IDC PlanScape

IDC PlanScape: Meervoudige Verificatie Implementeren

Mike Chapple

IDC PLANSCAPE-AFBEELDING

AFBEELDING 1

IDC PlanScape: Meervoudige verificatie implementeren

Bron: IDC, 2017

May 2017, IDC #US42539517

SAMENVATTING

Meervoudige verificatie biedt organisaties effectieve beveiliging die de zwakheden van verificatie op basis van kennis overwint en het netwerk, toepassingen en gegevens beschermt tegen steeds geavanceerdere bedreigingen. Door wachtwoorden met fysieke apparaten en/of biometrische metingen te combineren, voegen organisaties een extra laag sterke beveiliging toe en beschermen ze zichzelf tegen wachtwoorddiefstal.

De recente vooruitgang in meervoudige verificatie maakt deze technologie toegankelijker voor niet-technische eindgebruikers en dit maakt wijdverspreide implementatie door de organisatie heen mogelijk. Het gebruik van meervoudige verificatie kan nu zo eenvoudig zijn als een druk op een knop in een pop-upmelding die verschijnt op de smartphone die de gebruiker toch al bij zich had. De eenvoud van deze aanpak verbetert de veiligheid en verhoogt de tevredenheid van de gebruiker.

Het is verstandig voor organisaties die meervoudige verificatie willen implementeren een gefaseerde aanpak te overwegen voor gebruikers en diensten. Hierbij krijgen de gebruikers en toepassingen met een hoger risico voorrang om zo vroeg mogelijk in de implementatie zoveel mogelijk voordeel te behalen. Regelmatige communicatie met zowel management als eindgebruikers verhoogt de kans op een soepele implementatie.

Deze IDC-studie biedt senior technologieleiders een veelzijdige benadering van meervoudige verificatie.

"Meervoudige verificatie is een beproefde aanpak die eindelijk volwassen aan het worden is," zegt Mike Chapple, adjunct-analist in IDC's IT Executive Programma's (IEP). "Organisaties zien dat zij geconfronteerd worden met een groeinde dreiging van de compromittering van op wachtwoorden gebaseerde aanmeldingsgegevens. Op kennis gebaseerde verificatie biedt simpelweg niet voldoende bescherming tegen deze bedreigingen. Push-gebaseerde verificatie met smartphones is zowel eenvoudig voor eindgebruikers als kosteneffectief voor de organisatie."

WAAROM IS MEERVOUDIGE VERIFICATIE BELANGRIJK?

Organisaties die uitsluitend wachtwoorden gebruiken als verificatie lopen een groot risico in de huidige bedreigingsomgeving voor cybersecurity. Wachtwoorden zijn nog steeds een nuttig onderdeel van het beveiligingsprogramma van de organisatie, maar als middel om de identiteit van een gebruiker te bewijzen, vallen ze nu in de categorie 'noodzakelijk, maar niet voldoende'. Meervoudige-verificatiemethoden, lang het domein van geheime overheidsinstanties, financiële instellingen en andere organisaties met een aan paranoia grenzende houding ten aanzien van, zijn nu een cruciaal onderdeel van zelfs de meest routinematige technologische diensten.

Gegevens verzameld aan de hand van recente beveiligingsincidenten bevestigen deze stelling. In het "2017 Data Breach Investigations Report" onderzocht Verizon de details van duizenden beveiligingsincidenten die in 2016 plaatsvonden. "Bij 81% van de bevestigde gegevensinbreuken was er sprake van zwakke, standaard- of gestolen wachtwoorden." Dit onderstreept het feit dat wachtwoordverificatie niet langer kan volstaan voor belangrijkere diensten. Er is een grote kans dat elke dienst die op grote schaal actief is en afhankelijk is van wachtwoordverificatie al is gecompromitteerd door vijanden als deze dienst informatie of bronnen van enige waarde biedt.

Wat is er mis met wachtwoorden?

Het onderliggende probleem met wachtwoordverificatie ligt in het feit dat wachtwoorden simpelweg statische informatie zijn die gemakkelijk kunnen worden gestolen en door iemand anders dan de rechtmatige eigenaar kan worden gebruikt vanaf iedere plek waar toegang tot de toepassing is, wat vaak over de hele wereld is. Of de informatie nu van individuele gebruikers via social engineering komt of en masse van een gecompromitteerde website wordt gestolen, aanvallers kunnen wachtwoorden stelen zonder dat de eindgebruiker dit merkt en deze wachtwoorden vervolgens gebruiken om de identiteit van de gebruiker aan te nemen.

