Orange
Cyberdefense

Security today
Onderzoek onder Nederlandse IT-beslissers

Inhoudsopgave

Intro

Wanen we ons veiliger dan dat we werkelijk zijn?

IT-beslissers worden dagelijks op de proef gesteld om de kwaliteit van IT hoog te houden. De recente cyberaanvallen tonen aan dat Nederlandse organisaties kwetsbaar zijn. Zowel de publieke instellingen als bedrijven zijn slachtoffer. U kunt blijven doen alsof er niks aan de hand is en blijven beweren dat uw organisatie niet interessant is voor cybercriminelen, maar inmiddels weten we dat iedere organisatie kwetsbaar is.

IT staat voor een belangrijke uitdaging. Naast de toename van het aantal cyberaanvallen dient IT het thuiswerken vanwege de Covid-19 maatregelen optimaal te faciliteren. Niet alleen dienen ze de IT-infrastructuur goed ingericht te hebben om thuiswerken mogelijk te maken, maar ook moet de technologie goed beveiligd zijn tegen cyberaanvallen. Daarnaast is het inlichten van de medewerkers over de risico's hierbij van groot belang. Weten zij bijvoorbeeld wat zij kunnen bijdragen om cyberaanvallen te voorkomen? Hier ligt voor de IT-beslissers nog altijd een flinke uitdaging.

Veel cybercrime is nog onzichtbaar, wat resulteert in minder noodzaak om hierin te investeren. De cybercrime van tegenwoordig is echter een van de grootste bedrijfsrisico's. Aan sommige aanvallen gaan maanden van voorbereidingen vooraf. Om de informatie van uw organisatie en medewerkers veilig te stellen moeten we cyberdreigingen heel serieus nemen.

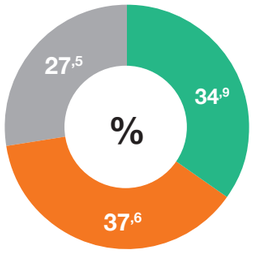
Om die reden hebben we onderzoek uitgevoerd onder IT-beslissers om inzichtelijk te maken hoe vaak organisaties te maken hebben gehad met cyberaanvallen, hoe men denkt hiermee om te moeten gaan en welke aanpassingen organisaties hebben getroffen met alle veranderingen rondom Covid-19. Met dit rapport geven we invulling aan de cybersecurity urgentie en komen wij met handreikingen om als organisatie digitaal weerbaarder te worden. Het mag niet zo zijn dat de business niet vooruit kan omdat cyberdreigingen voor obstakels zorgen.

Hoofdstuk 1

Veelvoor-komende cybercrime

Als het gaat om cybercrime is voorkomen beter dan genezen. U kunt cyberaanvallen beter tegenhouden, dan het lek repareren en uw data mogelijkerwijs op straat terugvinden. Organisaties die het er op gokken de dans te ontspringen, komen bedrogen uit. Maar hoe zorgt u er nu eigenlijk voor dat u voorbereid bent om incidenten het hoofd te bieden en de schade te beperken mocht uw organisatie toch slachtoffer worden van een hack of datalek?

Het is mogelijk uw organisatie te verzekeren tegen de gevolgen van hacking, verloren data en andere vormen van cybercriminaliteit. Hiermee verzekert u uw organisatie ervan de dat de impact minder groot is voor de dagelijkse business. Ervaren experts helpen u om databases en websites te repareren, belanghebbenden te informeren en juridische kosten te beperken. Iets meer dan een derde (35%) van de ondervraagden heeft zo'n verzekering, 38 procent geeft aan geen verzekering te hebben en bij de overige 28 procent is het onbekend. Maar met crime hebben ze zeker wel te maken.



Mijn organisatie is verzekerd tegen schade door cybercrime-aanvallen.

- Ja, geldt wel voor mij
- Nee, geldt niet voor mij
- Weet niet/geen mening

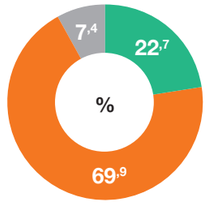
1.1 Vormen cybercrime

De uitbraak van de coronacrisis biedt cybercriminelen nieuwe mogelijkheden. Dat cybercrime steeds meer voorkomt, was al bekend, maar door de crisis wordt het organisaties niet makkelijker gemaakt en staan cybercriminelen continu in de aanval. De verplichting om thuis te werken kwam onverwacht en hierdoor waren computers en netwerken bijvoorbeeld nog niet goed beveiligd. Ook vindt er nu meer communicatie digitaal plaats en wordt online meer ontwikkeld. Het aantal mobiele devices en dus ook het aantal toegangspunten is snel gegroeid.

