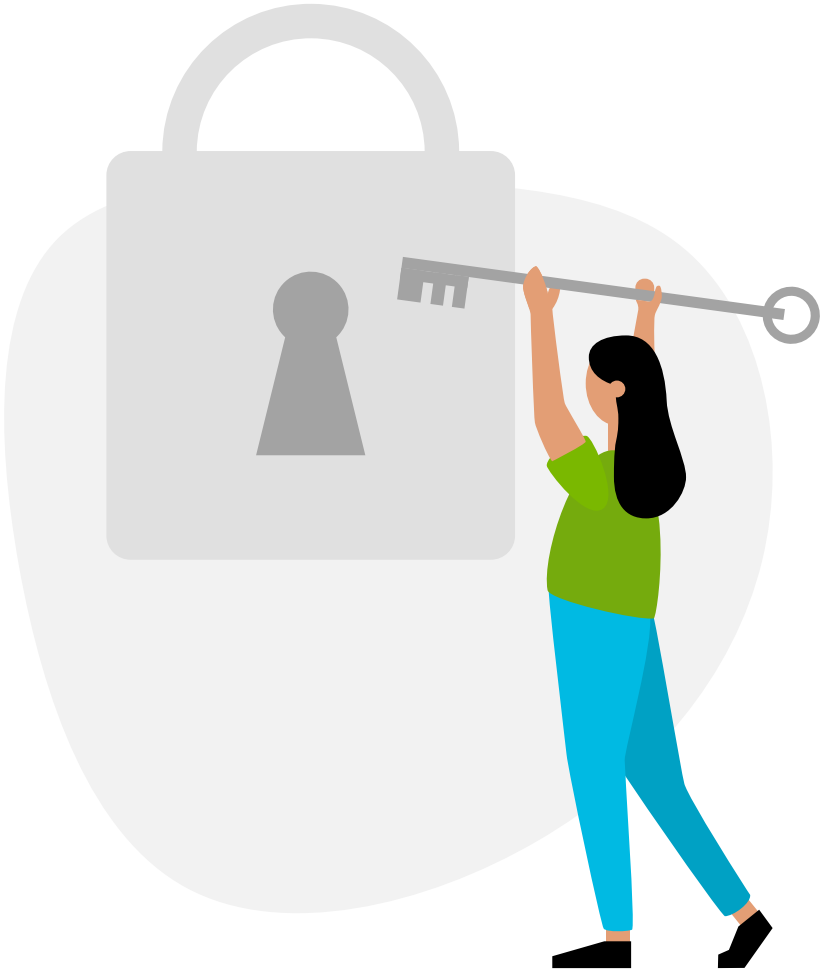
QS solutions

Whitepaper Enhance Security

Zero Trust: de meest robuuste beveiliging tegen cyberaanvallen

Verhoog je cybersecurity volwassenheid, bescherm je organisatie tegen cyberaanvallen en reageer veerkrachtig op incidenten met deze alomvattende beveiligingsstrategie.

Inhoud



Een culturele verschuiving

De coronapandemie zette ook onze digitale wereld op z'n kop. Terwijl het coronavirus zich in rap tempo over de wereld verspreidde en zorgde voor chaos, onzekerheid en verwarring, ontstond een digitaal walhalla voor cybercriminelen. Miljoenen mensen gingen immers thuiswerken en dat bracht grote risico's voor organisaties. Vaak werd gewerkt met een suboptimaal beveiligde infrastructuur en namen medewerkers hun toevlucht tot privé-apparatuur en moderne apps om met collega's en klanten te communiceren zonder toestemming van de IT-afdeling.

Ondertussen werden hackers opportunistisch en gingen steeds slimmer, meer geavanceerd en beter georganiseerd werken. En dat zien we terug in de cijfers. Wereldwijd steeg het aantal cyberaanvallen vorig jaar explosief. In Nederland verdubbelde zelfs in één kwartaal het aantal ransomware-aanvallen. Hackers kregen namelijk nóg meer manieren om binnen te dringen in systemen van organisaties. Ga maar na: hoeveel technologie heeft jouw organisatie allemaal nodig om up and running te blijven? Elke applicatie en elk apparaat is weer een risico. En door het massale thuiswerken heb je veel minder onder controle welke applicaties en apparaten je medewerkers gebruiken.

Het is dus niet meer de vraag of, maar wanneer jouw organisatie te maken krijgt met een beveiligingsbreuk.

