Nationale Cybersecurity Monitor 2022

Onderzoek onder 250 Nederlandse organisaties in opdracht van Infosecurity Magazine

Peter Vermeulen

Pb7 Research

April 2022

LuteijnMedia

Inhoud

Inleiding

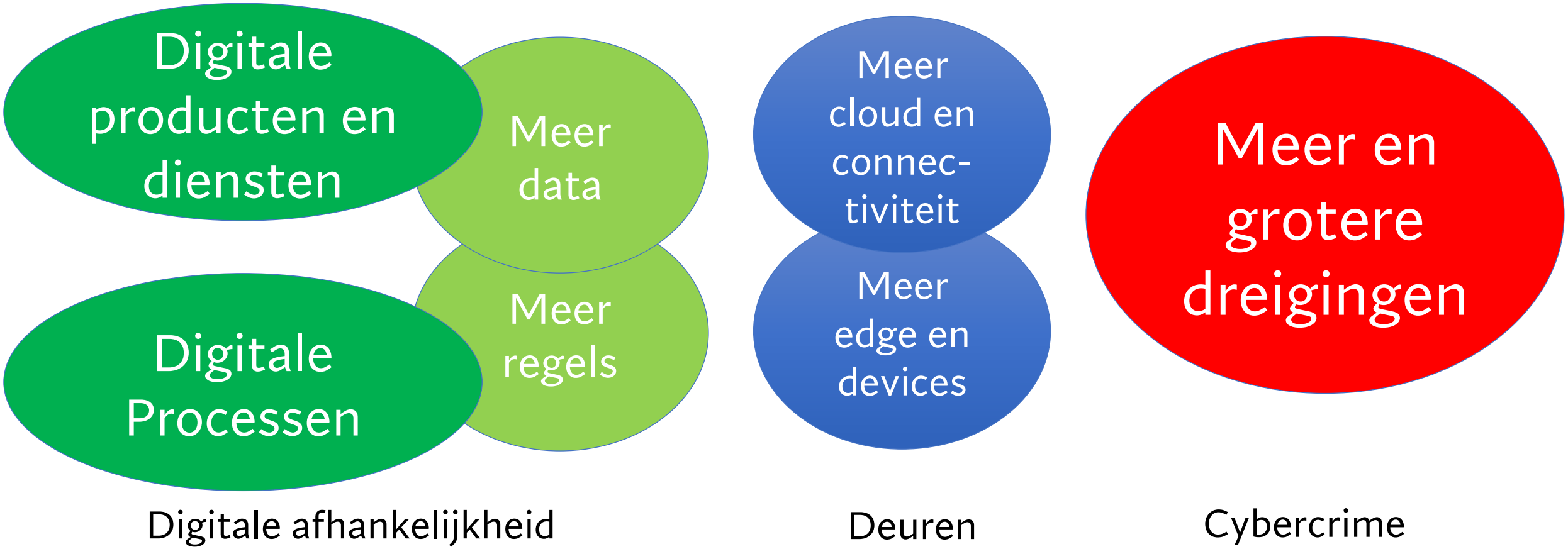
De laatste cybersecurity monitor dateert van twee jaar geleden, december 2019. In de tussentijd is er veel gebeurd. Heel veel. We hebben een pandemie zien ontstaan en schudden deze nu, twee jaar later, eindelijk van ons af. Inmiddels zijn we alweer een nieuwe grote crisis ingerold, met de invasie van Rusland in de Oekraïne. Is het toeval dat in de aanloop van deze oorlog een golf van ransomware over de wereld spoelde, of was dat eerder een gevolg van de ontwikkeling van coronaproof criminaliteit? Hoe dan ook kan het niemand ontgaan zijn dat het cyberdreigingsbeeld aanzienlijk is verslechterd.

Tegelijkertijd is de afhankelijkheid van IT voor bedrijven versneld toegenomen en zijn er door al die thuiswerkers een enorme hoeveelheid te beveiligen toegangspoorten tot het bedrijfsnetwerk ontstaat. Naast alle ontwikkelingen op IT-gebied, gaan bedrijven ook steeds meer investeren in IoT en neemt het bewustzijn toe dat de securityrisico's op OT-vlak steeds groter worden.

In de cybersecuritymonitor biedt onafhankelijk ICT-onderzoeksbureau Pb7 Research inzicht in hoe Nederlandse bedrijven en instellingen deze uitdagingen ervaren en hoe ze erop reageren.

Pb7 doet dat in opdracht van LuteijnMedia, uitgever van Infosecurity Magazine, één van de platformen van LuteijnMedia. Het onderzoek is financieel mogelijk gemaakt door Smile en Tesorion. Dit document geeft de analyse van Pb7 Research weer. De opdrachtgever en sponsors zijn het niet noodzakelijkerwijs eens met de gepresenteerde conclusies.

Waarom cybersecurity steeds belangrijker wordt

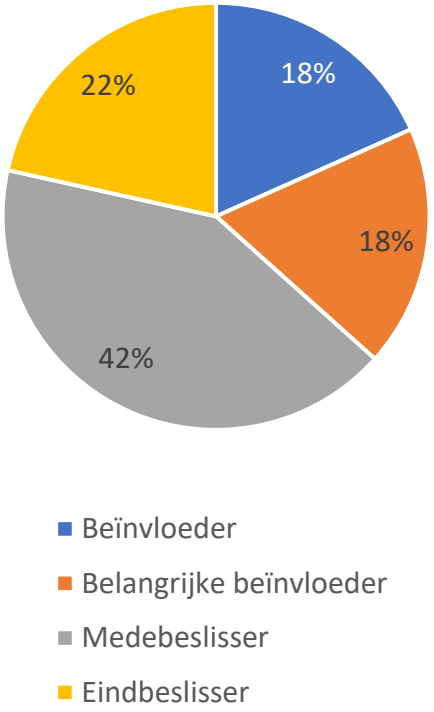


Over het onderzoek

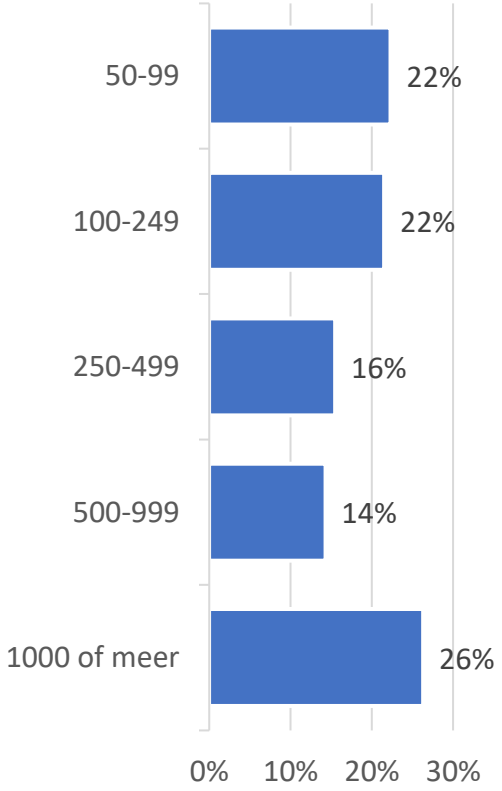
Pb7 Research heeft begin maart 2022, voor de invasie van Oekraïne, 250 IT en OT securitybeslissers die werkzaam zijn bij organisaties met 50 of meer medewerkers ondervraagd met behulp van een web gebaseerde survey. De vragenlijst is door Pb7 Research samengesteld. De sponsors kregen de mogelijkheid om enkele meeloopvragen toe te voegen.

De respondenten zijn voornamelijk eind- of medebeslissers bij investeringen in IT- en/of OT-beveiliging. Ongeveer de helft van de respondenten zijn werkzaam met bedrijven tussen de 50 en 250 medewerkers en de rest bij grotere organisaties. De respondenten zijn afkomstig van een business panel.

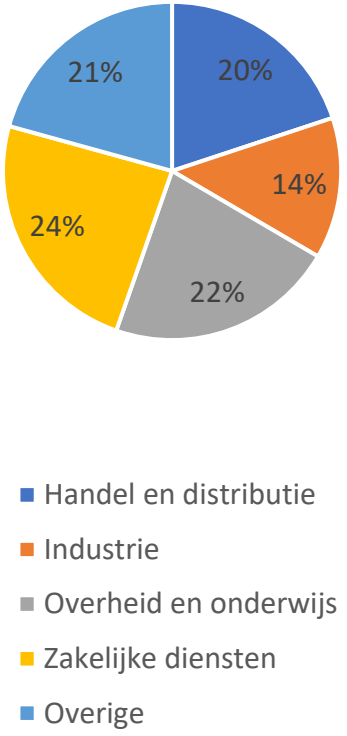
In welke mate bent u betrokken bij investeringen in IT- en/of OT beveiliging binnen uw organisatie?



Over hoeveel medewerkers beschikt uw organisatie?

