Dutch Cloud Community

Samen Digitaal Veilig en de rol van MSP's

NIS2 Quality Mark + veilige technische MSP standaarden

Kaseya®

Samen Digitaal Veilig

Samen Digitaal Veilig

- **Overheid en brancheorganisaties zijn samen het initiatief Samen Digitaal Veilig gestart.**
- >100 samenwerkende brancheorganisaties (185.000 leden) om bedrijven/organisaties te ondersteunen
- Informatie & tooling voor digitale veiligheid
- Hulp bij voldoen aan NIS2-wetgeving:

MKB Nederland

VNO NCW

>100
Branche-organisaties

Dutch Cloud Community

Samen Digitaal Veilig

NIS2 wetgeving ‘Gamechanger’

- NIS2-wetgeving zet cybersecurity in beweging zowel grote bedrijven als hun mkb-toeleveranciers
- De verzamelde brancheorganisaties communiceren met al hun leden (185.000 bedrijven) over het platform **Samen Digitaal Veilig** (SDV) voor meer online veiligheid
- Branches hebben een cybersecurity standaard voor 'gewone' mkb bedrijven ontwikkelt tbv. de toeleveringseten, het **NIS2 Quality Mark**
- **Samen Digitaal Veilig = het grootste online platform om NIS2 QM te halen**
- **Wij ontwikkelen partnerships met de MSP community in NL om alle bedrijven naar een hogere veiligheid te bewegen. Technisch maar ook qua interne veiligheid en de leverancierssketen.**

