INFORMATIE
BEVEILIGINGS
DIENST

# NVRR workshop/presentatie Jaarcongres
# De controle van de effectiviteit van informatiebeveiliging

Kees Hintzbergen

INFORMATIE
BEVEILIGINGS
DIENST

# Agenda

- Voorstellen
- Vragen!
- Wat is dat eigenlijk: risico?
- Hoe ziet de ideale wereld eruit?
  - Vanuit de CISO en vanuit de manager
  - Wie is verantwoordelijk?
  - Waarnemingen
- Een beetje BIG
- Privacy en ENSIA
- Onderzoeksvragen
- Vragen?

INFORMATIE
BEVEILIGINGS
DIENST

# Introductie

- Medeauteur van de BIG (2012)
- Medeauteur van de BIR2017
- Auteur van de BIO (heden)
- Medeauteur van diverse BIG-OP producten
- CERT/Helpdesk-medewerker IBD
- projectteamlid expert ENSIA
- Deelneming aan diverse overlegstructuren

INFORMATIE
BEVEILIGINGS
DIENST

# Doelen van de IBD

De IBD heeft drie concrete doelen. Hierbij staat kennisontwikkeling, kennisdeling en kennisvermeerdering op het vlak van informatiebeveiliging bij gemeenten centraal:

1. **Bewustzijn**

   het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.

2. **Preventie, detectie en coördinatie**

   het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.

3. **Projecten**

   het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen.

INFORMATIE
BEVEILIGINGS
DIENST

# Enkele vragen

INFORMATIE
BEVEILIGINGS
DIENST

# Enkele definities

- Definitie: Risico = kans * impact van een dreiging
- Dreiging: iemand kan onbedoeld kennis nemen van X
- Kans: laag
- Impact: hoog
- Risico: de kans dat iemand onbedoeld kennis kan nemen van X en de schade die dan ontstaat

- Dus een dreiging zegt op zichzelf nog niets of iets een laag of hoog risico is. Alleen de kans op en de impact als het gebeurd zegt wat.