Merkschade

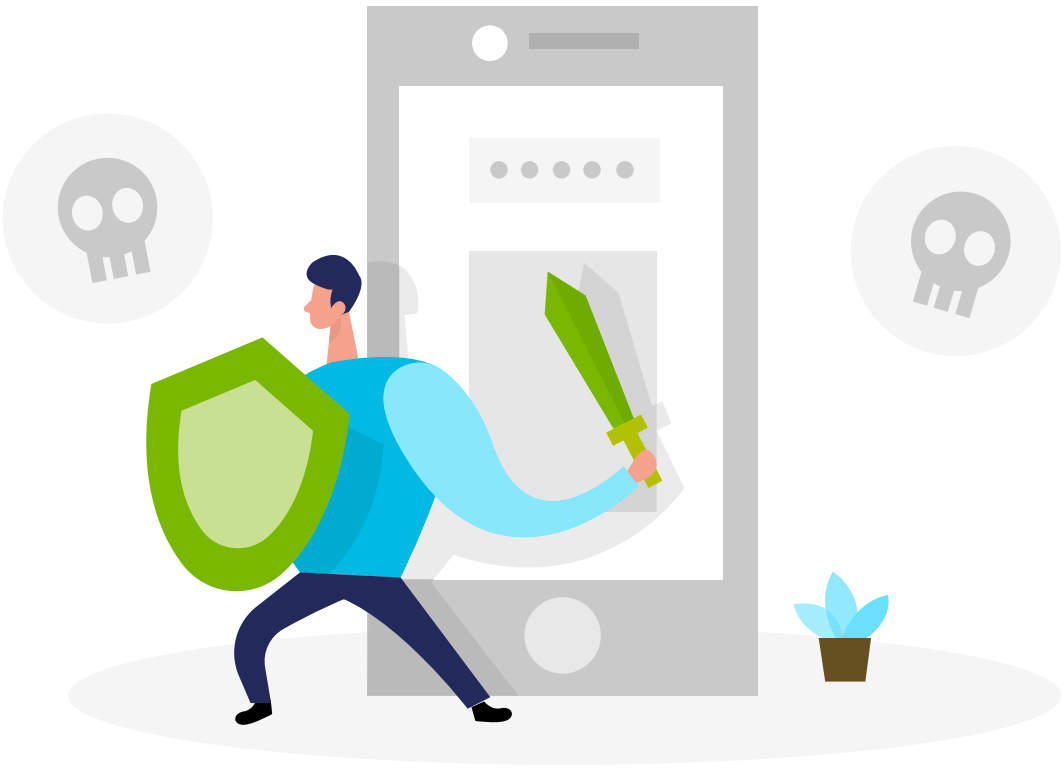
De schade van aanvallen met Ransomware-as-a-Service (RaaS) en Enterprise ransomware, ook bekend als Big Game Hunting (BGH) is bovendien gigantisch. Dat constateerde ook de Nationaal Coördinator Terrorismebestrijding en Veiligheid in zijn rapport Cybersecuritybeeld Nederland 2021. Dat heeft ook te maken met het feit dat het functioneren van organisaties en medewerkers dagelijks meer en meer afhankelijk wordt van onze IT-systemen, applicaties en apparaten. Bij een ransomware-aanval gaat het niet alleen om het betalen van losgeld, maar ook om verlies aan continuïteit, gevolgschade en herstelkosten. Zo'n aanval legt namelijk vitale processen plat en zorgt dat vertrouwelijke of gevoelige informatie mogelijk wordt gelekt of gepubliceerd. Je bedrijfsvoering staat daardoor onder druk en de naleving van bepaalde regelgeving kun je niet meer garanderen. En dat heeft óók gevolgen voor de reputatie van je organisatie en het vertrouwen van je klant.

Beveiliging is geen technologisch vraagstuk, maar een opgave voor je hele organisatie.

Steeds meer directieleden en managementteams beseffen dan ook dat beveiliging niet slechts een technologisch vraagstuk is. Het is een opgave voor de hele organisatie en vraagt om visie vanuit de boardroom. Cybersecurity is dus een vitaal onderdeel geworden van de organisatiestrategie, al wordt dat nog regelmatig vergeten. Maar een culturele verschuiving wordt wel langzaam zichtbaar.

