

NIS2

VAN PLAN NAAR PRAKTIJK

Mathijs van Pieterse & Tjeerd de Snoo



De kans dat uw organisatie wordt getroffen door een cyberaanval is vele malen groter dan dat er brand uitbreekt in uw pand.

Toch hebben we brandblussers, een evacuatieplan en verzekeringen tegen brand... maar hoe goed zijn we eigenlijk voorbereid op digitale aanvallen?

Wie doet er jaarlijks een brandoefening?

Wie doet er jaarlijks een cyberincident oefening?

Wat is NIS2?

- Europees
- Is het al verplicht?
- NIS2 t.o.v. NIS1
- Meer sectoren
- Strengere eisen
- Boetes

 Registratieplicht

 Zorgplicht

 Meldplicht

Waarom NIS2?

Wat is het doel van NIS2?

- Digitale weerbaarheid versterken
- Voorkomen van grote cyberaanvallen
- Duidelijke regels voor bedrijven

Is NIS2 belangrijk?

- Je moet eraan voldoen
- Samenwerken met leveranciers en partners om de hele keten veilig te maken.
- Boetes zijn hoog bij niet naleven

Valt mijn organisatie er ook onder?

NIS2 geldt voor veel organisaties in vitale sectoren.

Denk aan **transport, zorg, digitale diensten en logistiek**.

Ben je leverancier voor deze sectoren? Dan val je er vaak ook onder.

Hoe weet je of je erbij hoort?

- Kijk naar je sector
- Check het aantal werknemers en je omzet
- Essentieel of belangrijk? Dan moet je aan de slag!

Let op:

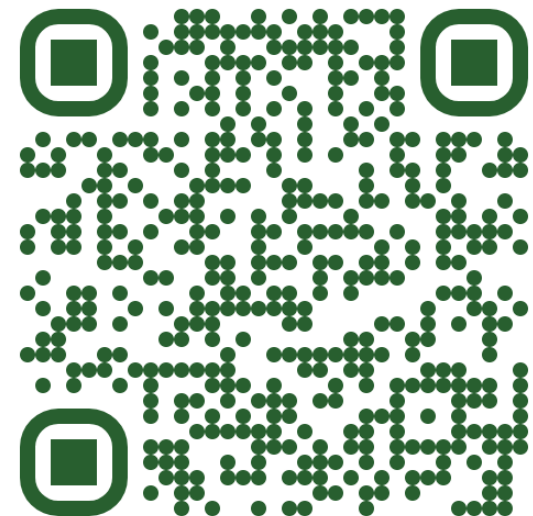
Val je hieronder?

Dan ben je verplicht je te registreren als NIS2-entiteit.

Dit is geen keuze!

De registratieplicht geldt voor iedereen die eronder valt.

Twijfel je? Check of jouw organisatie onder NIS2 valt en neem actie:



Waar beginnen we?



Interactie: Wie denkt dat NIS2 een IT-feestje is?



NIS2 is niet alleen een IT-feestje is. Iedereen in de organisatie heeft een rol.



Interactie: Is alleen techniek genoeg om veilig te zijn?



De meeste incidenten ontstaan door menselijk gedrag, niet door techniek

Zo pak je het aan

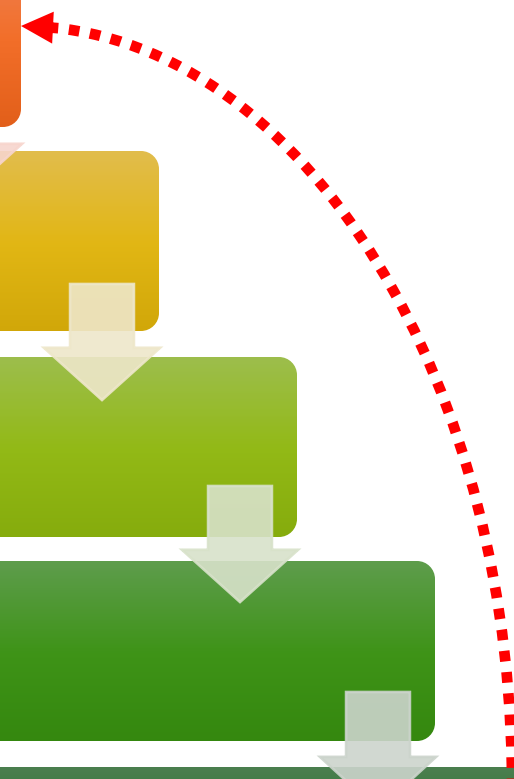
Maak een overzichtelijke tijdlijn of stappenplan.