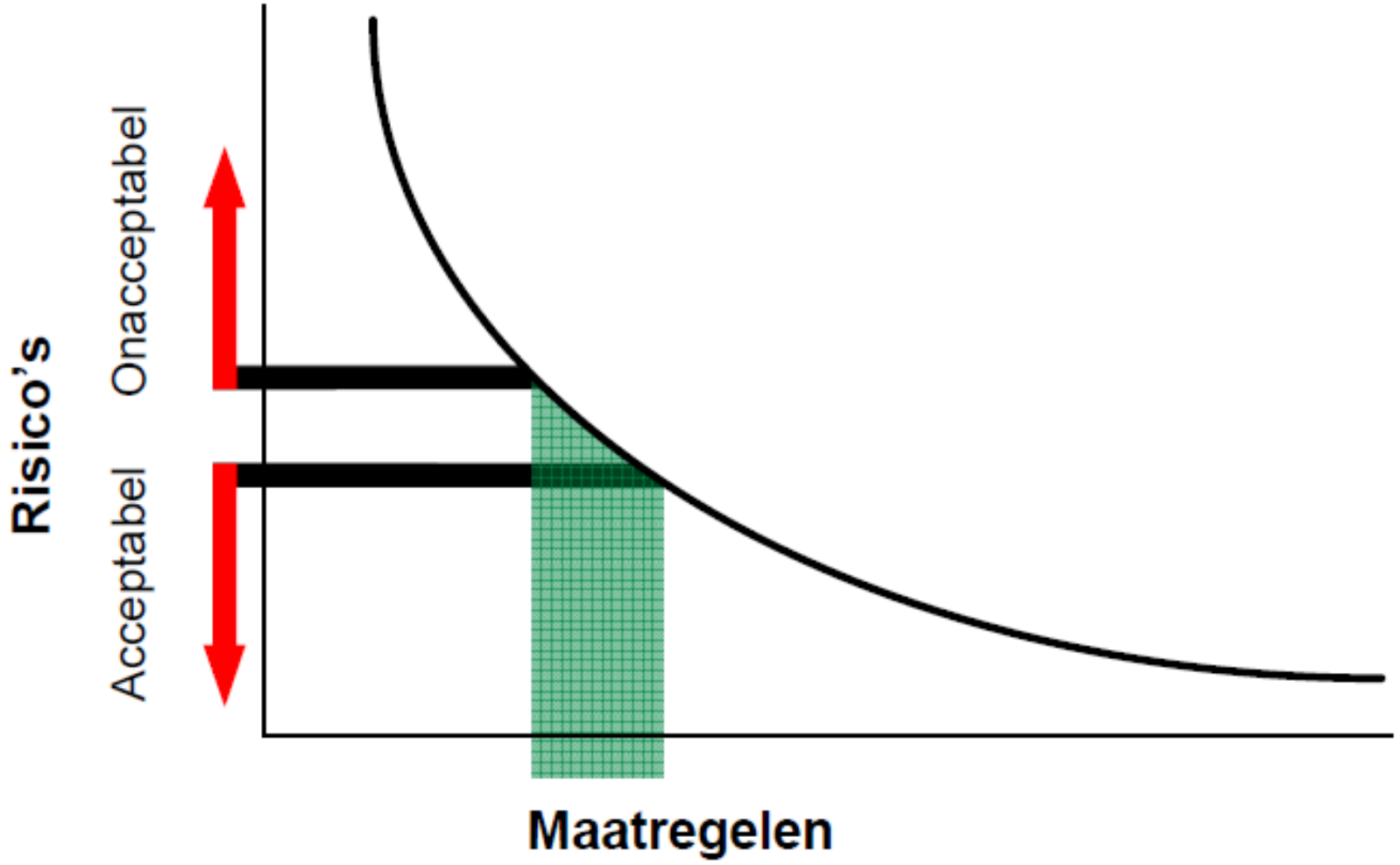
- Risicoanalyse versus Baseline

INFORMATIE BEVEILIGINGS DIENST

# Risico's en maatregelen

Waar gaat het hier om?

