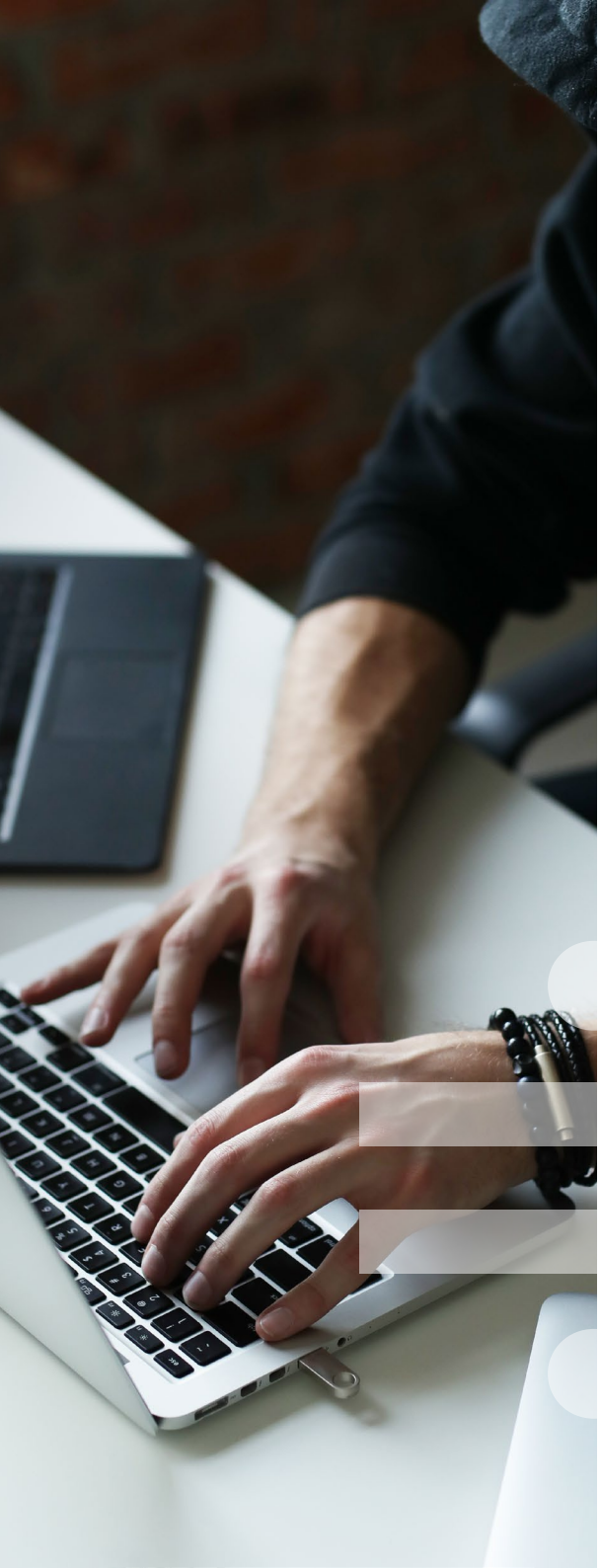
Solvinity
Secure Managed IT Services

CYBERSECURITY ONDERZOEK

Solvinity onderzoeksrapport | **Smarter Security 2023**

Inhoud



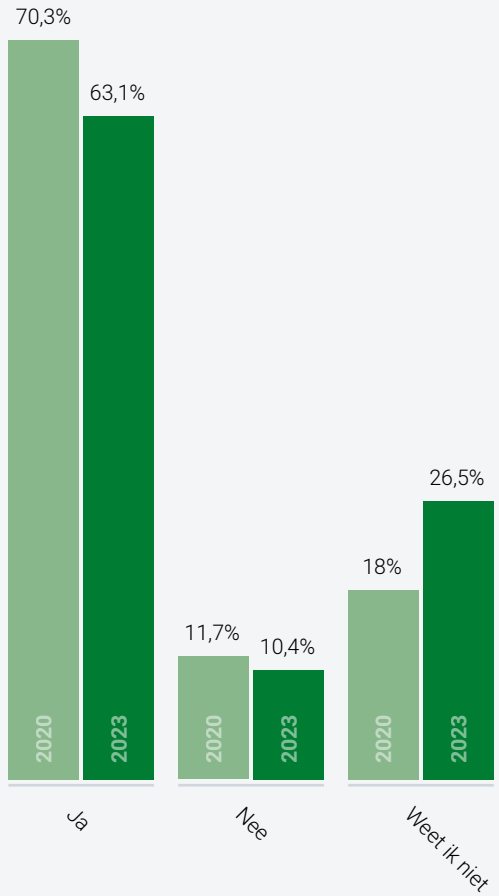
Introductie

Het belang van IT-security staat buiten kijf in een wereld waarin Nederlandse bedrijven wekelijks met honderden cyberaanvallen worden geconfronteerd. Toen wij drie jaar geleden ons eerste security-onderzoek uitvoerden, leek dat besef nog niet overal te zijn doorgedrongen. De onderzoeksresultaten lieten zien dat veel organisaties beperkt inzicht hebben in hun eigen kwetsbaarheid, waardoor ze snel hun weerbaarheid overschatten.

