# Bijlage E - Risico scenario's met kans en impact

## Risico scenario's

Zwakke plekken worden meestal in combinatie met elkaar gevaarlijk. De kunst is om de samenhang daarin te zien en om dan goed gekozen zwakke schakels sterker te maken. De samenhang tussen verschillende zwaktes wordt zichtbaar gemaakt in Risico scenario's.

De opsomming hieronder is het resultaat van een beoordeling op basis van ervaring. Er is niet gekozen voor een uitgebreide risico analyse omdat die veel tijd kost en de conclusie in termen van zwakke plekken, prioriteiten en acties in grote lijnen hetzelfde zullen zijn.

Er is gesproken over de noodzaak om een totale uitval van openbare nutsvoorzieningen als scenario op te nemen. Dit naar analogie van Argentinië en Uruguay, en de mogelijkheid dat dit via een Cyberaanval door een vreemde mogendheid is veroorzaakt. De conclusie van dat gesprek is dat het scenario kan worden verkend, maar dat dit niet primair als informatiebeveiligingsrisico geldt.

In Bijlage G zijn onderstaande scenario's nader uitgewerkt, met uitzondering van scenario 8 waarvan het risico zo laag is dat dit in eerste instantie geen hoge prioriteit verdient.

1. Een geavanceerde gerichte malware aanval legt de ICT van de gemeente twee weken stil. De gemeenteraad werkt met handgeschreven moties. Extra kosten voor losgeld, herstel en tijdelijke maatregelen lopen uiteindelijk in de miljoenen.
2. Ongerichte malware verstoort het werk van een aantal afdelingen gedurende een aantal dagen. Vanuit backups worden de meeste gegevens hersteld.
3. Een verloren privé telefoon zorgt dat gevoelige gegevens bekend worden.
4. Een USB-stick met informatie over burgers haalt het Haarlems Dagblad.
5. Een insluiper krijgt toegang tot gevoelige informatie en kopieert deze informatie naar het buitenland zonder dat dit wordt opgemerkt. Als dit later aan het licht komt dan is er onvoldoende informatie om te achterhalen wat er is gebeurd. Een belangrijke ketenpartner schort de samenwerking op omdat het politiek te riskant is om met Haarlem samen te werken.
6. Een bestand met gevoelige informatie wordt verstuurd via WeTransfer (of een andere Cloud-dienst op Internet). Het bestand komt bij de verkeerde persoon terecht. De gemeente moet een flink aantal inwoners informeren en excuses maken.
7. Een onbekende krijgt de inloggegevens van een account te pakken, en kan daarmee E-mail versturen. Haarlem verspreidt daarna SPAM en Malware. Als gevolg daarvan wordt Haarlem op Internet geblokkeerd en kan Haarlem gedurende 3 dagen niet meer per E-mail extern communiceren.
8. In een groot gebouw (Raakspoort) is lekkage waardoor alle elektriciteit moet worden uitgeschakeld. Herstel van het gebouw kost een week. De publieksbalies blijven gesloten, de inpandig ICT systemen zijn uitgeschakeld, werkplekken van ambtenaren in het gebouw zijn niet beschikbaar.

## Kans en impact

Volgens de geldende afspraken binnen de gemeente worden Kans en Impact gebruikt met een onderverdeling van klasse 1 tot en met klasse 5. In Bijlage F staat deze structuur en de indeling kort samengevat.

In onderstaande tabel staan restrisico's aangegeven die rekening houden met de reeds geïmplementeerde maatregelen. Uit scenario's volgt vaak een duidelijke impact, maar de kans is een inschatting waarover gediscussieerd kan worden. In bijlage G staat bij ieder scenario toegelicht op basis van welke overwegingen een bepaalde klasse voor de kans is gekozen.

Het Risico wordt berekend via de formule Risico = Kans x (Geld impact + Imago impact + Tijd impact)

| Scenario | Kans nu | Kans na uitvoering plan | Impact | | | Risico | Risico na uitvoering plan |
|---|---|---|---|---|---|---|---|
| | | | Geld | Imago | Tijd | | |
| 1 | 3 | 2 | 5 | 5 | 5 | 45 | 30 |
| 2 | 4 | 2 | 1 | 4 | 3 | 32 | 16 |
| 3 | 4 | 2 | 1 | 3 | 2 | 24 | 12 |
| 4 | 3 | 2 | 1 | 4 | 2 | 21 | 14 |
| 5 | 3 | 2 | 2 | 5 | 4 | 33 | 22 |
| 6 | 3 | 2 | 1 | 5 | 3 | 27 | 18 |
| 7 | 4-5 | 2 | 1 | 4 | 2 | 32 | 14 |
| 8 | 1 | 1 | 3 | 4 | 3 | 10 | 10 |

In de tabel is de hoogste aspectscore uitgelicht. Het imago – en daarmee het vertrouwen van de burger in de overheid – is het dominante aspect dat aan veel beveiligingsrisico's verbonden is. Het eerste scenario – de gerichte ransomware aanval – heeft daarnaast ook een dominante financiële component en de langste nasleep in tijd.

| Scenario | Risico (Geld) | Risico (Imago) | Risico (Tijd) | Rangorde (Geld) | Rangorde (Imago) | Rangorde (Tijd) |
|---|---|---|---|---|---|---|
| 1 | 15 | 15 | 15 | 1 | 3 | 1 |
| 2 | 4 | 16 | 12 | 4 | 2 | 3 |
| 3 | 4 | 12 | 8 | 4 | 6 | 6 |
| 4 | 3 | 12 | 6 | 6 | 6 | 7 |
| 5 | 6 | 15 | 12 | 2 | 4 | 2 |
| 6 | 3 | 15 | 9 | 6 | 5 | 4 |
| 7 | 5 | 18 | 9 | 3 | 1 | 4 |
| 8 | 3 | 4 | 3 | 8 | 8 | 8 |

Als de verschillende risico-dimensies in samenhang worden bekeken, dan is het zaak om vooral de risico-scenario's 1, 2, 5 en 7 vlot verder aan te pakken.

In Bijlage H zijn de mogelijke mitigerende acties bij de scenario's uitgewerkt. Kans x impact van scenario 8 is zo laag dat dit scenario niet verder is uitgewerkt.