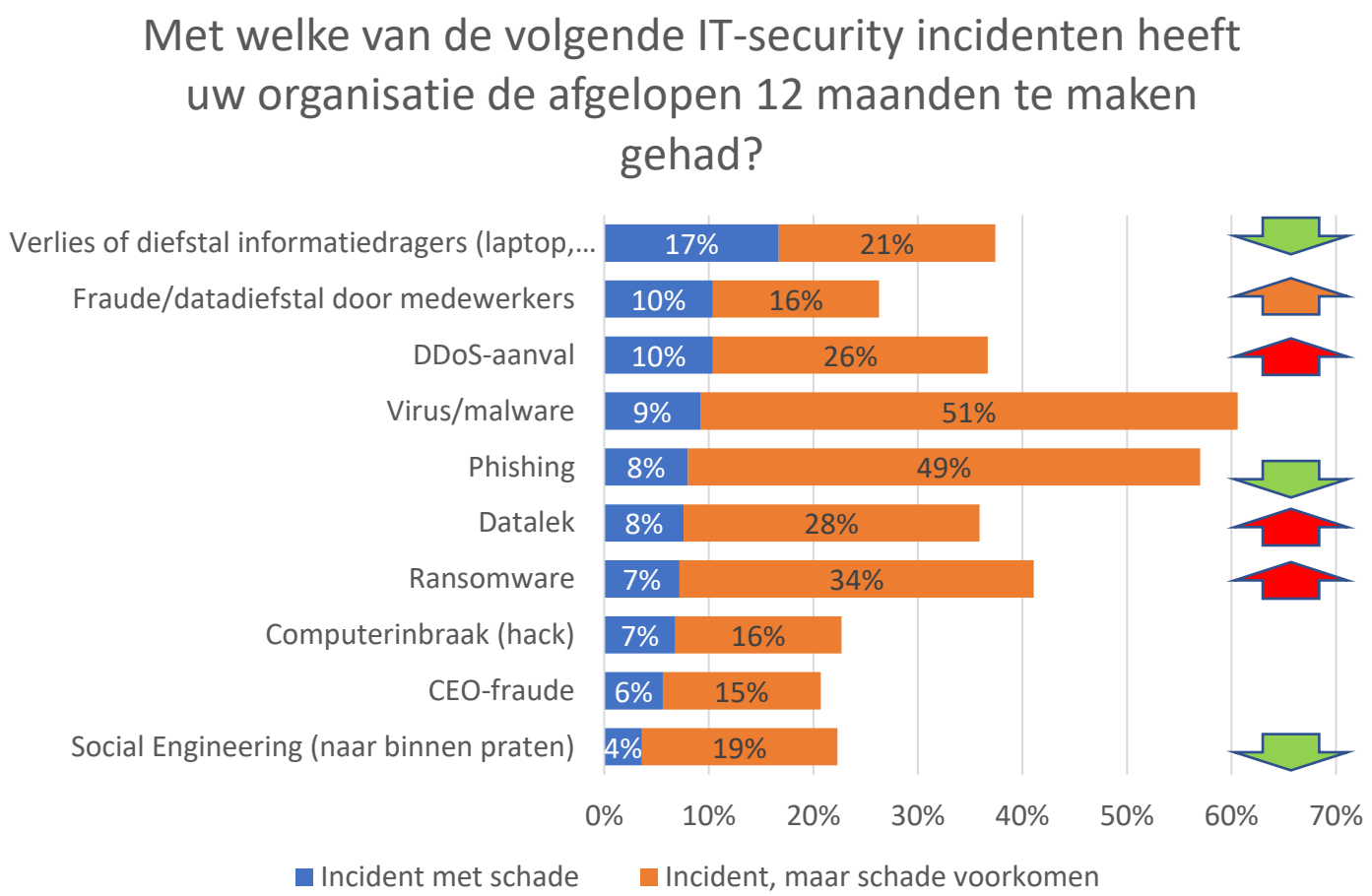


In welke sector is uw organisatie actief?



Dreigingsbeeld

Dreigingsbeeld



Over het geheel rapporteren de respondenten nu meer incidenten dan twee jaar geleden. We zien daarbij interessante verschuivingen.

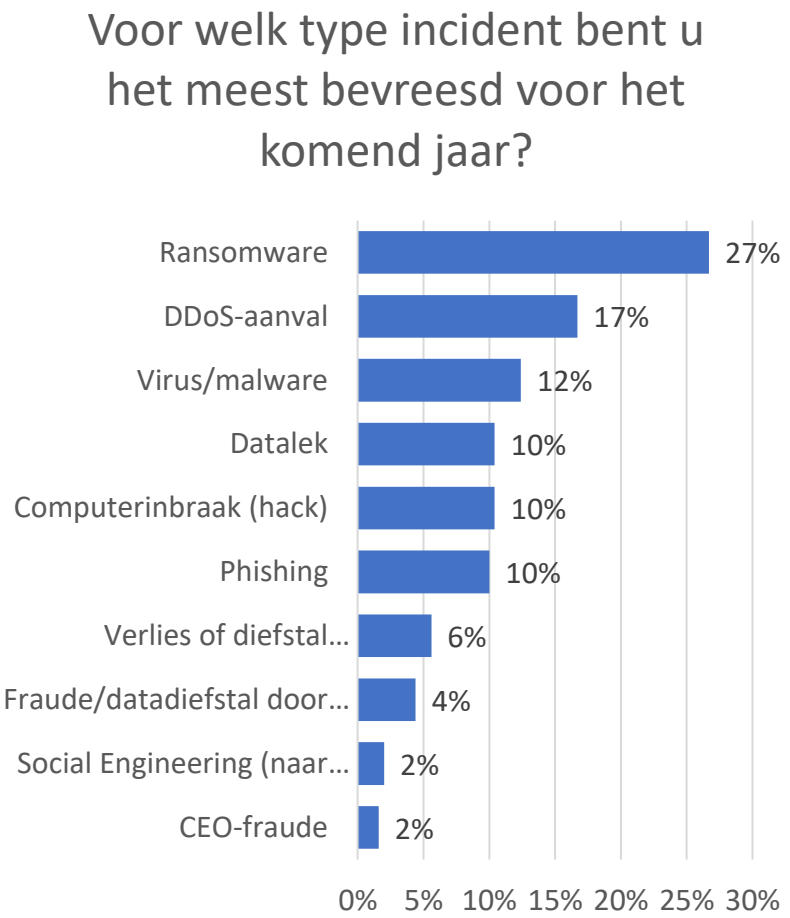
Het goede nieuws is dat sommige type incidenten in 2021 beduidend minder vaak voorkwamen dan in 2019. Vooral phishing, het verlies van informatiedragers als USB-sticks en laptops en social engineering kwamen minder voor. Op het gebied van phishing en social engineering is veel geïnvesteerd om het bewustzijn van medewerkers te verbeteren en dat lijkt zijn vruchten af te werpen. Tegelijkertijd moeten we waarschuwen voor de afnemende bereidheid die we in de uitkomsten waarnemen om in medewerkerstraining te blijven investeren. Dat zou de komende jaren nog wel eens tot een terugval kunnen gaan leiden.

Dreigingsbeeld

Dat er minder informatiedragers worden verloren, is goed verklaarbaar: met corona is het aantal reisbewegingen immers sterk teruggebracht. Zo wordt de kans vanzelf kleiner dat een laptop of USB-stick gestolen of verloren wordt. Nu het aantal reisbewegingen zich normaliseert, zal het aantal verloren informatiedragers naar verwachting weer toe gaan nemen. Het risico bestaat dat dit het aantal uit voorgaande jaren zelfs zal overtreffen, doordat veel meer werknemers over laptops beschikken om thuis mee te kunnen werken.

