ONDERZOEKSRAPPORT

Cybersecurity is essentieel voor digitaal fundament van de samenleving

Pleidooi voor de oprichting van een Digitalisatie Management Team, dat overheid en samenleving adviseert over cybersecurity

telindus
a Proximus company

1. Inleiding

De overheid lijkt meer en meer de regie te nemen als het gaat om het weerbaarder maken van de samenleving tegen cybercriminaliteit. Het besef groeit dat de bedreigingen en kwetsbaarheden in de digitale infrastructuur groot en talrijk zijn. Hoewel we in het recente verleden meer activiteiten hebben gezien van instanties als het Nationaal Cyber Security Centrum (NCSC) en hoewel de IT-sector blijft werken aan het vergroten van het bewustzijn rondom cybersecurity, blijkt dat we als maatschappij te weinig vooruitgang boeken. In het recente verleden hebben we bijvoorbeeld gezien dat delen van de vitale sectoren kwetsbaar zijn. Dat was het geval toen Citrix in 2020 een open achterdeur bleek te hebben en talloze overheidsinstellingen uit voorzorg de dienstverlening tijdelijk stillegden. Dat zagen we ook recent nog bij de kwetsbaarheid in de Apache Log4j-software. Los daarvan zoeken hackers continu naar mogelijkheden om binnen te dringen en data buit te maken of malware te planten, om uiteindelijk losgeld te kunnen eisen voor het ontsleutelen van systemen. En vandaag de dag waarschuwt het NCSC voor aanvallen van hackerscollectieven die het voorzien kunnen hebben op Nederland en Nederlandse instellingen vanwege de steun aan Oekraïne.

> **"... hoewel de IT-sector blijft werken aan het vergroten van het bewustzijn rondom cybersecurity, blijkt dat we als maatschappij te weinig vooruitgang boeken."**

Digitale weerbaarheid

Er zijn de laatste jaren ontegenzeggelijk grote vorderingen gemaakt als het gaat om digitale weerbaarheid in het Nederlandse bedrijfsleven en binnen de overheid. Dat is echter geen reden om achterover te leunen, denkend dat we de zaken voor elkaar hebben. Dit is een van de redenen waarom in het nieuwe kabinet een staatssecretaris digitalisering is benoemd. Zij zal zich in de eerste plaats richten op vier thema's, die duidelijk worden uit het beleid op hoofdlijnen dat onlangs naar de Tweede Kamer is gestuurd:

- Digitaal fundament.
- Digitale overheid.
- Digitale samenleving.
- Digitale economie.

Binnen het digitaal fundament wordt cybersecurity gezien als een essentiële randvoorwaarde voor succesvolle digitalisering en het is daarmee een prioriteit. Vanuit deze wetenschap zal de staatssecretaris collega's in het kabinet tot daadkracht willen aanzetten. Denk dan aan de ministers van Veiligheid en Justitie, die het cybersecurity-terrein coördineert, en van Economische Zaken, die zich inspant voor het realiseren van een hoogwaardige, betrouwbare en betaalbare digitale infrastructuur. Alom werd de aanstelling van een staatssecretaris voor digitalisering toegejuicht, maar er werden ook direct kanttekeningen bij geplaatst. Zo zou de bewegingsruimte beperkt zijn, evenals de budgetten - die veelal bij andere departementen gevonden moeten worden. Verder valt op dat staatssecretaris Alexandra van Huffelen (waarom geen minister?) niet echt bekend staat om haar kennis van de ICT-sector in het algemeen en cybersecurity in het bijzonder.