Security is inmiddels een trending topic. Daarom is nu het moment om te kijken naar de security-stand van zaken anno 2023. Niet alleen om te toetsen of het beeld van de eigen weerbaarheid realistischer is geworden, maar juist ook om te zien of dit wordt weerspiegeld in de genomen maatregelen en budgettering. Om die reden voerde PanelWizard in maart 2023 voor Solvinity een nieuw onderzoek uit onder ruim 400 IT professionals werkzaam bij Nederlandse organisaties met meer dan 200 medewerkers.

Een eerste blik op de onderzoeksresultaten schetst een positief beeld: 63,1% van de Nederlandse IT professionals is van mening dat hun organisatie voldoende weerstand kan bieden tegen cyberaanvallen. Dat is lager dan in 2020, toen 70,3% genoeg weerstand dacht te hebben. Een teken van hogere kwetsbaarheid, of een realistische bijstelling?

Denkt u dat uw organisatie zelf in staat is voldoende weerstand te bieden tegen cyberaanvallen?



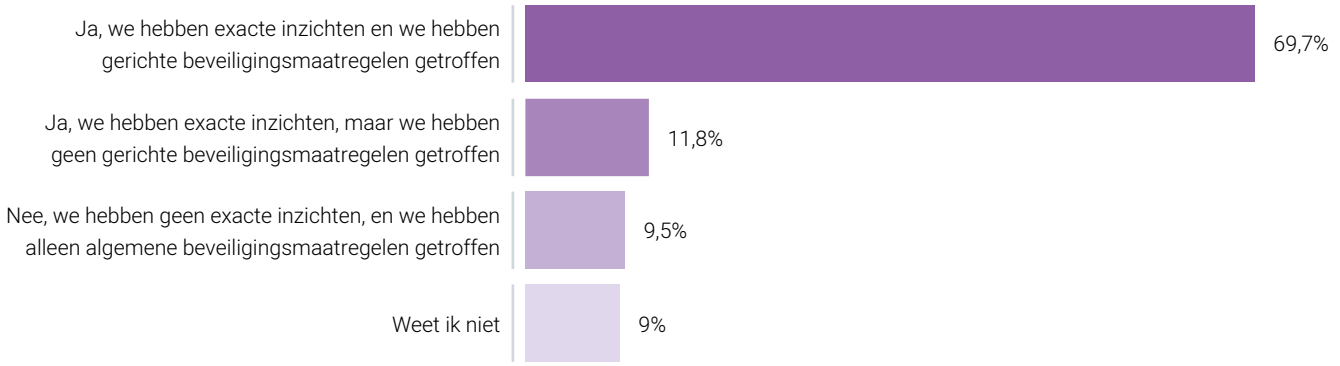
"Jarenlang werd vulnerability management gezien als een nice-to-have."

Meer aandacht voor security dan ooit

Alles begint met inzicht, schreven we in het eerste security-onderzoek van Solvinity. In 2020 wist slechts 49% van de ondervraagde IT-professionals waar hun organisatie kwetsbaar is en had daar gerichte maatregelen op genomen. In 2023 is dat percentage gestegen naar 69,7%. Dat klinkt Marc Guardiola, CTO bij Solvinity, als muziek in de oren. "Jarenlang werd vulnerability management gezien als een nice-to-have. Het is goed om te zien dat meer respondenten concluderen dat het een must-have is. Tegelijkertijd heeft bijna één op drie organisaties het nog niet op orde. Er is dus nog best wat te winnen."

Verschillende methoden worden gebruikt om verdacht netwerkverkeer te weren en bedrijfsdata veilig te houden. Daarbij wordt niet alleen firewalling ingezet (56,1% van de respondenten). Ook IPS en IDS-oplossingen (Intrusion Prevention en -Detection-systemen) worden veel gebruikt (30,6%). Opmerkelijk is dat 33% van de respondenten aangeeft een SIEM-oplossing (Security Information and Event Management) te gebruiken. "SIEM-tooling is een informatiesysteem dat wordt gevoed door andere systemen zoals firewalls en IPS- en IDS-tools. Zonder die hulpmiddelen heeft een SIEM-oplossing dus eigenlijk onvoldoende informatie om de juiste inzichten te bieden."

Heeft uw organisatie inzicht in de kwetsbaarheid van de IT-omgeving?

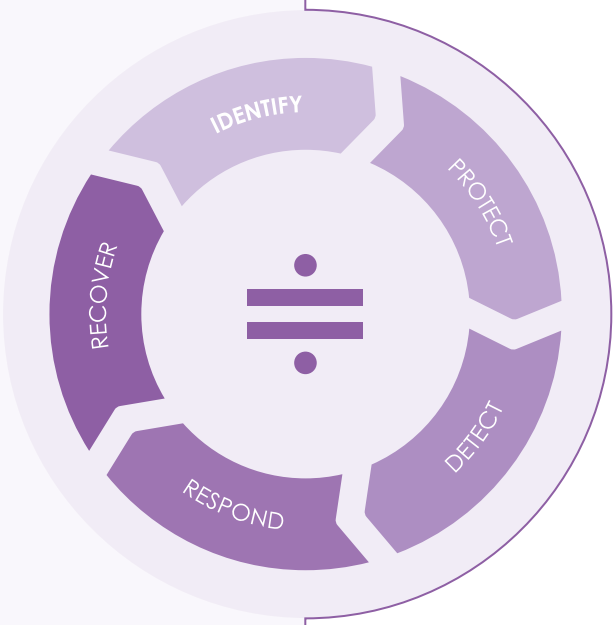


Dat er meer gebruik van SIEM dan IPS/IDS lijkt te worden gemaakt, ligt mogelijk aan het feit dat één op de tien van de respondenten liever niet aangeeft welke security tooling ze gebruiken. Bovendien heeft niet iedereen een helder beeld van de precieze securitystack die in gebruik is (18,4%). Dat vindt Guardiola helemaal niet erg: “Niet alle IT-professionals hoeven alle details te kennen. Zolang IT-management en de securityspecialisten maar weten hoe het in elkaar zit.” Dat 29,9% van de IT-managers en één op de tien securityprofessionals aangeven dit niet te weten, vindt hij wél zorgelijk.

