

STATE OF DIGITAL TRUST

PILLARS OF TRUST

C-LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE

1245.54°
753234.72°

IDENTITY

AUTOMATION

433.6°
24567.76°

ID 7021.4

THREATS

XX
SECURITY ALERT

ZERO TRUST

ENTERPRISES
EMPLOYEES
CUSTOMERS

6578.854°
6785.77°

GLOBAL STUDY

NOVEMBER 2022

digicert®

ONDERZOEKSRAPPORT DIGITAAL VERTROUWEN 2022

De interactie tussen mensen vindt in toenemende mate plaats via digitale kanalen in een wereld waarin alles non-stop met elkaar is verbonden. Dit is het gevolg van de digitale transformatie, maar ook van de pandemie. Hoe zorgen we voor vertrouwen in deze nieuwe wereld? We zoeken naar antwoorden op de volgende vragen:

- Hoe weten we of de mensen (en apparaten) waarmee we verbinding maken legitiem zijn?
- Hoe weten we of de gegevens die we gebruiken veilig zijn?
- Hoe zorgen we ervoor dat we goed zijn beveiligd en niet het slachtoffer worden van een cyberaanval?
- Hoe weten we of de applicaties en services die we gebruiken niet zijn gecompromitteerd?

Dit is allemaal niet makkelijk. Deze nieuwe wereld kent vele nieuwe kwetsbaarheden en de kosten van een gebrekkige beveiliging kunnen enorm oplopen. Want naast de kosten voor juridische procedures, eventuele boetes en herstelactiviteiten, zitten de hoogste kosten waarschijnlijk in het verlies van klantloyaliteit en het vertrouwen in een merk. Onderzoek van Forbes Insights heeft aangetoond dat bijna de helft (46%) van alle organisaties reputatie- en merkschade heeft geleden als gevolg van een inbreuk op de beveiliging door een buitenstaander¹.

Dit heeft de kwestie digitaal vertrouwen voor het voetlicht gebracht. Volgens Jennifer Glenn, Research Director van IDC, is digitaal vertrouwen de basis van het beveiligen van de online wereld. Het is bovendien onmisbaar voor organisaties die hun klanten, medewerkers en partners het vertrouwen willen bieden dat online bedrijfsprocessen en interacties veilig zijn.

In feite biedt digitaal vertrouwen de vrijheid om volledig deel te nemen aan de digitale wereld.

DigiCert is de wereldwijd toonaangevende leverancier van digitaal vertrouwen, die zowel individuen als bedrijven het vertrouwen biedt dat hun online aanwezigheid is beveiligd. Daarom heeft DigiCert er belang bij om te weten hoe organisaties over de hele wereld digitaal vertrouwen zien en hoever ze gevorderd zijn met het bieden ervan.

In Digitaal vertrouwen: de stand van zaken in 2022 onderzoekt DigiCert waar ter wereld bedrijven, medewerkers en consumenten digitaal vertrouwen al hebben omarmd.

¹The Reputational Impact of IT Risk – Forbes Insights

Wat is digitaal vertrouwen?

Volgens Jennifer Glenn, Research Director van IDC, is digitaal vertrouwen de basis voor het beveiligen van de onlinewereld. Het is bovendien onmisbaar voor organisaties die hun klanten, medewerkers en partners het vertrouwen willen bieden dat online bedrijfsprocessen en interacties veilig zijn.

Het fundament onder digitaal vertrouwen bestaat uit vier hoofdelementen:

1. Normen die definiëren wat vertrouwen inhoudt voor een bepaalde technologie of bedrijfstak.
2. Compliance en uitvoering voor het genereren of verifiëren van digitale certificaten waarmee vertrouwen wordt gewekt (op basis van

identiteit, integriteit en encryptie), met de garantie dat deze certificaten voldoen aan de vereisten van de normalisatie-instituten.

3. Vertrouwensbeheer om ervoor te zorgen dat bedrijven de levenscyclus van hun certificaten goed beheren en het beheer en de zichtbaarheid ervan hebben gecentraliseerd.
4. Vertrouwensketens die zorgen voor vertrouwen in complexe aanvoerketens voor bijvoorbeeld software, apparaten en content.

Digitaal vertrouwen is afgeleid van deze vier essentiële onderdelen. Bedrijven kunnen vertrouwen op derden om deze activiteiten te beheren, of ze zelf intern regelen.

'Digitaal
vertrouwen is de
basis voor het
beveiligen van de
onlinewereld.'

— Jennifer Glenn,
Research Director, IDC



HET BELANG VAN DIGITAAL VERTROUWEN

Dat er behoefte is aan digitaal vertrouwen wordt duidelijk uit de antwoorden van de deelnemers aan het onderzoek: 100% van de ondernemingen vindt digitaal vertrouwen belangrijk en de meeste bedrijven (90%) vinden het zelfs zeer belangrijk. Zo belangrijk zelfs dat bijna twee derde van hen wel eens is overgestapt naar een andere leverancier nadat ze het vertrouwen in hun oorspronkelijke leverancier hadden verloren. En vrijwel alle bedrijven (99%) denken dat als ze het vertrouwen van hun klanten kwijtraken, die klanten mogelijk overstappen naar de concurrent. Bijna de helft (47%) denkt dat zo'n overstap waarschijnlijk is.

Ook werknemers van de bedrijven zetten in op digitaal vertrouwen: 100% van hen zegt dat het belangrijk is, en 86% vindt digitaal vertrouwen zeer belangrijk. In hun rol binnen het bedrijf zou 99% van de werknemers overwegen om over te stappen naar een andere leverancier na een vertrouwensbreuk, en volgens ongeveer de helft (51%) zou die overstap 'waarschijnlijk' zijn.

Ten slotte vindt 68% van de consumenten digitaal vertrouwen belangrijk, en vindt een derde van hen (36%) het zeer belangrijk. Sterker nog, bijna de helft (47%) van de consumenten doet al geen zaken meer met een bedrijf waarin ze hun vertrouwen hebben verloren. Vooruitkijkend zou 84% een overstap overwegen en zou 57% dat waarschijnlijk doen. Opmerkelijk hierbij is dat hoe welvarender de consumenten zijn, hoe belangrijker ze digitaal vertrouwen vinden (58% van de consumenten met een bovenmodaal inkomen vindt digitaal vertrouwen belangrijk).

Werkwijze

Het onderzoek werd in september 2022 uitgevoerd door het in Dallas gevestigde Eleven Research. Het onderzoek werd telefonisch en per e-mail uitgevoerd onder 400 bedrijven en 400 consumenten over de hele wereld.