De onveiligheid van wachtwoordverificatie wordt versterkt door het feit dat gebruikers een intense afkeer van wachtwoorden hebben, omdat het lastig is ingewikkelde wachtwoorden te onthouden. Hierdoor gebruiken ze bij verschillende bedrijven en persoonlijke websites hetzelfde ingewikkelde wachtwoord. Aanvallers kennen dit gedrag en zullen regelmatig wachtwoorden stelen van minder goed beveiligde websites, zoals een nieuws- of sportwebsite en deze wachtwoorden gebruiken om te proberen in te loggen op gevoelige websites, zoals een bank of zakelijke VPN. Een inbreuk op Adobe's website in 2013 resulteerde bijvoorbeeld in de publicatie van meer dan 130 miljoen wachtwoorden op het internet. Een aanvaller die ABC Corporation in problemen wilde brengen, hoefde alleen maar in deze lijst te zoeken naar een account dat eindigt op @abc.com en vervolgens te proberen die gegevens te hergebruiken om in te loggen op een ABC-website. Met deze aanpak is de kans vrij groot dat de aanvaller een enkel hergebruikt wachtwoord vindt. In een enquête uit februari 2017 onder smartphonegebruikers ontdekte Keeper Security dat meer dan 80% wachtwoorden opnieuw gebruikt.

Meervoudige verificatie bouwt voort op wachtwoorden

Meervoudige verificatie biedt bedrijven de mogelijkheid om wachtwoorden aan te vullen met andere verificatietechnieken die niet afhankelijk zijn van geheime kennis van de gebruiker, die kan worden gestolen en hergebruikt. Deze technieken zijn niet nieuw. Beveiligingsprofessionals bedachten de term *multifactor* een aantal decennia geleden en hebben deze aanpak sindsdien selectief geïmplementeerd in zeer gevoelige applicaties, zoals de beveiliging tegen externe toegang tot datacenternetwerken. Drastische veranderingen in de cybersecurity-bedreigingsomgeving, waaronder de opkomst van geavanceerde persistente bedreigingen (APT's) en de publicatie van gegevens van grootschalige diefstallen van wachtwoorden, leiden organisaties er nu echter toe om meervoudige verificatie op een grotere schaal te implementeren.

Regelgeving stimuleert vaak implementatie

Sommige organisaties gebruiken meervoudige-verificatiemethoden als gevolg van externe regelgeving:

- De *Payment Card Industry Data Security Standard (PCI DSS)* vereist expliciet het gebruik van meervoudige verificatie voor administratieve toegang tot systemen en netwerken die creditcardgegevens opslaan, verwerken of verzenden.
- De *Federal Financial Institutions Examination Council (FFIEC)* maakt meervoudige verificatie niet verplicht, maar heeft banken en andere financiële instellingen een richtlijn gegeven die stelt dat de FFIEC leden "enkelvoudige verificatie als enige controlemechanisme als ontoereikend zien voor riskante transacties waarbij toegang nodig is tot klantinformatie of bedragen naar andere partijen worden overgemaakt."

- De regels van de federale overheid vereisen het gebruik van meervoudige verificatie om externe toegang tot *gevoelige overheidssystemen* te beveiligen.

Naast deze formele eisen verwachten veel auditoren dat organisaties het gebruik van meervoudige verificatie zullen overwegen in hun risicobeoordelingen en bij het ontwerp van beveiligingscontroles.

Meningen van gebruikers over meervoudige verificatie veranderen

Gebruikers staan nu zeer open voor meervoudige verificatie, wat is toe te schrijven aan verschillende factoren:

- Populaire consumentendiensten, zoals Google, Twitter, Facebook en LinkedIn, ondersteunen meervoudige verificatie, en verhogen hiermee het gebruikersbewustzijn en acceptatie van deze technologie.
- Media-aandacht voor datalekken en door de staat gesponsorde aanvallen op grote bedrijven verhoogt de bewustwording onder gebruikers van bedreigingen.
- Het wijdverspreide gebruik van smartphones voor meervoudige verificatie en hun constante beschikbaarheid voor gebruikers elimineren de noodzaak voor gebruikers om aparte hardware-apparaten bij zich te dragen die vaak worden vergeten, kwijtgeraakt of gestolen.

