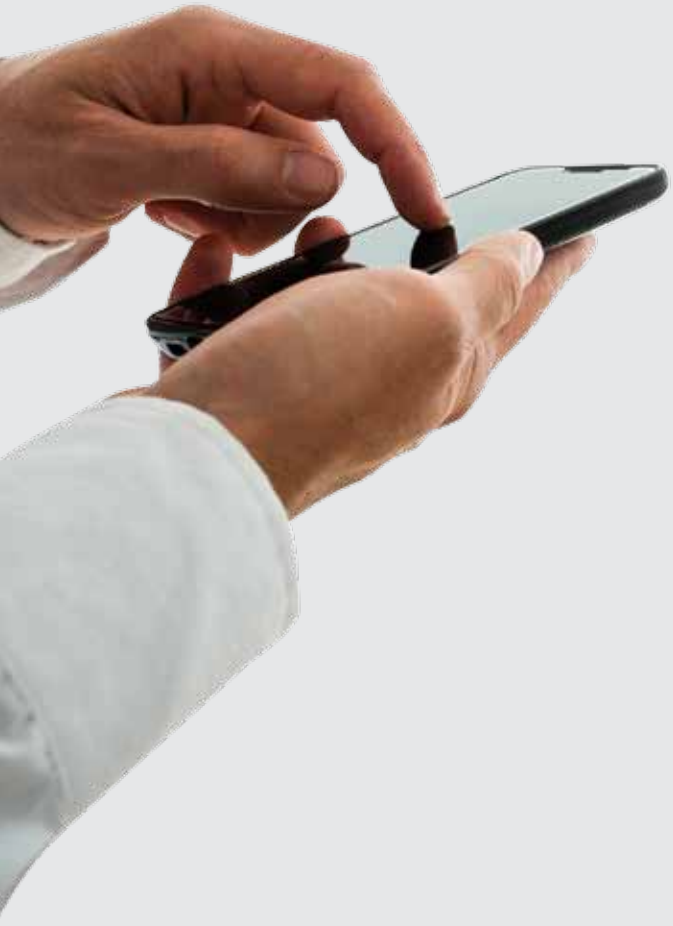
# Managementsamenvatting

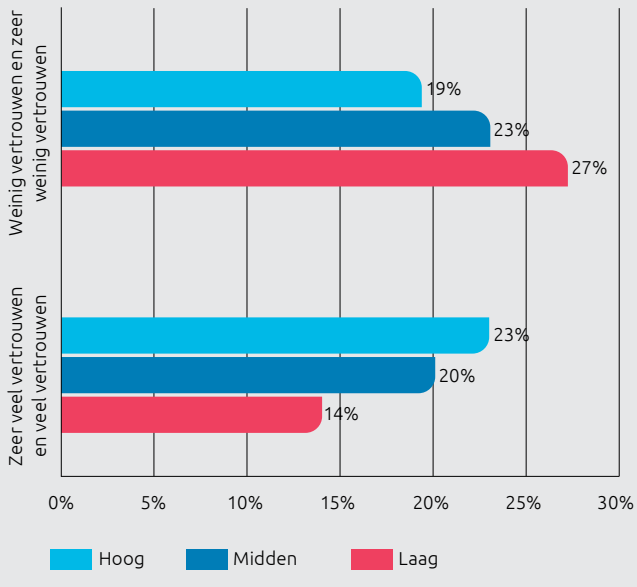
## Wantrouwen en vertrouwen in de digitale samenleving

De digitale samenleving is gebaseerd op vertrouwen. Het vertrouwen van de burger dat overheden en organisaties voorzichtig en integer met data omgaan. Dat persoonsgegevens niet op straat komen te liggen en de waarheid niet wordt gemanipuleerd.



Dat vertrouwen was er lange tijd blindelings. Niet zozeer omdat de burger nou zoveel vertrouwen had in de instituties, maar omdat de kennis ontbrak om te veronderstellen dat dat vertrouwen onterecht zou kunnen zijn. Want ga maar na: we wisten lange tijd niet wat er zou kunnen gebeuren als goede beveiliging zou ontbreken, of als kwaadwillenden met onze data aan de haal zouden gaan. We waren ons er ook totaal niet van bewust wat we allemaal weggaven, als we bijvoorbeeld een app installeerden. Aan welke risico's we ons blootstelden. De digitale samenleving kende immers geen precedent.