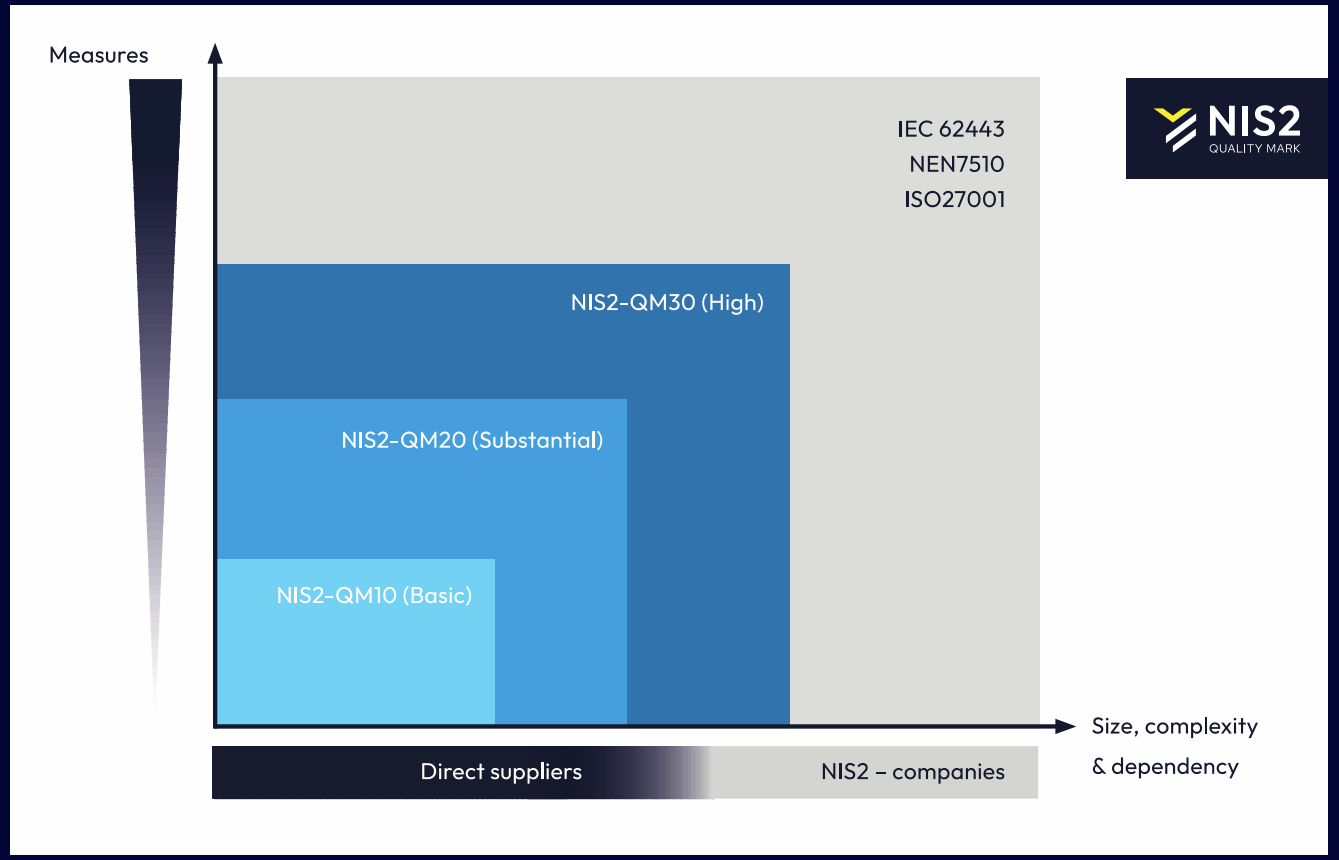
Samen Digitaal Veilig

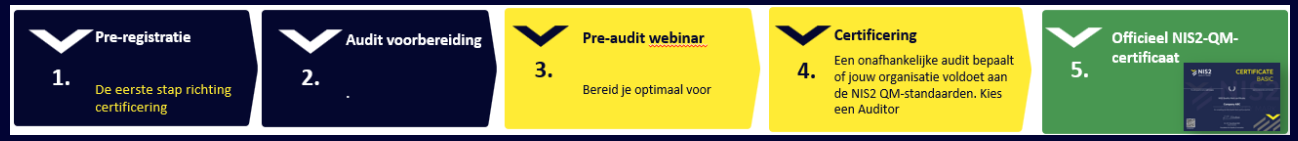
Bij risico passende niveaus

- NIS2 Quality Mark kent 3 niveaus, afgestemd op het belang en de omvang van de organisatie

NIS2 QUALITY MARK

- NIS2-QM-10 (Basic)
- NIS2-QM-20 (Substantial)
- NIS2-QM-30 (High)





GAP NIS2 met ISO27001/NEN7510

Veel organisaties denken dat ze compliant zijn zodra ze bijv. ISO27001 of NEN7510 hebben behaald. Maar dat is een misvatting.

Er zijn belangrijke verschillen geïdentificeerd, zoals:

- ✓ Registratieplicht
- ✓ Meldplicht
- ✓ Opleiding directie
- ✓ Strategisch plan inclusief handtekening directie
- ✓ Onder toezicht van een toezichthouder (vanuit de overheid dus)
- ✓ De leveringsketen is veel zwaarder qua controle en compliance voor jullie (zorgplicht)

Er zijn ook 15 (ook technische) verschillen met ISO27001.

Samen Digitaal Veilig

Partners

- Deelnemende Brancheverenigingen adviseren hun leden het Samen Digitaal Veilig platform te gebruiken voor concrete to-do-lijsten én een uitgebreide NIS2 ketenvragenlijst en webinar ondersteuning.

+

- Kennispartners 'verkopen' SDV licenties en leveren diensten en producten (Consultancy, PEN-testen, audits, EDR-oplossingen, scanservices en andere cyberproducten en -diensten.)

Samen Digitaal Veilig

Samen Digitaal Veilig

MSP's: meer druk, meer verantwoordelijkheid

Managed Service Providers krijgen te maken met steeds zwaardere eisen op het gebied van cybersecurity. Daarnaast moeten ze zowel hun klanten adviseren en ondersteunen als controle houden over hun leveranciers. De zorgplicht groeit aan alle kanten. Steeds meer bedrijven vertrouwen op MSP's, wat extra druk legt op professionalisering en standaardisatie van hun dienstverlening.

Heel veel toezichthouders

Toezichthouders gaan zich nadrukkelijker richten op alle MSP's. Zij worden gezien als vitale schakels. Toezichthouders: De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Leefomgeving en Transport (ILT), Inspectie van het Onderwijs (IvhO), Nederlandse Voedsel- en Waren Autoriteit (NVWA), Autoriteit Persoonsgegevens (AP) en Rijksinspectie Digitale Infrastructuur (RDI).

Beperkte certificering in de sector

De meeste MSP's beschikken nog niet over een passende certificering zoals bijv. het NIS2 Quality Mark. Hierdoor kunnen zij hun naleving van wet- en regelgeving moeilijk aantonen. Dat maakt hen onnodig extra kwetsbaar – zowel richting klanten als toezichthouders.