Het implementeren van meervoudige-verificatietechnologieën vermindert het beveiligingsrisico van een organisatie en maakt het mogelijk om in een steeds vijandelijkere bedreigingsomgeving actief te blijven.

WAT IS MEERVOUDIGE VERIFICATIE?

Meervoudige verificatie vereist het gelijktijdig gebruik van verificatietechnologieën van twee of meer afzonderlijke controlecategorieën om de identiteit van een gebruiker te controleren. De drie categorieën verificatiefactoren omvatten:

- **Verificatie op basis van kennis.** Deze technieken passen in de categorie 'iets dat u weet' en gaan ervan uit dat de gebruiker geheime informatie heeft. Het meestvoorkomende voorbeeld van verificatie op basis van kennis is een wachtwoord, maar deze variant heeft ook beveiligingsvragen, pincodes en soortgelijke technieken.
- **Verificatie op basis van bezit.** Deze technieken passen in de categorie 'iets dat u hebt'. De gebruiker moet hier een fysiek object voor hebben. In het verleden hebben beveiligingsteams gebruikgemaakt van verificatie op basis van bezit aan de hand van hardwaretokens die gebruikers aan hun sleutelhanger konden vastmaken. Dit is nu vervangen door verificatie op basis van smartphone of smartcard.
- **Biometrische verificatie.** Deze technieken passen in de categorie 'iets dat u bent' en meten een fysieke eigenschap van de gebruiker. Biometrische verificatietechnieken zijn onder andere vingerafdrukscanners, gezichtsherkenning, spraakherkenning en iris-/netvliesscanners.

Meervoudige verificatie vereist het gebruik van twee of meer verificatietechnieken die ten minste twee *verschillende verificatiecategorieën* vertegenwoordigen. Zo kan een organisatie bijvoorbeeld verificatie op basis van kennis combineren met verificatie op basis van bezit door gebruikers te vragen een wachtwoord in te voeren en vervolgens hun login te bevestigen met hun geregistreerde smartphone. Op dezelfde manier kan een systeem zowel om een vingerafdruk (biometrische verificatie) als een wachtwoord (op kennis gebaseerde verificatie) vragen. Voor een gedetailleerde beschrijving van

verificatiefactoren, zie *IDC TechScape: Worldwide Advanced Authentication* (IDC #US42418917, april 2017).

Wat is geen meervoudige verificatie?

Organisaties die op zoek zijn naar een snelle manier om aan regelgeving of contractuele vereisten voor meervoudige verificatie te voldoen, overwegen vaak om twee kennisgebaseerde verificatietechnieken te gebruiken tijdens hun inlogproces. Veel websites vragen gebruikers bijvoorbeeld niet alleen hun identiteit te bevestigen met een wachtwoord, maar ook om beveiligingsvragen te beantwoorden die op basis van informatie op hun kredietrapport verschijnt. Terwijl dit marginale veiligheidsvoordelen kan opleveren, is het niet zo veilig als een meervoudige-verificatiemethode. Het probleem met deze benadering is dat een aanvaller die toegang krijgt tot het wachtwoord van een gebruiker door middel van een social-engineeringaanval of andere middelen waarschijnlijk ook de antwoorden op beveiligingsvragen kan verkrijgen met soortgelijke technieken.

Toen de FFIEC voor het eerst financiële instellingen aanbeval om meervoudige verificatie te implementeren, reageerden veel banken door beveiligingsvragen aan hun inlogproces toe te voegen. De FFIEC reageerde hierop met een FAQ die hun standpunt verduidelijkte:

> Per definitie vereist echte meervoudige verificatie dat er factoren uit twee of meer van de drie categorieën worden gebruikt. Het gebruik van meerdere oplossingen uit dezelfde categorie op verschillende punten in het proces kan deel uitmaken van een gelaagde beveiliging of een andere aanpak op basis van compenserende controle, maar er is geen sprake van meervoudige verificatie.

Organisaties die meervoudige verificatie willen implementeren, moeten de verificatiefactoren die zij overwegen zorgvuldig tegen het licht houden om er zeker van te zijn dat zij daadwerkelijk factoren uit verschillende categorieën implementeren, en daarmee verschillende risicoprofielen.

