RAPPORT ‘DE WACHTWOORDVRIJE TOEKOMST’

Een rapport van Okta
Juni 2019

Dit is het rapport over een toekomst zonder wachtwoorden

Om te kunnen overleven en de concurrentie aan te kunnen in het huidige competitieve bedrijfsklimaat, moet elk bedrijf een technologiebedrijf worden.

Maar terwijl organisaties moeten en kunnen transformeren door nieuwe manieren vinden om het klantcontact te verbeteren en hun eigen mensen en data te beschermen tegen verschillende bedreigingen, brokkelt het vertrouwen in technologie af. Het vertrouwen van gebruikers wordt ondermijnd door problemen met veiligheid, privacy en toestemming bij veel technologie waar we op vertrouwen.

Traditioneel gezien berust de bescherming van onze online identiteit op één belangrijke methode: het wachtwoord. Wachtwoorden bieden ons al decennialang toegang tot onze digitale identiteit en tot alles wat we online doen. En al die tijd al zijn we getuige van hoe kwetsbaar het wachtwoord in feite is. Okta heeft onderzoek gedaan en daaruit blijkt welke impact wachtwoorden hebben op onze veiligheid en de kwaliteit van ons dagelijks leven.

Maar stelt u zich eens een wereld voor waarin onze veiligheid niet afhangt van een combinatie van letters en cijfers die heel gemakkelijk kan worden gemanipuleerd. Een wereld waar de toegang tot de zaken die we nodig hebben voor ons privéleven en werk, zo uniek is dat niemand anders dezelfde toegangscode kan hebben omdat die toegang gelinkt is aan ieders persoonlijke identiteit.

2019 is een keerpunt wat betreft veiligheid. Er zal een begin gemaakt worden met beveiliging die gebaseerd is op onze persoonlijke identiteit en die compleet wachtwoordvrij is. Individualiteit speelt daarbij een essentiële rol waarbij organisaties een vertrouwensrelatie kunnen opbouwen.

Hoe heeft Okta dit onderzoek uitgevoerd?

In opdracht van Okta heeft Opinium onderzoek gedaan onder 4013 werknemers uit het Verenigd Koninkrijk, Frankrijk en Nederland. De uitkomsten zijn in mei 2019 verzameld. We verwijzen naar dit onderzoek als 'het onderzoek van Okta' en naar de mensen die hebben gereageerd als de 'respondenten'.

LAND


2007


1003


1003

GESLACHT

50% vrouw

49% man

1% anders

LEEFTIJD

21% 18-34

52% 35-54

27% 55+

DIENSTVERBAND

82% fulltime

16% parttime

2% parttime (minder dan 8 uur)

MANIER VAN WERKEN

87% werkt op kantoor

13% werkt thuis/ op afstand

BEDRIJFSGROOTTE

13% micro & klein

*6% onbekend

30% middelgroot

52% groot

1 WACHTWOORDVRIJE BEVEILIGING WORDT REALITEIT

Vertrouwen en identiteit

Vertrouwen is de nieuwe maatstaf en organisaties moeten nu meer dan ooit aan hun klanten en werknemers laten zien dat ze het vertrouwen waard zijn. Alleen op deze manier is succes mogelijk. Het belang dat aan vertrouwen gehecht wordt, is het afgelopen decennium groter geworden. Dit komt door inbreuken op persoonsgegevens, cyberaanvallen en problemen met de privacy vanwege het uitvoerig tracken van onze digitale identiteit en het gebruik van deze informatie met als doel geld te verdienen.

Identiteit staat aan de basis van vertrouwen. Mensen letten tegenwoordig meer op hun identiteit en dus moeten bedrijven er beter op letten hoe ze met deze identiteiten omgaan.

Al decennialang zijn onze identiteit en beveiliging met elkaar verweven, en we hebben wachtwoorden gebruikt om deze te beschermen. Maar de realiteit is anders: wachtwoorden zijn bewezen een zeer ineffectieve methode voor beveiliging.

Dr. Maria Bada, onderzoeker aan Cambridge University, stelt dat het wachtwoord een van de grootste problemen is waar beveiligingstechnici al tientallen jaren tegenaan lopen.

