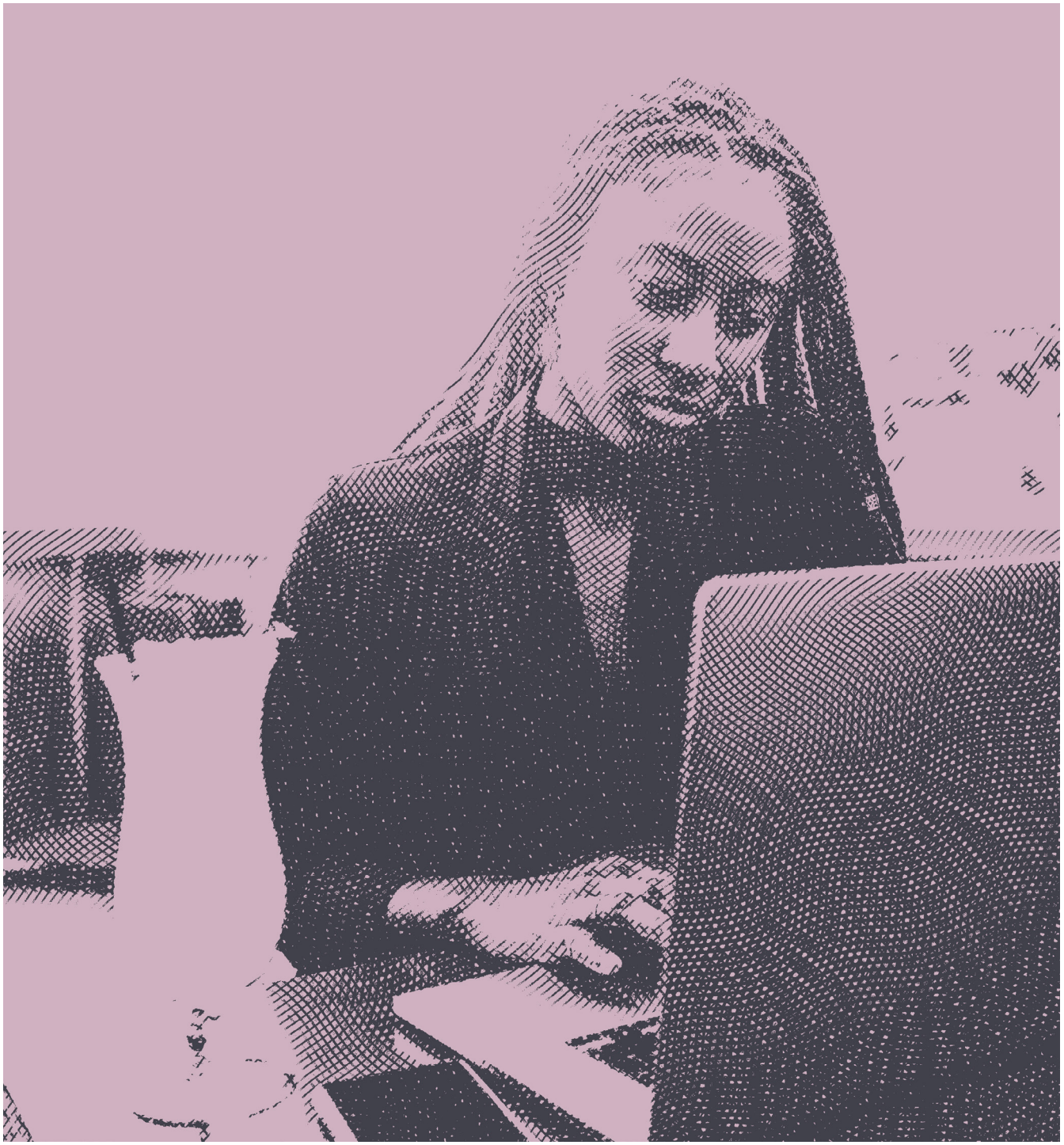
De Okta Digital Trust Index

Zoeken naar de grens van het menselijk vertrouwen in een snel evoluerende wereld



okta

Inhoud

01

Inleiding

03

Deel Een

Waarom vertrouwen consumenten bepaalde merken?

06

Deel Twee

Hoe de pandemie het gedrag van gebruikers heeft veranderd

08

Deel Drie

Wat doen organisaties hiermee?

