Whitepaper

Implementatie-handleiding voor multi-factor authenticatie

Januari 2023

Inhoudsopgave

Inleiding: uw verdediging versterken in tijden van mega-inbreuken

Het aantal geavanceerde cyberaanvallen blijft maar stijgen en een groot deel van die toename is te wijten aan aanvallen met inloggegevens. Volgens een recent rapport is het aantal aanvallen met e-mails op organisaties in de eerste helft van 2022 met 48% gestegen. In vergelijking met de zes maanden daarvoor waren meer dan twee derde van die aanvallen phishingpogingen om inloggegevens in handen te krijgen (een e-mail met een kwaadaardige koppeling om gevoelige accountgegevens te kunnen stelen). Bij deze aanvallen deden de criminelen zich voor als afkomstig van 265 verschillende merken.

Threat actors hebben geprofiteerd van de verschuiving naar remote werk door meer social engineering-tactieken zoals phishing toe te passen en door gebruik te maken van datalekken om accounts over te nemen. Multi-factor authenticatie (MFA) is daardoor nu een van de belangrijkste methoden geworden om te controleren of gebruikers ook zijn wie ze beweren te zijn. Met MFA kunnen organisaties de toegang tot al hun resources beschermen, inclusief het consumer/enterprise-web en mobiele apps, in een wereld waarin hybride en remote werken steeds normaler wordt. Overheden, regelgevende instanties en organisaties zien het cruciale belang in van een moderne Zero Trust-beveiligingsaanpak (vertrouw niets, controleer alles).

MFA is inmiddels een essentieel onderdeel geworden van een robuuste beveiligingsstrategie waarin identity een centrale plaats inneemt. Een voorbeeld: in januari 2022 werd in een uitvoeringsbesluit van het Office of Management and Budget van de Amerikaanse president phishingbestendige MFA als basisvereiste gesteld voor de modernisering van

cybersecurity voor alle federale instanties. Omdat overheden, organisaties en cybercriminelen zich doorlopend ontwikkelen, verandert ook de aard van MFA. Het gebruik van authenticatie zonder wachtwoorden neemt toe en devices (beheerde en onbeheerde) worden steeds belangrijker voor het evalueren van de beveiligingsstatus.

Deze handleiding geeft een overzicht van best practices om optimaal gebruik te maken van de mogelijkheden van MFA, inclusief passwordless authentication. We bespreken de resultaten van een enquête die we samen met IDG hebben uitgevoerd. Hieruit blijkt hoe belangrijk de rol is van identity en access management (IAM) in de moderne authenticatie en security, en wat de meest recente prioriteiten en adoptietrends van andere organisaties zijn. Met deze handleiding willen we organisaties ook graag inzicht geven in belangrijke zaken waarmee ze rekening moeten houden bij het ontwerpen van MFA-oplossingen, zoals:

- Phishingbestendige methoden implementeren
- Inzicht hebben in beleid en regelgeving
- Rekening houden met veranderende toegangsbehoeften

We sluiten af met praktisch advies voor mensen die MFA bouwen voor hun applicaties, op basis van de conclusies die we hebben kunnen trekken uit onze samenwerking met engineering- en productteams.

Implementeer phishing-bestendige MFA als onderdeel van een sterke IAM-strategie

De moderne bedreigingen op basis van identity kunnen verschillende vormen aannemen, zoals malware, hacking en phishing. Deze aanvallen kunnen downstream leiden tot diefstal van inloggegevens, accountinbreuken en exfiltratie van data. Om deze veelvoorkomende bedreigingen een halt toe te roepen, moeten organisaties hun beveiligingsstatus verhogen. De eerste verdedigingslinie daarbij is Identity. Organisaties die nog steeds vertrouwen op een legacy aanpak van Identity, zoals on-prem apps en firewalls, zijn bijzonder kwetsbaar voor geavanceerde aanvallen. Ze zijn dan voor de bescherming van hun organisatie en medewerkers afhankelijk van een traag, complex en gefragmenteerd framework.

Hierbij spelen verschillende factoren een rol: in de enquête die we samen met IDG hebben uitgevoerd, wijzen IT- en Security-managers op enkele specifieke problemen en statistieken met betrekking tot veilige authenticatie.