Ondernemingen

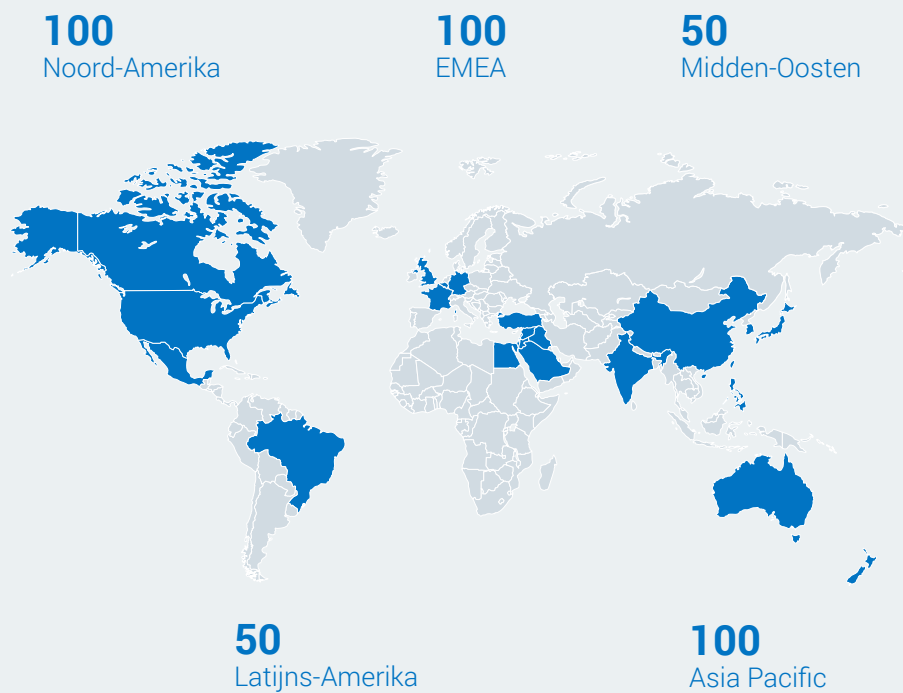
De ondervraagde deelnemers waren 400 senior en corporate managers van de afdelingen IT, Informatiebeveiliging en DevOps binnen bedrijven met minimaal 1000 werknemers. Wereldwijd waren de aantallen zoals te zien in afbeelding A op pagina 5.

Consumenten

Het onderzoek werd uitgevoerd onder 400 consumenten (m/v) wereldwijd (uit dezelfde regio's), uit verschillende leeftijdscategorieën en inkomensgroepen en met verschillende politieke voorkeuren: afbeelding B (zie p. 5).

'99% van de werknemers zou overwegen om over te stappen naar een andere leverancier na het verlies van digitaal vertrouwen.'





Afbeelding A.

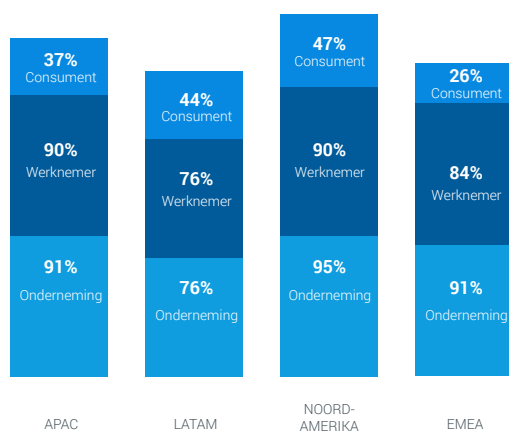


Afbeelding B.

HET BELANG DAT MENSEN STELLEN IN DIGITAAL VERTROUWEN VERSCHILT

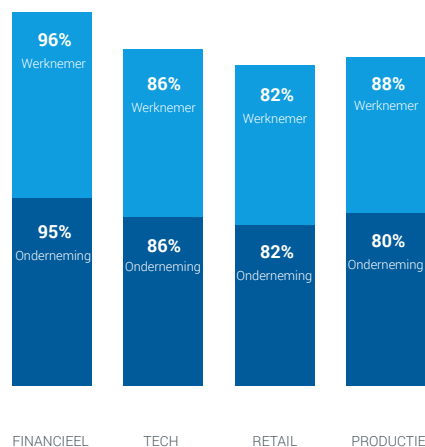
Bedrijven, werknemers en consumenten vinden digitaal vertrouwen allemaal belangrijk, maar de mate waarin is afhankelijk van diverse factoren.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER REGIO



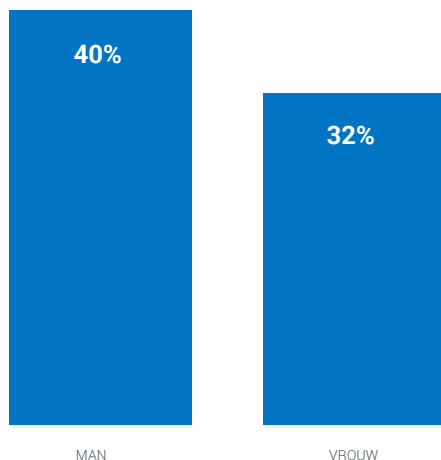
Het aantal bedrijven en werknemers dat digitaal vertrouwen zeer belangrijk vindt, is in Latijns-Amerika lager dan in de rest van de wereld. Bij consumenten lopen APAC en EMEA achter op de rest. Het feit dat 26% van de consumenten in EMEA vindt dat digitaal vertrouwen zeer belangrijk is, is verrassend gezien de invoering van de vrij strikte AVG in 2018.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER BEDRIJFSTAK



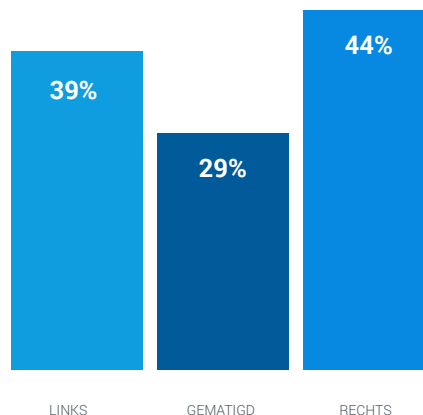
Het is niet verrassend dat financiële dienstverleners het meest geneigd zijn om digitaal vertrouwen zeer belangrijk te vinden.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER GESLACHT (CONSUMENTEN)