09

Deel Vier

Conclusies en aanbevelingen

11

Deel Vijf

Het beveiligen van de onderneming van de toekomst met Okta

> Vertrouwen is een overtuigende relatie met het onbekende.
>
> Rachel Botsman, Trust Fellow aan Oxford University's Saïd Business School

Inleiding

Vertrouwen begint met veiligheid

Door vele gebeurtenissen in 2020 is het begrip "vertrouwen" in ons leven op de voorgrond getreden. Plots werd het vertrouwen in overheden en instellingen voor de meesten van ons een cruciale zaak. Als onderdeel daarvan is het vertrouwen van klanten in merken essentieel geworden voor de winstgevendheid van een organisatie, te midden van een ernstige economische recessie. Daarnaast heeft het veel organisaties gedwongen om oude bezwaren te overwinnen en werknemers te vertrouwen om thuis te werken en te vertrouwen op het feit dat digitale kanalen de enige manier zijn om klanten te bedienen.

Dit alles speelt zich af tegen een achtergrond van toenemende bezorgdheid over digitale veiligheid, veroorzaakt door een ongekend aantal datalekken en cyberdreigingen. Tegelijkertijd gebeurde het tijdens een periode van strikte handhaving van wetgeving rondom dataprotectie, opportunistische social engineering scams en verhoogde verwachtingen van de consument ten aanzien van privacy. Uit een beoordeling van **INTERPOL** blijkt dat de phishingfraude als gevolg van de pandemie met 59% is toegenomen, samen met een toename van malware, ransomware, kwaadaardige internetdomeinen en 'fake news'. Criminelen proberen de angst en onzekerheid als gevolg van de instabiele sociale en economische situatie uit te buiten.

Voor een organisatie begint veiligheid bij vertrouwen. Dat houdt in dat een effectieve beveiliging alleen mogelijk is als een organisatie inzicht heeft in welke medewerkers, partners en klanten buiten de gebruikelijke kantooromgeving toegang kunnen krijgen tot gevoelige data en systemen. Het tegenovergestelde is echter net zo waar: vertrouwen begint met beveiliging. De beste manier om vertrouwen te winnen van betrokken partijen, is door effectieve security-tools en beleid aan te bieden, die vooral een focus hebben op consistent beheer van de identity van gebruikers. Dit is de snelste weg naar het verbeteren van productiviteit, en het opbouwen van loyaliteit en betrokkenheid: niet alleen onder werknemers en partners, maar ook onder klanten.

Om hier inzicht in te krijgen, heeft Okta onderzoek laten uitvoeren onder 13.000 kantoormedewerkers - waaronder meer dan 1.000 in Nederland - waarbij de volgende vragen werden beantwoord:

Hoeveel van ons vertrouwen wordt opgebouwd, onderhouden en verbroken in de digitale wereld?

Hoeveel vertrouwen hebben we wanneer we alleen via digitale kanalen en devices communiceren, los van menselijke connecties?

Zijn de acties van merken, organisaties en overheden voldoende om vertrouwen op te bouwen?

Welke externe factoren beïnvloeden onze bereidheid om te vertrouwen op digitale kanalen?

Methodologie:

Alle cijfers, tenzij anders vermeld, zijn afkomstig van YouGov Plc. De totale steekproefomvang was 13.163 kantoormedewerkers uit het Verenigd Koninkrijk, de Verenigde Staten, Australië, Duitsland, Frankrijk, Italië, Spanje, Zweden, Nederland en Japan. Hiertoe behoren 1.010 kantoormedewerkers uit Nederland. Het onderzoek vond online plaats tussen 26 november en 10 december 2020.

Wat we hier presenteren is de Okta Digital Trust Index: een rapport waarin het menselijke vermogen om digitaal te vertrouwen wordt onderzocht in een wereld die in toenemende mate wordt bepaald door de pandemische effecten. Tot slot geven we aanbevelingen voor individuen, bedrijven en publieke organisaties over hoe een echte, menselijke vertrouwensrelatie kan worden opgebouwd en waargemaakt.

> Vertrouwen is moeilijk te winnen, maar makkelijk te verliezen.
>
> Mark Carney, gouverneur van de centrale bank van Canada (2008-2013)

Deel Een

Waarom vertrouwen consumenten bepaalde merken?

