Van awareness naar actie:
Trends in Online Security & e-Identity

Connectis

SIDN Jouw wereld. Ons domein.

Inhoud

1 Inleiding & opzet

In Nederland internetten we relatief zorgeloos: de verbindingen zijn goed en het .nl-domein is een van de veiligste ter wereld. Voor dat laatste spannen SIDN en Connectis zich gezamenlijk in. We beheren het domein zorgvuldig, innoveren volop en ontwikkelen oplossingen voor online authenticatie zodat, gebruikers verantwoord kunnen inloggen.
Ook doen wij relevant onderzoek, zoals dit onderzoek naar trends in Digital Security en e-Identity.

Centraal in dit onderzoek staat het woord 'vertrouwen'. Hebben ondernemingen en consumenten vertrouwen in de veiligheid van het internet? Zijn zij zich bewust van de risico's en welke maatregelen nemen zij? Maken zij zich zorgen om hun online privacy? Vragen die al sinds 2012 aan de orde komen in ons brede onderzoek 'Trends in Internetgebruik'.

De thema's security en identity worden binnen het bredere domein internetgebruik steeds belangrijker. Dit is de reden dat SIDN en Connectis dit jaar voor het eerst een dedicated onderzoek 'Trends in Online Security en e-Identity' publiceren. In het onderzoek gaan wij in op de gevoelens bij consumentenen en ondernemers en proberen wij de resultaten te duiden met hulp van diverse experts. Daarmee willen wij niet alleen inzicht geven in de stand van zaken rond online security en e-identity, maar ook vooruitkijken naar de impact van trends als Internet of Things.

Onderzoeksmethodiek
Voor dit onderzoek werden 512 bedrijven van verschillende grootte en 2.095 consumenten (representatieve doorsnede voor de Nederlandse internetgebruiker) online bevraagd. Allen waren lid van het GfK Panel Online onderzoek (CAWI). De uitvraag vond plaats in februari/maart 2019.

Expertpanel
De resultaten presenteren we in dit trendrapport, aangevuld met de reacties van een expertpanel dat we zorgvuldig hebben samengesteld. Aan de hand van vijf stellingen besprak het panel verschillende thema's op het gebied van cybersecurity en e-identity: waar zitten de zwakke plekken in een organisatie, wat betekent Internet of Things (IoT) voor onze online veiligheid en wie moet ons eigenlijk beschermen – de markt, de overheid, of wijzelf?
> Meer over het expertpanel

Wij zijn SIDN
SIDN (Stichting Internet Domeinregistratie Nederland) is sinds 1996 verantwoordelijk voor het beheer van het .nl-domein. Onze missie: mensen en organisaties verbinden voor een zorgeloos digitaal bestaan. Samen met ruim 1.200 partijen in ons kanaal (de zogenaamde registrars) zorgen we ervoor dat meer dan 5,8 miljoen .nl-domeinnamen bereikbaar zijn. Daarnaast gaat SIDN over registratie, mutaties en geschillen, en dragen we bij aan de veiligheid van het internet in Nederland.
We doen onderzoek naar cybersecurity en monitoren verdacht gedrag. Hiervoor ontwikkelen we ook nieuwe diensten, zoals de Domeinnaam-bewakingsservice (DBS).

Wij zijn Connectis
Connectis verbindt organisaties, consumenten en landen met oplossingen voor online identificatie en authenticatie. Ons platform maakt het mogelijk dat gebruikers van online dienstverleners inloggen met DigiD, eHerkenning, iDIN, eIDAS, social logins en vele andere inlogmiddelen. Meer dan 350 organisaties maken gebruik van de Connectis Identity Broker voor het authenticeren van 14 miljoen gebruikers. Ruim 50.000 organisaties maken gebruik van onze software en eHerkenningsmiddelen om veilig in te loggen bij publieke en private dienstverleners. Connectis is opgericht in 2008 en sinds 2017 zijn we onderdeel van SIDN.

2 Cybercrime: bedrijven onderschatten risico's

Als ondernemer zonder webshop of online dienstverlening hoef je je geen zorgen te maken over cybercrime. Hackers hebben het op banken gemunt. Of andere organisaties waar veel geld omgaat, en dus iets te halen. Toch? Ons expertpanel constateert dat deze hardnekkige misvattingen nog altijd veel schade aanrichten. Het expertpanel begint daarom met een discussie over awareness: zijn bedrijven zich genoeg bewust van de risico's van cybercrime?

Respondenten zien het gevaar niet

Nog altijd denken veel ondernemers dat ze geen interessant doelwit voor hackers zijn zolang ze niets in de ICT of online verkoop doen. Zo ervaart slechts 9,9% van de respondenten uit ons onderzoek die geen online dienstverlening bieden, cybercrime als een bedreiging voor hun organisatie. De overgrote meerderheid (90,1%) ziet in cybercrime geen (ernstig) gevaar. Bij online dienstverleners liggen de verhoudingen iets anders, maar nog altijd ervaart zo'n 80% cybercrime niet als een dreiging. In totaal ziet 67,7% van de ondervraagden cybercrime als 'een beetje bedreigend'; volgens 17,6% is er zelfs geen vuiltje aan de lucht.

> Grafiek 1: In hoeverre ervaart u cybercrime voor uw organisatie als bedreigend? (bron GfK, n=512)

Reality check: elk bedrijf is een ICT-bedrijf

Zorgeloosheid alom dus, maar is die terecht? Het panel is unaniem: meer bewustzijn is nodig. Want ook bedrijven zonder webshop of online dienstverlening zijn een interessante en vaak makkelijke prooi voor cybercriminelen. Bij iedereen is wel iets te halen: inloggegevens, persoonlijke data of gevoelige bedrijfsgegevens bijvoorbeeld. Bovendien zijn kleinere bedrijven vaak de ingang naar hun grote toeleveranciers of klanten. Doordat werk- en bedrijfsprocessen bijna overal zijn gedigitaliseerd, kunnen criminelen hier via internet bij komen – soms zelfs kinderlijk eenvoudig. En als het gebeurt, kan de schade flink oplopen. Dat zag ook panellid Maria Genova, auteur van de boeken WHAT THE HACK! en Komt een vrouw bij de h@cker:

"Ik ken het voorbeeld van een transportbedrijf waar cruciale data werd 'gegijzeld' door cybercriminelen die ransomware hadden geplaatst. Gevolg: niemand kon meer bij de orders en klantgegevens. De hele organisatie lag plat, vrachtwagens konden niet uitrijden. De hackers vroegen €30.000,- om de data weer vrij te geven. Door de digitalisering is élk bedrijf inmiddels een ICT-bedrijf. Veel mensen vergeten dat."

Maria Genova (journalist, schrijver en spreker)

Cybersecurity, een IT-taak?

Daarbij komt dat veel bedrijven cybersecurity als een technisch vraagstuk zien, constateert het panel. Het onderwerp wordt dus ook op het bordje van de IT-afdeling of individuele ICT'er gelegd, vanuit de gedachte dat die de systemen dicht moet timmeren. Maar ICT'ers zijn niet per definitie cybercrime-experts: veiligheid vergt andere expertise dan performance en beschikbaarheid. Een voorbeeld: de ICT'er is in het Internet of Things-tijdperk niet altijd meer betrokken bij de inkoop van devices die verbinding maken met internet. Bovendien gaat cybersecurity verder dan techniek alleen. Hoe medewerkers met verdachte links en phishing-mails omgaan, is bijvoorbeeld net zo belangrijk als een goed antivirusprogramma. Misschien zelfs belangrijker.

