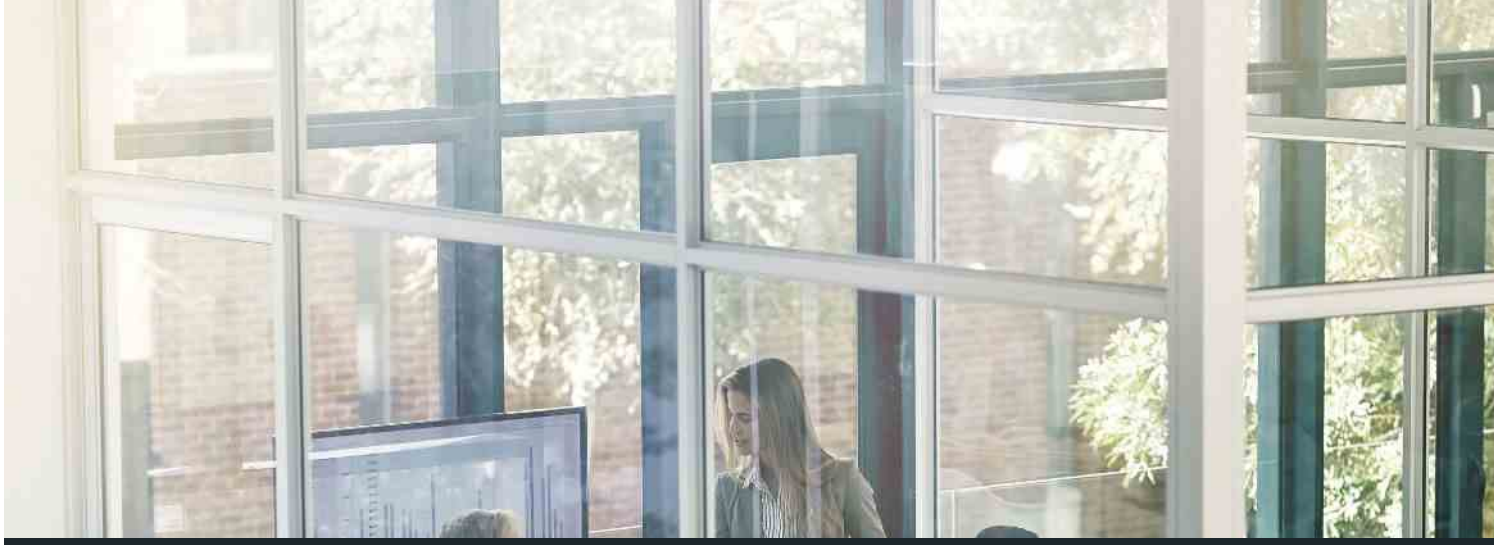
Solvinity
Secure Managed Cloud

CYBERSECURITY ONDERZOEK

Solvinity Cybersecurity Report | **2024**

Inhoud



Introductie

De toename van cybercrime, complexe regelgeving, de druk op de arbeidsmarkt, het is een cocktail die een slechte afdronk kan hebben. In deze context geeft Solvinity de huidige stand van zaken in Nederland met betrekking tot IT-security.

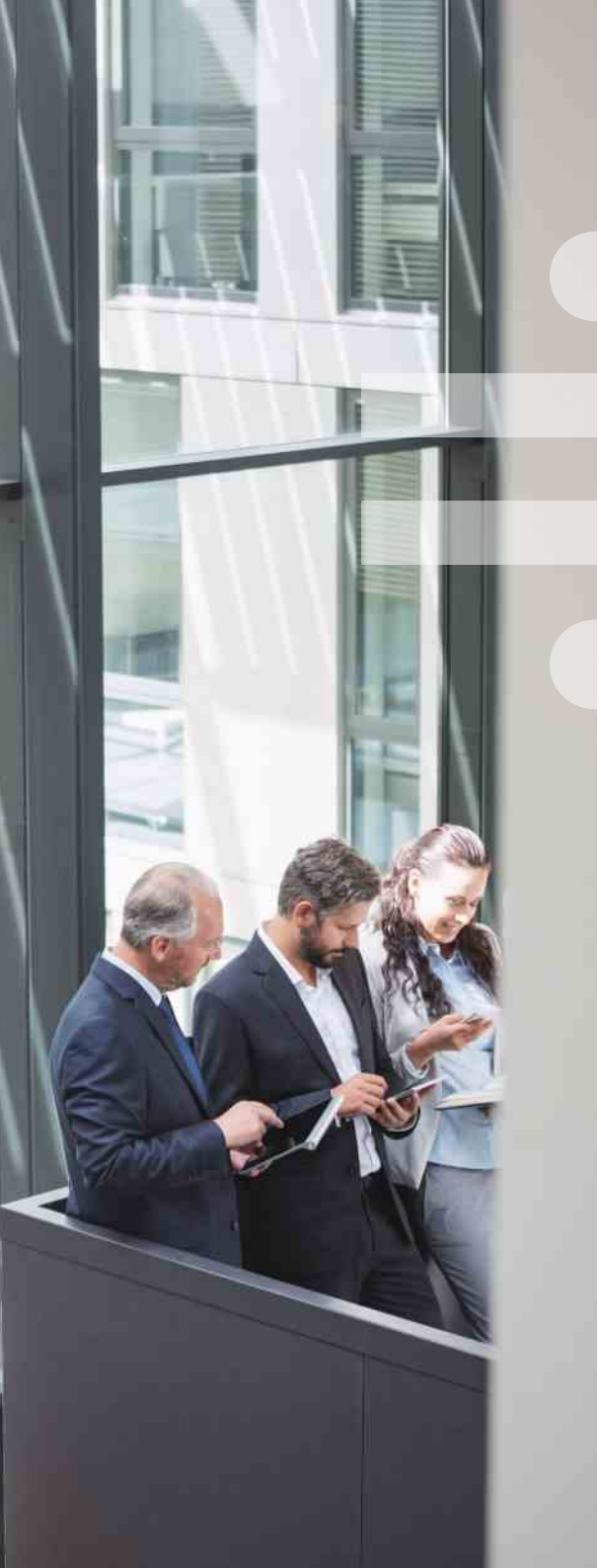
De Cyber Security Raad schreef dit jaar in een **brief aan het kabinet** dat cyberrisico´s in onze digitale infrastructuur en processen steeds meer toenemen. Zo werden begin 2024 de **websites van een aantal provincies platgelegd** door een DDoS aanval, maar ook de Bank Nederlandse Gemeenten en OV-NL werden met DDoS aanvallen bestookt.

Zijn we in Nederland weerbaar? Welke maatregelen hebben we getroffen en zijn die afdoende? Voldoen we aan regelgeving?

Deze vragen hebben we voorgelegd aan IT-professionals in een organisatie met meer dan 200 werknemers die binnen hun organisatie (mede)beslissend of verantwoordelijk zijn voor IT en die betrokken zijn bij één of diverse voorgelegde IT-activiteiten.

De resultaten hebben we besproken met experts van Solvinity, te weten Marc Guardiola, Chief Technology Officer (CTO) en Martin Maas, Chief Information Security Officer (CISO) en Kees Stammes, General Manager van Securify.

Deze derde editie van ons onderzoek voerden we uit in samenwerking met Panelwizard in april 2024. De uitkomsten van dit onderzoek zijn gebaseerd op 477 volledig ingevulde vragenlijsten.



MANAGEMENT SUMMARY

Hoe gaan we Nederland weerbaarder maken?

Het maakt soms uit of je bij een middelgroot bedrijf werkt, of een grote corporate. Of dat je kunt leunen op de uitgebreide toolbox in de public cloud of dat je een private cloud te beveiligen hebt. Of dat je als professional in het bestuur of management zit, of dat je als IT-medewerker in een team alle security tools en technologie moet implementeren en beheren.

Ondanks de verschillen, geven de resultaten van dit onderzoek aan dat het capaciteitsprobleem over de gehele linie groter is geworden: we komen goed geschoolde en ervaren IT-professionals tekort, en cybersecurityspecialisten in het bijzonder. Toch denkt twee derde van de ondervraagde IT-professionals dat het wel goed zit met de weerbaarheid. In dit rapport duiken we dieper in op de zorgen, uitdagingen en securitymaatregelen van IT-professionals in Nederlandse organisaties.

Cybercriminelen zitten niet stil en ook in regelgeving zijn er continu veranderingen. Daarom geven we als secure managed cloud provider algemene aanbevelingen voor het verhogen van weerbaarheid. Daarnaast bieden we klantspecifieke “secure managed cloud” oplossingen om een hoge beveiliging op verschillende cloudplatformen van onze klanten te waarborgen, zodat BV Nederland zijn werk veilig kan doen.

Belangrijkste bevindingen

- **Weerbaarheid tegen cyberaanvallen:** Twee derde (64%) van de respondenten vindt dat hun organisatie voldoende weerstand kan bieden tegen cyberaanvallen. Opvallend is dat dit percentage stijgt naarmate de organisatie groter is.
- **Grootste security uitdaging:** Drie op de tien IT-professionals zeggen dat hun grootste uitdaging het gedegen implementeren van de juiste beveiligingsmaatregelen is.
- **Uitdagingen per platform:** Public cloud gebruikers rapporteren de grootste uitdaging in het snel en adequaat reageren op security-incidenten, terwijl private en on-premise gebruikers meer moeite hebben met het tijdig detecteren van deze incidenten.
- **Hybride cloud meest gebruikt:** Bijna 40% van de ondervraagden geeft aan dat hun organisatie een hybride cloudomgeving gebruikt. Dit wordt gevolgd door on-premise (21%), private cloud (17%) en public cloud (16%).

Marc

"De opkomst van generatieve artificiële intelligentie (AI) biedt mogelijkheden voor geautomatiseerde beveiliging, maar brengt ook aanzienlijke nieuwe risico's met zich mee. Digitale aanvallen kunnen op een nog grotere schaal worden uitgevoerd, en phishing-aanvallen worden steeds realistischer en daardoor gevaarlijker."

