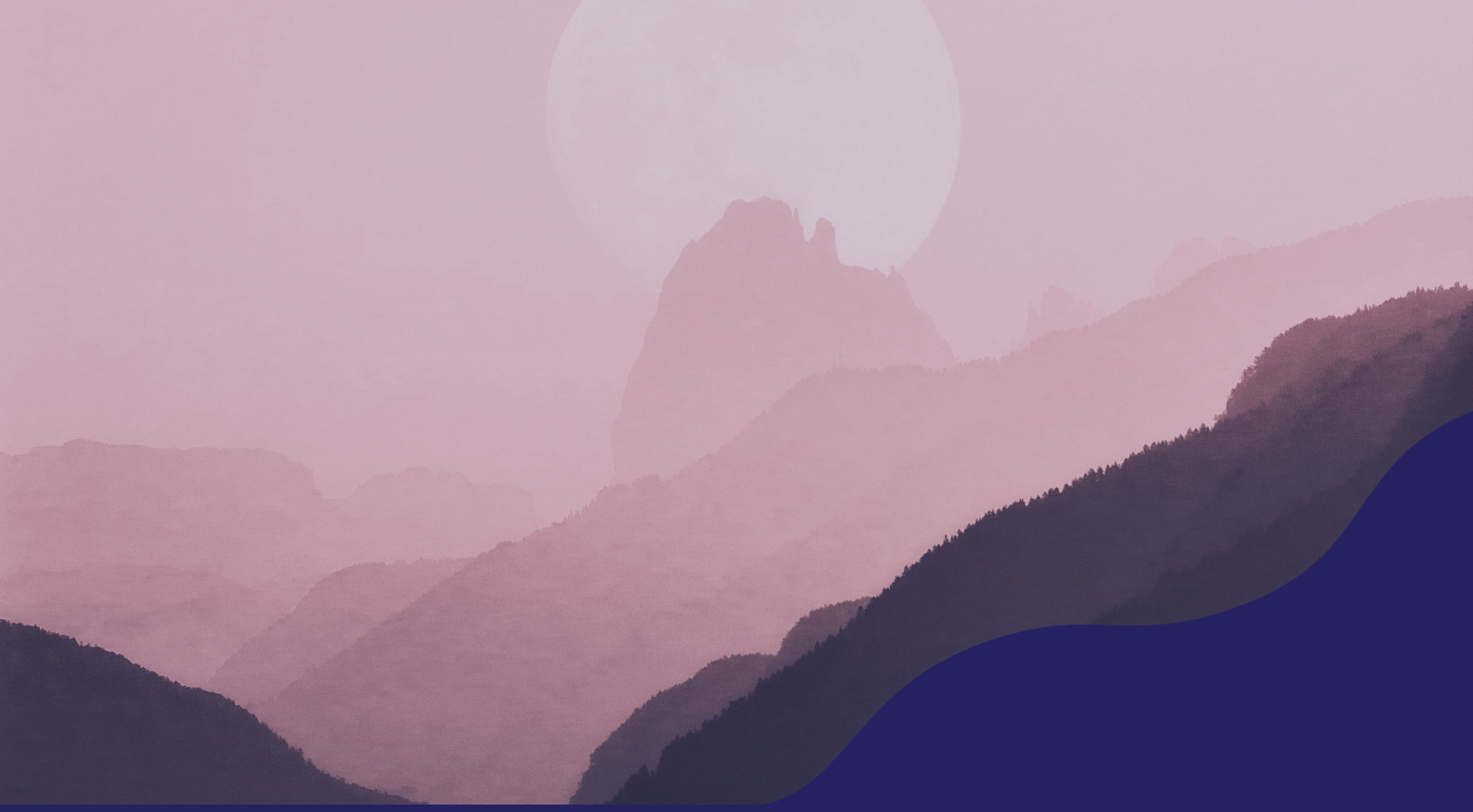
Whitepaper

NIS2-compliance vanuit intrinsieke motivatie

Een EU die weerbaarder is tegen cybercrime: dat is het doel van de veelbesproken nieuwe cybersecurity-richtlijn NIS2. Niet voldoen aan deze richtlijn kan ernstige gevolgen hebben, aangezien het C-level persoonlijk aansprakelijk is. In deze whitepaper staan we uitgebreid stil bij hoe compliance helpt om een stevig security-beleid op te stellen, door een nauwe samenwerking tussen C-level en IT-management. Aan de NIS2 voldoen, doet u uiteindelijk niet voor de Europese overheid, maar voor uw eigen veiligheid, de veiligheid van de keten en voor uw klanten.



