okta

ADAPTIEVE MULTI-FACTOR AUTHENTICATIE

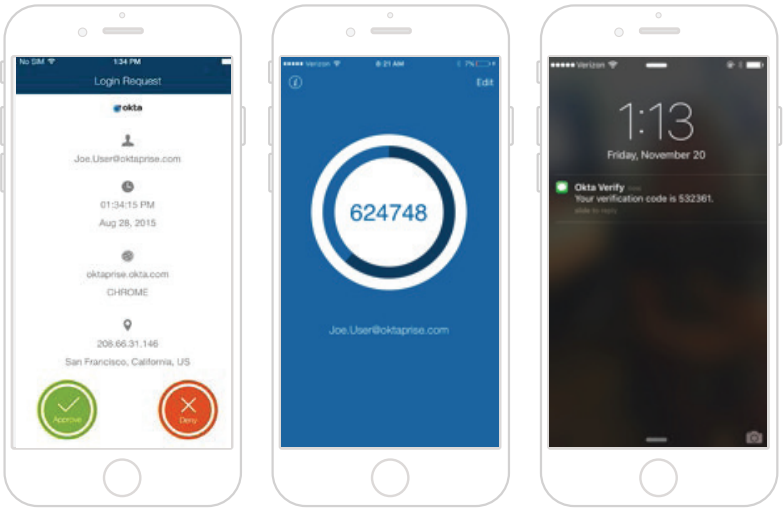
Whitepaper

Okta Benelux
Strawinskylaan 4117, 3rd Floor
1077 ZX Amsterdam,
The Netherlands

info_benelux@okta.com
+44 (800) 3688930

Samenvatting

De whitepaper biedt een overzicht van Okta Adaptive MFA (adaptieve multi-factor authenticatie van Okta). Voor beveiligingsbewuste organisaties die applicaties en data willen beveiligen, vormt Okta Adaptive MFA een uitgebreide, gebruiksvriendelijke en krachtige authenticatieoplossing. Deze oplossing biedt beleidsgebaseerd, contextafhankelijk toegangsbeheer, ondersteunt een breed scala aan moderne factoren, benut big-data-inzichten van duizenden organisaties en kan worden geïntegreerd met de applicaties en VPN's die organisaties nodig hebben. Met Okta Adaptive MFA beschikken organisaties over beveiliging op enterpriseniveau met een uitstekende gebruikerservaring.



Beveiliging is een C-Level aangelegenheid

Beveiligingslekken kunnen niet meer worden beschouwd als een IT-probleem. Het beveiligen van organisaties tegen reputatie- en financiële schade als gevolg van diefstal van vertrouwelijke data heeft de hoogste prioriteit van directieleden. Gemiddeld duurt het 205 dagen voordat organisaties ontdekken dat een beveiligingslek is ontstaan.[1] Dergelijke incidenten hebben grote en langdurige gevolgen. De getroffen organisaties zijn niet alleen aansprakelijk voor schade, maar de omzet kan ook afnemen doordat consumenten liever geen zakendoen en gegevens delen met organisaties die de vertrouwelijke data niet goed beveiligen.

Traditionele gebruikersauthenticatie is niet toereikend

Organisaties beveiligen de toegang tot VPN's en applicaties vanouds met enkelvoudige authenticatie: een wachtwoord. Wachtwoorden zijn niet alleen lastig te beheren, maar ook kwetsbaar voor allerlei aanvallen. Hackers gebruiken phishing, social engineering en andere steeds geavanceerdere technieken om wachtwoorden voor consumenten-, bank- en bedrijfsapplicaties te stelen. Deze aanvallen komen steeds vaker voor en IT- en securitymedewerkers zijn verantwoordelijk voor de implementatie van nieuwe beveiligingsmaatregelen om ze af te weren.

[1] http://www.itsecurityguru.org/tag/breach

De relatieve kosten van een datalek stijgen jaarlijks.[2]

Het percentage mensen dat phishingberichten opent. Elf procent klikt op de bijlage.[3]

Het percentage aanvallen op webapps dat voortvloeit uit gestolen logingegevens.[3]

Bij het datalek bij Anthem hebben hackers persoonlijke documenten uit databases van Anthem gestolen met illegaal verkregen logingegevens van admins. Met multi-factor authenticatie (Multi-Factor Authentication, MFA) hadden de hackers meer dan alleen de admin logingegevens nodig gehad om toegang tot de data van Anthem te krijgen. Het verlies van de data van bijna 78,8 miljoen mensen, waarvan 8,8 tot 18,8 miljoen niet eens klant van Anthem waren, zou zijn voorkomen met deze aanvullende verificatie.

