



Gemeente
De Ronde Venen

Rondetafelgesprek Informatiebeveiliging

15 juni 2023



Doel van deze ronde tafelsessie

- ▶ Met elkaar in gesprek over
 - ontwikkelingen op het gebied van informatiebeveiliging
 - Impact op het werkveld van informatieveiligheids professionals (CISO, PO, FG Informatiebeheer)
- ▶ Ontwikkelingen schetsen door Key2Control
- ▶ Bespreken wat de impact daarvan is aan de hand van een aantal stellingen



Gemeente
De Ronde Venen

Even voorstellen

- ▶ Patrick Zuiderwijk
- ▶ Nu sinds 5 jaar CISO en ENSIA coördinator
- ▶ Gemeente De Ronde Venen
In het Groene Hart, tussen Utrecht en Amsterdam
Mijdrecht, Abcoude, Wilnis, Vinkeveen, enz...
- ▶ Onderdeel van team Concerncontrol
samen met FG, VIC'er, controllers en CFO.



Inleiding

- ▶ Gebruiken nu zo'n 7 jaar Key2Control
- ▶ Begonnen met de BIG (ISMS)
Later BIO, Privacy (AVG) en WPG
- ▶ Recent besloten om uit te breiden met de andere normenkaders en onderdelen (risico en audit) van K2C
- ▶ Beginnen met de KIDO (Informatiebeheer, Archief)



Gemeente
De Ronde Venen

Uitdagingen voor elke CISO de komende jaren

- ▶ Nieuwe NIS2 wet (aansprakelijkheid, certificering, opleidingen, ketenafhankelijkheden)
- ▶ Audits op werking
- ▶ De buitenwereld bijhouden (oa zeroday's, en de onbeperkte middelen van hackers)



Gemeente
De Ronde Venen

Uitdagingen binnen onze gemeente

- ▶ Meekrijgen van de groep afhakers
- ▶ Uitbreidingen van ENSIA onderwerpen
- ▶ Kwetsbaarheden in de keten

Even voorstellen

Gerrit Goud

- 30 jaar ervaring als registeraccountant (RA)
- 20 jaar ervaring als IT auditor (RE)
- Senior consultant
- Actief bij gemeenten, gemeenschappelijke regelingen
- Focus op interne beheersingsvraagstukken op het gebied van informatiebeveiliging, privacybescherming (AVG en Wpg), bedrijfscontinuïteit, financiële- en fiscale rechtmatigheidsverantwoording



**Welke ontwikkelingen op
het gebied van
informatieveiligheid hebben
nú jullie aandacht?**

Ontwikkelingen IB/Cyberbeveiliging

- Toename digitaal dreigingsbeeld → ransomware is grootste
- Risicoparagraaf begroting → is dit risico opgenomen?
- Relatie CISO en CFO versterken. CISO heeft veelal geen budget. CFO gaat immers over financiële risico's/middelen
- Europese reactie → NIS2-richtlijn: zorgplicht, meldplicht en toezicht
- Nederlandse wetgeving → Wet Digitale Overheid (WDO) 1^e tranche: BIO of opvolger wordt wettelijk verankerd

Gemeenten ontkomen niet aan de NIS2 richtlijn, toch?

Er is thans onduidelijkheid

bestuur en organisatie financiën ruimte en milieu sociaal **digitaal** carrière juridisch

Binnenlands Bestuur

digitaal / nieuws

Zorgen over impact Europese richtlijn NIS2 op gemeenten

Gemeenten hebben snel duidelijkheid nodig over het opnemen van de Europese cyberrichtlijn NIS2 in de nationale wetgeving.

Marjolein van Trigt 05 juni 2023

Netwerk- en informatiesystemen (NIS2)

- Is van toepassing op overheidsdiensten, wat valt daaronder?
- In het wetsontwerp zijn gemeenten opgenomen
- Gaat ook over procesbesturingssystemen. Denk aan sluizen, bruggen, gemalen, (IoT)
- Richtlijn wordt vertaald naar Nederlands recht
- Eind 2024 van kracht (nieuwe Wbni)
- Toezicht door onafhankelijke autoriteit
- Boeteregime (vergelijkbaar met AVG)



NIS2-richtlijn: wat zijn gevolgen?

- Doel: Europa digitaal veiliger maken door digitale weerbaarheid te vergroten
- Weerbaarheid: van administratief naar feitelijk beveiligen → risicogebaseerde benadering, testen werking (opzet, bestaan en werking)
- ISMS verder professionaliseren, zorgdragen voor hoge adoptie. BIO of opvolger blijft de basis
- Verdiepingsslag op kritische informatiesystemen
- Verder professionaliseren FAB op kritische informatiesystemen
- BCM: mede tot doel om gevolgen van cyberincidenten te verkleinen → BCMS
- Incidentenbehandeling → meldingsvereisten naar toezichthouder en landelijk CSIRT ingeval sprake is van cyberincident

**Om informatiebeveiliging
serieus te nemen moeten
overheidsorganisaties zich
verplicht laten certificeren
op ISO27001**

Is ISO-certificering antwoord op NIS2?

- Uit BIO-evaluatie blijkt onder CISO's een sterke behoefte voor certificering. Is een kwaliteitskeurmerk, geen assurance
- ISO-27001 is een internationale standaard. BIO is daarvan afgeleid
- Alle provincies hebben in 2018 besluit genomen ISO gecertificeerd te zijn in 2023. Een aantal voldoen al aan deze eis
- Gemeenten hebben te maken met ketenpartners die wel ISO-gecertificeerd zijn. Zij hebben ook behoefte aan vertrouwen. ENSIA is daarop niet het antwoord!
- Onze software is voorbereid op ISO-certificering



Gemeente
De Ronde Venen

Dank voor jullie inbreng en aanwezigheid!