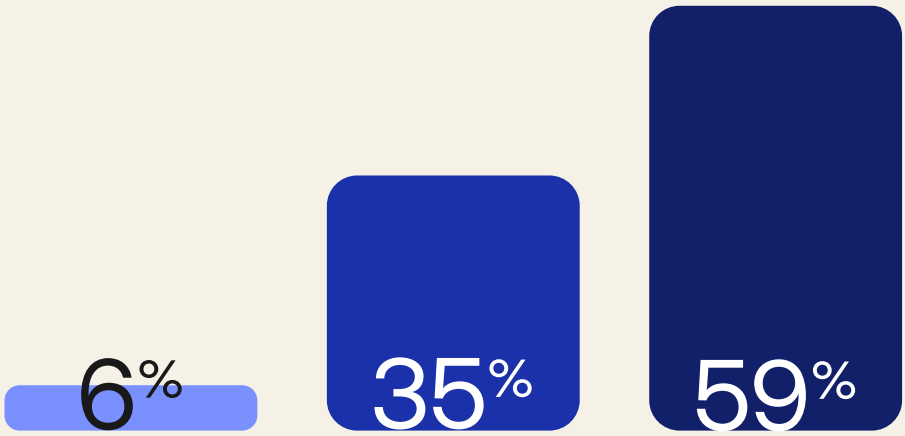
Belangrijkste problemen met wachtwoorden

Meer dan 1000 werknemers	**70%**
500-999 werknemers	**52%**

Inzicht: respondenten noemen meerdere problemen in verband met wachtwoorden, zoals gestolen inloggegevens en het gebruik van dezelfde wachtwoorden voor persoonlijke en werkaccounts.

MFA-niveaus waarvoor organisaties kiezen

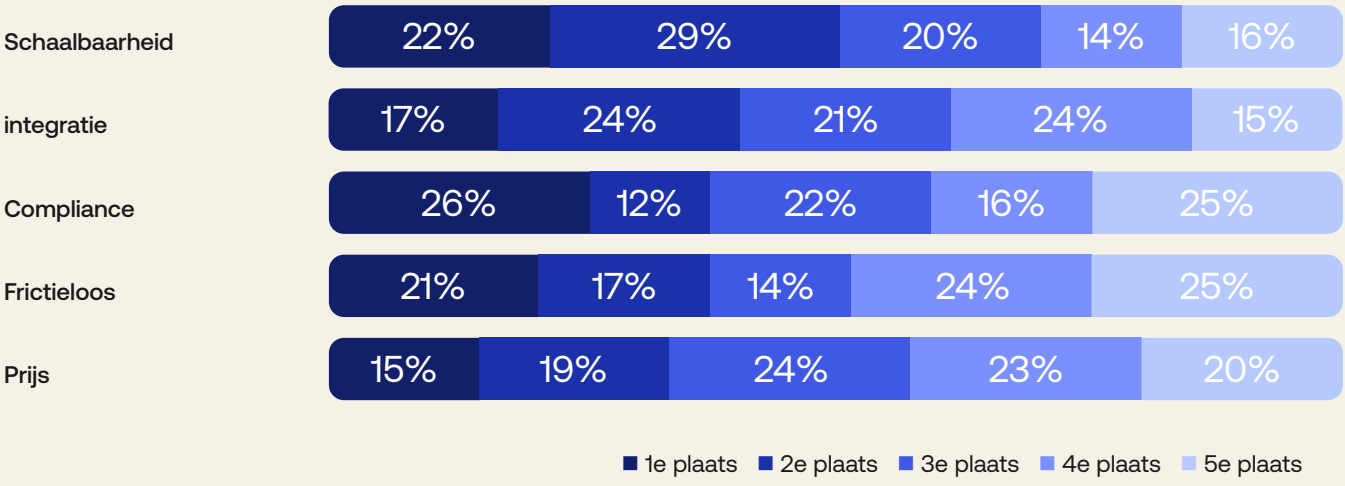
VP IT en hoger	**73%**
IT director/manager	**53%**



Inzicht: meer dan de helft (59%) zegt dat de strengste MFA-oplossing het meest geschikt is voor hun organisatie.

Belang van criteria bij het kiezen van een MFA-oplossing

De organisaties werd gevraagd alle vijf criteria te rangschikken van meest tot minst belangrijk.



Inzicht: 51% vindt schaalbaarheid een van de twee belangrijkste overwegingen bij het kiezen van een MFA-oplossing.

Overweeg het zekerheids-niveau van verschillende authenticatie-factoren

Over het algemeen wordt met authenticatie de identiteit gevalideerd met een van deze drie typen factoren:

- Iets dat u weet (een wachtwoord)
- Iets dat u hebt (een persoonlijke smartcard om uw identiteit te verifiëren)
- Iets dat u bent (een vingerafdruk)

Voor extra security worden bij MFA twee of meer typen factoren gebruikt. Er wordt meestal nog steeds een wachtwoord gebruikt, in combinatie met een tijdelijk token, een pushmelding naar een mobiele app of een biometrische factor. MFA kan echter op meerdere manieren worden toegepast. Elke methode heeft voor- en nadelen.