Kees

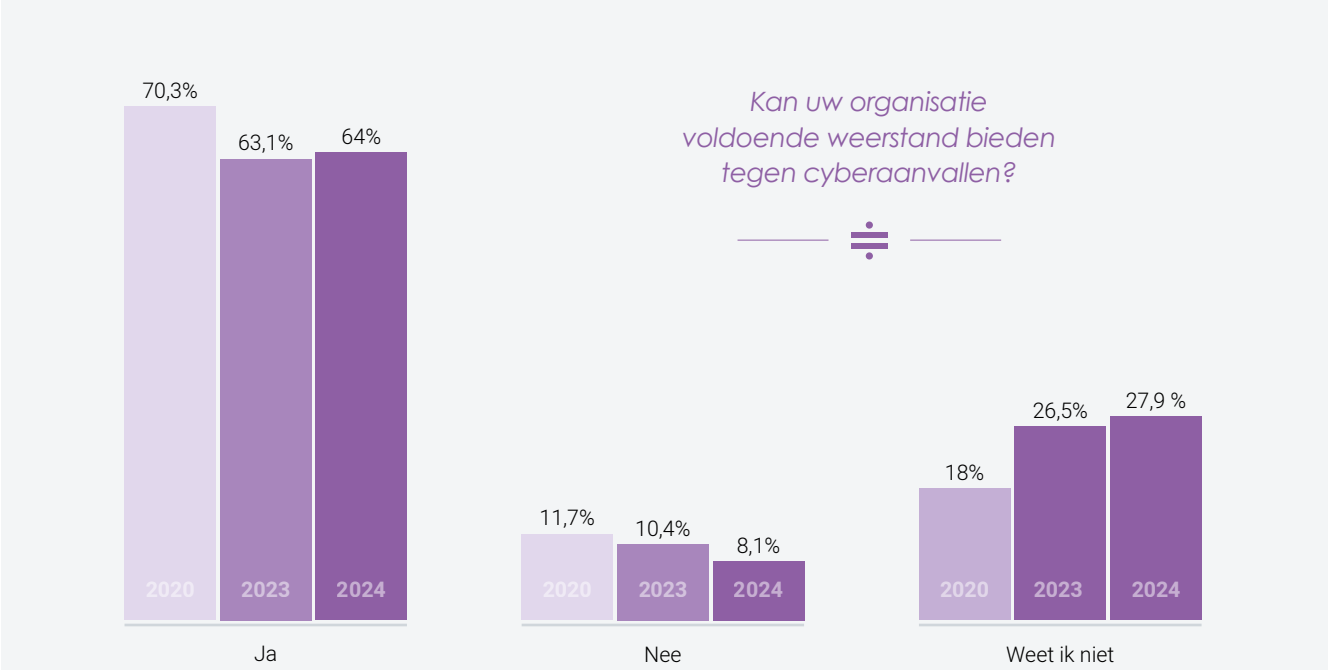
"De 64% duidt op meer zelfvertrouwen dan geoorloofd is, want in de praktijk zie ik dat elke pentest bevindingen oplevert en elke Red Teaming slaagt. Met eigen ogen kijken naar je weerbaarheid is niet voldoende, je hebt audits en testen nodig om jouw eigen implementatie enwaarheid te toetsen. Kleinere ondernemingen missen vaak kennis of expertise, maar erkennen dit wel en zijn daardoor realistischer. Eén onoplettende medewerker kan al een phishingaanval laten slagen. Ons advies: identificeer de kroonjuwelen, identificeer de voor jou relevante aanvallers en begin met een goede risicoanalyse. Vertaal dit naar een teststrategie om weerbaarheid te toetsen en zwakke plekken aan te pakken."

Cyberaanvallen - zijn we te onbezorgd?

Kan uw organisatie voldoende weerstand bieden tegen cyberaanvallen? Bijna twee derde (64%) zegt daarop volmondig "ja" en 8% zegt "nee". Bijna drie op de tien geven aan het niet te weten. De verschillen met voorgaande jaren zijn gering.

Hoe meer werknemers een organisatie heeft, hoe vaker men aangeeft voldoende weerstand te kunnen bieden (53% 200-499 werknemers tot 68% 1000 of meer werknemers). En hoe minder werknemers een organisatie heeft, hoe vaker men aangeeft **geen** weerstand te kunnen bieden (15% 200-499 werknemers tot 4% 1000 werknemers of meer).

Overigens is het vertrouwen bij IT-professionals die public cloud gebruiken met 55,3% het laagst, ten opzichte van het gemiddelde van 66,7% van alle andere omgevingen (private, on premise, hybrid).



Martin

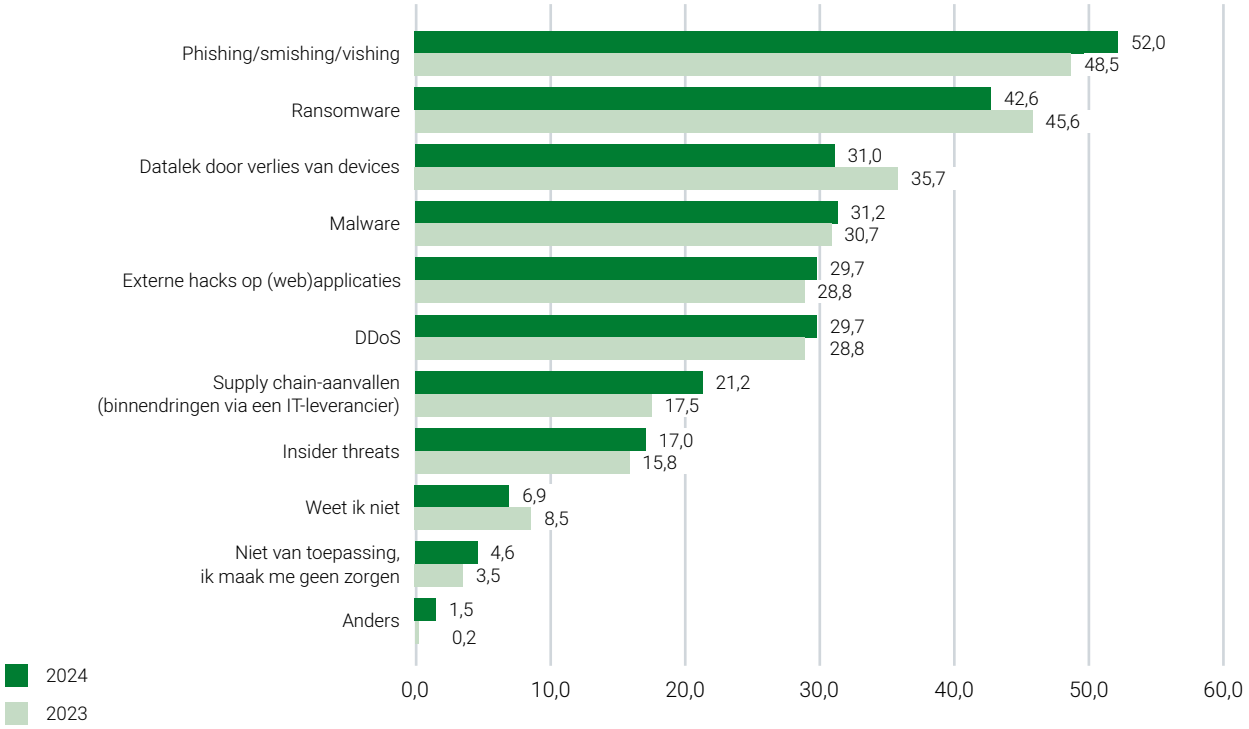
"Auditors vragen expliciet naar supply chain aanvallen. Ongemerkt krijgen veel bedrijven software in huis, waar een achterdeurtje ingebouwd is tijdens de ontwikkeling van de applicatie. Die geïnfecteerde software wordt vervolgens uitgeleverd, geïnstalleerd en gebruikt en via het achterdeurtje staat die omgeving dus wagenwijd open."

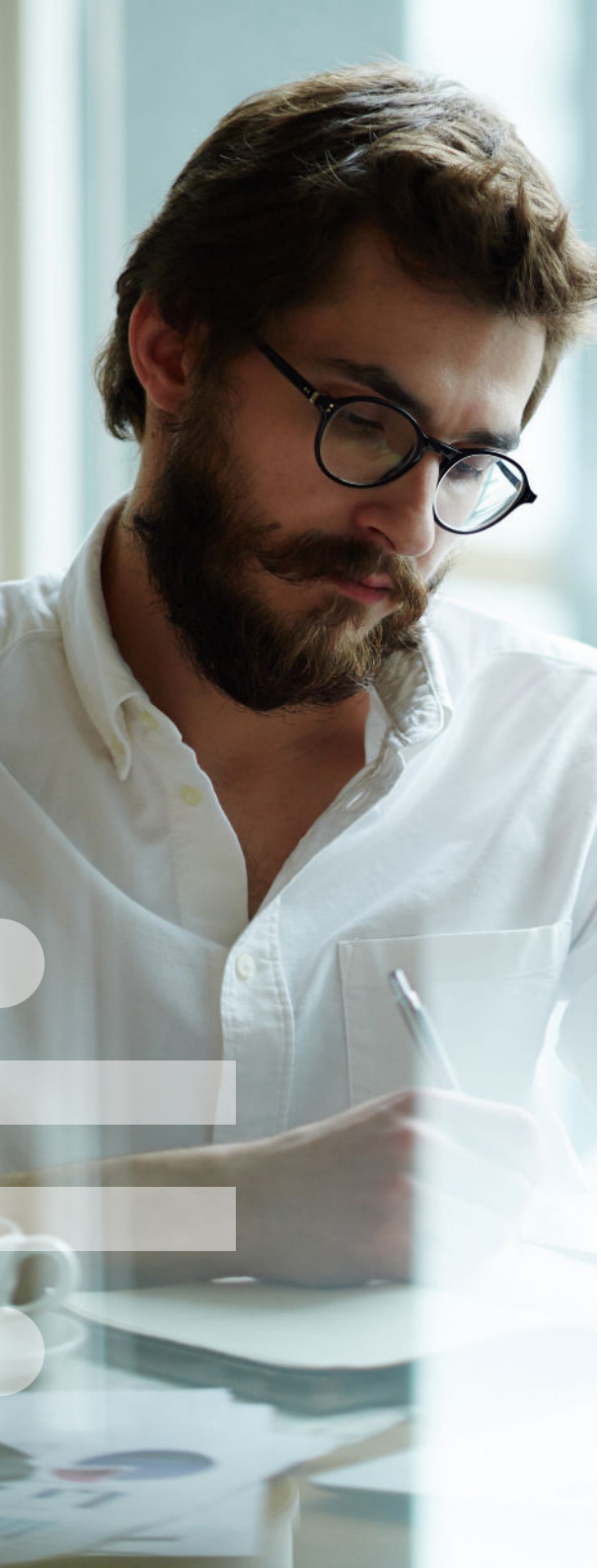
Waar maken we ons zorgen over?

Als het gaat om cyberbedreigingen, maakt ruim de helft van de ondervraagden zich het meeste zorgen om phising/smishing/vishing. In vergelijking met vorig jaar is dat toegenomen, net als de zorgen omtrent supply-chain aanvallen. Dit laatste betekent dat IT-professionals verder moeten gaan kijken dan hun eigen IT-platform en ook de gehele keten als ecosysteem weerbaar moeten maken. Dit is overigens één van de verplichtingen onder DORA, waarover later meer. Ruim vier op de tien maken zich (ook) zorgen om ransomware.

Vooral IT-professionals bij bedrijven van 500-999 werknemers maken zich meer dan gemiddeld zorgen over DDoS aanvallen, malware en supply chain aanvallen.