Met de onvermijdelijke overstap naar remote werken zijn kantoormedewerkers in 2020 digitaal ingestelde consumenten geworden, die veel meer tijd en geld online spenderen. De online omzetstijging van Nederlandse retailers was volgens het **CBS in Nederland in 2020 43,5%**.

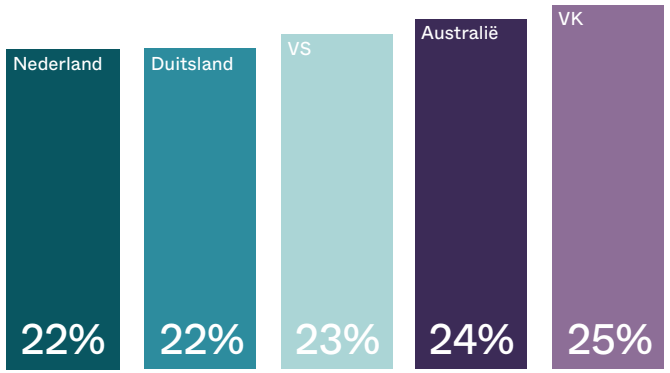
Aangezien 2021 een overgangsjaar is naar meer geïnstitutionaliseerde online activiteiten, staan merken voor een uitdaging om hun aandeelhouders te overtuigen van nieuwe vormen van vertrouwen en loyaliteit.

Vertrouwen is vandaag de dag moeilijk te winnen, maar gemakkelijk te verliezen. Hoewel aandeelhouders, investeerders en directies steeds meer waarde hechten aan ethiek, hebben wij ontdekt dat de focus van klanten ligt op fundamentele zaken.

30% van de Nederlandse respondenten geeft aan dat de betrouwbaarheid van de dienstverlening het meest waarschijnlijke criterium is voor hun vertrouwen in een digitaal merk, zoals bijvoorbeeld de garantie dat producten op tijd en in goede staat arriveren.

Ook veiligheid was voor hen van groot belang: ruim een vijfde (22%) zei dat veilige inlogmogelijkheden zoals multifactorauthenticatie (MFA) en andere maatregelen het vertrouwen in het merk kunnen versterken.

Deze behoefte aan veiligheid werd gedeeld door respondenten in het Verenigd Koninkrijk (25%), Australië (24%), de VS (23%) en Duitsland (22%).



Percentage van respondenten dat gelooft dat een veilige inlogmethode zoals multifactorauthenticatie (MFA) helpt bij het opbouwen van vertrouwen.

Datamisbruik is essentieel in vertrouwen

Dat wil niet zeggen dat ethiek er helemaal niet toe doet: 7% van de Nederlandse respondenten noemde ethiek als de belangrijkste factor om vertrouwen te creëren. Ethiek speelt voor consumenten ook een grote rol in de beslissing met welke merken ze geen zaken willen doen, met name op het gebied van “data-ethiek”.

Volgens de Nederlandse respondenten zijn de twee belangrijkste kenmerken die het wantrouwen richting een merk doen toenemen:

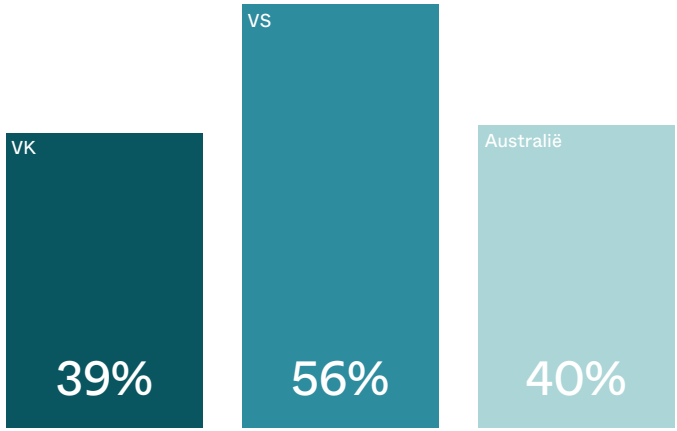
Het opzettelijk misbruiken of verkopen van persoonsgegevens	33%
Datalekken	17%

Beide zaken zijn niet alleen een ethische kwestie voor digitale merken, maar zijn ook in strijd met de privacywetgeving.

Om te ontsnappen aan de ontevredenheid van klanten en een mogelijk grote financiële en reputatieschade, moeten organisaties ervoor zorgen dat hun data goed beveiligd zijn, te beginnen met de beste aanpak voor identity management.