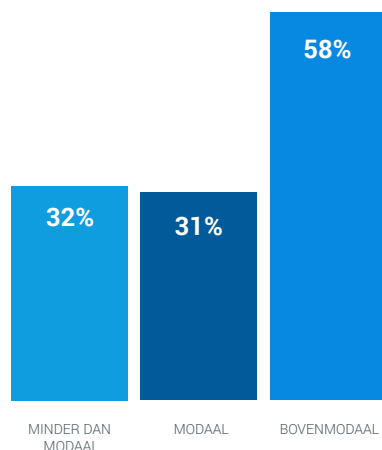
Onder consumenten vinden mannen digitaal vertrouwen belangrijker dan vrouwen.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER POLITIEKE VOORKEUR (CONSUMENTEN)



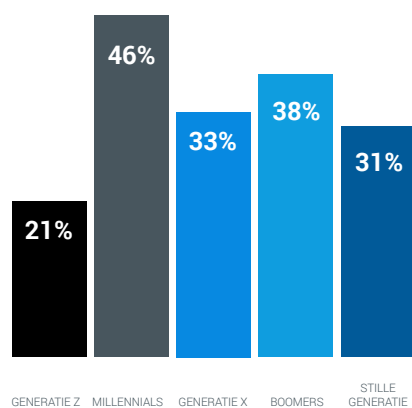
En eindelijk hebben we een onderwerp waar alle politici het over eens zijn! Alle kanten van het politieke spectrum vinden digitaal vertrouwen zeer belangrijk.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER INKOMENSGROEP (CONSUMENTEN)



Ook kennen consumenten met een bovenmodaal inkomen digitaal vertrouwen meer belang toe.

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER GENERATIE (CONSUMENTEN)



Het is interessant om te zien dat de twee jongste generaties (en de enige digital natives) zowel het minst als het meest geneigd zijn om digitaal vertrouwen zeer belangrijk te vinden.

WAAR KOMT DE INTERESSE IN DIGITAAL VERTROUWEN VANDAAN?

Er is dus een universele interesse in digitaal vertrouwen. Maar waarom eigenlijk? Waar komt die interesse vandaan? We hebben uiteenlopende factoren gevonden.

Het toenemende belang van gegevens. Volgens de respondenten is dit de belangrijkste stimulerende factor. Dit komt doordat de hoeveelheid gegevens jaarlijks met 23% stijgt.² Tot eind 2021 had het de mensheid 70 jaar gekost om 97 zettabytes aan gegevens te verzamelen. In 2025, dus slechts vier jaar daarna, zal deze hoeveelheid zijn verdubbeld tot 174 zettabytes. Dat betekent dat er in 2025 meer dan 20.000 gigabytes voor iedere persoon op aarde zal zijn!

Het gaat echter niet alleen om de hoeveelheid, maar ook om het belang van de gegevens. Die omvatten namelijk een schat aan persoonlijk identificeerbare informatie, zoals wat we kopen, welke sites we bezoeken, patiëntendossiers, socialemediaberichten, vakantiefoto's en nog veel en veel meer.

Een toenemend aantal doelwitten. Binnen bedrijven zijn de relatief statische netwerken met datacenters, hoofdkantoren en buitenlandse vestigingen veranderd in zeer complexe en hybride netwerken. Deze nieuwe netwerken vormen de schakel tussen datacenters, hoofdkantoren en andere vestigingen, maar omvatten tegenwoordig ook duizenden thuiswerkplekken, meerdere clouds, digitale apparaten, edge-netwerken en IoT-apparatuur.

In deze vrijwel onbegrensde netwerken is het aantal doelwitten vele malen groter.

Verwachtingen van klanten. Zoals we in het vorige gedeelte hebben gelezen, vindt 100% van de bedrijven en 68% van de consumenten digitaal vertrouwen belangrijk. Allemaal stappen ze waarschijnlijk over naar een concurrent als ze hun vertrouwen in een bedrijf verliezen. Daarmee is digitaal vertrouwen vitaal geworden voor bedrijven.

Toenemende aantallen kwaadwillenden. Het aantal personen dat iets slechts in de zin heeft, neemt elk jaar toe. Dit zijn:

- Black hat hackers
- Cybercriminelen
- Cyberterroristen
- Hacktivisten
- Interne kwaadwillenden
- Staatshackers
- Sensatiezoekers en trollen

Het bewijs van deze stijging is het recordaantal klachten dat in 2021 binnenkwam bij de IC3: 847.376 geregistreerde klachten, een stijging van 7% ten opzichte van 2020.³



²Big Growth Forecasted for Big Data – IDC

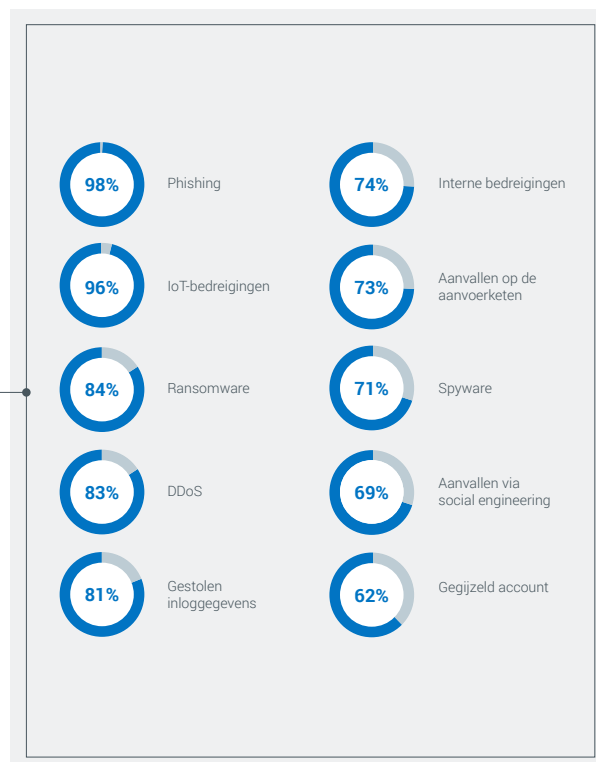
³FBI Internet Crime Complaint Center (IC3)

WAT STAAT ER OP HET SPEL?

Wat moeten bedrijven beschermen? 100% van de bedrijven gaf aan klantloyaliteit belangrijk te vinden. Dit is logisch als je bedenkt hoe waarschijnlijk het is dat klanten overstappen naar een ander als ze het vertrouwen in een bedrijf verliezen.