Investeringen in cybersecurity stijgen nauwelijks

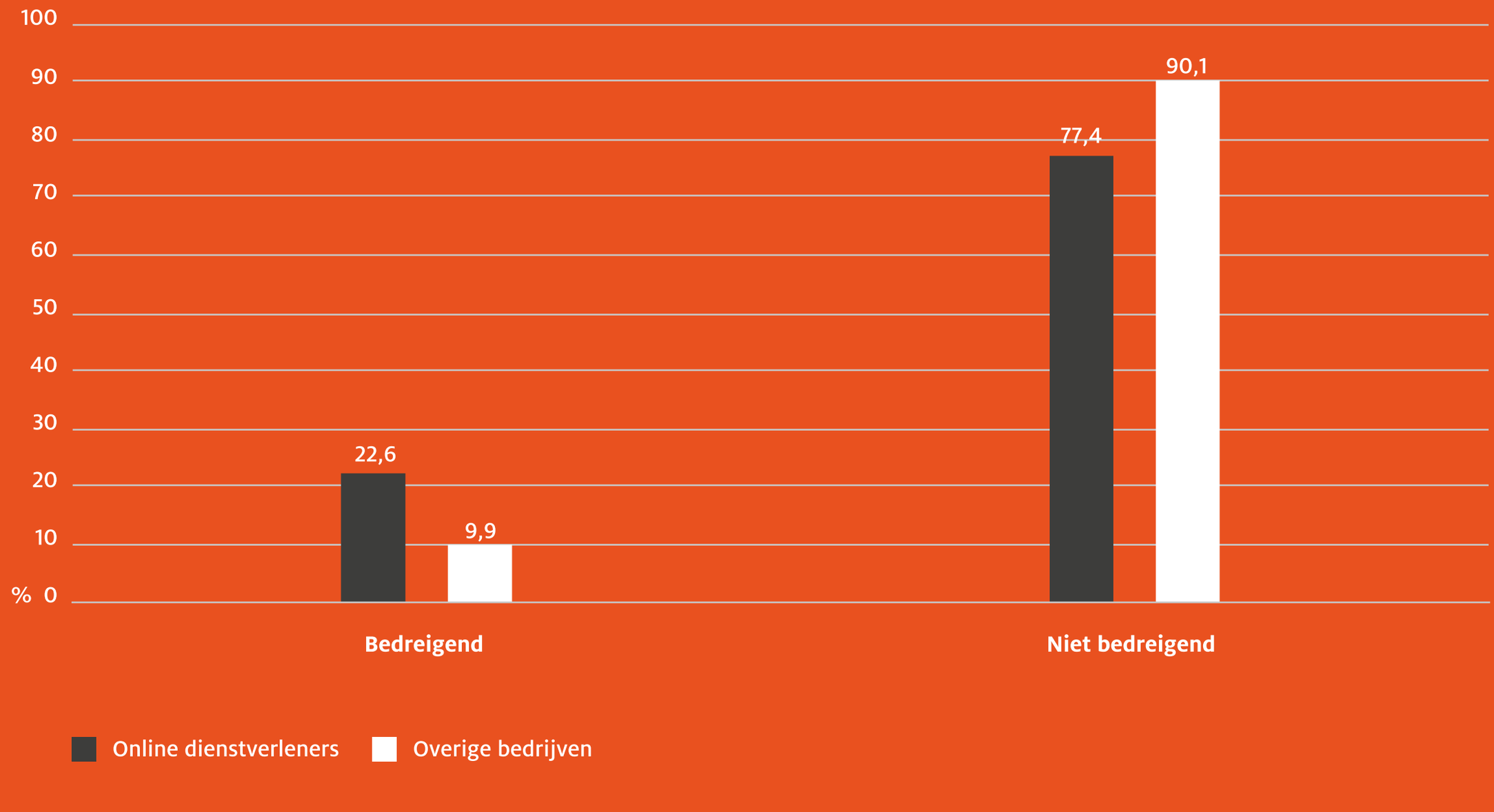
Het panel is het erover eens dat er nog veel te winnen valt als het om 'awareness' en 'sense of urgency' gaat. Maar hoe zit het met de investeringen in cybersecurity; blijven die ook achter? Uit ons onderzoek blijkt dat de budgetten hiervoor in de afgelopen twaalf maanden grotendeels gelijk zijn gebleven. Zelfs onder de respondenten die cybercrime als een reële dreiging zien, geeft 69,4% aan dat er niet meer geld is vrijgemaakt voor beveiliging van bedrijfsprocessen. Meer gepercipieerde dreiging bij bedrijven leidt dus nauwelijks tot extra investeringen.

> Grafiek 2: In hoeverre verwacht u dat het budget -als het gaat om de bescherming tegen cybercrime- er voor de komende 12 maanden uit zal zien?

"Online security moet geen apart hoofdstuk zijn, maar een geïntegreerd onderdeel van je organisatie."

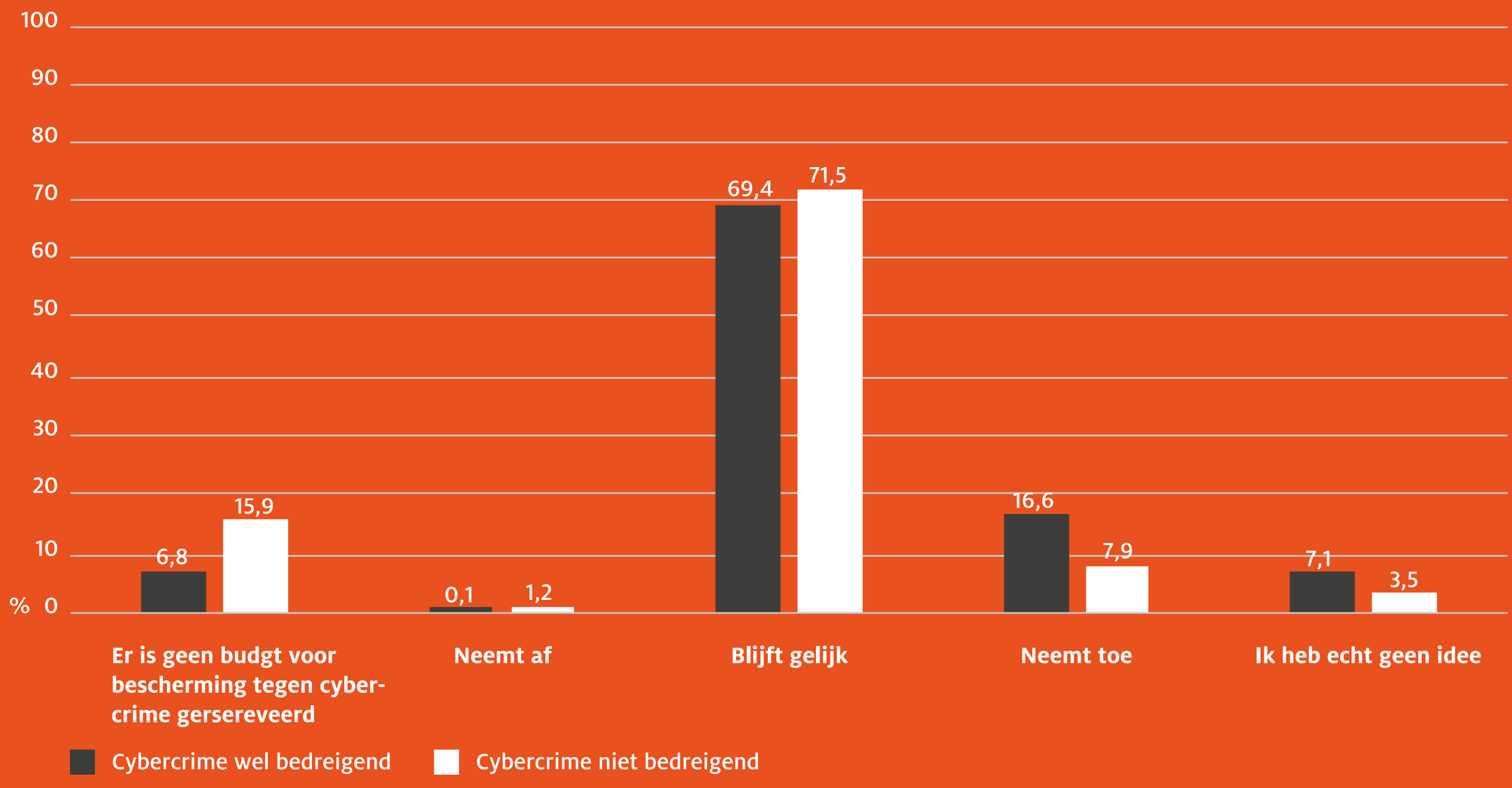
Kees Monshouwer (Monshouwer Internet Diensten)

Online dienstverleners ervaren meer dreiging cybercrime



Grafiek 1: In hoeverre ervaart u cybercrime voor uw organisatie als bedreigend? (bron GfK, n=512)

Investeringen cybersecurity stabiel



Grafiek 2: In hoeverre verwacht u dat het budget -als het gaat om de bescherming tegen cybercrime- er voor de komende 12 maanden uit zal zien? (bron GfK, n=512)

3 Online Security is mensenwerk

Veel ondernemingen benaderen online security als een technisch probleem: ze leggen het onderwerp neer bij hun IT-afdeling en investeren vooral in de bescherming van hun systemen. Maar een minstens zo belangrijke schakel is de mens. Misschien wel de belangrijkste, want hij gebruikt op grote schaal login-methodes die hij zelf als onveillig beschouwt en gebruikt onveilige privé-logins in 'veilige' bedrijfsomgevingen. Ook klikt hij stug door op onveilige linkjes. Het goede nieuws volgens ons expertpanel: wie vandaag concrete stappen zet om de organisatie veiliger te maken, boekt morgen al
resultaat.