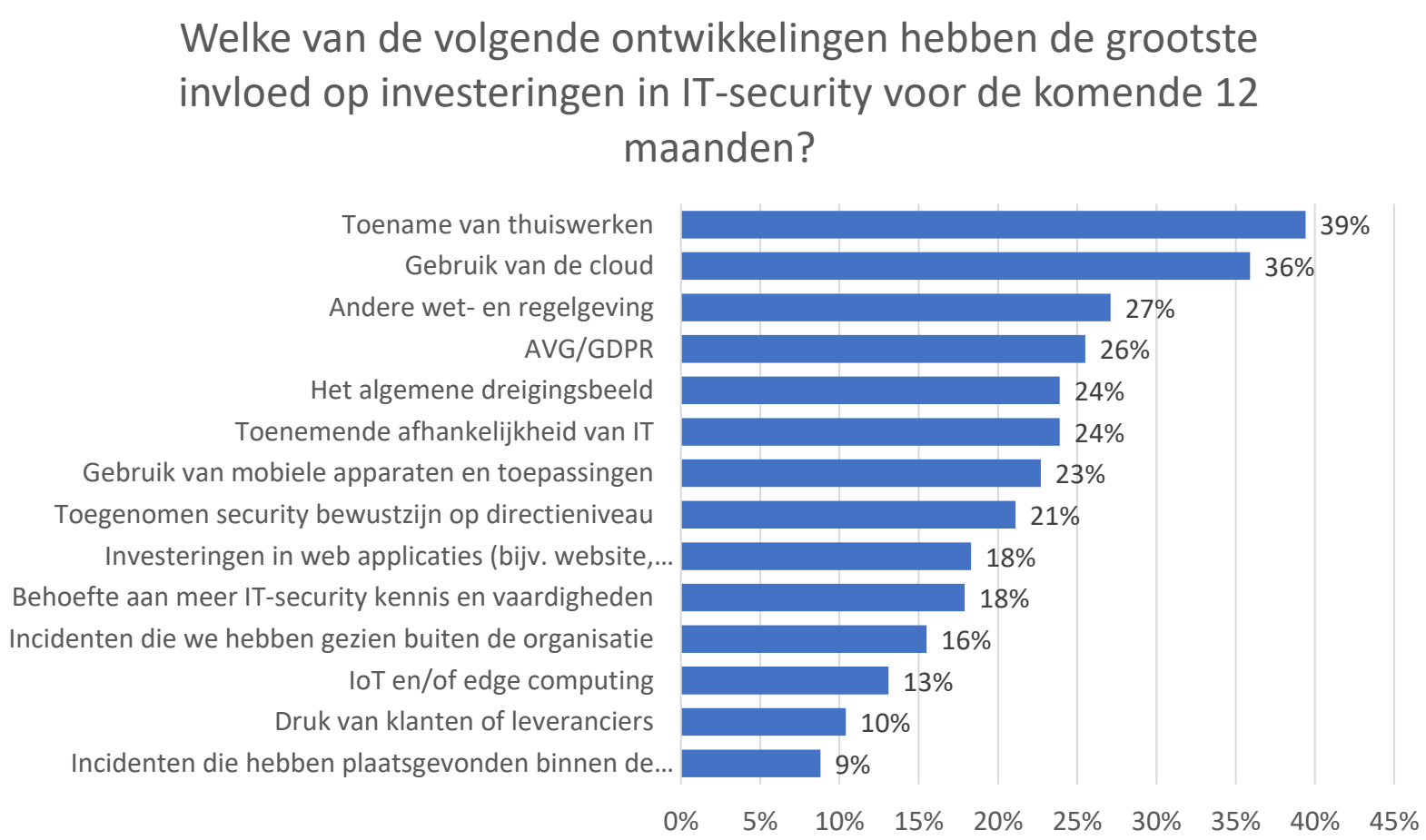
Tegenover deze “meevallers” staat een aantal type incidenten dat aanzienlijk vaker dan voorheen tot schade leidt. In absolute zin hadden bedrijven vooral veel vaker met DDOS-aanvallen en datalekken te maken. Maar de sterkste groei zien we in ransomware aanvallen. Twee jaar geleden gaf 2% van de ondervraagde bedrijven aan een ransomware incident met schade te hebben gehad. Nu gaat het inmiddels om 7% van alle organisaties. Zorgelijk daarbij is dat de schade van juist deze incidenten in steeds meer gevallen aanzienlijk is.

Hoewel ransomware niet het meest voorkomende incident is, is het door het schaderisico inmiddels wel het meest gevreesde incident. Na ransomware worden vooral DDOS-aanvallen gevreesd. Opvallend is dat de meeste organisaties zich minder zorgen maken over het verlies van data, waardoor ze met sancties uit (onder meer) de AVG te maken kunnen krijgen.



Strategie en investeringen

Strategie en investeringen



Drivers

Het veranderende dreigingsbeeld behoort niet tot de belangrijkste redenen om te investeren in IT-security. Twee jaar geleden gold de toenemende afhankelijkheid van IT als de belangrijkste drijfveer om te investeren in IT-security, gevolgd door cloud, het gebruik van mobiele apparaten en de AVG. De afhankelijkheid van IT heeft in pandemietijd het gezicht van veilig thuis kunnen werken gekregen. Cloud is in deze tijd alleen maar belangrijker geworden voor veel organisaties en is net achter thuiswerken drijfveer nummer 2.

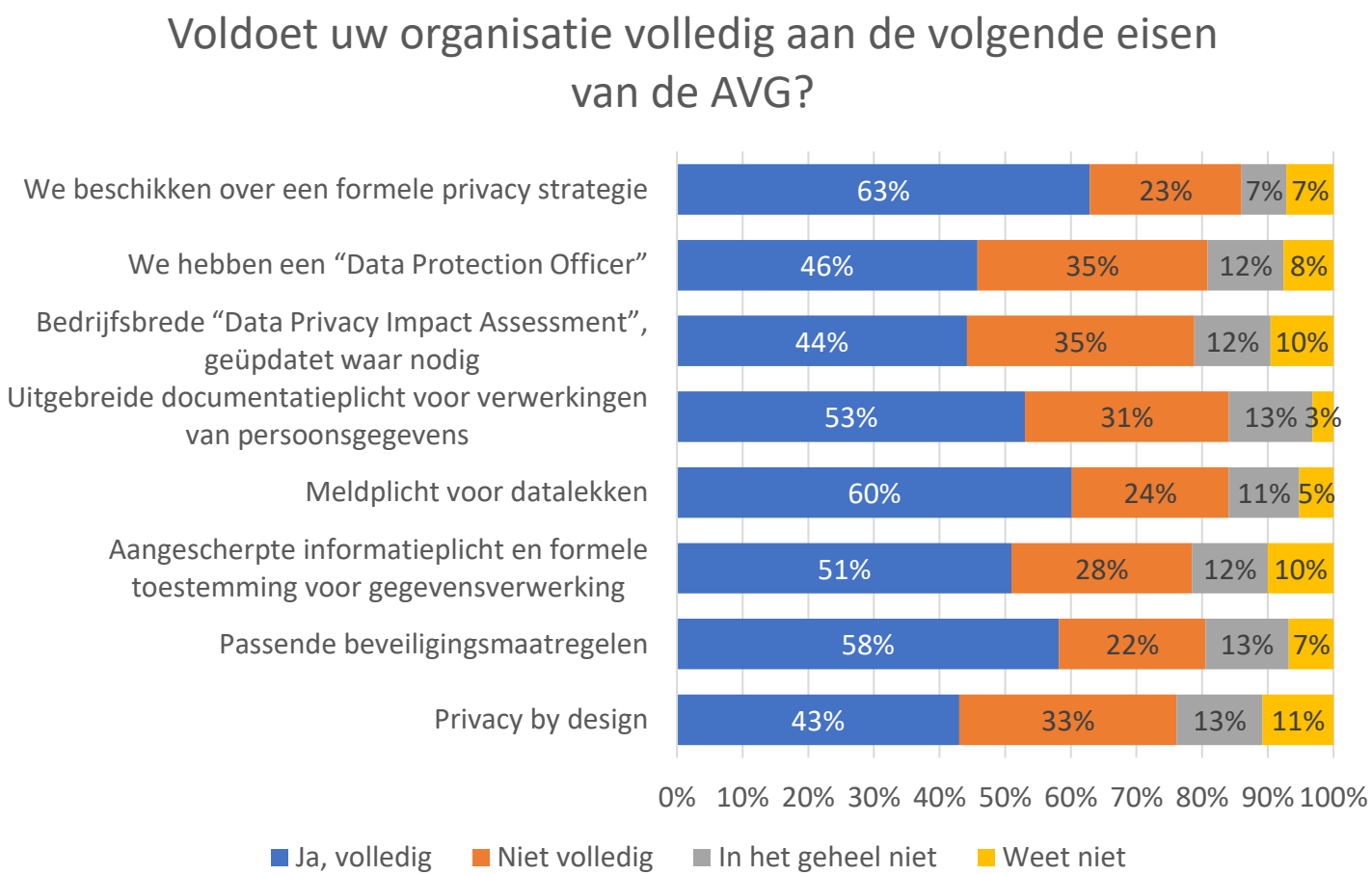
Wetgeving, waaronder AVG, blijft een belangrijke drijfveer waar de afgelopen jaren niet veel aan is veranderd. Misschien zouden we mogen verwachten dat de AVG als drijfveer voor security-investeringen zo