Om beter voorbereid te zijn is het goed om te weten welke vormen van cybercrime er bestaan en waar organisaties nu veelal mee te maken hebben. In ons onderzoek hebben we de respondenten vier vormen voorgelegd en hebben we hen de vraag gesteld of ze hier weleens slachtoffer van zijn geweest (zie Tabel 1). Malware is hierbij de meest voorkomende cybercrime; bijna een derde van de organisaties geeft aan hier weleens slachtoffer van te zijn geweest, 24 procent is slachtoffer geweest van een hack (illegale inbraak in computers/netwerken), 22 procent van ransomware en 21 procent van een DDoS-aanval.

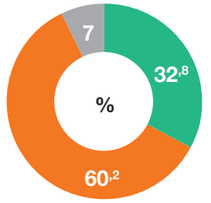
Tabel 1

- Ja, geldt wel voor mij
- Nee, geldt niet voor mij
- Weet niet/geen mening

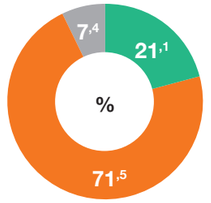


Mijn organisatie is weleens slachtoffer geweest van ransomware/gijzelsoftware.*

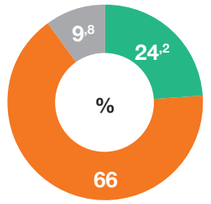
* Mailware die een computer en/of gegevens die erop staan blokkeert en vervolgs de gebruiker geld vraagt om de compter/gegevens te bevrijden.



Mijn organisatie is weleens slachtoffer geweest van andere mailware.



Mijn organisatie is weleens slachtoffer geweest van een DDos-aanval.

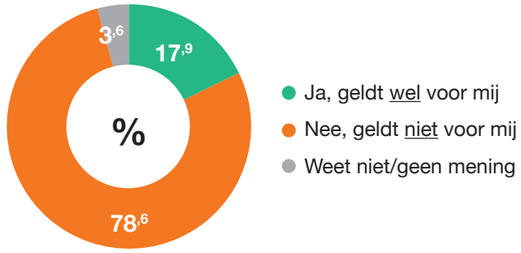


Mijn organisatie is weleens slachtoffer geweest van een hack (illegale inbraak in computers/netwerken).

1.2 Ransomware

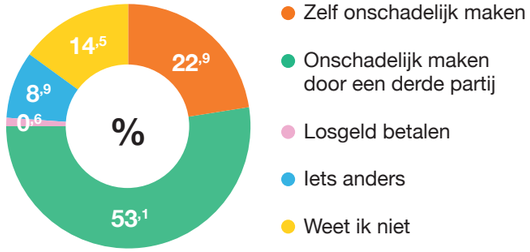
Mocht u slachtoffer worden van ransomware, hoe gaat u er dan mee om? De meningen van organisaties die al eens slachtoffer waren, zijn heel anders dan degene die het nog nooit meemaakten. Van degenen die slachtoffer zijn geweest, heeft 19 procent weleens betaald aan de maker. Onder organisaties die nog nooit slachtoffer zijn geweest, heerst meer bravoure. Slechts 1 procent denkt over te gaan tot betaling aan de maker. 23 procent gaat zelf proberen de ransomware onschadelijk te maken en meer dan de helft (53%) zou dat aan een externe partij uitbesteden. 9 procent doet iets heel anders: “we laten het gewoon gebeuren en zetten daarna een recente back-up terug” of “we lichten de politie in”.

U heeft aangegeven dat uw organisatie weleens slachtoffer is geweest van ransomware/ gijzelsoftware. Heeft uw organisatie weleens losgeld betaald aan de maker(s) van de ransomware/ gijzelsoftware?



Deze vraag is alleen gesteld aan degenen die aan hebben gegeven dat hun organisatie slachtoffer is geweest van ransomware.