Cyberbestendig worden

De security beleggen bij de IT-afdeling, kan dus niet meer. Ook een pure focus op de veiligheid van je IT-infrastructuur heeft geen zin. Want daarmee red je het niet. Je moet beseffen en accepteren dat mensen fouten gaan maken. En dat het slechts een kwestie van tijd is voordat een ongeautoriseerd persoon toegang heeft tot jouw IT-omgeving. Dat kun je in deze digitale wereld namelijk niet meer voorkomen. En een groter veiligheidsbewustzijn onder medewerkers kan die risico's ook niet wegnemen. De vraag is dus: hoe gaat jouw organisatie om met digitale dreigingen? Hoe volwassen zijn jouw cybersecuritymaatregelen? En kun je proactief handelen wanneer dat nodig is?



Als organisatie gaat het er dus om dat je cyberbestendig moet worden: je moet cyberaanvallen kunnen overleven, kritieke processen en activiteiten kunnen handhaven en nieuwe technologieën kunnen omarmen. De continu veranderende dreigingen vergen ook een duidelijke wendbaarheid; je moet kunnen meebewegen met wat er gebeurt. Maar wel vanuit een heldere visie. En met een doordachte, strategische aanpak van informatiebeveiliging met uitgekiende processen, waardoor je je kritieke processen en activiteiten blijft beschermen, altijd alert blijft en snel en veerkrachtig reageert op incidenten. En dat alles zonder de productiviteit van de organisatie te raken. Dat is dé uitdaging voor security op dit moment.

Omarm de *Zero-Trust* mindset

Waar begint dan die cyberbestendigheid? En hoe kom je tot een sterke beveiligingsstrategie? Feit is dat een traditionele databeveiliging niet meer volstaat. Een veilig en compliant netwerk on-site inrichten voor je organisatie, en proberen daar alle bedrijfsmiddelen onder te brengen, is niet meer van deze tijd. In dit digitale tijdperk is een bredere, maar bovenal ook adaptieve strategie nodig. Eentje die zich kan aanpassen aan de toenemende complexiteit en dynamiek van onze manier van werken. Die er rekening mee houdt dat medewerkers altijd en overal moeten kunnen werken, vanuit ieder apparaat. Het enige dat ze hoeven te doen, is inloggen op hun digitale werkplek. Dat brengt andere risico's met zich mee en vereist een herziene cybersecuritystrategie.

Nieuw gedachtegoed

Moderne beveiliging staat of valt dus bij het beschermen van waar we tegenwoordig vooral ons werk doen: in de cloud, op onze digitale werkplekken. Ofwel: je moet alle medewerkers, apparaten en applicaties beveiligen, waar die zich ook bevinden. Daarvoor moet je als organisatie op zoek naar een nieuw gedachtegoed. Naar een nieuwe visie op beveiliging, waarbij je de productiviteit van je de medewerkers niet negatief beïnvloedt. Want wanneer securitymaatregelen vooral een barrière voor de productiviteit vormen, maak je ook de verkeerde keuzes. En dan kiezen medewerkers andere – lees: onbeveiligde – paden om alsnog hun doelen te behalen.

Alleen met *Zero Trust* maak je je organisatie weerbaar tegen hedendaagse digitale dreigingen én blijf je nieuwe vormen van cybercrime voor.

Onze manier van werken verandert bovendien snel. En dat geldt ook voor cybercriminelen. Digitale bedreigingen evolueren voortdurend en jouw beveiliging kan niet simpelweg alle bedreigingen bijbenen. Je loopt op z'n best altijd nét achter de nieuwste cyberaanvallen aan. *Zero Trust* is daarom het enige juiste uitgangspunt in deze tijd: vertrouw nooit, controleer altijd. Vanuit deze visie richt je je op de beveiliging en compliance van bedrijfsmiddelen, ongeacht hun fysieke locatie of plaats in het netwerk. Elke aanvraag behandel je dan als een aanvraag die afkomstig is van een onbeveiligd netwerk. Je kijkt dus niet alleen wie vanuit welke applicatie of welk apparaat probeert binnen te komen: je combineert binnen *Zero Trust* alle aspecten en verifieert elke aanvraag volledig, voordat je die (eventueel met voorwaarden) goedkeurt of niet. Alleen op die manier kun je je organisatie beschermen tegen alle digitale bedreigingen én blijf je nieuwe vormen van cybercrime voor.

