Als accountantskantoor grip krijgen op informatiebeveiliging in de praktijk

INTRODUCTIE

- Reindert Doorn
- Adviseur IT & Verandermanagement bij DOCCO
- Digitale transformaties bij accountantskantoren
- Specialisatie privacy & security

INTRODUCTIE

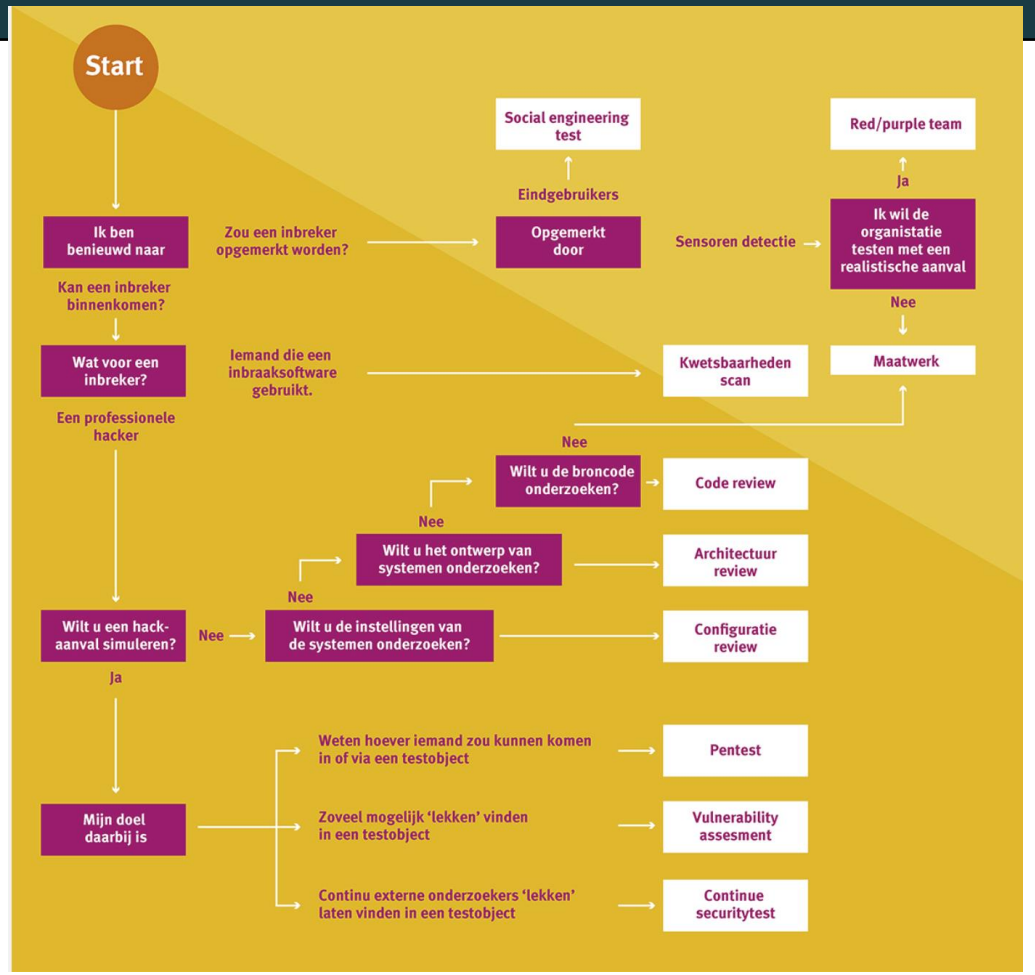
- Niet over klanten, continuïteit, waardering, dienstverleningskansen, maar het eigen kantoor

INTRODUCTIE

- We doen maar wat in de praktijk!
- Naar beste inzicht:
  - Met beperkte middelen
  - Met beperkte kennis die voorhanden is
- Geen onwil… urgentie = bekend

INTRODUCTIE

- We schakelen hulp in
- Aantal cybersecuritybedrijven verdubbeld!
- Losse ‘flodders’?



INTRODUCTIE

- We doen maar wat, omdat een raamwerk ontbreekt!
- We houden grip op…

WIE HEEFT ER WÉL VOLDOENDE GRIP?

