Password-less: Weg met wachtwoorden voor dagelijks gebruik

Sander Berkouwer, SCCT
Raymond Comvalius, NextXpert

WAZUG.NL
AZURE USER GROUP NL

Introductie

Raymond Comvalius
NextXpert
Onafhankelijk architect
@NextXpert

Sander Berkouwer
CTO bij SCCT BV
DirTeam.com
@SanderBerkouwer

Achtergrond

Waarom we af moeten van wachtwoorden

Waarom wachtwoorden slecht zijn

Wachtwoorden zijn problematisch

Ze kunnen worden:

- Gekraakt
- Gestolen
- Onderschept
- Afgekeken
- Gephisht
- Hergebruikt

Wachtwoorden staan in de weg

Mensen zijn niet gemaakt om wachtwoorden te onthouden
Password resets kosten organisaties klauwen met geld

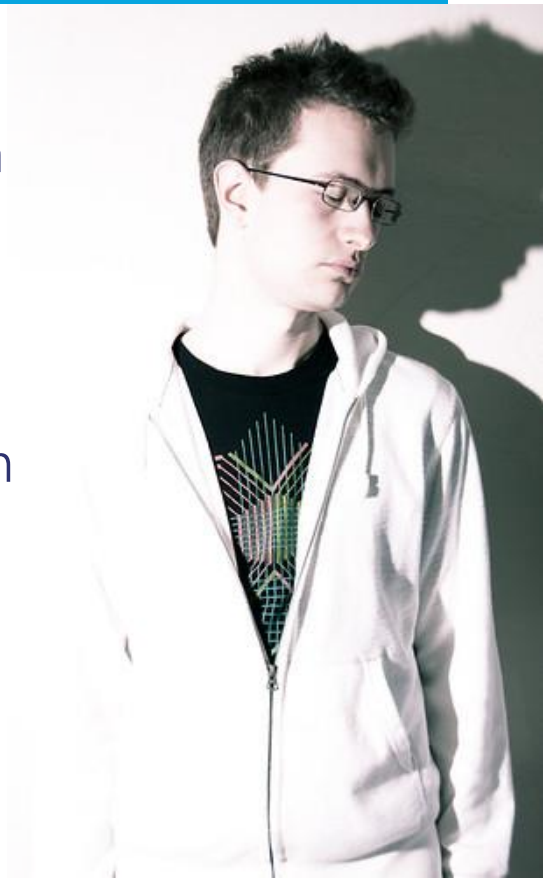
Hoe slecht zijn ze?

81%

81% van alle digitale Incidenten in 2018 werden veroorzaakt door zwakke, gelekte en standaard wachtwoorden.

20%

20% van alle IT-kosten van organisaties gaat op aan het helpen van medewerkers hoe om te gaan met wachtwoorden.



Maar wat er gebeurt zoal rondom ons?

