Informatiebeveiliging
Eigen huis op orde

PREVENTIE

Rol bestuur

- Voorbeeldfunctie
  - Bewustwording
  - Zelf regels naleven
  - Voorbeeld
- Faciliteren
  - Mensen en middelen beschikbaar stellen
  - Bevorderen open cultuur
- Borgen
  - P&C cyclus
    - ENSIA
  - Informatiebeveiligingsbeleid en -plan
    - Vaststellen
    - Controleren
    - Evalueren
- Sturen
  - Risicomanagement
    - Periodiek gesprek met CISO
      - Waar lig je wakker van?
      - Hoe staan we ervoor?
      - Zijn de risico's acceptabel?
      - Kansen voor innovatie?
    - 10 Bestuurlijke principes BIO
      - 100% Veilig bestaat niet
      - Pas toe of leg uit
    - Kosten-/batenanalyse

Organisatie

- Structuur
  - Gemeentesecretaris eindverantwoordelijk
    - Lijnmanagement verantwoordelijk
    - Chief Information Officer (CIO)
    - Chief Information Security Officer (CISO)
    - Privacy Officer (PO)
    - Functionaris Gegevensbescherming (FG)
- Cultuur
  - Open cultuur, leren van fouten
  - Testen
    - Pentesten
    - Ethische hackers
    - Vaststellen privacy risico's (PIA's)
  - Integriteit (ambtseed)
  - Oefenen
    - Crisisgame IBD
    - Phishing mails
    - Mystery guest
    - (e)-training

- Systemen
  - Informatiesystemen
    - Basisbeveiligingsniveau (BBN) vaststellen obv baseline toets en risico-analyse
      - BBN 1 (geen gevoelige informatie)
      - BBN 2 (vertrouwelijke informatie)
      - BBN 3 (geheime informatie)
  - Fysieke toegang
- Processen
  - Informatiebeveiligingsbeleid
    - Strategisch niveau
    - Tactisch niveau
    - Operationeel niveau
      - IB maatregelen
      - Calamiteitenplan
    - Uitvoeren volgens PDCA cyclus
  - Middelen borgen in P&C cyclus
    - Verantwoording afleggen aan College B&W
      - Audit (ENSIA)

Krachtenveld

- Leveranciers Informatiesystemen
- Netwerkpartners waaronder samenwerkingsverbanden
- Uitvoeringsorganisaties gemeentelijk beleid (bijv. Sociaal Domein)
- Veiligheidsregio

CRISIS

Rol bestuur

- Woordvoering
  - Transparant
  - Juiste informatie
  - Gericht op herstel vertrouwen burger
- Waarderen incident obv (maatschappelijke) impact (vergelijk GRIP)
  - Calamiteitenplan
  - Opschalen
  - Afstemmen binnen college B&W
  - Raad informeren
- Crisisorganisatie inrichten
  - GS
  - FG
  - CISO
  - Lijnmanagement
  - Woordvoering
  - OOV (eventueel)

Organisatie

- Nemen van crisismaatregelen
  - Schade beperken
  - Hulp IBD of andere partijen inroepen
  - Schade herstellen
  - Contact met politie en OM
  - Evalueren
- Betrokkenen informeren

Wet- en regelgevin

- Melden datalek bij Autoriteit Persoonsgegevens (AP)
- Aangifte doen

Krachtenveld

- Media
- Leveranciers Informatiesystemen
- Netwerkpartners waaronder samenwerkingsverbanden
- Uitvoeringsorganisaties gemeentelijk beleid (bijv. Sociaal Domein)
- Veiligheidsregio

Innovatie

- Is in lijn met en versterkt het ambitieniveau van de gemeente
- BIG DATA in beleids- en uitvoeringsprocessen
  - Eigen data anders gebruiken
  - Linked data (koppelen met data van derde partijen)
  - Nieuwe data ophalen (bijvoorbeeld sensoren in openbare ruimte)
- Kansen en risico's
  - Security by design
    - Uitvoeren Data Protection Impact Assessment (DPIA)
  - Risicomanagement
    - 10 Bestuurlijke principes BIO
  - Business case
- Ethische vragen
  - Van wie is de data?
  - Doelbinding

HET FUNDAMENT

Informatiebeveiliging

- Definitie informatiebeveiliging
  - Beschikbaarheid van informatie (Is de informatie er als we die nodig hebben?)
  - Integriteit van informatie (Klopt het?)
  - Vertrouwelijkheid van informatie (Kunnen alleen de juiste mensen erbij?)
- Wettelijk normenkader
  - Van Baseline Informatiebeveiliging Gemeenten (BIG) naar Baseline Informatiebeveiliging Overheid (BIO)
    - Verplichte standaard
    - Risicomanagement
  - Algemene Verordening Gegevensbescherming (AVG)
  - SUWI, BRP, PUN, BAG en BGT
- Informatiebeveiliging is een continu proces
  - Doorlopen volgens de Plan-Do-Check-Act cyclus (PDCA)