Stel dat uw organisatie slachtoffer wordt van ransomware/gijzelsoftware, wat zou uw organisatie doen om weer toegang te krijgen tot de geblokkeerde computers/gegevens?



Deze vraag is alleen gesteld aan degenen die aan hebben gegeven dat hun organisatie geen slachtoffer is geweest van ransomware.

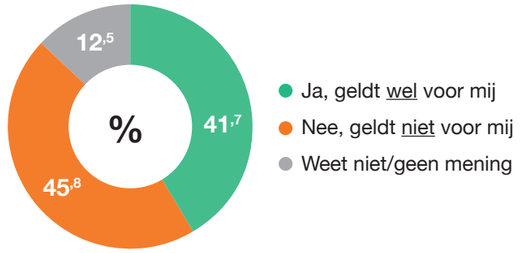
1.3 Datalek

Uit ons onderzoek blijkt dat ruim vier op de vijf (82%) respondenten in de afgelopen vier jaar te maken heeft gehad met een datalek. Dit is een schrikbarend hoog percentage als we ons bedenken dat de hoeveelheid aanvallen per jaar alleen maar toenemen. We spreken van een datalek of privacylek als persoonsgegevens in handen vallen van derden die geen toegang tot de gegevens zouden mogen hebben. Ook is er sprake van een datalek wanneer persoonsgegevens verloren zijn geraakt en er geen back-up is. Een datalek is het gevolg van een beveiligingsprobleem of menselijke fout en deels te voorkomen.

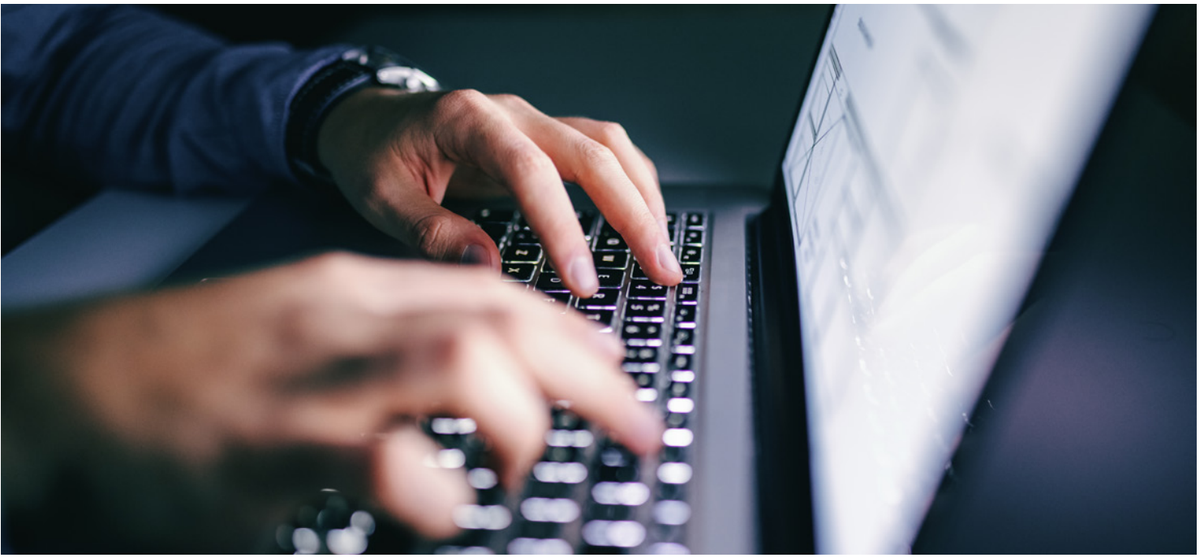
Van alle organisaties die te maken hebben gehad met een datalek geeft bijna de helft aan (42%) het intern te hebben opgelost, zonder dit te melden bij de Autoriteit Persoonsgegevens. En 13 procent weet niet of het gemeld is. Sommige datalekken zijn zo klein dat dit voor (bijna) geen schade zorgt. Andere datalekken daarentegen, hebben soms grote impact op veel mensen. In sommige gevallen moeten de betrokkenen van een datalek op de hoogte worden gesteld.