Bestuurders hebben een andere risico perceptie en acceptatie dan de CISO



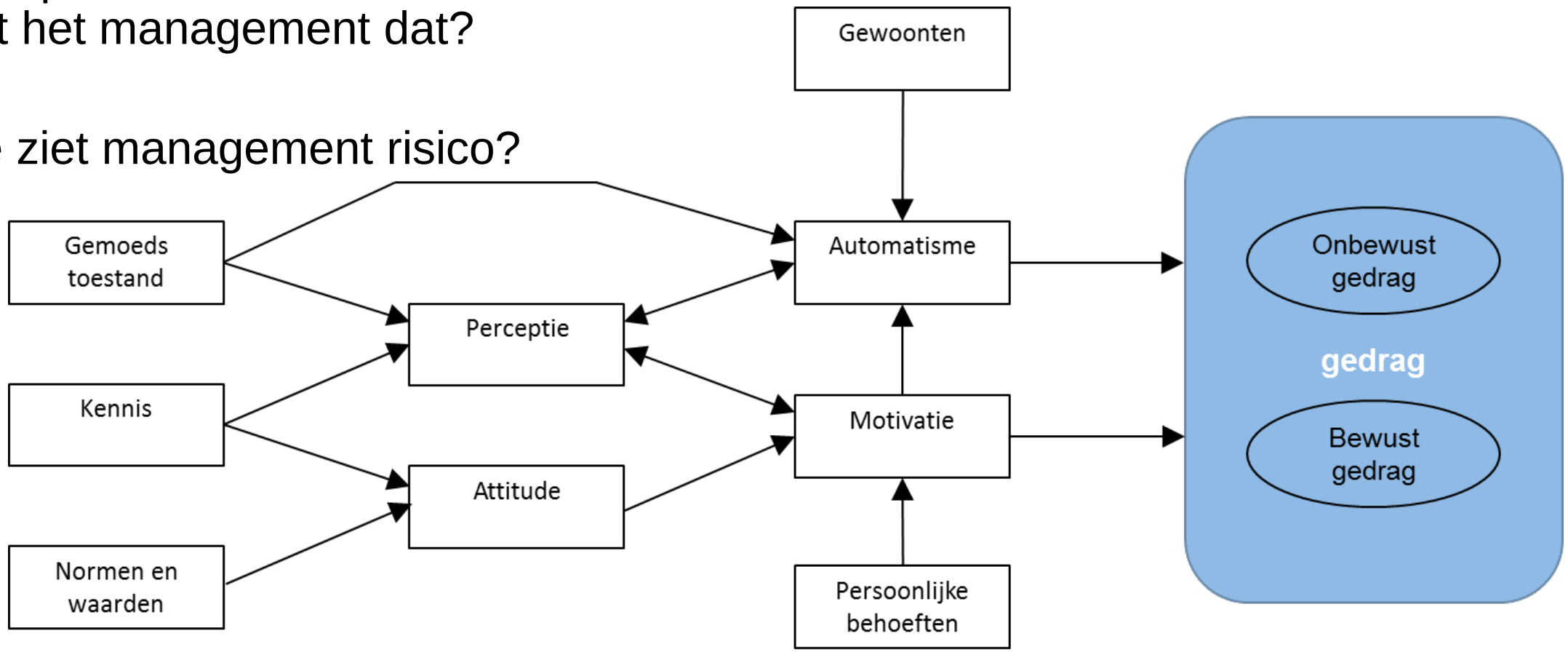

Model van Marcel Spruit

INFORMATIE
BEVEILIGINGS
DIENST

# Verschillende verwachtingen?

Waar plot de CISO risico's en waar doet het management dat?

Hoe ziet management risico?



INFORMATIE BEVEILIGINGS DIENST

# Wie is verantwoordelijk?

Ik kan niet zeggen hoe het in een gemeente geregeld is maar idealiter:

1. Portefeuillehouder (wethouder of burgemeester) (politiek)
2. Gemeentesecretaris (bedrijfsvoering/ambtelijk)
3. Proceseigenaar / lijnmanager
4. Werkvloer

En dan hebben we nog de controle (1th, 2th, 3th line of defence)
En U!

Wat is dan de CISO?

De CISO is de adviseur van allemaal!

INFORMATIE
BEVEILIGINGS
DIENST

# Waarnemingen

- Weinig onderzoeken over informatieveiligheid
- Veel van die onderzoeken zijn:
  - Pentesten (techniek)
  - Bewustwording (mens)
- Veel wollig taal gebruik
- Weinig oorzaak gevolg onderzoek
- Weinig proces onderzoek
- Veel maatregel onderzoek

INFORMATIE
BEVEILIGINGS
DIENST

# Oorzaak en gevolg

- Als bij een pentest een gat gevonden wordt, wat is er dan aan de hand?
  - De systeembeheerder heeft iets niet goed ingericht?
  - De systeembeheerder heeft misschien geen goede opdracht gekregen?
  - De systeembeheerder heeft geen kennis?
  - De ICT-manager heeft niet gecontroleerd?
  - De ICT-manager heeft geen goede opdracht gekregen?
  - De ICT manager heeft geen goede opdracht gegeven?
  - Het hoofd ICT heeft niet gecontroleerd?
  - Het hoofd ICT heeft geen goede opdracht gekregen?
  - De opdrachtgever heeft geen eisen gesteld aan zijn ICT afdeling?
  - De opdrachtgever heeft geen goede eisen gesteld aan zijn ICT afdeling?
  - De opdrachtgever heeft niet gecontroleerd?
  - Het gemeentelijk beleid gaat niet in op de noodzaak voor een goede firewall?
    - En zo zijn er legio vragen te bedenken!