Strategie en investeringen

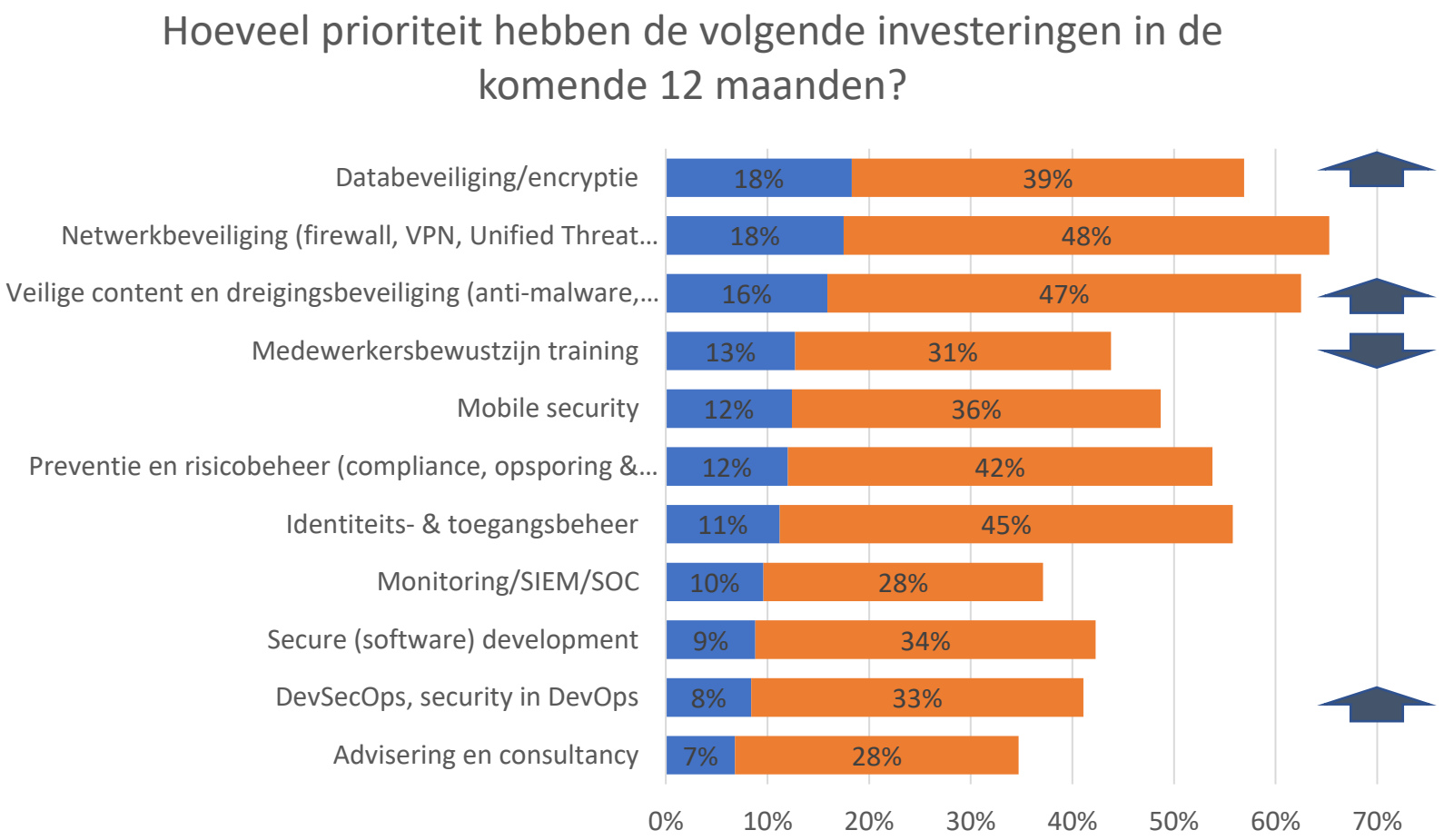
langzamerhand naar de achtergrond verdwijnt. Toch blijkt ook nu weer dan nog altijd veel organisaties de boel wat dat betreft nog niet op orde hebben. Voor een deel worden bedrijven door de schade en schande van datalekken wijs. Voor een ander deel ontbreekt de juiste aansturing om nieuwe oplossingen “private-by-design” te maken. Uit de survey blijkt dat de aandacht voor het laatste duidelijk is verslapt.

Investeringen

Onder invloed van onder meer het thuiswerken, de versnelling in het gebruik van de cloud en de dreiging van bijvoorbeeld ransomware, nemen de investeren in IT security versneld toe. Twee jaar geleden groeiden de uitgaven toch al met 11% per jaar. Nu zien we een groei van 19% over 2021 met een



Strategie en investeringen

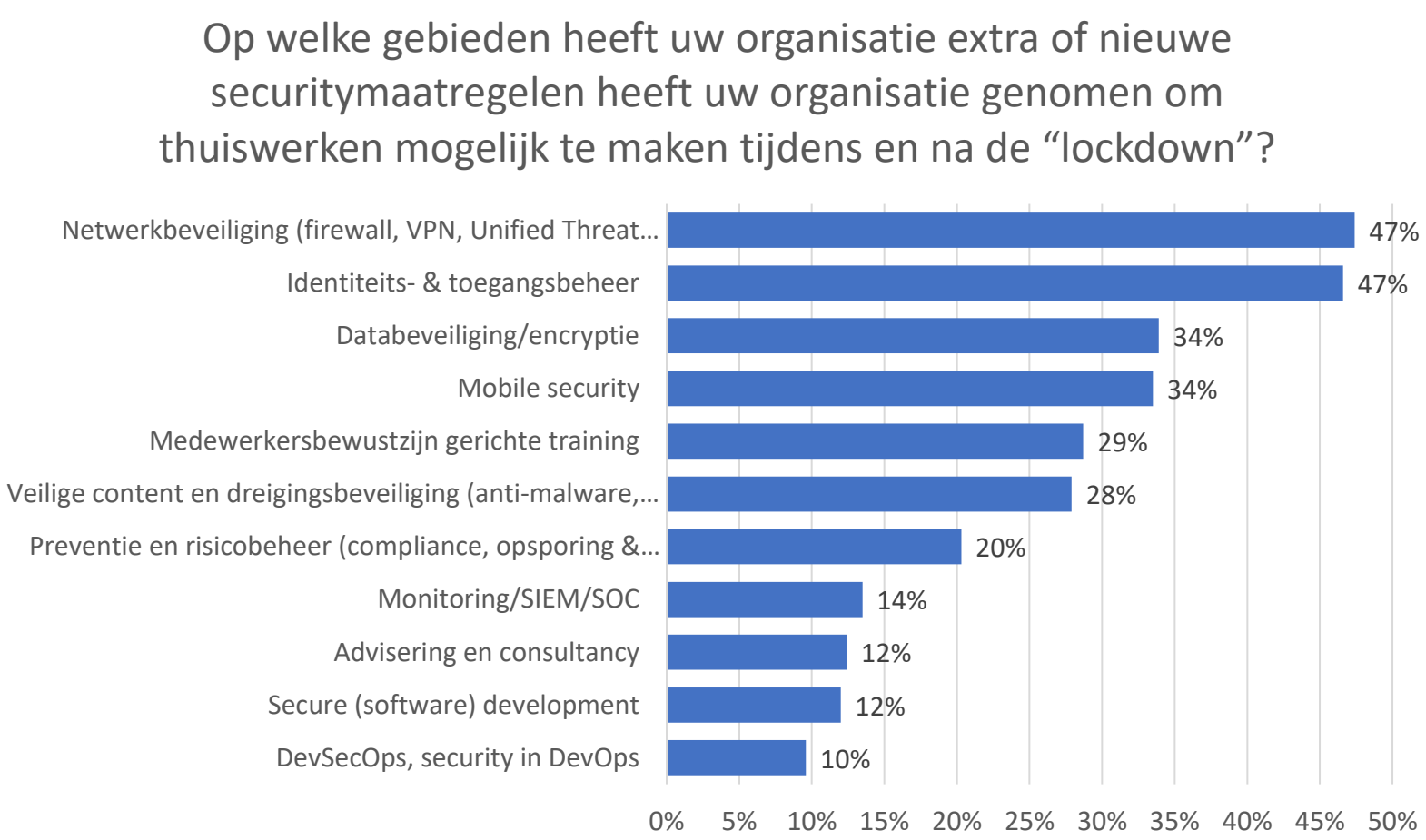


verwachting van nog eens 18% voor 2022.

Onder invloed van de marktontwikkelingen zien we dat ook de investeringsprioriteiten wat aan het verschuiven zijn. Voor het eerst zien we dat databeveiliging & encryptie het meest genoemd wordt als topprioriteit, zij het op de voet gevolgd door netwerkbeveiliging en veilige content en dreigingsbeveiliging. Ook deze laatste wordt nu vaker dan voorheen als een topprioriteit beschouwd.

Een stuk lager op de lijst vinden we DevSecOps, dat maar bij 8% een topprioriteit heeft, maar toch ook nog bij 33% een hoge prioriteit. Toch is dat een sterke toename ten opzichte van 2020 en zien we dus dat dit door steeds meer organisaties wordt omarmd.

Strategie en investeringen



Covid

Zoals we constateerden, heeft Covid een grote invloed op de IT-security investeringen. Van de ene op de andere dag moest thuiswerken mogelijk worden gemaakt. Daarbij diende security zo snel mogelijk te worden opgeschaald om dat verantwoord te kunnen faciliteren. Dat heeft vooral tot investeringen geleid in netwerkbeveiliging en, vaak wat later, identiteits- en toegangsbeheer.