De Algemene verordening gegevensbescherming (AVG) stelt zeer strenge eisen aan de registratie van datalekken. Alle datalekken moeten worden gemeld binnen 72 uur na ontdekking. Meldt u de datalek niet? Dan mag de Autoriteit Persoonsgegevens boetes opleggen die in het ergste geval kunnen oplopen tot € 20 miljoen of 4 procent van de jaarlijkse wereldwijde omzet per overtreding.

U heeft aangegeven dat uw organisatie in de afgelopen 4 jaar weleens te maken heeft gehad met een datalek. Heeft uw organisatie in de afgelopen 4 jaar weleens een datalek intern opgelost, zonder het te melden bij Autoriteit persoonsgegevens?



Deze vraag is alleen gesteld aan degenen die aan hebben gegeven dat hun organisatie in de afgelopen 4 jaar weleens te maken heeft gehad met een datalek.



Hoofdstuk 2

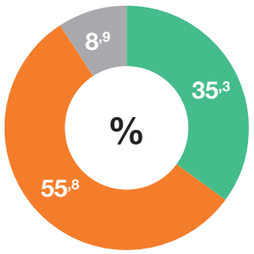
Het belang van security in de organisatie

Security-experts roepen organisaties op om cybersecurity toe te voegen aan de bedrijfsstrategie. De risico's zijn immers enorm: processen plat, data op straat, imagoschade, et cetera. Voor iedere organisatie is het essentieel dat de primaire bedrijfsprocessen onaangetast en operationeel blijven. Door cybersecurity te integreren met de bedrijfsstrategie kan het de organisatie veel geld en tijd besparen en imago-schade beperken.

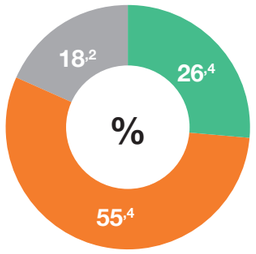
Het belang dat Nederlandse organisaties aan security toekennen is wisselend. Aan de ene kant is het niet de hoogste prioriteit. Zo zegt 35 procent dat het (her)inrichten van werkplekken – zowel thuis als op kantoor – bij zijn organisatie meer prioriteit heeft (gehad) dan cybersecurity. En bij ruim een kwart (26%) van de organisaties is het nakomen van wet- en regelgeving belangrijker dan security zelf.

En aan de andere kant zegt 43 procent dat zijn organisatie de komende tijd een groter gedeelte van het IT-budget gaat gebruiken om de cybersecurity te verbeteren. Door Covid-19 stonden overal de budgetten onder druk. Toch heeft 78 procent niet in het IT-budget hoeven snijden; 'slechts' 19 procent van de organisaties zag zich daartoe genoodzaakt. Opmerkelijk is dat 36 procent – en dat is best veel – van de IT-beslissers aangeeft zelf niet volledig op de hoogte te zijn van eventuele veiligheidsrisico's als hij nieuwe apps/programma's op het bedrijfsnetwerk installeert. Gelukkig is een grotere groep van 55 procent dat wel.

● Ja, geldt wel voor mij ● Nee, geldt niet voor mij ● Weet niet/geen mening



Het (her)inrichten van werkplekken (zowel thuis als op kantoor) heeft bij mijn organisatie meer prioriteit (gehad) dan cybersecurity.



Binnen mijn organisatie wordt er meer aandacht besteedt aan het nakomen van wet- en regelgeving op het gebied van cybersecurity dan aan cybersecurity zelf.

2.1 Bewustzijn

Uit onderzoek blijkt dus dat bijna de helft van de organisaties het IT-budget gaat gebruiken om cybersecurity te verbeteren, maar ook dat cybersecurity nog niet de hoogste prioriteit heeft. Maar voordat u begint met het verbeteren van de cybersecurity dient u allereerst te weten waarin u moet verbeteren. Vanuit dit perspectief kunt u gericht aan de gang gaan. Het gaat niet altijd specifiek om de beveiliging van de technologie zoals netwerken, clouddiensten en websites, maar ook om de verbetering van het bewustzijn van de medewerkers en van uw klanten.