De impact van mobility

Vanwege de toenemende mobiliteit van medewerkers moeten organisaties de toegang tot applicaties en data op een andere manier beveiligen. Applicaties worden tegenwoordig met mobiele devices gebruikt vanuit huis, cafetaria's en hotels. Gebruikers willen beschikken over de flexibiliteit om vanaf elke plaats te connecten, zodat IT- en securitymedewerkers beveiligde toegang moeten bieden vanaf onbekende netwerken en apparaten.

De voordelen van MFA

MFA is ontworpen om organisaties te beschermen tegen allerlei aanvallen met gestolen logingegevens. Bij MFA moeten gebruikers naast hun primaire wachtwoord nog iets indienen om te worden geauthenticeerd: iets wat de gebruiker is, heeft of weet. Zelfs als het wachtwoord van een gebruiker wordt gestolen, zorgt MFA ervoor dat het gebruikersaccount wordt beschermd tegen ongeoorloofde toegang, omdat hackers nog een aanvullende factor moeten stelen of nabootsen.

[2] Ponemon Institute Report: 2015 Global Cost of a Data Breach.

[3] Verizon Data Breach Investigations Report.

Uitdagingen van oudere MFA-oplossingen

Slechte gebruikerservaring

Hoewel MFA significante voordelen biedt, kan MFA op verschillende manieren verstorend zijn voor eindgebruikers. Oplossingen met fysieke tokens zijn duur en moeilijk te beheren. Het traceren en vervangen van tokens brengt aanzienlijke kosten met zich mee. Eindgebruikers vinden het omslachtig om fysieke tokens mee te nemen en geheime codes in te voeren. Bij bedrijven met een strikt MFA-beleid moeten eindgebruikers zich dagelijks vaak opnieuw authenticeren, wat leidt tot een afname van de productiviteit en een toename van frustraties.

Moeilijk te beheren

Oudere, losstaande MFA-producten zijn lastig te implementeren. IT-teams moeten het MFA-product afzonderlijk integreren met elke applicatie en elk systeem. Het is complex om aanvullende applicaties en gebruikers te beschermen met MFA, zodat het moeilijk is om implementaties op te schalen. Bij het ontwikkelen van afzonderlijke integraties kunnen bepaalde resources buiten de boot vallen, omdat beheerders vergeten of niet weten dat deze ook moeten worden beschermd met MFA.

Niet schaalbaar

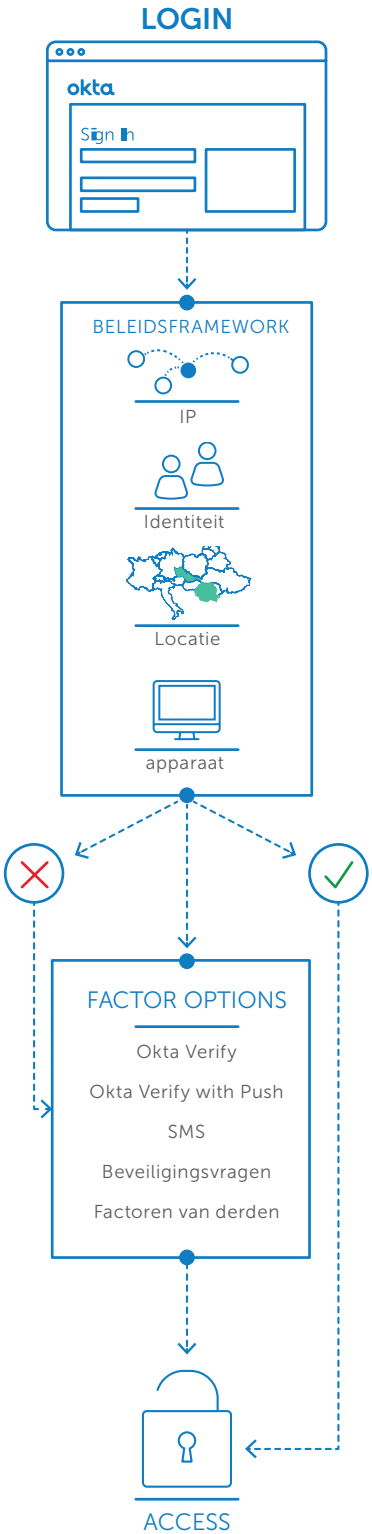
Met losstaande MFA-producten moeten organisaties erop vertrouwen dat applicaties en systemen ondersteuning bieden voor leveranciersspecifieke integraties, zodat geen brede MFA-bescherming voor alle apps en resources mogelijk is. Nu steeds meer organisaties cloudapps adopteren, merken ze dat deze applicaties de ingebouwde integraties van hun MFA-leverancier vaak niet ondersteunen. Deze cloudapplicaties bieden geen ondersteuning voor MFA of gebruiken een eigen mechanisme, zoals geheime codes via sms of beveiligingsvragen. Dit veroorzaakt verwarring bij eindgebruikers, omdat zij nu andere logingegevens en MFA-factoren moeten gebruiken voor de verschillende applicaties en services waarmee ze werken.