VAN INZICHT NAAR ACTIE

Inzicht in netwerkverkeer en gebruikersgedrag is cruciaal voor iedere integrale securitystrategie, die volgens het NIST-framework bestaat uit enkele fasen:

1. In Identify en Protect draait het om het identificeren van kwetsbaarheden en het inrichten van de verdediging.
2. In Detect en Respond gaat het om de tijdige detectie van en reactie op beveiligingsincidenten.
3. En wanneer het ‘mis’ gaat, moet je in Recover snel kunnen herstellen.



Solvinity helpt zijn klanten de juiste maatregelen te treffen om het gehele NIST-framework af te dekken. Hoe wij dit doen? Bekijk onze Managed Security Services.

"Securitymedewerkers moeten goed weten welke hardening precies wordt toegepast."

De basis niet op orde?

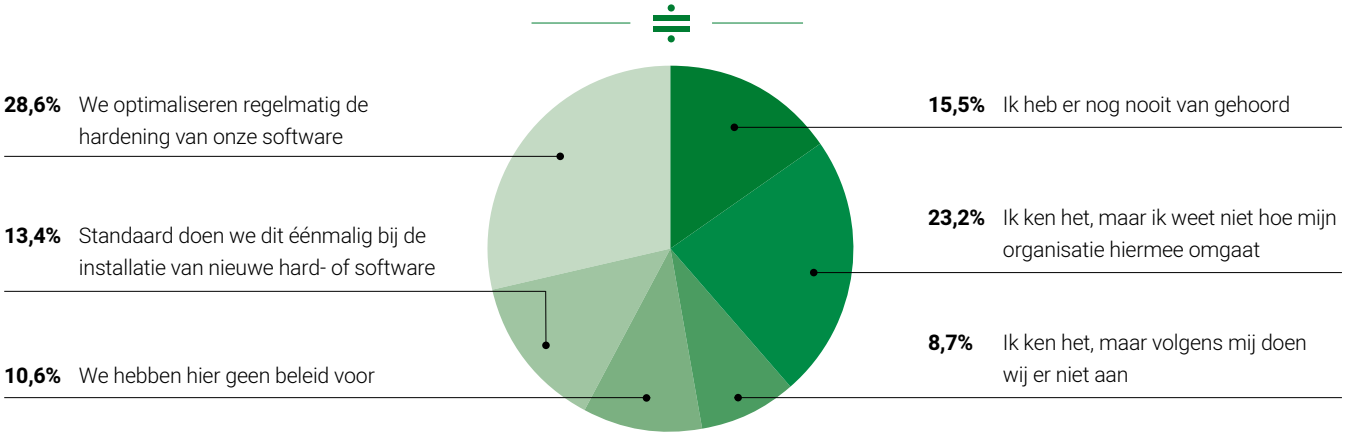
Vulnerability management omvat niet alleen monitoring en verdediging van bedrijfssystemen. Onder de paraplu van vulnerability management vallen tal van basishygiënemaatregelen die bedrijven moeten treffen, waaronder hardening en patch management.

Hardening

Hardening is een verzameling van maatregelen om het aanvalsoppervlak van een bedrijfsnetwerk te verkleinen. Denk onder meer aan het uitschakelen van niet-gebruikte softwarecomponenten, het gebruik van sterke en periodiek veranderende wachtwoorden, en de inregeling van de juiste toegangsrechten. Uit het onderzoek blijkt dat respondenten inmiddels bekender zijn met het concept. Terwijl in 2020 26% van de IT-professionals nog nooit van hardening had gehoord, is dat in 2023 gedaald tot 15,5%.

In 2020 kende 5% van de respondenten de term wel, maar wist toen niet hoe de organisatie met hardening omging. Dát percentage is in 2023 gestegen naar 23%. Dat is niet direct reden tot zorg, volgens Guardiola. "Hardening is basishygiëne, dus het kan goed zijn dat het wordt uitgevoerd, maar respondenten niet precies weten hoe of wanneer." Wederom zien we echter dat één op de tien van de ondervraagde securityprofessionals hier onzeker over is. Dat is reden tot zorg voor Guardiola. "Er zijn een paar redenen om bepaalde hardeningmaatregelen níet te treffen, bijvoorbeeld als applicaties er niet meer door functioneren en je het doel van de hardeningmaatregel op een andere manier kan bereiken. Maar securitymedewerkers moeten goed weten welke hardening precies wordt toegepast. Dit percentage zou dus nul moeten zijn."

Hoe gaat uw organisatie om met hardening?



"Capaciteitsgebrek staat haaks op het besef dat security cruciaal is."

