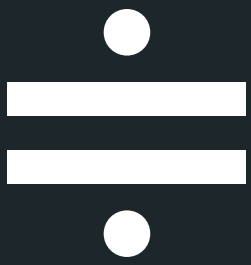
# SECURITY ONDERZOEK

**ONDERZOEKSRAPPORT** SECURITY AWARENESS 2020

Solvinity
Secure Managed IT Services



## Inhoud

# Solvinity Security Awareness Onderzoek

**88% van de Nederlandse IT-verantwoordelijken zegt de beveiliging van de eigen organisatie onder controle te hebben. 70% denkt prima zelfstandig weerstand te kunnen bieden aan cybercrime. Toch installeert 80% niet alle patches en updates en neemt nog niet de helft specifieke maatregelen om de eigen kwetsbaarheid te verkleinen. De kloof tussen de perceptie en de realiteit van de eigen veiligheid is groot…**

In juli 2020 hield PanelWizard in opdracht van Solvinity een onderzoek onder ruim 500 Nederlandse IT-verantwoordelijken bij bedrijven met 200 medewerkers en meer, om in beeld te brengen hoe Nederlandse organisaties aankijken tegen hun eigen digitale weerbaarheid.

Het onderzoek volgt op een golf securityincidenten, van het stilleggen van thuiswerkservers vanwege onopgeloste kwetsbaarheden, tot grootschalige ransomware-aanvallen en een explosieve stijging van het aantal cybercrime-delicten, dat dit jaar voor het eerst het aantal woninginbraken overstijgt. Ondanks deze alarmerende ontwikkelingen gaf ruim 88% van de Nederlandse IT-verantwoordelijken een positief antwoord op de vraag of de eigen organisatie de beveiliging van de IT-omgeving onder controle heeft. 26% is er zelfs zeker van en 62,4% heeft in elk geval het gevoel van wel. De vervolgvragen in het onderzoek maken duidelijk dat organisaties vaak een veel te rooskleurig beeld hebben van de eigen weerbaarheid.

*Heeft u het idee dat uw organisatie de beveiliging van de IT-omgeving onder controle heeft?*

# Gebrekkig inzicht maakt organisaties kwetsbaar

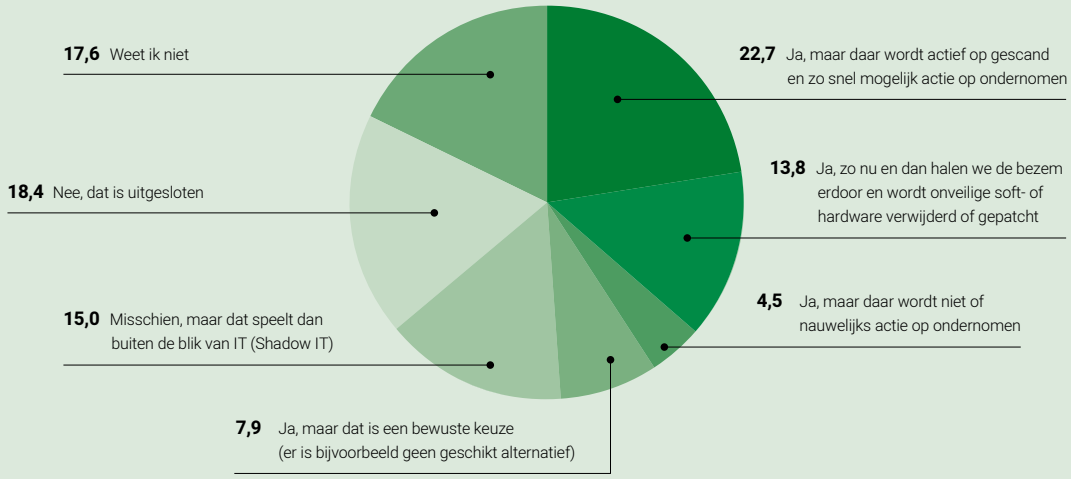
Op de vraag of binnen de organisatie software, hardware of diensten worden gebruikt waarvan de respondenten weten dat ze niet veilig zijn, antwoordt 18,4% van de IT-verantwoordelijken resoluut dat dat is uitgesloten. Marc Guardiola, CISO bij Solvinity, noemt dat onwaarschijnlijk: "Zonder draconische maatregelen is het vrijwel onmogelijk te voorkomen dat zo nu en dan apparaten op het netwerk worden aangesloten, of software wordt gebruikt, of online diensten worden aangeklikt, die niet door IT zijn goedgekeurd."