Risico's in kaart brengen.

Vastleggen en borgen.

Medewerkers trainen en bewust maken.

Aantoonbare compliance organiseren.



Risico's in kaart brengen

Bepaal wat je wil beschermen

- Denk aan klantgegevens, unieke kennis/patent, je reputatie of continuïteit

Breng risico's in kaart

- Kijk naar interne én externe risico's, zoals fouten, cyberaanvallen of leveranciers.

Analyseer de risico's

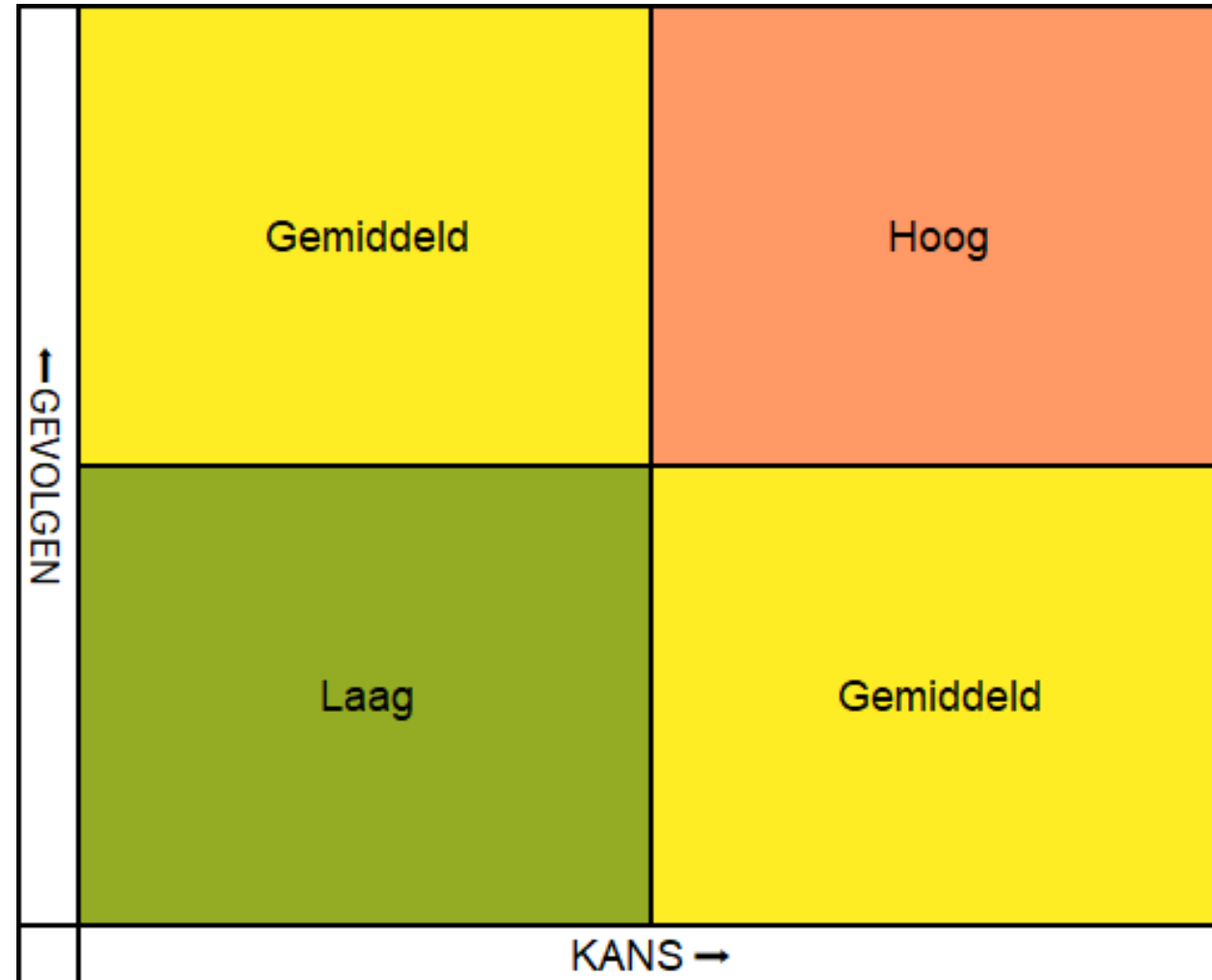
- Hoe groot is de kans dat het gebeurt? Wat zijn de gevolgen?