**Figuur 1: Vertrouwen in de digitale samenleving is verdeeld (naar opleidingsniveau).**



## Schade en schande

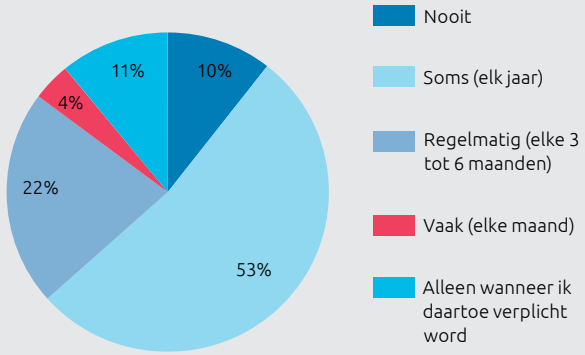
De afgelopen tijd zijn we door schade en schande wijs geworden. We komen erachter dat publieke en private organisaties data verzamelen, voor vaak onduidelijke en daardoor altijd discutabele doeleinden. Dat onze persoonlijke data door gebrekkige authenticatie minder veilig zijn dan we dachten en dat hacks enorme gevolgen kunnen hebben. En de data die wij zelf toevertrouwen aan partijen, blijken minder veilig dan we aannamen. Met de grootscheepse migratie van data naar de cloud hebben we er een gigantisch potentieel informatielek bijgekregen. Ons massale gebruik van social media levert een datagoudmijn op die ook niet bepaald veilig blijkt. Dankzij Cambridge Analytica kwamen de dagelijkse Facebook-beslommeringen van 80 miljoen mensen op straat te liggen. Waarbij de onduidelijke privacy-instellingen van Facebook zelf overigens goed van pas kwamen.

En daarbij blijft het niet. Omdat zoveel partijen zoveel van ons af weten, kunnen we makkelijk gemanipuleerd worden. Datzelfde Cambridge Analytica gebruikte Facebook-gegevens om de Amerikaanse presidentsverkiezingen te beïnvloeden. Fake news – u leest er meer over in de artikelen op pagina 14 en 54 - vindt een vruchtbare voedingsbodem; online zit iedereen in zijn eigen bubbel, mede dankzij de slimme algoritmes van partijen als Google. Daardoor wordt het makkelijk de mening van mensen te manipuleren en de waarheid eenzijdig te belichten.

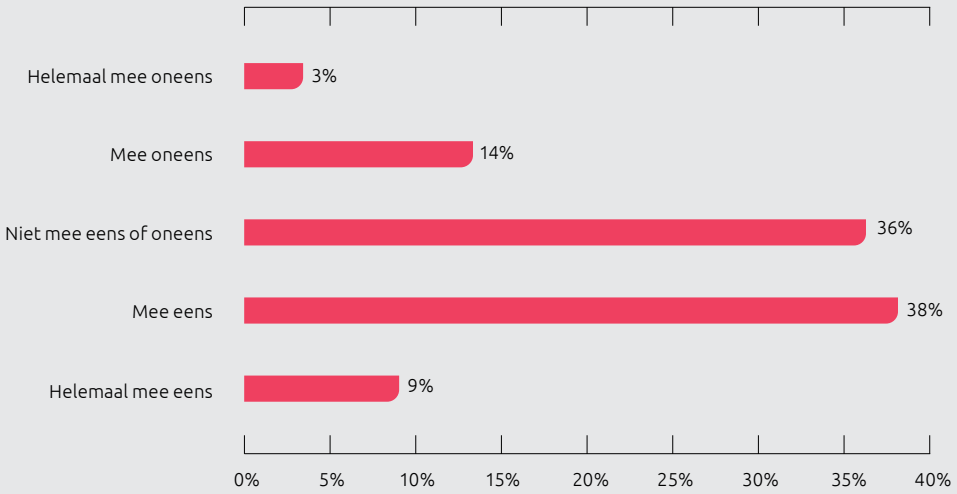
Met de razendsnelle intrede van steeds nieuwe innovaties – Internet of Things, robotisering, Artificial Intelligence – komt onze cybersecurity ook onder druk te staan. De digitale weerbaarheid van mensen en organisaties blijft achter bij de toenemende dreiging.