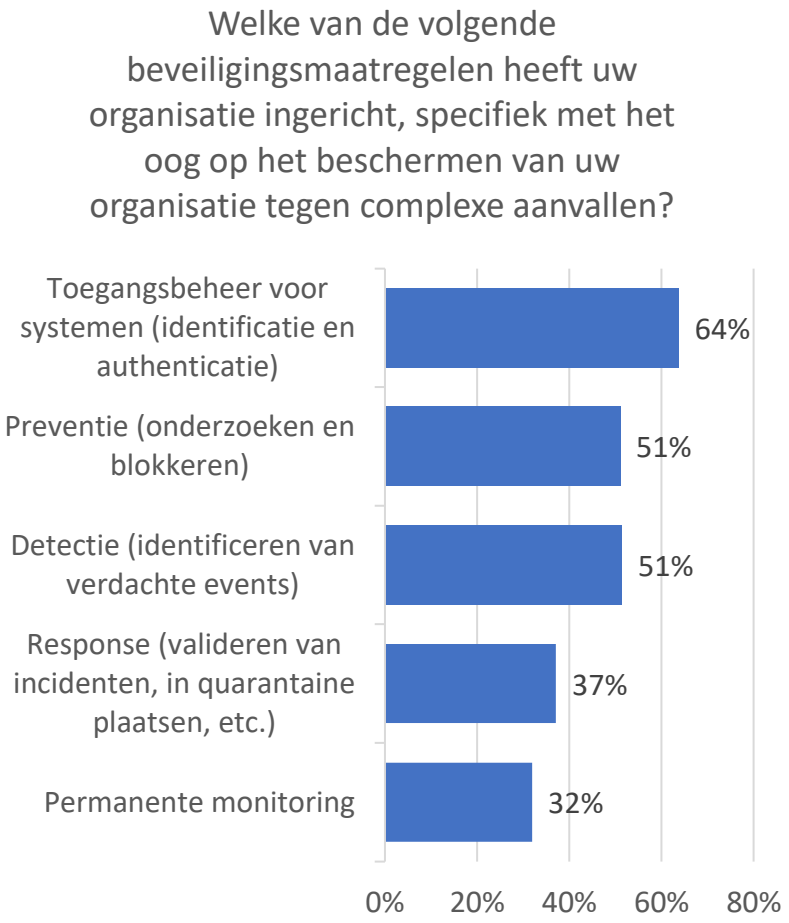
Intussen zien we dat organisaties thuiswerken niet langer als noodgreep beschouwen, maar als een realiteit. Daardoor blijven ze ook de komende tijd investeren in een veilige thuiswerkomgeving.

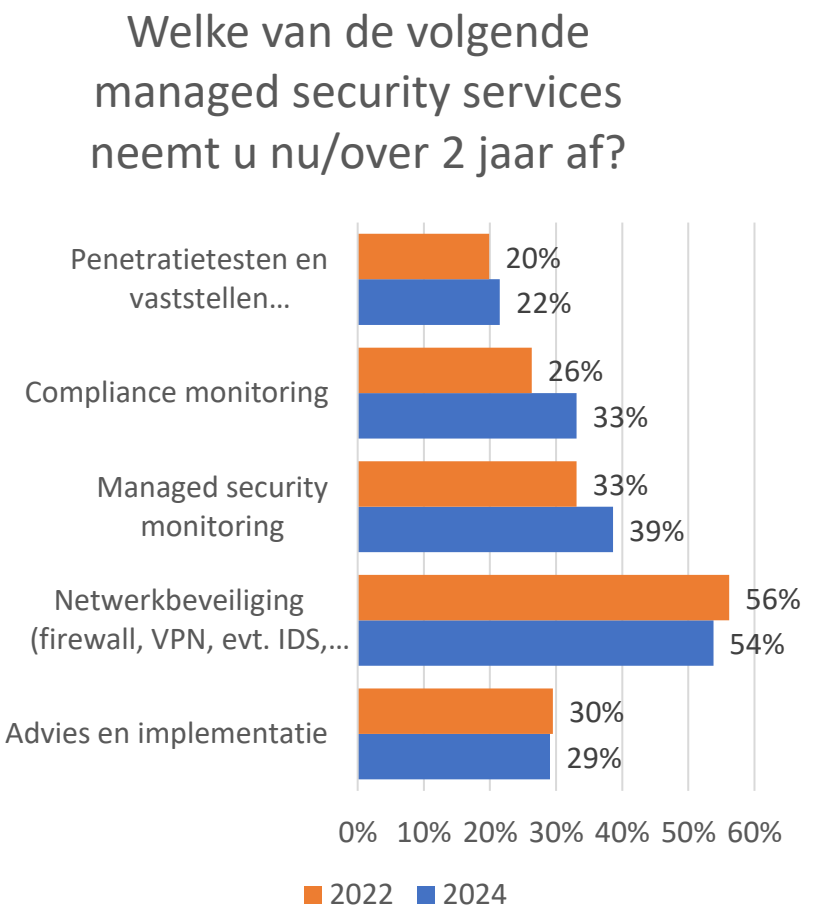
Strategie en investeringen

Monitoring

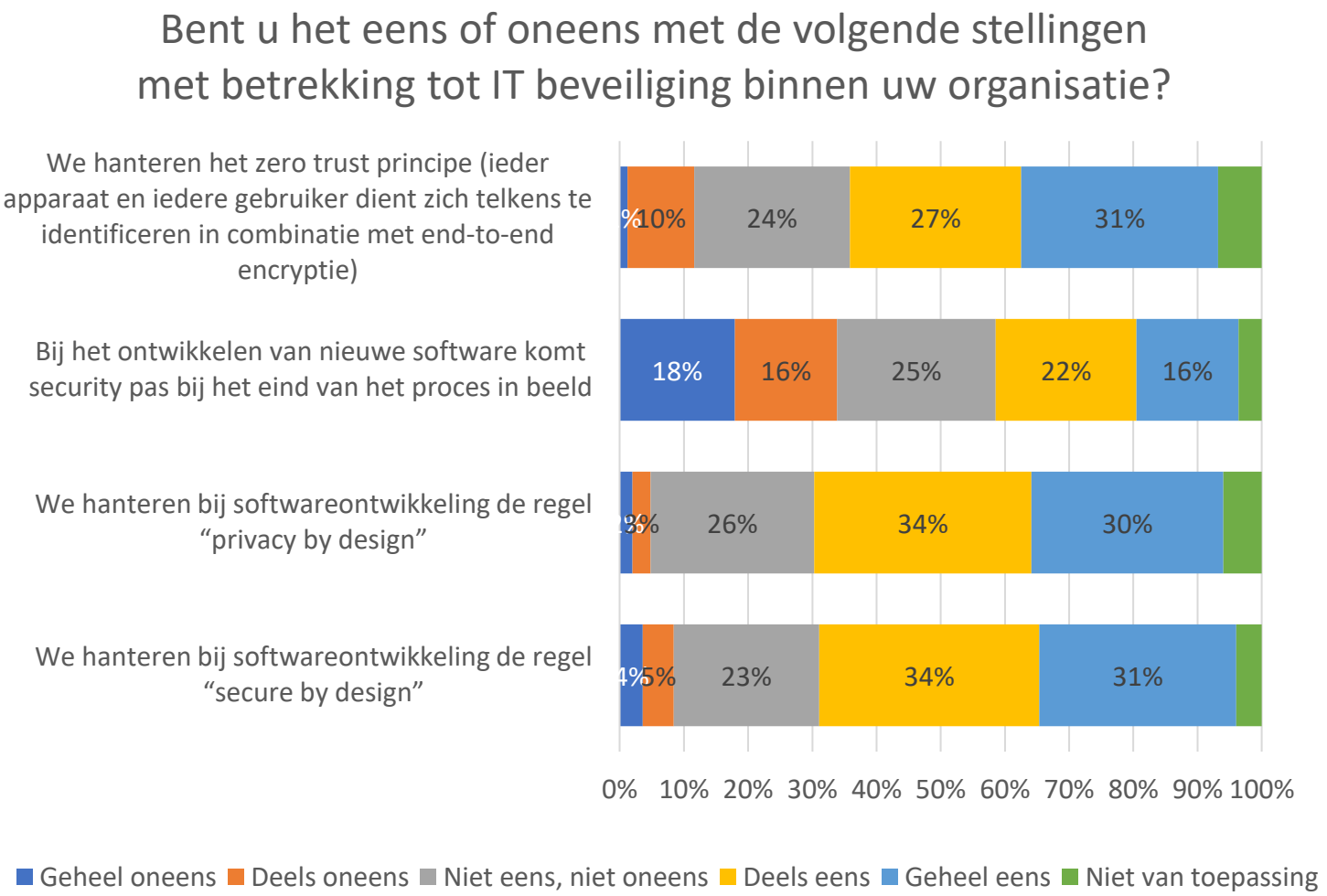
Monitoring is de laatste jaren in opkomst, maar de opkomst gebeurt met horten en stoten. Organisaties erkennen vaak de wenselijkheid of noodzaak, als onderdeel van een aanpak om de organisatie tegen complexe aanvallen te beschermen, of uit compliance-overwegingen.

Het beginnen met monitoring is meestal niet zo ingewikkeld. De uitdaging ligt hem vooral in het optuigen van policies en een organisatie die de meldingen zinvol en efficiënt kan verwerken. Het gebruiken van managed monitoring oplossingen kan daar bij helpen en daarin verwachten respondenten dan ook een duidelijke groei. Ook hierbij geldt dat de effectiviteit daarvan staat en valt bij ene juiste inbedding.