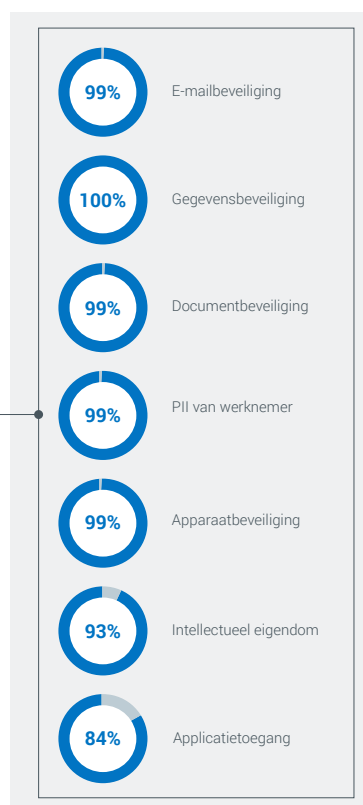
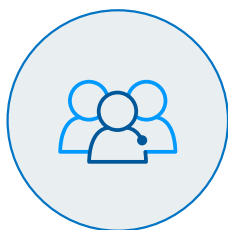
Dit zijn de soorten aanvallen waarover de respondenten zich het meeste zorgen maken (op volgorde van belangrijkheid):

VOOR ONDERNEMINGEN...



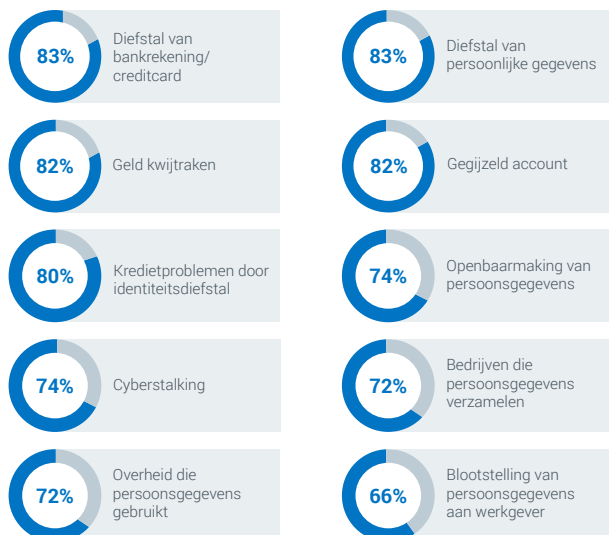
Werknemers maken zich vooral zorgen over hun persoonsgegevens.

VOOR WERKNEMERS...



Bij consumenten gaat het om allerlei onderwerpen:

CONSUMENTEN VREZEN DEZE AANVALLEN...



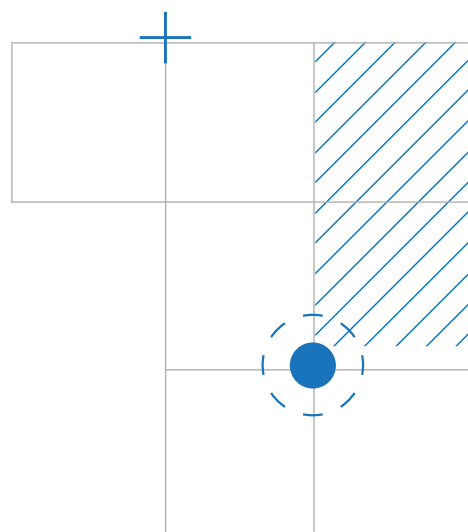
CONSUMENTEN WILLEN BESCHERMING VOOR...



Wij vroegen ons af of bedrijven en consumenten op één lijn zitten voor wat betreft de bescherming van wat consumenten het belangrijkste vinden (wachtwoorden, persoonlijk identificeerbare informatie, enzovoort). Vrijwel alle aanvallen waarbij consumentengegevens op straat komen te liggen, worden geïnitieerd via e-mail.⁴ Maar terwijl bedrijven van alles doen om consumenten te beschermen, staat het beveiligen tegen phishingaanvallen in de praktijk op de een-na-onderste plek. Bovendien wordt phishing genoemd als het soort aanval waarover bedrijven zich het meeste zorgen maken.

Dus hoewel bedrijven zich richten op wat consumenten belangrijk vinden, zullen ze nog het nodige moeten doen voordat ze het door consumenten gewenste niveau aan bescherming bieden.

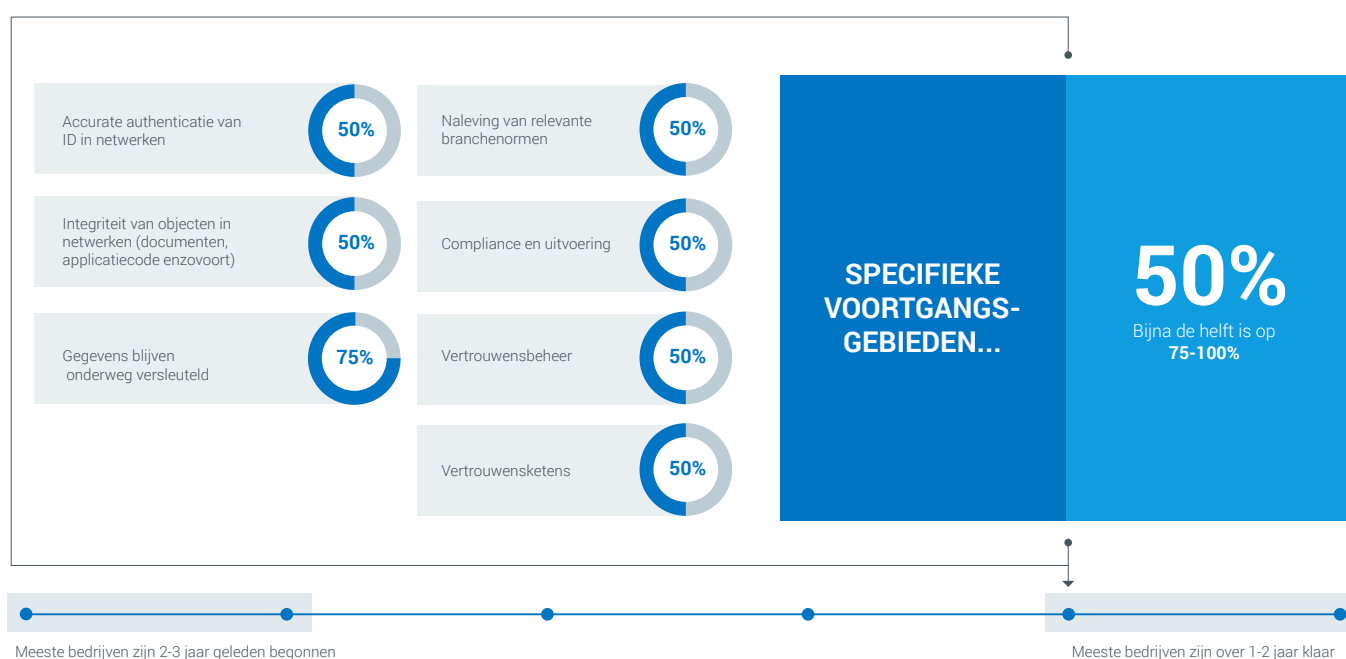
⁴Why Your Business Needs Better Email Security – Guardian Digital



WAT DOEN BEDRIJVEN AAN HET OPTIMALISEREN VAN DIGITAAL VERTROUWEN?