Drie principes

De *Zero Trust Architectuur* is gebaseerd op drie principes:

1. Verifieer expliciet

Verifieer en autoriseer altijd op basis van alle beschikbare gegevenspunten, inclusief gebruikersidentiteit, locatie, apparaatstatus, service of werkbelasting, gegevensclassificatie en afwijkingen.

2. Gebruik de minst bevoorrechte toegang

Beperk gebruikerstoegang met *just-in-time* en *just-enough-access* (JIT/JEA), op risico's gebaseerd adaptief beleid en gegevensbescherming die zowel gegevens als productiviteit helpen beveiligen.

3. Ga uit van schending

Minimaliseer de schade bij incidenten en voorkom zijwaartse bewegingen door de toegang voor netwerk, gebruiker, apparaat en app te segmenteren. Controleer of alle sessies *end-to-end* zijn versleuteld. Gebruik analyses om dreigingen in beeld te krijgen, te detecteren en de verdediging te verbeteren.

Voortdurende waakzaamheid

Zero Trust Architectuur komt uit de koker van The Open Source Group, een grote, internationale en onafhankelijke groep cybersecurityprofessionals. Zij zagen in dat beveiligingscontroles wel beter worden, maar ook dat kwaadwillenden steeds creatiever worden met nieuwe strategieën voor cyberaanvallen. En dat terwijl de beveiligingsperimeter veel dynamischer is geworden en moeilijker is te beheren: je hebt data on-site én in cloud datacenters, maar ook medewerkers die werken vanuit huis met hun eigen apparaten en regelmatig ook niet-geaccordeerde programma's gebruiken voor hun werk.

Eenmalige of periodieke investeringen in beveiligingscontroles helpen dan niet. *Zero Trust* is in deze digitale wereld van werken het enige dat werkt. Juist omdat het een voortdurende verificatie vereist, met een permanente controle tot in de puntjes. Van de identiteit van de gebruiker tot de hostingomgeving van de applicatie. *Zero Trust* vraagt daarom ook om een continue aandacht voor beveiliging. Om een permanente waakzaamheid en non-stop evaluatie: zijn jouw beveiligingscontroles en securitymaatregelen nog relevant en doeltreffend?

Kies voor een holistische benadering van cybersecurity

Zero Trust als beveiliging is geen kant-en-klaar product of een simpele oplossing die je slechts hoeft te implementeren. Het vergt inzicht in je organisatieprocessen, (rollen van) gebruikers, gebruikte applicaties en apparaten. Op basis daarvan kun je een strategie ontwikkelen waarmee je bedreigingen sneller kunt detecteren, de impact van incidenten beter kunt beperken en sneller kunt herstellen, om uiteindelijk (klant) data beter te beschermen. En die inzichten moet je ook voortdurend controleren en kunnen bijstellen.

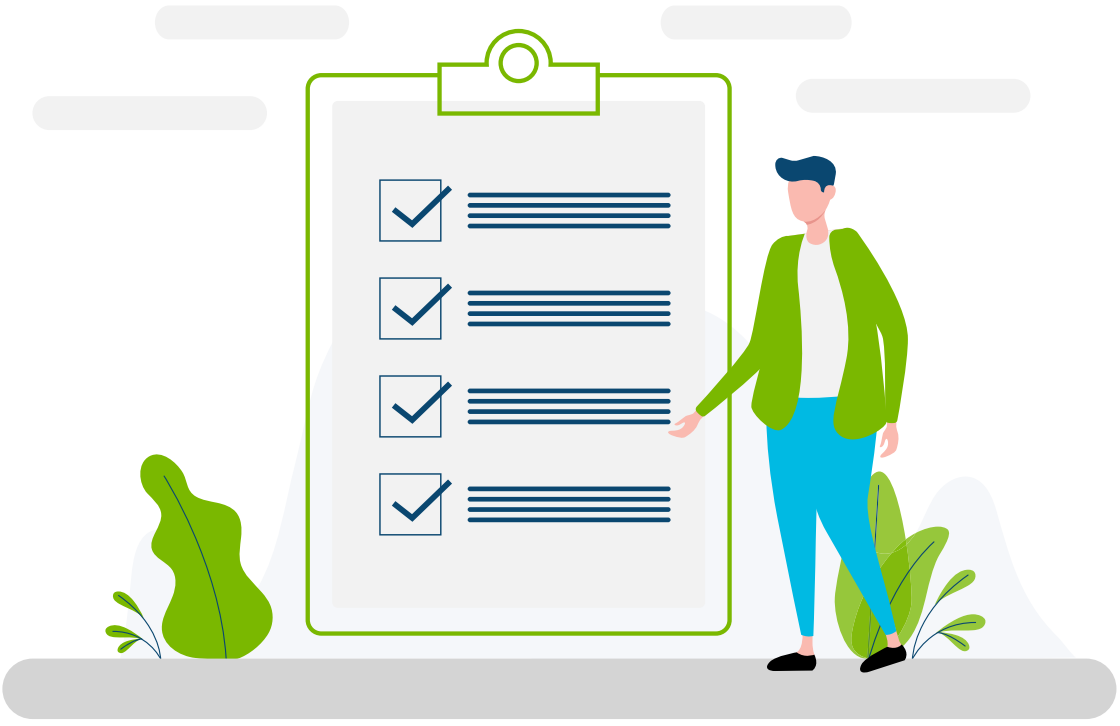
De kracht van *Zero Trust* is dan ook de breedte van de ontwikkelde strategie, die zich bovendien aanpast aan de veranderende complexiteit en samenstelling van de werkomgeving. Tegelijk wil je niet dat je beveiliging een belemmering vormt voor werken op kantoor of thuis. De adaptieve strategie betekent niet dat gebruikers aan de voorkant veranderingen moeten opmerken. Of telkens nieuwe manieren moeten aanleren om tot hun programma's of werkbestanden te komen.