BELANG / WAARDE

- Waarom van belang

BELANG / WAARDE

- Waarom van belang

Onderwerp: ICt- en beveiligingsbeleid

Hoi [redacted]

In het kader van onze cyberverzekering komt de vraag naar boven of ons ICT/Beveiligingsbeleid is vastgelegd en of we deze regelmatig testen.

Nu hebben we volgens mij de juiste maatregelen wel getroffen maar natuurlijk niet in een handboek vastgelegd.
Ik heb het idee dat jullie dat bij Docco wel vaker tegenkomen en er wellicht iets mee hebben gedaan.

Heb je binnenkort tijd om hier over te praten?

Met vriendelijke groet,

BELANG / WAARDE

- De waarde
  - Risicogerichte aanpak

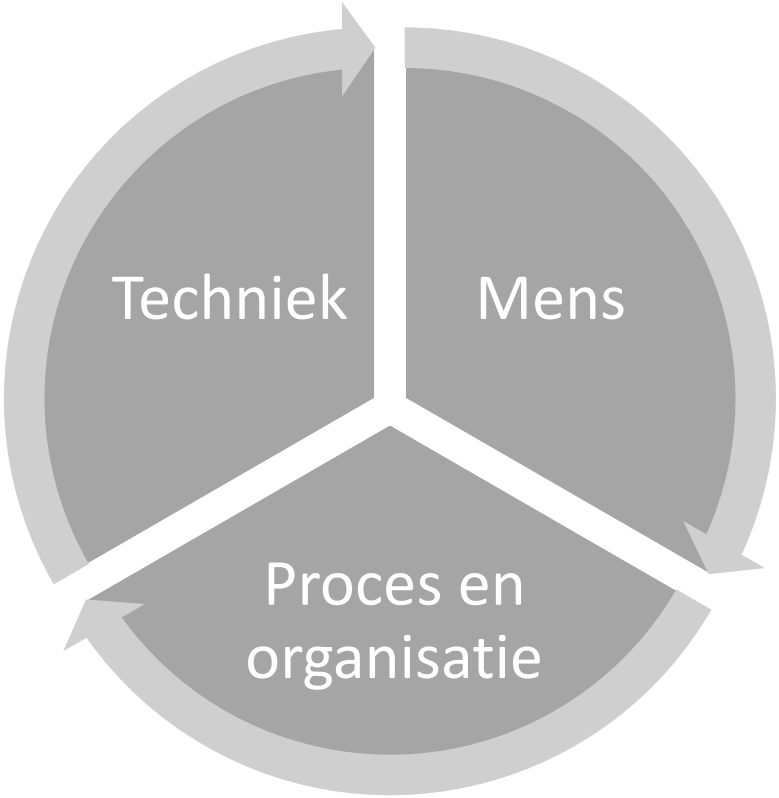
Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland

CSBN 2021

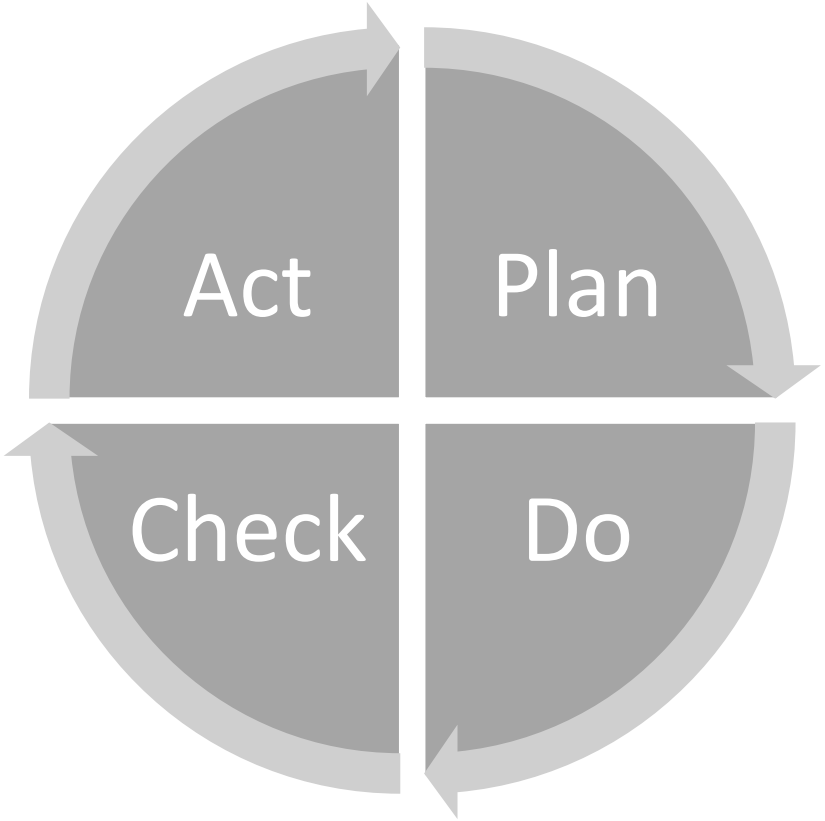
BELANG / WAARDE

- De waarde
  - Holistische aanpak



BELANG / WAARDE

- De waarde
  - Continue proces



EEN ISMS ALS BASIS

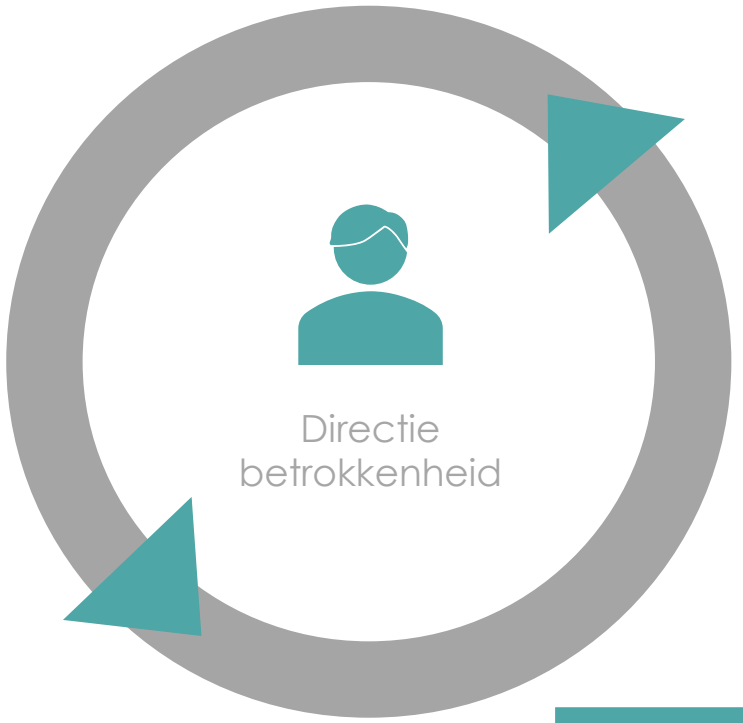
EEN ISMS ALS BASIS

- Informatiebeveiligings-management systeem
- Structuur voor beheersing
- Waardevol raamwerk:
  - Risicogedreven, continue verbetering
- ISMS is opstapje naar auditing/certificering
- ISO27001: certificering over opzet, bestaan en werking ISMS

ISO27001

- Certificeerbare norm (-/+ accreditatie)
- Internationale standaard en erkenning
- Maatregelen en best practices: ISO27002
- Add-on voor AVG: ISO27701
- Update raamwerk ‘21/’22
- Waarborg waar steeds meer partijen op steunen / om vragen
- Basis hygiëne? Geen summum

Basisbeginselen



Context

Aanpak

Risico & behandeling

Maatregelen kiezen
techniek – proces - mens

Procedures & beleid
opstellen/afspreken

Continuïteits-
maatregelen

Verbeteren

Herbeoordeling

Evalueren

Testen en reviews

Voortdurend bijhouden

Incidenten

Actuele lijst ‘assets’

Basisbeginselen

- Voordat ik verder ga…
- Duur?
- Een basis Excel template kan al waarde hebben!