Smartphones spelen een cruciale rol bij meervoudige verificatie

Het wijdverbreide gebruik van smartphones is een van de belangrijkste drijfveren voor de gebruikersacceptatie van meervoudige-verificatietechnologieën. Enkele voordelen van het gebruik van smartphones als tweede factor zijn:

- Gebruikers hebben smartphones altijd bij zich en ze hebben dus altijd toegang tot het apparaat als ze zich moeten verifiëren.
- Bedrijven kunnen vaak vertrouwen op het persoonlijk bezit van smartphones als een tweede verificatiefactor voor de overgrote meerderheid van hun gebruikers. Hiermee worden de kosten van het aanschaffen van speciale hardwaretokens en het beheer van deze apparaten vermeden. Dit vermindert de totale eigendomskosten van meervoudige-verificatieoplossingen.
- Gebruikers zijn vertrouwd met het verificatieproces via hun telefoon met pincodes en/of biometrische verificatie.

Het eerste gebruik van smartphone-apps als meervoudige-verificatieapparaten vertrouwde op het gebruik van pincodes, zoals in de Google Authenticator-app, weergegeven in afbeelding 2. In een doorsneeproces met meervoudige verificatie met deze aanpak zouden gebruikers:

- Toegang krijgen tot de toepassing waarbij ze inloggen met een gebruikersnaam en wachtwoord waarmee de verificatie op basis van kennis wordt voltooid.

- Een eenmalig wachtwoord ingeven op basis van de app op hun smartphone. Deze code kan op verzoek worden gegenereerd of periodiek worden veranderd. Als de gebruiker de juiste code geeft op basis van tijd en toegangsvolgorde, dan bewijst dit het bezit van het apparaat en voltooit het de tweede verificatiefactor.

AFBEELDING 2

Smartphonegebaseerde wachtwoordverificatie

Bron: Google, 2017

Een pincode als meervoudige verificatie is omslachtig voor gebruikers die het snel zat zijn dat ze de verificatie-app moeten openen en naast hun wachtwoord ook een toegangscode moeten invoeren. Onlangs begonnen leveranciers van meervoudige verificatie nieuwe pushverificaties te verkopen die net iets anders werken:

- De gebruiker verstrekt een gebruikersnaam en wachtwoord op dezelfde manier als bij andere technieken.
- Het verificatiesysteem verzendt vervolgens automatisch een pushmelding naar de geregistreerde smartphone van de gebruiker waarin wordt gevraagd om de login goed te keuren. Een voorbeeld van deze melding van Duo Security wordt weergegeven in afbeelding 3.
- De gebruiker klikt op een enkele knop om het inlogverzoek goed te keuren.

AFBEELDING 3

Pushverificaties op smartphones

Bron: Duo Security, 2017

Pushverificaties bereiken dezelfde veiligheidsdoelstellingen als pincodes, maar op een manier die waarschijnlijk sneller wordt geaccepteerd door eindgebruikers.

WIE ZIJN DE BELANGRIJKSTE BELANGHEBBENDEN?

Voor een succesvolle implementatie van meervoudige verificatie is er een partnerschap tussen hoger management, technologen, lijnmanagers en eindgebruikers nodig. Individuen in deze rollen spelen een belangrijke rol in het uitbrengen van meervoudige-verificatietechnologieën (zie tabel 1).

TABEL 1

Belangrijkste belanghebbenden

Rol	Verantwoordelijkheid
Hoger management	Laat steun zien voor het initiatief van meervoudige verificatie, bij voorkeur door voorop te lopen in het gebruik en een pleitbezorger voor de technologieën te worden.
Chief Information Officer (CIO)	Bied de financële en personele middelen die nodig zijn om de implementatie te ondersteunen. Dien als belangrijkste contactpersoon voor andere senior executives met vragen of problemen.
Chief Information Security Officer (CISO)	Leid het implementatie-initiatief voor meervoudige verificatie, coördineer middelen binnen de IT-organisatie en zorg ervoor dat beveiligingsdoelstellingen tijdens de implementatie worden bereikt.
Lijnmanagers	Steun het initiatief tijdens gesprekken met eindgebruikers, help ze de business case voor meervoudige verificatie begrijpen en wijs hen, waar nodig, de weg naar technische-ondersteuningsmiddelen zien.
Personeel juridisch advies en IT-naleving	Zorg ervoor dat implementatie van meervoudige verificatie voldoet aan alle wettelijke of regelgevende verplichtingen die invloed hebben op de organisatie.
Personeel informatiebeveiliging	Word een expert in de implementatie en deel het technische eigendom met het identiteits- en toegangsbeheerteam. Neem deel aan communicatie en voorlichtingsacties.
Personeel identiteits- en toegangsbeheer	Integreer meervoudige-verificatietechnologie met bestaande identiteits- en toegangsbeheersystemen. Deel de technische verantwoordelijkheid met het informatiebeveiligingsteam van de organisatie.
Applicatie-eigenaars	Zorg ervoor dat toepassingen die geen gebruik maken van een centraal verificatiesysteem goed zijn geïntegreerd met meervoudige-verificatietechnologieën.
Eerstelijns IT-medewerkers	Help eindgebruikers met de registratie van het apparaat en de verificatievragen. Dien als voorvechter van het initiatief.
Eindgebruikers	Registreer meerdere apparaten in het meervoudige-verificatiesysteem.

