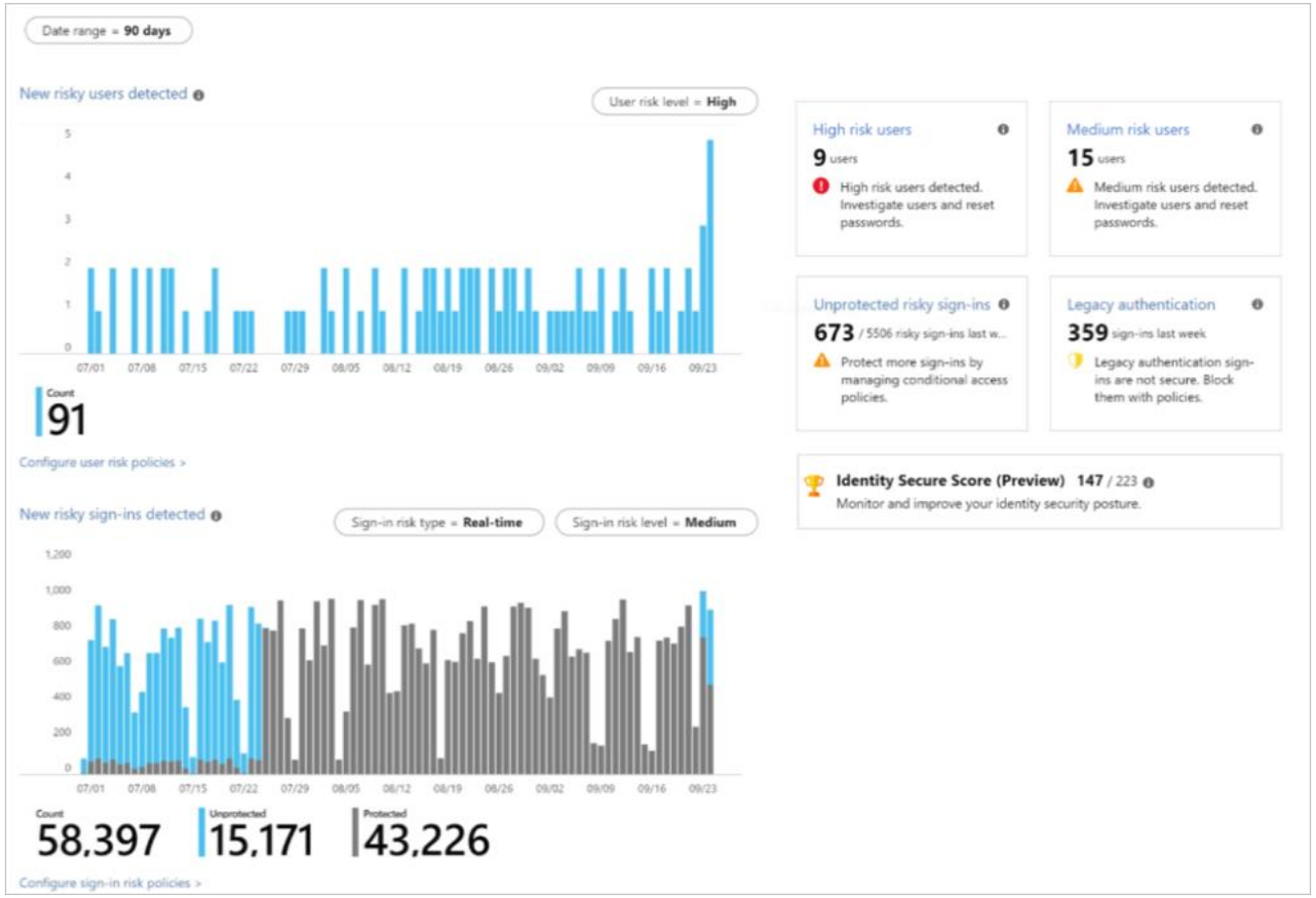
GA o non GA? Owner o non Owner?

- Minimizzare gli utenti con permessi globali
- Gestire i ruoli privilegiati con processi ben stabiliti
- Stessa cosa per le sottoscrizioni Azure
- Entra Permissions Management (CIEM)

Per facilitare la scelta dei ruoli:

AZURE DAY

Gli admin si gestiscono «in casa»



- Managed Accounts for Admins
- Devono essere su Azure AD, meglio se sul proprio tenant
- Niente guest (Outlook.com, live, hotmail)
- Protezione con Identity Protection