Gebruikers moeten niet alleen hun wachtwoord onthouden, maar ook het systeem en de gebruikersnaam of -id dat ermee gepaard gaat. Ze moeten onthouden of, en indien ja, wanneer ze een wachtwoord veranderd hebben en daarnaast natuurlijk het eigenlijke wachtwoord[1]. Gebruikers kunnen wachtwoorden die zelden gebruikt worden of heel vaak aangepast worden, simpelweg niet onthouden.

Uit onderzoek blijkt dat het onthouden van meer dan twee of drie sterke wachtwoorden, meer van het menselijk geheugen vergt dan mogelijk is. En zelfs het onthouden van die twee of drie wachtwoorden is al lastig als deze maar af en toe gebruikt worden[2].

[1] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' -- a Human/Computer Interaction Approach to Usable and Effective Security.
[2] Schacter, D. L., Addis, D. R., Hassabis, D., Martin, V. C., Spreng, R. N., and Szpunar, K. K. (2012). The future of memory: remembering, imagining, and the brain.

De uitdaging voor bedrijven

Voor bedrijven zijn wachtwoorden de oorzaak van verschillende problemen. Volgens het Data Breach Investigation Report van Verizon uit 2018 is 81% van de inbreuken door hacken het gevolg van een zwak, gestolen of hergebruikt wachtwoord[3]. De gevolgen van zo'n lek kunnen rampzalig zijn. De gemiddelde kosten van gestolen gegevens is $148[4] en het totale kostenplaatje van een datalek komt gemiddeld neer op $3,9 miljoen. Als er sprake is van een lek, kunnen organisaties opnieuw geraakt worden. De kans op herhaling van een datalek ligt gedurende de volgende 2 jaar op 32%. Om nog maar te zwijgen over de reputatieschade die vaak niet meer te repareren is.

Voor bedrijven en het wachtwoordgebruik van hun werknemers is zo'n cyberincident vaak de grootste zorg. Daarnaast komen er uit het onderzoek van Okta nog andere problemen naar voren die dagelijks een impact hebben op de bedrijfsprocessen.

Het onderzoek van Okta naar wachtwoorden toont aan dat wanneer mensen hun wachtwoord vergeten:

37%
niet kan inloggen op zijn account

37%
geen toegang heeft tot benodigde informatie of gegevens

19%
vertraging oploopt

Wachtwoorden belemmeren de productiviteit. En met een gestage afname van de productiviteit is een bedrijf niet in staat om de concurrentie bij te benen en zal het klanten die een uitstekende klantenservice verwachten, moeten teleurstellen.

[3] Verizon Enterprise. (2018). 2018 Data Breach Investigations Report.
[4] Ibm.com. (2019). Cost of a Data Breach Study.

Uitdagingen voor werknemers

Uit het onderzoek van Okta blijkt dat respondenten gemiddeld 10 wachtwoorden moeten onthouden voor gebruik in het dagelijks leven en dat ze per maand gemiddeld zo'n drie wachtwoorden vergeten. Het is bekend dat het grootste beveiligingsrisico voor werkgevers de werknemers zijn - bijna de helft (49%) van organisaties in elke sector krijgt te maken met serieuze incidenten als gevolg van fouten van werknemers[5].

Het is zorgelijk dat dit op de korte termijn waarschijnlijk niet zal veranderen. Uit het onderzoek van Okta blijkt dat wachtwoorden die gevoelige informatie bevatten, zelden veranderd worden. Wachtwoorden op het werk worden maar drie keer per jaar veranderd en andere wachtwoorden voor bijvoorbeeld bankrekeningen, telefoontoegang, persoonlijke e-mail en accounts op sociale media, worden gemiddeld maar één keer per jaar veranderd.

10

WACHTWOORDEN

moeten er (gemiddeld) onthouden worden in het **dagelijkse leven**

 **11**

 **12**

 **9**

3

WACHTWOORDEN

worden (gemiddeld) **per maand vergeten**

 **3**

 **2**

 **3**

18

PROCENT

Voelt zich **gestresst en/ of bezorgd** door of over het **aantal wachtwoorden** dat onthouden moet worden

 **21%**

 **12%**

 **19%**

[5] Kaspersky Industrial CyberSecurity. (2018). The State of Industrial Cybersecurity 2018 | Kaspersky Industrial CyberSecurity.