Bron: IDC, 2017

HOE KAN MIJN ORGANISATIE PROFITEREN VAN MEERVOUDIGE VERIFICATIE?

Het implementeren van meervoudige verificatie is natuurlijk een belangrijke technisch project voor een IT-organisatie, maar nog meer draait het omveranderingsmanagement. Organisaties moeten hun implementaties voor meervoudige verificatie zorgvuldig plannen om de tevredenheid van de gebruiker te vergroten en de kans op een soepel uitrolproces met minimale verstoring van de bedrijfsactiviteiten te vergroten.

Begin met een proefuitrol

Net als bij andere grote technologische initiatieven raadt IDC aan de implementaties voor meervoudige verificatie te beginnen met een proefinitiatief. Dit initiatief is ontworpen als proof-of-concept voor de technologie zodat alle technische problemen kunnen worden opgelost voordat grotere aantallen gebruikers er last van hebben. Tijdens deze proefuitrol moeten organisaties:

- Valideren dat de geselecteerde meervoudige-verificatietechnologie kan worden geïntegreerd met de bestaande infrastructuur en diensten.
- Controleren of de aanmeldingservaring voor eindgebruikers voldoet aan zowel technische eisen als eisen van de gebruikerservaring.
- De impact op de helpdesk en eerstelijns IT-ondersteuning tijdens het uitrolproces inschatten.
- Controleren of de routineverificatie werkt zoals verwacht en gebruikers vraagt om zich opnieuw te verifiëren met het gewenste interval.
- Communicatieve hulpmiddelen testen om ervoor te zorgen dat de redenen achter het initiatief duidelijk worden overgedragen en dat de stappen die gebruikers moeten nemen om hun apparaten voor meervoudige verificatie te registreren duidelijk zijn.

Organisaties die proefprojecten voor meervoudige verificatie uitvoeren zijn vaak geneigd om de pilot tot IT-medewerkers te beperken in een poging eindgebruikers te 'beschermen' tegen blootstelling aan onbewezen technologie. Hoewel deze aanpak goed is bedoeld, vermindert het de effectiviteit van de proef door de technologie alleen aan een technisch publiek bloot te stellen. Implementaties voor meervoudige verificatie stellen belangrijke eisen aan veranderingsmanagement en organisaties wordt aangeraden gebruikers met verschillende niveaus van technische expertise in de eerste implementatie op te nemen.

Voeg gebruikers toe in fases

Nadat de proef succesvol is afgerond moet de organisatie een planning maken om de meervoudige verificatie in fases te implementeren voor alle gebruikers. Een aantal factoren die moeten worden overwogen bij het ontwerpen van de grootschalige implementatie:

- **Beschikbaarheid van zowel eerste- als tweedelijns IT-ondersteuning ter ondersteuning van de implementatie.** Maak gebruik van de ervaringen tijdens de proef om de ondersteuningslasten en de grootte van de groepen in te schatten om het beschikbare IT-personeel niet te overstelpen.
- **Geef voorrang aan gebruikers met een hoog risico voor opname in het systeem.** Gebruikers met bijzondere toegang tot systemen en toepassingen zullen de meeste negatieve impact op de organisatie hebben als hun accounts worden gecompromitteerd en moeten dus voorkeur krijgen bij de implementatie van meervoudige verificatie.
- **Gebeurtenissen in de bedrijfscyclus die de planning kunnen beïnvloeden.** Zorg dat gebruikers meervoudige verificatie niet beginnen te gebruiken rondom belangrijke gebeurtenissen. Het financiële personeel moet bijvoorbeeld niet worden ingepland om tijdens de de week van de jaarafsluiting met meervoudige verificatie te beginnen. Op dezelfde manier moeten verkopers niet beginnen met het systeem tijdens de piekperiode aan het eind van een kwartaal, waarin ze vaak nog deals moeten afronden..