Inhoudsopgave

Wat zijn de doelen van deze whitepaper?

Het hoofddoel:

- U op de hoogte brengen van de mogelijke impact van NIS2 op uw organisatie, aan de hand van essentiële vragen die C-level en IT-management onderling moeten bespreken.

Dat doen we aan de hand van deze subdoelen:

- U informeren over NIS2: welke sectoren vallen eronder, wanneer gaat de richtlijn in, en welke stappen moet u nemen ter voorbereiding?
- Het belang laten zien van compliance, ook als u hier niet toe verplicht bent.
- Uitleggen hoe de NIS2 aanknopingspunten geeft voor een stevig security-beleid.
- Het belang laten zien van het verhogen van uw budget voor cybersecurity.

NIS2: de samenvatting

De Network and Information Security Directive (NIS2) is een EU-richtlijn op het gebied van cybersecurity die ingaat op 17 oktober 2024. Zoals de naam al verraadt, is er sprake van een update van de eerdere NIS-richtlijn. Het voornaamste verschil is de reikwijdte: veel meer sectoren zijn verplicht zich aan de NIS2 te houden. Daar leest u meer over in de sectie 'Voor wie is de NIS2?' in deze whitepaper.

Het doel van deze richtlijn: EU-lidstaten weerbaarder maken tegen cybercriminaliteit, die de afgelopen jaren flink is toegenomen en naar verwachting alleen nog maar zwaarder zal worden. De lidstaten worden krachtiger doordat afzonderlijke bedrijven serieus werk moeten maken van hun cybersecurity. Om dat mogelijk te maken, is er sprake van een zorgplicht: voor de veiligheid van uw eigen organisatie, voor de keten waarin u werkt en voor uw klanten. Ook is er een meldplicht: wanneer er een incident is, moet u dat binnen 24 uur melden bij de toezichthouder.

Let op: er is geen sprake van een papieren maatregel, noch van een verzekering. Wat de NIS2 wél is, is een concrete set maatregelen om werk te maken van security. Met papier houdt u uw organisatie immers niet veilig; wél met beleid.

Niet vergeten: op het niet naleven van de richtlijn staan flinke boetes: maximaal 10 miljoen euro of 2% van de totale wereldwijde jaaromzet. Dat is geen keuze die u zelf mag maken: de hoogste van die twee bedragen geldt. Daar komt ook nog eens bij kijken dat directieleden persoonlijk aansprakelijk zijn voor het niet naleven van de regels. Dat is nog afgezien van gemiste omzet en reputatieschade. Als dat geen stok achter de deur is om NIS2 op C-level te bespreken én om extra securitybudget vrij te maken.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) raadt deze stappen aan om goed voorbereid te zijn op NIS2 en om compliance daarmee te realiseren:

1. Maak een risicoanalyse en -beoordeling van de fysieke en digitale risico's die de dienstverlening van uw organisatie kunnen verstoren.
2. Neem waar mogelijk maatregelen die de organisatie beter beschermen tegen deze risico's.
3. Zorg voor procedures die uw organisatie in staat stellen om incidenten die bedrijfsprocessen (kunnen) verstoren te detecteren, monitoren, op te lossen en te melden.

Bronnen:
Digitale Overheid, Europol, NCTV

Voor wie is de NIS2?

Zoals gezegd is er een lijst met sectoren die zich verplicht aan deze richtlijn moeten houden. Daarnaast is er een aantal voorwaarden waaraan moet worden voldaan. De organisatie in kwestie moet namelijk vijftig medewerkers of meer hebben en een balans of omzet van minstens tien miljoen per jaar.