Inlogparadox: gemak versus gedoe

Uit ons onderzoek blijkt dat er een discrepantie bestaat tussen hoe vaak inlogmethodes worden gebruikt en hoe veilig we ze vinden. Wat wij veel gebruiken, vinden wij onveilig. Wat wij veilig vinden, gebruiken wij minder. Zo geeft 57,2% van de respondenten aan dagelijks in te loggen via social media, zoals Google en Facebook. Opvallend, want slechts 14,4% van de respondenten ervaart dit als veilig.

> Grafiek 3: In welke mate vindt u dat de volgende manieren van inloggen uw privacy goed beschermen?

Ook inloggen met een gebruikersnaam en wachtwoord blijft populair: 54,4% van de ondervraagden doet dit elke dag wel een keer, terwijl slechts 37,5% van hen dit als veilig bestempelt. iDIN en DigiD – twee inlogmethoden die juist als veilig worden gepercipieerd – worden juist minder vaak gebruikt.

Volgens het panel valt deze 'inlogparadox' grotendeels te verklaren door het verschil in gebruiksgemak: een wachtwoord aanmaken is zo gebeurd, terwijl je voor DigiD moet wachten tot er een activeringscode in je (offline) brievenbus ligt. De veiligere methoden zouden eigenlijk gebruiksvriendelijker moeten worden.

Biometrie nog niet populair

Daarnaast is er behoefte aan keuze in online identiteiten; overal inloggen met een veilige login als iDIN of DigiD is niet wenselijk als je er ook nog een anoniem social media-account op na wilt houden. Ook biometrisch inloggen lost het vraagstuk 'security-versus-gebruiksgemak' niet helemaal op, want je vingerafdruk biedt wel veilige toegang – maar geen bescherming van je privacy. Bovendien is biometrisch inloggen vooralsnog niet populair. UIt het onderzoek blijkt dat maar 11% van de respondenten hier een voorkeur voor heeft.

Veiligheid lijkt niet 'te koop'

De meest gebruikte, en als onveilig beoordeelde inlogmethoden zijn gratis. Zijn consumenten misschien bereid om voor een veilige, gebruiksvriendelijke inlogmethode te betalen? Dat is lastig, denkt André Koot van Nixu Benelux: "Vanuit identity providers is er geen business case. Bovendien zijn mensen zich vaak niet bewust van de risico's, waardoor de betalingsbereidheid beperkt blijft.' Remco Poortinga – van Wijnen van SURFnet voegt hieraan toe: 'Het is een illusie dat partijen 100% veiligheid kunnen bieden. 'Wij zijn veilig' kan nooit een USP zijn."

> Grafiek 4: Welke vorm(en) van cybercrime ziet u voor uw organisatie als meest bedreigend? (bron GfK, n=512)

‘1234’ nog steeds populair wachtwoord
Voorlopig blijft inloggen met een zelfgekozen wachtwoord dus dagelijkse kost. En juist daardoor gaat er veel mis. Ondanks waarschuwingen gebruiken mensen vaak eindeloos hetzelfde – vaak bedroevend zwakke – wachtwoord, en dan ook nog voor meerdere accounts. Slechts 22,7% van de respondenten in ons onderzoek gebruikt een extra beveiligd wachtwoord, en maar 20% kiest voor tweefactor-authenticatie. Ook opvallend: 60% van de consumenten logt in op onbeveiligde wifi-netwerken. Zou je kunnen zeggen dat in cybersecurity de mens de zwakste schakel is?

De mens als ‘lek’
In ieder geval valt er bij ‘de mens’ veel te winnen, vindt het panel. Aad van Boven (SecureMe2) constateert: ‘32% van de cyber alarmen die wij binnenkrijgen, is human-geïnitieerd. Daarbij gaat het niet om DDoS-aanvallen, maar om cybercrime op basis van ‘social engineering’: phishing, mails met ransom- of malwarelinkjes. CEO-fraude zien we ook veel, waarbij de CEO van een organisatie overtuigend wordt getriggerd om nietsvermoedend een bedrag over te maken naar het rekeningnummer van een crimineel. Stuk voor stuk zeer impactvolle vormen van cybercrime, die je niet voorkomt met alleen een goed antivirusprogramma.’
> Grafiek 5: In hoeverre bent u bereid te betalen voor: (bron GfK, n=2095)

Veiligheid begint bij kennis
Dat mensen een zwakke schakel vormen in cybersecurity, is minder slecht nieuws dan het lijkt. Het betekent namelijk dat ze invloed hebben op hun online veiligheid. En dat gedrag dus een knop is waar je aan kunt draaien. Hiervoor is vooral kennis nodig: welke vormen van cybercrime zijn er, hoe herken je ze en hoe ga je ermee om? Awarenesstrainingen kunnen helpen om medewerkers alerter en doortastender maken. Toch wordt hier nog nauwelijks in geïnvesteerd: slechts 16% van de bedrijven steekt geld in training en instructie, zo blijkt uit ons onderzoek. Ook worden trainingen niet genoeg herhaald, vindt het panel.

“Awareness-trainingen zijn effectief: medewerkers worden alerter op cybersecurity, weten beter hoe ze met bijvoorbeeld phishing-mails moeten omgaan en spreken ook hun collega’s hierop aan. Maar veel organisaties denken dat één awareness-training genoeg is. Terwijl je de materie vaker moet zien om hem goed te begrijpen, te onthouden en toe te passen. Awareness-training is geen kwestie van een vinkje zetten: zo, da’s gedaan. Het is een continue investering in je organisatie. Veel bedrijven zien awareness-trainingen als kostenpost, maar de kosten zijn een schijntje vergeleken met wat je bespaart als je een hack of een datalek kunt voorkomen.

Sommige organisaties maken een rekensom en komen tot de conclusie dat ze bijvoorbeeld 80.000 euro schade hadden, omdat de computers versleuteld waren en alle medewerkers een dag lang niet konden werken. Dus als je met een training een verkeerde muisklik op een vrij standaard phishingmail kunt besparen, heb je als bedrijf een enorme winst. Jammer dat veel bedrijven dat pas beseffen nadat ze gehackt zijn.”

Maria Genova, journalist, schrijver en spreker

Online veiligheid als taboe
En dan speelt er volgens het expertpanel nog iets anders: schaamte. Waar brand en inbraak openlijk worden besproken, treden bedrijven liever niet naar buiten over de cyberaanval die ze voor de kiezen kregen. Individuele medewerkers zijn vaak bang om voor dom, slordig of nalatig te worden versleten: 'Had je maar niet op dat linkje moeten klikken'. "Terwijl je precies op je menselijke zwakheden wordt gepakt. Het is moeilijk om je daartegen te wapenen," zegt André Koot van Nixu Benelux.

"Is een bedrijf gehackt, dan blijft het vaak muisstil. Vaak gaat het namelijk om concurrentiegevoelige informatie. Klanten lopen bovendien weg als ze horen dat hun leverancier slachtoffer is geweest van cybercrime, en dat hun data hierdoor mogelijk gevaar heeft gelopen. Door de imagoschade, als gevolg van een hack, kunnen bedrijven echt in de problemen raken."