Over welke cyberdreigingen maakt u zich het meest zorgen? U kunt meerdere antwoorden geven.

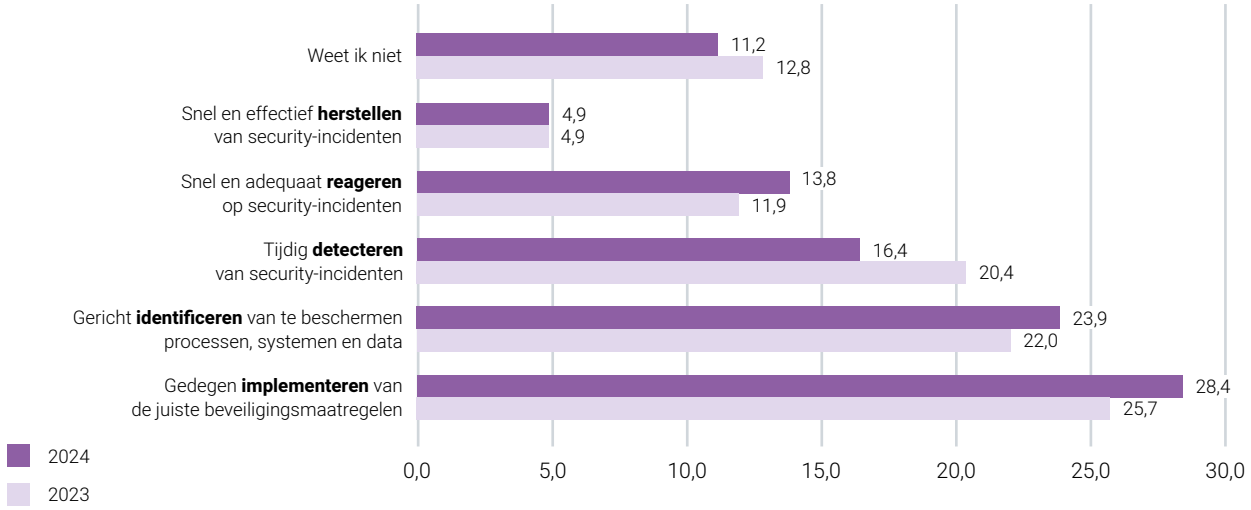




Wat zijn de uitdagingen op het gebied van security?

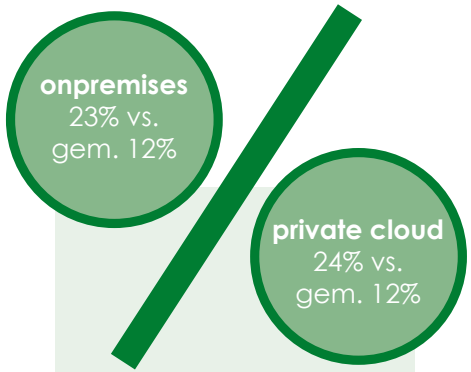
De grootste security-uitdaging die men ervaart binnen de IT-omgeving is het gedegen **implementeren** van de juiste beveiligingsmaatregelen, gevolgd door het gericht **identificeren** van te beschermen processen, systemen en data. Opmerkelijk is wel dat de middelgrote bedrijven (200-499 werknemers) hier met afstand de grootste uitdaging in zien en verhoudingsgewijs minder op het implementeren van de maatregelen.

Wat is de grootste security-uitdaging binnen uw IT-omgeving?



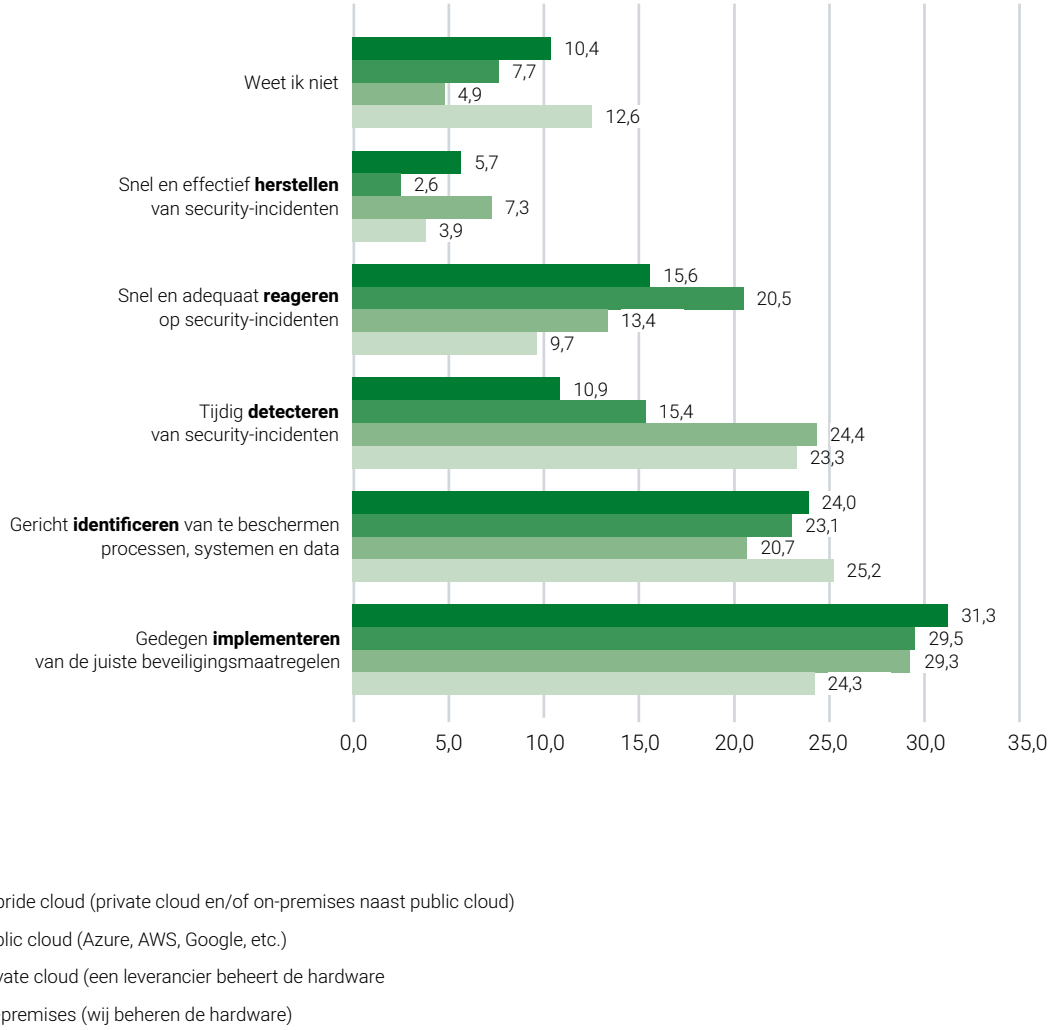
Kees

"Bij on-premise omgevingen is identificatie uitdagender door kennisgebrek, terwijl er bij hybride omgevingen meer geleund wordt op partners zoals Microsoft, AWS, Google en managed serviceproviders zoals Solvinity. Hier liggen de uitdagingen vooral bij implementatie. Public cloud biedt veel beveiligingsopties, maar door de snelle veranderingen is het lastig te bepalen wat te kiezen en te implementeren."



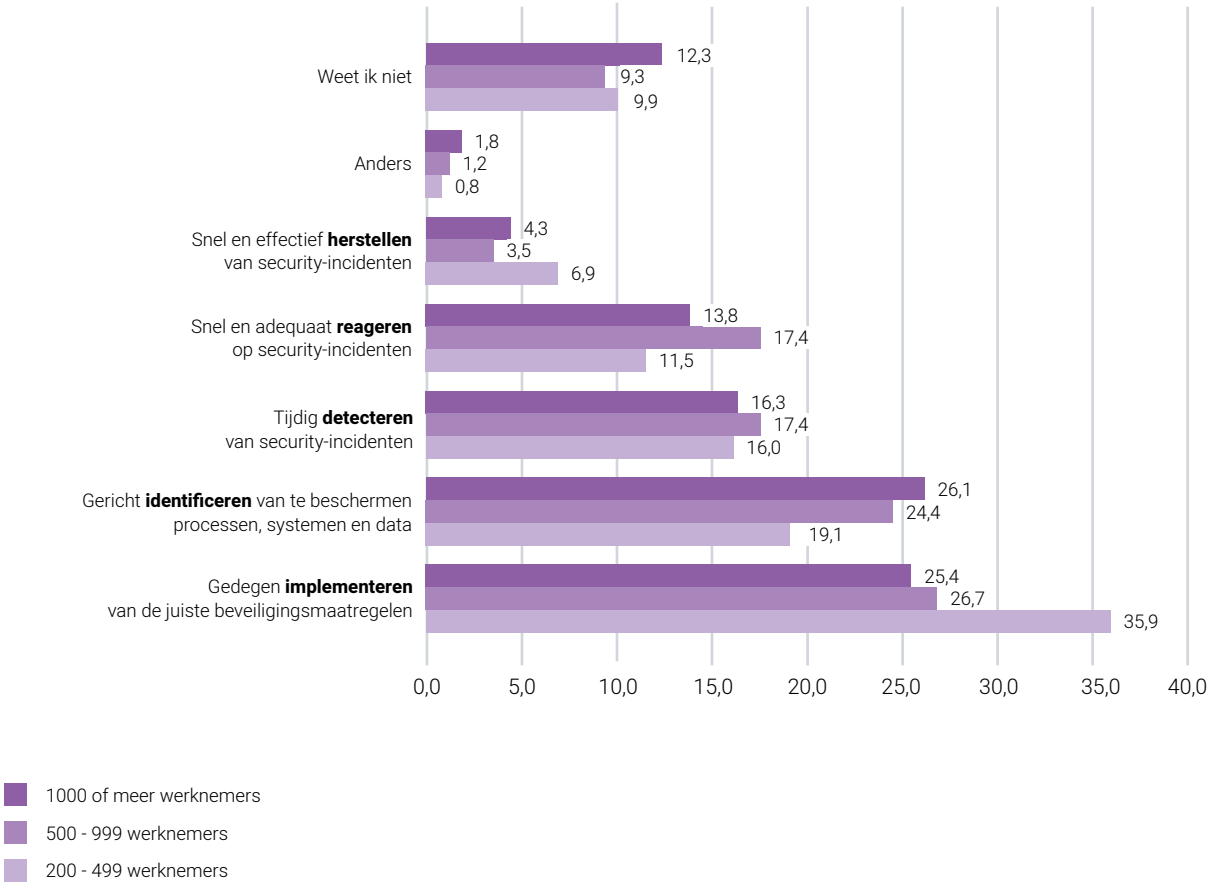
IT-professionals die werken met een 'onpremises' of 'private cloud' omgeving geven vaker aan dat het tijdig **detecteren** van security-incidenten een grote uitdaging is binnen hun IT-omgeving (resp. 23% en 24% vs. gem. 12%).