> **Wat zou de meerwaarde zijn van een Digitalisatie Management Team, met al zijn kennis en tentakels in de samenleving? Telindus is voorstander van een DMT en zou graag een van die experts zijn die aanschuift bij een DMT."**

Binding met de samenleving

Het is dan ook interessant om te zien hoe de mensen die dagelijks tijdens hun werk te maken hebben met cybersecurity hier tegenaan kijken. Telindus voerde een onderzoek uit onder 1.049 werkende Nederlanders tussen de 18 en de 67 jaar met een kantoorbaan. Vinden zij de overheid inderdaad verantwoordelijk voor cybersecurity of wijzen deze kenniswerkers toch vooral naar zichzelf als werknemers en consumenten om zich beter te wapenen tegen cybercriminaliteit? En hoe hoog is het vertrouwen in een bewindspersoon die zich focust op digitalisering, wat kunnen we van haar verwachten? De vraag is ook of één post in de regering ervoor zorgt dat er voldoende binding is met de samenleving. Zou Van Huffelen zich niet moeten omringen met experts - wetenschappers, securityexperts van leveranciers, opsporingsdiensten, bedrijfsleven - vergelijkbaar met een Outbreak Management Team dat de overheid adviseert over zaken omtrent Covid-19? Wat zou de meerwaarde zijn van een Digitalisatie Management Team, met al zijn kennis en tentakels in de samenleving? Telindus is voorstander van een DMT en zou graag een van die experts zijn die aanschuift bij een DMT.