Er zijn verschillende typen authenticators beschikbaar die in sterkte variëren. Bij Okta hanteren we de volgende zekerheidsniveaus voor authenticators:

LAAG: wachtwoorden, beveiligingsvragen, eenmalige wachtwoorden (OTP's) via sms, spraak of e-mail, en OTP-apps zoals Authy en Google Authenticator

GEMIDDELD: mobiele pushmeldingen en OTP's met fysieke tokens

HOOG: PIV-smartcard (Personal Identity Verification) of CAC-smartcard (Common Access Card), FIDO 2.0 / WebAuthn + CTAP2

Het zekerheidsniveau is natuurlijk niet de enige overweging voor organisaties die hun MFA willen versterken. De authenticators moeten ook eenvoudig kunnen worden geïmplementeerd en gebruiksvriendelijk zijn voor het personeel en de klanten. Daarnaast moeten ze bestand zijn tegen specifieke typen bedreigingen, zoals MitM- (Man-in-the-Middle) of AitM- (Adversary-in-the-Middle) aanvallen. Er gaat echter niets boven het versterken van de security met de hoogste zekerheidsfactoren.

Het gebruik van sms als factor is bijvoorbeeld wel een snelle manier om MFA te introduceren voor gebruikers, maar het biedt niet het hoogste zekerheidsniveau. Veelvoorkomende securityproblemen, zoals sim-kaping en grootschalige smishing- en vishingaanvallen, ondermijnen het zekerheidsniveau dat sms-authenticatie kan bieden. Wij adviseren daarom met klem om sterkere MFA-factoren te gebruiken, zoals Okta Verify Push of biometrie (via WebAuthn of, voor overheidsinstellingen in de VS, PIV/CAC-smartcards.)

Best practices voor het ontwerp van sterke MFA

1. Bekijk (en heroverweeg) uw MFA-policies

Bekijk voordat u een MFA-oplossing implementeert met welke risico's en specifieke bedreigingen uw organisatie te maken heeft. Welke resources en aanvalsvectoren hebben voor u de hoogste prioriteit? In een goed doordachte, op risico's gebaseerde policyconfiguratie moet step-up authenticatie worden geactiveerd wanneer het risico echt hoog is.

Er kan bijvoorbeeld een policy worden gebruikt die bepaalt dat er om de acht uur een tweede factor vereist is wanneer er vanuit een bekend netwerk wordt ingelogd, of dat die tweede factor alleen nodig is wanneer er vanaf een nieuw device of een nieuwe geolocatie wordt ingelogd. Of misschien hebt u een bepaalde groep gebruikersaccounts met uitgebreide toegang tot gevoelige data en wilt u daarvoor een stringentere policy hanteren. Denk hierbij bijvoorbeeld aan developers binnen de organisatie die toegang hebben tot broncode of leidinggevenden met toegang tot gevoelige data. Voor deze accounts kunt u een sterker factortype vereisen of kunt u de gebruikers vragen om op extra MFA-prompts te reageren. U kunt zelfs overwegen om MFA te implementeren voor gevoelige acties binnen applicaties. Door fijnmazigere controles mogelijk te maken voor acties die bijzonder gevoelig zijn (zoals het goedkeuren van inkooporders of het overboeken van geld), verlaagt u niet alleen de risico's, maar kunt u ook soepel security implementeren die voldoet aan geldende compliancevereisten.

Elke extra verificatie moet zo transparant mogelijk en frictieloos zijn. De user experience moet goed zijn zonder dat dit ten koste gaat van de security.

2. Plan en zorg voor alternatieve toegangsmogelijkheden

Voor gebruikers die wel internettoegang hebben, maar weinig of geen bereik van hun service provider (bijvoorbeeld in een vliegtuig met wifi, een huis op het platteland of de kelder van een betonnen gebouw), werken spraak- of sms-oproepen niet altijd. In zulke gevallen is Okta Verify met push of een eenmalig wachtwoord (OTP) een betere keuze, omdat daarbij de communicatie op de internetverbinding van de telefoon versleuteld is. Hardwaredevices die event-gebaseerde of tijdgebaseerde eenmalige wachtwoorden (TOTP's) genereren, hebben helemaal geen communicatiekanaal nodig en het is lastig om ze te manipuleren of kopiëren. Fysieke devices zijn echter vaak duur en medewerkers kunnen ze thuis laten liggen of kwijtraken. Factortypen zijn daarom wellicht niet de beste optie voor tijdelijke medewerkers of mensen in functies met een groot verloop.