Wat is de grootste security-uitdaging binnen uw IT-omgeving?



Overigens geven de public cloud gebruikers van alle ondervraagden het meest aan dat zij een grotere uitdaging zien in het snel en adequaat kunnen reageren op security uitdagingen dan de private, hybrid en on-premise gebruikers. (grafiek) terwijl juist de private en on-premise gebruikers het tijdig detecteren als een grotere uitdaging zien.

Wat is de grootste security-uitdaging binnen uw IT-omgeving?



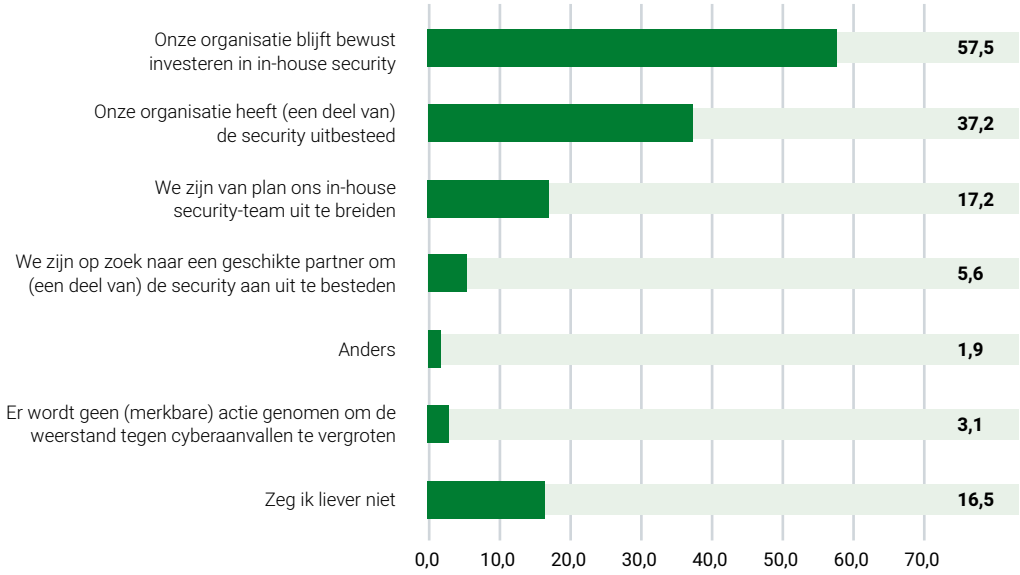
Marc

"We kunnen veel tools inzetten en veel automatiseren, maar er blijven mensen nodig om de weerbaarheid op peil te houden en maatregelen op het gebied van cybersecurity in te voeren en te beheren. Er is een tekort aan cybersecurity professionals om beveiligingsproblemen te voorkomen en op te lossen."

Wie zorgt er voor de weerbaarheid?

De manier waarop de meeste organisaties zich wapenen tegen cyberaanvallen is door het bewust blijven investeren in in-house security; bijna zes op de tien geven dit antwoord.

Op welke manieren wapent uw organisatie zich tegen cyberaanvallen?



IT professionals met management verantwoordelijkheid zeggen vaker van plan te zijn om hun in-house security-team uit te breiden (27% vs. gem. 16%). Dat zegt iets over de aandacht voor security binnen bedrijven. Het is niet verwonderlijk want in de meeste onderzoeken staat het punt "Cybersecurity" in de top 3 van aandachtspunten voor CIO's.

in-house security

IT-professionals met een 'hybride cloud' omgeving geven vaker aan dat hun organisatie bewust blijft investeren in in-house security.

65% vs. gem. 53%

security uitbesteed

Degenen die werken met een 'private cloud' zeggen vaker dat hun organisatie (een deel van) de security heeft uitbesteed.

53% vs. gem. 34%

'on-premises'

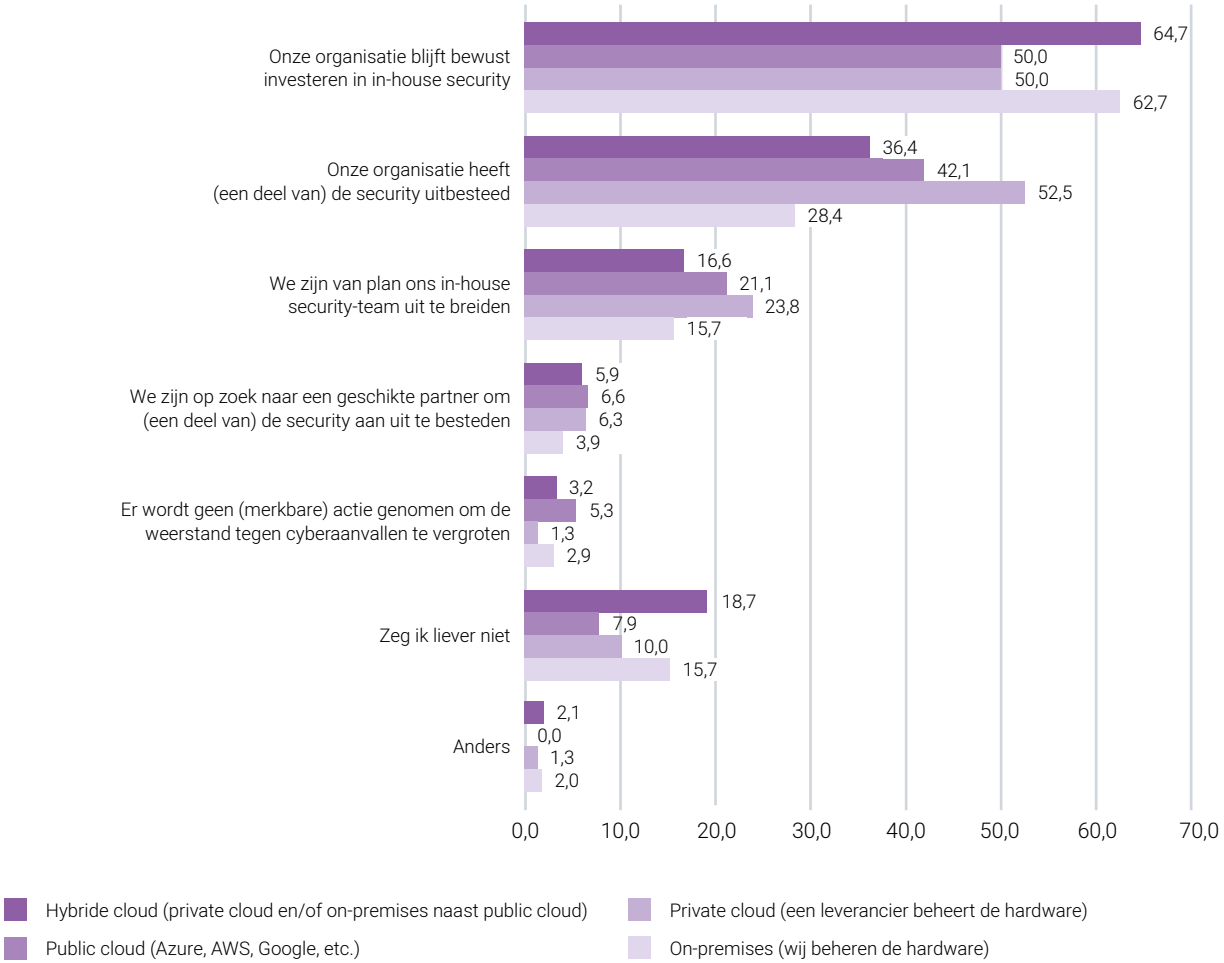
Degenen die hun IT-omgeving omschrijven als 'on-premises' geven dit juist minder vaak aan.

28% vs. gem. 40%

Wie zorgt er voor de weerbaarheid?

Verschillen per platform

Op welke manieren wapent uw organisatie zich tegen cyberaanvallen?



Hebben we de basis wel op orde: hardening en patching

Marc

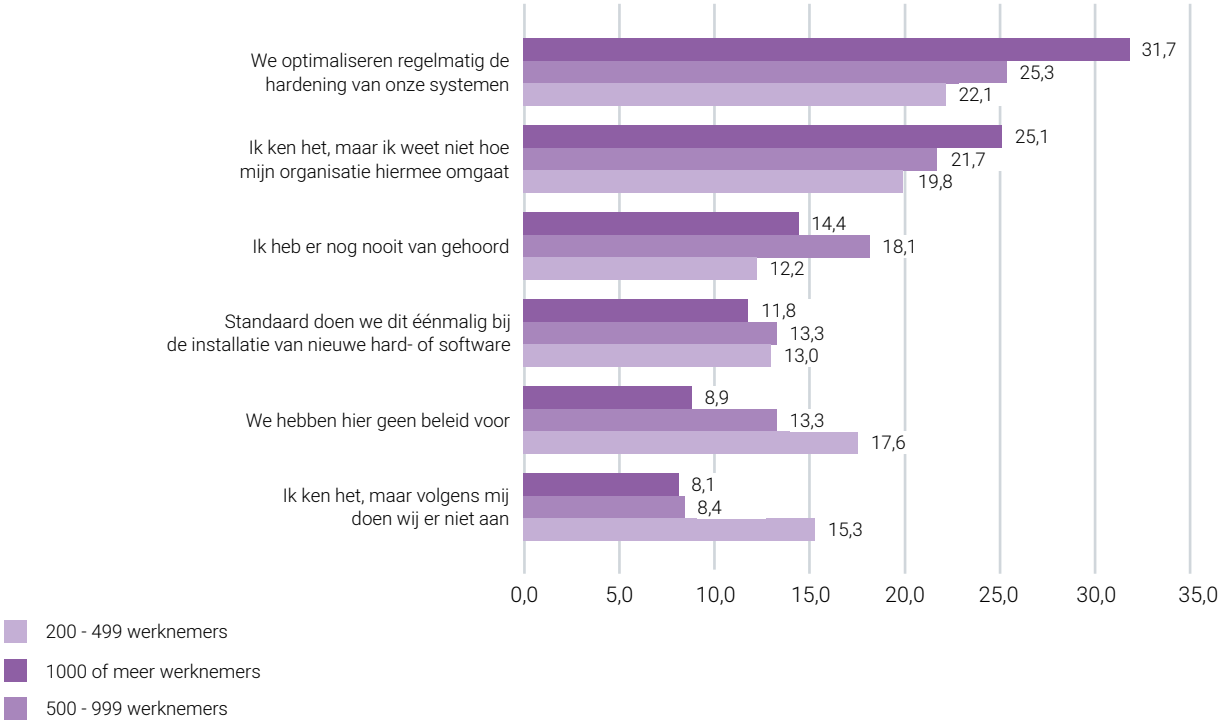
"In 2023 meldde nog ruim 10% van de organisaties geen beleid te hebben, en dat percentage is nu zelfs gestegen naar 12%. Dit baart me zorgen, want het betekent dat de situatie verslechtert. Hardening moet beginnen zodra je een nieuwe dienst bouwt of iets toevoegt. Gelukkig leveren leveranciers nu geen systemen meer met standaardwachtwoorden zoals root=root. Misschien denken IT-professionals daarom dat ze minder oplettend hoeven zijn, maar het is essentieel te weten hoe alles is ingesteld. De standaard stijgt, en daarmee ook de eisen."