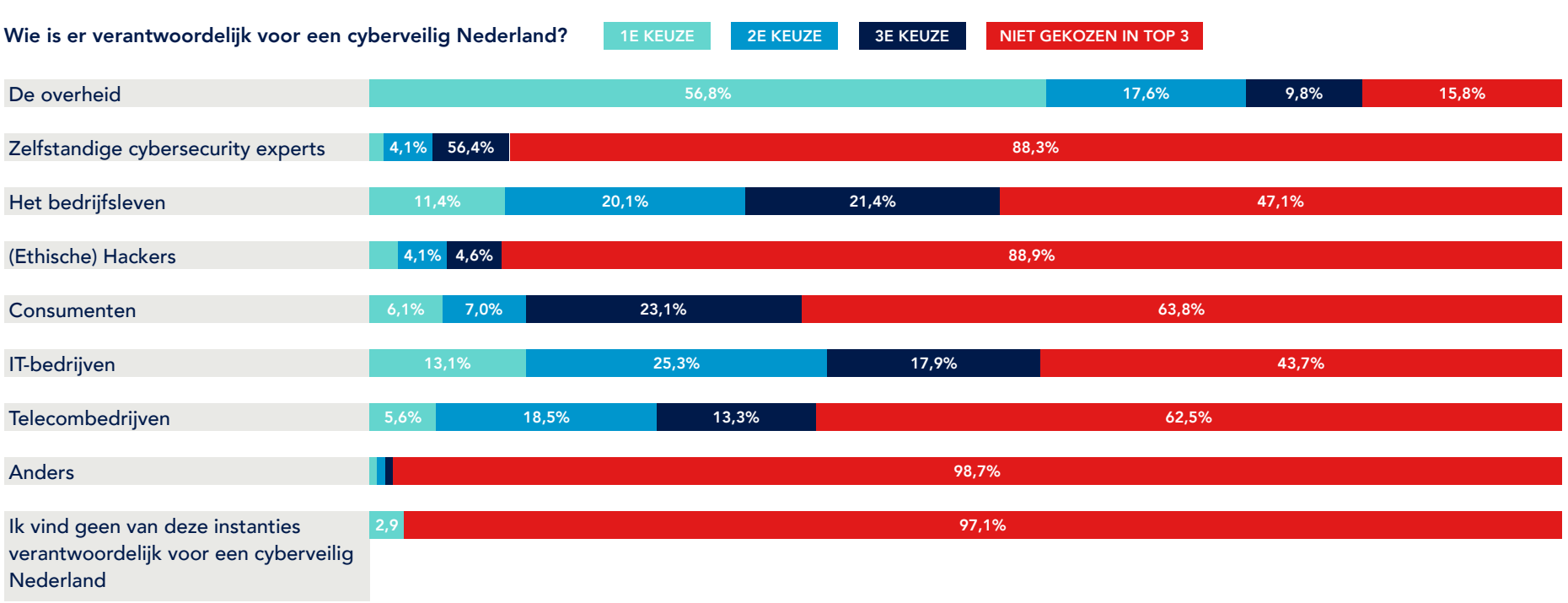
2. Daadkrachtige overheid

Dat de overheid nu daadkrachtiger optreedt en zichtbaarder is in het domein van cybersecurity komt dus onder andere tot uiting in de aanstelling van een staatssecretaris digitalisering. Verder zien we dat dit kabinet vanaf 2027 structureel 300 miljoen euro investeert in onder andere de slagkracht van de AIVD, MIVD, NCSC en het bredere beleidsterrein van economische veiligheid, cybersecurity en de vitale infrastructuur. De overheid zelf hanteert de stelregel ‘security by design’ als het om haar eigen systemen gaat. Op Europees niveau wordt samengewerkt aan de herziening van de Europese Netwerk- en Informatiebeveiligingrichtlijn (NIB2), waardoor veel meer bedrijven in essentiële en belangrijke sectoren, zoals drinkwater en de zorg, te maken krijgen met wettelijke verplichtingen op het gebied van cybersecurity. Hoewel sommige analisten van mening zijn dat het niet goed is regels op te leggen en dat we het meer moeten hebben van zelfregulering, is het goed dat er duidelijke kaders zijn. Je weet als organisatie wat je minimaal nodig hebt om aan de richtlijn te voldoen en je weet dat je hierover moet rapporteren.

Hoewel sommige analisten van mening zijn dat het niet goed is regels op te leggen en dat we het meer moeten hebben van zelfregulering, is het goed dat er duidelijke kaders zijn."

Overheid verantwoordelijk voor cyberveilig Nederland

Deze ontwikkeling, waarin de regie en verantwoordelijkheid liggen bij de overheid, wordt aangemoedigd door een overgrote meerderheid van de respondenten (85 procent). 57 procent zet de overheid op nummer 1 op de vraag wie er verantwoordelijk is voor een cyberveilig Nederland. Dit wil niet zeggen dat de overheid alles moet afdwingen met wet- en regelgeving, maar deze percentages geven wel aan dat de overheid het voortouw moet nemen om bijvoorbeeld dreigingsinformatie te delen en IT-bedrijven met elkaar aan tafel te krijgen om samen te werken in het kader van cybercriminaliteit. Nu is kennis erg versnipperd en dat werkt niet effectief. Dat terwijl bijvoorbeeld Cisco zijn wereldwijde dreigingsinformatie breed deelt met klanten, andere security partijen en communities. En ook



een bedrijf als Davinsi Labs, onderdeel van de Proximus Groep, heeft zijn handen vol aan het verzamelen en delen van threat intelligence. Telindus doet er vervolgens alles aan om de informatie van onze partners tijdig bij de klant te krijgen. 13 procent van de respondenten is zelfs van mening dat IT-bedrijven verantwoordelijk zijn voor een cyberveilig Nederland. Een iets kleiner aantal (11 procent) vindt dat het bedrijfsleven zelf verantwoordelijk is voor een cyberveilig Nederland.

De basis van succesvol securitybeleid

Ten slotte valt op dat 6 procent van de ondervraagde kantoorwerkers zichzelf als consument en eindgebruiker verantwoordelijk vindt. Dan hebben we het over bewustzijn, dat nog altijd het fundament is onder effectief securitybeleid. De basishygiëne, zou je het kunnen noemen. Het wordt voor de eindgebruiker op de laptop van zijn werk en de consument met al zijn verschillende communicatiekanalen erg ingewikkeld. De cyberaanvallen worden steeds brutaler en geavanceerder. Toch ligt hier de basis van een succesvol securitybeleid. Je kunt als eindgebruiker veel zelf voorkomen en risico's vermijden, als je maar goed uitkijkt. Het is net als met oversteken: eerst links kijken, dan rechts kijken en dan nog een keer links.