INFORMATIE
BEVEILIGINGS
DIENST

**Het is geen enkele moeite om een zwakheid of een probleem te vinden, maar leggen we dan de vinger op de juiste zere plek?**

**Ieder systeem is te hacken!**

INFORMATIE
BEVEILIGINGS
DIENST

# Hiërarchie van de BIG

De BIG bestaat uit 10 hoofstukken, 133 controls, 309 maatregelen

| | |
|---|---|
| 5 | Beveiligingsbeleid |
| 6 | Organisatie van informatiebeveiliging |
| 7 | Beheer van bedrijfsmiddelen |
| 8 | Personele beveiliging |
| 9 | Fysieke beveiliging en beveiliging van de omgeving |
| 10 | Beheer van Communicatie- en Bedieningsprocessen |
| 11 | Toegangsbeveiliging |
| 12 | Verwerving, ontwikkeling en onderhoud van informatiesystemen |
| 13 | Beheer van informatiebeveiligingsincidenten |
| 14 | Bedrijfscontinuïteitsbeheer |
| 15 | Naleving |

INFORMATIE BEVEILIGINGS DIENST

# Pentesten?

## 12.6 Beheer van technische kwetsbaarheden

**Doelstelling**

Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

### 12.6.1 Beheersing van technische kwetsbaarheden

*Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.*

1. Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal het melden van incidenten aan de Informatiebeveiligingsdienst, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.

2. Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd

INFORMATIE BEVEILIGINGS DIENST

# Bewustwording?

### 8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

*Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.*

1. Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.[10]
2. [A]Bespreek het onderwerp informatiebeveiliging in functionerings- en beoordelingsgesprekken van medewerkers die risicovolle functies bekleden.

INFORMATIE
BEVEILIGINGS
DIENST

# De verantwoordelijkheid van (lijn) managers!

### 15.2.1 Naleving van beveiligingsbeleid en -normen

*Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.*

1. Het lijnmanagement is verantwoordelijk voor de uitvoering en de beveiligingsprocedures en de toetsing daarop (o.a. jaarlijkse in control verklaring). Conform de Strategische Baseline zorgt de CISO, namens de gemeentesecretaris, voor het toezicht op de uitvoering van het beveiligingsbeleid. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door of vanwege de CISO dan wel door interne of externe auditteams.

2. [A]In de P&C cyclus wordt gerapporteerd over informatiebeveiliging aan de hand van het in control statement.

INFORMATIE
BEVEILIGINGS
DIENST

# Privacy en ENSIA

- Verwerkingsregister
- Functionaris gegevensbescherming
- Privacy by design
- Privacy by default
- Recht van betrokkene
- Procedure voor DPIA's
- Procedure voor beheer
- **Logging voor applicaties (voor controle medewerkers!)**
- **Incidentmanagementproces cfm AVG**
- Verwerkersovereenkomsten/contracten/externe partijen
- Register van datalekken
- Privacy beleid (gegevens beschermingsbeleid)

INFORMATIE
BEVEILIGINGS
DIENST

# Vertrouwelijkheid

- 80% van de BIG is direct of indirect gerelateerd aan vertrouwelijkheid!
  - Toegangsbeveiliging
  - Toegangsrechten
  - Beoordeling van toegangsrechten
  - Netwerk toegang
  - Inlogprocedures
  - Beperken toegang tot informatie
  - Informatie uitwisseling
  - Encryptie
  - Proces voor melden
  - Incidentbeheer
  - Back-up

INFORMATIE
BEVEILIGINGS
DIENST

# Privacy en ENSIA

- Verwerkingsregister
- Functionaris gegevensbescherming
- Privacy by design
- Privacy by default
- Rechten van betrokkene
- Procedure voor DPIA's
- Procedure voor beheer
- **Logging voor applicaties (voor controle medewerkers!)**
- **Incidentmanagementproces cfm AVG**
- Verwerkersovereenkomsten/contracten/externe partijen
- Register van datalekken
- Privacy beleid (gegevens beschermingsbeleid)

INFORMATIE
BEVEILIGINGS
DIENST

# Nog even weer over die pentest

- Wat wordt er eigenlijk bekeken met een gemiddelde (penetratie) pentest?
  - Is er een apparaat te vinden dat..
  - Kwetsbaarheden (zijn de instellingen goed, staan alle updates er op)
  - Kan ik binnen komen?