AZURE DAY

Gli admin separati

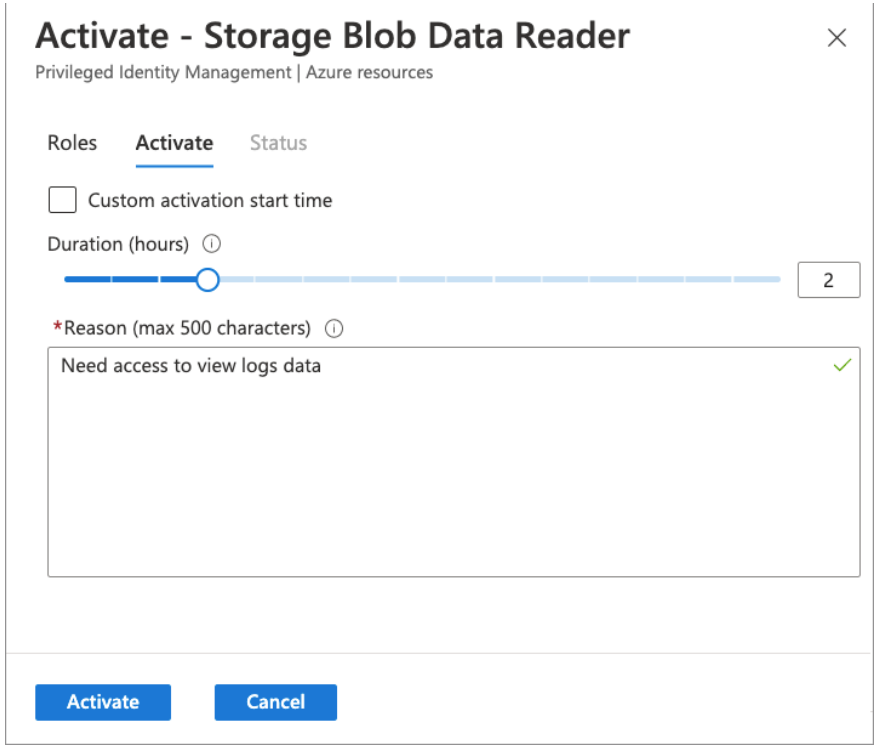
- Gli account per la produttività (email, teams, etc.) e gli account amministrativi non devono essere gli stessi.
- Creare un account amministrativo senza licenza, ma con forward su un email di produttività.

- Con account cloud si reduce il lateral movement.
- Il phishing rimane uno dei vettori più important di attacco, anche per gli admin.

AZURE DAY

Admin per poco

- Just in time anche per i permessi amministrativi con PIM.
- Impostare workflow di approvazione
- Se l'account ha sempre permessi attivi è anche più difficile la parte di auditing.



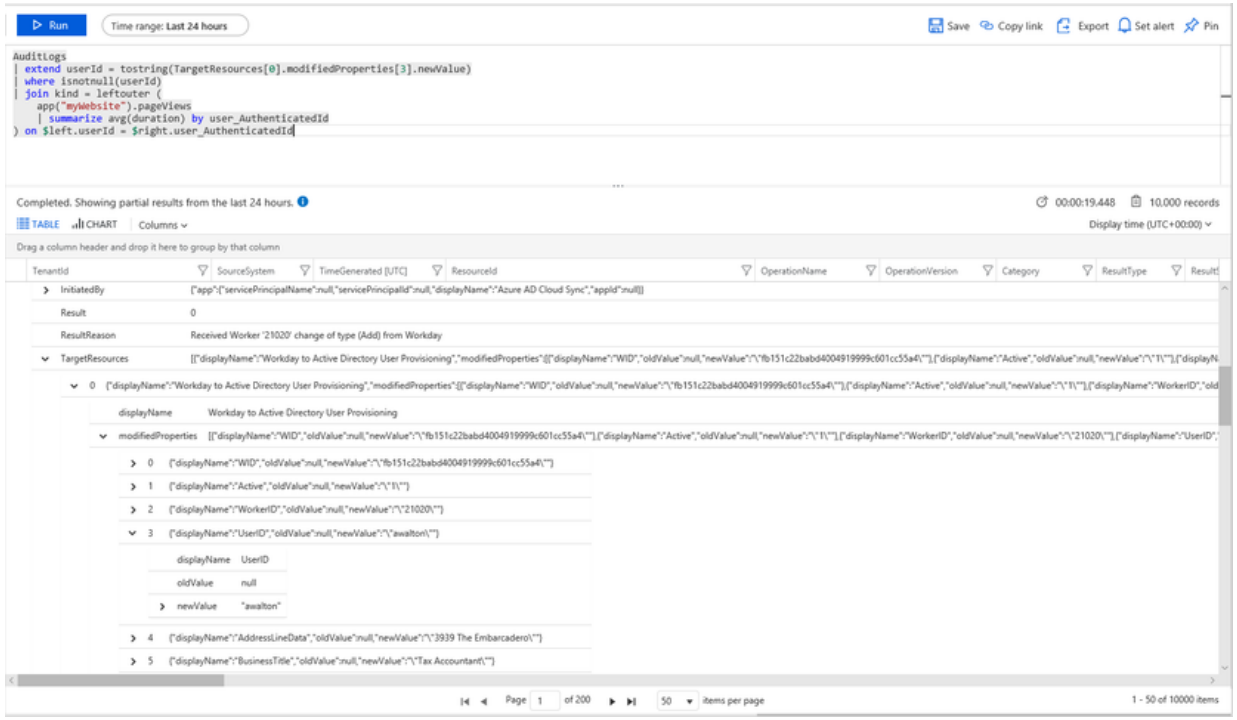
AZURE DAY

In caso di emergenza rompere il vetro

- E se i servizi MFA sono giù?
- Si possono usare le FIDO2
- Due, cloud-only, e con il dominio .onmicrosoft.com
- Questa volta il ruolo è permanent
- Tendenzialmente metodi MFA diversi da quelli usati per gli altri admin
- Niente metodi «phone-based» o Conditional Access Policies
- Auditing

AZURE DAY

Che succede nel regno?