Brede alertheid

Een omvangrijke strategie ontwikkelen voor *Zero Trust* binnen jouw organisatie is ingewikkeld. Je moet zorgen dat die strategie voortdurend meebeweegt met je organisatie en met je gebruikers. Je wil allesomvattend zijn, maar beseft ook dat je wil gebruikmaken van nieuwe technieken. Je kunt niet de focus op verouderde systemen verliezen, want cybercriminelen maken handig gebruik van alle mogelijke kwetsbaarheden.

Zero Trust **vraagt om een minimale basis aan securitymaatregelen op alle facetten en een scherpe monitoring.**

Het enige wat dan helpt, is een holistische benadering hanteren op je cybersecurity. Je moet de volledige reikwijdte van je informatiebeveiliging inzien. En een voortdurende alertheid aanmeten, wat betekent dat je alle risico's in kaart moet brengen voor al jouw gebruiksidentiteiten, apparaten, applicaties, data, infrastructuur en netwerken. Sterker nog, je moet zorgen dat je op alle facetten van security een minimale basis aan maatregelen implementeert en die scherp monitort. Waarbij je ook rekening houdt met de prioriteiten van je organisatie, de aanwezige technologieën, processen en de impact van veranderingen.



Solide beveiliging

Voor *Zero Trust* moet je dus controlemechanismen en technologieën implementeren op alle fundamentele elementen, waaronder:

- Een krachtig identiteits- en toegangsbeheer voor personen, services en IoT-apparaten dankzij een betere verificatie met gebruikersauthenticatie, identiteitsverificatie en controle op gebruikersrechten en compatibiliteit.