Organisaties moeten MFA-factoren kiezen die geschikt zijn voor de meest uiteenlopende scenario's. Er zijn maar weinig oplossingen die voor alle situaties geschikt zijn. Over het algemeen zorgen de volgende implementatietips voor zowel een verbeterde security als een uitstekende user experience:

- Geef gebruikers de keuze uit meerdere factoren, zodat ze altijd een back-up hebben. Als de ene authenticatiefactor bijvoorbeeld een wachtwoord is, kunt u daarnaast detectie van gelekte wachtwoorden gebruiken om gebruikers te waarschuwen en het gebruik van gelekte wachtwoorden blokkeren.
- Gebruik alleen sterke, phishingbestendige factortypen en schakel waar mogelijk over op passwordless MFA, of voor Amerikaanse overheidsinstellingen op PIV/CAC-smartcards.
- Controleer de oorsprong van de web-URL vóór de authenticatie. Inloggegevens moeten gekoppeld zijn aan het domein waar het toegangsverzoek vandaan komt.
- Laat gebruikers biometrie als tweede factor gebruiken als de hardware dit ondersteunt, bijvoorbeeld met Windows Hello en Touch ID. Dit maakt het voor de eindgebruiker gemakkelijker en het verhoogt de zekerheid dat gebruikers ook zijn wie ze zeggen te zijn.

3. Vereis voor gevoelige apps hogezekerheidsfactoren en phishing-bestendige authenticators als onderdeel van uw MFA-policies

Zoals eerder gezegd zijn niet alle authenticators phishingbestendig. Authenticators zijn niet allemaal in dezelfde mate bestand tegen social engineering. Ze brengen allemaal kosten en risico's met zich mee voor aanvallers die een account willen overnemen. OTP's op basis van sms kunnen bijvoorbeeld vrij makkelijk worden onderschept. Push-authenticators zijn door statische phishingcampagnes die gericht zijn op inloggegevens lastiger te kraken dan authenticators die OTP's gebruiken.

De combinatie van een pushbericht met de vraag aan de gebruiker om een getal op de inlogpagina te identificeren, biedt een betere beveiliging tegen verschillende aanvalstechnieken, waaronder aanvallen die gebruikmaken van MFA-moeheid. Authenticators op basis van hardware bieden de hoogste zekerheid.

Het US National Institute of Standards and Technology (NIST) biedt de meest betrouwbare definitie van phishingbestendigheid. Volgens het NIST vereist phishingbestendigheid dat het kanaal dat wordt geauthenticeerd, cryptografisch is gekoppeld aan de output van de authenticator. Dit betekent dat het domein (het adres) van de website waarbij u zich aanmeldt, gekoppeld moet zijn aan uw authenticator. Dit zorgt ervoor dat uw inloggegevens niet kunnen worden doorgegeven aan een phishingwebpagina.

Verschillende authenticators die beschikbaar zijn in het Okta-platform voldoen aan deze definitie. Okta ondersteunt roaming FIDO2 WebAuthn-authenticators (security keys) en deviceafhankelijke FIDO2 WebAuthn-authenticators (bijvoorbeeld Face ID, Touch ID of Windows Hello). Bovendien ondersteunen we het gebruik van authenticatie met PIV-smartcards binnen de inlogpolicies van een app om toegang te krijgen tot specifieke apps. Afhankelijk van uw implementatiemodel voldoet ook FastPass (de deviceafhankelijke passwordless authenticator van Okta) aan deze definitie. Het verplicht stellen van het gebruik van ten minste één phishingbestendige authenticator beschermt de organisatie tegen geavanceerde phishingaanvallen via social engineering- en AitM-aanvallen.

4. Wees zorgvuldig met compliancevereisten

De meeste IT-compliancenormen zoals PCI DSS, SOX en HIPAA schrijven krachtige controles voor gebruikersauthenticatie voor. Dit is voor organisaties vaak een van de hoofdredenen om MFA te implementeren. Als u aan dergelijke normen moet voldoen, is het belangrijk dat u precies weet wat de vereisten zijn, zodat u uw configuratie en policies daarop kunt afstemmen. Voor PCI- en HIPAA-compliance is bijvoorbeeld een sterke authenticatie vereist met ten minste twee van drie sterke authenticatiemethoden. SOX is minder gericht op technologie, maar om voor een audit te slagen, moet u wel kunnen bewijzen dat de financiële en boekhoudkundige gegevens van uw organisatie veilig zijn. Voor IT-compliance moet u de relevante normen implementeren en moet u kunnen bewijzen dat u aan de normen voldoet. Een zorgvuldige documentatie moet deel uitmaken van uw configuratie- en implementatieproces, zodat u snel bewijs kunt genereren als er een audit plaatsvindt. U zult uzelf daar later dankbaar voor zijn (net als uw organisatie).

5. Stem uw MFA af op de beveiliging van een steeds meer hybride werkend personeelsbestand

Remote en hybride werkende werknemers en externen hebben toegang nodig tot resources in de cloud. Een solide beveiliging is daarbij essentieel. De onboarding van nieuwe medewerkers moet bij voorkeur op kantoor gebeuren, waar de huidige medewerkers persoonlijk toegang hebben tot IT. Remote werken zorgt echter voor nieuwe uitdagingen bij het implementeren van en het oplossen van problemen met MFA.