Voor de respondenten in alle andere landen gold het opzettelijk misbruiken of verkopen van data eveneens als de belangrijkste reden om een merk te wantrouwen. Terwijl datalekken de op een na grootste zorg waren voor respondenten in landen als het Verenigd Koninkrijk (17%), Australië (16%), de VS (15%) waren storingen of fouten een belangrijkere factor in het schenden van vertrouwen voor respondenten in Frankrijk (23%), Spanje (21%) en Zweden (16%).

Hieruit blijkt dat, hoewel data-ethiek van het grootste belang blijft, een perfecte klantenservice niet uit het oog mag worden verloren.



Percentage van respondenten die vertrouwen hebben verloren in een bedrijf ten gevolge van een datalek of vergelijkbaar incident.

Wanneer het vertrouwen wordt geschonden

Het is duidelijk dat vertrouwen van vitaal belang is voor digitale merken om te slagen in het huidige, zeer competitieve, businesslandschap.

66% van de Nederlandse respondenten zegt dat ze waarschijnlijk geen aankoop zouden doen bij een bedrijf dat ze niet vertrouwen.

Als merken het vertrouwen eenmaal hebben gewonnen, moeten ze ongetwijfeld hard werken om dit te behouden, waarbij effectieve cyber security een essentiële rol speelt.

Meer dan een kwart (26%) van de Nederlandse respondenten zegt het vertrouwen in een organisatie te hebben verloren als gevolg van een datalek of iets dergelijks. Dit percentage is nog hoger in de VS (56%) en Australië (40%).

Na zo’n gebeurtenis stopte bijna een derde (29%) van Nederlandse gebruikers definitief met de dienstverlening van de organisatie en 37% verwijderde zijn of haar account bij de organisatie. Een nog groter aantal (39%) veranderde gebruikersinstellingen als wachtwoorden en e-mailadressen, waaruit het belang van veilige log-ins voor een blijvend vertrouwen blijkt.

Onder de Nederlandse respondenten hadden de jongeren opmerkelijk minder begrip voor slechte dataverwerking en -beveiliging bij de merken waarbij zij kochten. Zo’n 56% van de 18- tot 24-jarigen zegt na een inbreuk geen vertrouwen meer te hebben in de diensten van een organisatie, tegenover 26% van alle Nederlandse respondenten en slechts 11% van de oudste groep respondenten.

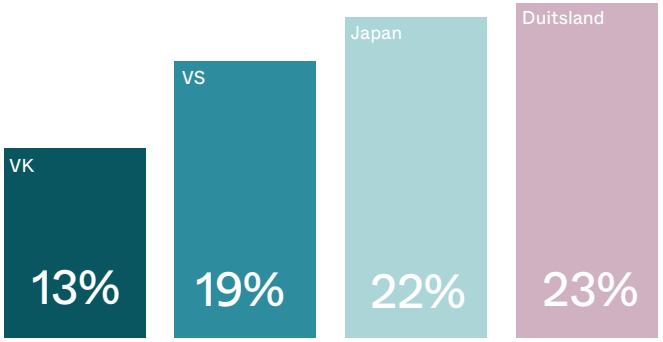
35% gaf aan dat ze geen aankoop zullen doen als het een onbekende website betreft.

Aangezien deze jongere generaties de drijvende kracht achter de toekomstige economie zijn, moeten organisaties ervoor zorgen dat hun professionals kunnen voldoen aan deze hogere verwachtingen op het gebied van cyber security.

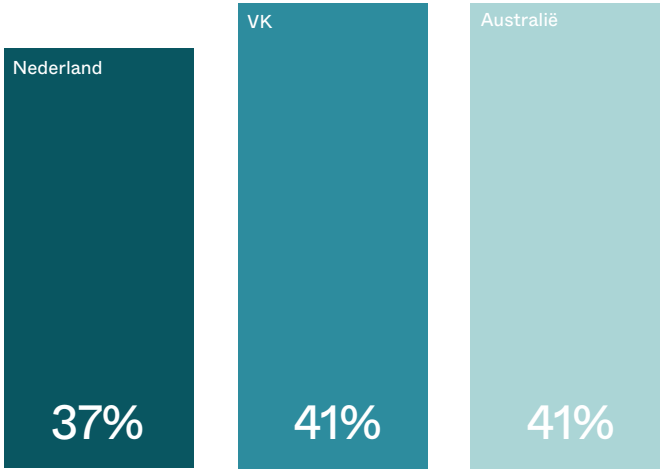
> Jongere generaties zullen de besluitvormers van de toekomst worden. Het is dus belangrijk om voorbereidingen te treffen en ervoor te zorgen dat goede service en cyber security centraal staan in de bedrijfsvoering met als doel de behoeften van de klant af te stemmen op de professionals.
>
> Walter Geers, Regional director Northern Europe, Okta