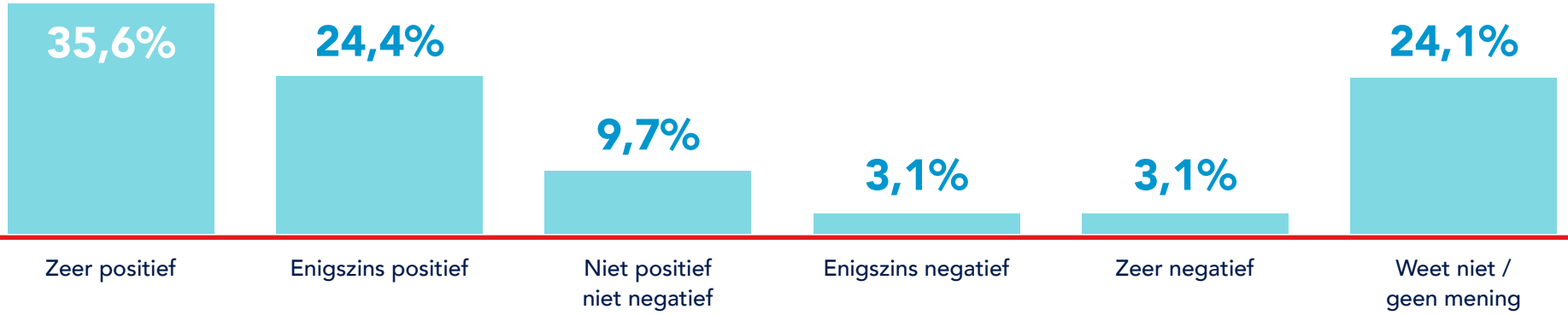
3. Succesvolle digitalisering gaat niet zonder cybersecurity

We kunnen dus vaststellen dat we vrij massaal naar de overheid kijken als het gaat om succesvol cybersecuritybeleid. In dit opzicht is de aanstelling van Van Huffelen een goede stap. Dit wordt bevestigd door het onderzoek. 60 procent van de respondenten is zeer of enigszins positief over de aanstelling van de nieuwe staatssecretaris van Digitalisering. Slechts 6 procent is ronduit negatief en de rest heeft zich nog geen mening kunnen vormen. We hebben de respondenten ook om een toelichting gevraagd. Degene die positief zijn over de nieuwe bewindspersoon wijzen erop dat security steeds belangrijker wordt in een samenleving die steeds digitaler wordt. Het is goed dat de overheid nu centraal initiatieven gaat ontplooien. Verder zien we de volgende uitspraken:

- De overheid gaat de komende tijd steeds meer automatiseren en de beveiliging van kwetsbare nutsbedrijven en infrastructuur kun je niet aan de markt overlaten."
- De wereld is aan alle kanten verbonden maar dat brengt ook gevaren met zich mee, omdat we ook alles maar aan elkaar knopen. Tegen die gevaren moeten we ons centraal beschermen."
- Digitalisering [...] is de drijfveer voor de grote veranderingen in de afgelopen 30 jaar en de overheid loopt ver achter in zowel stimuleren van investeringen als regulering."
- Dit past bij de moderne tijd. Digitalisering is niet meer weg te denken in onze maatschappij en het is goed dat de belangen en regels daarvan via een staatssecretaris betere aandacht krijgen."
- Hadden ze 30 jaar geleden al moeten instellen."
- Het is eigenlijk al veel te laat dat deze persoon is aangesteld. De samenleving, en zeker de overheid, moet meer ingericht worden op digitale veiligheid en zoveel mogelijk uit digitale technologie halen op een verantwoorde manier."
- We leven in een tijd leven waarin het steeds vaker voorkomt dat er sprake is van cybercrime, hacks, DDoS-aanvallen, stelen van digitale gegevens, etc. De consument/particulier in z'n eentje kan hier niets of niet veel aan doen."

Bovenstaande reacties moeten de huidige regering toch als muziek in de oren klinken, louter steun voor de beslissing. Kanttekening is wel dat veel respondenten het eigenlijk veel te laat vinden.

Hoe staat u tegenover de aanstelling van de nieuwe staatssecretaris van Digitalisering?