Bedrijven spannen zich in voor digitaal vertrouwen. Veel organisaties zijn twee tot drie jaar geleden begonnen met werken aan digitaal vertrouwen en zijn tot op minimaal 75% van hun doel gevorderd. Ze verwachten over een tot twee jaar klaar te zijn.

Digitaal vertrouwen kent vele aspecten. We hebben onderzocht met welk van deze aspecten bedrijven het verste zijn gevorderd.



Doelstellingen voor digitaal vertrouwen: De ondernemingen gaven duidelijk aan dat de hoogste prioriteit voor digitaal vertrouwen de klantloyaliteit is. 100% van de respondenten noemde dit doel belangrijk, waarmee het boven aan de lijst komt te staan. Maar er waren nog meer doelstellingen.



Uitdagingen voor digitaal vertrouwen:

Ondernemingen zijn al een eind op weg met digitaal vertrouwen, maar dat is niet zonder slag of stoot gegaan. De belangrijkste uitdaging die werd genoemd door de IT was het beheer van digitale certificaten; dat vond 100% van de bedrijven belangrijk. Het naleven van regels en omgaan met de enorme omvang van wat ze moeten beschermen, stond daar direct onder met 99%. De overige uitdagingen waren de complexiteit van het beveiligen van een omvangrijk en dynamisch netwerk met apparatuur van vele leveranciers, en het gebrek aan vaardigheden bij werknemers.

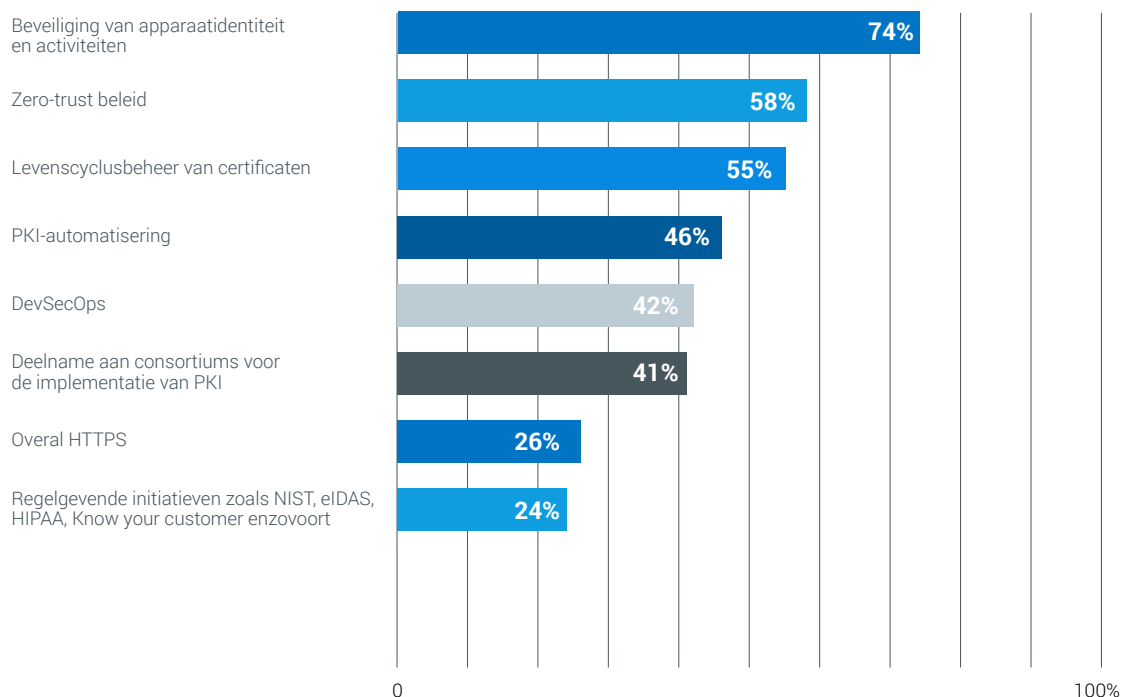


Activiteiten op het gebied van digitaal vertrouwen:

Een breed scala aan initiatieven kan van invloed zijn op het digitaal vertrouwen dat bedrijven wekken. De meeste ondernemingen zijn op zijn minst begonnen met zulke initiatieven, maar het is nuttig om te weten welke daarvan inmiddels volledig zijn geïmplementeerd.

Bovenaan staan apparaatidentiteit en beveiliging van operationele activiteiten, wat volledig is geïmplementeerd bij 74% van de ondernemingen. Zero-trust beleid staat op plaats twee, maar is bij slechts 58% van de bedrijven volledig geïmplementeerd. Het enige andere initiatief dat volledig is geïmplementeerd bij meer dan de helft van de bedrijven (55%) is het levenscyclusbeheer van certificaten. Daarna volgen:

V22: Hoe bent u betrokken bij de volgende activiteiten met betrekking tot digitaal vertrouwen? (Reeds geïmplementeerd)