Strategie en investeringen



Software ontwikkeling

Bij software ontwikkeling hebben we de afgelopen jaren een trend gezien naar secure by design en privacy by design. Deze trend lijkt een beetje te stokken. Het aantal organisaties dat aangeeft deze regels te hanteren, is de afgelopen twee jaar helaas niet toegenomen.

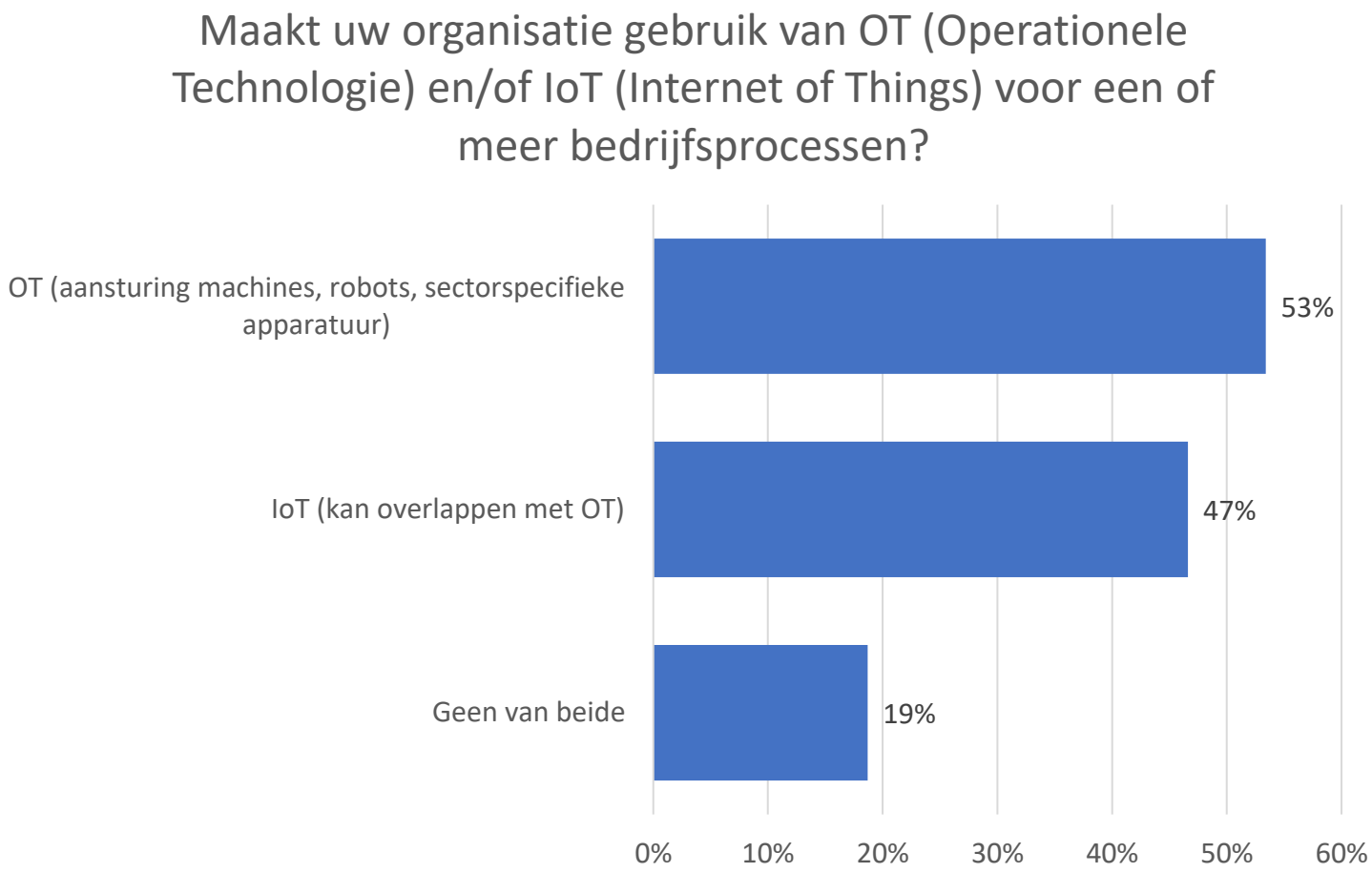
Verder zien we dat bij veel bedrijven security nog altijd pas aan het eind van het proces in beeld komt. Om het glas toch halfvol te krijgen, moeten we terug naar pagina 12, waar we constateerden dat er een sterke toenemende interesse voor DevSecOps bestaat. Maar bij de meeste organisaties kunnen we er voorlopig nog niet omheen dat security te laat in het ontwikkelproces komt, met alle risico’s van dien.

OT en IoT

OT en IoT

In de cybersecuritymonitor kijken we niet alleen naar IT-security, maar ook naar IoT-security en OT-security. Volgens de respondenten beschikt meer dan de helft over Operationele Technologie (OT) en bijna de helft over IoT-oplossingen.

IoT en OT hebben een wat twijfelachtige reputatie op het gebied van veiligheid. Bij OT gaat het veelal over toepassingen waar niet zoveel mis mee kan gaan, totdat ze benaderbaar worden via het Internet of een bedrijfsnetwerk (bij 57% van de OT-gebruikers). Veel toepassingen zijn daar op security-vlak niet goed op voorbereid en het ontbreekt ook nogal eens aan het juiste bewustzijn bij de beheerder van OT-oplossingen. Op het gebied van IoT is de netwerkcomponent van nature al ingebakken, maar blijkt ook dat het veel oplossingen aan ingebakken veiligheid ontbreekt.

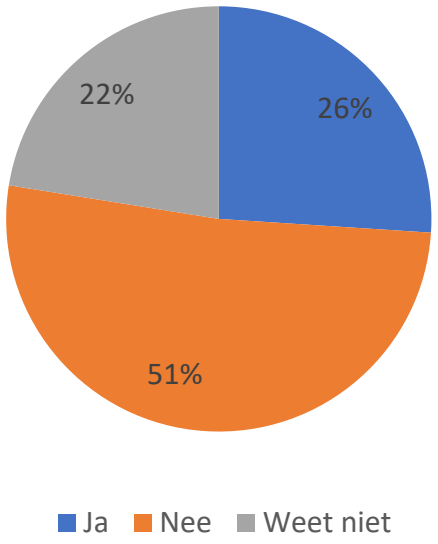


OT en IoT

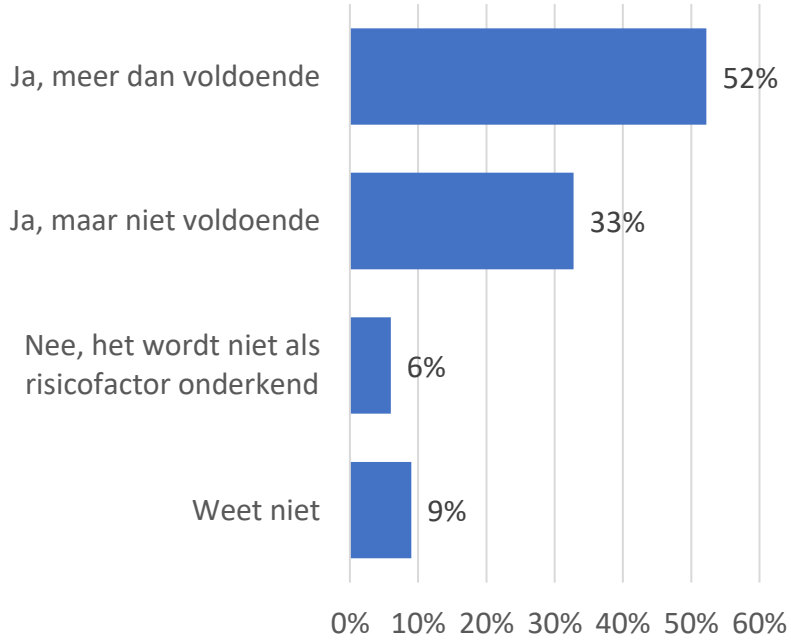
Gelukkig zien we in de surveyuitkomsten dat cyberdreigingen steeds serieuzer worden erkend als risicofactor. Volgens 52% van de OT-gebruikers wordt cybersecurity voldoende erkend als risicofactor. Bij een op de drie wordt het erkend, maar moet het bewustzijn verder verbeterd worden. Gelukkig zegt nog maar 6% dat het geheel niet als risicofactor wordt erkend.

Deze erkenning brengt voor de OT-gebruiker nieuwe uitdagingen met zich mee. Twee jaar geleden werd nauwelijks onderkend dat de aandacht voor security een remmend effect op innovatie kan hebben. Inmiddels geeft 26% toe dat cybersecurity risico's een rem vormen op digitale vernieuwingen op het gebied van OT. Oftewel: vernieuwingen moeten worden getoetst op securityrisico's.