Om de MFA-implementatie zo snel mogelijk te laten verlopen, kunt u het beste factoren toepassen waarmee gebruikers snel aan de slag kunnen (bijvoorbeeld ingebouwde biometrie in devices of mobiele apps zoals Okta Verify) en niet hoeven te wachten totdat ze een hard token ontvangen. Ze hebben dan snel toegang tot de resources die ze nodig hebben om aan het werk te gaan. Voor de onboarding van nieuwe medewerkers gebruiken sommige organisaties op dit moment virtuele onboardingsessies. Ze sturen dan instructies naar het persoonlijke e-mailadres van de medewerkers, zodat ze alvast informatie kunnen overdragen voordat de nieuwe medewerkers toegang hebben tot hun zakelijke e-mail.

6. Maak een plan voor verloren devices

Organisaties die BYOD (Bring Your Own Device) toestaan, zien dat medewerkers steeds vaker persoonlijke devices gebruiken om toegang te krijgen tot assets van de organisatie. Deze onbeheerde devices brengen echter verschillende securityrisico's met zich mee. Veel organisaties met BYOD-policies hebben te maken met datalekken via devices van medewerkers. De beveiliging van deze open dreigingsvector moet dus een hoge prioriteit krijgen.

Met device assurance policies kunt u als onderdeel van uw authenticatie op meerdere securitygerelateerde attributen controleren, bijvoorbeeld op de versie van het besturingssysteem, schijf-encryptie en jailbreak/root-detectie. Device assurance policies zorgen voor een extra beveiligingslaag bovenop de regels van de authenticatiepolicies om de beveiligingsstatus van het gebruikte device te valideren.

Waar ook rekening mee moet worden gehouden, is het feit dat medewerkers vaak data van de organisatie op hun eigen desktop/laptop downloaden. Het is dan belangrijk om te kunnen afdwingen dat gebruikers na het invoeren van een wachtwoord op een MFA-vraag moeten reageren om hun computer te ontgrendelen. In de meeste compliancerichtlijnen is MFA vereist. De mogelijkheid om dit op computerniveau te kunnen toepassen, voorkomt desktopgerelateerde aanvallen en beschermt data wanneer een laptop kwijtraakt of gestolen wordt.

Alles wat gebruikers hebben, kunnen ze echter ook kwijtraken. Daarom is het belangrijk dat uw draaiboek voor de IT-helpdesk een procedure bevat voor hoe te handelen als iemand een device verliest. Zorg ervoor dat er voor alle devices die voor MFA worden gebruikt, de volgende stappen worden uitgevoerd als het device als verloren wordt gemeld:

- Alle actieve sessies afsluiten en de gebruiker vragen zich opnieuw te authenticeren
- Het device loskoppelen van het account en de toegangsrechten van de gebruiker
- Informatie van de organisatie op mobiele devices op afstand wissen (gebeurt meestal op devices die eigendom zijn van de organisatie)

Het is ook belangrijk de activiteiten van het account van de gebruiker te controleren tot aan het moment waarop het device verloren raakte om vast te stellen of er ongebruikelijke activiteiten hebben plaatsgevonden. Houd rekening met de mogelijkheid van een beveiligingslek en zorg voor de juiste escalatie als er iets verdachts wordt gevonden. Zodra de acute securityproblemen zijn aangepakt, moet de werknemer zo snel mogelijk weer aan het werk kunnen met een vervangend device of tijdelijke inlogmethode. De werknemer kan bijvoorbeeld gewoon weer aan de slag nadat zijn/haar identiteit is gecontroleerd via een gesprek met de IT-helpdesk, terwijl u intussen vervangende factoren implementeert.

7. Overweeg adaptieve MFA te gebruiken

Step-up MFA biedt ruimte voor fijnmazige controle op hoe en wanneer MFA wordt toegepast, maar er moet wel goed worden gekeken naar de configuratie ervan. Zelfs bij policies en criteria die zorgvuldig zijn gedefinieerd, wilt u soms in staat zijn om gaandeweg toegangsbeslissingen te nemen op basis van wijzigingen met betrekking tot gebruikers of devices.