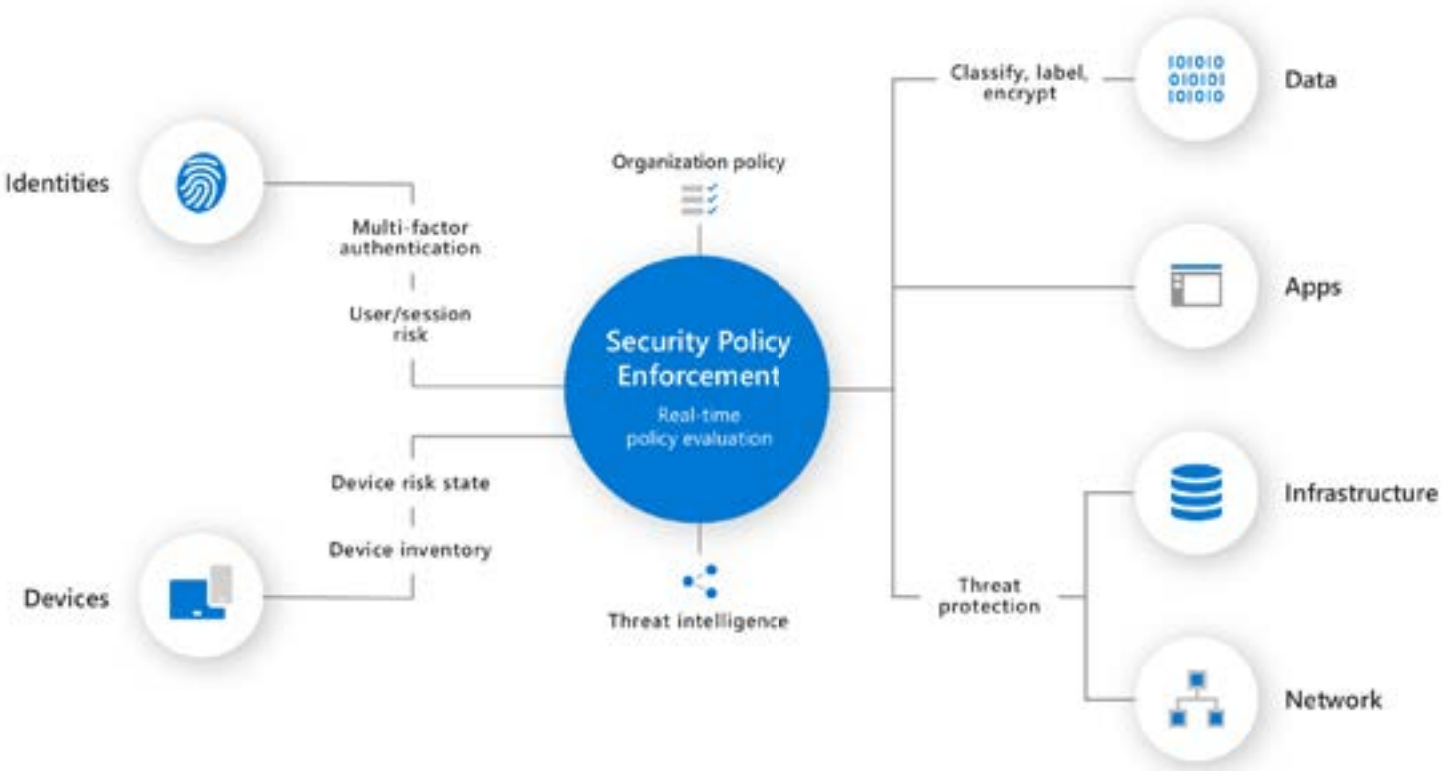
- Met hetzelfde *Zero Trust*-beleid als endpoint security, kun je voorkomen dat *Bring Your Own Device (BYOD)* een probleem wordt.

- Door applicaties te segmenteren, waardoor je extra controles en technologieën kunt inbouwen die schaduw-IT en abnormaal gedrag detecteren, passende machtigingen in applicaties waarborgen, toegang verlenen op basis van realtime analytics, gebruikersacties beperken en veilige configuratie-opties valideren.

Al deze elementen zijn een belangrijke signaalbron en een controlelaag voor handhaving. En door de data van de verschillende elementen te analyseren met de inzet van kunstmatige intelligentie herken je bedreigingen sneller en beter waardoor je direct geautomatiseerd actie kunt ondernemen. Deze tools helpen je ook achterhalen wat er is gebeurd, wat er is gecompromitteerd en hoe je herhaling voorkomt. En zo bouw je aan een solide verdediging.

Holistische aanpak van *Zero Trust*

Binnen de holistische aanpak voor *Zero Trust* moet je komen tot een adaptieve strategie die past binnen de visie van je organisatie en die alle identiteiten, apparaten, data, applicaties, de IT-infrastructuur en het IT-netwerk omvat. De strategie moet dus een brede reikwijdte hebben en een voortdurende alertheid op alle elementen garanderen.



Tijd voor een assessment

Hoewel *Zero Trust*-beveiliging het meest effectief is als je het direct integreert in je hele digitale landschap, is dat in de praktijk vaak niet mogelijk. Klein beginnen is het devies omdat het vaak niet haalbaar is om meerdere grote wijzigingen in één keer te realiseren. Organisaties moeten daarom een gefaseerde aanpak hanteren en zich eerst specifiek richten op bepaalde gebieden waar hun cybersecurity nog onvoldoende volwassen is. Die gebieden worden mede bepaald op basis van de beschikbare resources en prioriteiten. Welk budget is beschikbaar? Wat zijn de directe zakelijke behoeften? Oftewel: wat moet je nú aanpakken en wat is mogelijk?