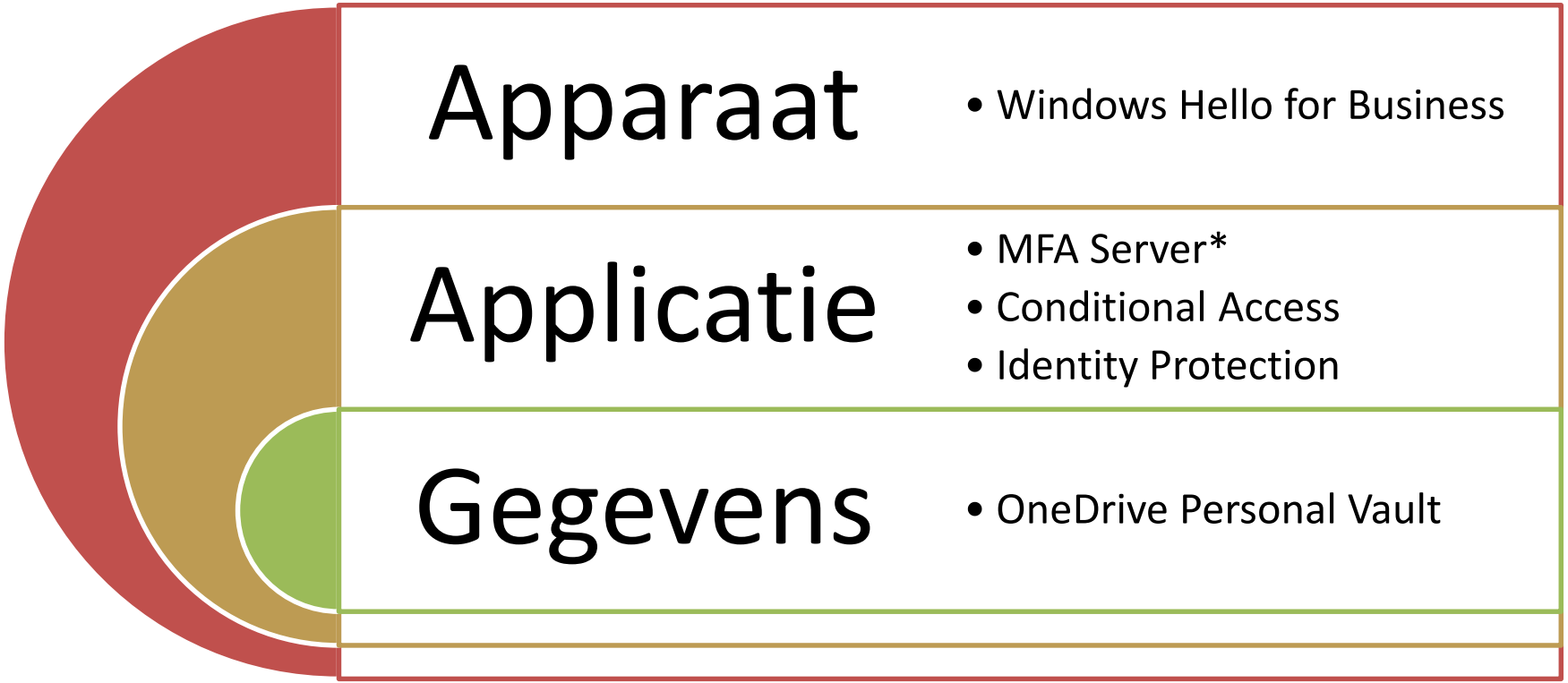
Gemeente Lochem

Remote Desktop Server rechtstreeks op het Internet geplaatst
Geen IP whitelisting, RDP Guard of Multi-factor Authentication
Kwaadwillenden hebben alles versleuteld en eisten losgeld.
https://www.lochem.nl/laatste-nieuws/nieuwsbericht/gemeentenieuws/gemeente-lochem-door-het-oog-van-de-naald-bij-hack-2553.html

Christelijk Lyceum *********

Op bezoek na datalek, keylogger van leerling
Ook Remote Desktop Server rechtstreeks op het Internet geplaatst
Acties: Remote Desktop Web Access geplaatst
RD Web Access gepubliceerd met Azure AD App Proxy
Conditional Access toegepast

Wat er vandaag technisch beschikbaar is



Demo

OneDrive Personal Vault

Windows Hello for Business

Windows Hello for Business

Kijk mama, zonder wachtwoorden!