Werk aan de winkel

Er is nog veel te doen. Een significante minderheid van de respondenten (9%) gaf aan dat ze geen enkel digitaal kanaal vertrouwen als het gaat om veilig beheer van hun data, maar dat percentage was nog hoger in Duitsland (23%), Japan (22%) en de VS (19%). Bovendien werd duidelijk dat apps voor zakelijke communicatie (10%) met meer vertrouwen worden gebruikt dan persoonlijke apps (6%).



Percentage van respondenten dat geen enkel digitaal kanaal vertrouwt in de omgang met hun data.



Percentage van respondenten dat websites van de overheid het meest betrouwbaar acht.

Van alle digitale kanalen in Nederland werden websites van de overheid het meest betrouwbaar geacht (37%), vergelijkbaar met Australië (41%) en het Verenigd Koninkrijk (41%).

> Het is geweldig dat mensen websites van de overheid boven elk ander digitaal kanaal vertrouwen als het gaat om de verwerking van hun gegevens. Het is belangrijk dat de overheid prioriteit blijft geven aan cyber security-maatregelen en de beveiliging van persoonsgegevens.
>
> Dr. Jessica Barker

Deel Twee

Hoe de pandemie het gedrag van gebruikers heeft veranderd

44% van de Nederlandse respondenten zegt tegenwoordig “altijd” of “vaak” thuis te werken, en diezelfde werknemers zullen meer flexibiliteit in het thuiswerk-beleid eisen zodra de crisis voorbij is.

Maar terwijl ze thuis werken, worden velen blootgesteld aan een toename van cyberbedreigingen die erop gericht zijn zowel hun bedrijfslogins als persoonlijke identiteitsgegevens te stelen.

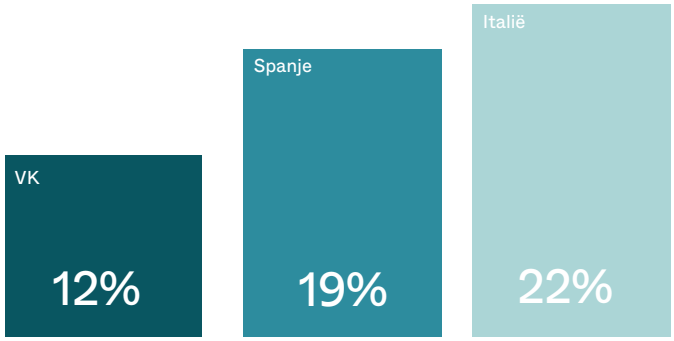
Phishing is gedurende 2020 de favoriete tactiek van veel cybercriminelen geworden. Phishing-e-mails waren vooral succesvol als ze informatie over COVID-19-vaccins of als ze dringende (maar vervalste) updates van betrouwbare instellingen beloofden en zo probeerden ontvangers te verleiden om te klikken. In april werden door alleen al Google dagelijks 18 miljoen malware- en phishing-e-mails die verband hielden met COVID-19 geblokkeerd.

Misschien is het is dan ook niet verrassend dat 47% van de Nederlandse respondenten zegt voorzichtiger te zijn geworden met het online verstrekken van persoonlijke informatie over zichzelf, terwijl slechts 1% zegt daar nu minder huiverig voor te zijn.

Het thuiswerken heeft de respondenten ook bezorgder gemaakt voor phishing-e-mails (43%), datalekken (42%) en zelfs door AI gegenereerde “deepfakes” die worden gebruikt om valse informatie te verspreiden (41%).

23% van de respondenten denkt in de toekomst het meeste risico te lopen op identiteitsdiefstal, wat begrijpelijk is gezien de toename van phishing-aanvallen die velen ook zelf hebben ervaren.