Kees Monshouwer, Monshouwer Internet Diensten

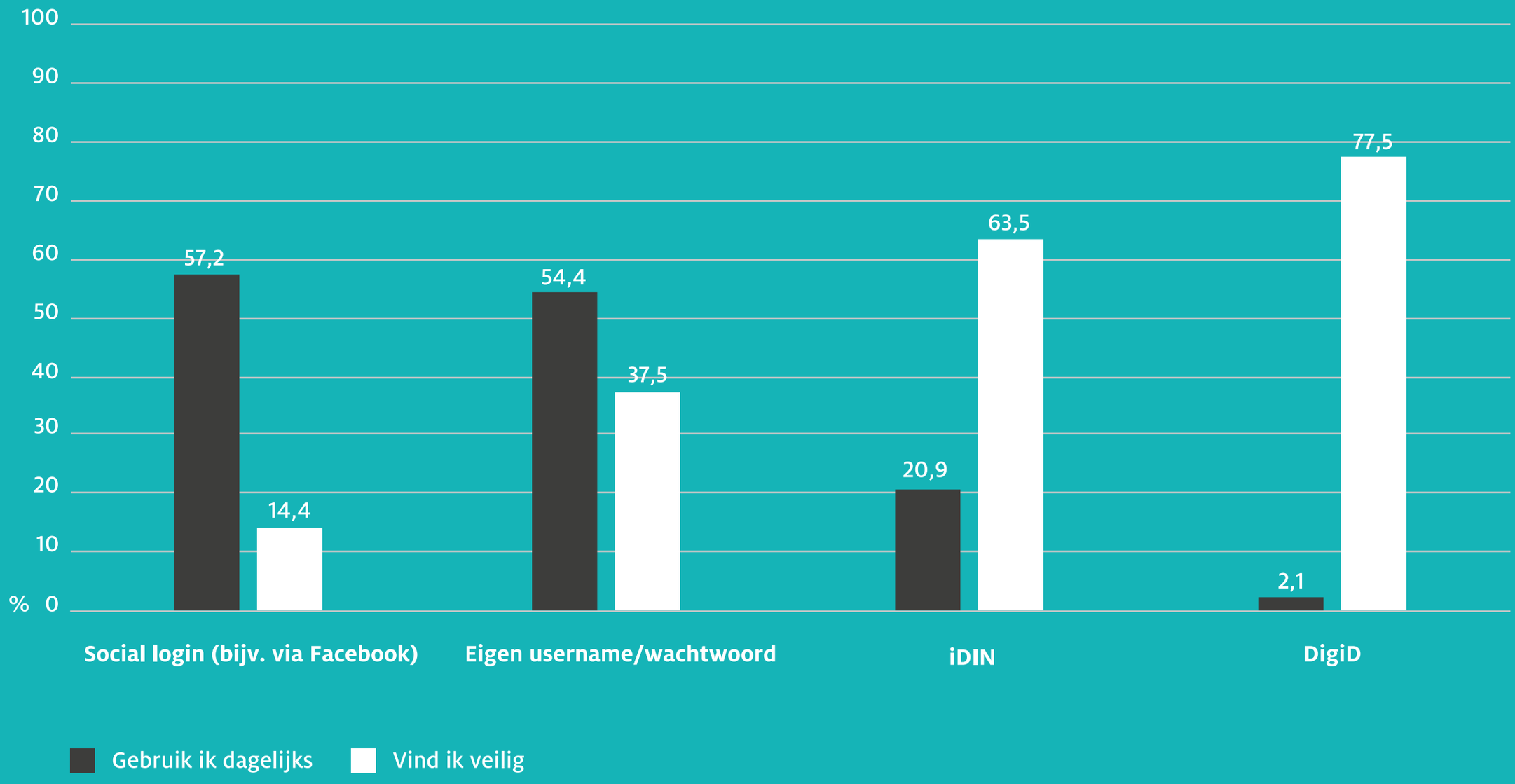
Bespreekbaar maken loont
Om als organisatie weerbaarder tegen cybercrime te worden, moet dus eerst het taboe worden doorbroken. Zo wordt het onderwerp bespreekbaar en durven medewerkers een incident of 'fout' wél te melden. Vervolgens kunnen herhaalde awarenesstrainingen ervoor zorgen dat de onderneming adequater met cybercrime omgaat. Zo zet je al een flinke stap richting een veiligere bedrijfsvoering.

Nodig inkoop uit op het IT-feestje
Security is geen exclusief IT-feestje, ook procurement draagt verantwoordelijkheid. Door een vaak jarenlange ontwikkeltijd zijn veel nieuwe (software)producten namelijk al onveilig als ze op de markt komen. Door security in hun requirements op te nemen, kunnen inkopers voorkomen dat er 'troep' de organisatie binnensluipt. En bij afschrijvingen geldt: de technische levensduur van een apparaat loopt af als de software niet meer betrouwbaar is. Het expertpanel is streng: 'maar hij doet het nog prima' is geen excuus. Wordt je product niet meer ondersteund, dan is het tijd om het te vervangen. Security wordt dus een steeds belangrijker aspect van de product life cycle. Zeker nu het aantal IoT-devices zeer snel toeneemt.

Morgen mee beginnen
Concrete tips om je organisatie weerbaarder te maken tegen cybercrime. Met dank aan Aad van Boven & Maria Genova.

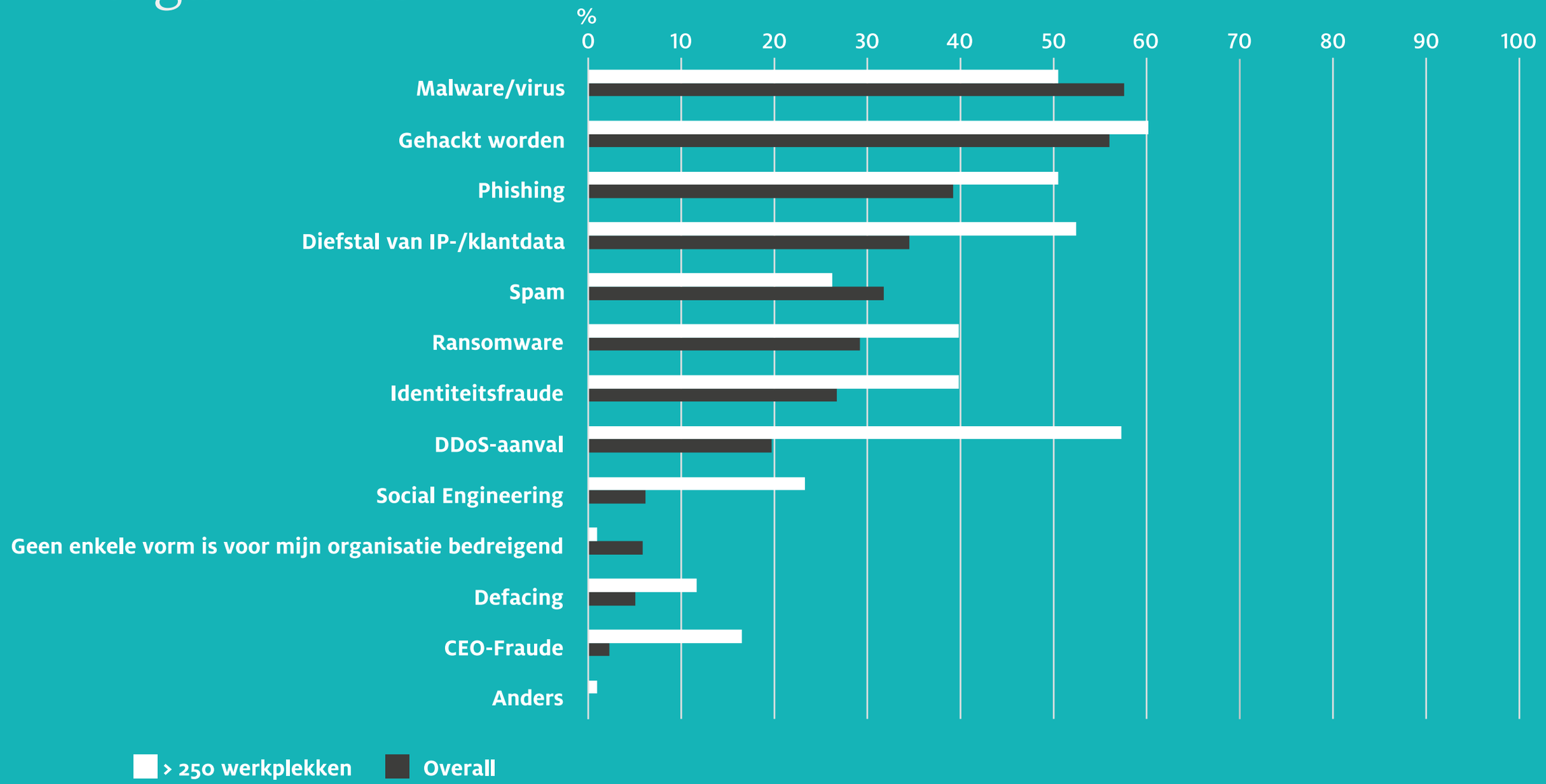
- Organiseer 'interactieve awarenesstrainingen'; verstop bijvoorbeeld een datalek in je bedrijf.
- Toon beveiligingstips op de screensaver van je bedrijf.
- Stuur binnen je organisatie op 'sterke wachtwoorden'.
- Benadruk de noodzaak van updaten.
- Gebruik 2-factor authenticatie altijd, als het mogelijk is.
- Zet IoT-devices op een ander netwerk dan je bedrijfssystemen.
- Schakel UPNP uit op de router en test op open poorten!
- Blijf nadenken!