Een belangrijk punt in de reis naar *Zero Trust* is daarom een beginpunt bepalen: hoe volwassen is jouw cybersecurity nu? Hoe groot is de reikwijdte van je informatiebeveiliging? Van daaruit kun je bouwen aan de cyberweerbaarheid van de organisatie. Als je wilt beginnen met *Zero Trust* hoef je dus niet als organisatie jouw IT-infrastructuur volledig opnieuw uit te vinden. Je bouwt verder in de hybride IT-omgeving en ondersteunt die omgeving zonder dat je direct bestaande oplossingen volledig hoeft te vervangen.

Wie wil starten met *Zero Trust*, moet eerst de volwassenheid van zijn cybersecurity in beeld brengen.

Waar start jouw reis naar *Zero Trust*?

Om te beoordelen in hoeverre jouw organisatie klaar is voor *Zero Trust*, moet je de volwassenheid van jouw cybersecurity in beeld brengen. De volgende elementen geven daarvoor een sterke indicatie:

- Hoe sterk is de authenticatie? Gebruik je een sterke Multi Factor Authenticatie? Hoe minimaliseer je het risico van identiteitsinbreuk?

- Hoe adaptief is jouw toegangsbeleid? Hanteer je heldere beleidsregels voor acceptabele toegang tot resources? En hoe dwing je die af?

- Maak jij al werk van microsegmentatie? In hoeverre is jouw organisatie op weg naar een allesomvattende en gedistribueerde segmentatie met behulp van softwarematig gedefinieerde microperimeters?

- Werk je al met geautomatiseerde waarschuwingen en herstelacties om de gemiddelde tijd tussen aanval en reactie te minimaliseren?

- Gebruik je al kunstmatige intelligentie en cloud-intelligence om in realtime afwijkingen te detecteren en hierop te reageren?

- In hoeverre classificeer en bescherm jij je data? Hoe minimaliseer je gevoelige data tegen blootstelling aan schadelijke of onbedoelde exfiltratie?

Een cybersecurity assessment brengt een helder overzicht van kwetsbaarheden en risico's. Op basis daarvan kun je gericht prioriteiten bepalen en een plan van aanpak opstellen.

Gericht verbeteren dankzij helder inzicht

Om daadwerkelijk inzicht te krijgen in de mate van volwassenheid van je cybersecurity op alle relevante elementen, adviseren we bij QS solutions een cybersecurity assessment. In korte tijd en met een kleine investering krijg je inzicht in welke cyberrisico's er zijn voor jouw hybride IT-omgeving en in hoeverre je huidige securitymaatregelen voldoende bescherming bieden. Je krijgt inzicht in potentiële kwetsbaarheden en risico's en kunt geïnformeerde besluiten nemen over prioriteiten binnen je cybersecurity: hier gaan we eerst ons securitybudget aan besteden. Met een cybersecurity assessment prioriteer je dus de risico's voor jouw organisatie en kun je een effectief en efficiënt verbeterplan opstellen op basis van feiten.

Over QS solutions

Bij QS solutions adviseren we organisaties uit te gaan van *Zero Trust*. Want wij weten hoe kwetsbaar organisaties zijn. Én welke gevolgen het kan hebben als een organisatie niet proactief de cybersecurity volwassenheid verbetert. We starten met onze *Cyber Security Assessment Tool (CSAT)* om snel en eenvoudig de status van de beveiliging in beeld te brengen. Op basis daarvan kunnen we gericht de grootste risico's aanpakken. Bijvoorbeeld met de cloudnative beveiligingsoplossingen van Microsoft. Omdat je met het Microsoft-platform de uiteenlopende beveiligingsrisico's beheerst en zorgt dat eindgebruikers altijd productief en veilig blijven werken. Met een periodiek assessment blijf je bovendien altijd *on top of your security game* en weet je feilloos welke mogelijke kwetsbaarheden je dringend moet aanpakken. Dé manier om op basis van feiten een actieplan te definiëren.

Wil je weten hoe je beveiliging ervoor staat?

Dankzij onze Cyber Security Assessment Tool (CSAT) ben je in no-time op de hoogte van alle digitale kwetsbaarheden en cyberrisico's in jouw organisatie. Neem contact op met QS solutions voor meer informatie of een afspraak:

T: +31 (0)33 – 71 22 111
E: marketing@qssolutions.nl

solutions