Basisbeginselen

- 1: Denk vooraf na over de context

- Organisatiecultuur/leiderschap
- Actieplan/planning/resources
- Vaardigheden en competenties

Basisbeginselen

- 2: Benoem de grootste risico's

- Welke bedreigingen vormen een risico
- Kans * Impact
- Waar is actie op nodig (maatregelen)
- Restrisico

- www.digitaltrustcenter.nl/risicoklasse

Basisbeginselen

- 3: Kies en neem maatregelen

- Vanuit risicoanalyse
- Lijst met maatregelen (Rapport DTC, lijsten NBA, e.a.)
- Start met max. 20!
- Techniek, proces én mens
- Moet na verloop van tijd veranderen – stand der techniek

Basisbeginselen

- 4: Bepaal waar je afspraken over wilt maken

- Beleid/procedures, vb.
- In/uit dienst, toekennen rechten
- On/offboarding klanten
- Backups
- Omgang met wachtwoorden

Basisbeginselen

- 5: Houd overzichten bij

- Houd zicht en grip
- Leverancierscontracten (!)
- Apparaten, servers, certificaten, MFC’s
- Verantwoordelijken benoemen

Basisbeginselen

- 6: Houd overzichten bij

- Incidenten, ook niet datalekken
- Oorzaak, correctieve en preventieve maatregelen

Basisbeginselen

- 7: Werk aan voortdurende verbetering (I)

- Periodieke bespreking (directie)
- Herbeoordelen risico's en maatregelen

Basisbeginselen

- 7: Werk aan voortdurende verbetering (II)

- Voortdurende bewustwording
- Technische testen
- Interne en externe audits (bij certificering)

Basisbeginselen

- 8: Werk aan continuïteitsmanagement

- In iteratie II
- Handelingsplan
- Oefening
- Evaluatie - verbetering


WELKE VRAGEN STEL JIJ

Let op de keten

- Advies NCSC voor aandacht
- Normen als ISO en verordeningen als AVG haken in op ketenbelang
- Steeds meer incidenten in de keten door grote kwetsbaarheden
- Uitbesteden is niet verantwoordelijkheid verleggen
- Keten steeds complexer

Bedrijf onderschat cyberrisico's ketenpartners

15 juli 2021 14:32 | Pim van der Beek

Topic Security

Security-incidenten bij leveranciers en aanvallen op de software van partners vormen vaak een groot risico voor de eigen organisatie. Toch ziet maar één op de vijf bedrijven de mogelijke impact van die cyberrisico's in. Dat is de uitkomst van de Ordina Digital Monitor 2021.

Onderzoeksbureau Markteffect ondervroeg voor de Ordina Digital Monitor 2021 ruim twaalfhonderd ict-besluitvormers uit Nederland. Het onderzoek spitste zich dit jaar specifiek toe op cybersecurity.

Slechts één op de vijf ict-besluitvormers (22 procent) schat de risico's op een hack of datalek door leveranciers en software als 'groot' of 'zeer groot' in. Specialist in de beveiliging van bedrijfsinformatie, Vincent Meijer, noemt dat een 'verontrustend laag percentage'. Hij licht toe dat hacks en datalekken 'helaas' dagelijkse kost zijn.

'Organisaties richten zich steeds vaker modulair in om op de wensen en behoeften van de markt in te spelen. Zij worden zo afhankelijker van allerlei softwareoplossingen van verschillende leveranciers, die integraal onderdeel zijn van de keten. Die ketens worden groter, complexer en daarmee ook kwetsbaarder', aldus de expert van Ordina.

Kaseya en Solarwinds

Meijer wijst er op dat door de onderlinge verbondenheid het risico ontstaat om elkaar, in het geval van een incident, te besmetten.

Let op de keten

- Beveiligingsniveau bij de ander = beveiligingsniveau bij jou!
- Kritischer kijken, waarborgen vereisen
- Vragen om te stellen / Afspraken maken met IT-leverancier
  https://www.digitaltrustcenter.nl/sites/default/files/2020-06/handreiking_afsprakenmetITleverancier_DTC.pdf
- Voer alsnog gesprek / controleer afspraken indien eerder onvoldoende aandacht voor was

Jullie kunnen dit!

- Risicobeheersing
- Opzet, bestaan, werking / auditcycles
- Laat mes aan twee kanten snijden:

  kansen in de klantrelatie!

Bedankt!

- Handige Excel template ontvangen?
- reindert@docco.nl