Waarom blijven organisaties toch vasthouden aan een methode die tot nu toe ontoereikend blijkt?

De afhankelijkheid van wachtwoorden heeft ertoe geleid dat organisaties en softwareaanbieders strengere eisen stellen aan de wachtwoorden die goedgekeurd worden. Iedereen heeft wel eens te maken gehad met een wachtwoord waarbij op het scherm te zien is hoe sterk dit wachtwoord is, en de vereisten van een mix van cijfers, hoofdletters, kleine letters en speciale tekens. Maar dit alleen is niet genoeg om de beveiliging te verbeteren - en in veel gevallen worden zelfs deze maatregelen niet genomen.

DR MARIA BADA
Onderzoeker aan Cambridge University

Zelfs in organisaties die gebruikers expliciet uitleggen hoe een sterk wachtwoord in elkaar moet zitten, voldoen velen niet aan de regels en kiezen toch voor een zwak wachtwoord.

De gebruikerswaarneming van de veiligheid kan invloed hebben op de bereidwilligheid om te voldoen aan de wachtwoordvereisten. Beveiligingsmechanismen- en beleid dat geen rekening houdt met de dagelijkse praktijk van het werk, de organisatiestrategie en de gebruiksvriendelijkheid kunnen leiden tot een onveilige werkpraktijk en een lage motivatie van gebruikers met betrekking tot de beveiliging.[6]

Onderzoekers hebben ook gekeken naar het verband tussen cultuur, taal en persoonlijkheidsdimensies op het wachtwoordgedrag. Er is echter geen verband gevonden op één persoonlijkheidskenmerk na: vriendelijkheid.[7]

Wachtwoorden zijn vaak behoorlijk onthullend. Ze worden vaak ter plekke bedacht, dus gebruikers kiezen voor iets waar ze op dat moment direct aan denken of voor iets dat emotioneel van belang is. Zo bekeken maken wachtwoorden dus gebruik van de dingen die zich net onder het oppervlak van ons bewustzijn bevinden. Criminelen maken gebruik van deze informatie en met een klein beetje onderzoek is een wachtwoord gemakkelijk te raden.

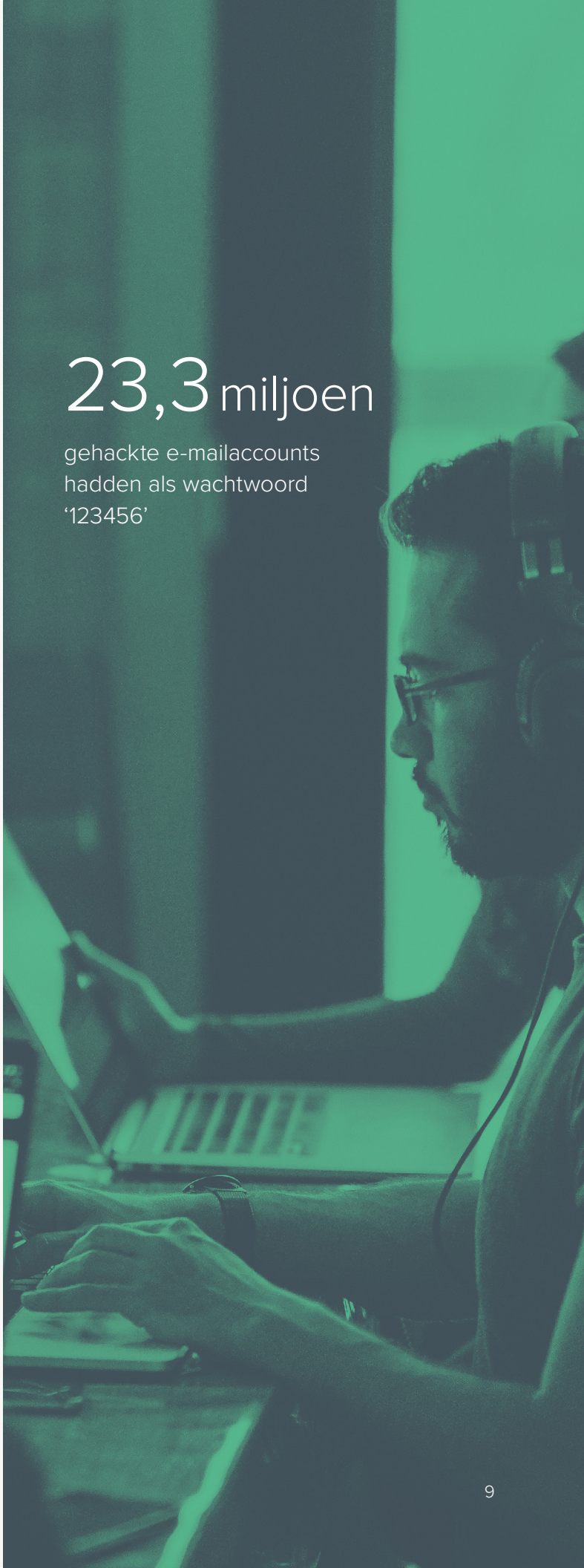
[6] Adams, A., & Sasse, M. A. (1999). Users are not the enemy.
[7] Kawu, A. A, Muhammad, I, Awal A, and Abdullah, M. B (2018). Effect of mental state on password selection among mobile phone users.