Deze sectoren moeten voldoen aan de NIS2:

NIS – Vitale aanbieders

- Gezondheidszorg
- Watervoorziening
- Vervoer
- Energie
- Digitale infrastructuur
- Digitale dienst-aanbieders
- Bankwezen en financiële marktinfrastructuur

NIS2 – Toegevoegde sectoren

- Voedingsindustrie
- Ruimte-industrie
- Afval- en waterbeheerbedrijven
- Aanbieders telecomdiensten en energievoorziening
- Beheerders van spoorweginfrastructuur
- Financiële diensten
- Post- en koeriersdiensten
- Overheidsdiensten
- Producten van bepaalde kritieke sectoren
- Digitale aanbieders van o.a. social networking services

Bron: NCTV

Valt u onder één van deze sectoren, of bent u toeleverancier van een organisatie die daaronder valt? Dan moet u zich ook aan de NIS2 houden. Maar dit zijn de verplichte gevallen. Bij PQR adviseren we namelijk: iedere organisatie zou hier werk van moeten maken, ook wanneer NIS2-compliance niet verplicht is voor u. De NIS2 is er niet om uw werkzaamheden moeilijker te maken. Integendeel, de richtlijn is er om u na te laten denken over wat u moet doen wanneer u getroffen wordt door een cyberaanval. Het slechte nieuws: dat zal vroeg of laat gebeuren, hoe goed u ook beveiligd bent.

Het goede nieuws is dat u dan voorbereid bent om de schade te minimaliseren. Dan voorkomt u ook situaties waarin uw verzekering de geleden schade niet blijkt te vergoeden. U kunt de NIS2 het beste zien als een uitgebreide lijst met aandachtspunten, in plaats van een last. Laat u ook gerust verrassen: wellicht heeft u veel van de punten al behoorlijk goed op orde en hoeft u alleen nog te finetunen. Sterker nog, u kunt gerust nog een paar stappen verder gaan en niet alleen aan de minimale vereisten voldoen, maar uit eigen motivatie flink aan uw security werken.

Er zijn namelijk verschillende redenen om compliance te realiseren, ook wanneer de NIS2 niet verplicht is voor u:

- Doordat u uw security-beleid formuleert, begrijpen uw C-level en uw IT-management veel beter van elkaar waarmee ze bezig zijn en hoe ze elkaar kunnen helpen.
- Klanten en medewerkers geven u in vertrouwen informatie, veelal zelfs privacygevoelige of bedrijfskritische informatie. Neem de bescherming en beschikbaarheid van die informatie serieus en houd deze veilig als betrouwbare organisatie.
- U zorgt ervoor dat de gehele keten waarin u opereert veiliger wordt: niet alleen u dus, maar ook uw toeleveranciers, zelfs als geen van u onder de NIS2-verplichting valt.
- U kunt uw compliance als argument naar voren schuiven in uw marketing en tijdens tenders.
- U voorkomt natuurlijk boetes, die ongetwijfeld heel wat hoger uitvallen dan uw extra security-kosten.
- Maar bovenal: u heeft maatregelen genomen die niet alleen voor compliance zorgen, maar die er óók voor zorgen dat u in controle bent over uw bedrijf.

Essentiële vragen voor een gesprek tussen C-level en IT-management

Maar hoe kunt u zich nu het beste op de NIS2 voorbereiden? We zeiden het al: door C-level en IT-management grondig met elkaar in gesprek te laten gaan. Daarvoor hebben we de onderstaande vragen opgesteld.

Behoort u tot het C-level? Dan kunt u deze vragen stellen aan uw IT-management, om zo een onderbouwd idee te krijgen van waar uw organisatie staat qua businesscontinuïteit:

- Hoelang duurt het voordat we weer operationeel zijn na een ransomware-aanval?
- Welke en hoeveel gegevens zijn we dan kwijt?
- Hebben we meer data dan noodzakelijk? Wat er niet is, kan ook niet kwijtraken.
- Hoe snel ontdekken we dat er een aanval gaande is?
- Wat doen we tegen een aanval tijdens de vrijdagmiddagborrel of op kerstavond?
- Wat zijn de eerste stappen die we ondernemen als er een crisis uitbreekt?
- Staat er (klant)data van ons bij toeleveranciers en weten we zeker dat die hun security op orde hebben?
- Hebben we een (getest) business continuïteitsplan en hebben we hier onze toeleveranciers ook in meegenomen?
- Weten we zeker dat onze verzekering de (volledige) schade na een cyberaanval vergoedt of moeten we sterker inzetten op preventie?