2.2 Vertrouwen klant

De gevolgen van een cyberaanval zijn groot. Een aanval kan uw volledige organisatie platleggen en tel daar de financiële schade, een deuk in uw imago en extra tijd en kosten om alles weer op orde te krijgen hierbij op. Dit maakt het nog eens extra belangrijk om veel aandacht te geven aan beveiliging tegen cybercrime. Nu het onderwerp steeds vaker in de media verschijnt, kan het uiteindelijk zelfs effect hebben op de keuze van de klant.

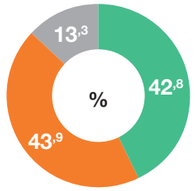
Zonder goede beveiliging brengt u niet alleen bedrijfsgegevens in gevaar, maar ook die van de klant. Sinds mei 2018 is de AVG van kracht. Met de ingang van deze wet is de bescherming van persoonsgegevens, waaronder die van uw klanten, nog belangrijker. Een overtreding van de privacywet kan een boete tot gevolg hebben. Het is dus erg belangrijk om goed op de hoogte te zijn hoe u alle bedrijfsinformatie veilig stelt en daarmee dus een boete weet te voorkomen.

2.3 Medewerkers

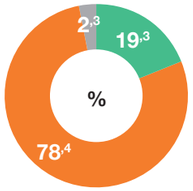
Een van de eerste dingen die u kunt doen om de veiligheid te verbeteren is de awareness rondom cybersecurity vergroten. Maar dit is lastig, wanneer er binnen organisaties weinig bewustzijn is over de risico's en gevolgen van cybercrime. Begin bij het scherp houden van uw werknemers, bijvoorbeeld door voorbeelden te laten zien hoe je data-encryptie toepast, maar ook hoe phishing e-mails eruit zien.

Uit ons onderzoek is gebleken dat 51 procent van de ondervraagde IT-beslissers weet dat werknemers van hun organisatie weleens gegevens versturen zonder data-encryptie toe te passen. En 38 procent weet dat werknemers weleens apps op hun werktelefoon geïnstalleerd hebben waardoor de kans op datalekken toenam. Met het gedrag van werknemers gaat het dus nog niet altijd goed. De respondenten wijten dat veelal aan bewustzijn. Bijna de helft (44%) vindt dat werknemers te weinig bewustzijn hebben als het gaat om het veilig omgaan met bedrijfsdata of data van klanten. Logisch dus dat 56 procent van de organisaties op dit moment bezig is met bewustzijn creëren rondom cybersecurity bij de werknemers.

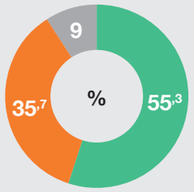
● Ja, geldt wel voor mij ● Nee, geldt niet voor mij ● Weet niet/geen mening



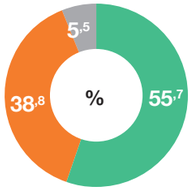
Mijn organisatie gaat de komende tijd een groter gedeelte van het IT-budget gebruiken om de cybersecurity te updaten.



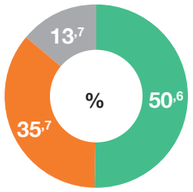
Mijn organisatie heeft in het IT-budget moeten snijden vanwege de coronacrisis.



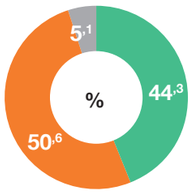
Ik ben volledig op de hoogte wat de eventuele veiligheidsrisico's zijn als ik nieuwe apps/prgamma's op het bedrijfsnetwerk installeer.



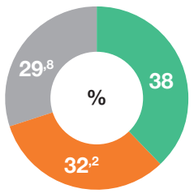
Mijn organisatie is op dit moment bezig met bewustzijn creëren rondom cybersecurity bij de medewerkers.



Ik weet dat mijn werknemers van mijn organisatie weleens gegevens versturen zonder dat deze beveiligd zijn, terwijl dit wel zou moeten.



Ik vind dat mijn collega's/ werknemers momenteel te weinig bewustzijn hebben voor het veilig omgaan met onze data/data van onze klanten.



Werknemers van mijn organisatie hebben weleens apps op hun werktelefoon geïnstalleerd waardoor de kans op datalekken toenam.