Wachtwoorden: een ideaal doelwit voor cybercriminaliteit

Volgens het National Cyber Security Centre in het Verenigd Koninkrijk hadden 23,3 miljoen e-mailaccounts als wachtwoord '123456'[8], terwijl miljoenen andere gebruikers wachtwoorden instelden als 'wachtwoord' of de naam van hun favoriete voetbalteam of band.

Ongeacht de inspanningen van een bedrijf om de aandacht voor sterke wachtwoorden te vergroten, zullen gebruikers toch op zoek gaan naar een wachtwoord dat ze gemakkelijk kunnen onthouden. Dit komt met name door het aantal wachtwoorden dat ze moeten onthouden.

Jarenlang zijn wachtwoorden beschouwd als een adequate manier van beveiligen, en de kosten vergeleken met alternatieven waren laag. Er is vaak sprake geweest van een zogenaamd 'nieuw tijdperk' waarin de technologiesector aankondigde dat het einde van het wachtwoord in zicht was. Er zijn nu twee verschillen: aan de ene kant bestaat er een groeiende behoefte vanuit beveiliging om de status quo aan te passen.



[8] Ncsc.gov.uk. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security.

2 HET VERBORGEN PROBLEEM VAN WACHTWOORDBEVEILIGING

Wachtwoorden en de geestelijke gezondheid op het werk

De afgelopen jaren hebben we gezien hoe onze maatschappij investeert in het begrijpen en bespreekbaar maken van mentale en geestelijke problemen. Nu pas beginnen we met het bespreekbaar maken van dergelijke problemen op de werkvloer. Uit recent onderzoek[9] blijkt dat maar liefst 1 op de 6 jonge mensen in zijn/haar leven te maken krijgt met een angststoornis. Vorig jaar bleek uit onderzoek van de American Psychiatric Association (APA) dat bijna 40% van de Amerikanen zich angstiger voelde dan in 2017. De toename van angstgevoelens op de werkvloer wordt veroorzaakt door verschillende factoren, maar veiligheid en beveiliging is een factor die lange tijd niet gezien is.

DR MARIA BADA
Onderzoeker aan Cambridge University

> De potentiële impact van het vergeten van een wachtwoord kan het stressniveau enorm verhogen en op den duur kan dit uitmonden in een inzinking of burn-out.
>
> Dat is het gevolg van het feit dat ons brein gevoelig is voor waargenomen dreiging. Door voortdurend bezig te zijn met potentiële risico's en dreiging online, worden we hypergevoelig voor stress. Op de lange termijn kan dit zorgen voor mentale problemen.

[9] Anxiety UK. (2019). Young People and Anxiety - Anxiety UK.