Bent u IT-manager? Dan is de NIS2-voorbereiding dé kans om deze vragen aan uw directie voor te leggen:

- Welke gegevens mogen de hackers echt niet in handen krijgen?
- Hoe lang mag de organisatie onbereikbaar zijn na een aanval?
- Welke afdelingen moeten als eerste geholpen worden en welke als laatste?
- Wat zijn onze bedrijfskritische systemen en processen?
- Hoeveel procent van mijn budget mag ik besteden aan security?
- Hoeveel kwetsbaarheden zijn acceptabel?
- Hoe belangrijk is het om tijdig te weten dat we digitaal aangevallen worden?
- Kan er meer budget vrijgemaakt worden voor security?

Het assessment als startpunt voor beleid

Om snel weer operationeel te zijn na een cybersecurity incident, is een goed plan noodzakelijk. Maar hoe stelt u zo'n plan op? Wie heb je daarvoor nodig? Iedereen weet dat back-ups cruciaal zijn, maar welk beleid hanteert u hiervoor? Dagelijkse back-ups of zelfs back-ups per uur is een optie, maar als het lang duurt om ze te herstellen, gaat er alsnog veel data verloren. Wat is een aanvaardbare hersteltijd en tegen welke kosten? Snelle herstelopties zijn beschikbaar, maar past dat binnen uw budget? En wat gebeurt er als uw back-ups ook aangetast zijn? Opslag op een andere locatie of het uitbesteden van het beheer kunnen oplossingen zijn.

Vervolgens kunt u aan de slag. Een stappenplan is maatwerk. Onderstaand vindt u een beknopt voorbeeld van hoe dit er uit kan zien:

- Bepaal of NIS2 op uw organisatie van toepassing is.
- Voer een stakeholder analyse uit.
- Stel een projectteam samen.
- Voer een risicoanalyse uit en neem ook uw toeleveranciers hierin mee.
- Stel een passend beveiligingsniveau vast.
- Stel het beleid op.
- Implementeer incidentmanagement en maak een plan van wat u gaat doen bij een security-incident.
- Behandel geïdentificeerde risico's en pas maatregelen toe.
- Onderzoek, beoordeel, monitor en kies uw leveranciers en partners op hun staat van cybersecurity.
- Train uw bestuur en medewerkers periodiek op cyberveiligheid en bewustzijn, door middel van simulaties.
- Rapporteer aan de overheid en voldoe aan de wetgeving.
- Draag zorg voor continue monitoring en evaluatie van de resultaten.
- Controleer periodiek en verbeter, want het dreigingsbeeld verandert continu.

Tevens is op het gebied van voorkomen, is serieus beleid nodig. Zoals gezegd, uiteindelijk wordt u vroeg of laat slachtoffer van een succesvolle aanval, maar dat wil niet zeggen dat u het criminelen maar zo gemakkelijk mogelijk moet maken. Ga na wat uw zwakke plekken zijn. Via welke endpoints kunnen criminelen ook de rest van uw IT aanvallen? Gaat u deze risico's accepteren of actie ondernemen? De meeste organisaties – ook de grotere – werken hiervoor samen met IT-dienstverleners. Die beschikken namelijk over de specialistische expertise en capaciteit aan IT'ers die bij de meeste bedrijven ontbreekt.

Hoe begint u eigenlijk met beleid maken, indien u dat nog onvoldoende doet? Ook hiervoor kunt – of beter gezegd: móét – u een dienstverlener inschakelen. U krijgt pas een goed beeld van hoe uw organisatie erbij staat, als iemand van buiten óók beoordeelt of u aan de richtlijn voldoet. Dit gebeurt aan de hand van een assessment, dat u onder meer de risicoanalyse en -beoordeling oplevert die NCTV u adviseert te maken. Een beoordeling leidt tot een plan, dat tot beleid leidt, dat resulteert in een veiligere gang van zaken. Maar laten we eerst wat uitgebreider naar de risicoanalyse kijken.