- Maar wat is eigenlijk de meest interessante vraag?

INFORMATIE
BEVEILIGINGS
DIENST

# Procesvragen!

- Waar dient een firewall voor?
  1. De voordeur op slot houden
  2. Controleren wie er door gaat
  3. Controleren wat er door gaat

  Aldus is een veel interessantere vraag:
  Wordt er wel gekeken naar wie er door gaat en wat er door gaat?

  En als er naar gekeken wordt:
  Wat wordt er dan mee gedaan?

Als je niet weet wat je ziet, heb je ook geen incidenten en is er niets aan de hand!

INFORMATIE
BEVEILIGINGS
DIENST

# Goede onderzoeksvragen gaan over het proces!

- Even weer terug naar risico's….
- Welke risico's ziet u waarvan de impact hoog is en de kans hoog?

INFORMATIE
BEVEILIGINGS
DIENST

# Onderzoeksvragen Lijn

- Zijn de verantwoordelijkheden juist belegd?
- Hebben alle ICT-middelen een verantwoordelijke eigenaar (en weet die dat ook?) (ook en vooral informatie!)
- Draagt het bestuur en management actief IB uit?
- Hoe is de cultuur om risico's te melden?
- Zit de CISO bij het bestuur aan tafel?
- Is de CISO voldoende hoog gepositioneerd?
- Is risicomanagement structureel ingebed als proces?
- Vraagt het bestuur om rapportages en doen ze er dan wat mee?
- Is IB geborgd tot in de haarvaten van de organisatie?
- Wordt er lering getrokken van incidenten?
- Is er een incidenten registratie?
- Staat IB op de bestuurlijke agenda?
- Wat is er ingevuld bij ENSIA!?

INFORMATIE
BEVEILIGINGS
DIENST

# Onderzoeksvragen Privacy

- Controleren de lijnmanagers regelmatig of de juiste mensen toegang krijgen tot de juiste informatie?
- Is de systeem/toegangs/applicatie logging zo ingericht dat een effectieve controle mogelijk is?
- Kan uitgesloten worden dat niet rechthebbenden toegang hebben tot informatie?
- Is er een actueel overzicht van wie welke rechten en welke toegang heeft tot informatie?
- Zijn de beveiligingseisen ook verwerkt in contracten?
- Hebben lijnmanagers een dataclassificatie uitgevoerd en is dat controleerbaar?
- Is de dataclassificatie vertaald naar eisen voor ICT/leveranciers?
- Is er een actueel overzicht van datalekken? (wettelijke eis)
- Wordt er lering getrokken uit datalekken?
- Wordt er gerapporteerd in de lijn?

INFORMATIE
BEVEILIGINGS
DIENST

# Wat kan de IBD voor u betekenen

- U kunt bij ons terecht voor:
  - Alle IB gerelateerde vragen!
  - BIG vragen
  - Tips en truuks
  - Toegang tot de community
  - Een lijstje van bij ons bekende onderzoekspartijen

  - Let wel: vertrouwenspositie!

INFORMATIE
BEVEILIGINGS
DIENST

# Samenvatting

INFORMATIE
BEVEILIGINGS
DIENST

# Vragen?

INFORMATIE
BEVEILIGINGS
DIENST

Informatie over de IBD en allerhande ondersteunde documenten zijn te vinden op onze website:
https://www.informatiebeveiligingsdienst.nl/

Op de  IBD-community kan onderlinge dialoog en kennisuitwisseling over informatiebeveiliging plaatsvinden
https://community.informatiebeveiligingsdienst.nl/

VNG Realisatie