Uit het onderzoek van Okta blijkt dat wachtwoorden direct in verband staan met stress. Daarbij reageerden respondenten negatief wanneer ze veel verschillende wachtwoorden moesten onthouden:

18%

van de respondenten voelt zich **gespannen/bezorgd**

47%

(bijna de helft) voelt zich **geïrriteerd** of **opgejaagd**

In grote bedrijven kan dit oplopen tot **52%**, voor kleine bedrijven (micro) neemt het af tot **36%**

63%

(twee derde) zegt dat **negatieve emoties** worden opgeroepen

Dit percentage is het hoogste in Frankrijk **(73%)** in vergelijk met het VK **(67%)** en Nederland **(52%)**

Het vergeten van een wachtwoord is voor nog meer mensen de oorzaak van negatieve emoties: 62% voelt zich gespannen of geïrriteerd vanwege het vergeten van een wachtwoord. Dit is het hoogst in het VK (69%) in vergelijking met Frankrijk (65%) en Nederland (53%).

DR MARIA BADA
Onderzoeker aan Cambridge University

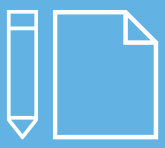
> Wachtwoordvermoeidheid, de stress die gebruikers ervaren door de eisen om een groot aantal wachtwoorden te bedenken, (her)in te voeren, te onthouden en regelmatig te veranderen, kan de oorzaak zijn van extreme stress.
>
> Een aantal beleidslijnen op het werk kan deze wachtwoordvermoeidheid tot gevolg hebben. Werknemers vragen om het wachtwoord te veranderen terwijl er gewerkt wordt of het werk hiervoor onderbreken kan leiden tot gehaaste en zwakke wachtwoorden die weer snel vergeten worden. Het verlopen van een sessie waarna de gebruiker weer opnieuw moet inloggen kan leiden tot dezelfde emoties.

De mentale druk van het wachtwoord

Mensen maken zich zorgen als ze een wachtwoord vergeten, maar het vergeten van een wachtwoord op zichzelf houdt geen beveiligingsrisico in. De meerderheid van het aantal lekken door hacken wordt veroorzaakt door hergebruikte, gestolen of zwakke wachtwoorden: voor een persoon is het riskanter om een onveilig wachtwoord en geheugensteuntjes te gebruiken dan om het wachtwoord te vergeten en opnieuw in te stellen:

34%

van de gebruikers gebruikt **hetzelfde wachtwoord** voor **meerdere accounts**



26%

noteert ze op **papier**

17%

noteert ze op hun **telefoon** of **computer**

6%

geeft zelfs het gebruik toe van **bekende** wachtwoorden

In totaal gebruikte 78% van de respondenten een onveilige manier om zich zijn wachtwoord te herinneren. In de leeftijdscategorie 18-34 jaar loopt dit op tot 86%. Dit is verrassend als men in gedachten houdt dat jonge mensen van kinds af aan leren om technologisch goed vaardig te zijn, en dus ook vaardig met betrekking tot cyberbeveiliging. Dit kan echter ook te maken hebben met het feit dat mensen van 18-34 jaar gemiddeld genomen meer apps, apparaten en technologieën gebruiken en dus meer wachtwoorden nodig hebben. Daarom maken ze gebruik van andere methoden om al deze wachtwoorden te onthouden. Frankrijk (87%) heeft het hoogste aandeel mensen dat een onveilige methode hanteert, gevolgd door Nederland (79%) en het VK (74%).

DR MARIA BADA
Onderzoeker aan Cambridge University

> Helaas lijkt het er niet op dat stress met betrekking tot gegevensbeveiliging ertoe leidt dat de meerderheid van de mensen zijn gewoontes omtrent persoonlijke cyberbeveiliging aanpast.
>
> Vaak moet iemand eerst het slachtoffer worden van criminaliteit voordat diegene het wachtwoord aanpast. Wat gebruikers ertoe kan brengen om hun instelling met betrekking tot cyberbeveiliging te veranderen, is na te denken over de kosten en baten van het risico van een onveranderd wachtwoord ten opzichte van de kosten van het wachtwoord regelmatig veranderen.

Wachtwoordmanagers en Single Sign-On oplossingen

– Van veel wachtwoorden naar één

Er zijn makkelijke manieren om de wachtwoorddruk te doen afnemen. Wachtwoordmanagers zijn een handig alternatief: er is een sterk wachtwoord (of zin) nodig om de kluis te openen waarin alle persoonlijke wachtwoorden worden bewaard. Zo'n oplossing stelt de gebruiker in staat om sterke, unieke wachtwoorden te bedenken voor elke afzonderlijke dienst die hij gebruikt zonder dat hij zich druk hoeft te maken over het onthouden ervan. Maar uit het onderzoek blijkt dat slechts 14% van de respondenten gebruikmaakt van zo'n wachtwoordmanager. Het kopen, installeren en beheren van nog een extra softwareprogramma kan een hindernis zijn, en het gebruik ervan tussen verschillende apps en apparaten verloopt nog niet helemaal naadloos.