Een manier om de last van ondersteunend personeel te verlichten en de ervaring van de eindgebruikers te verbeteren is een opt-inperiode te bieden waarinj ze zich kunnen aanmelden voor meervoudige verificatie en onmiddellijk kunnen beginnen met de technologie te gebruiken. Veel

gebruikers zullen hier gebruik van maken om zich op eigen tempo te kunnen aanmelden en dus geen deel te hoeven uitmaken van de fases van verplichte invoering die volgen.

Voeg gelijktijdig diensten toe

Naast het implementeren van meervoudige verificatie voor gebruikers moeten organisaties ook een plan maken voor de inzet van meervoudige verificatie door het portfolio van IT-diensten heen. IDC raadt organisaties aan twee belangrijke factoren te overwegen bij het plannen van de uitrol van hun dienst:

- **Risico op compromittering.** Organisaties moeten overwegen hoe waarschijnlijk het is dat een aanvaller de dienst aanvalt en wat voor impact het op de organisatie heeft als dit gebeurt. Deze twee criteria bepalen samen het risico dat een organisatie loopt. Voor meer over het evalueren van risico, zie *IT Security Foundation: Assessing IT Adversarial Risk for Digital Transformation* (IDC #US41083616, maart 2016).
- **Moeilijkheidsgraad van implementatie** De technische kenmerken van de dienst en het gekozen meervoudige-verificatieplatform van de organisatie zullen verschillende techische moeilijkheidsgraden opleveren voor de implementatie van de dienst.

Organisaties kunnen desgewenst een matrix ontwikkelen die vergelijkbaar is met die in afbeelding 4 om te helpen met het prioriteren van de uitrol van de dienst. De inhoud van de matrix zal variëren op basis van de infrastructuur van de organisatie en de leverancierskeuze. Nadat deze matrix is ingevuld moet het IT-team doorgaans beginnen met het implementeren van de meervoudige verificatie bij diensten met een hoog risico/lage moelijkheidsgraad in de linkerbovenhoek. Vervolgens gaan ze verder naar beneden en naar rechts, eindigend met diensten met een laag risico/hoge moeilijkheidsgraad in de hoek rechtsonder. Deze aanpak geeft de beste afweging tussen impact en inspanning.

AFBEELDING 4

Prioritering van diensten voor de implementatie van meervoudige verificatie

Bron: IDC, 2017

Communiceer regelmatig

Het belang van regelmatige communicatie over het initiatief voor meervoudige verificatie met eindgebruikers, management en andere belanghebbenden kan niet vaak genoeg worden benadrukt. Veranderingen aan verificatiemethoden zijn een regelmatige bron van angst, onzekerheid en twijfel onder eindgebruikers. Het projectteam moet ervoor zorgen dat deze zorgen worden verlicht door regelmatig te communiceren en de verhalen te benadrukken van eindgebruikers die succesvol zijn gemigreerd en de extra beveiliging waarderen.

Sommige organisaties kiezen ervoor de technische en onbekende begrip 'meervoudige verificatie' te vervangen door een vriendelijkere term als ze met eindgebruikers communiceren. Zo kunnen organisaties bijvoorbeeld verwijzen naar het initiatief als 'inloggen in twee stappen' of 'verbeterde beveiliging'.