Daarom is het verstandig de infrastructuur actief te scannen, zodat direct passende actie kan worden ondernomen als dergelijke 'Shadow IT' opduikt in het netwerk, vindt Guardiola.

Maar dat doet slechts 23% van de respondenten. 14% haalt hooguit zo nu en dan de bezem door het netwerk. "De overige 63% heeft geen idee of doet in feite of zijn neus bloedt."

*"Slechts 23% scant de infrastructuur actief op ongewenste hardware, software of diensten"*

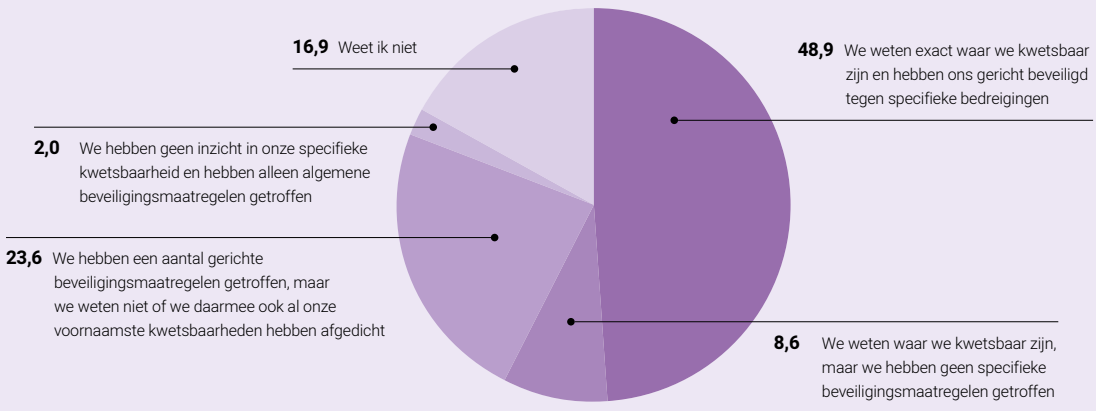
*Worden binnen uw organisatie software, hardware of diensten gebruikt waarvan u weet dat deze niet veilig zijn?*



"Alles begint met inzicht", meent Guardiola. "Als je niet weet waar je kwetsbaar bent, kun je jezelf nooit goed verdedigen." Terwijl eigenlijk iedere organisatie op de hoogte zou moeten zijn van de risico's die ze lopen en hoe die het best worden afgedekt, geeft slechts 49% van de respondenten aan exact te weten waar hun organisatie kwetsbaar is en daar ook gerichte maatregelen op te nemen. De overige 51% geeft toe niet goed op de hoogte te zijn van de eigen kwetsbaarheid, of daar in elk geval geen gerichte maatregelen op te hebben genomen. "Inzicht in hoe je IT-infrastructuur in elkaar zit en wat zich daar afspeelt is de enige manier om een realistische inschatting te kunnen maken van de mogelijke risico's die een organisatie loopt."