Phishing (18%) en gegevensdiefstal (12%) maken de top drie compleet.



Percentage van respondenten dat zich zorgen maakt over wachtwoorddiefstal.

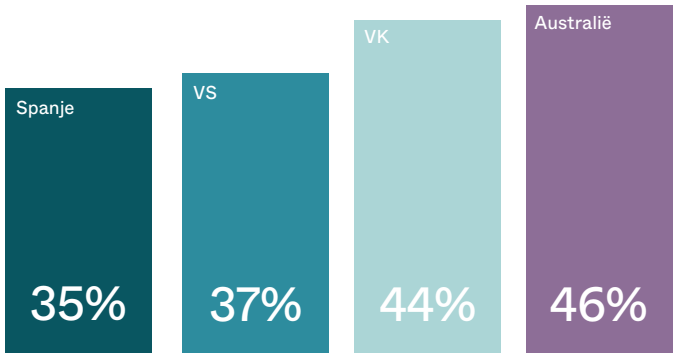
Respondenten in Nederland (11%) maakten zich enigszins zorgen over diefstal van wachtwoorden, maar kantoormedewerkers in Italië (22%) en Spanje (19%) voelden zich hier aanzienlijk meer door bedreigd. Dit toont aan dat de reis naar wachtwoordloze authenticatie alleen maar noodzakelijker zal worden.

We moeten ons realiseren dat een individu niet alleen kan worden blootgesteld aan cyberdreigingen door gerichte aanvallen op zichzelf en zijn devices, maar ook door huisgenoten met online risicovol gedrag.

> “Het dreigingsprofiel bij thuiswerken is om meerdere, complementaire redenen verhoogd. Mensen zijn devices en thuisnetwerken gaan delen, evenals fysieke ruimten. Hierdoor nemen de risico’s toe en komen geschreven documenten en vertrouwelijke telefoongesprekken in gevaar. De huidige ‘collega’s’ kunnen variëren van vertrouwde familieleden tot nauwelijks bekende huisgenoten, terwijl de zekerheid van beschikbare collega’s en een IT-helpdesk wegvalt. Daar komt nog bij dat de gedrags- en veiligheidsmentaliteit die werknemers voorheen aannamen, onbewust in het gedrang kan komen als ze moeten jongleren tussen werk en privé.
>
> Ben King, CSO EMEA, Okta

Tijd voor transparantie

De voornaamste reden die Nederlandse respondenten aangaven voor hun toegenomen voorzichtigheid online tijdens de pandemie was berichtgeving over online bedreigingen in de media (32%), idem voor respondenten in Australië (46%), de VS (37%) en Spanje (35%).



Percentage van respondenten dat aangeeft dat media-aandacht over bedreigingen hun voorzichtigheid online tijdens de pandemie heeft verhoogd.

Hoewel het goed is om te zien dat journalisten hun steentje bijdragen aan de voorlichting van het publiek, ligt hier een duidelijke kans voor digitale organisaties om een grotere rol te spelen bij het vergroten van het bewustzijn voor klanten en om zo relaties op te bouwen. Door naast bewustwording in te zetten op multifactorauthenticatie (MFA) kunnen organisaties meer zekerheid bieden aan bezorgde consumenten, wat de inkomsten en het concurrentievoordeel ten goede komt.

Ook voor werkgevers is hier een rol weggelegd. Door niet alleen het bewustzijn te vergroten, maar ook verouderde technologie, die kwetsbaar kan zijn voor online bedreigingen, te vervangen en de effectiviteit van beveiligingsmaatregelen als end-point anti-malware aan te tonen, kunnen ze werknemers het vertrouwen geven dat ze thuis net zo goed beschermd zijn als op kantoor.

Het vergroten van het vertrouwen in de tools die werknemers gebruiken voor thuiswerken zal uiteindelijk de productiviteit ten goede komen.

Deel Drie

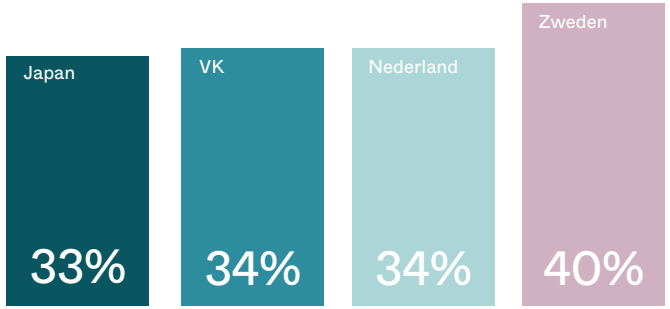
Wat doen organisaties hiermee?