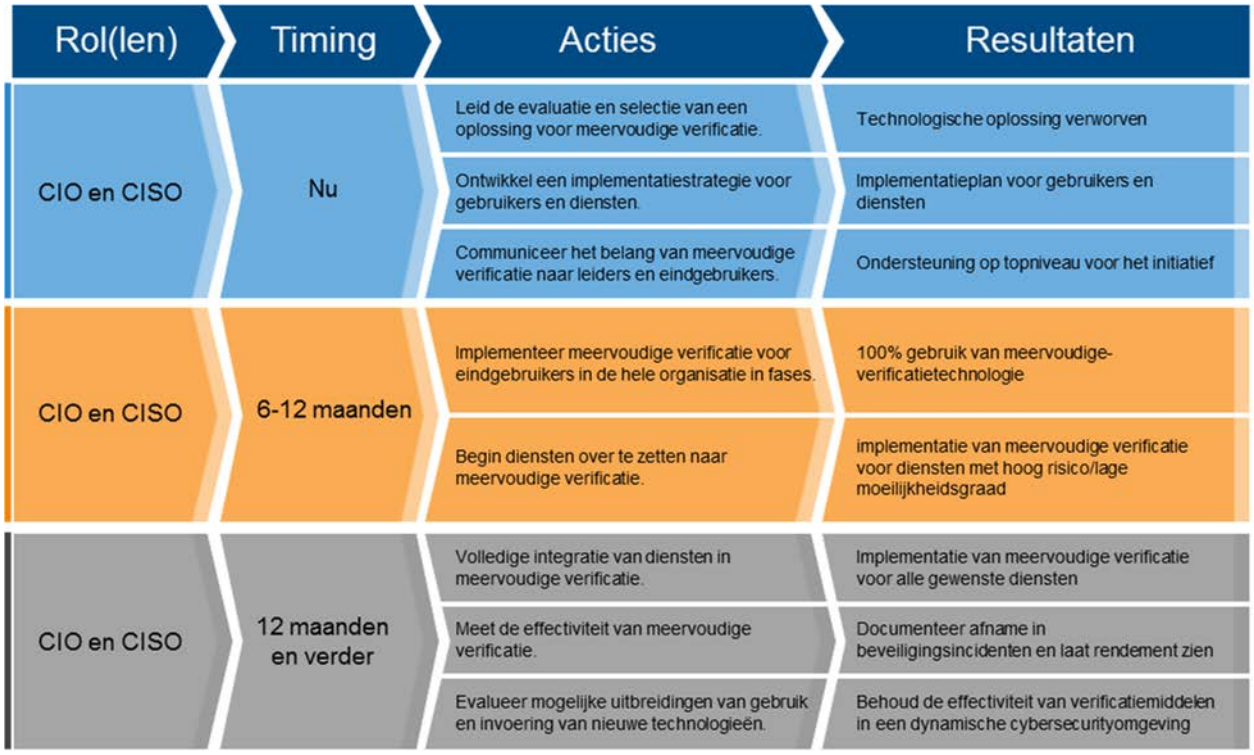
Succesvolle communicatie-inspanningen trekken soms ook vergelijkingen met de ervaringen die eindgebruikers hebben met meervoudige-verificatietechnologie voor consumenten. Ze zouden kunnen zeggen dat deze "technologie lijkt op wat u mogelijk gebruikt om uw financiële, mail-, of socialemedia-accounts te beschermen".

AANBEVELINGEN

Meervoudige verificatie speelt een cruciale rol in het beschermen van een organisatie tegen steeds vaker voorkomende aanvallen met wachtwoorden. IDC raadt organisaties die geen meervoudige verificatie hebben geïmplementeerd of het alleen voor een beperkt aantal gebruikers hebben geïmplementeerd aan het voor alle gebruikers te implementeren. Afbeelding 5 biedt onze essentiële richtlijnen over dit onderwerp.

AFBEELDING 5

Essentiële richtlijnen voor het implementeren van meervoudige verificatie



Bron: IDC, 2017

GERELATEERD ONDERZOEK

- *IDC TechScape: Worldwide Advanced Authentication, 2017* (IDC #US42418917, april 2017)
- *The Era of the Password Has Passed* (IDC #IcUS41963216, november 2016)
- *Worldwide Identity and Access Management Forecast, 2016-2020: Mobile and User Behavior Analytics Drive Growth* (IDC #US41644516, augustus 2016)

Over IDC

International Data Corporation (IDC) is de voornaamste wereldwijde leverancier van marktinformatie, adviesdiensten en evenementen voor de informatietechnologie-, telecommunicatie- en consumententechnologiebranche. IDC ondersteunt ICT-deskundigen, leidinggevenden en investeerders bij beslissingen op basis van de harde feiten over de aankoop van technologie en de strategie van bedrijven. Er zijn ruim 1.100 IDC-analisten werkzaam in 110 landen die op mondiale, regionale en lokale schaal advies geven over technologie, mogelijkheden en trends. Al 50 jaar voorziet IDC zijn klanten van strategisch advies ten behoeve van hun belangrijkste zakelijke doelstellingen. IDC is een dochteronderneming van IDG, 's werelds grootste media-, onderzoeks- en evenementenbedrijf op het gebied van technologie.

Hoofdkantoor

5 Speen Street
Framingham, MA 01701
VS
508,872.8200
Twitter: @IDC
idc-community.com
www.idc.com