Adaptieve MFA stelt toegangspatronen vast en past vervolgens de policy rondom iedere gebruiker of groep aan. Zo is er bijvoorbeeld voor een werknemer die geregeld op reis is en e-mails vanuit het buitenland stuurt, misschien alleen op bepaalde tijden een tweede authenticatiefactor nodig, terwijl werknemers die nooit elders werken, onmiddellijk een MFA-vraag krijgen als ze dat opeens wel doen. Op risico gebaseerde policies, zoals het sturen van een vraag voor step-up authenticatie bij een toegangspoging tot resources via een niet-geautoriseerde proxy of het automatisch blokkeren van toegang vanaf bekende schadelijke IP-adressen, kunnen ook worden geactiveerd in geval van verdachte gebeurtenissen. Adaptieve MFA is een krachtig hulpmiddel om dynamische policies automatisch in de loop van de tijd aan te passen. Het gaat daarbij om policies die stringent genoeg zijn om alle bescherming te bieden die uw organisatie nodig heeft, maar ook flexibel genoeg om de gebruikers als individuele personen te behandelen.

8. Voer de implementatie gefaseerd uit

Complexe implementaties en policies werken meestal niet meteen helemaal goed. Wanneer een proceswijziging van invloed is op alle medewerkers, moet u tijdens de implementatie de effectiviteit ervan altijd volgen en erop voorbereid zijn om policies zo nodig af te stemmen op basis van wat u ziet. Voer uw implementatie in fasen uit en laat IT/Security als eerste beginnen met het gebruik van MFA. Van daaruit kunt u verder gaan met verschillende gebruikersgroepen. Als u al vroeg in het proces vertrouwd raakt met de auditfunctionaliteit, hebt u daar veel profijt van bij het oplossen van problemen met en het aanpassen van de policyconfiguratie in de toekomst.

Nadat u MFA bijvoorbeeld hebt geïmplementeerd voor een specifieke groep gebruikers, kunt u de audittools gebruiken om de adoptie en het gebruik te controleren. Probeer een mechanisme voor feedback van gebruikers te implementeren. Gebruikers zullen niet altijd de tijd nemen om schriftelijk feedback te geven. Een audit trail geeft dan enig inzicht in wat ze feitelijk hebben ervaren. Kostte het drie pogingen om hun OTP in te voeren? Gaven ze het op? Zulke problemen kunnen duiden op een verkeerde configuratie, een hiaat in de voorlichting aan de gebruikers of simpelweg een scenario waarmee geen rekening is gehouden in het aanvankelijke plan. Door gebruik te maken van audittools en gebruikers te stimuleren feedback te geven, kunnen alle belanghebbenden ervan op aan dat het systeem naar behoren werkt en dat nieuwe securitypolicies zijn geadopteerd.

9. Licht gebruikers voor

Het gebruik van MFA om de risico's te beperken die verbonden zijn aan toegang met alleen een wachtwoord, is cruciaal in de huidige digitale wereld. Sommige gebruikers vinden het echter lastig en zijn bang dat het ze extra tijd kost naast hun toch al drukke werkzaamheden. Het is van essentieel belang dat iedereen, van het management tot IT-teams en van securityteams tot eindgebruikers, begrijpt waarom u overstapt op MFA. De hele organisatie moet erachter staan en iedereen moet zijn/haar eigen rol in de beveiliging van de organisatie begrijpen en accepteren. Voorlichting helpt gebruikers in te zien welke voordelen deze extra stap biedt voor de security.

Vaak stuurt de IT-afdeling e-mails waarin de aanstaande wijzigingen worden aangekondigd. Er kunnen ook phishingoefeningen binnen de organisatie worden uitgevoerd om te laten zien hoe zelfs de meest ervaren medewerkers kunnen worden misleid om hun inloggegevens prijs te geven. Zorg dat medewerkers de beschikking krijgen over screenshots, veelgestelde vragen en contactgegevens, zodat ze gemakkelijk om hulp kunnen vragen.

Begrijp en beheer de kwetsbaarheid van uw accountherstel-procedure

De veiligheid van multi-factor authenticatie staat of valt met de gebruikte procedure voor accountherstel. In recente zaken die uitgebreid in het nieuws zijn geweest, maakten aanvallers misbruik van zwakke plekken in het proces voor accountherstel om de controle te krijgen over een account.

Laten we eens kijken hoe dit zou kunnen gebeuren bij een organisatie met de naam Acme. De webapplicatie van Acme biedt MFA op basis van een soft token app die is geïnstalleerd op de telefoon van een gebruiker. De gebruiker kan een telefoonnummer registreren om een alternatieve secundaire factor voor accountherstel te ontvangen voor het geval de gebruiker geen toegang heeft tot het soft token. Hoe sterk de secundaire factor van Acme is, hangt nu af van de sterkte van de processen van de telecomprovider voor de authenticatie van de klant en het doorsturen van oproepen of sms-berichten. Lukt het een aanvaller om zich voor te doen als de gebruiker en een medewerker van de klantenservice te overtuigen of onder druk te zetten om oproepen of sms-berichten door te sturen naar een nummer van de aanvaller?