Patchmanagement

De afgelopen drie jaar zijn de gevolgen van gebrekkig patch-management volop in het nieuws geweest. Breed uitgelichte ransomware-aanvallen en andere hacks bleken het gevolg van kwetsbaarheden waar patches voor beschikbaar waren. Je kan je dan afvragen, waarom was er niet op tijd gepatcht?

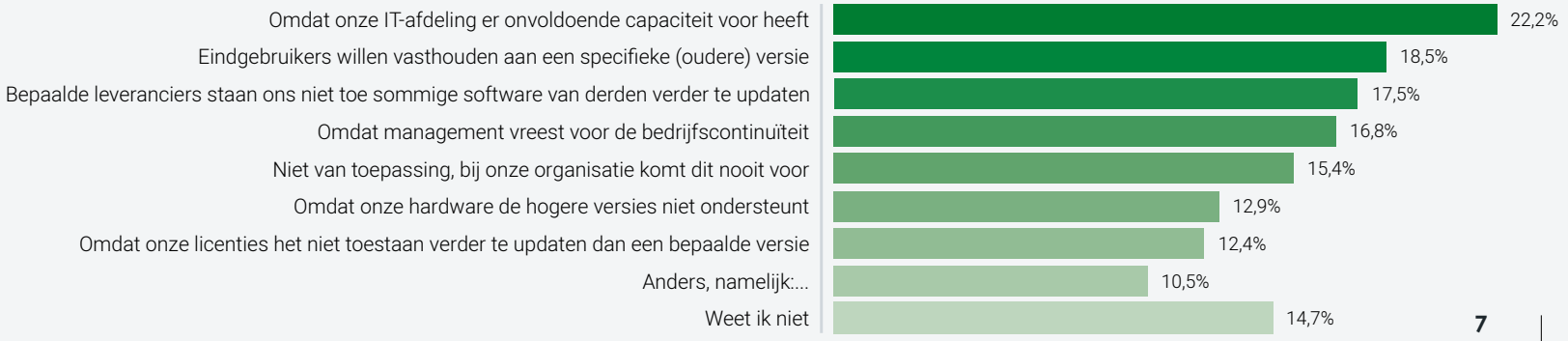
De onderzoeksresultaten geven uiteenlopende redenen aan om patches uit te stellen. Een opvallende maar zorgelijke reden om patching uit te stellen is capaciteitsgebrek. 22,2% geeft aan om deze reden soms geen patches door te voeren. Capaciteitsgebrek staat haaks op het besef dat security cruciaal is.

Volgens Guardiola zijn er heel weinig valide redenen voor uitstel. "Bijvoorbeeld, als software op te oude hardware draait, moet je verbeteringen doorvoeren in je lifecycle management. Hetzelfde geldt voor gebruikerswensen: gewenning is nooit een valide reden om op security in te binden."

Kwalitatieve resultaten tonen dat patching relatief vaak wordt uitgesteld om nieuwe updates eerst goed te testen. Dat is begrijpelijk, want patches kunnen onbedoelde verstoringen van de dienstverlening opleveren. Toch adviseert Guardiola om snel te patchen. "Het is mogelijk om applicaties geautomatiseerd te testen. Door het automatiseren van tests zou het installeren van securitypatches geen vertraging mogen oplopen."

In 2020 werd nog in 37,8% van de gevallen patching uit- of afgesteld omdat management vreesde voor de bedrijfscontinuïteit. Dat is nu met 16,7% fors lager. Guardiola: "De afgelopen jaren hebben ransomware-aanvallen aangetoond waar kwetsbaarheden toe kunnen leiden. Hierdoor zie ik dat organisaties een andere risicoafweging zijn gaan maken, en dat juich ik toe."

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



"Doorlopende scanning en testing van de security is nodig in het razendsnel veranderende IT-landschap."

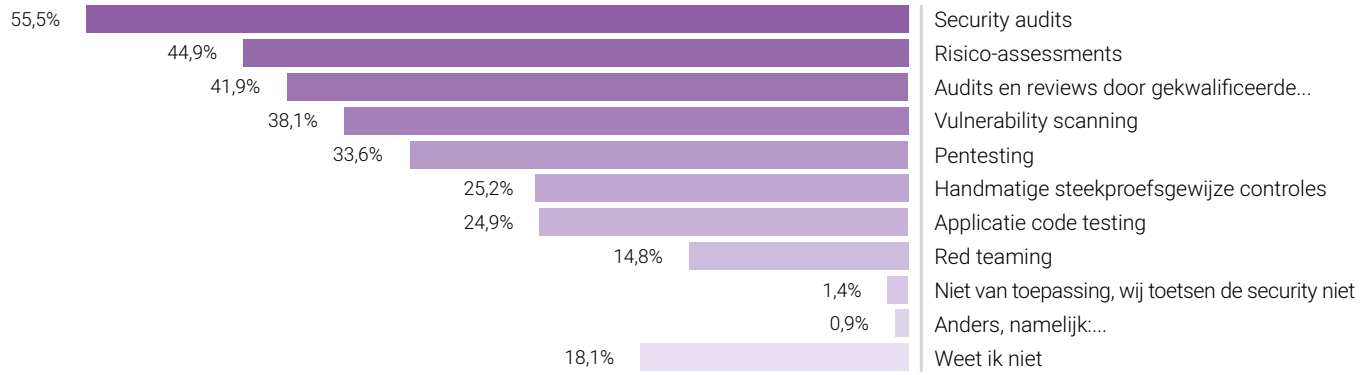
Security testing: verder kijken dan audits

In het onderzoek is ook gevraagd naar de testmethoden die organisaties inzetten om hun security te toetsen. Audits steken met kop en schouders tussen de antwoorden uit. 55,5% van de respondenten toetst hun security via audits en 41,9% laat dit doen door gekwalificeerde instanties. 44,9% zet risico-assessments in als toetsingsmethode.