Password-less, strong authentication,

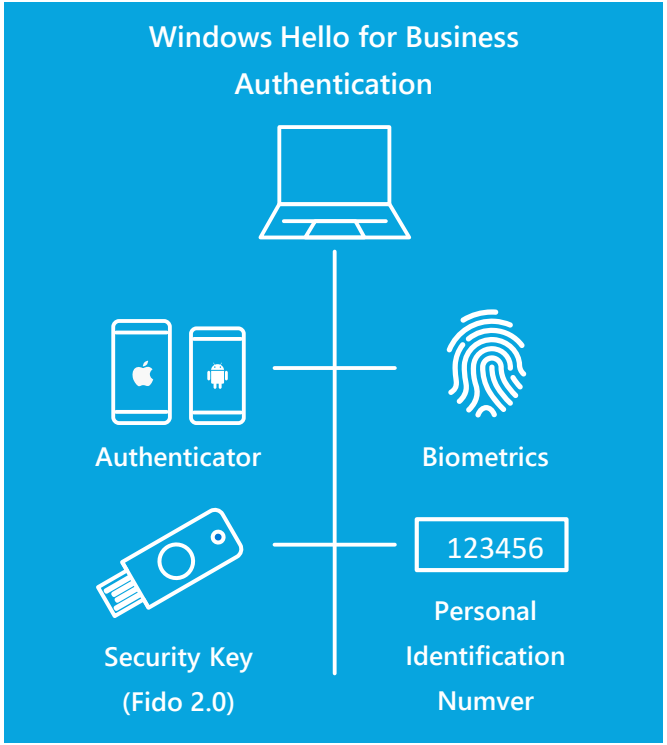
Beschikbaar op Windows 10

Standaard multi-factor authentication

PIN, vingerafdruk of app is eerste factor

Enrollment (gelinkt aan TPM chip) is 2e factor

Single Sign-On



Windows Hello for Business Uitrolscenario's

Azure Active Directory-only

Na Azure AD Join, gelijk Windows Hello-registratie voor je kiezen
Device Registration en authenticatie vinden plaats tegen Azure AD

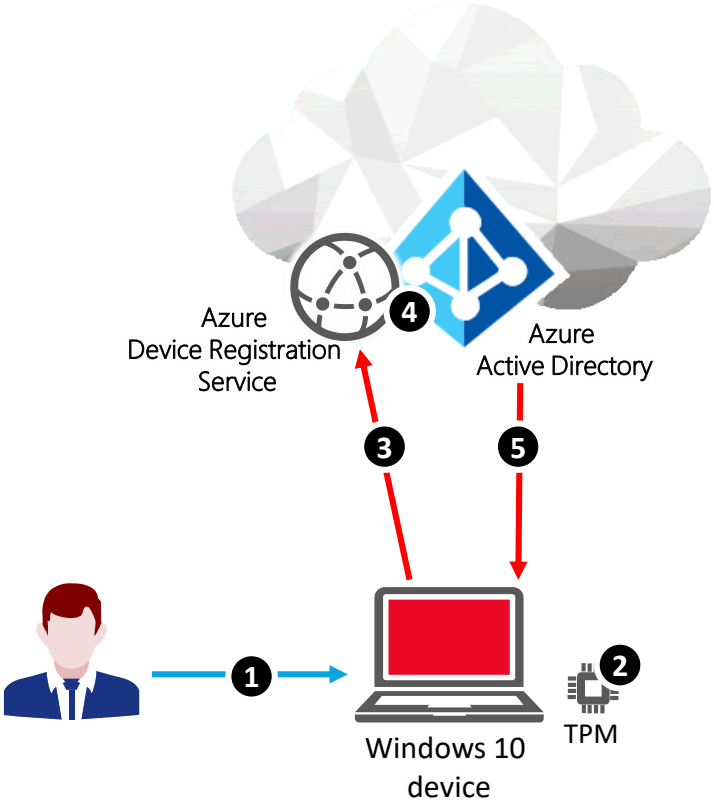
Hybrid

Device Registration en authenticatie vinden plaats tegen Azure AD
Vereist Azure AD Connect en alle objecten in scope voor synchronisatie
Voorkeursscenario: Windows Server 2016 Domain Controllers

