Agenda

- Informatiebeveiligingsbeleid (TIC: b&w 18 aug)
- Architectuurplaat
- Dreigingsbeeld
- Acties
- ENSIA (TIC: b&w 17 mrt)
- Casus: “Leren van Lochem”

gemeente Overbetuwe

Informatiebeveiligingsbeleid

- Draait om informatie (dus niet alleen ICT)
- Aanpak is gestoeld op de Baseline Informatiebeveiliging Overheid (BIO) en risico-gedreven cyclisch proces
- Betreft de gehele bedrijfsvoering
- Lijnmanager verantwoordelijk voor maatregelen informatiebeveiliging

Architectuurplaat

- Architectuur plaat tonen

Dreigingsbeeld

De Informatiebeveiligingsdienst (IBD) onderscheidt vier typen dreigingen:

- Intern en onbedoeld, bijvoorbeeld fouten van medewerkers met incidenten als gevolg
- Extern, bedoeld maar en ongericht, bijvoorbeeld grootschalige phishing- en ransomwarecampagnes.
- Extern, bedoeld en gericht, bijvoorbeeld doelgerichte pogingen om geld of informatie buit te maken
- Intern en bedoeld, bijvoorbeeld fraude en ondermijnende activiteiten van eigen medewerkers.

Acties

- Maatregelen: organisatorisch, technisch, menselijk
- Bewustwording informatieveiligheid
  - Enquête
  - Phishing, polls, artikelen
  - Handreikingen / deelbeleid
  - NIVO groep informatieveiligheid
  - Continue aandacht
- Rapporteren

ENSIA*

- Jaarlijkse collegeverklaring
- Zelfevaluatie
- Digid en Suwinet

*Eenduidige Normatiek Single Information Audit

Leren van Lochem

- Filmpje “Leren van Lochem”