Hoofdstuk 3

Effecten van de lockdown

Tijdens de lockdown zijn er verschillende noodmaatregelen getroffen om thuiswerken mogelijk te maken. Bij noodmaatregelen denken we al snel aan een laptop, bureaustoel en andere faciliteiten die vallen onder een ergonomisch ingerichte thuiswerkplek, maar denk ook eens aan een goed werkende cloudomgeving. En hoe zit het eigenlijk met die noodmaatregelen die we niet met ons blote oog kunnen waarnemen, zoals de beveiliging van de technologie? Deze noodmaatregelen zijn misschien nog wel belangrijker. Het treffen van maatregelen en voorzieningen voor een betere beveiliging bij thuiswerken is zeer raadzaam. Indien de beveiliging niet op orde is, veranderen uw gegevens al snel in een ware goudmijn voor cybercriminelen.

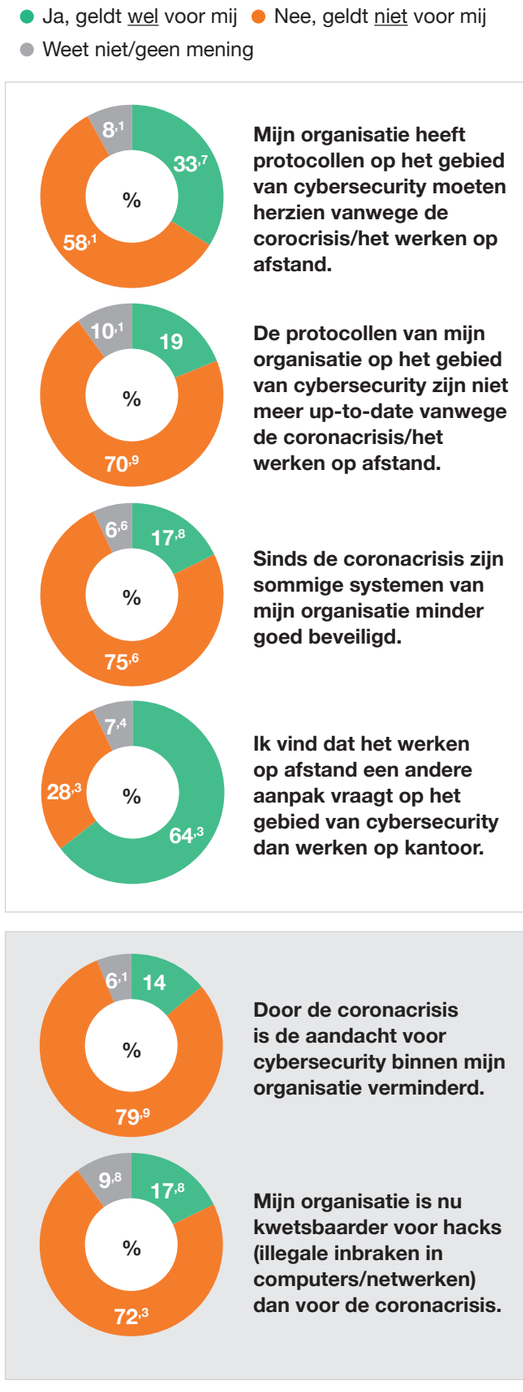
3.1 Thuiswerken

Driekwart van de organisaties geeft aan dat er protocollen bestaan wat betreft veiligheid van data waar werknemers zich aan moeten houden. Hoewel het nog onduidelijk is wanneer we met zijn allen weer wat vaker mogen plaatsnemen aan ons kantoorbureau, heeft een derde van de organisaties de protocollen al herzien vanwege de coronacrisis. 19 procent van de organisaties vindt dat de protocollen voor cybersecurity niet meer up-to-date zijn. We hebben hen dan ook de vraag gesteld of werken op afstand een andere aanpak vergt van cybersecurity dan werken op kantoor. Jazeker, 64 procent onderschrijft dat. Dit is een goede eerste stap. Maar het onderzoek bewijst ook dat nog een klein percentage daadwerkelijk de protocollen heeft aangepast, terwijl het risico om aangevallen te worden tijdens de coronacrisis aanzienlijk is toegenomen.

3.2 Kwetsbaarheid

Nu we weten hoeveel procent van de organisaties daadwerkelijk bestaande protocollen heeft betreffende veiligheid en data, is het interessant om te kijken hoeveel aandacht hieraan besteed wordt. Dat een protocol bestaat, betekent niet direct dat er veel aandacht aan besteed wordt. Door de uitbraak van het virus hebben we ervaren alert te blijven. Cybercriminelen zijn altijd op zoek zijn naar de nieuwste mogelijkheden om in te breken in uw systemen.