Achter de feiten aanlopen

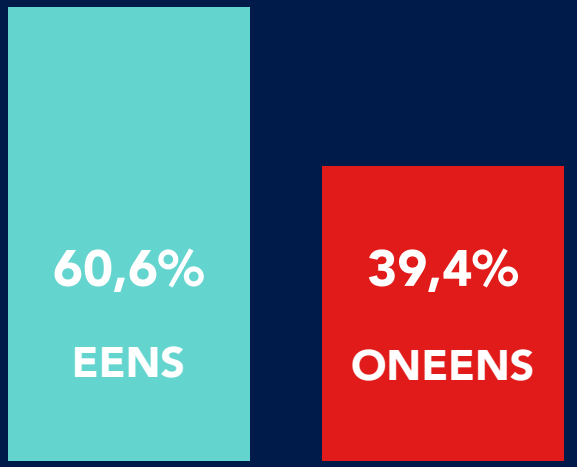
Maar eerlijk is eerlijk, er zijn ook negatieve sentimenten ten aanzien van de staatssecretaris van digitalisering, hoewel deze veruit in de minderheid zijn. Uiteraard komt een aantal reacties van mensen die überhaupt geen vertrouwen (meer) hebben in de politiek. Ook valt op dat een flink aantal respondenten geen vertrouwen heeft in de bewindspersoon omdat die geen achtergrond en kennis zou hebben in de IT: “totaal geen kennis van zaken, zal weer kapitalen aan ‘adviseurs’ gaan uitgeven”. Of deze: “Het is een politicus en die heeft geen verstand van deze zaken.” En deze respondent ziet het ook somber in: “We lopen hoe dan ook achter de feiten en de criminelen aan. Het is wachten op een verkeersinfarct op de digitale snelweg en het hacken van vitale systemen van ministeries en infrastructuur; er zou héél veel geld naar bestrijding en preventie moeten maar dat heeft de staatssecretaris toch niet.”

Aanpak van cybercriminaliteit was te versnipperd

Uit het onderzoek blijkt dat men in het verleden de aanpak van cybercriminaliteit te versnipperd vond. Vervolgens zien we dat bijna 90 procent van mening is dat in de Nederlandse IT-infrastructuur en regelgeving, fundamentele veranderingen nodig zijn om cyberaanvallen tegen te gaan. Je zou dus kunnen zeggen dat er een flink mandaat nodig is om fors in te grijpen. De staatssecretaris zal snel met concrete plannen moeten komen om het vertrouwen te krijgen van de samenleving en samen met het bedrijfsleven en IT-ondernemingen de juiste maatregelen te nemen.

4. Pleidooi voor DMT: Digitalisatie Management Team

Om dit vertrouwen te wekken en inderdaad als een daadkrachtige overheid op te treden, zou de regering er goed aan doen een Digitalisatie Management Team aan te stellen. Dit kun je vergelijken met het Outbreak Management Team dat de minister van Volksgezondheid in de COVID-crisis adviseerde. Ruim 60 procent van de respondenten vindt dit een goed idee. Leden van dit adviesorgaan hebben kennis van zaken, weten waarover zij spreken en kunnen de gevolgen van maatregelen - of het uitblijven daarvan - goed beargumenteren. Zo'n DMT bestaat uit mensen uit het bedrijfsleven (grootbedrijf en MKB), IT-dienstverleners, digitale forensische experts en wetenschappers. Een beslissing van de overheid in het kader van cybersecurity heeft zo veel meer gewicht als er een groep experts achter staat. Deze mensen kunnen het ook goed uitleggen wanneer zij bij Op1 of Jinek bepaalde keuzes komen uitleggen.