Veel werkgevers hebben stappen ondernomen om hun thuiswerkers te beschermen tegen de toename van cyberdreigingen. Nieuwe beveiligingstoepassingen en -technologieën, zoals MFA (29%), waren de populairste maatregelen, gevolgd door betere opleidingen voor personeel (24%). Beide zijn van cruciaal belang voor het vergroten van het vertrouwen van werknemers.

Zorgwekkend is echter het feit dat 22% van de respondenten aangeeft dat zijn werkgever tot nu toe niets heeft gedaan om een pandemie-gerelateerde toename van online bedreigingen te bestrijden. Dit percentage is nog hoger in de vastgoedsector (52%), media en marketing (36%) en kunst en amusement (36%).

> “
>
> In bedrijfstakken die niet zo digitaal ingesteld zijn, werken werknemers vaak met minder geavanceerde technologie, waardoor ze misschien niet nadenken over maatregelen die worden genomen om online risico’s te bestrijden. Zij die van oudsher met hogere niveaus van cyberdreiging te maken hebben, zoals banken, technologie en detailhandel, hebben waarschijnlijk ook een proportioneel groter beveiligingsbudget dan andere sectoren.
>
> In alle sectoren hebben CIO’s en CSO’s hun tijd moeten verdelen tussen het ondersteunen van sectorspecifieke behoeften en beveiligingseisen, vaak twee zeer verschillende taken.
>
> Ben King, CSO EMEA, Okta

Bovendien geeft meer dan een derde (34%) van de Nederlandse kantoormedewerkers aan dat ze niet zeker weten of hun werkgever proactieve beveiligingsmaatregelen heeft genomen, net als in Zweden (40%), het Verenigd Koninkrijk (34%) en Japan (33%).
Dit is een gemiste kans, omdat het wijst op een gebrek aan transparantie tussen business- en IT-leiders en hun werknemers. Je kunt de beste cyberbeveiligingssystemen ter wereld hebben, maar als het personeel er niet van op de hoogte is, zal je organisatie niet in staat zijn om meer vertrouwen rondom werknemers te creëren.



Percentage van respondenten dat niet wist of zijn werkgever maatregelen had genomen om de beveiliging aan te scherpen.

> Cybercriminelen leren altijd nieuwe trucjes, zoals veel werknemers weten. Veel werknemers zijn op hun hoede voor phishing, datalekken en nieuwe risico's zoals deepfake fraudes. Bedrijven moeten er daarom voor zorgen dat zij op dit gebied zo veel mogelijk voorop blijven lopen en deze nieuwe bedreigingen steeds weer met een nieuwe aanpak bestrijden.
>
> Ben King, CSO EMEA, Okta

Het is duidelijk dat IT-leiders in 2021 moeten beginnen met het uitrollen van waterdichte, risicogerelateerde oplossingen voor identity management om digitaal vertrouwen te stimuleren, om de productiviteit van het personeel te verhogen en internetrisico's tot een minimum te beperken. Verder moeten ze meer transparantie bieden over alle nieuwe technologieën en het door hen te ondersteunen beveiligingsbeleid.

Deel Vier

Conclusie en aanbevelingen

IDC[1] definieert vertrouwen als de voorwaarde voor het nemen van beslissingen tussen twee of meer entiteiten, gebaseerd op hun onderlinge relatie. Daarnaast is het een "verbetering van het onderwerp 'beveiliging' met attributen zoals risico, compliance, privacy en zelfs bedrijfsethiek".

Het is een concept dat geen enkele IT- of businessleider vandaag de dag nog kan negeren, aangezien de digitale transformatie niet alleen cyberaanvallen vergroot, maar ook nieuwe kanalen biedt om klanten en medewerkers te ondersteunen. Als het vertrouwen is gewonnen, kan dit niet alleen schade beperken maar ook inkomsten voor organisaties verhogen.

In organisaties begint dit met een Zero Trust-benadering, gericht op identity met als ultiem doel een op risico gebaseerd access management, herhaaldelijke en flexibele authenticatie en probleemloze toegang.