Meestgebruikte inlogmethoden het minst vertrouwd



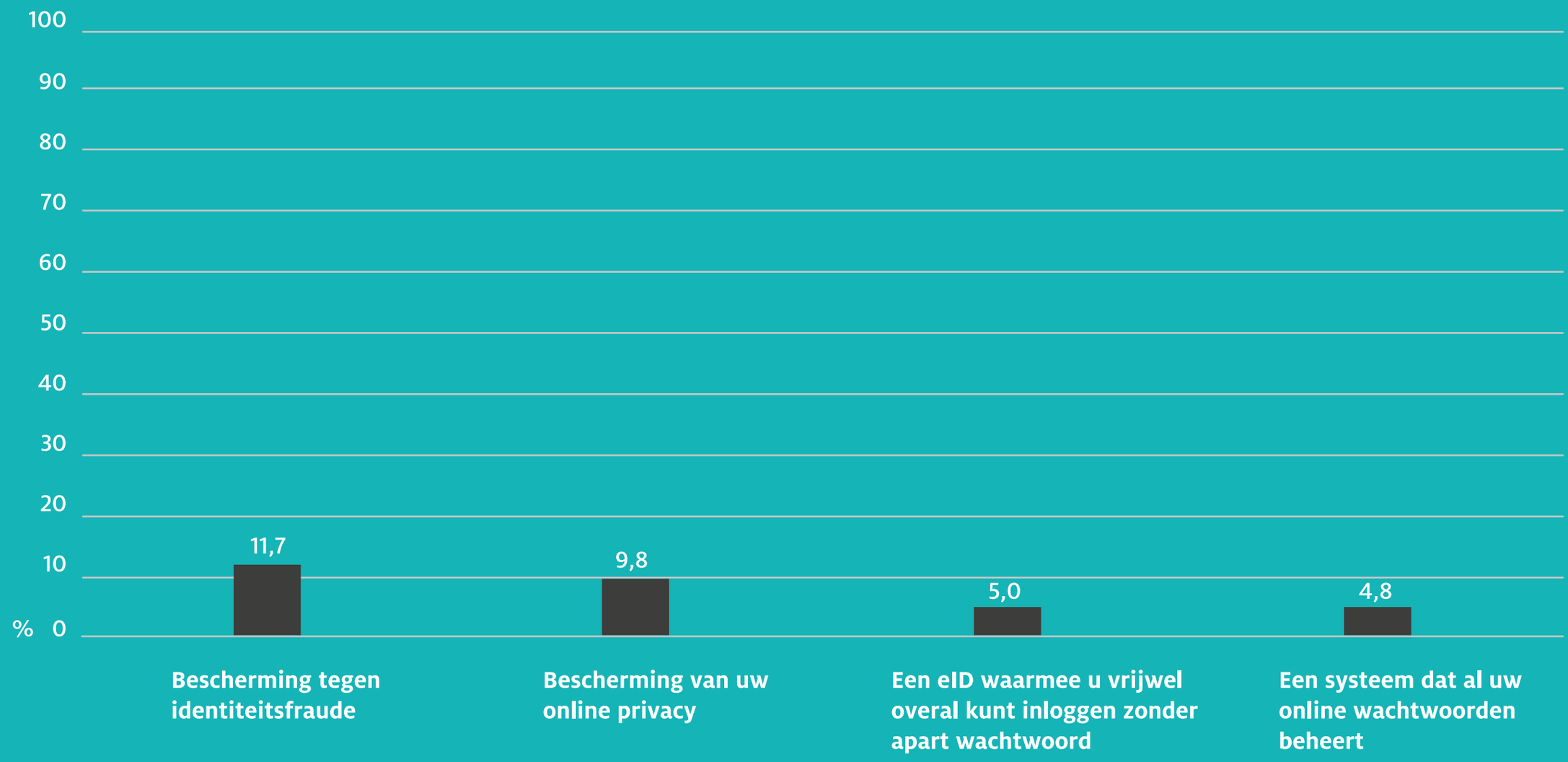
Grafiek 3: In welke mate vindt u dat de volgende manieren van inloggen uw privacy goed beschermen? Hoe vaak maakt u gebruik van deze inlogmogelijkheden? (bron GfK, n=2095)

Focus op technische dreigingen, vooral bij kleine organisaties



Grafiek 4: Welke vorm(en) van cybercrime ziet u voor uw organisatie als meest bedreigend? (bron GfK, n=512)

Betalingsbereidheid consumenten beperkt



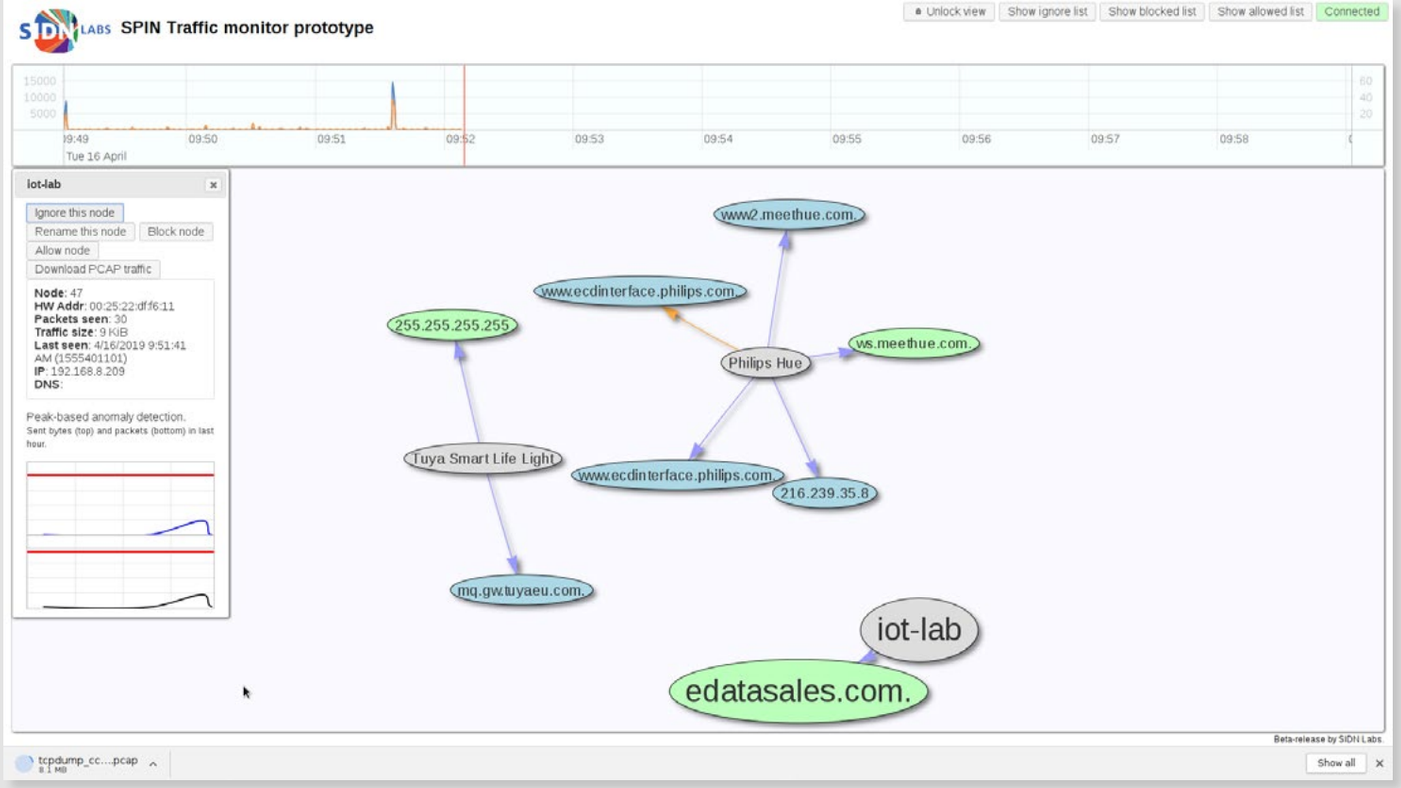
Grafiek 5: In hoeverre bent u bereid te betalen voor: (bron GfK, n=2095)

4 Internet of Things: hoe houden wij het veilig?

Onbekend maakt in dit geval bepaald niet onbemind. Wel onbevreesd. Het expertpanel vindt het daarom van belang om eerst te definiëren wat het IoT precies is. Snel volgt het unanieme antwoord: alles wat geen computer of server is, maar wel via het internet is aangesloten op een netwerk. Van fitbits tot lampen en van slimme koffiezetapparaten tot smart-tv's: we bestellen ze online en het liefst spotgoedkoop, vaak uit China. Vervolgens steken we enthousiast de stekker in het stopcontact, zonder te weten welke veiligheidsrisico's we daar eigenlijk mee lopen. We staan bovendien pas aan het begin van een exponentiële groei van devices die verbinding maken met internet.