Voor elke secundaire factor is een betrouwbaar alternatief nodig. Daarom moeten organisaties veilige herstelprocessen ontwerpen. Welke aanpak het beste is, hangt af van de situatie, maar er zijn wel enkele best practices:

Houd het herstel van de primaire en secundaire factor onafhankelijk van elkaar.

Het is belangrijk om het herstel van de secundaire factor te scheiden van het herstel van de primaire factor. Als een aanvaller toegang krijgt tot de primaire authenticatiefactor, is de secundaire factor niet meer betrouwbaar wanneer deze opnieuw kan worden ingesteld met het uitgelekte wachtwoord. De herstelprocedure voor de secundaire factor moet volledig losstaan van de herstelprocedure voor het wachtwoord. Als de herstelprocedure bijvoorbeeld een e-mail is, moet de secundaire factor via een ander kanaal worden hersteld.

Betrek er een admin bij.

Een admin kan in uiteenlopende scenario's een geavanceerde authenticatie-methode met hoge zekerheid implementeren. Voor grote ondernemingen is het relatief eenvoudig om leden van de organisatie te authenticeren met gedeelde geheimen die zijn afgeleid van het werk of het profiel van de medewerker, de organisatie en relaties tussen mensen. Het is bijvoorbeeld mogelijk om de manager van een medewerker te vragen de gebruiker te authenticeren en vervolgens IT toestemming te geven om de MFA opnieuw in te stellen.

Als het om consumenten gaat, kan een admin een gebruiker vragen stellen op basis van een uitgebreide set gedeelde geheimen. Bankapplicaties voor consumenten verzamelen bij de onboarding bijvoorbeeld veel persoonlijke gegevens, die als gedeelde geheimen kunnen worden gebruikt om het account te herstellen. Ook recente gebeurtenissen in de geschiedenis van de gebruiker met de applicatie of de organisatie kunnen bruikbare gedeelde geheimen zijn. De evaluatie van een set gedeelde geheimen kan via web of spraak worden geautomatiseerd. Vaak biedt dit een hogere zekerheid dan een mens, omdat social engineering hier minder grip op heeft.

Zorg voor een alternatief voor de secundaire factor.

Veel scenario's vereisen een geautomatiseerde methode voor het herstel van de tweede factor (bijvoorbeeld producten met een groot aantal gebruikers waarbij een-op-een-support te duur is of wanneer de operationele kosten moeten worden verlaagd). Wanneer de gebruiker al bij de onboarding wordt ingeschreven bij meer dan één tweede factor, kan die gebruiker een tweede factor herstellen door de authenticatie te doorlopen via een alternatieve tweede factor. Een eenvoudig en goedkoop voorbeeld is gebruikers een (fysieke of afdrukbare) kaart te geven met een set codes die maar één keer kunnen worden gebruikt als alternatief voor de tweede factor.

Bescherm inlog-procedures tegen brute force- en credential stuffing-aanvallen

De beschikbaarheid van goedkope computerresources neemt toe. Hierdoor worden authenticatiesystemen ook steeds kwetsbaarder voor brute force-aanvallen. Er zijn echter een paar eenvoudige technieken waarmee de security van uw MFA aanzienlijk kan worden verbeterd wanneer een wachtwoord is uitgelekt.

Analyseer logboeken en waarschuwingen.

Verzamel en analyseer mislukte pogingen om toegang te krijgen met een secundaire factor. Als er verschillende mislukte inlogpogingen zijn gedaan met een tweede factor, stuurt u de gebruiker of een admin een waarschuwing over dit verdachte gedrag en vraagt u de gebruiker om een nieuw token te gebruiken.

Gebruik een out-of-band token.

Een tweede factor die wordt geverifieerd via een kanaal dat losstaat van de primaire factor, biedt extra bescherming tegen brute-force-aanvallen en phishing. Stel, een populaire nieuwe factor stuurt de gebruiker een pushmelding op een mobiele telefoon met informatie over het authenticatieverzoek en een prompt om het verzoek te accepteren of te weigeren. Dit kanaal is niet toegankelijk voor een traditionele brute-force-aanval.

Neem het beheer van risico's, bruikbaarheid en kosten op in het ontwerp

Het ontwerp van een MFA-voorziening heeft een grote impact op de security, bruikbaarheid en kosten, in elke context. Een tweede factor met hogere zekerheid kan in sommige gevallen als een onnodige extra belasting voelen voor eindgebruikers en admins. Dit kan dan weer gevolgen hebben voor de adoptie van MFA voor uw product, wat ten koste gaat van de security. Hier zijn enkele best practices om de risico's, bruikbaarheid en kosten in evenwicht te houden:

Bied uiteenlopende opties die geschikt zijn voor gevarieerde gebruikerspopulaties.