Maak keuzes

- Accepteer, beperk, verzeker of stop het risico.

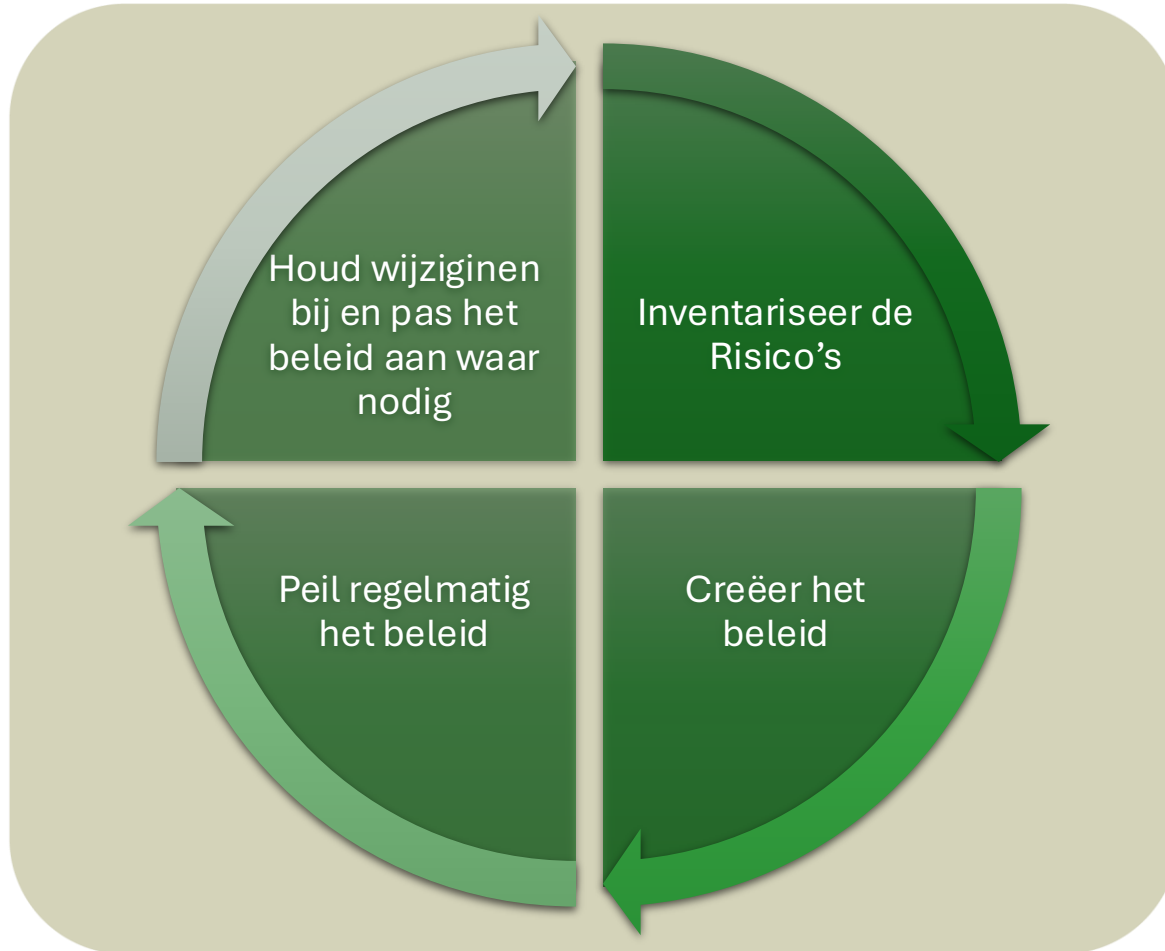
Voorbeeld:

bedrijfskritiek planningsysteem in de Cloud



Persoonlijk betrokken

Vastleggen en borgen



- Gebruik een risico-checklist
- Maak samen een lijst van systemen en data
- Breng leveranciers in kaart
- Noteer wie toegang heeft en wie verantwoordelijk is
- Wijs een verantwoordelijke binnen je organisatie aan
- Plan korte sessies voor beleid
- Stel een vast meldpunt voor incidenten in
- Bespreek beveiliging en updates elke maand.