Audits en control zijn belangrijk

Regelmatige audits of pentests zijn van groot belang voor MSP's. Hierdoor laat je zien dat systemen en processen goed beveiligd zijn. Die toetsing is essentieel om aan te tonen dat je je zorgplicht serieus neemt.

Voorkom reputatieschade door NIS2QM certificering

Cyberincidenten bij klanten kunnen leiden tot juridische claims, financiële schade en omzetverlies. Maar ook reputatieschade ligt op de loer. Behoud het vertrouwen van je klanten en zorg er als MSP voor dat je je cybersecurity op orde hebt, via de NIS2-QM certificering.

ENISA adviseert Nationale overheden: Neem MSP's onder de loep

Het Europese agentschap ENISA adviseert EU-landen expliciet om speciale aandacht te hebben voor MSP's. Hun toegang tot klantdata en systemen maakt hen kwetsbaar én belangrijk. Ook MSP's die niet rechtstreeks onder NIS2 vallen, krijgen hier mee te maken.

Zorgplicht richting leveranciers

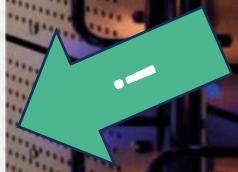
MSP's moeten onder NIS2 ook hun toeleveringsketen — de leveranciers — beoordelen op risico's. Structurele controle op deze partijen is vaak nog niet ingeregeld. Daardoor kunnen onzichtbare zwakke schakels in de keten ontstaan. Zonder toetsing of duidelijke beveiligingsafspraken levert dat grote risico's op.

Juridisch risico groeit

Zonder aantoonbaar beleid, aantoonbare zorgplicht, goed ingeregelde interne processen en juiste certificering lopen MSP's steeds meer risico om juridisch aansprakelijk te worden gesteld voor beveiligingsproblemen. Voorkom dit. Neem nu de juiste stappen.

Zorgplicht richting mkb-klanten

Veel mkb-klanten gaan ervan uit dat hun MSP alle digitale veiligheid regelt. Als zich een incident voordoet, wordt de verantwoordelijkheid vaak bij de MSP gelegd – ook wanneer de klant zelf niets heeft geregeld. Dit vergroot het aansprakelijkheidsrisico van de MSP aanzienlijk. Aantoonbaar je zorgplicht regelen wordt essentieel.



www.samendigitaalveilig.nl

Zorgplicht communicatie ....

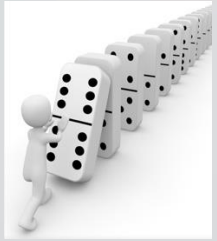
- **Wat is nodig?** Zorgplicht moet je doen zonder sales push en bestaat uit een reeks van (juridische) zorgplicht communicatie naar je klant(en)

Stap 1:
Brief op papier aan directie met zorgplicht over Cyberveiligheid

Stap 2

‘Zorgplicht communicatie reeks’ (niet commercieel van aard)
Minimaal 3 tot maximaal 6 mails

Stap 3:
Zorgplicht reeks afsluiten met gesprek/eindbrief directie + de keuze voor ondertekening aanbod incl. certificering of Vrijwaringsverklaring