De pandemie heeft de behoefte aan een dergelijke aanpak versneld. Organisaties moeten erop kunnen vertrouwen dat hun externe gebruikers werkelijk zijn wie ze zeggen dat ze zijn, aangezien bedriegers in steeds groteren getale proberen te infiltreren in bedrijfsnetwerken. Het is daarnaast ook nodig om het vertrouwen van werknemers te bevorderen, zodat zij productiever kunnen werken.

Het begrip vertrouwen strekt zich ook uit tot interacties met klanten. Als verantwoordelijke beheerders van klantdata moeten de digital-first organisaties van vandaag dat vertrouwen voortdurend koesteren.

Op die manier worden loyaliteit en succes gestimuleerd, zelfs nu data- en identity-dieven hun inspanningen tijdens de pandemie hebben opgevoerd. Ook in deze context begint vertrouwen met security, met identity als centrale pijler. Dat betekent dat digitale merken hun klanten moeten voorzien van de tools die ze nodig hebben om zich probleemloos en veilig te authentiseren.

[1] IDC Perspective, 2020, Future of Trust: Defining Trust, April 2020, #US46185920

Samenvatting van de belangrijkste aanbevelingen:

Business-/IT-leiders moeten transparant zijn naar thuiswerkende werknemers over de cyberbeveiligingsmaatregelen en het beleid dat ze implementeren, om zo het vertrouwen en de betrokkenheid van het personeel te bevorderen.

Nieuwe beveiligingstools zoals MFA en biometrie voor authenticatie zonder wachtwoord zijn van vitaal belang voor de bescherming tegen diefstal van identiteitsgegevens van consumenten en de beveiliging van externe toegang voor werknemers.

Meer interne training over bescherming tegen phishing en best practices op het gebied van beveiliging zijn nodig om de risico's van remote werken te beperken.

Houd uw beveiligingsstrategie up-to-date om ervoor te zorgen dat deze zich aanpast aan het veranderende bedreigingslandschap, de wettelijke risico's en de houding ten opzichte van vertrouwen.

Toon de effectiviteit van beveiligingsmaatregelen aan thuiswerkers aan, zodat zij erop kunnen vertrouwen dat ze thuis net zo goed beschermd zijn als op kantoor.

Overheden en digitale diensten moeten prioriteit geven aan maatregelen op het gebied van cyber security en privacy om de data van burgers veilig te houden tijdens de pandemie, en tijdens het nieuwe normaal.

De ethiek rondom data is belangrijk voor klanten, dus bedrijven moeten ervoor zorgen dat ze zich aan de regelgeving houden, misbruik voorkomen, risico op inbreuk verkleinen en zo aan de verwachtingen van de consument voldoen.

Zorg ervoor dat uw organisatie voldoet aan de hogere beveiligings- en privacyverwachtingen van jongere consumenten, om de loyaliteit van een in economisch opzicht belangrijke groep te bevorderen.

Deel Vijf

Het beveiligen van de onderneming van de toekomst met Okta

Identity is de basis om op vertrouwen gebaseerde, veilige organisaties te bouwen. Met de Okta Identity Cloud kunnen businessleiders wereldwijd vol vertrouwen de beste digitale ervaringen creëren voor hun werknemers en klanten.

Beveilig uw medewerkers - waar ze ook zijn - met **Okta's oplossingen voor workforce identity**. Krijg de tools om cloud journeys te beveiligen en automatiseren, met volledige ondersteuning voor hybride omgevingen.

Gebruik **Okta's customer identity-oplossingen** om veilige, naadloze klantervaringen op te bouwen die de verwachtingen van uw developers en gebruikers overtreffen.

Over Okta

Okta is de toonaangevende onafhankelijke aanbieder van identity voor de business. De Okta Identity Cloud maakt het voor organisaties mogelijk om op een veilige manier de juiste mensen op het juiste moment met de juiste technologieën te verbinden. Met meer dan 6.500 vooraf gebouwde integraties met applicaties en infrastructuuraanbieders kunnen Okta-klanten eenvoudig en veilig gebruik maken van de beste technologieën voor hun organisatie. Meer dan 9.400 organisaties, waaronder Just Eat Takeaway.com, Mazars, De Belgische Voetbalbond, Siemens, T-Mobile en Oxfam vertrouwen op Okta om de identiteit van hun werknemers en klanten te helpen beschermen.

Okta.com

okta