Valkuilen



Alleen in techniek denken:

Denken dat techniek alleen genoeg is, zonder aandacht voor mensen en processen.



Geen duidelijke rollen:

Geen duidelijke afspraken maken over wie wat doet bij een incident.



Leveranciers & partners vergeten:

Vergeten om leveranciers en partners te betrekken bij je beveiligingsmaatregelen.



Alleen reageren, niet proactief voorkomen:

Alleen reageren als er iets misgaat, in plaats van vooraf risico's te bespreken.

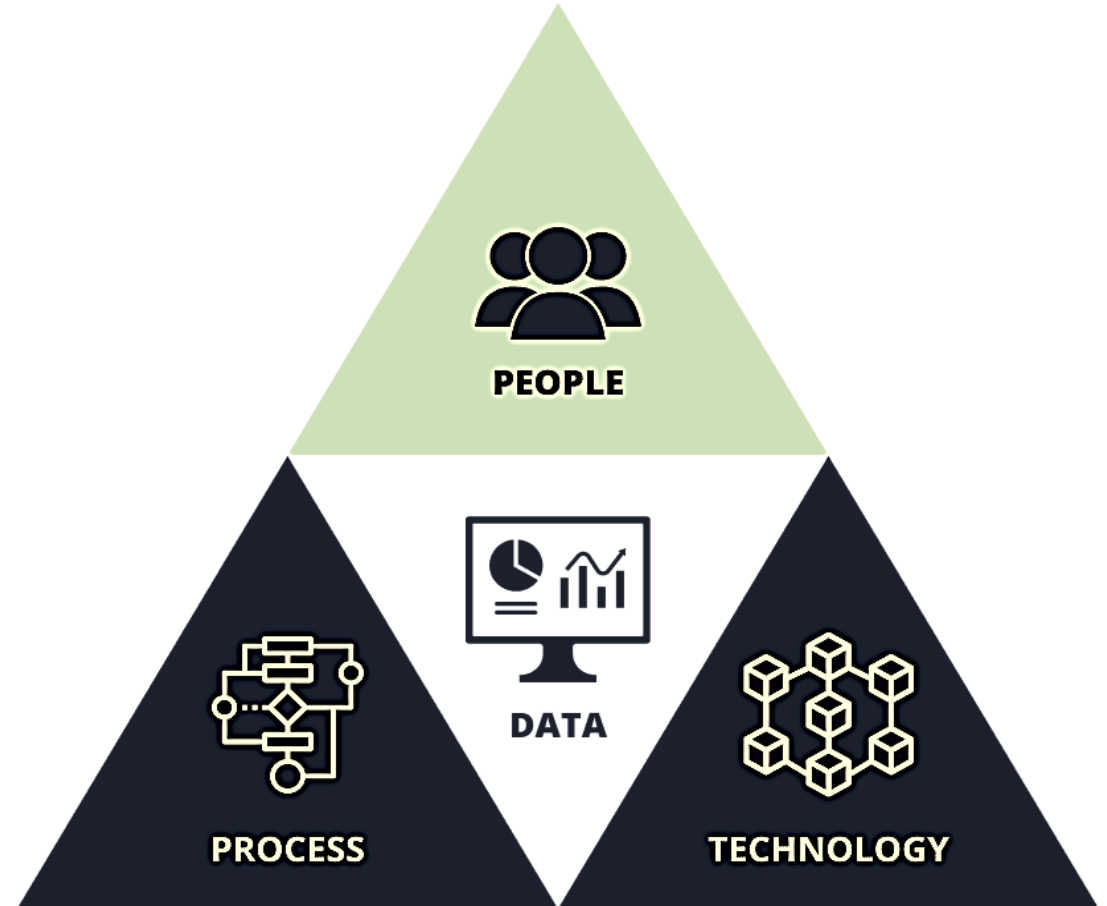


Set and Forget:

Geen vaste momenten plannen om beleid en maatregelen te herzien.

Eindresultaat

- Je weet waar je risico's zitten.
- Je weet waar je data staat.
- Je onderneemt sneller actie bij een cybersecurity incident
- Je voldoet aantoonbaar aan de NIS2-richtlijn
- Je laat aan klanten en partners zien dat je cybersecurity serieus neemt



Persoonlijk betrokken

**Doe de zelftest online
Plan een sessie met Symbis!**

Één ding is zeker! NIS2 maakt duidelijk:

**Cyberveiligheid is geen keuze meer,
het is een plicht.**