Active Directory on-premises

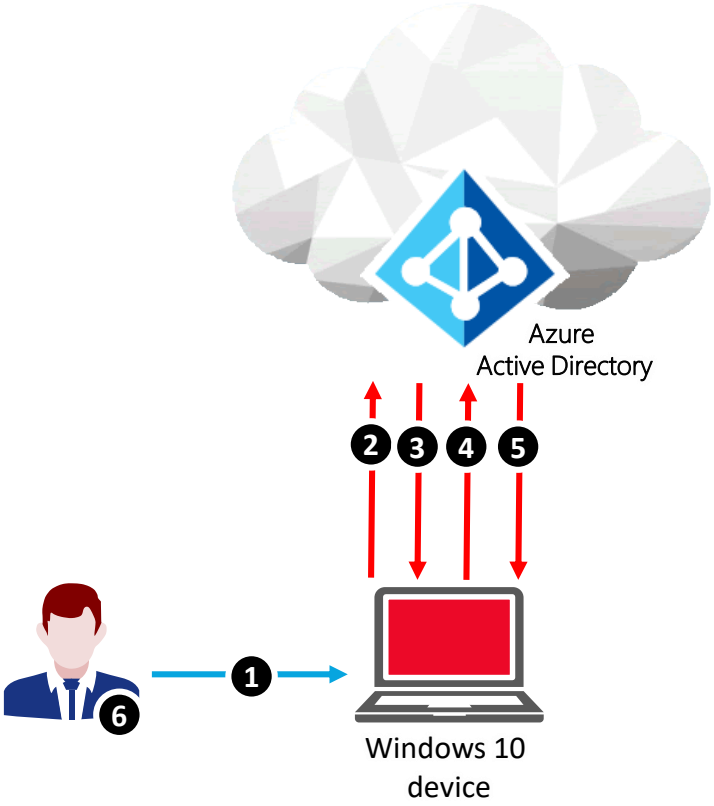
Device Registration vindt plaats tegen AD FS
AD FS dient het Windows Server 2016 FBL te draaien
Voorkeursscenario: Windows Server 2016 Domain Controllers met Key Trust
(anders minimaal één Certification Authority nodig voor Certificate Trust)

Windows Hello registratie



1. Persoon meldt aan met wachtwoord en MFA en registreert biometrische aanmeldmethode.
2. Windows genereert een Windows Hello for Business sleutel in TPM, beschermd met biometrische aanmeldmethode en *attestation blob*.
3. Windows stuurt publieke sleutel van HfB certificaat, attestation blob en AIK certificaat naar Azure DRS.
4. Azure DRS verifieert de HfB sleutel met de attestation blob en registreert sleutel met useraccount.
5. Azure retourneert de sleutel ID.

Aanmelden met Windows Hello



1. Persoon meldt aan met biometrische optie.
2. Windows stuurt ‘Hello’.
3. Azure AD stuurt ‘nonce’.
4. Windows stuurt ondertekende ‘nonce’ met Windows Hello sleutel.
5. Azure AD stuurt PRT, ID token en versleutelde sessiesleutel, gekoppeld aan TPM.
6. Persoon heft Single Sign-On toegang tot cloud en on-premises applicaties.

Demo

Aan de slag met een Windows Hello for Business Security Key

Microsoft's Password-less Journey

Deploy Windows Hello for Business to offer password-replacing options	Reduce the user-visible password surface area, by not prompting end-users for passwords anymore	Transition into a password-less environment where passwords are no longer the norm	Eliminate passwords from the identity provider

Wat als…

Iedereen password-less authenticatie gebruikt?

We gaan van wachtwoordresets naar PIN-resets

Wachtwoorden verlopen, maar mensen gebruiken ze niet meer

Waarschijnlijk een toename in wachtwoordresets, totdat…

Iedereen geen wachtwoorden meer heeft?

We moeten gaan bedenken hoe we Azure AD Join doen

We moeten gaan bedenken hoe we accounts uitdelen

… een hele hoop processen gaan op de schop

Demo

Password-less Azure AD Join

Afsluitend