37% van de ondervraagden geeft aan nog nooit van hardening gehoord te hebben of wel te kennen, maar niet te weten hoe hun organisatie hiermee omgaat. Gelukkig geeft bijna drie op de tien aan dat zij regelmatig de hardening van hun systemen optimaliseren. Maar ook voor de ruim 12% die dit standaard eenmalig doet bij de installatie van nieuwe hard- of software geldt; dit is echt niet voldoende!

Hoe gaat uw organisatie om met hardening?

Degenen die werkzaam zijn in een organisatie met 200 t/m 499 werknemers geven vaker aan dat zij bekend zijn met hardening, maar dat hun organisatie hier volgens hen niet aan doet (15% vs. 8% 500 of meer werknemers) of dat zij hier geen beleid voor hebben (18% vs. 9%). Degenen die werkzaam zijn bij een organisatie met 1000 of meer werknemers geven vaker aan dat zij regelmatig de hardening van hun systemen optimaliseren (32% vs. 23% 200 t/m 999 werknemers). Degenen die hun IT-omgeving omschrijven als 'hybride cloud' geven dit eveneens vaker aan (38% vs. gem. 22%).

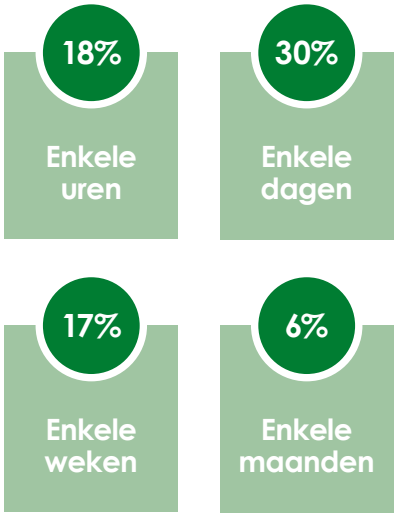
Hoe gaat uw organisatie om met hardening?

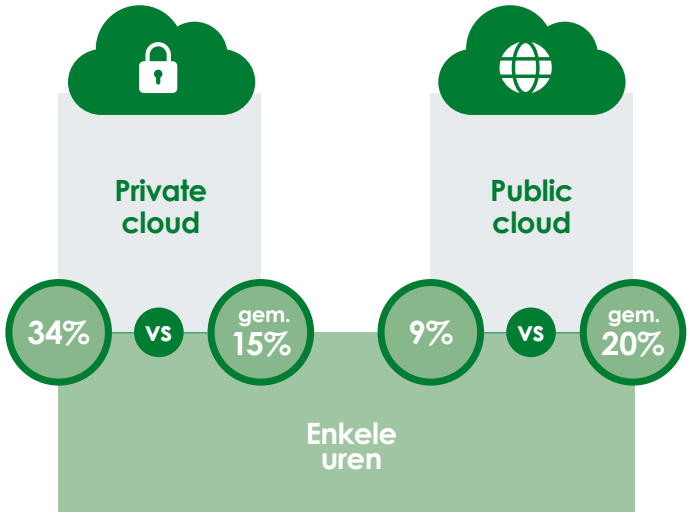


Updates en patching?

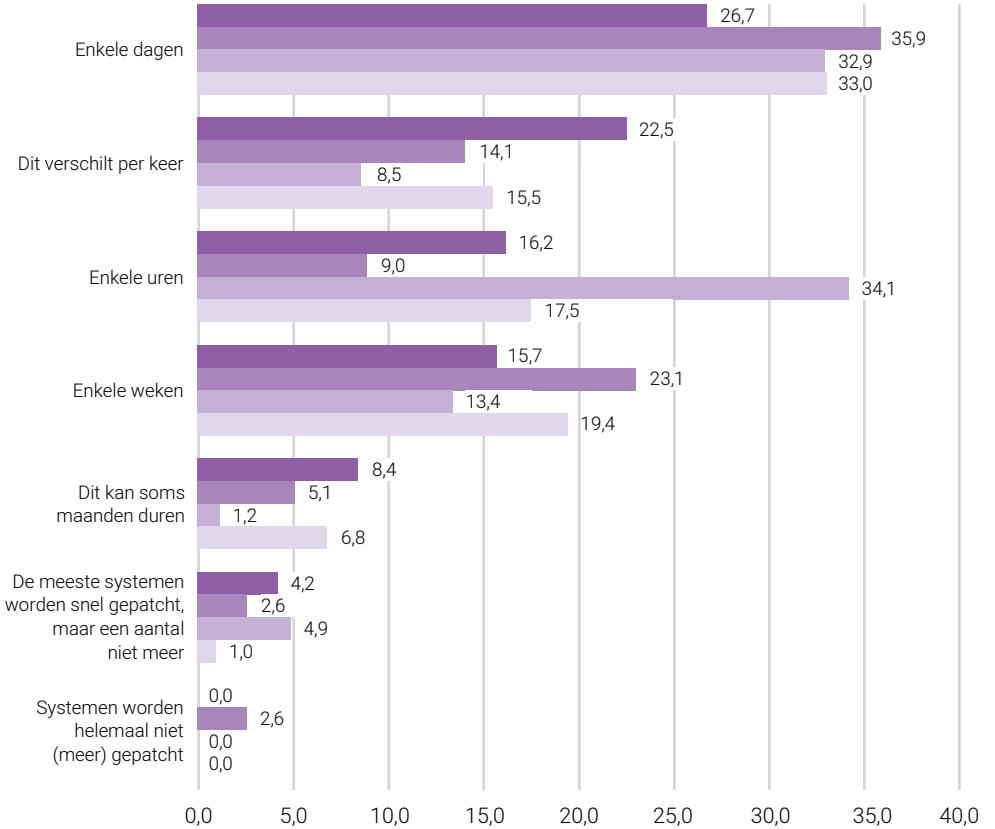
Bij bijna een vijfde duurt het gemiddeld enkele uren voordat updates en patches worden geïnstalleerd in hun organisatie. Bij drie op de tien kan dit enkele dagen duren. Bij 17% kan dit enkele weken duren en bij 6% kan dit soms maanden duren. Degenen die hun IT-omgeving omschrijven als 'private cloud' geven vaker aan dat updates en patches binnen enkele uren worden geïnstalleerd (34% vs. gem. 15%). Degenen die hun IT-omgeving omschrijven als 'public cloud' geven dit juist minder vaak aan (9% vs. gem. 20%). Dat maakt dat de IT-professionals in de private cloud duidelijk koplopers zijn als het gaat om het snel installeren van updates en patches.

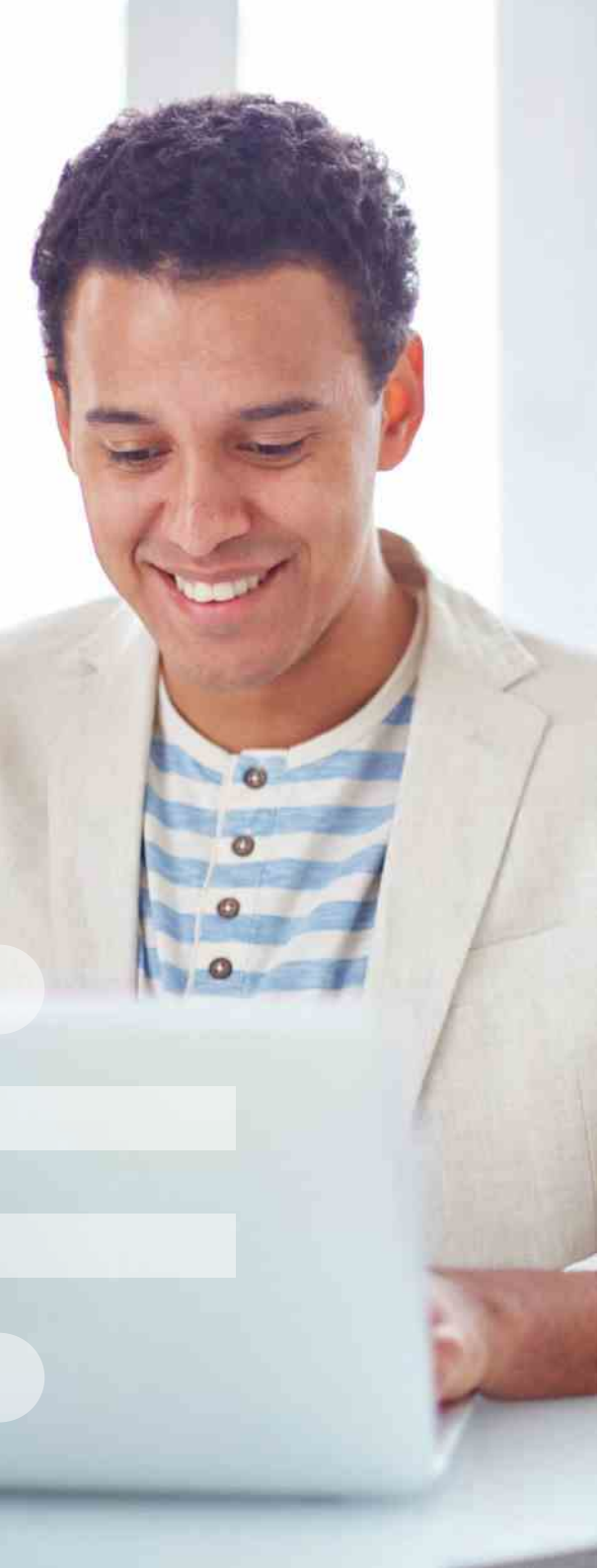
Hoe lang duurt het gemiddeld voordat updates enpatches worden geïnstalleerd bij uw organisatie?