Maar audits zijn niet waterdicht en tussen twee auditmomenten kan er ontzettend veel gebeuren. Het is daarom beter wanneer organisaties regelmatig hun security toetsen, zodat ze geen vals gevoel van veiligheid krijgen. Dat kan met handmatige steekproeven, zoals 25,2% aangeeft, maar ook met behulp van applicatie code testing (24,9%) en vulnerability scanning (38,1%). "Een audit kan een vinkje op een checklist zijn", aldus Guardiola. "Maar dat gaat voorbij aan het eigenlijke doel: zorgen dat je je securityzaken op orde hebt. Doorlopende scanning en testing van de security is nodig in het razendsnel veranderende IT-landschap."

Intensievere toetsingsmethoden zoals pentesting (33,6%) en red teaming (14,8%) worden minder vaak ingezet dan audits. "Ook een solide securitybasis moet doorlopend worden getoetst. Daarbij kun je niet alles standaardiseren of automatiseren", zegt Guardiola. "Tijdens pentesten en red teaming-exercities komen kwetsbaarheden aan het licht die je met andere methoden over het hoofd ziet. Onderschat dus nooit het belang van menselijk vernuft!"

Welke methoden gebruikt uw organisatie om de security te toetsen?



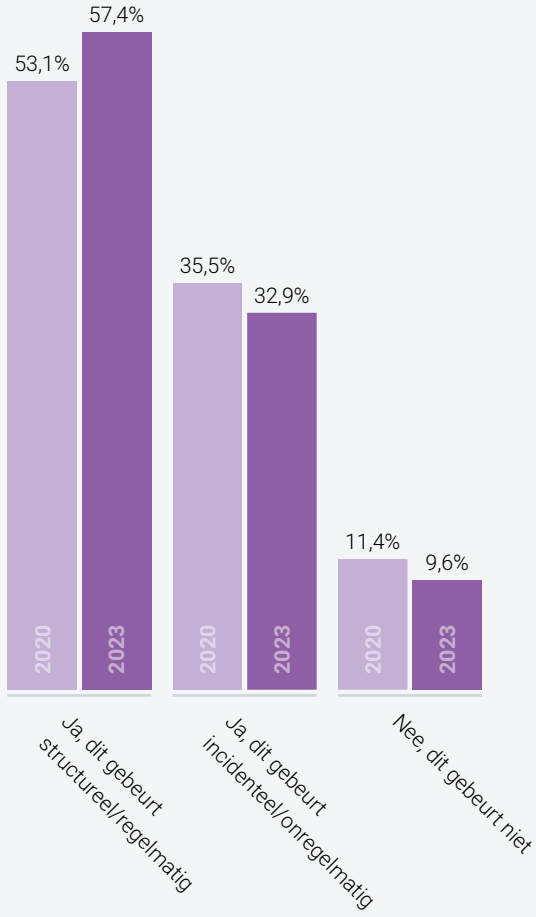
De menselijke factor

Hoewel securitytechnologie en audits redelijk breed worden ingezet, is er nog veel te verbeteren in de security awareness onder medewerkers. Bijna één op de tien organisaties (9,6%) traint en toetst het personeel helemaal niet. 57% doet dit structureel wel. Dit is amper meer dan in 2020, toen met 53,1% slechts de helft aangaf structureel te trainen en te toetsen.

Dat is verontrustend. Geen aandacht voor security awareness is vragen om problemen, omdat veel hacks slagen vanwege een menselijke fout. Gaten in de security awareness van medewerkers zijn juist waarom phishing-mails onverminderd populair zijn – omdat ze werken. Het advies van Guardiola is simpel: "Blijf organisatiebreed werken aan security awareness. Test niet alleen je systemen, maar ook je mensen."

> "Blijf organisatiebreed werken aan security awareness. Test niet alleen je systemen, maar ook je mensen."

Worden de medewerkers in uw organisatie getraind en getoetst op Security Awareness?