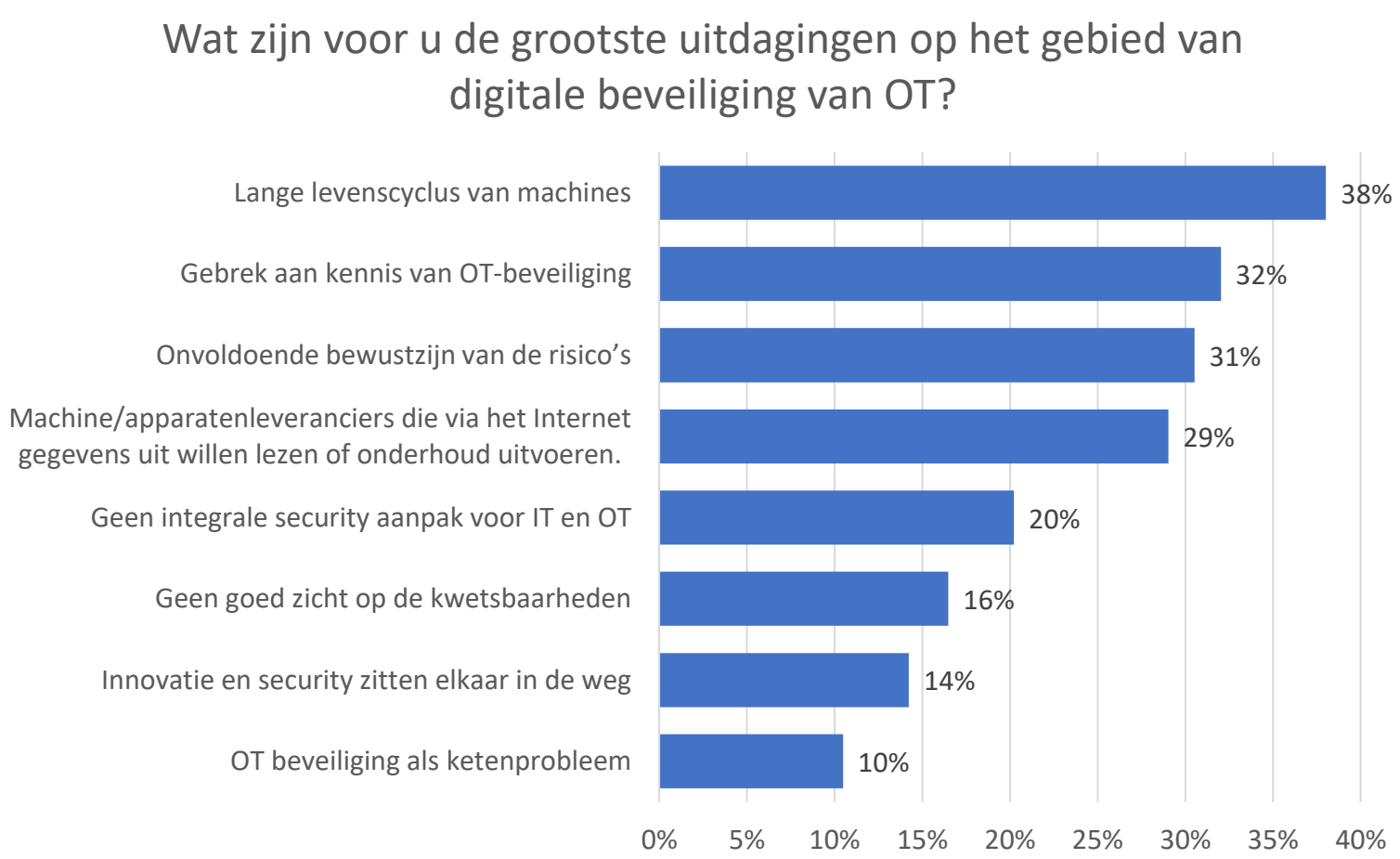
Weerhouden cybersecurity risico's uw organisatie van digitale vernieuwingen op het gebied van OT (Operational Technology)?



Wordt cybersecurity binnen uw organisatie (voldoende) erkend als risicofactor binnen de productieomgeving/OT?



OT en IoT

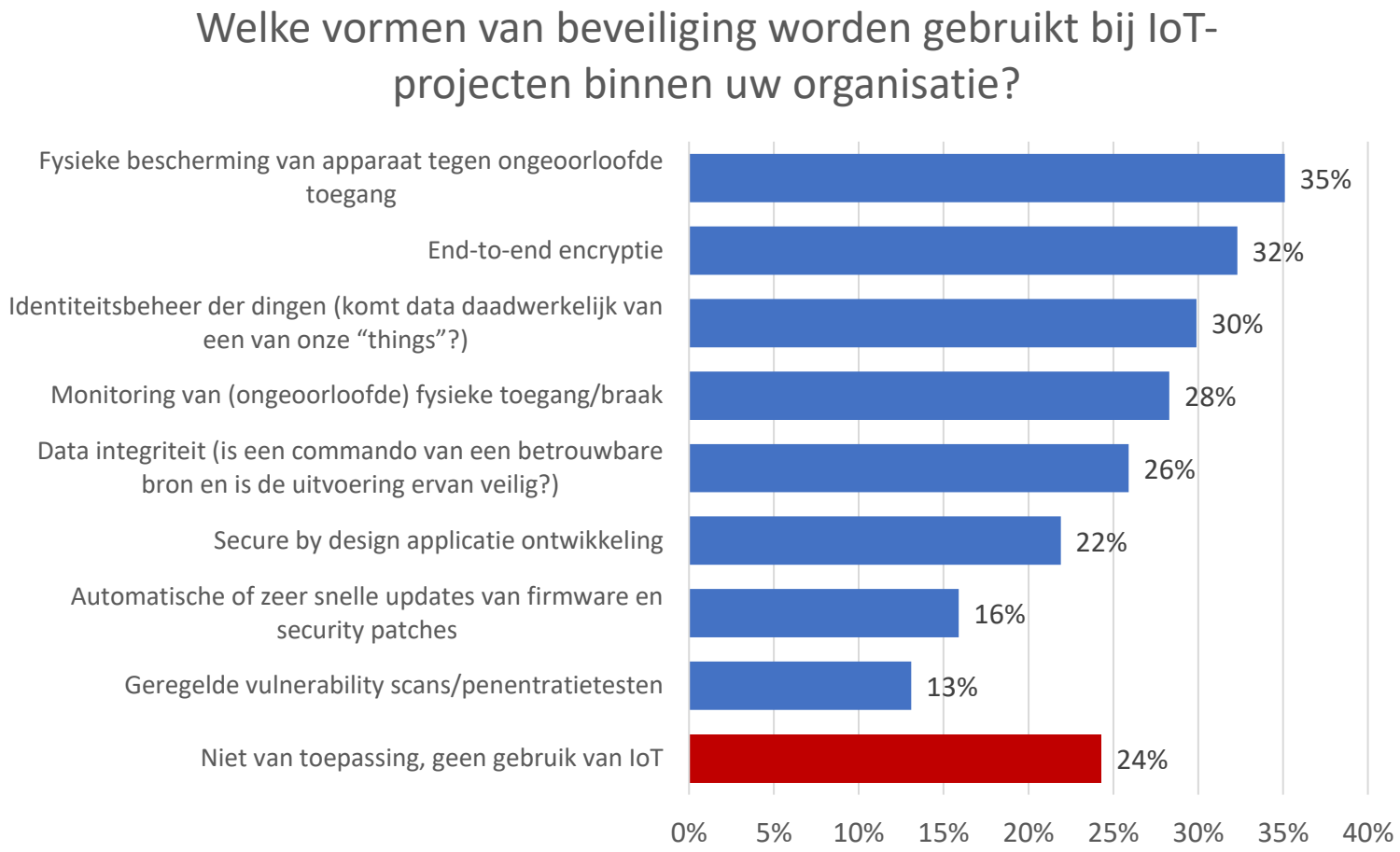


Vervolgens zijn vaak aanvullende security maatregelen nodig, of moet soms in het geheel worden afgezien van een gewenste aanpassing. Uiteindelijk moet ook bij OT security in het ontwikkelproces een plaats krijgen.