"Meer dan de helft van de alarmen die we binnenkrijgen, komt uit IT die geen computer of server is. In 90% van de gevallen gaat het om producten die via ElCheapo, AliExpress of eBay zijn gekocht. In december zie je trouwens een duidelijke piek: afgelopen Sinterklaas en kerst kwamen er 11.500 nieuwe IoT-devices in onze huishoudelijke netwerken bij. We bestellen alles wat los en vast zit en knallen het zo online. Dus als het IoT wordt 'gedemoniseerd', tja...dan is dat niet ten onrechte."

Aad van Boven (SecureMe2)



Afbeelding 1: Realtime overzicht van apparaten die verbinding maken met Internet via een router (Bron: Spin4home.nl)

Meerderheid consumenten ziet weinig tot geen gevaar
Kennisgebrek leidt tot onderschatting, ben je geneigd te zeggen op basis van ons onderzoek. Op de vraag of IoT het internet onveiliger maakt, ruiken de meeste respondenten hooguit lichte onraad: 41,5% antwoordde 'iets minder veilig'. Daartegenover staat een relatief grote groep die zich wel degelijk zorgen lijkt te maken en verwacht dat het internet 'veel onveiliger' wordt (33,7%). Vrijwel verwaarloosbaar zijn de optimisten: 'iets veiliger' (3,0%) en 'veel veiliger' (0,3%). Opvallend is het deel dat denkt dat het niet uitmaakt (21,6%). Tel je hen namelijk op bij de behoedzamen, dan valt te concluderen dat ruim twee derde van de ondervraagden de risico's bagatelliseert – of ze niet ziet.
> Grafiek 6: Invloed IoT op veiligheid (bron GfK, n=2095)

Risico neemt toe na aankoop
Gemak en prijs lijken bij aanschaf volgens het expertpanel boven veiligheid te gaan. Beter opletten bij de aankoop? Volgens sommige panelleden schuilt het grootste gevaar van IoT-devices in de levensduur. Veel consumenten weten niet dat een slimme lamp een probleem kan vormen, stellen geen wachtwoord in en lopen daarmee vanaf dag één risico. Nog veel vaker zal het voorkomen dat ze vergeten te updaten. Of daarmee stoppen, waardoor een device vanzelf minder veilig wordt. Zo zetten ze hun deur steeds verder open voor online onheil, aldus Kees Monshouwer: "Hoe lang die dingen meegaan, dáár zit het grote gevaar. Alles wat nu veilig is, is het dat over tien jaar nog steeds?"

"Mensen vinden het een raar idee dat een vaatwasser, een webcam of een tv een wachtwoord heeft, dat bedenken ze zelf niet. En als ze het al lezen, ergens op pagina 5 van de manual, beseffen ze niet dat zo'n stom wachtwoordje toegang geeft tot andere apparaten in je netwerk. Er zou dus met koeienletters boven aan elke gebruiksaanwijzing moeten staan: STEL EERST EEN UNIEK WACHTWOORD IN!"

Maria Genova, journalist, schrijver en spreker

Wie van de drie?
Gelet op de voorspelde omvang van het datalek in Nederlandse huishoudens, dringt de verantwoordelijkheidsvraag zich als vanzelf op. Wie moet ons veilig houden in de opmars van het Internet der Dingen: fabrikanten, het Rijk, wijzelf? Het panel is in beginsel streng, bij monde van Aad van Boven:"Simpele zaak: er wordt data gelekt via jouw apparaat. Als eigenaar ben je dan ook verantwoordelijk."

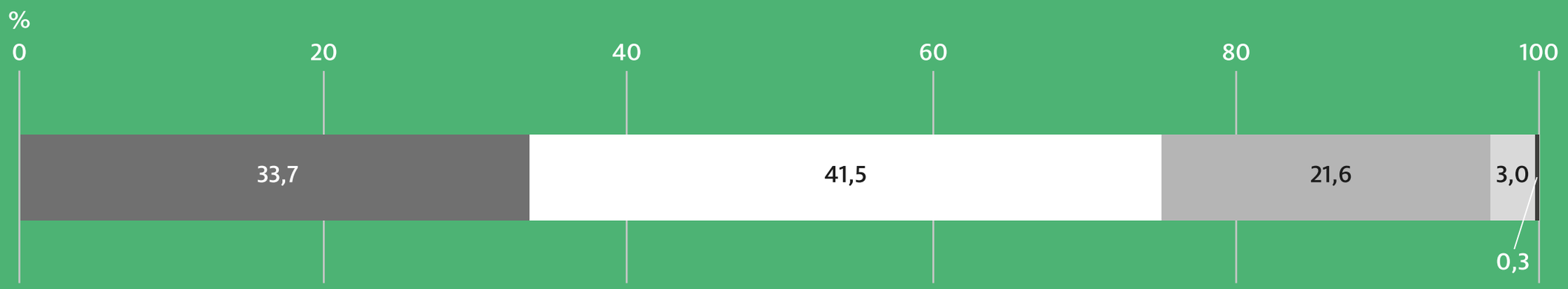
Dat mag volgens de letter der wet misschien zo zijn. Maar veelal onbewust onbekwame consumenten hiermee opzadelen, lijkt toch een beetje onrechtvaardig. Het zit de experts dan ook niet lekker. De producent dan? Gespreksleider Esther Makaay (SIDN en Connectis) verwacht ook van die kant geen wonderen: "Producenten en leveranciers weten dat er een basishygiëne moet zijn, en houden zich daar lang niet altijd aan."

Dan blijft er maar één partij over: de overheid. Hoewel niet van harte, vindt iedereen er uiteindelijk wel iets voor te zeggen dat de politiek voor duidelijke wet- en regelgeving moet zorgen. In dat licht ziet men de nieuwe Europese richtlijn voor cybersecurity (ingevoerd op 12 maart jongstleden) als een goede zaak. Deze richtlijn voorziet onder meer in een certificering voor IoT-apparaten die in Europa zijn verkocht. In eerste instantie vrijwillig, maar in 2023 wordt gekeken of dit verplicht moet worden gesteld.

"Veel consumenten beseffen niet hoe onveilig het IoT nu al is. Slechter kan bijna niet, dus een lichtpuntje is dat het alleen maar beter kan worden. Ik denk overigens wel dat daar een taak voor de overheid ligt. Die zal zich uiteindelijk genoodzaakt zien om in te grijpen en kaders te stellen."

André Koot, Nixu

Meerderheid bezorgd om risico's IoT



- Het wordt veel minder veilig
- Het wordt iets minder veilig
- Dit verandert niet
- Het wordt iets veiliger
- Het wordt veel veiliger

Grafiek 6: Invloed IoT op veiligheid (bron GfK, n=2095)

5 Markt, overheid of wijzelf: wie moet ons beschermen?

De vraag is of meer online veiligheid een private of publieke oplossing vereist. Anders gezegd: moet de markt het oplossen, is het een overheidstaak of ons eigen 'pakkie-an'? Het expertpanel twijfelt, en ook ons onderzoek laat even wisselende als verrassende uitkomsten zien. En nu we het toch over overheidsbemoeienis hebben: wat is eigenlijk het effect van de AVG, een jaar na de invoering van deze wet? Kortom: relevante vragen, goed voor een geanimeerd slotdebat.

Regels zinloos zonder sancties
Aan het publiek/privaat-vraagstuk ging tijdens de paneldiscussie een ander onderwerp vooraf. Alle experts waren hierover stellig en eensgezind: wetgeving is alleen effectief als er sancties aan zijn verbonden. Aad van Boven vat het krachtig samen: 'Compliance en security zijn niet hetzelfde!'

"Security wordt vaak als een IT-probleem gezien, waarbij compliance met nog meer regels elk lek moet zien te dichten. Allebei onjuist. Online veiligheid is een beleidskwestie, het gaat over bedrijfsvoering: welke prioriteiten stel je, hoe richt je processen in. Het is een management-issue, waarbij het management zelf juist vaak de issue is. Ceo's hebben de meeste rechten op hun laptop, maar maken de grootste fouten. Je kunt zo veel regels opleggen als je wilt, maar veiligheid draait uiteindelijk altijd om gedrag."