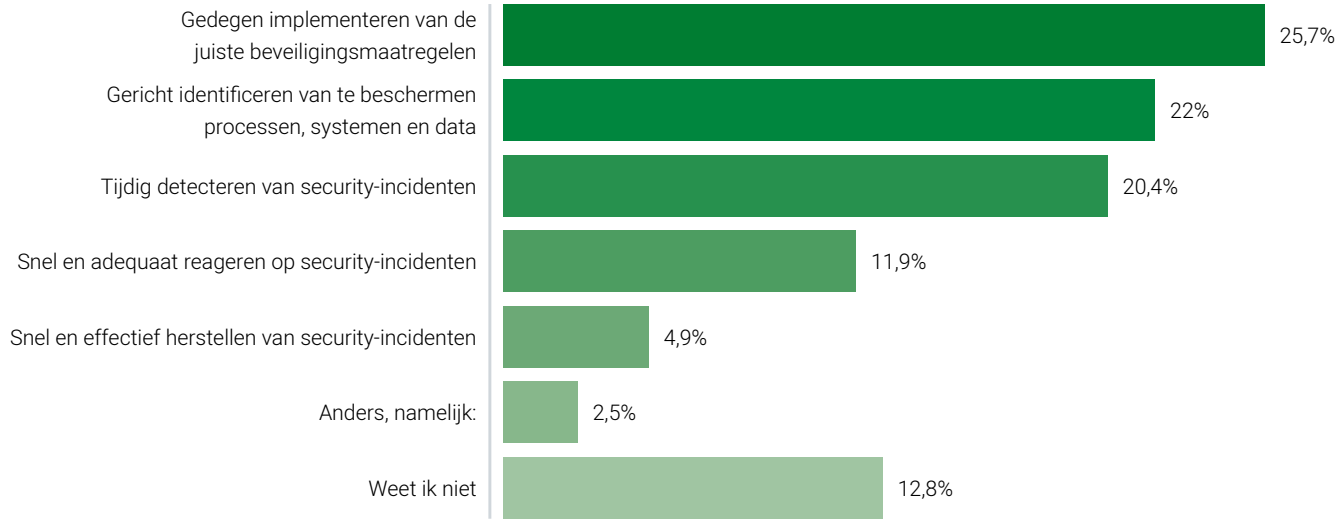
"Het is belangrijk dat je je gezicht laat zien bij developers."

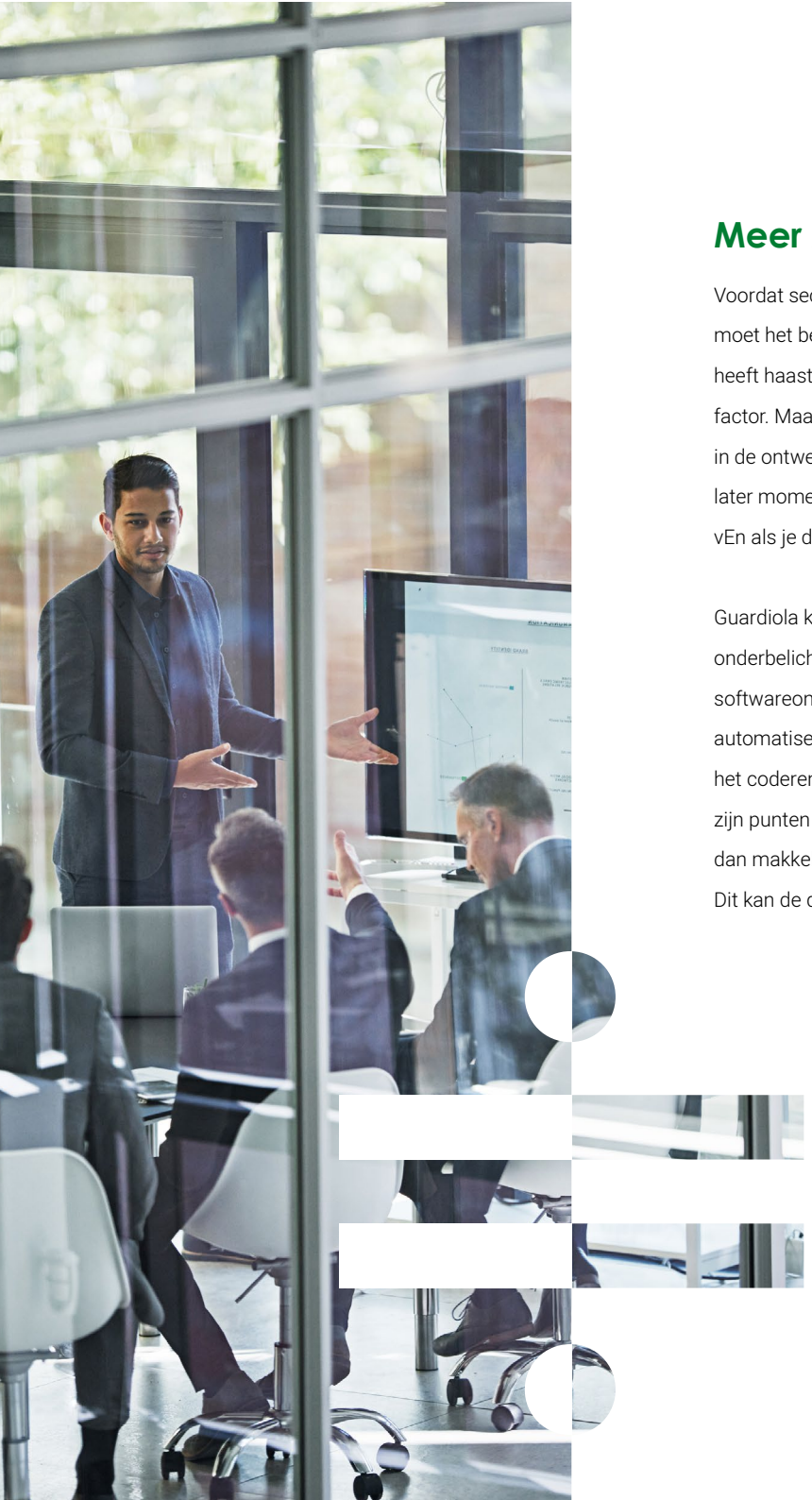
Veiligheid vanaf het begin

Hoewel de wereld zich beter bewust is van het belang van security, is dit dus nog lang niet zo goed in de organisatie gebakken als zou moeten. Niet alleen onder eindgebruikers, zoals in het vorige hoofdstuk genoemd, maar ook in het IT-ontwikkelproces. De resultaten tonen aan dat security niet altijd in een vroeg stadium wordt meegenomen – terwijl dat wel zou moeten.