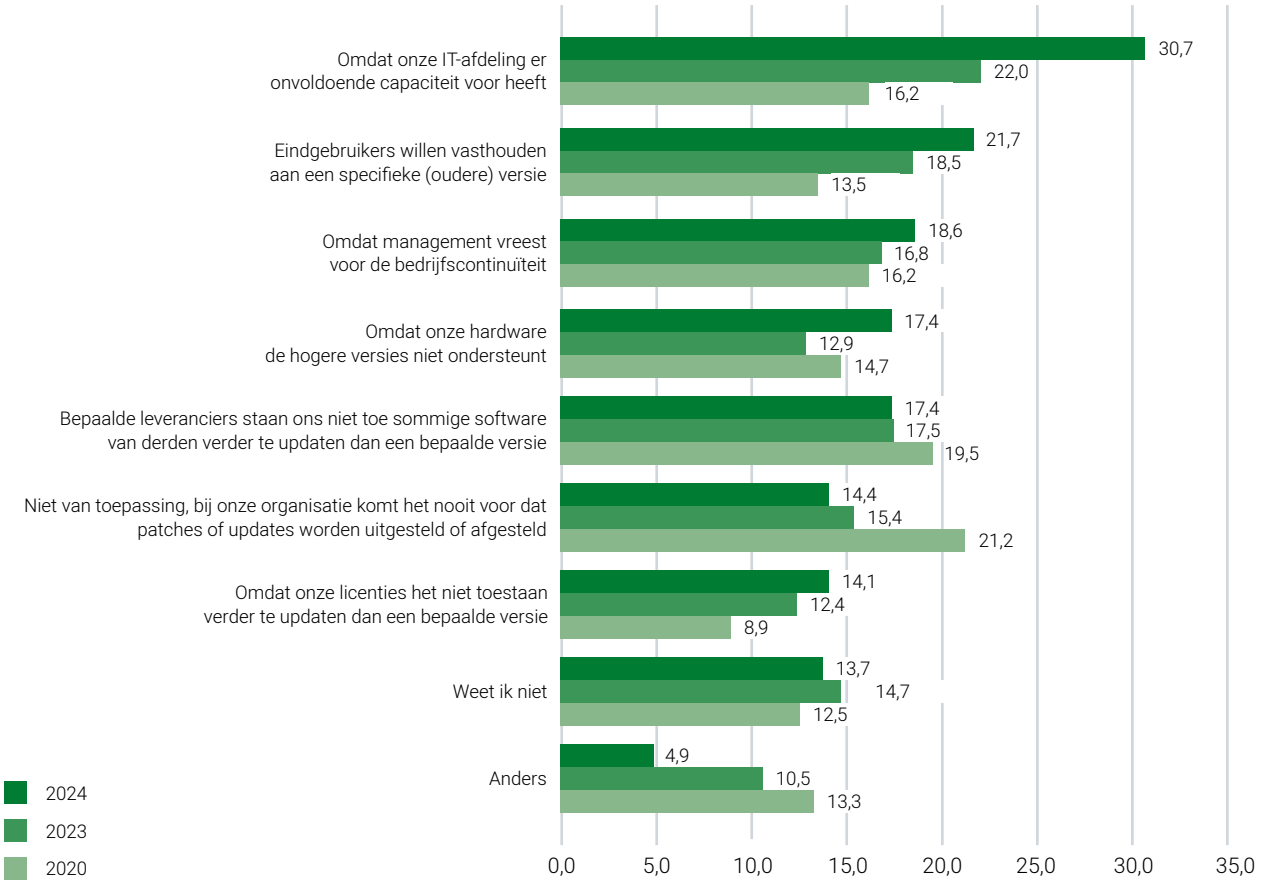
Hoe lang duurt het gemiddeld voordat updates enpatches worden geïnstalleerd bij uw organisatie?

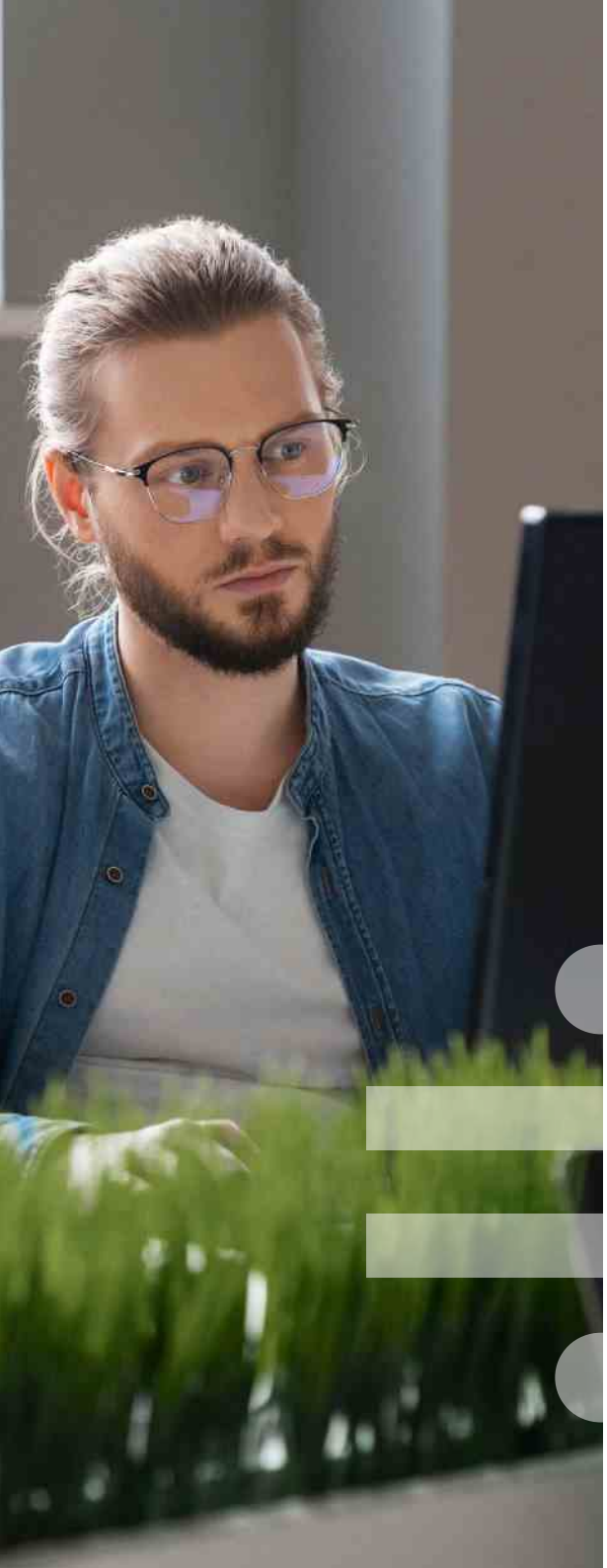




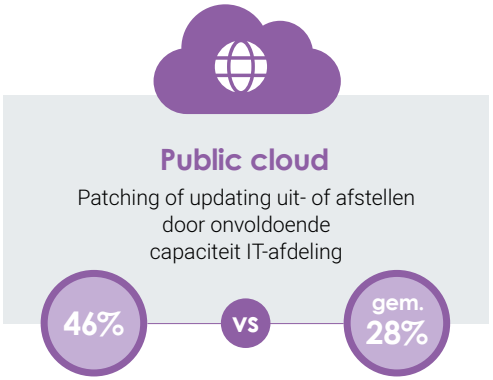
De meest gekozen reden waarom (soms) wordt besloten om patching of updating uit of af te stellen is omdat de IT-afdeling er onvoldoende capaciteit voor heeft en dat is sinds vorig jaar enorm gestegen. Daarnaast wordt relatief vaak aangegeven dat eindgebruikers willen vasthouden aan een specifieke (oudere) versie en/of omdat management vreest voor de bedrijfscontinuïteit.

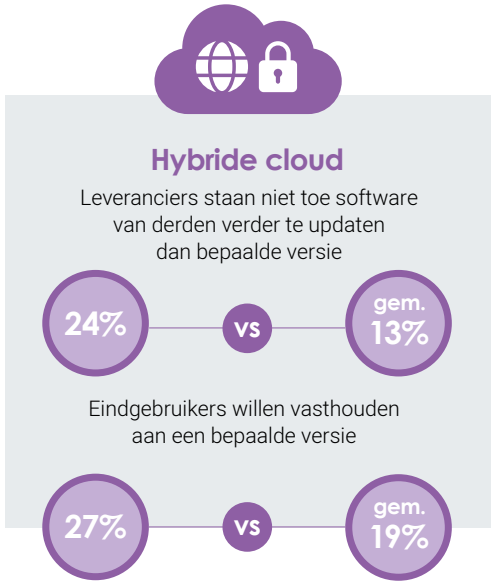
Waarom wordt (soms) besloten patching of updating uit/af te stellen?





Gebruikers met een 'public cloud' omgeving geven vaker aan dat (soms) wordt besloten om patching of updating uit/af te stellen omdat de IT-afdeling er onvoldoende capaciteit voor heeft (46% vs. gem. 28%). En gebruikers van een 'hybride cloud' geven vaker aan dat bepaalde leveranciers het niet toestaan om sommige software van derden verder te updaten dan een bepaalde versie (24% vs. gem. 13%) en dan eindgebruikers willen vasthouden aan een specifieke (oudere) versie (27% vs. gem. 19%).

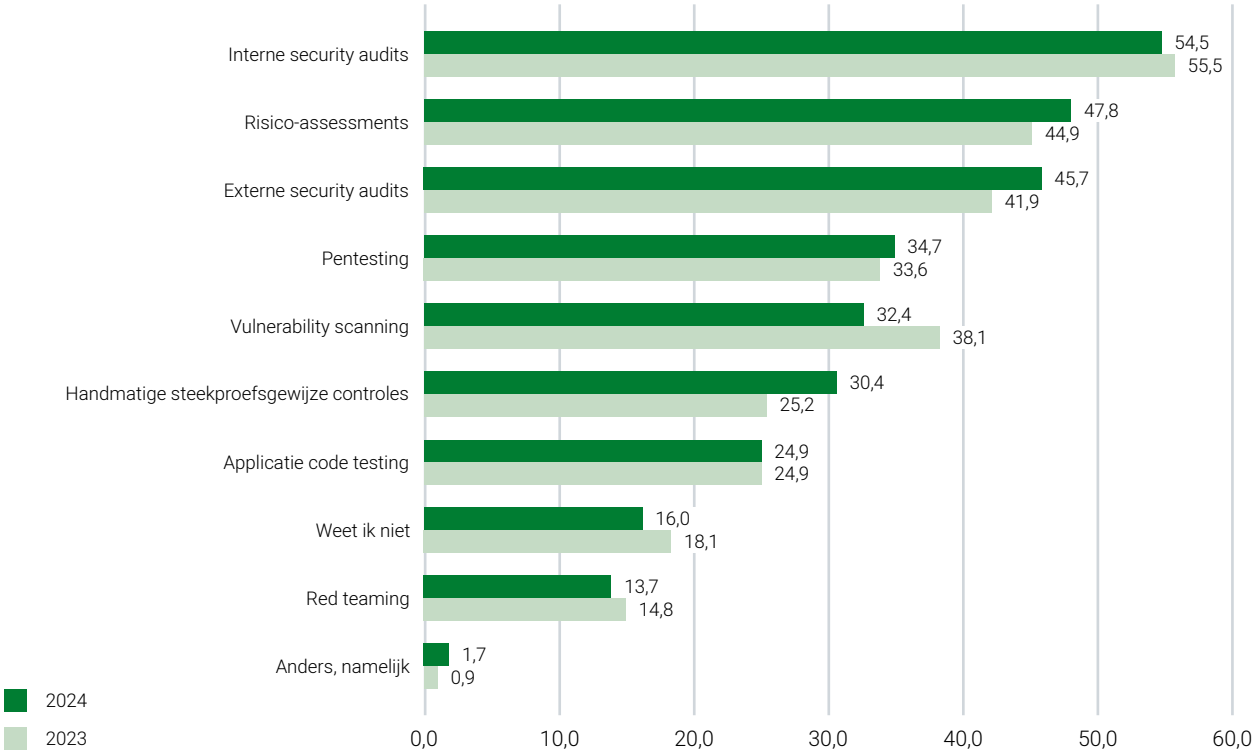




Wat zetten we in om onze weerbaarheid te toetsen?