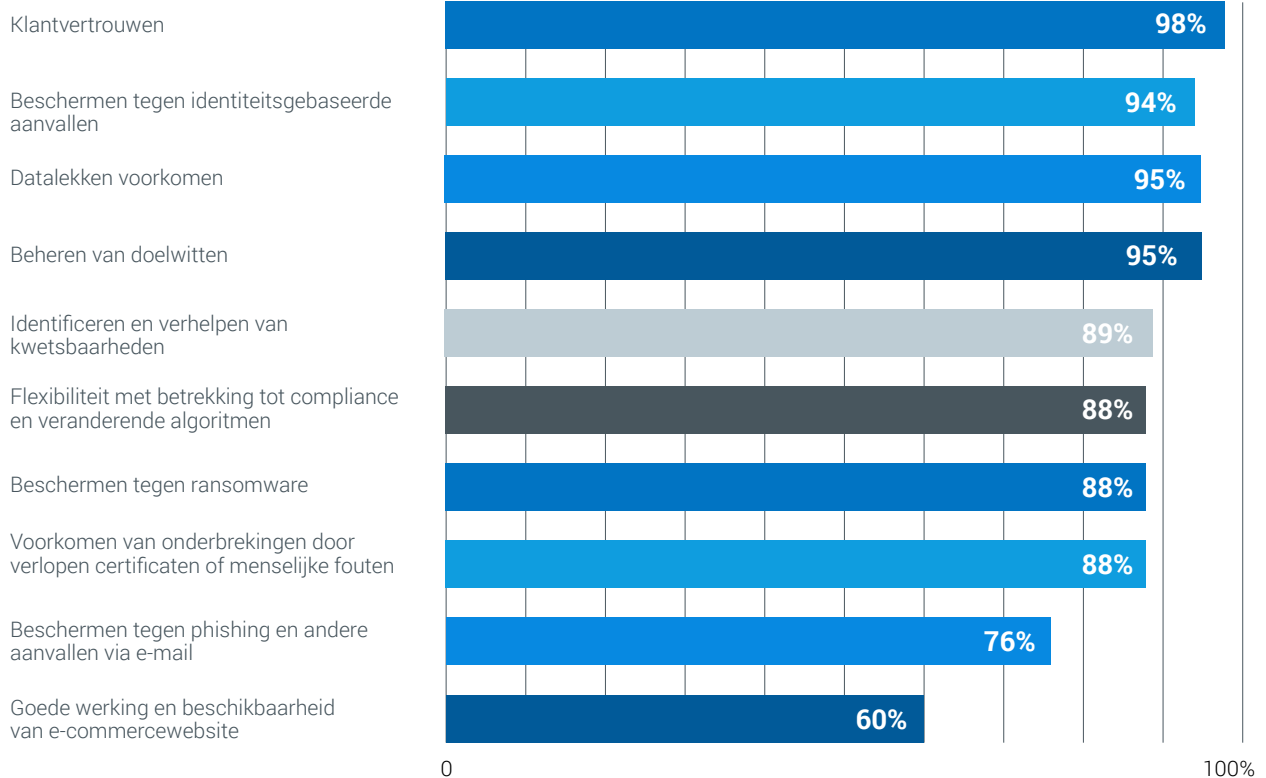


HOE GOED PRESTEREN BEDRIJVEN MET BETREKKING TOT DE MEETGEGEVENS VOOR DIGITAAL VERTROUWEN?

In het geheel genomen doen ondernemingen het vrij goed met betrekking tot diverse meetgegevens voor digitaal vertrouwen. Een voorbeeld daarvan is hun belangrijkste doel, klantvertrouwen. 98% doet het goed op dat gebied; 61% zelfs zeer goed. Ze doen het ook goed op het gebied van het voorkomen van datalekken (95%, met 51% zeer goed) en identiteitsgebaseerde aanvallen (94%, met 50% zeer goed).

Voor acht van de tien meetgegevens die we hebben onderzocht, gaven zeven van de acht bedrijven aan dat ze het goed deden op dat gebied. Alleen het voorkomen van phishing en andere aanvallen via e-mail en de prestaties en beschikbaarheid van e-commercewebsites bleven achter, met respectievelijk 76% en 60%.

V23: Hoe goed presteert u op de volgende gebieden? (Redelijk/zeer goed)



Klanten zien verbetering

Alle bedrijven (100%) gaven aan dat digitaal vertrouwen belangrijk is voor hun klanten, en 91% zei dat hun klanten digitaal vertrouwen zelfs zeer belangrijk vinden.

Dus is het cruciaal om te inventariseren hoe consumenten hun digitale vertrouwen ervaren. Vanuit het perspectief van de ondernemingen ziet het er goed uit: 99% van de ondernemingen zegt dat hun klanten meer vertrouwen hebben in het door hen geboden digitaal vertrouwen dan in het verleden. Bijna 73% zegt dat het vertrouwen zelfs aanzienlijk hoger ligt.

Wat vinden de bedrijven daarvan? Zijn die net zo optimistisch als de consumenten? Het blijkt dat de percentages vrijwel identiek zijn. Toen we vroegen hoeveel vertrouwen de ondernemingen hebben in de bedrijven waarmee ze zakendoen, gaf 98% aan dat het vertrouwen was toegenomen, en 76% dat het zelfs aanzienlijk was toegenomen.

Maar dat zijn de cijfers voor B2B. Hoe zit het met B2C? Hier zijn de cijfers toch wat minder optimistisch. Minder dan de helft gaf aan dat hun digitaal vertrouwen in de organisaties waarvan ze klant zijn was gestegen ten opzichte van het verleden, en 54% zei dat er nog ruimte was voor verbetering.

'91% van de klanten beschouwt digitaal vertrouwen als zeer belangrijk.'



Resultaten Noord-Amerika

Noord-Amerika (de VS en Canada) is wereldwijd koploper voor wat betreft het aantal respondenten dat digitaal vertrouwen zeer belangrijk vindt. Dit geldt voor bedrijven, werknemers en consumenten.

Opmerkelijk is dat Noord-Amerikaanse consumenten zich meer zorgen maken over cyberbedreigingen (zoals het hacken van bankrekeningen of creditcards en kwijtraken van hun geld) dan consumenten in de rest van de wereld, behalve in de regio Asia Pacific. In APAC is 91% van de consumenten bezorgd over deze bedreigingen, ten opzichte van 85% in Noord-

Amerika en respectievelijk 77% en 78% in EMEA en LATAM.

Dit zie je ook terug in de hoge scores die consumenten toekennen aan Noord-Amerikaanse bedrijven. Wat het succes van digitaal vertrouwen betreft, zegt 31% van de Noord-Amerikaanse consumenten dat ze aanzienlijk meer vertrouwen hebben in de bedrijven waarmee ze zakendoen. Consumenten in APAC zitten in de middenmoot met 19%. In Latijns-Amerika is dit percentage 24% en slechts 19% en 15% in respectievelijk APAC en EMEA.

Resultaten APAC

In het geheel genomen wordt digitaal vertrouwen in de regio APAC gezien als zeer belangrijk. Hier houdt men zich meer bezig met digitaal vertrouwen dan in elke andere regio, afgezien van Noord-Amerika.

Dit komt deels doordat consumenten in deze regio zich meer zorgen maken over cyberbedreigingen (zoals het hacken van bankrekeningen of creditcards en kwijtraken van hun geld) dan consumenten in de rest van de wereld. In APAC is 91% van de consumenten

bezorgd over deze bedreigingen, ten opzichte van 85% in Noord-Amerika en respectievelijk 77% en 78% in EMEA en LATAM.

