

“Spion op je Pad”

Een Serious Boardgame over Informatiebeveiliging voor gemeenten



Auteur: M. de Blaeij (Ministerie van Economische Zaken) en de IBD

Datum: 28 november 2016

Versie: IBD

Licentie: 

Credits

Ontwerp en eigendom:

Dit is oorspronkelijk het gamedesign document van “*Spion op je Pad*” – een serious game (bordspel) over informatiebeveiliging bedoeld voor medewerkers van het ministerie van EZ. Deze game is ontworpen door de Directie Bedrijfsvoering van EZ. Het intellectueel eigendom ligt bij de Directeur Bedrijfsvoering van EZ.

Marthijn de Blaeij, ontwerper van het spel, heeft namens de directeur Bedrijfsvoering EZ de IBD toestemming gegeven het spel aan te passen voor gemeenten.

De IBD hanteert voor haar versie van dit spel de volgende licentie: [Creative Commons](#) – naamsvermelding – niet commercieel – geen afgeleide werken.

Doel van dit document:

Dit document was bedoeld als basis voor het ontwerpen van de game en wordt door de IBD aangepast en gebruikt om de achtergrond en mogelijke inzet van de game toe te lichten.

LET OP! Dit is geen handleiding voor het spelen van de game. Dit wordt in een apart document (bij de game) gevoegd voor de spelleider.

Meer informatie

Mocht u vragen hebben over de game, dan kunt u contact opnemen met info@ibdgemeenten.nl of bellen met de IBD helpdesk 070 204 55 11.

Inhoudsopgave

Deel 1: Achtergrond

1.1	Doelgroep.....	4
1.2	Aanleiding.....	4
1.3	Inzichten	4
2.1	Doel van de game	6
2.2	Doelgroep	6
2.3	Leerdoel.....	6
2.4	Leereffecten	6
3.1	Samenvatting van de game	7
3.2	Vraagkaarten	7
3.3	Incidenten.....	7
3.4	Handleiding.....	8

Deel 1: Achtergrond

1.1 Doelgroep

Gemeenten en hun medewerkers. De game vereist geen technische kennis en is op alle niveaus en afdelingen in te zetten.

1.2 Aanleiding

De awareness ten aanzien van informatiebeveiliging en privacy is soms onvoldoende ontwikkeld bij gemeentelijke medewerkers. Daarnaast is awareness op dit vlak nooit ‘afgerond’. Alertheid op dit onderwerp heeft continu aandacht nodig binnen de gemeentelijke organisatie. Enerzijds ontberen medewerkers soms de skills en tools om hun informatie goed te kunnen beveiligen. Anderzijds zijn er diverse andere blokkades, zoals bureaucratie, onvoldoende budget, tijd of onwetendheid en schaamte. Medewerkers komen en gaan. De alertheid zakt weg na verloop van tijd. Door snelle maatschappelijke, technische ontwikkelingen en nieuwe tactieken van cyber criminelen, ontstaan nieuwe risico's. Ook vanuit bestuur en management wordt nut en noodzaak van informatiebeveiliging niet altijd gezien. Vragen als: “waar moeten wij nu bang voor zijn?”; “wat is het risico?”; en “welke voorbeelden zijn er?” komen nog veelvuldig voor bij het bestuur en management.

Het lekken van informatie en het nemen van risico's op informatiebeveiliging, is op te delen in twee segmenten:

- Bewust (met opzet, door eigen medewerkers of derden).
- Onbewust (onvoldoende awareness, door eigen medewerkers of derden).

Het probleem dat met deze game wordt aangepakt ligt met name bij de groep “onbewust door eigen medewerkers”.

1.3 Inzichten

Ambtenaren moeten altijd zorg dragen voor een betrouwbare overheid. Immers de overheid heeft een voorbeeld functie voor bedrijven, organisaties en burgers op het gebied van betrouwbaarheid. Ambtenaren hebben tijdens de uitvoering van hun werk, altijd de keuze op welke manier informatie wordt uitgewisseld met collega's en/of derden. Denk daarbij aan papier, digitaal, gesprek etc.

Tijdens de uitvoering van een proces is niet alle informatie op alle momenten even vertrouwelijk. Het is een continu dynamisch spel met overwegingen. Belangrijke centrale vraag bij de overwegingen voor bovenstaande dreigingen is vaak: “Staat het morgen in de krant?” en zo ja; “Komt er dan gedoe van?”. Maar niet alleen reputatieschade speelt een rol. Met name gemeentelijke medewerkers zouden zich bewust moeten zijn van de privacy risico's bij het werken met gegevens van burgers en bedrijven.

Kritische dossiers gemeenten (lijst niet volledig):

- Gemeentelijke financiën
- ICT en informatiebeveiliging
- Fysieke beveiliging
- Personeelsdossiers en ziekteverzuim medewerkers
- (Persoons) gegevens bedrijven en burgers
- Gegevens sociaal domein

Belangrijke andere inzichten op het gebied van informatiebeveiliging zijn:

- Men heeft een eigen verantwoordelijkheid maar ook een gezamenlijke verantwoordelijkheid.
- Men dient oog te hebben voor risico's, dat is nu niet altijd het geval.
- De kans is groter tijdens overdrachtsmomenten (bijv. van directie X naar directie Y, of in samenwerking met ketenpartners).
- De kans is groter als de er deadlines gehaald moeten worden.
- Wanneer informatie digitaal is opgeslagen, dan is verspreiding makkelijker en is voorzichtigheid geboden.