De methode die het meest gebruikt wordt om de security te toetsen is het uitvoeren van interne security audits; ruim de helft geeft dit antwoord. Ruim vier op de tien gebruiken (ook) de methodes risico-assessments en/of externe security audits. Ten opzichte van 2023 zijn er kleine verschillen, wel valt de daling in vulnerability scans op.

Welke methoden gebruikt uw organisatie om de security te toetsen?



Kees

"Maar 1/3e van de organisaties geeft aan pentesten uit te voeren. Daarmee lijkt het erop dat grotere organisaties denken met certificeringen en audits alles op orde te hebben. Onze tests tonen elke keer het tegendeel aan. Zeker bij onze Red Teaming-projecten slaagt elke aanval. Kwetsbaarheden zitten in de hele keten, van een open poort in de firewall tot kwetsbaarheden in applicaties wat uiteindelijk resulteert in het verstoren van de operatie. Vinkjes en audits beschermen je niet. Test je omgeving en organisatie met scenario's, verhelp kwetsbaarheden en verbeter je reactie door te oefenen."

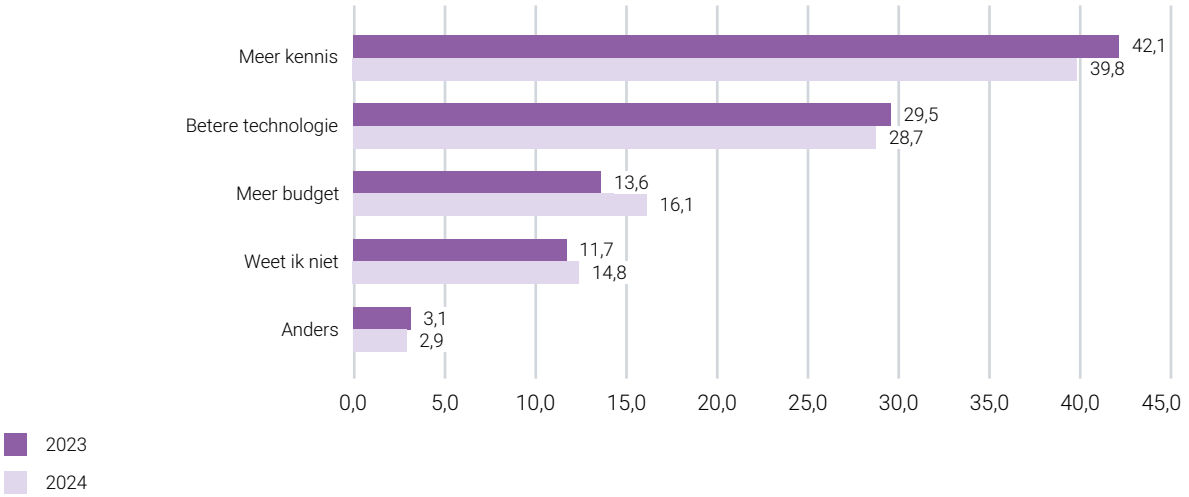
Hoe meer werknemers een organisatie heeft, hoe vaker men vulnerability scanning uitvoert (23% 200- 499 werknemers tot 38% 1000 of meer werknemers). Eenzelfde beeld is zichtbaar als het gaat om applicatie code testing (16% tot 28%). Degenen die hun IT-omgeving omschrijven als 'hybride cloud' geven alle voorgelegde methodes vaker aan.

De IT-professionals met hybride cloud omgevingen zijn hier de koplopers in het toetsen van de weerbaarheid en beveiliging van de IT-omgeving.

Wat hebben we nodig

Meer kennis wordt het vaakst genoemd als topprioriteit om de organisatie voor te bereiden op het gebied van toekomstige security-ontwikkelen; vier op de tien geven dit antwoord, gevolgd door betere technologie. Kleinere bedrijven geven vaker aan betere technologie en meer budget nodig te hebben dan de andere bedrijfsgroottes. Terwijl de public cloud en on-premise gebruikers met name aangeven meer kennis nodig te hebben.

Wat is in uw ogen de topprioriteit om uw organisatie voor te bereiden op het gebied van toekomstige security-ontwikkelingen?

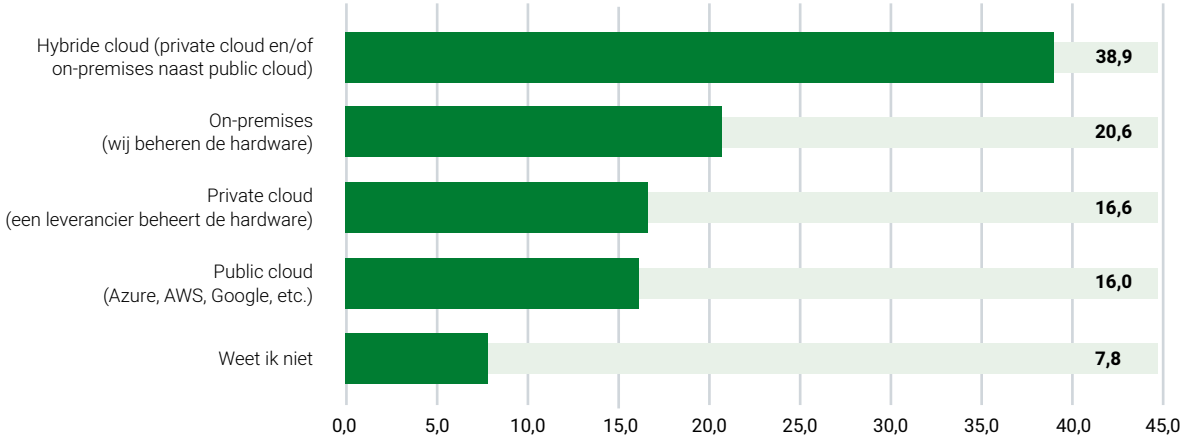


Martin

"Bij private en on premise omgevingen wordt minder extern belegd, mogelijk omdat IT-professionals bij die platformen het gevoelsmatig meer onder controle denken te hebben. Dit leidt mogelijk tot een gevoel van schijnveiligheid. Dit kun je voorkomen door juist specialisten van buiten naar je omgeving te laten kijken. Die hebben echt een andere bril op!"

Private cloud, hybrid cloud, public cloud

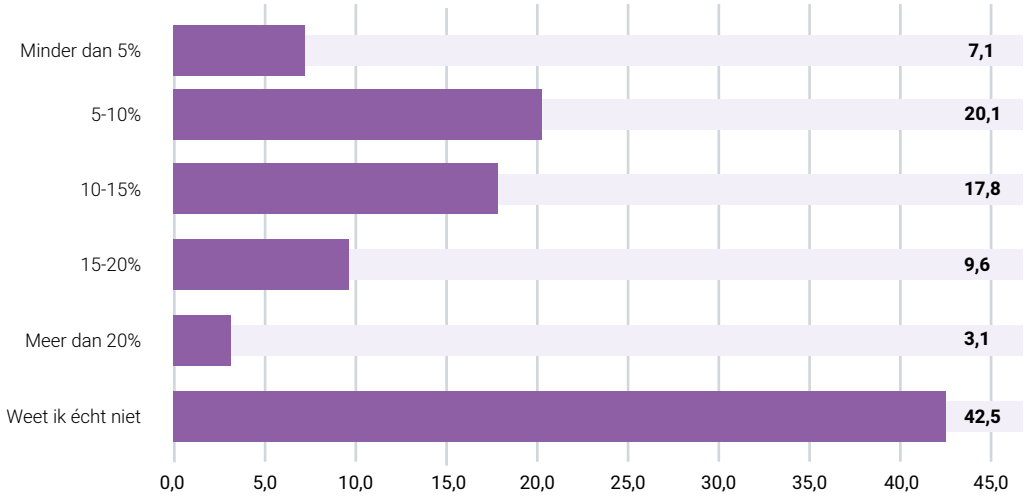
Van de ondervraagden geeft bijna 40% aan dat hun organisatie een hybride cloud gebruikt, gevolgd door on-premise (21%), 'private cloud' (17%) of 'public cloud' (16%) als het best passend als omschrijving van hun IT-omgeving.



Wat hebben we er voor over?

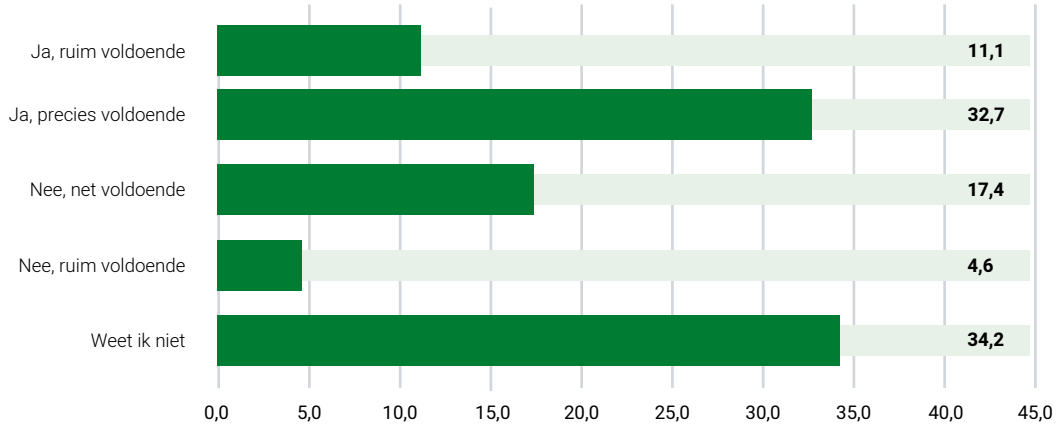
Het budget voor IT-security beslaat meestal tussen de 5-10% (20%) en 10-15% (18%) van het totale IT-budget. 7% geeft aan dat minder dan 5% van het IT-budget van hun organisatie gaat naar IT-security en een tiende geeft aan dat dit ligt tussen de 15% en 20%. Ruim vier op de tien vinden het budget voor security (ruim) voldoende om de security van hun organisatie te waarborgen.