De risicoanalyse in het kort

Tijdens een risicoanalyse worden potentiële bedreigingen geïdentificeerd en geanalyseerd, door een zowel organisatorisch als een technisch comité. Dat bekijkt onder andere ontwerpen, processen en techniek in detail. Voor elke bedreiging wordt bepaald hoe groot de kans is dat deze zich voordoet en wat de mogelijke schade zou zijn als dit daadwerkelijk gebeurt.

Op basis van een risicoanalyse kunnen verschillende keuzes en maatregelen worden overwogen, zoals de volgende:

- Voorkomen: maatregelen om te voorkomen dat een incident plaatsvindt of om de kans daarop te verkleinen.
- Verkleinen: maatregelen om de impact van een incident te beperken zodra het zich voordoet.
- Accepteren: het bewust accepteren van het risico en de mogelijke gevolgen, zonder verdere actie te ondernemen.
- Overdragen: het afdekken van de financiële risico's door middel van verzekeringen of de overdracht van operationele risico's door middel van outsourcing.

Nadat het type behandeling gekozen is, wordt vervolgens de risicoscore toegekend op basis van een heatmap. De 'kans van optreden' is voor elke organisatie gelijk. De impact van een incident verschilt echter wel per organisatie, want als de productie stil ligt is het financiële risico groter, dan wanneer er geen verlofaanvragen gedaan kunnen worden.

De heatmap ziet er bijvoorbeeld zo uit:

Impact	Kans		
	Hoog	Midden	Laag
Hoog	9	6	3
Midden	6	4	2
Laag	3	2	1

Kans
Dit is de waarschijnlijkheid dat een bepaald voorval plaatsvindt. Deze kans wordt vaak uitgedrukt in termen van frequentie (bijvoorbeeld eens per jaar) of als een waarschijnlijkheid (bijvoorbeeld 10% kans dat het incident plaatsvindt binnen een jaar).

Impact
Dit betreft de consequenties of de gevolgen van het voorval, mocht het plaatsvinden. De impact kan variëren van minimaal tot catastrofaal, afhankelijk van het specifieke risico. Het kan worden gekwantificeerd in termen van financiële kosten, gezondheidsproblemen, tijdverlies of andere schadelijke uitkomsten.

Er zijn verschillende mogelijke benaderingen om de schatting van de risicogrootte te maken:

- Kwalitatieve methode: de risico's worden ingeschat op basis van ervaring en intuïtie, zonder gebruik te maken van numerieke gegevens.
- Kwantitatieve methode: het concreet meten van risico's, waar mogelijk, met behulp van kwantificeerbare en meetbare criteria. Deze risico's worden vaak uitgedrukt in termen van financiële impact. Ook worden ze aan elkaar gekoppeld, omdat het kan gebeuren dat meerdere risico's om dezelfde maatregelen vragen.

Op basis van dit resultaat wordt er een prioriteit bepaald, afhankelijk van de complexiteit een doorlooptijd. Vervolgens kan er gewerkt worden aan een risicobehandelplan waaruit concrete acties voortvloeien.

NIS2 en managed services

Het is belangrijk om realistische verwachtingen te hebben: NIS2-compliance bereiken is geen kant-en-klare oplossing, maar vereist maatwerk. Dit is een doorlopend proces, vergelijkbaar met bijvoorbeeld de AVG. Elke nieuwe implementatie of leverancier vereist opnieuw evaluatie van de compliance.

Managed services kunnen wél helpen en ondersteunen om aan de richtlijn te (blijven) voldoen. Voor vrijwel ieder security-probleem is dienstverlening mogelijk: van firewalls en virusscanners, tot bewustzijnstrainingen aan uw directie en uw medewerkers. Na het uitvoeren van een NIS2-assessment kunt u gericht op zoek gaan naar de juiste managed services om uw zwakke plekken aan te pakken. Dat klinkt misschien ingewikkeld, maar ook hiervoor geldt: u hoeft dit niet alleen te doen. Een goede IT-dienstverlener blijft immers met u meebewegen en adviseert u proactief, zodat u ook in de toekomst blijft voldoen aan de NIS2.

Hoe helpt PQR u met de NIS2?