Deel 2: De game

2.1 Doel van de game

De spelers moeten ervoor zorgen dat de “Spion” de waardevolle informatie die het team heeft, niet in bezit krijgt. Hij wil namelijk de waardevolle informatie gebruiken om te publiceren. De spelers nemen ieder de rol aan van medewerker bij de gemeente en worden geacht om als team samen te werken tijdens de soms ingewikkelde processen en onder tijdsdruk. Men speelt dus met elkaar tegen de game, en niet tegen elkaar.

2.2 Doelgroep

Gemeentelijke medewerkers op alle niveaus en verschillende achtergronden zouden de game moeten spelen. De game omvat situaties waar elke gemeentelijk medewerker in terecht kan komen waarbij alertheid op de gevoeligheid van informatie vereist is.

De game wordt gespeeld in een groep van maximaal 10 personen. De game dient geleid te worden door één of twee spelleiders.

2.3 Leerdoel

Na het spelen van *Spion op je Pad*, gaat het “belletje” rinkelen bij medewerkers, wanneer zij in aanraking komen met vertrouwelijke informatie of zich bevinden in een situatie waarbij zich een risico kan voordoen.

2.4 Leereffecten

Na het spelen van *Spion op je Pad*:

- Herkent men de situaties waarin zich een risico voordoet;
- heeft men oog voor het beveiligen van informatie bij het dagelijkse werk;
- realiseert men zich dat lekken schadelijk is voor de gemeente en haar imago;
- kan men goed omgaan met de ter beschikking staande (ICT) middelen;
- is men nieuwsgierig naar de ter beschikking staande middelen;
- is men niet huiverig om incidenten te melden; en
- weet men bij wie men terecht kan met vragen m.b.t. privacy en informatiebeveiliging.

Deel 3: Gameplay

3.1 Samenvatting van de game

Op speelbord 2 staan de 10 medewerkers en de Spion tegenover elkaar. De medewerkers in het licht (wit) en de Spion in het duister (zwart). Eén van de medewerkers heeft het betreffende dossier met waardevolle informatie. Tijdens verschillende gebeurtenissen stapt de Spion richting het licht (kan nooit meer terug), en stappen de medewerkers richting het duister (kunnen wel terug). Zodra de Spion de medewerker met het dossier heeft gepakt, heeft het team verloren. Wanneer de medewerkers twee van de drie andere paden op het andere speelbord 1 hebben afgerond voordat de Spion het document heeft, heeft het team gewonnen.

Deze drie andere paden zijn:

- 1) kwaliteit van het werk
- 2) snelheid van het werk
- 3) informatiebeveiliging

De spelers moeten iedere keer een keuze maken tussen deze drie factoren om tot een goed einde te komen. Een “goed einde” is hierbij relatief; het kan zijn dat je hoog scoort op snelheid maar laag scoort (misschien zelfs verliest) op informatiebeveiliging. Dit sluit aan bij de realiteit. In de dagelijkse praktijk zijn de keuzes die je maakt ook niet altijd in alle opzichten optimaal. De keuze om maximaal te beveiligen kan bijvoorbeeld tijdverlies als consequentie meebrengen.

Als een speler aan de beurt is mag hij/zij 1 stap doen op 1 van de 3 paden. Ieder stapje op ieder pad geeft een van de twee volgende opties:

- Een vraag (multiple choice en gesteld door de spelleider = inhoudelijk + persoonlijk)
- Een incident (zonder keuze, maar wel te voorkomen, consequentie zwaar, vooraf te lezen)

3.2 Vraagkaarten

Het spel bevat een dertigtal vragen met verschillende situaties. De speler moet zelfstandig een vraag beantwoorden als men terecht op een vakje “V”.

De complete lijst met 30 vragen en antwoorden+puntentelling is verder uitgewerkt in apart document voor de spelleider. Daarnaast is er een ppt bijgeleverd om de vragen te tonen op groot scherm aan de spelers.

3.3 Incidenten

In Spion op je Pad zijn er naast de vraagkaarten 10 incidenten, die kunnen gebeuren wanneer een speler een pion op een vakje met een “I” plaatst. Een incident is een praktijkbeschrijving van een informatielek of een risico. De beschrijvingen staan afgedrukt op het speelbord en voor iedere speler tijdens gehele spel te lezen. De beschrijving heeft soms een relatie met de paden kwaliteit, snelheid en informatiebeveiliging. Bijvoorbeeld: “Als je op het pad Snelheid verder bent dan punt X, dan,

als je niet verder bent dan” Hiermee wordt de druk om te presteren op de paden verder opgevoerd Na de beschrijving staat ook bij een incident een consequentie. Het verschil met de vraagkaarten is, is dat de consequenties vooraf bekend zijn bij de spelers (want afgebeeld op spelbord).

De complete lijst met 10 incidenten is verder uitgewerkt in apart document.

3.4 Handleiding

De game mechanics zijn uitgebreid beschreven in een handleiding voor de spelleider. Dit is een apart document.

Daarnaast krijgt iedere speler een kaart met daarop de beknopte spelregels.