Samen Digitaal Veilig




IT is niet langer ondersteunend aan de business.
IT is de business

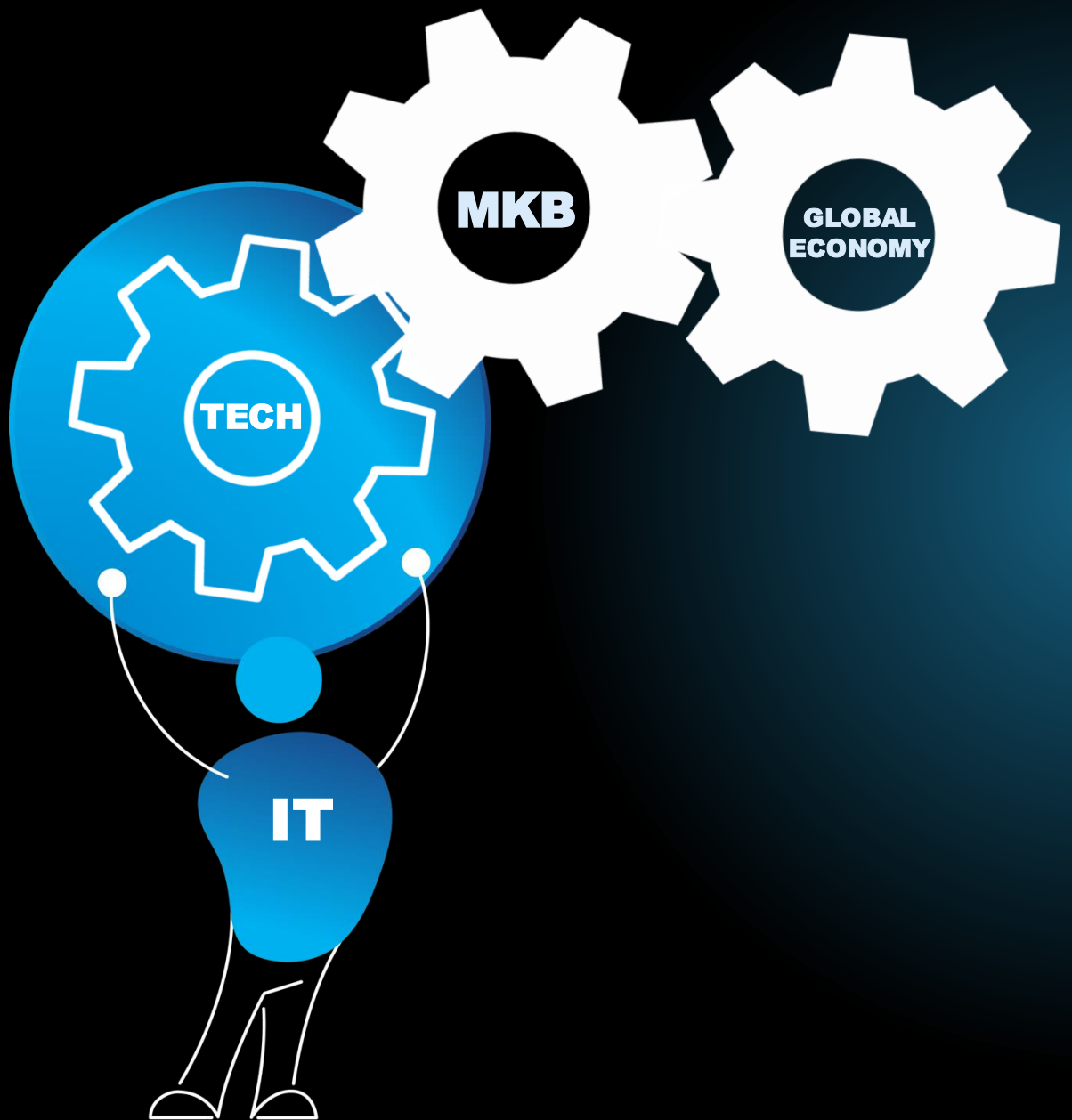



MKBs zijn de ruggengraad van onze global economy

90%

van de wereldwijde ondernemingen zijn MKB organisaties

- Funtioneren niet zonder digitale tools
- Focussen op eigen onderneming
- Geen expertise in technisch beheer



MKB organisaties zijn afhankelijk van MSPs of kleine IT teams.

Jullie zijn de onbezongen HELDEN van de economie

De multi-functionele IT expert moet alles doen met...

TEVEEL TOOLS
van verschillende vendoren

KRIMPENDE BUDGETTEN
en andere bronnen

MEER WERKDRUK
en gebruikersvragen

Gefragmenteerde tools
beperkt de efficiency
en hindert jullie
prestaties.

Kaseya 365

Jullie alles-in-een platform to GET *IT* DONE.