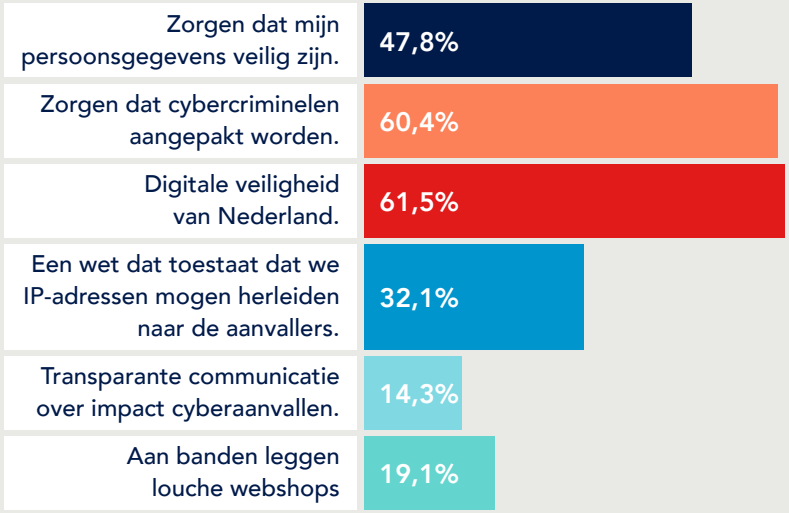


Ik vind dat er naast het OMT (Outbreak Management Team) ook een DMT (Digitalisatie Management Team) in het leven mag worden geroepen. Dit als adviesorgaan voor de Staatssecretaris van Digitalisering, zoals het OMT dat is voor Volksgezondheid.

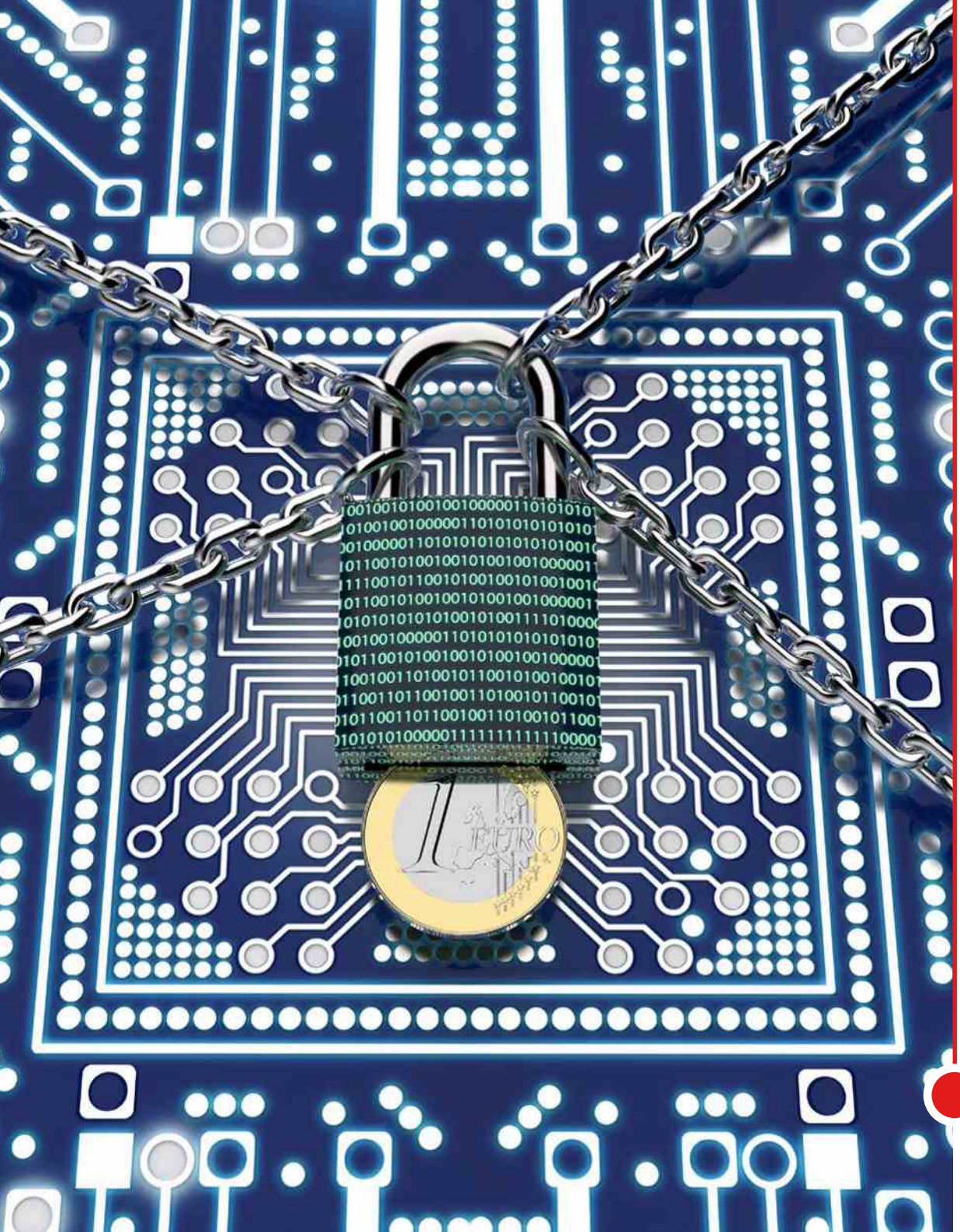
Prioriteiten staatssecretaris van Digitalisering