André Koot (Nixu)

AVG: goede wet, maar papieren tijger
Wat voor organisaties geldt, gaat volgens het panel ook op voor een heel land. De AVG wordt als voorbeeld genomen en het oordeel luidt: prima wet, maar zonder handhaving verslapt de aandacht weer.

"Die AVG was even 'hot news', zeker toen directies en leidinggevenden in aanloop naar de invoering een stortvloed aan waarschuwingsmails kregen. Maar nu, bijna een jaar later, is de aandacht flink verslapt. Het mkb maakt gewoon een risicoanalyse: hoge impact, pakkans nihil. Dus ogen dicht, vingers in je oren en vrolijk verder. Je hebt sancties nodig, anders verandert er niets."

Aad van Boven (SecurMe2)

Juristen blijven alert, ICT'ers minder
Dat zien wij ook terug in de onderzoeksresultaten. Kijken we naar wat onze respondenten hierover zeggen, dan blijkt de brede 'AVG-awareness' van een jaar geleden inderdaad redelijk geslonken. We vroegen zowel ICT'ers als juristen in hoeverre de AVG hun bewustzijn over persoonsgegevens in de organisatie heeft veranderd. De juristen laten op dit punt een specifieke uitschieter zien: 'in zeer sterke mate', zegt maar liefst 72,3%. Niet zo raar, want er zijn weinig rechtsgeleerden te vinden die 'loopt wel los' over een wet zeggen.

> Grafiek 7: In welke mate heeft de AVG het bewustzijn ten aanzien van persoonsgegevens binnen uw bedrijf beïnvloed? (bron GfK, n=512)

Bij de ICT'ers geeft slechts 2,2% hetzelfde antwoord (zeer sterk veranderd), terwijl ruim een derde (33,8%) zegt dat hun bewustzijn over persoonsgegevens 'in sterke mate' is veranderd door de AVG. Bijna de helft (48,8%) antwoordt dat dit 'in enige mate' het geval is. En al met al toch een vrij fors aandeel (15,2%) zegt dat hun bewustzijn 'helemaal niet' is veranderd. Samengevat: onder ICT'ers lijkt het urgentiebesef na een jaar erg laag, juristen reageren karaktercongruent en blijven beroepsmatig alert.

Het expertpanel blijft ondertussen praktijkvoorbeelden noemen. Zo verwijst Maria Genova naar het bankwezen:

"DNB en de ECB vaardigden formele veiligheidsrichtlijnen uit, redelijk vrijblijvende oekazes over wat wel en niet meer mocht. Had weinig effect, totdat ze banken gingen bezoeken en ondervragen: "Hebben jullie je security op orde? Laat maar zien." Dat werkte wel, want regels zijn alleen effectief als er een incentive is om ze na te leven. Met boxjes afvinken creëer je schijnveiligheid."

Maria Genova (auteur, journalist, spreker)

Het panel twijfelt

Blijft over de finale vraag wie er nu formeel moet waken over onze online veiligheid: de markt, die hiervoor producten en diensten kan ontwikkelen? Of de overheid, die met wet- en regelgeving (mits gehandhaafd) bescherming kan afdwingen?

De discussie in het expertpanel rond e-ID & de AVG laat zien hoe ambivalent dit is. Enerzijds zien zij de overheid als verantwoordelijk, want die heeft de AVG tenslotte gemaakt. Aan de andere kant komen veel security-ontwikkelingen uit de markt, zonder bijdrage van diezelfde overheid. En waar de overheid wél meedeed, was dat niet bepaald een succes. Laat dat soort projecten aan de markt over, die heeft er alles voor in huis.

Jongeren wijzen naar de overheid

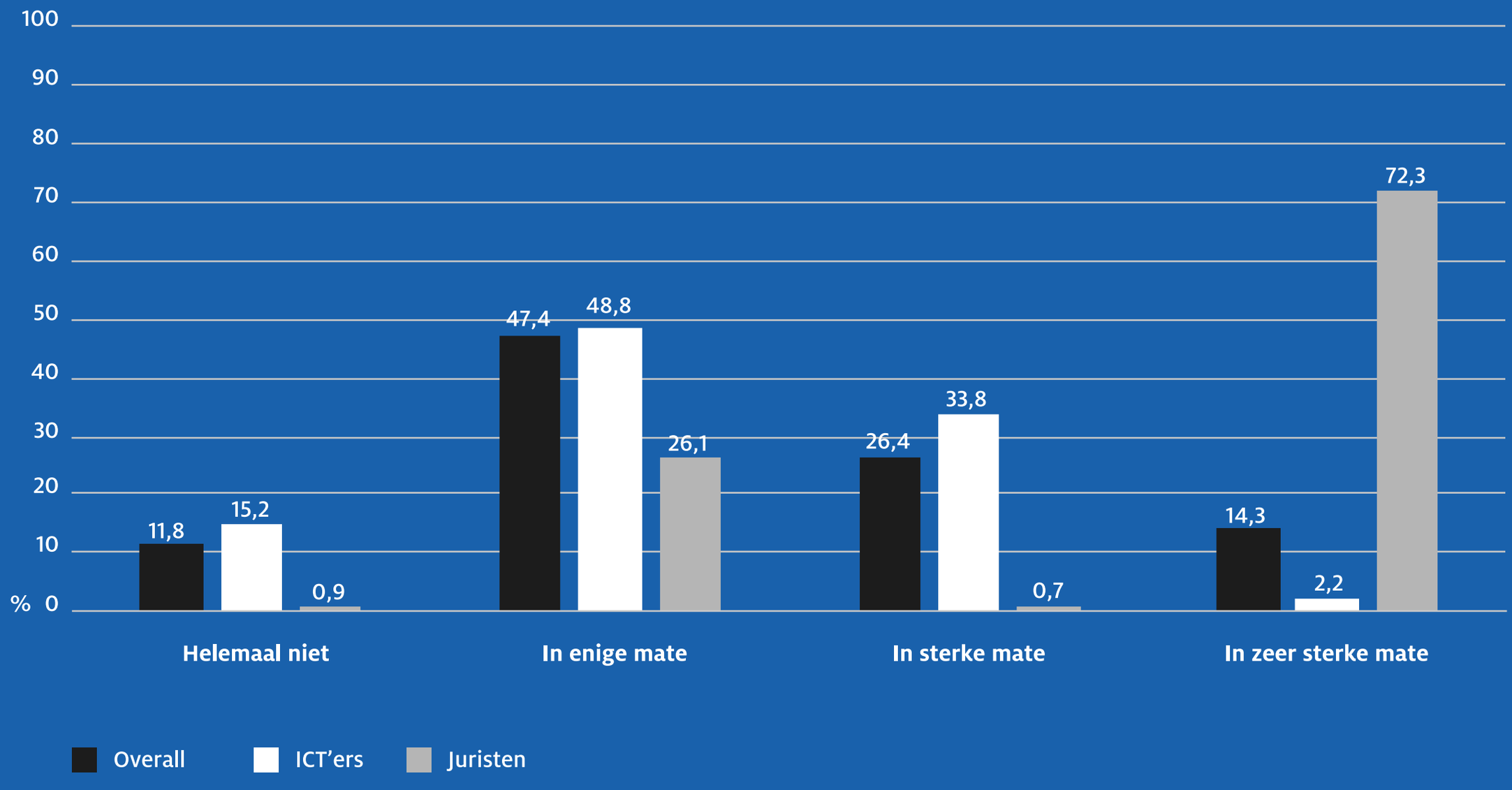
Het laatste woord is aan onze respondenten. Wat antwoorden zij op de vraag wie er primair verantwoordelijk is voor de online veiligheid van consumenten? In tegenstelling tot ons expertpanel, dichten beide groepen ondervraagden de markt juist een relatief beperkte rol toe: 12,7% (iedereen) versus 18,0% (jongeren). De race gaat dus tussen onszelf en de overheid, waarbij alle ondervraagden bij elkaar overtuigend voor eigen verantwoordelijkheid kiezen (57,6%), met de overheid als goede tweede (29,7%). Opvallend is wel dat jongeren relatief veel verantwoordelijkheid leggen bij de overheid (40,8%). Dat schept verwachtingen voor de toekomst die de politiek serieus zou moeten nemen.