Cybersecurity vraagt om een volledig overzicht, wat ook terug te zien is in de set aan maatregelen van de NIS2. Elke blinde vlek kan immers een ingang zijn voor cybercriminelen. PQR biedt uitgebreide expertise op het gebied van security, privacy, organisatorische en technologische maatregelen. Daardoor zijn we een one-stop shop op gebied van managed services, ook op gebied van IT-security. Het beveiligen van endpoints, mitigeren van securityincidenten, oplossingen goed afstellen op uw behoeften, op tijd patches uitvoeren: daarvoor kunt u op ons rekenen. Wanneer wij dit allemaal op ons nemen, eventueel in samenwerking met uw vaste security-leveranciers, houden we uw gehele IT in het oog; ook de economische en juridische kanten er van. Indien wij uw gehele IT in beheer hebben, kunnen we gericht veranderingen doorvoeren, op alle plaatsen waarop dat nodig is.

Onze aanpak is gericht op het behalen van NIS2-compliance en omvat onder meer gesprekken met uw medewerkers op alle niveaus, resulterend in een gedegen risicoanalyse en roadmap die continu wordt bijgewerkt. Samen met u vertalen we de resultaten van het assessment naar actief beleid, voor systemen en gebruikers. Aan de hand daarvan zorgen we ervoor dat u voor oktober 2024 compliance hebt gerealiseerd en dat u gemakkelijker voorsorteert op veranderingen in de toekomst.

Het gaat bij PQR niet alleen om het implementeren van technologie, maar ook om het behouden van de balans tussen veiligheid en gebruiksvriendelijkheid. Niemand wil immers gehinderd worden tijdens alledaagse werkzaamheden, omdat de security zo streng is.

Continue monitoring
PQR biedt twee oplossingen voor continue monitoring. We lichten ze nader toe.

Security Operations Center Services
Vanuit het Security Operations Center (SOC) monitort PQR mogelijke dreigingen binnen de IT-omgeving van onze klanten. De security-experts bewaken continu alle IT-elementen: on-premises, werkplekken (edge) en cloud assets. Bedreigingen, aanvallen en incidenten worden geanalyseerd en direct opgevolgd of worden, afhankelijk van de gemaakte afspraken, met een duidelijk advies doorgezet naar uw eigen IT-afdeling.

Met deze SOC Services kunnen organisaties rekenen op 24/7 monitoring op incidenten, aanvallen en bedreigingen. Bovendien zijn ze verzekerd van directe actie om schade te voorkomen. Periodiek rapporteren we de incidenten en doen we aanbevelingen om de veiligheid te vergroten. Tevens biedt PQR een dedicated Security Officer, die als uw directe aanspreekpunt fungeert.

Security Information & Event Management
Het PQR SOC biedt beheerde security diensten aan zoals security monitoring & response. Hiervoor zetten wij onder andere ons SIEM in. Dit is de tooling die wordt ingezet voor monitoring en detectie van security-events binnen de IT-omgeving.

De security-analisten van het SOC houden de meldingen uit het SIEM nauwlettend in de gaten en ondernemen waar nodig actie. Daarnaast biedt PQR diverse andere securitydiensten aan, zoals consultancy-diensten, beveiligingsadvies, implementatie van securitysoftware en het uitvoeren van security scans om de IT-veiligheid te verbeteren. Deze diensten worden ingezet om de volledige IT-omgeving te beschermen, zowel on-premises, hybride als in de cloud.

PQR: uw rustmaker in security

PQR is sinds 1990 een toonaangevend bedrijf in de IT-sector, juist door de focus minder te leggen op technologie, maar op het menselijk aspect. Alles wat we doen, doen we met één doel in het achterhoofd: rust maken voor onze klanten. U hoeft zich door ons advies en onze managed services niet langer zorgen te maken om zaken als automatisering, security en natuurlijk NIS2-compliance. Neem gerust contact met ons op om te horen wat we voor elkaar kunnen betekenen.

Tot slot: de NIS2 is nog niet op ieder punt al even duidelijk ingevuld. Wij houden de ontwikkelingen daarom voor u in de gaten. Zodra er belangrijke nieuwe informatie is, communiceren we dat natuurlijk ook naar u. Hou onze website in de gaten: www.pqr.com

U kunt erop vertrouwen dat deze whitepaper up-to-date is.

PQR B.V.
Papendorpseweg 91
3528 BJ Utrecht
Nederland

T +31 30 662 97 29
info@pqr.nl
www.PQR.com
@PQRnl