We hebben in het onderzoek de vraag gesteld wat er bovenaan de agenda moet staan van de staatssecretaris van Digitalisering. Dan tekent zich een scherpe top-3 af. Op 1 en 2 staan: 'Digitale veiligheid van Nederland' en 'Zorgen dat cybercriminelen worden aangepakt'. Beide prioriteiten scoren meer dan 60 procent. Op de derde plaats staat 'ervoor zorgen dat mijn persoonsgegevens veilig zijn', met 32 procent.

Wat moet er bovenaan de agenda van de staatssecretaris van Digitalisering staan?

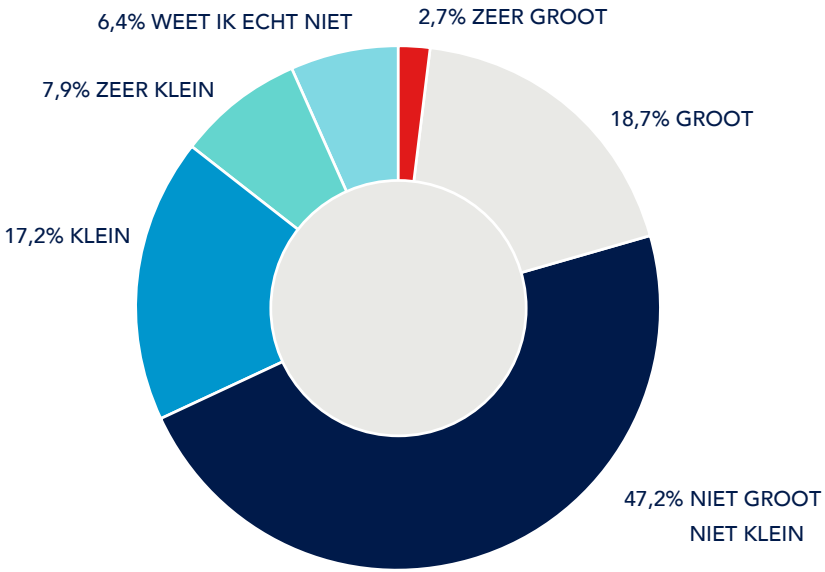


Een DMT zou ook een grote impuls zijn voor het bewustzijn van de gevaren van cybercriminaliteit. Ondanks het feit dat dit bewustzijn best hoog is, kunnen hier nog altijd stappen worden gezet. Bijna niemand gelooft dat we over 5 jaar van ransomware verlost zijn omdat we cybercriminelen te slim af zijn. En bijna 85 procent is ervan overtuigd dat we ransomware in stand houden door aanvallers te betalen. Een vijfde van de respondenten acht de kans dat de organisatie waar hij of zij werkt wordt platgelegd door ransomware groot of zeer groot. Een kwart acht die kans klein tot zeer klein. De helft durft zich niet uit te spreken of heeft geen idee. Telindus heeft al eerder opgeroepen om als overheid en industrie de handen ineen te slaan en te zorgen voor een fonds. Dit zou kunnen worden opgebouwd door bedrijven en instellingen en worden aangesproken op het moment dat een organisatie is getroffen; het fonds is dan bestemd voor het herstellen van de IT-infrastructuur zonder dat er losgeld betaald wordt. Ook een mooie taak voor het nieuwe DMT.