Vier op de vijf respondenten van de organisaties zegt dat er binnen hun organisatie net zoveel aandacht is voor cybersecurity als voor de coronacrisis. Slechts 14% ervaart een verminderd aandachtniveau. Tegelijk zegt 18% van de organisaties dat sommige systemen vandaag minder goed beveiligd zijn dan voor de lockdown. Onderaan de streep voelt 18% van de organisaties zich nu kwetsbaarder voor hacks dan voorheen.



Conclusie

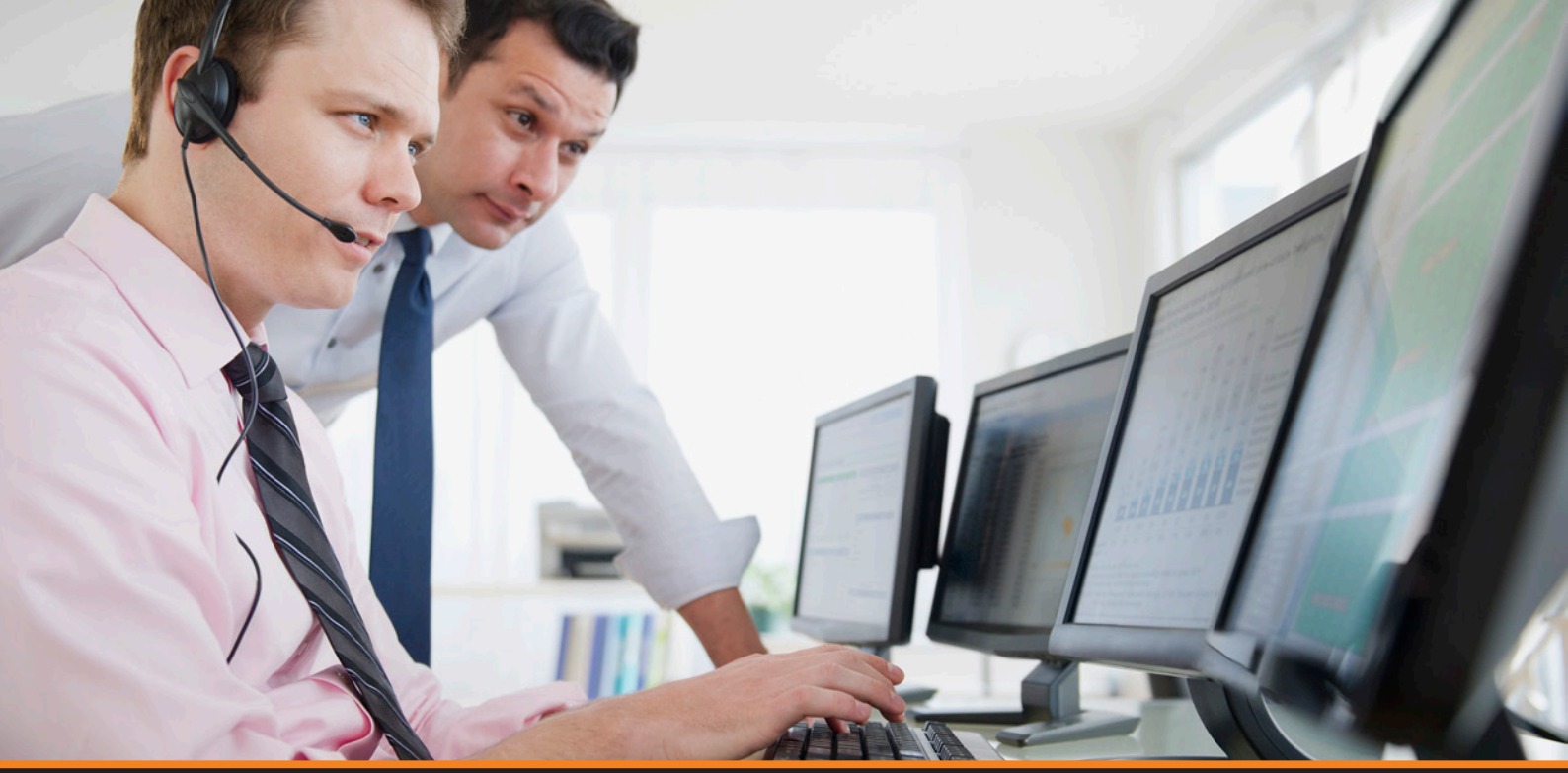
Uit het onderzoek blijkt dat organisaties aandacht voor cybersecurity hebben, maar niet zodanig dat security uitmaakt van de bedrijfscultuur en strategie. Het komt nog te vaak voor dat organisaties de risico's van de aanvallen onderschatten en medewerkers nog teveel vrijheid krijgen. Door gebrek aan kennis en aandacht worden berichten onbeveiligd verzonden en willekeurige applicaties op zakelijke devices gedownload. Er is nog een grote inhaalslag nodig om noodzaak en nut van cybersecurity in de organisaties te vergroten.