MSP

Markets

Consolidation

Managed Services vs Project

Emerging MSP’s

Regional/International

Platform vs. Tools

Security

Co-Managed

Compliance

NIS2

SMB

MKB

Cyber Resilience

Non-IT

Value vs. Perceived Value

NIS2

Engine Economy

Digitally integrated

Sales Challenges

“The winners of tomorrow sell based on strategic impact, cost control, reduced risk and efficiency”- Robin Robins

Differentation / Positioning

Thought Leadership

Managed Services vs Build your own

Business Value vs. Tech

Compliance as a service

Stakeholder Management

Leadgen

Churn / Upsell / Cross-sell / Self service

Market is maturing

Sector / legal (DORA/NIS2 etc)

Boutique vs. Scale

Business outcomes / ROI / scalability

Create sense urgency

What’s in it for who

How to reach them and how to make them switch

The right mix / focus / strategy

Portfolio

Maatregelen	Klant	Partner	Samen		Portfolio
4.1 Beveiliging en beheer gebruikersapparaten				V	EDR PW Managers Encryption EMM Vulnerability management Hardening
4.4 Bestrijding en preventie van malware				V	Antivirus, EDR E-mail security Security awareness Encryptie Firewalling
4.5 Informatiebehoud: back-up en herstel				V	Advisory (plannen) Backup (on premise) Backup (cloud)
4.7 Software op computers en apparaten up-to-date houden				V	Asset Inventory Vulnerability scanning Risico bepalen Patching, updates, hardening
4.9 Netwerksegmentatie: regels vast stellen en toepassen voor het segmenteren van groepen gebruikers, informatiesystemen en informatiediensten				V	Advisory: architectuur, Zero Trust Firewall, Microsegmentatie
4.10 Authenticatie op cruciale systemen				V	IAM Multi Factor Authenticatie Solutions
4.11 Logbestanden: logbestanden van relevante gebeurtenissen registreren en analyseren				V	Logmanagement SIEM NDR MDR, XDR SOAR SOC

Samen Digitaal Veilig en Kaseya portfolio

- Samen Digitaal Veilig heeft een simpel platform om (gedeeltelijk) compliant te zijn/worden/aan te kunnen bieden.
- 3 Quality Marks, welke ‘ben ik’?
  - 10 – Basis – elke organisatie zou dit moeten naleven
  - 20 - Belangrijk – als jouw klant slechte alternatieven heeft
  - 30 - Essentieel – als jouw klant geen alternatief heeft
- Op weg naar NIS2 / IEC 64443 / NEN 7510 / ISO 27001 compliance

Quality Mark 10 (QM10)

Basis beveiliging van organisatie, informatie en bedrijfsmiddelen

Term regel	Product/Suite
Backup	Kaseya 365 Endpoint (backup), Kaseya 365 User (SaaS backup), Datto BCDR
Keten beveiliging	Compliance Manager GRC
Overzicht/inzicht bedrijfsmiddelen	Kaseya 365 Endpoint (RMM), PSA (Assets)
Educatie bestuurders	Kaseya 365 User (BullphishID)
Registratie/rapportage incidenten	Kaseya 365 Endpoint Pro (EDR/SOC)
Bestrijding/voorkoming malware	Kaseya 365 Endpoint (EDR, AV, DNS Filtering)
Updates van OS/applicaties	Kaseya 365 Endpoint (Patch Management, Advanced Software Management), optioneel Vulscan en vPentest

Quality Mark 20 (QM20)

Alles van QM10 maar met extra maatregelen

Term regel	Product/Suite
Bescherming informatie van de keten	Compliance Manager GRC
Voorbereiding bedrijfscontinuïteit	Datto BCDR, Unitrends, reguliere backup
Acceptabel gebruiken bedrijfsmiddelen, inleveren bedrijfsmiddelen,	IT Glue
Verzamelen bewijsmateriaal incidenten	Kaseya 365 Endpoint Pro (MDR)
Security beleidstraining	Kaseya 365 User (BullphishID)
Netwerk segmentatie	Datto Networking, Datto Secure Edge

Quality Mark 30 (QM30)

Alles van QM20 maar met extra maatregelen

Term regel	Product/Suite
Informatiebeveiliging mbt leveranciers	Compliance Manager GRC
Evaluatie mbt leveranciers	Compliance Manager GRC
Geheimhouding samenwerking	IT Glue
Cryptografie/versleuteling van data	K365 Endpoint (RMM), K365 User (SaaS Alerts), Network Detective Pro
Overzichten geleverde apparatuur/oplossingen	Autotask PSA, RMM, IT Glue, Network Detective Pro
Bewustwording InfoSec	Kaseya 365 User (BullphishID)
Testen van de beveiliging omgeving	Vulscan, Vonahi (pentest)
Uitgebreidere segmentatie netwerk	Datto Networking (DNA, Switch, AP, Secure Edge)