BIO Baseline Informatiebeveiliging Overheid
voor een veilige digitale overheid

CIP

Wordt informatieveiligheid daadwerkelijk chefsache?

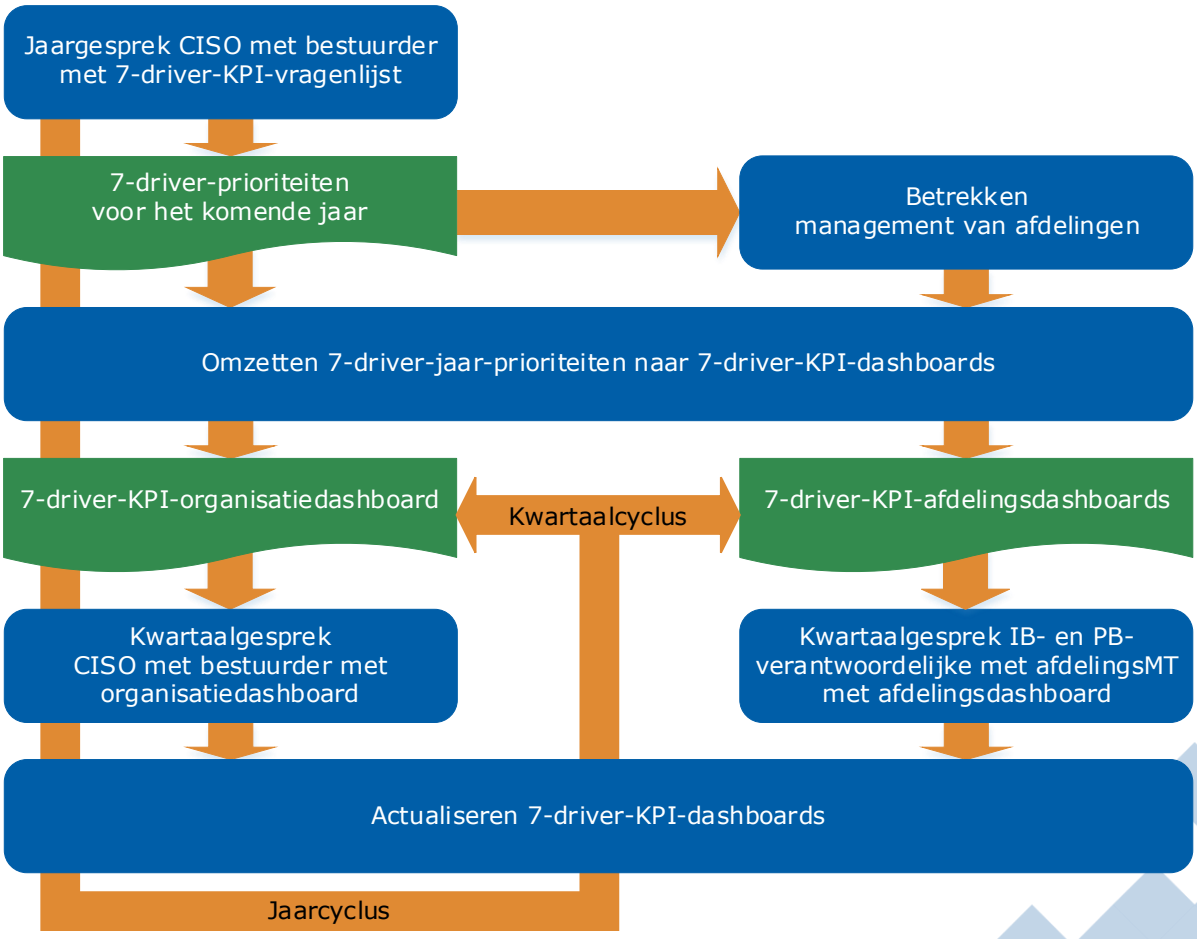
Stel uw organisatie is gehackt. De pers belt u als bestuurder.
Wat is uw reactie?

- Voor security heb ik mijn mensen, een prima team.
- Zij hebben me herhaaldelijk verzekerd dat we in control zijn.
- Deze hack is een uitzondering; het blijft mensenwerk.
- Aan het herstel wordt op dit moment hard gewerkt.
- Nadere informatie kan ik nu niet geven.

- Voor security heeft onze organisatie een gedegen aanpak.
- Risico's zijn in kaart gebracht, ook die van een hack zoals deze.
- De meest gevoelige gegevens zijn extra afgeschermd. Deze zijn niet geraakt.
- Door onze back-up-aanpak zijn we binnen 6 uur weer volledig in bedrijf.

De 7-driver-KPI-aanpak zorgt ervoor dat u de blauwe reactie kunt geven en dat deze nog klopt ook!

Jaar- en kwartaalcyclus 7-driver-KPI's



Rijksoverheid · Interprovinciaal Overleg ip · VNG Vereniging van Nederlandse Gemeenten · UNIE VAN WATERSCHAPPEN

BIO Baseline Informatiebeveiliging Overheid
voor een veilige digitale overheid

CIP

Suggesties voor 7-driver-KPI's

1. Risico's:
   - Bepaal de top-risico's en de daarvoor meest relevante maatregelen.
2. Inkoop:
   - Breng leveranciers- en andere ketenafspraken in lijn met de BIO en aanvullende kaders.
   - Benut de ICO-wizard om dit te borgen.
3. Bijwerken:
   - Breng security-wijzigingen tijdig aan. Vervang oude software op tijd.
4. Veilig thuiswerken:
   - Pas twee-factorauthenticatie consequent toe.
   - Stel hoge(re) eisen aan bijzondere toegang (beheer/testen met name).
5. Afscherming:
   - Regel CERT- en SOC-diensten.
   - Bescherm top-risicoapplicaties tegen domino-effecten door segmentatie.
6. Crisismanagement:
   - Heb een waterdichte herstel-aanpak voor top-risicoapplicaties.
   - Oefen regelmatig cybercrisismanagement.
7. Maturiteit:
   - Meet de kwaliteit van security-processen met self assessments (BIO-SA en PriSA).
   - Houd medewerkers scherp op feitelijk security-gedrag met bijvoorbeeld red-teaming.

Fasegewijs verrijken

Voer de 7-driver-KPI-aanpak gefaseerd in, bijvoorbeeld:
- Kies 3 maatregelen uit de 7-driver-set.
- Rapporteer daarover 3-maandelijks en bespreek dat in MT-overleggen.
- Verrijk de rapportages in volgende jaren, dus elk jaar 2/3 dashboard-items erbij.

Dashboard jaar 1
- Waterdicht herstel top-risico's
- ICO bij nieuwe contracten en ketenafspraken
- SOC-diensten inregelen

Dashboard jaar 2
- Twee-factorauthenticatie
- Plaats top-risico-applicaties in aparte segmenten/Zero Trust
- Waterdicht herstel top-risico's
- ICO bij nieuwe contracten en ketenafspraken
- SOC-diensten inregelen

Dashboard jaar 3
- Maturiteit meten en versterken (self assessments/red teaming)
- Vervangen oude software
- ICO ook voor herijking bestaande ketenafspraken
- Twee-factorauthenticatie
- Plaats top-risico-applicaties in aparte segmenten/Zero Trust
- Waterdicht herstel top-risico's
- ICO bij nieuwe contracten en ketenafspraken
- SOC-diensten inregelen

Scan de QR-code voor het hele verhaal

Versie 1.2 definitief

Rijksoverheid · Interprovinciaal Overleg ip · VNG Vereniging van Nederlandse Gemeenten · UNIE VAN WATERSCHAPPEN