Niet alle typen gebruikers kunnen worden beveiligd

Doordat het aantal gebruikers in een organisatie en hun verscheidenheid blijven toenemen, is het wellicht niet mogelijk om één specifiek type MFA-factor te benutten voor mobiele of internationale gebruikers of voor bepaalde gebruikersgroepen die vanwege hun functie niet beschikken over een smartphone. Bij veel callcenters mogen medewerkers bijvoorbeeld geen eigen mobiele apparaten meenemen.

Een nieuwe benadering tot beveiliging: slimmer, gebruiksvriendelijker en uitgebreider

Okta Adaptive MFA biedt een antwoord op de problemen van oudere, losstaande MFA-producten door beveiliging op ondernemingsniveau en een uitstekende gebruikerservaring te bieden met beleidsgebaseerd, contextafhankelijk toegangsbeheer, ondersteuning voor een breed scala aan moderne factoren, big data-analyses en ingebouwde integraties voor alle applicaties en VPN's die organisaties moeten beveiligen.



Minder risico met contextafhankelijk toegangsbeheer

Contextafhankelijk toegangsbeheer van Okta helpt organisaties om de risico's te verminderen door te onderzoeken wanneer, waar en hoe gebruikers toegang krijgen tot tapplicaties en data. Organisaties kunnen desgewenst aanvullende authenticatie verlangen, de reikwijdte beperken of toegang weigeren afhankelijk van de gebruiker, het netwerk of het land van waaruit verbinding wordt gemaakt, en het apparaat dat wordt gebruikt. Beheerders zijn zelfs in staat om de toegang aan te passen op basis van de verificatiefactor die de gebruiker selecteert en de wijze waarop de primaire authenticatie is uitgevoerd.

Met het nauwkeurige contextafhankelijke toegangsbeleid van Okta Adaptive MFA kunnen eenvoudig aanvullende resources worden beveiligd met een tweede factor, zonder dat dit gevolgen heeft voor de normale gebruikersactiviteit. Gebruikers worden niet bij elke aanmeldingspoging geverifieerd, maar alleen wanneer dat nodig is.

Uitgebreide dekking van gebruikers met een moderne verzameling Tweede factors

Dankzij integratie van een breed scala aan tweede factoren en een flexibel toegangsbeleid hoeft de IT zich niet meer te bekommeren over de vraag of gebruikers de nieuwste smartphone hebben of mogelijk geheel niet over een telefoon beschikken. Okta Adaptive MFA kan alle gebruikers beveiligde toegang bieden met factoren die zijn gebaseerd op de functie, bevoegdheden en werkomgeving van de gebruiker. Met opties die gebruikmaken van smartphones, zoals Okta Verify with Push, kan de identiteit van eindgebruikers snel en eenvoudig worden geverifieerd. Voor gebruikers zonder smartphones ondersteunt Okta Adaptive MFA tevens afwijkende factoren, zoals geheime codes per sms. Bovendien biedt Okta ondersteuning voor integraties met diverse factoren van derden, zoals Yubikey. Daardoor is het eenvoudig om over te schakelen tussen factoren, bijvoorbeeld van RSA naar Okta Verify with Push. Met het toegangsbeleid van Okta kunnen beheerders bepalen welke factoren vereist, optioneel en uitgeschakeld zijn voor specifieke gebruikers en groepen. Ook kunnen zij redundante factoren instellen om de IT-supportkosten te beteugelen.