*"Slechts 49% weet exact waar hun organisatie kwetsbaar is en heeft daar gerichte maatregelen op genomen"*

*In hoeverre heeft uw organisatie inzicht in de kwetsbaarheid van de eigen IT-infrastructuur?*



# Updates en patches worden soms helemaal niet geïnstalleerd

Inzicht in de kwetsbaarheid van de organisatie is cruciaal om weloverwogen beslissingen te kunnen nemen over maatregelen die essentieel zijn voor de veiligheid van de organisatie. Een voorbeeld is de omgang met updates en patches. IT-leveranciers kondigen geregeld maatregelen aan die nieuw ontdekte kwetsbaarheden in hun producten moeten verhelpen. Dat betekent ook dat op dat moment algemeen bekend is dat die kwetsbaarheden bestaan. Vanaf dat moment is er een redelijke kans dat kwaadwillenden daar misbruik van proberen te maken. Begin 2020 was onduidelijkheid over de installatie van patches en updates de belangrijkste reden waarom een groot aantal Nederlandse bedrijven, overheden en instellingen hun thuiswerkoplossingen voor alle zekerheid offline moesten halen.

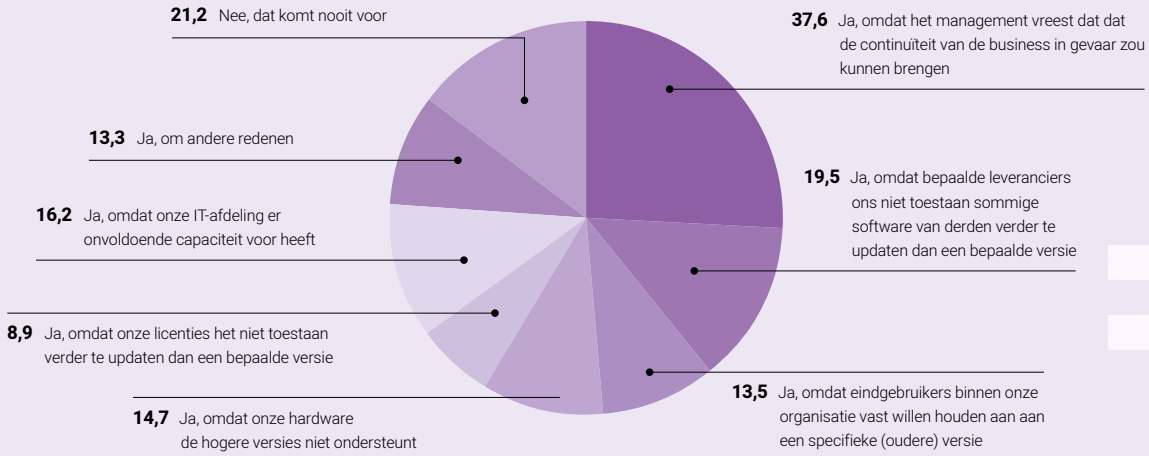
Slechts 49% van de respondenten geeft aan patches en updates die de leverancier beschikbaar stelt binnen enkele dagen te installeren. 24% heeft daar weken voor nodig en 8% wacht zelfs maanden of langer. Sterker: bijna 80% geeft aan dat bepaalde patches en updates soms helemaal niet geïnstalleerd worden. De voornaamste reden die daarvoor in het onderzoek wordt genoemd (38%) is dat het management patches en updates tegenhoudt, omdat gevreesd wordt dat het de business in gevaar zou kunnen brengen. “Daar kunnen legitieme redenen voor zijn”, denkt Guardiola. “Ernstiger vind ik dat bij 13% van de organisaties eindgebruikers zo’n update tegenhouden omdat ze geen verandering willen. Of nog erger: dat 16,2% aangeeft dat de IT-afdeling onvoldoende capaciteit heeft om zich met patches en updates bezig te houden.”

Soms is de risicoafweging begrijpelijk, zegt Guardiola. “Patches en updates installeren is niet zonder gevaar. Stel dat je bijvoorbeeld zware operationele technologie hebt draaien, waarbij storingen direct miljoenen kunnen kosten, terwijl de potentiële schade van exploitatie van zo’n kwetsbaarheid heel klein is: dan kan ik me voorstellen dat een bedrijf zo’n update niet direct wil doorvoeren, of op zijn minst eerst grondig wil testen.”