Op deze manier vallen we ten prooi aan verschillende uitingen van cybercrime, waarbij criminelen op allerlei manieren dankbaar gebruik weten te maken van onze onbekwaamheid en onwetendheid.

**Figuur 2: Een op de 10 mensen verandert zijn wachtwoord nooit.**




**Figuur 3: 47% ziet een minder duidelijk onderscheid tussen echte en valse feiten versus 5 jaar geleden.**



*Steeds meer blijkt dat de digitale samenleving is gebaseerd op drijfzand. We zijn wakker geworden in de digitale realiteit. En die realiteit bevalt ons maar matig.*

**Erik Hoorweg**
**Capgemini Consulting**

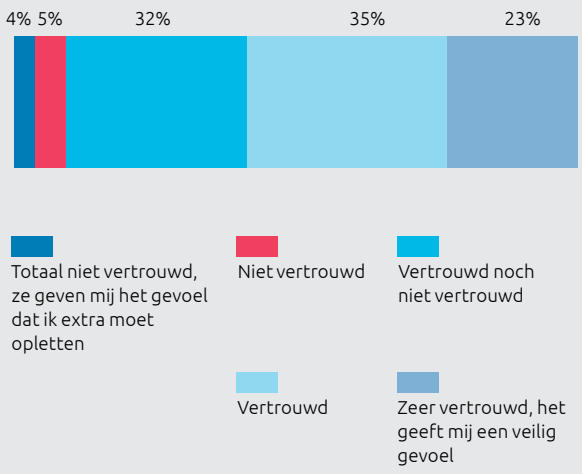
## Tipping point

Daarmee zijn we aanbeland op een tipping point. Het punt dat vertrouwen dreigt om te slaan naar wantrouwen. Want wie kunnen we nog vertrouwen? We keren Facebook de rug toe. We stemmen tegen het Wiv-referendum. We verliezen ons geloof in de media, de overheid en de private sector. De groeiende rol van Artificial Intelligence wordt veelal met achterdocht bezien.

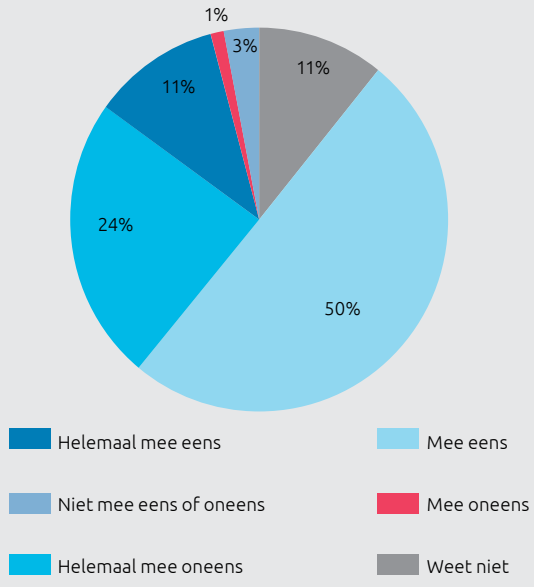
Nu de burger zich bewust is geworden van de risico's van de digitale samenleving, komt die onder druk te staan. Want wat gebeurt er, als burgers hun consent intrekken? Als ze niet langer goedkeuren dat organisaties toegang hebben tot hun gegevens? Moderne bedrijfsmodellen in de publieke en private sector zijn afhankelijk van data, waaronder persoonsgegevens. Zonder die consent valt dat geheel als een kaartenhuis in elkaar.