Proactieve beveiliging en risicogebaseerde adaptieve authenticatie

Met big data analytics van Okta worden risicoscores berekend op basis van uitgebreide gebruikersprofielen om het aantal valspositieve resultaten te beperken en proactieve beveiliging te bieden voor applicaties en data. Beveiligingsteams kunnen de inzichten van Okta in miljoenen gebruikers, apparaten en authenticatieverzoeken benutten om mogelijke aanvallen te herkennen en ongeoorloofde toegang te voorkomen. In tegenstelling tot losstaande MFA-producten die niet het gehele plaatje zien, heeft Okta Adaptive MFA toegang tot Okta-data over single sign on en mobility management in bedrijven. Met deze combinatie van contextuele data van alle authenticatieactiviteiten van een gebruiker wordt de beveiliging verbeterd doordat het hackers moeilijker wordt gemaakt om zich voor te doen als een legitieme gebruiker.

Belangrijker is nog dat Okta Adaptive MFA niet alleen maar waarschuwingen genereert. Okta biedt centraal toegangsbeheer voor alle applicaties en wanneer Okta Adaptive MFA een abnormaal authenticatieverzoek detecteert, wordt de potentiële hacker automatisch tegengehouden. Beheerders hebben bovendien de optie om het risico te verminderen door de toegang volledig te blokkeren of slechts te beperken tot bepaalde resources.

Eenvoudige implementaties met ingebouwde integraties voor alle apps en VPN's

De 100% cloudgebaseerde adaptieve MFA-oplossing van Okta stelt organisaties in staat om alle applicaties en de kritieke infrastructuur te beveiligen met robuuste authenticatie. Beheerders kunnen snel nieuwe toepassingen en VPN's toevoegen met de ruim 500 SAML- en RADIUS-integraties in het Okta Application Network (OAN). Dankzij gecentraliseerd beheer van gebruikers, apparaten en MFA-beveiliging vallen er geen gaten in de dekking wanneer gebruikers en resources worden toegevoegd, gewijzigd en verwijderd.

Beschikbaar voor ontwikkelaars

Het implementeren van MFA is altijd problematisch geweest voor ontwikkelaars die eigen toepassingen en portalen creëren. Okta Adaptive MFA is beschikbaar via API's en de Okta Sign-on Widget, zodat toegangs-, intrekkings- en authenticatiefuncties eenvoudig kunnen worden geïmplementeerd. Ontwikkelaars kunnen snel sterke authenticatie toevoegen aan allerlei maatwerktoepassingen. Met de API's van Okta Adaptive MFA kunnen zij bovendien de gewenste merkidentiteit toevoegen aan de MFA-ervaring. Hierdoor kunnen gebruikers over de eenvoud en het gemak van Okta Adaptive MFA beschikken via een aangepaste gebruikersomgeving.

Conclusie

Met Okta Adaptive MFA kunnen IT- en securitybeheerders effectieve beveiligingsmaatregelen implementeren om applicaties en de infrastructuur te beschermen, zonder dat dit ten koste gaat van de gebruikerservaring. Okta levert een slimmere MFA-oplossing die is gebaseerd op contextuele data over gebruikers, devices en gedrag, alsmede een uitgebreide verzameling moderne factoren om elke gebruiker te ondersteunen. Het is eenvoudig om nieuwe applicaties en gebruikers toe te voegen. Daardoor kan snel rendement op investeringen worden geboekt en is het eenvoudig om van bestaande, lokale MFA-producten te migreren naar de kosteneffectievere cloudgebaseerde oplossing van Okta. Met geïntegreerde single sign on (SSO) en enterprise mobility management maakt Okta het eenvoudig om gebruikers, apparaten en applicaties te beveiligen.

okta

Voor meer informatie kunt u de volgende website bezoeken:
okta.com/learn/Adaptive-MFA