De andere kant van het verhaal is dat de gebruikte IT soms zelf de veiligheid in de weg zit. 20% van de respondenten geeft aan dat bepaalde leveranciers hun gebruikers niet toestaan software van derden verder te updaten dan een bepaalde versie. “Doen ze dat toch, dan vervalt bijvoorbeeld de ondersteuning”, vertelt Guardiola. 14,7% geeft aan dat bepaalde hardware niet overweg kan met hogere softwareversies en 9% geeft aan dat hun licenties hen niet toestaan bepaalde software verder te updaten. “Op zo’n moment word je eigenlijk in gijzeling genomen door je eigen IT”, stelt Guardiola.

*“Bijna 80% installeert niet alle patches en updates”*

*Wordt binnen uw organisatie (weleens) besloten de installatie van updates en patches uit- of af te stellen?*




**NOTE:** Bij deze vraag waren meerdere antwoorden mogelijk

## Weloverwogen maatregelen op basis van inzicht en ervaring

In het onderzoek werd ook gekeken naar de invloed van IT outsourcing. Veel IT-afdelingen **kampen met een hoge werkdruk**. In combinatie met de toenemende complexiteit van IT en het stijgende aantal securityincidenten, besluiten steeds meer organisaties het beheer van hun IT-omgeving uit te besteden. De coronacrisis, en de noodzaak om ook onder dergelijke omstandigheden de bedrijfscontinuïteit te kunnen garanderen, lijkt deze trend te versterken. Voor de respondenten in dit onderzoek zijn bedrijfscontinuïteit en het feit dat IT niet tot de kerntaken van de organisatie behoort, de voornaamste afwegingen om met een Managed Service Provider in zee te gaan.

Ook vanuit securityperspectief is dat vaak verstandig, vindt Guardiola. "Je vindt nu eenmaal meer mensen met verstand van zaken bij een organisatie die zich echt specialiseert in het veilig beschikbaar houden van IT." Solvinity klanten hebben bijvoorbeeld minder moeite om hun digitale werkomgeving eenvoudig en overal te benaderen dan andere organisaties (66% tegen 55%). Maar uit het onderzoek komen ook andere belangrijke verschillen naar voren tussen organisaties die hun IT zelf beheren en organisaties die hun IT (deels) uitbesteden.

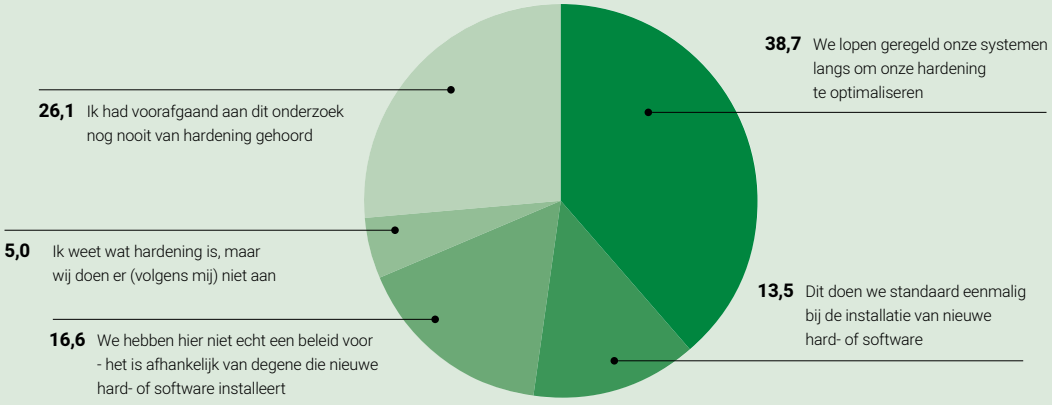
# Nog nooit van hardening gehoord?