Het DMT kan eveneens een rol spelen zoals bij het vergroten van het bewustzijn omtrent het gebruiken van openbare Wifi-hotspots voor het werk, bijvoorbeeld in de trein of in een hotel. 50 procent doet dit nooit; 5 procent doet dit 3 keer in de week of vaker. Die 50 procent is mooi, maar je kunt ook zeggen dat de andere helft zich nog eens achter de oren moet krabben. Is een openbare wifiverbinding wel zo verstandig? Nee, beaamt ruim 86 procent, en toch maken ze er gebruik van. Het is tijd dat hiervoor een zero trust-beleid wordt opgesteld, zodat medewerkers wel kunnen werken op een publieke hotspot, maar absoluut niet bij bedrijfskritische gegevens kunnen.

De kans dat je organisatie wordt platgelegd door ransomware

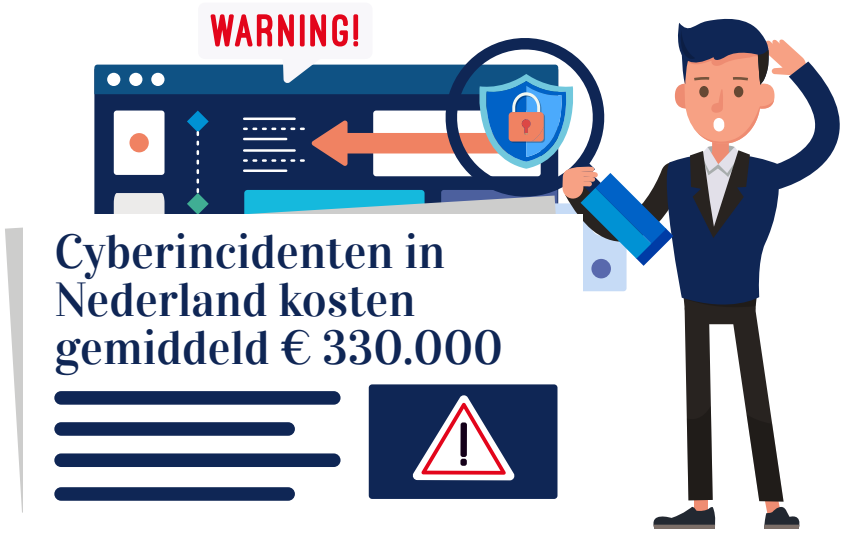


4. Conclusie

Het is duidelijk dat de stap van de overheid om gericht aan de slag te gaan met digitalisering en cybersecurity wordt aangemoedigd door de samenleving. De staatssecretaris van of voor digitalisering zal zich nog wel moeten bewijzen. Uit het onderzoek komt ondubbelzinnig naar voren dat het bewustzijn van de gevaren van cybersecurity is gegroeid en dat de samenleving vindt dat de overheid de regie moet pakken. De overheid kan deze uitdaging echter niet alleen aan. Om cybersecurity werkbaar, efficiënt, betaalbaar en succesvol te maken, moeten overheid en IT-bedrijven samenwerken. We mogen dit moment niet voorbij laten gaan!

> **Uit het onderzoek komt ondubbelzinnig naar voren dat het bewustzijn van de gevaren van cybersecurity is gegroeid en dat de samenleving vindt dat de overheid de regie moet pakken."**

Telindus heeft dit onderzoek onder andere uitgevoerd om een beeld te krijgen van de perceptie rondom cybersecurity en digitalisering. Waar hebben medewerkers behoefte aan, wie moet volgens hen het initiatief nemen en hoe zien zij hun eigen rol om cybersecurity naar een hoger niveau te krijgen? Telindus zet zich via verschillende kanalen in om organisaties te adviseren de juiste maatregelen te nemen om kwetsbaarheden te omzeilen en optimaal te profiteren van de digitale transformatie. De organisatie van de toekomst is namelijk een digitaal weerbare; optimaal balancerend tussen gebruiksgemak en securitymaatregelen. Gebruik de uitkomsten van dit onderzoek dan ook om deze balans te vinden voor je eigen organisatie.



telindus
a Proximus company

Krommewetering 7
3543 AP Utrecht
T: +31 (0)30 – 247 77 11
www.telindus.nl