Uitdagingen

Twee jaar geleden legden veel respondenten de verantwoordelijkheid voor OT-securityfalen vooral neer bij machineleveranciers die zo nodig online onderhoud wilden uitvoeren. Nu zien we dat bedrijven veel beter begrijpen waar de risico's binnen de bestaande configuraties zich bevinden. De belangrijkste uitdaging op het gebied van OT-security is de lange levenscyclus van machines. Lang niet altijd wordt de software up-to-date gehouden en lang niet altijd wordt er lang genoeg voldoende gedaan aan software-

OT en IoT



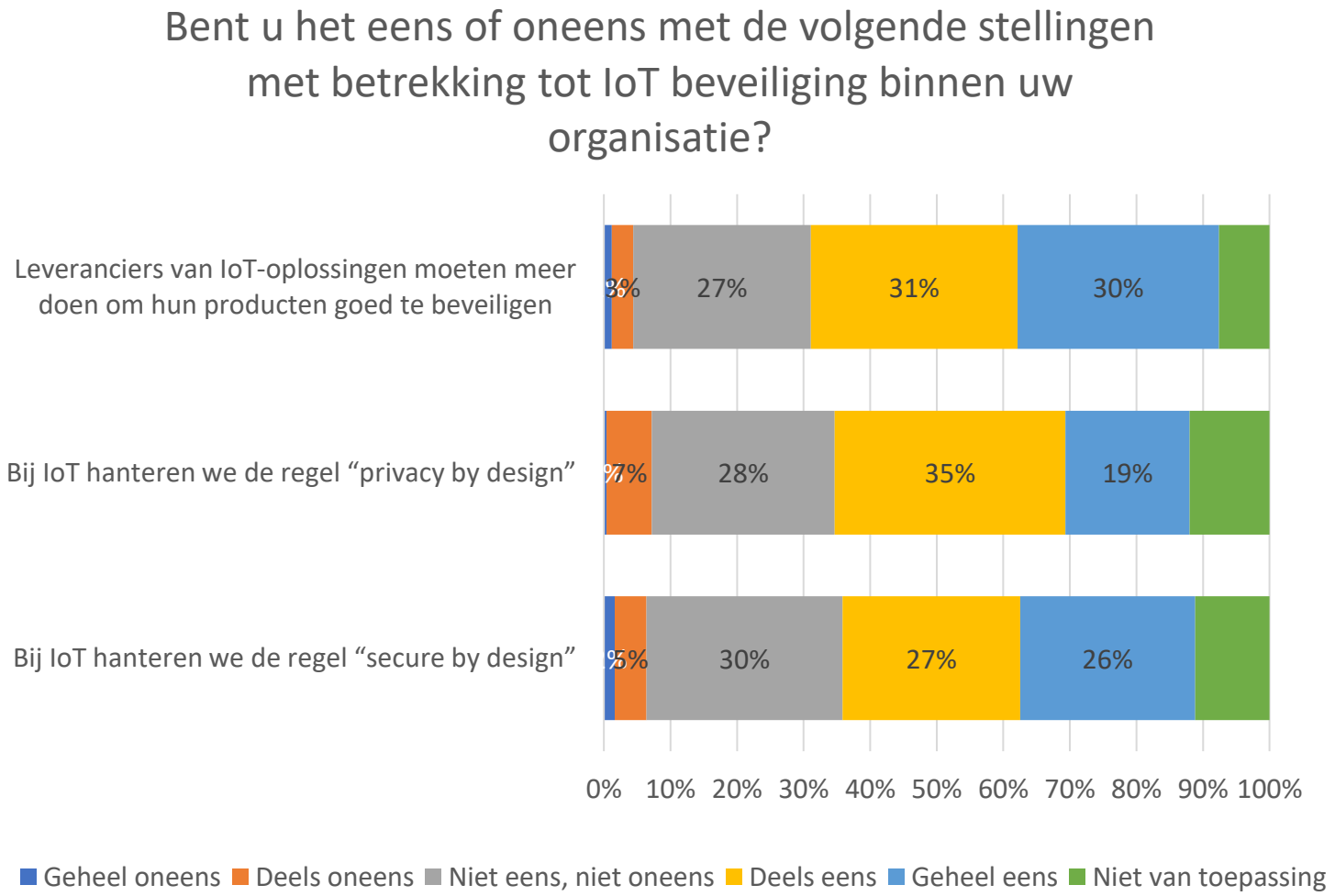
onderhoud. Los daarvan geven de respondenten toe dat ze niet echt klaar zijn voor serieuze bedreigingen op het gebied van OT. Er is vaak een gebrek aan kennis op het gebied van OT-beveiliging en het ontbreekt nog altijd vaak aan bewustzijn omtrent de risico’s.

IoT

Zoals gezegd hebben we respondenten niet alleen over OT, maar ook over IoT (Internet of Things) bevraagd. Ook daar zien we een groeiend bewustzijn ten aanzien van de risico’s op het gebied van cybersecurity.

Dat leidt tot een toenemende hoeveelheid aan voorzorgsmaatregelen. De meest voorkomende, fysieke bescherming van het apparaat, valt wellicht binnen het meer traditionele domein, maar is daarom

IoT en OT



Niet minder van belang. Ook zien we dat veel organisaties end-to-end encryptie en identiteitsbeheer toepassen. Wat wel opvalt, is dat snel patchen bij de maatregelen onderaan bungelt. Hoewel dat altijd als dringend advies nummer 1 wordt gegeven, zijn er blijkbaar de nodige obstakels (zorgen over of het apparaat nog wel naar behoren werkt, of het ontbreken van een duidelijk proces) die dat voorkomen.

Ook zien we dat privacy en secure by design ontwikkelingen niet terug in de top. Ongeveer de helft van de IoT-gebruikers maakt er wel in enige mate gebruik van, maar het lijkt niet altijd een goed beschreven proces te zijn.

Conclusies

Samenvatting

IT Security
De investeringen in cybersecurity zijn duidelijk aan het versnellen. Aan de ene kant zijn bedrijven, aangespoord oor Corona, versneld aan het digitaliseren. Zoals het werken (thuis) als het bedienen van de klant (online) moet digitaal en natuurlijk veilig worden gefaciliteerd.

Aan de andere kant is het dreigingsbeeld sterk verslechterd. Steeds meer organisaties hebben te maken met ransomware en DDOS-aanvallen die beide serieuze schade veroorzaken, veel meer dan enkele jaren terug. Het goede nieuws is dat medewerkers minder laptops en andere informatiedragers verloren. Dat is dan ook een stuk lastiger als je door Covid thuiswerkt.

Het thuiswerken heeft er wel voor gezorgd dat organisaties veel hebben geïnvesteerd in extra security, met name netwerkbeveiliging en identiteits- en toegangsbeheer. Voor het komende jaar worden er juist veel extra investeringen verwachten op het gebied van databeveiliging & encryptie (voor het eerst de meest voorkomende topprioriteit) en secure content & threat management. Ook zien we een toenemende aandacht voor DevSecOps. Daar staat tegenover dat de aandacht voor privacy by design en security by design wat lijkt te verslappen.

Verder constateren we dat de aandacht voor medewerkerstraining onder druk staat. Teveel organisaties verwachten dat medewerkers “het nu wel weten” en zijn terughoudend met opfriscursussen.

Op het gebied van de AVG zien we dat er veel bedrijven zijn die het serieus aanpakken, maar dat er ook nog veel laksheid in de markt zit. Wellicht wordt dat gevoed door de beperkte capaciteit van de Autoriteit Persoonsgegevens, maar het baart ons toch wel enige zorgen.

OT en IoT security
Op het gebied van OT en IoT security zien we een groeiend bewustzijn ten aanzien van de securityrisico’s. Op het gebied van OT wordt niet meer boven alles gewezen naar de leveranciers van apparaten en machines als grootste beveiligingsrisico. Men onderkent de uitdaging van de lange levenscycli van OT-omgevingen, hiaten in de eigen OT-security kennis en dat het bewustzijn verder moet verbeteren.

Op het IoT-vlak zien we dat de inspanningen in beginnen te lopen in vergelijking met IT. Hoewel zaken als secure by design nog onvoldoende worden omarmd, geldt dat minder voor zaken als encryptie en IoT-identiteitsbeheer.

Opdrachtgevers onderzoeksteam

LuteijnMedia
Dit onafhankelijke onderzoek is uitgevoerd in opdracht van LuteijnMedia, uitgever van 6 crossmediale platforms in de IT en telecom waaronder Infosecurity Magazine.

Op het snijvlak van technologie en beleid informeert Infosecurity Magazine 3.500+ Nederlandse CISO's, CTO's, managers en professionals verantwoordelijk voor de informatiebeveiliging in hun organisatie over recente ontwikkelingen op het gebied van informatiebeveiliging.

Dit onderzoek is mede mogelijk geworden door financiële bijdragen van **Tesorion**, de grootste zelfstandige Nederlandse cybersecurity dienstverlener en **Smile**, makers van de meest veelzijdige en flexibele software voor elke vorm van risicomanagement, -assessment en integraal en positief verbeteren.

Pb7 Research
Pb7 levert onderzoek en advies gericht op het succesvolle gebruik van ICT in de Benelux. Pb7 ondersteunt ICT marketeers en strategen door het identificeren en analyseren van kansen en uitdagingen in de markt en de concurrentie, en de vertaling daarvan naar aanbevelingen op het vlak van positionering en campagnes.

Pb7 Research is in januari 2012 door Peter Vermeulen opgericht. Sinds 2012 heeft Pb7 een sterke track record gecreëerd met onderzoeksprojecten voor bedrijven zoals AWS, Capgemini, Cisco, DINL, Dutch Data Center Association, Exact, HP, IDG, Kaspersky Lab, KPN, MacAfee en Sogeti en overheden waaronder de Provincie Flevoland en de Rijksdienst voor Ondernemend Nederland (RVO). Pb7 richt zich voornamelijk op de markten voor cloud, IT security en datacenters.

Peter Vermeulen
Eigenaar en hoofdonderzoeker
+31 657 585 156
peter@pb7.nl
www.pb7.nl

Eric Luteijn
Uitgever en hoofdredacteur
+31 653 510 690
eric@luteijnmedia.nl
www.luteijnmedia.nl
www.infosecuritymagazine.nl