Het helpt niet dat één op de vijf softwareontwikkelaars (19,3%) niet weet wat de grootste security-uitdagingen zijn binnen hun organisatie. Hierdoor kunnen zij (onbedoeld) deze uitdagingen juist verergeren. Volgens Guardiola zouden securitymedewerkers zichtbaarder moeten zijn in de organisatie om security top-of-mind te houden. "Het is belangrijk dat je je gezicht laat zien bij developers."

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





Meer zichtbaarheid voor security

Voordat security kan worden ingebakken in het ontwikkelproces, moet het belang gevoeld worden binnen de organisatie. “Iedereen heeft haast en security wordt al snel gezien als een vertragende factor. Maar wanneer je ervoor kiest security niet mee te nemen in de ontwerpfase van infrastructuur of applicaties, moet je op een later moment maatregelen gaan nemen om deze te beveiligen. vEn als je dan al niet te laat bent, kost het nóg meer tijd en geld.”

Guardiola kan zich goed voorstellen waarom security by design onderbelicht is. “Traditioneel kwamen IT’ers lang niet altijd met softwareontwikkeling in aanraking. Maar in het tijdperk van automatisering kom je daar niet meer onderuit: je bent al snel aan het coderen, al is het glue code om processen te verbinden. Ook dat zijn punten waar het mis kan gaan – door een scriptfoutje kun je dan makkelijk geautomatiseerd een foute configuratie doorvoeren. Dit kan de deur openzetten voor binnendringers.”

Tot slot is volgens Guardiola het beeld dat security vooral tijds- en arbeidsintensief is, niet meer van deze tijd. “Veel code testing kan worden geautomatiseerd”, zegt hij. “Door geautomatiseerde toetsingsmomenten in een DevSecOps-proces te bouwen, garandeer je een zekere mate van veiligheid.”

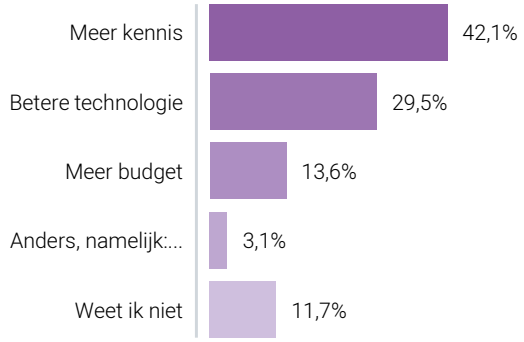
> “Door geautomatiseerde toetsingsmomenten in een DevSecOps-proces te bouwen, garandeer je een zekere mate van veiligheid.”

Cloud als antwoord op capaciteitsgebrek?

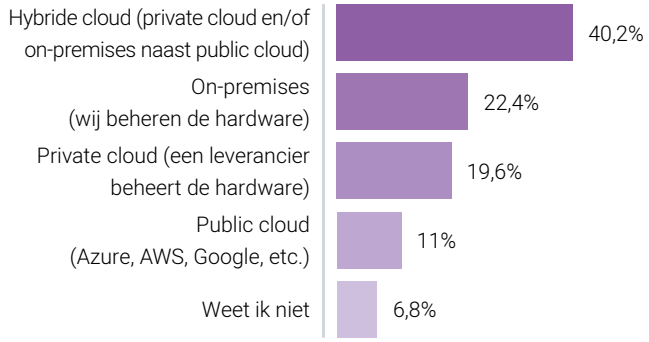
Capaciteitsgebrek loopt als een rode draad door de onderzoeksresultaten heen. Ruim één op de vijf (22,2%) van de respondenten geeft aan dat er te weinig capaciteit is om patching uit te voeren (zie grafiek blz. 7), vergeleken met 16% in 2020. Voor 42,1% is het binnenhalen van de benodigde kennis de topprioriteit om de organisatie ook in de toekomst veilig te houden. Of zoals kwalitatieve antwoorden het stellen: 'meer kennis', 'meer mensen', 'meer personeel'.

Legacy on-premises infrastructuren slokken veel IT-capaciteit op, omdat er veel handmatig werk aan te pas komt. Toch werkt nog 22,4% van de IT-professionals met dit soort omgevingen. Daarnaast werkt 40,2% met hybride cloud waar, vooral in het private deel, ook veel legacy kan voorkomen. Public en (geoutsourcete) private cloud-omgevingen bieden daarentegen veel betere mogelijkheden tot automatisering. En daarmee wordt broodnodige capaciteit vrijgespeeld.

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



Wat is de beste omschrijving van de IT-omgeving binnen uw organisatie?



