



AZURE DAY



Admin Odyssey: Navigating towards more secure Azure AD Admin Accounts

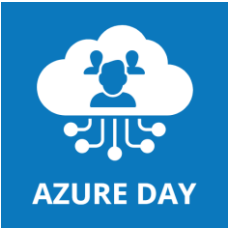
Pietro Visentin @ Moresi.com



Thanks to



Microsoft



avanade



4wardPRO

AN IMPRESOFT COMPANY



LXOBRA

Reti
Società Benefit



Packt>





AZURE DAY

WhoAml



Pietro Visentin

Head of Security @ Moresi.com

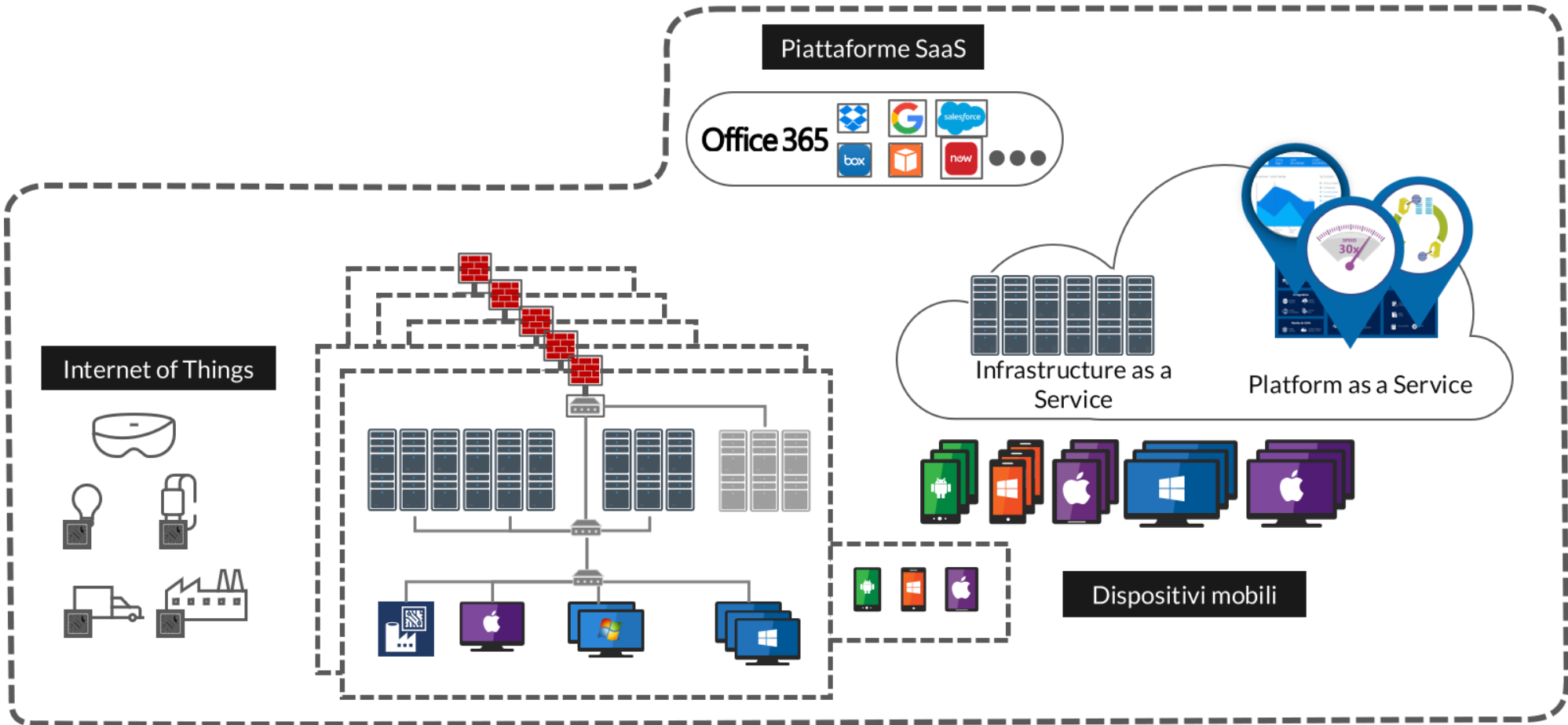


Azvise.com



AZURE DAY

Le identità come focus



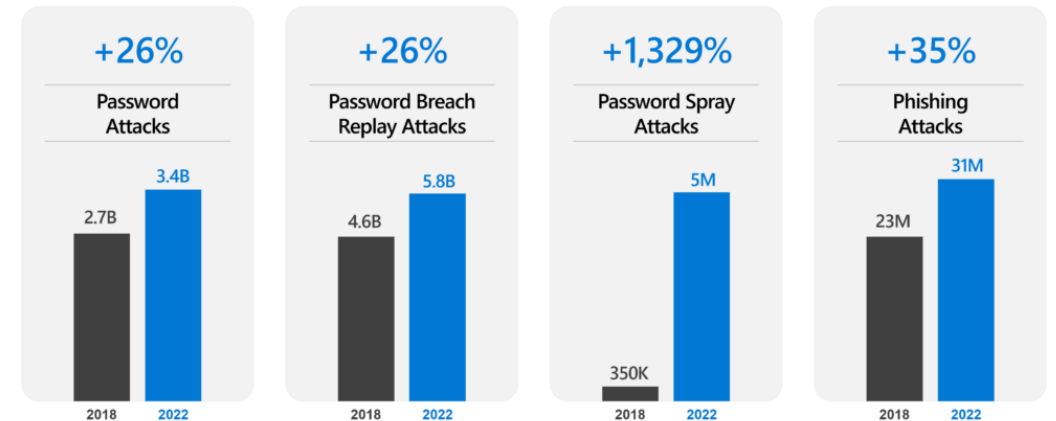


AZURE DAY

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

AVERAGE MONTHLY ATTACKS



Source: Microsoft internal logs



AZURE DAY

Passwordless per gli admin

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

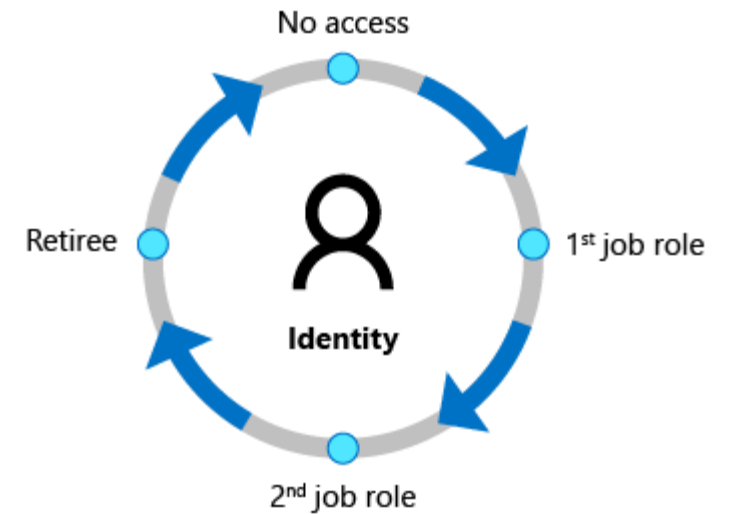
Bad: Generic Password	Less Bad: Password and...	Better: Password and...	Best: Passwordless
123456 qwerty password iloveyou Password1	 SMS  Voice	 Authenticator app (push notifications)  Software Tokens OTP  Hardware Tokens OTP	 Authenticator app (passwordless)  External security key  Windows Hello  Passkeys



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.

Activate - Storage Blob Data Reader

Privileged Identity Management | Azure resources

Roles **Activate** Status

Custom activation start time

Duration (hours) ⓘ

2

*Reason (max 500 characters) ⓘ

Need access to view logs data ✓

Activate **Cancel**



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?

Run Time range: Last 24 hours Save Copy link Export Set alert Pin

```
AuditLogs
| extend userId = toString(TargetResources[0].modifiedProperties[3].newValue)
| where isnotnull(userId)
| join kind = leftouter (
  app("mywebsite").pageViews
  | summarize avg(duration) by user_AuthenticatedId
) on $left.userId = $right.user_AuthenticatedId
```

Completed. Showing partial results from the last 24 hours. 00:00:19.448 10,000 records

Display time (UTC+00:00)

