Lock-out na aanpassen password?

Tips & tricks

Heeft u govroam als primary SSID? Komt het voor dat uw eindgebruikers een lockout krijgen op hun kantoorvoorzieningen als hun wachtwoord net is aangepast? Hieronder enkele manieren die kunnen helpen dit ongemak te minimaliseren.

Deze oplossingen maximaliseren het gebruiksgemak en de inzet van govroam. Let wel: dit probleem wordt *nie*t veroorzaakt door govroam, deze sluist 'slechts' op een veilige manier de authenticatie van de eindgebruiker door.

Het probleem en de oorzaak

Eindgebruikers raken toegang kwijt tot hun kantoorautomatisering na wijzigen van het wachtwoord.

- Treedt op wanneer het Active Directory (AD)-account gebruikt wordt voor wifi-toegang
- Eindgebruikers wijzigen hun wachtwoord van de Active Directory (die toegang geeft tot hun kantoorvoorzieningen zoals e-mail, Citrix etc.)
- Vervolgens vergeten ze het nieuwe wachtwoord in te stellen op hun mobiele apparaten waarin ze (govroam) wifi geconfigureerd hebben
- Wanneer hun apparaat te vaak met het oude wachtwoord op wifi probeert in te loggen, blokkeert de AD het hele account, dus ook voor e-mail etc.

Oplossingen

Zoals toegepast door enkele aangesloten organisaties, aangevuld met enkele suggesties van govroam specialist Erik Dobbelsteijn.

1. <u>Gebruikers instrueren</u>:

   Voorafgaand aan een password-wijziging, de eindgebruikers middels email en/of sms-berichten tijdig attenderen (inclusief instructies) op de aanstaande passwordwijziging en er op wijzen dat ze meteen het wachtwoord op hun apparaten moeten aanpassen..

   Uiteraard werkt dit alleen, als de gebruikers zélf daadwerkelijk iets doen met deze herinnering(en).

2. Het wachtwoord automatisch laten aanpassen via EMM/UEM

   Organisaties die apparaten op afstand beheren, kunnen in de mogelijkheid zijn om het wifi-profiel voor de gebruiker te configureren. Het EMM/UEM systeem moet dan de accountgegevens kunnen achterhalen, en deze kunnen (en mogen) 'pushen' naar het eindgebruikersapparaat. Dit werkt alleen voor managed devices, dus niet voor BYOD.

3. Sterkere wachtwoorden langer geldig laten zijn (conform NIST aanbeveling):

   Al langer adviseert het National Institute of Standards and Technology (NIST) om het beleid om regelmatig wachtwoorden aan te passen die relatief zwak zijn, te vervangen door beleid dat het gebruik van langere wachtwoorden (liefst hele zinnen) toestaat voor een langere periode van bijvoorbeeld 1 jaar. Daardoor verdwijnt het probleem niet, maar komt het in ieder geval minder vaak voor.

   Deze oplossing kan uiteraard worden gecombineerd met de andere oplossingen.

4. Soft-lockout:

   De wifi-toegang blokkeren, maar niet het AD-account. Door bijvoorbeeld op de RADIUS server een wachtperiode te hanteren na 3x foutief inloggen op wifi, terwijl de policy op AD bijv. 5x hanteert, zal de AD het account niet locken.

   Met het toepassen van deze methode wordt de IT-afdeling minder belast, weet beter te achterhalen wat het precieze probleem is (namelijk uitsluitend wifi gerelateerd) en heeft de gebruiker de mogelijkheid om zélf alsnog het password te wijzigen op het apparaat voordat zij compleet in de lockout situatie terecht komen.

5. Gebruik van een 'Application specifiek password':

   Ofwel andere dan AD-accounts gebruiken voor wifi-toegang. Dit houdt in dat een ander, specifiek account gebruikt wordt voor de wifi-dienst. Deze manier maakt het mogelijk dat het AD-account niet gebruikt wordt voor applicaties die minder belangrijk geacht worden, zoals wifi-toegang.

6. Gebruik van certificaten (EAP-TLS):

   Het uitgeven van certificaten vervangt het gebruik van wachtwoorden. Het genereren, gecontroleerd uitgeven en distribueren naar mobiele apparaten is een flinke klus om op te zetten, waarbij mobility-management kan helpen.

   Tijdens gesprekken met verschillende deelnemers hebben wij sterke voorstanders en mínder sterke voorstanders van deze mogelijkheid gesproken vanwege de impact. Voor organisaties

die al een EMM/UEM tool gebruiken, is de stap minder groot. Ook dan nog moeten certificaten worden ingetrokken bij misbruik of uitdiensttreding, dus de PKI moet daarvoor geschikt zijn.

Aanvullingen op bovenstaande oplossingen? Dan horen we graag van u!
Eventuele opmerkingen en/of aanvullingen graag per e-mail sturen naar frits.kuus@govroam.nl.