Voor bedrijven bestaat er een nog betere oplossing, namelijk het inzetten van de Single Sign-On (SSO)-oplossing. Dit heeft alle voordelen van een wachtwoordmanager en daarnaast nog meer. Gebruikers hoeven maar een wachtwoord te onthouden en krijgen daarmee toegang tot alle applicaties. En nog beter: omdat SSO-oplossingen achter de schermen gebruikmaken van moderne protocollen als SAML 2.0 en OpenID Connect, zijn voor verbindingen met moderne applicaties geen wachtwoorden meer nodig. Zo is de toegang nog beter beveiligd. SSO maakt ook het toevoegen van sterke multifactor-authenticatie gemakkelijk en helpt toegang tot alle geïntegreerde applicaties te beschermen.

3

WAT IS HET ALTERNATIEF VOOR HET WACHTWOORD?

Innovatie en integratie

De technologische innovaties van de afgelopen tien jaar hebben bedrijven een heel scala van nieuwe mogelijkheden gegeven om op verschillende manieren met beveiliging om te gaan. Nu kunnen organisaties verschillende methodes, zoals biometrie, combineren met traditionele methoden die nog veilig zijn om te gebruiken, en zo inadequate methoden helemaal elimineren. Na jaren van valse voorspelling is er eindelijk licht aan het einde van de tunnel van de wachtwoordvrije toekomst.

Uit het onderzoek van Okta blijkt dat men wel oren heeft naar biometrische authenticatie met de volgende voordelen:

GEBRUIKSGEMAK DAGELIJKS LEVEN

24% werk

28% persoonlijk

MAAKT ACCOUNTS VEILIGER

15% werk

20% persoonlijk

VERMINDERT ANGSTGEVOELENS

13% werk

16% persoonlijk

MINDER BEZORGD OVER BEVEILIGING

8% werk

11% persoonlijk

TOENAME VAN PRODUCTIVITEIT

11% werk

8% persoonlijk

In de toekomst: Biometrie

Biometrische authenticatie die gebruikmaakt van vingerafdrukken en herkenning van de ogen, het gezicht en de stem werd hoofdzakelijk ingesteld om beter te beschermen tegen ongeautoriseerde toegang tot accounts of systemen. In tegenstelling tot gebruikersnamen, wachtwoorden en pincodes zijn deze gegevens voor iedereen uniek.

Biometrische authenticatie wordt al meer gebruikelijk op apparaten voor persoonlijk gebruik en op het werk. Daarnaast zijn bedrijven ook bezig om hun eigen beveiligingsmaatregelen op basis van biometrie in te stellen.

Uit het onderzoek van Okta blijkt dat biometrie in de smaak valt en geaccepteerd wordt als extra veiligheidsmaatregel op het werk of zelfs ter vervanging van wachtwoorden:

16% van respondenten verwacht **authenticatie door middel van vingerafdruk**

6% verwacht **gezichtsherkenning**

4% verwacht **irisherkenning** bij apparaten op het werk

Maar liefst 70% van de respondenten gebruikt privé biometrische gegevens of zou dit overwegen, 24% denkt dat dit het dagelijks leven op het werk zou vergemakkelijken, en 13% denkt dat het de stress en angstgevoelens op het werk zou verminderen, wat suggereert dat de impact van wachtwoordgebruik op de geestelijke gezondheid wat verzacht zou kunnen worden door gebruik van biometrische authenticatie.

Respondenten denken ook dat het gebruik van biometrie helpt om werkaccounts beter te beveiligen (15%) en verwachten dat ze zich minder zorgen zouden maken over de veiligheid (8%). Biometrie zou ook helpen om de productiviteit op het werk te verhogen, aldus 11% van de respondenten.