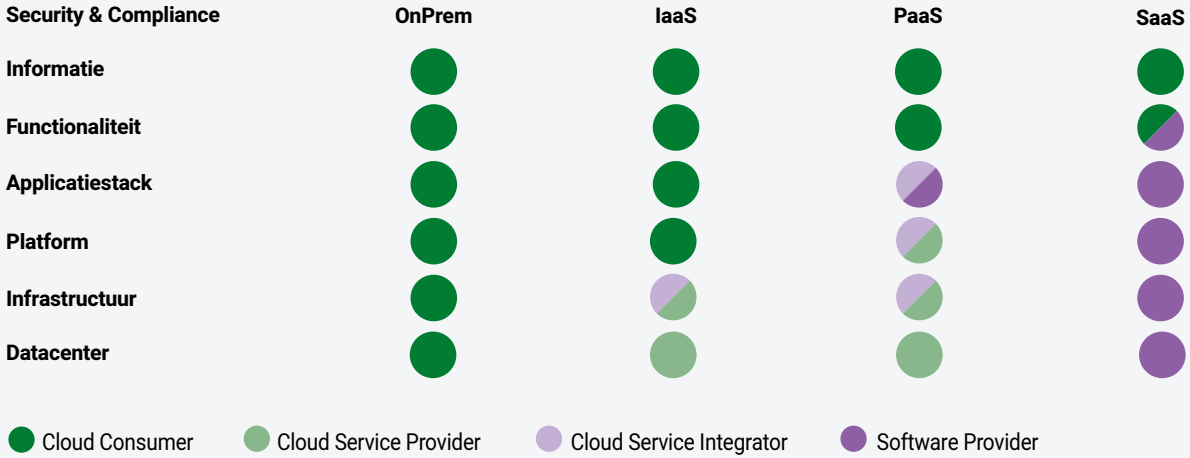
"Met onze ervaring zorgen we voor de meest private public cloud."

Met name in public cloud-omgevingen is er een 'snoepwinkel' aan kant-en-klare oplossingen beschikbaar. Mits je daar op de juiste manier mee om kunt gaan, kan dat aanbod aan tooling een organisatie helpen de IT-werkzaamheden significant te versnellen. Bovendien neemt het Shared Responsibility Model van de cloud enkele verantwoordelijkheden weg op securitygebied. De cloud provider is immers verantwoordelijk voor de security van zijn datacenters en basisinfrastructuur. Zo hoeft de eigen IT zich alleen te richten op patching en netwerkbeveiliging van de eigen data en applicaties.

"Ik ben een groot voorstander van cloud, maar besef wel dat hier specialistische kennis voor nodig is", zegt Guardiola. "Niet alleen om de kosten onder controle te houden, ook security moet je in de cloud vanaf het begin goed aanvliegen."

Daar komen andere vraagstukken bij kijken dan IT'ers gewend zijn in on-prem omgevingen. Het open karakter van public cloud, de 'snoepwinkel' waar je van alles aan en uit kan zetten, vergt een zorgvuldige balans tussen veiligheid en flexibiliteit. Guardiola: "We weten het als geen ander, dankzij jarenlange ervaring in het beveiligen van private, hybride en public cloud-omgevingen. En met die ervaring zorgen we voor de meest private public cloud."

Shared Responsibility Model



Conclusie: Blijf investeren

De meeste organisaties (31%) uit het onderzoek besteden 5-10% en 27% besteedt 10-15% van het IT-budget aan security. Voor bijna één op de vier respondenten zijn deze budgetten onvoldoende en 32,8% is hier onzeker over. Gelukkig verwacht 47,9% dat het budget toe zal nemen volgend jaar.

Budgetverhogingen komen niet als een verrassing, gezien de vele zorgen van IT-professionals over onder meer ransomware (45,6%), phishing (48,5%), datalekken door verlies van apparaten (35,7%), DDOS en externe hacks op (web)applicaties (beiden 28,8%).

Volgens 53,9% van de respondenten gaat het geld met name naar het verstevigen van de in-house securitycapaciteit. 39,5% wapent zich tegen dreigingen door (een deel van) hun security juist te outsourcen. Het is een cruciale keuze voor de meeste organisaties.

"Zeker als we zien dat ruim één op de vijf patches wordt uitgesteld vanwege capaciteitsgebrek, zou het voor iedere organisatie een prioriteit moeten zijn om de nodige kennis en mensen aan boord te krijgen," zegt Guardiola.

De schaarste van IT-talent stelt organisaties continu voor onmogelijke keuzes: focus op security, innovatie of onderhoud. Solvinity biedt een scala aan onder andere beveiligings- en compliancediensten. Wij verzorgen de security, het beheer en innovatie, zodat jouw experts zich kunnen richten op de eigenlijke kerntaken van de organisatie.

> "39,5% wapent zich tegen dreigingen door (een deel van) hun security juist te outsourcen. Het is een cruciale keuze voor de meeste organisaties."

Over welke cyberdreigingen maakt u zich het meest zorgen?

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. Of even wilt sparren over de actuele dreigingen en oplossingen om jouw organisatie veilig te houden.

Neem contact met ons op via
info@solvinity.com of 020 36 43 600

Solvinity
Secure Managed IT Services

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

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

Met secure managed IT services ondersteunt en adviseert Solvinity organisaties met hoge beveiligingseisen in hun digitale transformatie.

	Managed Cloud Outsourcing	Security & Compliance Lango Workspace	Service Integration 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, aanvullende diensten op het gebied van pentesting, red teaming en agile security.		
	Certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001 en PCI DSS. Als eerste Managed Service Provider in Nederland SOC 1 & 2 compliance rapporten voor de gehele beheeromgeving van niet alleen de private, maar ook de Azure cloud.		
	Solvinity levert aan de (rijks-)overheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, Translink (OV-chipkaart), ING en ONVZ.		
	350 medewerkers	2021: omzet 59 mln	Amsterdam, Assen Amersfoort, Den Bosch