Ruim 20% vindt dat het budget net tot ruim onvoldoende is, maar bijna 44% vindt het ruim of precies voldoende. Zes op de tien verwachten dat het budget dat hun organisatie in 2025 zal besteden aan IT-security zal toenemen ten opzichte van 2024. Een zesde verwacht dat het budget gelijk zal blijven. Slechts 2% denkt dat het budget zal afnemen in 2025.



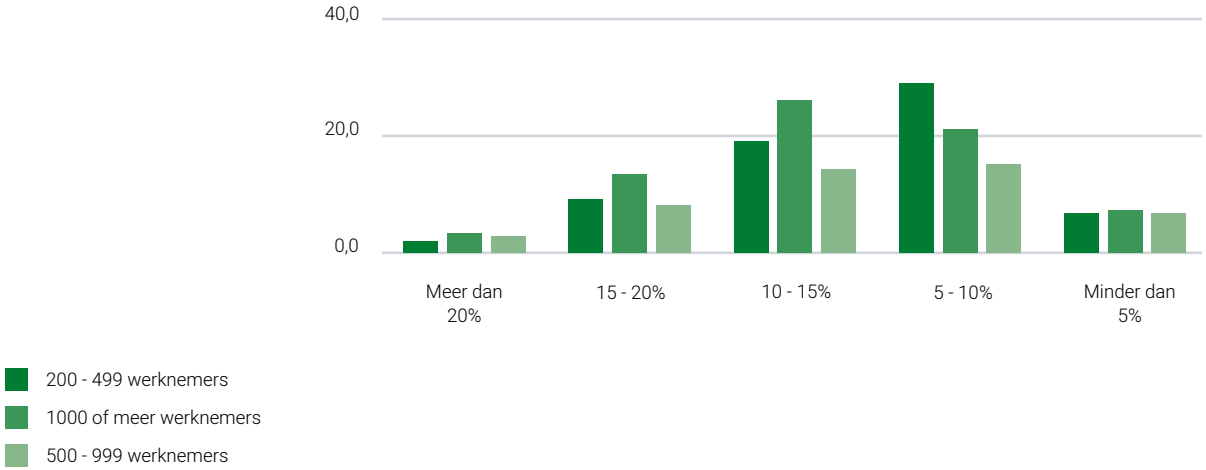
Marc

"Nieuwe oplossingen zijn complex, het implementeren en beheren ervan vraagt heel wat van organisaties. Je hebt eigenlijk altijd 30 dingen nodig of je nou een groot, of middelgroot bedrijf bent. Maar de investeringen vormen relatief gezien percentueel een grotere hap van de omzet van kleiner bedrijf. Deze belasting is dus a-synchroon en daar maak ik me zorgen over. Vooral met betrekking tot het voldoen aan van BIO en NIS2 tot DORA. Een bedrijf van 200 man krijgt dat moeilijk voor elkaar, hoe hard ze daar ook voor werken."



Ruim vier op de tien (42%) weten niet hoeveel procent van het IT-budget van hun organisatie gaat naar IT-security. Dit wordt minder vaak aangegeven door degenen die (onder andere) betrokken zijn bij IT-management (28% vs. gem. 44%). En juist vaker door degenen die werkzaam zijn bij een organisatie met 1000 of meer werknemers (51% vs. 31% 200-999 werknemers).

Budget/bedrijfsgrootte



Aanbevelingen voor een beheersbare en weerbare omgeving

1. **Bouw een goede basis en houd die op orde**
2. **Kijk verder dan je eigen omgeving, test je ergste nachtmerrie**
3. **Maak gebruik van AI, maar mét beleid**
4. **Gebruik een holistische aanpak, anders loop je vast**

Martin

"De moeite die gedaan wordt om ergens binnen te komen, wordt vaak onderschat. Professioneel gehackt worden is een reëel risico. Je kunt 90 à 95% van de aanvallen tegenhouden door je omgeving "fris" te houden. In de cloud worden snel omgevingen aangemaakt en vaak vergeten na het testen. Wie heeft toegang? Is alles gepatcht? Dit geldt voor zowel test- als productieomgevingen. Hackers maken geen onderscheid, dus waarom geen MFA of vulnerability scanning in testomgevingen?

Veel inbraken beginnen bij niet-productieomgevingen. APIs worden snel aangemaakt en vergeten, maar vormen een kwetsbare poort. Werk beveiligingssoftware en -systemen regelmatig bij en patch ze om beschermd te blijven tegen de evoluerende cyberdreigingen in 2024."

1 Bouw een goede basis en houd die op orde

- Gebruik MFA en vulnerability voor test- en productieomgevingen
- Voer patches zo spoedig mogelijk uit
- Test je back up & recovery
- Gebruik immutable back ups

2 Kijk verder dan je eigen omgeving, test je ergste nachtmerrie

- Doe een Security gap analyse en krijg inzicht in de staat van jouw weerbaarheid en een roadmap om deze weerbaarheid stapsgewijs te verhogen.
- Onder DORA verplicht, maar zeker geen overbodige luxe voor elk bedrijf: zorg voor een teststrategie inclusief Red Teaming test.
- In bijna elk bedrijf wordt software op een agile manier ontwikkeld, zorg voor veilige applicaties met regelmatige code reviews.

Kees

"Een goede test strategie bestaat uit 4 pijlers:

1. **Code**
2. **Applicatie**
3. **Infrastructuur**
4. **Organisatie**

Op elk niveau spelen namelijk verschillende belangen met verschillende risico's. Weet wat je kroonjuwelen zijn en weet wie je aanvallers zijn. Op basis daarvan kan er een teststrategie opgezet worden. Daarin wil je ten minste een Red Teaming test in hebben. Een test op organisatieniveau, waarbij je jouw ergste nachtmerrie bewust gaat testen. Wij zien bij de vele Red Teaming testen die wij uitvoeren dat we vrijwel altijd tot het doel komen.

Na de test is vaak het besef dat er nog veel werk aan de winkel is om de weerbaarheid van de organisatie op alle vlakken te verhogen. De bevindingen uit de testen worden verwerkt in een roadmap en uiteindelijk opgelost. Dat, samen met de ontwikkelingen van de aanvallers, zorgt ervoor dat het risicoprofiel op de verschillende pijlers weer wijzigt en dat heeft dus weer invloed op de teststrategie. Dat betekent dat je die net als de risicoanalyse jaarlijks bijwerkt."

3 Maak gebruik van AI, maar mét beleid

- Maak gebruik van AI-gestuurde detectietools die in staat zijn om potentiële deepfakes in multimedia-inhoud, waaronder afbeeldingen en video's, te identificeren die werknemers tijdens hun werk tegenkomen.
- Check je eigen scripts, voorkom foute configuraties.

4 Gebruik een holistische aanpak, anders loop je vast

Dat kan omdat in de public cloud zoveel mogelijk geautomatiseerd wordt. In beheer helpen geautomatiseerde security en compliance checks om als organisatie zelf ook beter in control te zijn.

Maar met het gebrek aan kennis en expertise én de nodige mankracht, is het voldoen aan compliance eisen in een hybrid of private cloud nog geen sinecure.

Dan kom je er alleen met een holistische aanpak waarbij je over alle vereisten heen, één overkoepelende set van controls implementeert. Maar dat kost nog steeds veel tijd en geld. Wij nemen voor onze klanten zorgen uit handen door voor gebruikers van ons Solvinity Private Cloud én de door ons beheerde Azure cloud omgevingen, jaarlijks de SOC 1 en SOC 2 audits uit te laten voeren.

- Bespaar kosten en manuren met de Proof of SOC 2 compliance service

Marc

"AI speelt een steeds grotere rol in security, maar niet iedereen heeft toegang tot deze technologie. SIEM-toepassingen kunnen worden geautomatiseerd voor rapportages over false positives, maar dit vereist een effectieve aanpak. Handmatige verwerking is niet langer wenselijk, dus automatisering moet rekening houden met het integreren van data uit verschillende security tools, bijvoorbeeld in een datalake of SIEM.

Om weerbaar te zijn, adviseer ik AI-gebruik niet te verbieden, maar een beleid te ontwikkelen. Cybercriminelen benutten AI volledig, dus om niet achter te blijven, moet je minstens even goed uitgerust zijn. Maak gebruik van AI met beleid en begrijp de implicaties van generative AI."

Kees

"De public cloud maakt het voldoen aan compliance gemakkelijker – voor een actueel overzicht van de compliance met ISO 27001 status hoef je weinig te doen, dat zit bijvoorbeeld ingebakken in Azure. Dat geldt trouwens ook voor een flink aantal maatregelen binnen SOC 1 en SOC 2 – daar zijn security controls waarvan Microsoft checkt of ze worden uitgevoerd."

Oplossingen voor een hogere weerbaarheid

Wil je meer weten over wat Solvinity voor jouw bedrijf kan doen?

De inzichten in dit onderzoek bieden een indicatie van de weerbaarheid van Nederlandse organisaties. Heb je vragen hoe jouw organisatie zich hiertegen verhoudt? Solvinity staat voor je klaar. Ook wanneer je eigen specialisten hebt, die je vrij wilt spelen voor innovatie. Of wanneer je een partner nodig hebt om je security te evalueren.

Wij ontwerpen, bouwen en beheren cloudplatformen voor bedrijven en instellingen die een hoge mate van beveiliging vereisen. Met onze kennis, ervaring en serviceportfolio bieden we onze klanten oplossingen om hun IT-omgeving optimaal te laten functioneren én bieden je oplossingen om jouw cloudplatform veilig te houden.

WIL JE MEER WETEN?

Neem contact met ons op via
info@solvinity.com of
+31 (0)20 36 43 600
of bezoek onze website
solvinity.com.

Solvinity
Secure Managed Cloud

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
www.solvinity.com

Solvinity ontwerpt, bouwt en beheert de complexe platformen waarop bedrijfskritische applicaties veilig en optimaal functioneren.

	Managed Cloud	Security & Compliance	Service Integration
	Outsourcing	Lango Workspace	Application Services
	Solvinity onderscheidt zich op het gebied van cybersecurity met een uitgebreid portfolio aan securitydiensten en -oplossingen en biedt, met een meerderheidsbelang in Securify.nl, aanvullende cybersecurity diensten.		
	Daarnaast heeft het bedrijf certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001, PCI DSS en heeft het als eerste MSP in Nederland SOC 1 en 2 compliance rapporten voor de gehele beheeromgeving van de private én Azure cloud.		
	Solvinity levert Secure Managed Cloud Services aan organisaties met hoge beveiligings-eisen. Hiermee ondersteunt het bedrijf de (rijks-)overheid, gemeenten en toon-aangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, TransLink (OV-chipkaart), ING en ONVZ.		
	300 medewerkers	2022: omzet 62 mln	Amsterdam, Assen Amersfoort, Den Bosch