Hierbij spelen de IT-beslissers een onmisbare rol. Het is erg belangrijk dat zij deze rol daadwerkelijk gaan dragen. Want een goede beveiliging is essentieel, maar dit werkt alleen als er goede afspraken zijn gemaakt, hier de juiste aandacht aan wordt besteed en de medewerkers op de hoogte zijn bij wie ze zich moeten melden wanneer er een verdachte situatie ontstaat. Want hoe weet u zeker dat u niet het volgende slachtoffer bent? Cybercriminelen zijn tenslotte meesters in het vinden van uw zwakke plek.

We kunnen concluderen dat cybersecurity niet meer mag ontbreken in uw bedrijfsstrategie. Hiermee beschermt u niet alleen alle bedrijfsinformatie, maar ook uw zakelijk succes. Klanten leggen immers in vertrouwen hun informatie in uw handen. Wacht niet langer en tref nu de essentiële voorbereidingen om cyberaanvallen buiten de deur te houden, zoals het afsluiten van een cyberverzekering en het integreren van security in de IT infrastructuur.

Over het onderzoek

399 deelnemers, dit zijn 252 mannen en 147 vrouwen. Verspreid over Nederland, maar vooral uit het westen. 78% heeft een kantoorbaan waarin ze veelal achter een bureau en beeldscherm zitten. 81% is (mede)beslissend of eindverantwoordelijk voor IT en automatisering. Dit zijn er dus 323.



Over Orange Cyberdefense

Orange Cyberdefense is de deskundige cybersecurity businessunit van Orange Group en biedt managed security, detectie en respons diensten aan organisaties over de hele wereld. Als dé beveiligingsprovider van Europa streven we ernaar de vrijheid te beschermen en een veiligere digitale samenleving op te bouwen. Wij zijn een bedreigingsonderzoeks- en inlichtingengestuurde beveiligingsprovider die ongeëvenaarde bescherming biedt tegen huidige en opkomende bedreigingen.
Met een trackrecord van meer dan 25 jaar op het gebied van informatiebeveiliging, meer dan 250 onderzoekers en analisten en 16 CyberSOC's verspreid over de hele wereld en verkoop- en servicesondersteuning in 160 landen, kunnen wij wereldwijde bescherming bieden met lokale expertise en onze klanten ondersteunen gedurende de hele levenscyclus van bedreigingen.

Voor meer informatie, bezoek www.orangecyberdefense.com/nl
of volg ons op LinkedIn, Twitter en onze blogs.

Orange is een van 's werelds meest toonaangevende telecommunicatiebedrijven met een omzet van 42,2 miljard euro en 266 miljoen klanten wereldwijd op 31 december 2019. Orange is genoteerd aan de Euronext Parijs (ORA) en aan de New York Stock Exchange (ORAN). In december 2019 presenteerde Orange zijn nieuwe "Engage 2025" strategisch plan, onderbouwd met sociale en ecologische verantwoording. Door de snelle groei in gebieden als B-to-B-diensten en het centraal stellen van data en KI in innovatie, zal de hele Orange Group een aantrekkelijke en verantwoordelijke werkgever zijn.

Orange Cyberdefense
Orteliuslaan 1001
3528 BE Utrecht
088 1234 200
info@orangecyberdefense.nl
www.orangecyberdefense.nl