> Grafiek 8: Wie ziet u als primair verantwoordelijk voor online veiligheid van consumenten? (Bron gfK, n=2095)

Dit alles leidt tot drie conclusies:

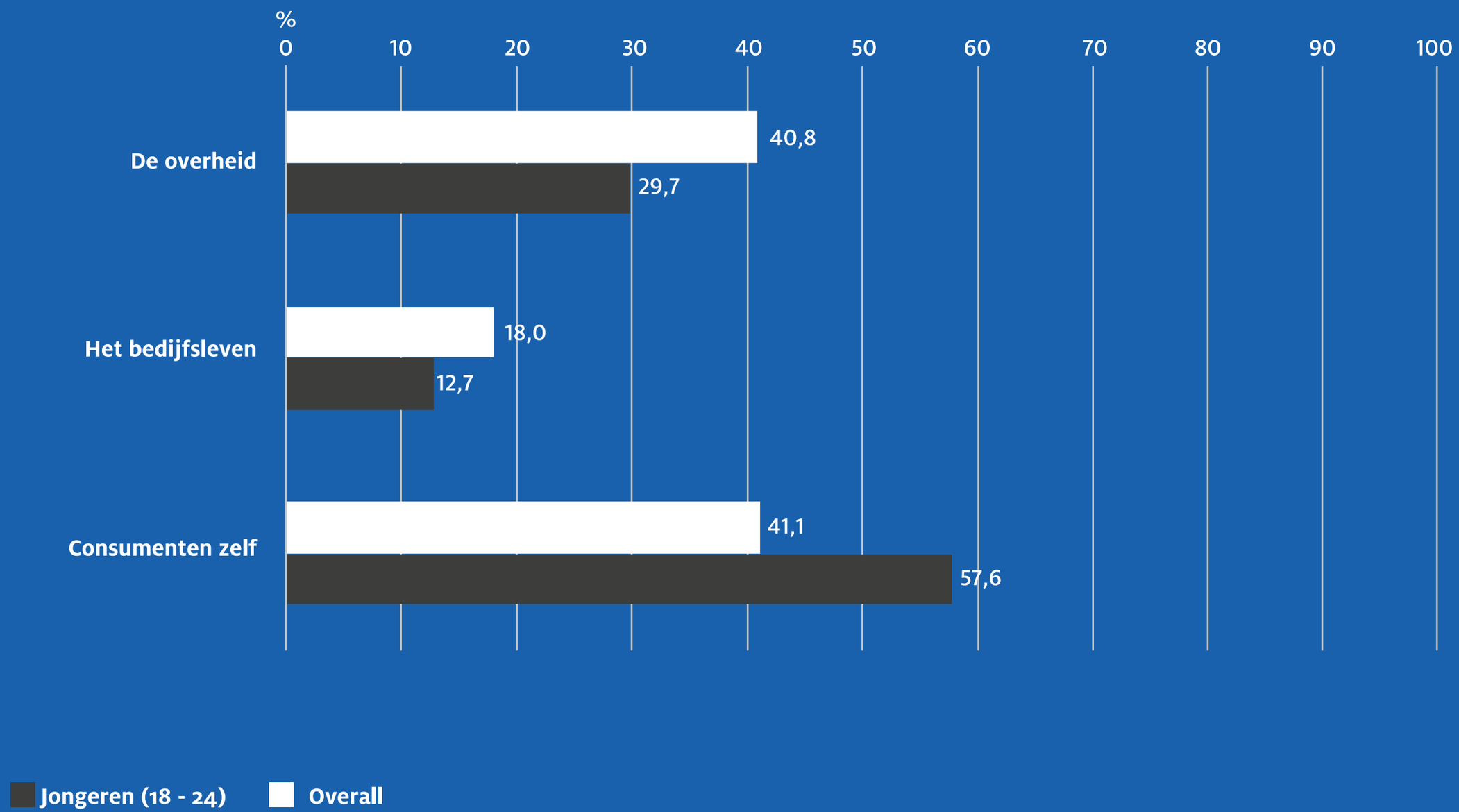
1. Dankzij een gewaardeerde AVG speelt de overheid op dit moment indirect een positieve rol in het online veiligheidsvraagstuk.
2. Om een wassen neus-effect te voorkomen, is het wel belangrijk dat de overheid haar eigen wet- en regelgeving handhaaft. Precies zoals dat in de private sector ook een positief verschil maakt.
3. Tegen de overheid zouden we willen zeggen: 'you better shape up', want er is een digitale generatie in aantocht die online veiligheid vrij vanzelfsprekend als een overheidstaak beschouwt.

AVG leeft vooral bij juristen



Grafiek 7: In welke mate heeft de AVG het bewustzijn ten aanzien van persoonsgegevens binnen uw bedrijf beïnvloed? (bron GfK, n=512)

Jongeren verwachten grotere rol overheid



Grafiek 8: Wie ziet u als primair verantwoordelijk voor online veiligheid van consumenten? (Bron gfK, n=2095)

6 Ontmoet het expertpanel

Aad van Boven (SecureMe2) Vanuit zijn operationele ICT-achtergrond vervulde Aad tussen 1990 en 2008 vaste functies in o.a. de energie-, telecom- en zorgsector. Rode draad in zijn werk: beschikbaarheid, performance en veiligheid van ICT-infrastructuren. Daarna werd hij als zelfstandige ingehuurd, meestal om als programma- of projectmanager complexe en vastgelopen ICT-projecten vlot te trekken. In 2016 startte Aad SecureMe2, met als doel organisaties via hoogwaardige technologie weerbaarder te maken in het spanningsveld tussen toenemende cyber-dreigingen en steeds striktere wet- en regelgeving.

Maria Genova (auteur/journalist) Als onderzoeksjournalist schreef Maria o.a. 'Komt een vrouw bij de h@cker'. Mede dankzij dit succes-volle boek, wordt ze veel gevraagd om te spreken over identiteitsfraude, privacy en informatiebeveiliging. Ze gaf honderden interactieve lezingen in alle sectoren, gedreven door haar missie: zo veel mogelijk mensen en bedrijven weerbaar maken tegen de groeiende digitale gevaren.

André Koot (Nixu) Behalve een zeer ervaren adviseur op het gebied van informatiebeveiliging, is André specialist op het gebied van Identity Management en Autorisatiebeheer.Hierover heeft hij een uitgesproken mening: het zijn verschillende vakgebieden. Daarnaast voert hij een persoonlijke kruistocht tegen misbruik van het woord 'cyber'.

Esther Makaay (Connectis) Als deskundige op het gebied van inter-nettechnologie is Esther gespecialiseerd in digitale identiteiten. Voor Connectis ontwikkelt ze innovaties op het gebied van eID. Enkele van haar expertisevelden: vertrouwenskaders, digitale identiteiten en eID-schema's, DNS (SEC) en (nieuwe) topleveldomeinen.

Kees Monshouwer (Monshouwer Internet Diensten) Kees is registrar van SIDN en lid van de Commissie Techniek van de Vereniging van Registrars. Kortom: een ervaren ondernemer in de hostingbranche. De laatste jaren adviseerde hij SIDN en haar registrars vaak over de implementatie van open standaarden voor een veiliger internet (DNSSEC).

Remco Poortinga-van Wijnen (SURFnet) Na zijn studie Elektrotechniek (Universiteit Twente, 1997) begon Remco als software developer bij Ericsson. Zijn volgende halte: het Telematica Instituut, waar hij onder meer als research engineer werkte. Door zijn ruime ervaring in middleware, federatief identity management, software-architectuur, security- en projectmanagement, trad hij in 2008 in dienst bij SURFnet. Als teamhoofd Security & Privacy is Remco, samen zijn collega's, verantwoordelijk voor de dienstverlening binnen deze deelgebieden, en de innovatie hiervan.

Aad van Boven, Kees Monshouwer Remco Poortinga-van Wijnen, Esther Makaay, Maria Genova en André Koot.

Colofon

Dit is een verslag van een onderzoeksrapport dat is samengesteld door GfK in opdracht van SIDN en Connectis.
Aan dit verslag werkten mee:

GfK
Henk Delfos – Industry Lead
Ewout Witte – Business Analist

SIDN
Michiel Henneke – Marketingmanager
Christiene Bouwens – Marketingmanager
Marnie van Duijnhoven – Communicatiemanager

Connectis
Ellen Breugem - Manager Marketing & Communicatie
Esther Makaay - Business & eID Analyst

Tekstwerf
Rosanne Koppert - Copywriter
Joa Smits – Copywriter

Heb je vragen over het onderzoek, mail dan naar
communicatie@sidn.nl

SIDN
Postbus 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
T +31 (0)26 352 55 00
www.sidn.nl

Connectis
Postbus 975
3000 AZ Rotterdam
Weena 327-329
3013 AL Rotterdam
T +31 (0)88 012 02 22
https://connectis.com