Nadruk op educatie

Hoewel het gebruik van biometrie veel voordelen kent, zijn mensen niet volledig overtuigd. 86% van de respondenten geeft aan bedenkingen te hebben bij het delen van biometrische gegevens op het werk. Toen we deze respondenten vroegen waarom ze deze data liever niet op het werk deelden, zei:

21% 

dat zijn **biometrische gegevens** mogelijk **gekaapt** zouden worden, zodat ze deze in de toekomst niet meer zouden kunnen worden gebruikt

15% 

dat het **te moeilijk te implementeren** zou zijn. Hetzelfde aantal stelde te denken dat de technologie **zal falen** waardoor men geen toegang meer zou hebben tot benodigde informatie

13% 

de technologie niet te vertrouwen

Er is dus werk aan de winkel om deze misverstanden omtrent de werking van biometrische technologieën weg te nemen en vertrouwen op te bouwen.

Een voorbeeld: veel werknemers zouden onterecht kunnen denken dat het gebruik van Touch ID of Face ID op een iPhone of iPad of Windows Hello For Business het mogelijk maakt voor bedrijven om naar believen toegang te krijgen tot biometrische gegevens. In werkelijkheid zijn de biometrische gegevens zeer goed beschermd en niet toegankelijk voor externe partijen, zelfs niet voor het besturingssysteem van het apparaat in kwestie. Het is juist diep ingebed in de beveiligingshardware van het apparaat (zoals Secure Enclave of Trusted Platform Module). Dit betekent dat zelfs Apple of Microsoft er niet bij kunnen, laat staan een werkgever.

Het is aan de organisaties en aan hen die de biometrische technologie ontwikkelen om te laten zien hoe de gegevens veilig zullen worden bewaard en om daarnaast de voordelen en het gebruiksgemak van deze technologie te verkondigen om zo de aanvankelijke bedenkingen weg te nemen.

DR MARIA BADA
Onderzoeker aan Cambridge University

Biometrie wordt nu al een tijdje breed ingezet: mobiele telefoons en computers maken bijvoorbeeld gebruik van vingerafdrukken. Daaruit blijkt dat gebruik van biometrie op privéapparaten zoals op de iPhone al is ingeburgerd.

Uit het onderzoek van Okta blijkt dat er nog steeds bedenkingen bestaan als het gaat om het delen van biometrische gegevens met de werkgever. Dit kan gemakkelijk verklaard worden vanuit het gebrek aan eerdere ervaring met het gebruik van biometrische gegevens op dit gebied van ons dagelijks leven.

> Maar het gedegen technische begrip dat gedurende het afgelopen decennium verkregen is en de volwassenwording van de systemen die aangeboden worden door leveranciers kunnen alleen maar resulteren in een toename van de waarschijnlijkheid dat wachtwoorden en symbolen op een zeker moment tijdens het werkzame leven van de meesten lezers van dit rapport vervangen zullen worden.
>
> Een verwacht voordeel van de gebruiksvriendelijkheid van biometrie is dat er niets vergeten, verloren of gestolen kan worden; individuen dragen hun kenmerken namelijk altijd bij zich. Daardoor wordt het geheugen van de gebruiker minder belast en dit ondersteunt het gebruiksvriendelijkheidsprincipe van de universele toegang.[10]

Nieuwe biometrische standaarde

Biometrische technologieën zoals vingerafdrukscanners en gezichtsherkenning zijn nu al de norm voor de toonaangevende apparaten voor particulier gebruik. Een project van de FIDO-alliantie en World Wide Web Consortium (W3C), genaamd in FIDO2, introduceerde in maart 2019 de W3C Web Authentication (WebAuthn) browser API-standaard voor web-authenticatie en het FIDO Client to Authenticator Protocol (CTAP). WebAuthn geeft webapplicaties de mogelijkheid om gebruikersauthenticatie makkelijker en veiliger te laten verlopen door gebruik te maken van beveiligingssleutels én platformauthenticatoren. WebAuthn maakt gebruik van publieke-sleutelcryptografie om gebruikers te beschermen tegen geavanceerde phishing-aanvallen en wordt nu ondersteund door alle toonaangevende browsers (Chrome, Firefox, Microsoft Edge en binnenkort Safari) en besturingssystemen.