Respondenten werd gevraagd hoe hun organisatie omgaat met hardening. Hardening is het proces waarbij de instellingen van hard- en software worden gecontroleerd op veiligheid. Om misbruik te voorkomen worden ongebruikte poorten en services bijvoorbeeld zo veel mogelijk gesloten. "26% van de respondenten had vóór ons onderzoek nog nooit van hardening gehoord," zegt Guardiola, "en dat gold vooral voor respondenten die niet samenwerken met een Managed Service Provider."

*"26% heeft nog nooit van hardening gehoord"*

Tegelijkertijd blijkt uit de antwoorden ook dat niet alle Managed Service Providers gelijk zijn. "Hardening is arbeidsintensief", zegt Guardiola. "In tegenstelling tot bij veel bedrijven die security zelf proberen te doen, zie je dat de meeste MSP's wel een vorm van hardening toepassen." Uit het onderzoek blijkt echter ook dat relatief veel service providers hardening vooral invullen als eenmalige controle bij de installatie van nieuwe hard- of software. "Veel outsourcers hebben geen vast beleid voor hardening en laten het aan de betrokken specialisten om te bepalen hoe en wanneer ze het toepassen. Dat ligt bij Solvinity duidelijk anders", vertelt Guardiola. "Continuous Hardening is bij ons standaard: onze mensen controleren bij elke aanpassing in het netwerk of deze wel zo veilig mogelijk wordt doorgevoerd."

*Welke van onderstaande stellingen beschrijft het best de manier waarop uw organisatie omgaat met hardening?*

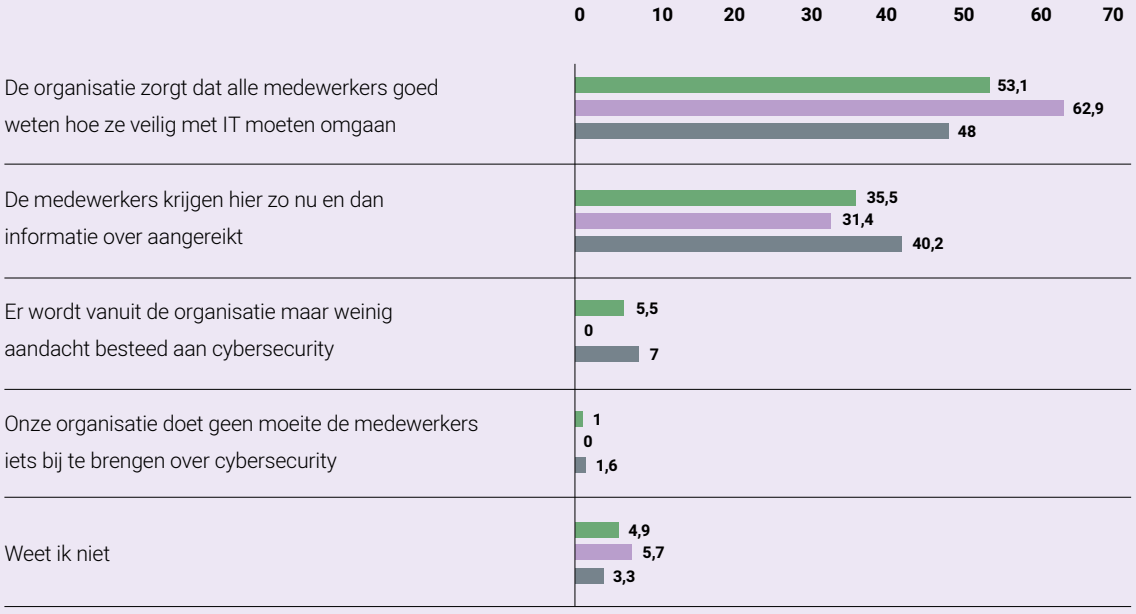


# Meer aandacht voor voorlichting

Een ander aspect waar verschillen zichtbaar zijn tussen MSP's, is de mate waarin medewerkers worden voorgelicht over cybersecurity. "Gemiddeld zegt 53,1% van de respondenten dat al hun medewerkers goed weten hoe ze veilig met IT moeten omgaan", zegt Guardiola. Bij Solvinity klanten geeft juist 63% aan dat iedereen goed is voorgelicht, terwijl dat getal bij de overige MSP's op 48% ligt. "Zo zie je maar dat het wel degelijk uitmaakt hoeveel aandacht een Managed Service Provider heeft voor cybersecurity. Kennelijk is bij andere MSP's soms toch meer afstand ontstaan tussen business en IT", denkt Guardiola.