- Esportare i Log verso Log Analytics
- Abilitare Unified Audit Logs
- Must Learn KQL
- Senza alert non ci si accorge di molto

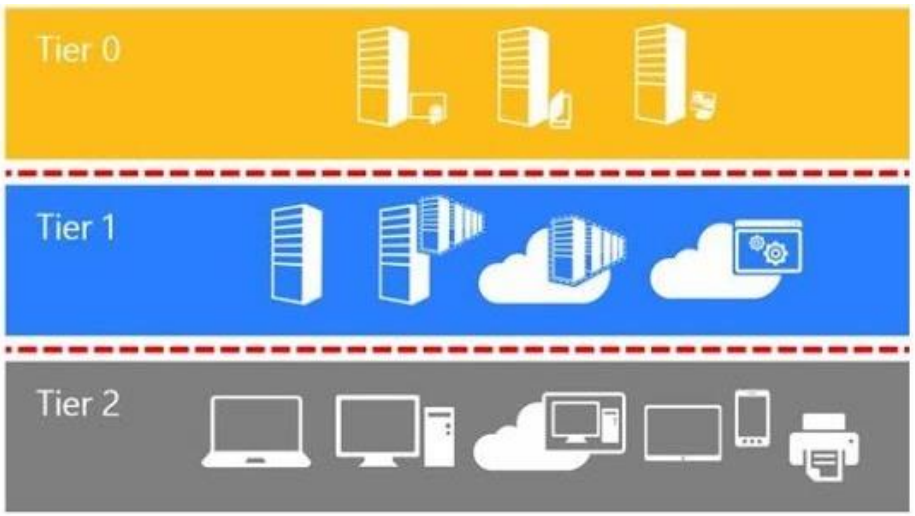
AZURE DAY

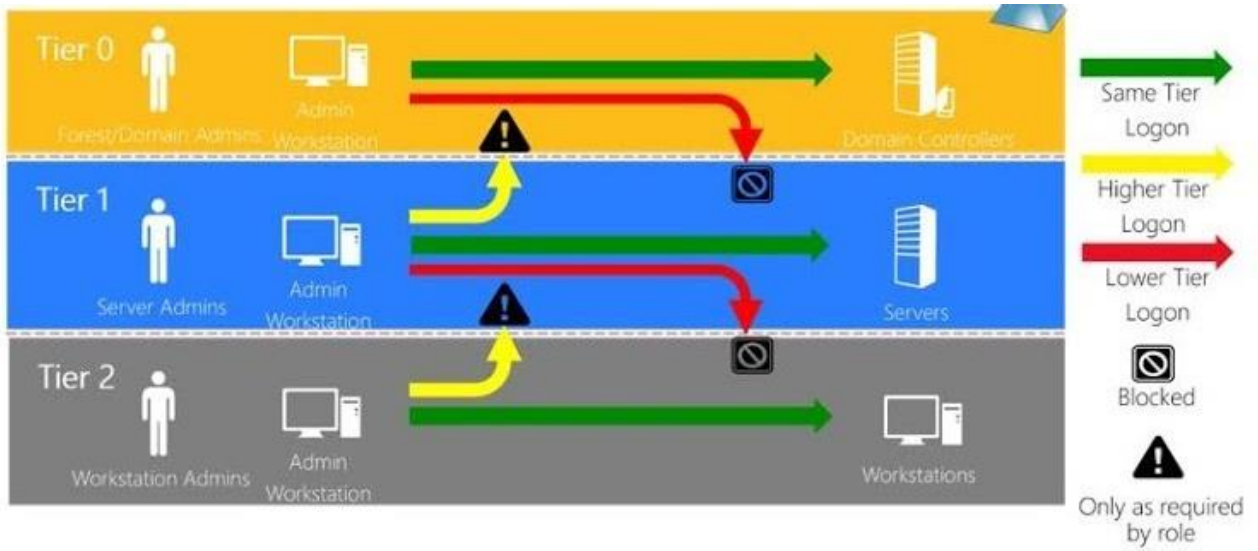
E le workstation?

- Baseline di sicurezza per Windows 10
- Monitoring
- Dove possibile, PAW! (o quantomeno con standard più elevati)
- Azure AD Joined
- Possibilità di accedere ai portali solo da determinati device (escludendo gli emergency admins)

AZURE DAY

Non dimentichiamo AD





- La sicurezza di AD in ambienti ibridi è altrettanto importante
- Usare Purple Knight o PingCastle
- Il tiering model di AD

Question Time

AZURE DAY

Thank You!!!

Thanks to

Microsoft

avanade

4wardPRO
AN IMPRESOFT COMPANY

altitudo

BC Soft
consulenza sistemi informativi

LOBRA

Reti
Società Benefit

UNIKEY
Bringing IT knowledge to the people

stickermule

Packt›