Voor consumenten en werknemers betekent dit dat het vertrouwen behouden blijft, aangezien WebAuthn een veiligere verificatiemethode is waarbij geen sprake is van de risico's die bij wachtwoorden horen. Wanneer dit gecombineerd wordt met zeer veilige biometrische technologie op het apparaat zelf – dus de combinatie 'wie ben je' en 'wat weet je' – zijn gebruikersnamen en wachtwoorden niet langer noodzakelijk. Dit betekent dat de IT-teams van bedrijven geregistreerde apparaten die in het bezit zijn van de eindgebruiker kunnen gebruiken als authenticatiemethode.

Dit is een fundamentele verandering, aangezien dit het 'dreigingsmodel' compleet verandert. Eerder kon iedereen waar ook ter wereld de toegangscodes stelen of raden en zo toegang verkrijgen. Maar vandaag de dag kunnen via WebAuthn alleen mensen die letterlijk toegang hebben tot de beveiligingssleutel of het apparaat toegang verkrijgen, en als daarbij ook gebruik wordt gemaakt van biometrie, is er nog maar één persoon die toegang heeft.

[10] Fairhurst, M.C., Guest, R.M., Deravi, F. and George, J. (2002). Using Biometrics as an Enabling Technology in Balancing Universality and Selectivity for Management of Information Access.

4

WACHTWOORDVRIJ VANDAAG AL MOGELIJK

Nu organisaties en personen meer belang hechten aan identiteit en vertrouwen, is er behoefte aan maatregelen om ervoor te zorgen dat onze identiteiten goed beschermd zijn.

We zien nu al dat onderdelen van organisaties – werkgevers, app-ontwikkelaars, fabrikanten van apparaten of aanbieders van IT-beveiliging – het vertrouwen dat de gebruiker in hen heeft weten te vergroten.

Uit het onderzoek van Okta blijkt dat de huidige en meest gebruikte methode voor het veiligstellen van apps, apparaten, systemen en accounts het wachtwoord is - maar deze methode is ontoereikend: wachtwoorden zijn makkelijk te hacken, moedigen onveilig gebruik aan, en veroorzaken stress, angstgevoelens en een afname van de productiviteit. Het is daarom tijd om anders over het wachtwoord te gaan denken.

We hebben al gezien hoe moderne SSO-oplossingen en sterke, phishingproof authenticatiemethoden een meer robuuste en logische manier creëren om een onderneming te beveiligen. Dezelfde aanpak is nodig om een wachtwoordvrije wereld mogelijk te maken. Okta draagt bij aan het ontwikkelen van een veilige, wachtwoordvrije toekomst voor ondernemingen die gemakkelijk in elk bedrijf van elke grootte en binnen elke branche te implementeren is.

Okta combineert de belangrijke capaciteiten van Single Sign-On en Adaptive Multi-factor Authentication (MFA) met de biometrische authenticatiemethoden die voor de industrie gangbaar zijn. Door de combinatie van een volledige contextuele risicoanalyse en WebAuthn authenticatoren die sterk bestand zijn tegen phishing en niet omzeild of gekloond kunnen worden zijn we in staat om wachtwoorden te vervangen bij organisaties

Organisaties kunnen de apparaten die mensen toch al hebben op een zeer veilige manier inzetten waarbij het respect voor de privacy blijft bestaan en er geen sprake is van het lekken van informatie over met wie er gecommuniceerd wordt of wat voor apps er worden gebruikt.

TODD MCKINNON
CEO en medeoprichter van Okta

Bij Okta geloven we sterk in het potentieel van technologie. Daarnaast denken we dat voor alle organisaties, ongeacht grootte of branche, die de verschuiving naar een technologische organisatie maken, vertrouwen de nieuwe maatstaf is. In de huidige samenleving moeten bedrijven gebruikmaken van de technologie die hen in staat stelt om snel te innoveren en daarbij niet de veiligheid, privacy en toestemmingscontroles uit het oog verliezen waardoor ze het vertrouwen kunnen winnen. Als authenticatiefactor zijn wachtwoorden niet langer geschikt, en bedrijven moeten niet meer afhankelijk zijn van deze onbetrouwbare methode. In 2019 zullen we de eerste golf organisaties zien die compleet wachtwoordvrij werken en de klanten van Okta bevinden zich in de voorhoede.

Ga naar **www.okta.com** voor meer informatie over onze aanpak