Drag a column header and drop it here to group by that column

TenantId	SourceSystem	TimeGenerated [UTC]	ResourceId	OperationName	OperationVersion	Category	ResultType	Result
>	InitiatedBy	[{"app":{"servicePrincipalName":null,"servicePrincipalId":null,"displayName":"Azure AD Cloud Sync","appId":null}]						
	Result	0						
	ResultReason	Received Worker '21020' change of type (Add) from Workday						
>	TargetResources	[{"displayName":"Workday to Active Directory User Provisioning","modifiedProperties":[{"displayName":"WID","oldValue":null,"newValue":"fb151c22babd4004919999c601cc55a4"}, {"displayName":"Active","oldValue":null,"newValue":"1"}, {"displayName":"WorkerID","oldValue":null,"newValue":"21020"}]						
>	0	[{"displayName":"Workday to Active Directory User Provisioning","modifiedProperties":[{"displayName":"WID","oldValue":null,"newValue":"fb151c22babd4004919999c601cc55a4"}, {"displayName":"Active","oldValue":null,"newValue":"1"}, {"displayName":"WorkerID","oldValue":null,"newValue":"21020"}]						
	displayName	Workday to Active Directory User Provisioning						
>	modifiedProperties	[{"displayName":"WID","oldValue":null,"newValue":"fb151c22babd4004919999c601cc55a4"}, {"displayName":"Active","oldValue":null,"newValue":"1"}, {"displayName":"WorkerID","oldValue":null,"newValue":"21020"}]						
>	0	[{"displayName":"WID","oldValue":null,"newValue":"fb151c22babd4004919999c601cc55a4"}]						
>	1	[{"displayName":"Active","oldValue":null,"newValue":"1"}]						
>	2	[{"displayName":"WorkerID","oldValue":null,"newValue":"21020"}]						
>	3	[{"displayName":"UserID","oldValue":null,"newValue":"awalton"}]						
	displayName	UserID						
	oldValue	null						
>	newValue	"awalton"						
>	4	[{"displayName":"AddressLineData","oldValue":null,"newValue":"3939 The Embarcadero"}]						
>	5	[{"displayName":"BusinessTitle","oldValue":null,"newValue":"Tax Accountant"}]						

Page 1 of 200 50 items per page 1 - 50 of 10000 items

- 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?

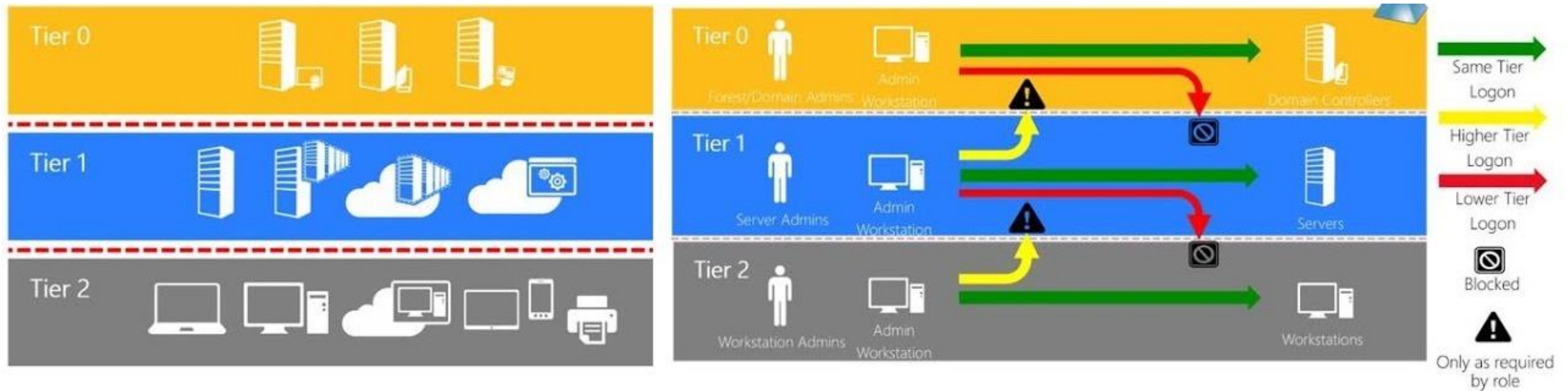
- Baseline di sicurezza per Windows 10
- Monitoring
- Dove possibile, PAW! (o quantomeno con standard più elevati)
- Azure AD Joined
- Possibilità di accedere ai portali solo da determinati device (escludendo gli emergency admins)





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

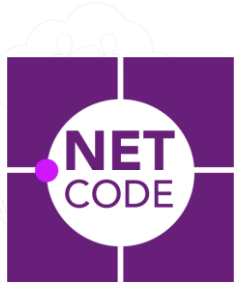
Question Time





AZURE DAY

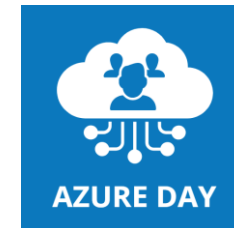
Thank You!!!



Thanks to



Microsoft



avanade



4wardPRO

AN IMPRESOFT COMPANY



LXOBRA

Reti
Società Benefit



Packt>