*"53% zorgt dat al hun medewerkers weten hoe ze veilig met IT moeten omgaan"*

*In welke mate wordt er binnen uw organisatie richting de medewerkers aandacht besteed aan cybersecurity?*



## Conclusie:

## Secure Managed Services houden de risico's beperkt

Cybersecurity is niet eenvoudig, benadrukt Guardiola. "Er is maar één zekerheid en dat is dat 100% veiligheid niet bestaat." Bovendien zijn de middelen, die een organisatie voor cybersecurity ter beschikking staan, niet bepaald oneindig. "Dat betekent dat je voortdurend moet afwegen wat de meest effectieve maatregelen zijn om de risico's voor jouw specifieke organisatie zo klein mogelijk te houden." Helaas blijkt uit dit onderzoek dat veel organisaties maar beperkt inzicht hebben in hun eigen kwetsbaarheid. De neiging om de eigen weerbaarheid te overschatten is daardoor groot.

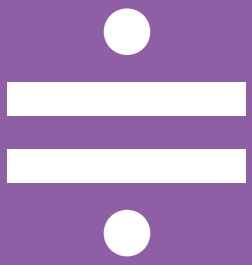
Om een realistisch beeld te krijgen van de weerbaarheid van de organisatie, is het nodig tijd en middelen vrij te maken om gedegen inzicht te krijgen in de hele IT-infrastructuur. "Vervolgens heb je mensen nodig die de kennis en expertise hebben om, samen met de business, een inschatting te maken van de mogelijke risico's en de meest effectieve middelen om die risico's af te dekken", zegt Guardiola. Voor organisaties waar de IT-afdeling toch al onderbezet en overbelast is, blijkt dat geen realistische oplossing. De beste manier om ervoor te zorgen dat de organisatie tegen de meest voorkomende vormen van cybercriminaliteit beschermd is, is een beroep te doen op een ervaren Secure Managed Service Provider.

# Over Solvinity

Solvinity levert Secure Managed IT Services in de public, private en hybrid cloud voor organisaties met hoge beveiligings-eisen. De diensten van Solvinity bestaan onder meer uit innovatieve cloud solutions, outsourcing, managed hosting en werkplekoplossingen zoals Lango Workspace. Voor organisaties die zelf software ontwikkelen biedt Solvinity oplossingen zoals Integrated Delivery en 'Stretched' DevOps. De organisatie onderscheidt zich met zeer hoge standaarden voor cyber-security en certificeringen volgens nationale en internationale normen als ISO 27001, ISO 14001, ISO 9001, SOC 1, SOC 2 en NEN 7510. Solvinity levert diensten aan onder andere de (rijks-)overheid, waaronder het ministerie van Justitie en Veiligheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, waaronder Trans Link Systems (OV-chipkaart), TNO, ING, Ahold en ONVZ. Solvinity heeft ruim 250 medewerkers, verspreid over vier vestigingen in Amsterdam, Assen, Amersfoort en Den Bosch. In 2019 haalde het bedrijf een jaaromzet van 47,8 miljoen euro. Kijk voor meer informatie op **www.solvinity.com**, of volg Solvinity op **Twitter** en **LinkedIn**.

**Meer weten over Solvinity?**

Neem contact met ons op! Bel **+31 (0)20 36 43 600**
of mail ons op **info@solvinity.com**



Solvinity®

Secure Managed IT Services

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

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