Bij verschillende gebruikerspopulaties horen ook verschillende risiconiveaus, en dus ook verschillende zekerheidsniveaus. Een admin heeft bijvoorbeeld een groter toegangsbereik dan een individuele gebruiker. Het kan dan nuttig zijn om voor admins een sterkere tweede factor te gebruiken, terwijl de rest van het personeel een meer gebruiksvriendelijke optie krijgt. Bij consumenten zullen verschillende gebruikers ook verschillende voorkeuren hebben als het gaat om de verhouding tussen security en bruikbaarheid voor hun account. Als een bekendere optie met een lagere zekerheid, zoals sms, wordt gebruikt, kan dit meer security bieden dan een optie met hogere zekerheid die niet algemeen is geadopteerd.

Ondersteun federatieve identities en authenticatie.

Federatieve identity, ook wel federatieve single sign-on (SSO) genoemd, is een methode om de identiteit van een gebruiker in meerdere identity management-systemen te koppelen. Gebruikers kunnen dan snel tussen systemen schakelen terwijl de security behouden blijft. Veel grote organisaties implementeren authenticatie en MFA lokaal voor identities die ze beheren, met federation voor resources. Productontwikkelingsteams kunnen het beheer van policy- en securityprocessen dan uitbesteden aan klanten en partners. Wanneer deze gebruikers MFA onafhankelijk kunnen implementeren, kunnen ze de hier genoemde overwegingen optimaliseren op basis van hun specifieke omstandigheden en beperkingen. Een partner kan bijvoorbeeld het beheer van accountherstel zo ontwerpen dat het aansluit bij hun specifieke IT-functie. Een extra voordeel van deze vorm van uitbesteding is dat gebruikers met één token toegang hebben tot alle resources.

Hoe Okta het spel verandert

Okta's moderne benadering van identity management is bij uitstek geschikt om organisaties te helpen identity management, inclusief MFA, zelf te regelen om datalekken en andere risico's terug te dringen. Okta helpt u het volgende te doen:

Snel MFA toepassen voor uw personeel en klanten.

- MFA snel en eenvoudig implementeren, met meer dan 7000 kant-en-klare verbindingen op het Okta-applicatienetwerk.
- De dekking uitbreiden naar on-prem applicaties met support voor RADIUS, RDP, ADFS en LDAP, evenals op headers gebaseerde authenticatie en Kerberos via Okta Access Gateway
- Intelligente, contextafhankelijke toegangsbeslissingen nemen op basis van device- en verbindingsattributen
- Minder afhankelijk worden van wachtwoorden met single sign-on en passwordless authenticatie

Identity met vertrouwen centraal stellen.

- Accountbeheer minder complex maken
- Uniforme toegang bieden voor gebruikers om wachtwoorden overbodig te maken en tegelijkertijd een positieve experience te bieden
- Risico's verkleinen en wildgroei aan identiteiten terugdringen door de toegang tot services te beperken via intelligente SAML-verbindingen

De aanvalsmogelijkheden beperken en snel reageren op gelekte inloggegevens.

- Provisioning en deprovisioning automatiseren om consistente onboarding te versnellen en orphan accounts uit te schakelen
- Security-policies uitbreiden naar maatwerkapplicaties via SCIM, SDK's en de uitgebreide API's van Okta
- Zorgen dat de juiste applicaties op het juiste moment het juiste toegangsniveau krijgen met workflows voor toegangsverzoeken en volledig identity lifecycle management

Bekijk deze demo om te zien hoe eenvoudig het is om de oplossing van Okta voor adaptieve multi-factor authenticatie te beheren en het authenticatieproces uit te voeren.

Meer informatie over de Adaptive MFA-oplossingen van Okta vindt u op https://www.okta.com/nl/products/adaptive-multi-factor-authentication/

Conclusie: een routekaart voor geslaagde MFA

Multi-factor authenticatie is voor applicatiedevelopers over de hele wereld een best practice geworden om de toegang tot hun applicaties te beveiligen. U moet achter de schermen echter heel wat werk verzetten om optimaal te profiteren van de kracht van MFA-security zonder het werk van uw personeel te verstoren. Best practices zijn onder andere het analyseren van de herstelprocedure voor de tweede factor, systemen zo ontwerpen dat ze bestand zijn tegen brute force-aanvallen en het juiste evenwicht zien te vinden tussen security, bruikbaarheid en kosten.

Een moderne, geautomatiseerde aanpak van MFA kan organisaties helpen de toegang te controleren, herstel op een veilige manier te automatiseren en het risico op datalekken drastisch te verkleinen.

Whitepaper

Implementatie-handleiding voor multi-factor authenticatie

okta

Okta Inc.
Strawinskylaan 4117, 3rd Floor
1077 ZX Amsterdam The Netherlands
info@okta.com
+31 (20) 888 1388