Wat het succes van digitaal vertrouwen betreft, zegt 19% van de consumenten in APAC dat ze aanzienlijk meer vertrouwen hebben in de bedrijven waarmee ze zakendoen. In Noord-Amerika en Latijns-Amerika is dit percentage respectievelijk 31% en 24%, en in de regio EMEA zelfs maar 15%.

Resultaten LATAM

In zijn algemeenheid blijft Latijns-Amerika achter op de rest van de wereld voor wat betreft de mate waarin digitaal vertrouwen wordt beschouwd als zeer belangrijk.

Dit komt deels doordat consumenten in Latijns-Amerika zich minder zorgen maken over cyberbedreigingen (zoals het hacken van bankrekeningen of creditcards en kwijtraken van hun geld) dan consumenten in de rest van de wereld. In LATAM is slechts 78% van de

consumenten bezorgd over deze bedreigingen, ten opzichte van 91% in APAC, 85% in Noord-Amerika en 77% in EMEA.

Het succes van digitaal vertrouwen in deze regio is relatief hoog: 24% van de consumenten in LATAM zegt aanzienlijk meer vertrouwen te hebben in de bedrijven waarmee ze zakendoen. Ter vergelijking: deze percentages kwamen uit op 31% in Noord-Amerika en 19% en 15% in respectievelijk APAC en EMEA.

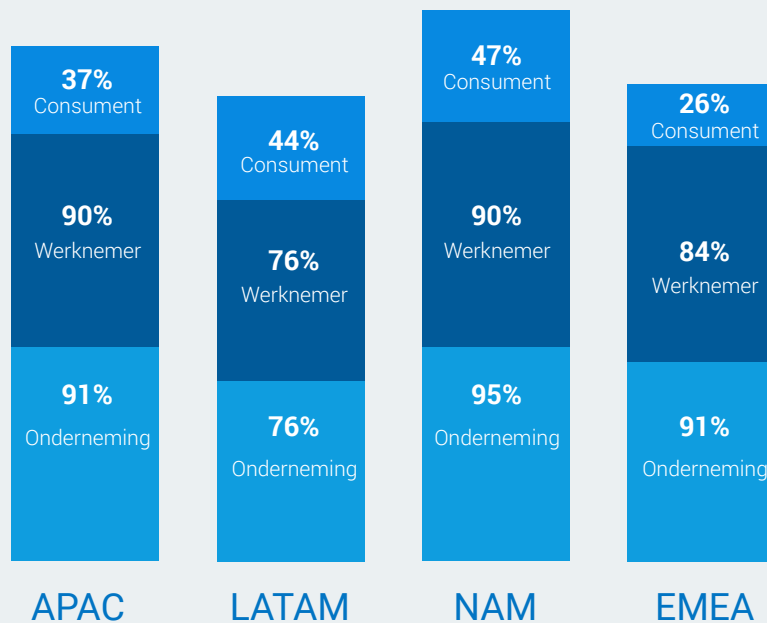
Resultaten EMEA

Voor een regio met een relatief strenge privacywetgeving (AVG) zijn de consumenten in EMEA verrassend blasé wanneer het op digitaal vertrouwen aankomt. Over het geheel genomen staat EMEA op de derde plaats voor wat betreft de mate waarin digitaal vertrouwen wordt gezien als zeer belangrijk. Maar bij het beter bestuderen van de gegevens wordt duidelijk dat de ondernemingen in EMEA er veel belang aan toekennen, en werknemers het gemiddeld belangrijk vinden. Het aantal consumenten dat digitaal vertrouwen als zeer belangrijk beschouwd, is ongeveer de helft van dat van Noord-Amerika.

Dit komt overeen met de zorgen over cyberbedreigingen. Consumenten in EMEA maken zich het minste zorgen over cyberbedreigingen zoals het hacken van bankrekeningen of creditcards en het kwijtraken van geld. Slechts 77% van de consumenten in EMEA maakt zich hier zorgen over, in vergelijking met 78% in LATAM, 85% in Noord-Amerika en 91% in APAC.

Dit past ook bij het relatief lage percentage EMEA-consumenten die zeggen dat hun vertrouwen in de bedrijven waarmee ze zakendoen de afgelopen jaren is gestegen (slechts 15%). Daarmee loopt de regio achter op APAC (19%), LATAM (24%) en Noord-Amerika (31%).

DIGITAAL VERTROUWEN BESCHOUWD ALS ZEER BELANGRIJK PER REGIO



WAT WE KUNNEN LEREN VAN DE KOPLOPERS

Zoals we hebben kunnen zien, doen ondernemingen het vrij goed op het gebied van digitaal vertrouwen. Naar aanleiding daarvan wilden we weten of dit voor alle ondernemingen geldt, of dat er typen bedrijven zijn die het veel beter of slechter dan gemiddeld doen.

Hiervoor hebben we hun antwoorden de volgende scores gegeven:

Scoresysteem

- | | |
|--------------------------|----|
| • Zeer slecht | -2 |
| • Redelijk slecht | -1 |
| • Niet slecht, niet goed | 0 |
| • Redelijk goed | +1 |
| • Zeer goed | +2 |

Vervolgens hebben we drie individuele scores toegekend voor een totaalscore van elke respondent. De respondenten zijn in drie niveaus verdeeld:

Prestatieniveaus digitaal vertrouwen bij ondernemingen

- Hoogste niveau (score in de bovenste 30% van alle respondenten)
- Middenmoot (middelste 30%)
- Laagste niveau (onderste 30%)

Deze indeling bracht een aantal dramatische verschillen naar voren tussen de bedrijven die het beste presteren (hoogste niveau) en die het slechtste presteren (laagste niveau).

Hoeveel beter?

Het spreekt vanzelf dat het hoogste niveau het beter doet op het gebied van de meetgegevens voor digitaal vertrouwen, omdat de indeling in niveaus is bepaald op basis daarvan. Maar het is interessant om te zien hoe véél beter het hoogste niveau presteert dan het laagste niveau. Bijvoorbeeld: drie keer zo veel bedrijven op het hoogste niveau zeggen goed te presteren voor wat betreft de werking en beschikbaarheid van e-commercewebsites, en 2,9 keer zo veel bedrijven zeggen dat ze goed bezig zijn met het voorkomen van phishing en andere e-mailaanvallen. De prestaties op het hoogste niveau liggen tussen de 10% en 300% hoger voor alle meetgegevens:



DE KLANTEN VAN ORGANISATIES OP HET **HOOGSTE NIVEAU** VERTROUWEN DIE ORGANISATIES AANZIENLIJK VAKER DAN DE KLANTEN VAN HET **LAAGSTE NIVEAU**.