Er speelt bovendien nog een factor. Onze nationale en persoonlijke veiligheid staat of valt, zoals de artikelen op pagina 18 en 40 van dit rapport betogen, in belangrijke mate met het vermogen data te vergaren, delen en analyseren. Dit lijkt op gespannen voet te staan met privacy. Maar privacy is een mensenrecht en veiligheid een basisvoorwaarde om daarvan te kunnen genieten. Het is dan ook de kunst om een juiste balans te vinden tussen deze twee thema's.

**Figuur 4: Slechts 9% voelt zich niet vertrouwd met het groeiend aantal camera's in openbare ruimtes.**




**Figuur 5: 61% maakt zich zorgen over beveiliging van IoT-apparatuur.**



*Het moge duidelijk zijn: voor iedereen in het veiligheidsdomein is een rol weggelegd als het gaat om de verbetering van gegevensbescherming en de vergroting van digitale veiligheid. Als we serieus omgaan met die verantwoordelijkheid, is de eerste stap gezet richting het herstel van het beschadigde vertrouwen van de burger.*

**Erik Hoorweg**
**Capgemini Consulting**

## Kans

De actoren binnen het veiligheidsdomein zijn zich de afgelopen jaren meer bewust geworden van hun rol in het herstellen van het vertrouwen en borgen van de veiligheid. Dat heeft al de nodige maatregelen opgeleverd.

De overheid heeft bijvoorbeeld de Algemene verordening gegevensbescherming opgetuigd, die de privacy van burgers beter moet beschermen en strengere technische en organisatorische eisen stelt aan de vergaring van data door organisaties. Er gelden aanvullende wetten en regels voor opsporingsdiensten bij de omgang met gegevens. We zien dat landen als Duitsland de oorlog verklaren aan fake news, met verstandige inzet van slimme algoritmes. En we zien ook ontwikkelingen in de strijd tegen cybercrime en cyber-bedreigingen uit het buitenland; minister Grapperhaus noemde dat een topprioriteit van het nieuwe kabinet – in nadrukkelijke (internationale) samenwerking met overheden en private sector. Overigens loopt Nederland ook nu al voorop als het gaat om cybersecurity.

Partijen in het veiligheidsdomein zullen dergelijke maatregelen moeten beschouwen als een kans. Ten eerste om hun zaken op orde te brengen. De nieuwe wetgeving vereist immers dat organisaties inzicht verschaffen in hun gegevenshuishouding. Aangezien die nu vaak diffuus is, is een herstructurering en vereenvoudiging van het applicatielandschap nodig. Daarvan plukken de organisaties zelf ook de vruchten.

En er is meer. Bij de introductie en ontwikkeling van nieuwe producten en diensten zullen organisaties vanaf het begin het veiligheidsaspect moeten betrekken. De potentiële impact voor de veiligheid van de burger moet altijd top of mind zijn.

## Goed en kwaad

Technologie kan worden ingezet voor verschillende doeleinden. Goedaardige en kwaadaardige. De afgelopen tijd leek het alsof het kwaad in de technologie de overhand had gekregen. Het is nu aan alle betrokkenen om het goede te benadrukken. Om de vaak disruptieve technologie in te zetten voor veiligheid, zonder de privacy van individuen te beschadigen. Om de menselijke maat in technologie te zoeken en de burger niet aan zijn lot over te laten, maar bij de hand te nemen. Om waar mogelijk het partnership met die burger aan te gaan en de rol van de burger als participant in de bescherming van onze veiligheid weloverwogen vorm te geven. Om het vertrouwen in – en de betrouwbaarheid van – digitale ontwikkelingen te vergroten en te borgen. En om, binnen die context, te werken aan grotere veiligheid.


## Over de auteur:

Drs. Erik Hoorweg MCM is vice president bij Capgemini Consulting en verantwoordelijk voor de publieke sector.

**Voor meer informatie kunt u contact met de auteur opnemen via:**

erik.hoorweg@capgemini.com |

https://www.linkedin.com/in/erik-hoorweg-296b593/


De cijfers in rapport zijn gebaseerd op het GFK onderzoek (N=1000, December 2017) in opdracht van Capgemini Nederland B.V.