²Big Growth Forecasted for Big Data – IDC

³FBI Internet Crime Complaint Center (IC3)

DE BESTE ONDERNEMINGEN DOEN HET **VEEL BETER** OP HET GEBIED VAN DIGITAAL VERTROUWEN DAN DE SLECHTSTE



Waarom doen de bedrijven op het hoogste niveau het zoveel beter?

Er zijn een aantal opvallende verschillen tussen het hoogste en laagste niveau, die bepalend zijn voor de grote verschillen in de uitkomsten:

- **Houding:** Het hoogste niveau zal viereneenhalf keer vaker denken dat het verlies van het vertrouwen van een klant zal leiden tot het weglopen van die klant. Ook zijn de bedrijven op dit niveau eerder geneigd te denken dat digitaal vertrouwen van invloed is op hun merkreputatie, verkopen en marge. Daarnaast zeggen ze ook 5,6 keer zo vaak dat ze van partner zouden switchen bij verlies van vertrouwen in die partner.
- **Vroege start:** De koplopers zijn verder gevorderd met digitaal vertrouwen en zullen de inspanningen eerder voltooien dat de bedrijven op het laagste niveau.
- **Meer zorgen over cyberbedreigingen:** Het hoogste niveau neemt cyberbedreigingen veel serieuzer. De bedrijven op dat niveau maken zich 1,5 tot 2,3 keer zo vaak zorgen over cyberbedreigingen.
- **Meer bezig met algemene bescherming tegen cyberaanvallen:** Het hoogste niveau beschikt tot wel drie keer zo vaak over belangrijke beschermingsmaatregelen tegen cyberaanvallen.

HOEVEEL VAKER HOUDT HET **HOOGSTE NIVEAU** ZICH BEZIG MET:

Deelname aan implementatie van PKI



Zero-trust beleid



PKI-automatisering



Overall HTTPS



Levenscyclusbeheer van certificaten



Beveiliging van apparaatidentiteit en activiteiten

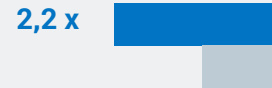


HET **HOOGSTE NIVEAU** MAAKT ZICH MEER ZORGEN OVER BEPAALDE BELANGRIJKE CYBERBEDREIGINGEN:

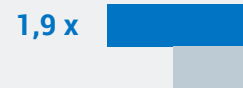
Aanvallen via social engineering



Spyware



Aanvallen op de aanvoerketen



Gegijzeld account



Ransomware



Waar moet digitaal vertrouwen worden beheerd?

De beslissing over waar in een onderneming digitaal vertrouwen moet worden geregeld is belangrijk. Wat dit onderwerp betreft, bestaat er een flink verschil van mening tussen de bedrijven op het hoogste en laagste niveau.

Het hoogste niveau is er ruimschoots van overtuigd dat de CIO zich moet bezighouden met digitaal vertrouwen binnen de IT-organisatie. Op het laagste niveau vindt men het een zaak van de beveiligingsafdeling.

Dit betekent niet dat de beveiligingsafdeling of hun activiteiten als minder belangrijk worden beschouwd. Het duidt eerder op het besef dat de CIO een beter beeld heeft van de totale technologische voetafdruk van een organisatie, en weet hoe belangrijk digitaal vertrouwen is voor het succes van die organisatie. Deze bevindingen laten zien dat de koplopers digitaal vertrouwen op een strategische manier benaderen.

DE CONCLUSIES VAN DIGICERT

DigiCert is de wereldwijd toonaangevende leverancier van digitaal vertrouwen, die zowel individuen als bedrijven het vertrouwen biedt dat hun online aanwezigheid is beveiligd, en zich al vanaf het prille begin bezighoudt met digitaal vertrouwen. Hier volgen onze vijf adviezen voor bedrijven die het succes van de koplopers willen evenaren:



Maak van digitaal vertrouwen een strategische noodzaak. Dit is een van de dingen waarmee de ondernemingen op het hoogste niveau zich duidelijk onderscheiden. Zij zien in dat digitaal vertrouwen van invloed is op de bedrijfsresultaten zoals merkreputatie, klantloyaliteit, omzet en marge.



Zet een speciale afdeling voor digitaal vertrouwen op binnen uw organisatie, met een zichtbare leidinggevende die beslissingen kan nemen.



Realiseer u dat digitaal vertrouwen een steeds belangrijker onderwerp is voor uw gebruikers, waaronder consumenten, en dat het succes en de reputatie van uw bedrijf rechtstreeks zijn gelinkt aan uw vermogen om digitaal vertrouwen op hoog niveau te bieden.



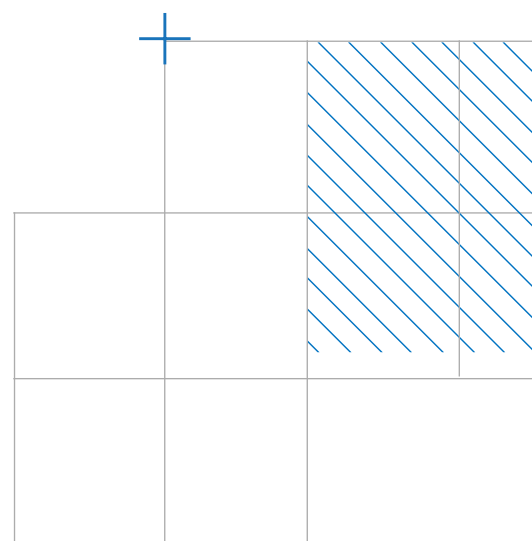
Haal specialisten binnen om u te helpen. Een van de uitdagingen op het gebied van digitaal vertrouwen die werden genoemd was een gebrek aan vaardigheden bij werknemers. Ga aan de slag met een partner die ruimschoots ervaring heeft met de hoofdelementen van digitaal vertrouwen, en die oplossingen kan bieden voor het eenduidige beheer van vertrouwen binnen de hele organisatie.



Onthoud dat uw klanten belang hechten aan digitaal vertrouwen. Wees duidelijk in uw communicatie over digitaal vertrouwen en vertel niet alleen dat u het belangrijk vindt, maar laat ook zien wat u eraan doet.

Dit is in lijn met een onderzoek van Bain & Company⁵, waaruit blijkt dat het verhogen van het klantbehoud met 5% leidt tot een winstverhoging tussen de 25% en 95%. Gezien de grote kans dat klanten weglopen bij een bedrijf zodra ze hun vertrouwen erin verliezen, moet het maximaliseren van digitaal vertrouwen een verplicht onderdeel van de bedrijfsactiviteiten zijn.

⁵Prescription for Cutting Costs – Bain & Company



|||



1245.54°
753234.72°

|||



IoT



digicert®