

Informatiebeveiligingsbeleid 2024-2027

Gemeente Beuningen



Datum: December 2023
Versie: 13
Status: Definitief
Auteur: Corynne de Vocht

Samenvatting

De afhankelijkheid - en daarmee het belang - van een betrouwbare informatievoorziening wordt steeds groter. Digitalisering en ketenintegratie nemen binnen onze processen alleen maar toe. Bovendien streven we als organisatie naar data gedreven werken om zo onze processen en dienstverlening te verbeteren.

Informatiebeveiliging is geen doel op zich. De op informatiebeveiliging gebaseerde maatregelen zijn nodig om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te bewaken. Hoe kwetsbaar we als gemeente zijn, laten cyberaanvallen en beveiligingslekken bij andere gemeenten zien. Informatiebeveiliging is geen eenmalige activiteit, maar een continu proces gericht op het doorlopend beheersen van risico's.

Het college, de gemeentesecretaris en de managers hebben een essentiële rol in informatieveiligheid. Het college is bestuurlijk verantwoordelijk en de gemeentesecretaris is samen met het management (managementteam) verantwoordelijk voor de uitvoering. Het college geeft met het vaststellen van dit beleid een duidelijke richting aan informatieveiligheid en laat zien dat zij informatieveiligheid als randvoorwaarde ziet voor een betrouwbare en veilige informatievoorziening.

De speerpunten van het informatiebeveiligingsbeleid 2024-2027 zijn:

- dataclassificatie voor het bepalen van het beschermingsniveau en risicobereidheid;
- risicomanagement en het integreren van informatieveiligheid in processen en procedures;
- bewustwording verhogen om het succes van (cyber)criminelen te verkleinen;
- vaststellen en effectueren van aanvullende beleidsdocumenten en procedures.

De speerpunten dragen bij aan de aanbevelingen van de rekenkamer om te groeien naar volwassenheidsniveau 3 (volgens het model van het Centrum Informatiebeveiliging en Privacybescherming). Ook komen we met deze speerpunten tegemoet aan de aanbevelingen uit de ENSIA-audits. Verder zal door de verwachte benoeming van de gemeente als essentiële entiteit in de Wet beveiliging netwerk- en informatiesystemen (Wbni) de noodzaak voor risicomanagement en maatregelen verder toenemen.

Dit informatiebeveiligingsbeleid dient samen met het privacy beleid als kapstok voor aanvullende beveiliging- en privacy beleidsdocumenten, procedures en standaarden van de gemeente, zoals onderstaand schema laat zien.



De managers zijn verantwoordelijk voor de resultaten van de afdelingen en daarmee ook voor informatieveiligheid. Risicomanagement en het treffen en effectueren van maatregelen horen daar bij. Veel maatregelen worden vanuit bedrijfsvoering organisatie breed geïmplementeerd, maar organisatorische en of procedurele maatregelen blijven bij de afdeling. In de praktijk geven kwaliteitsmedewerkers of applicatiebeheerders vaak ondersteuning. Toch is het nodig dat managers op de hoogte zijn van kwetsbaarheden in hun processen en systemen. Alleen zo kunnen zij risico's inschatten en de impact bepalen. Risicomanagement is de basis voor informatiebeveiliging, waar de manager beslist en de CISO adviseert.

Inhoudsopgave

1.	Inleiding	5
1.1	Leeswijzer	5
1.2	Wat is informatiebeveiliging?	5
1.3	Privacy & Gegevensbescherming (AVG)	5
1.4	Bestuurlijke visie en ambitie voor informatiebeveiliging	6
1.5	Speerpunten van beleid	8
2.	Het beleid	9
2.1	Doel	9
2.2	Ontwikkelingen	9
2.2.1	Baseline Informatiebeveiliging Overheid	9
2.2.2	Network and Information Security 2 en Wet beveiliging netwerk- en Informatiesystemen	9
2.2.3	De 10 bestuurlijke principes voor informatiebeveiliging (zie bijlage 1)	10
2.2.4	Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten	10
2.2.5	Informatie uit incidenten en inbreuken op de beveiliging	10
2.3	Standaarden informatiebeveiliging	11
2.4	Plaats van het beleid	11
2.5	Scope informatiebeveiliging	11
2.6	Uitgangspunten	12
2.6.1	Doelen	12
2.6.2	Belangrijkste uitgangspunten	12
2.6.3	Invulling van de uitgangspunten	13
2.6.4	Randvoorwaarden	14
3	Samenhang privacybescherming en informatiebeveiliging	14
4	Organisatie, taken en verantwoordelijkheden	15
4.1	Aansturing: managementteam	15
4.2	Uitvoering: managementteam	16
4.3	Controle en verantwoording	16
4.3.1	ENSIA	16

Bijlage 1. De 10 bestuurlijke principes voor informatiebeveiliging volgens VNG

1. Inleiding

Deze beleidsnota beschrijft het informatiebeveiligingsbeleid voor de jaren 2024-2027 en vervangt het in 2018 vastgestelde 'Informatiebeveiligingsbeleid 2018-2021 gemeente Beuningen'.

Deze nota is richtinggevend en wordt aangevuld met onderwerp specifieke beleidsdocumenten en werkinstructies voor informatiebeveiliging.

Met dit informatiebeveiligingsbeleid zet de gemeente Beuningen een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente te continueren en voort te gaan op stappen die in de voorgaande jaren gezet zijn. De basis voor dit beleid is de NEN-SO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG, zie bijlage 1.

1.1 Leeswijzer

Hoofdstuk 2 behandelt de kern van het beleid. Dit beleid wordt aangevuld met onderwerp specifieke beleidsregels. In het jaarlijkse, door het managementteam vast te stellen, informatiebeveiligingsplan worden deze aspecten van informatiebeveiliging verder uitgewerkt en geconcretiseerd. Als basis dient hiervoor het rekenkameronderzoek, input van de managers, de CISO, de privacy functionarissen (PO en FG), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van ENSIA. In de jaarlijkse beveiligingsplannen staan de acties en planning, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 behandelt de samenhang tussen privacybescherming en informatiebeveiliging. Tot slot beschrijft hoofdstuk 4 welke taken en verantwoordelijkheden horen bij welke afdelingen en managers.

1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan *“het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen”*.

Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politieke bestuur, alle medewerkers, inwoners, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de

toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en de veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat (lees verder bij hoofdstuk 3).

1.4 Bestuurlijke visie en ambitie voor informatiebeveiliging

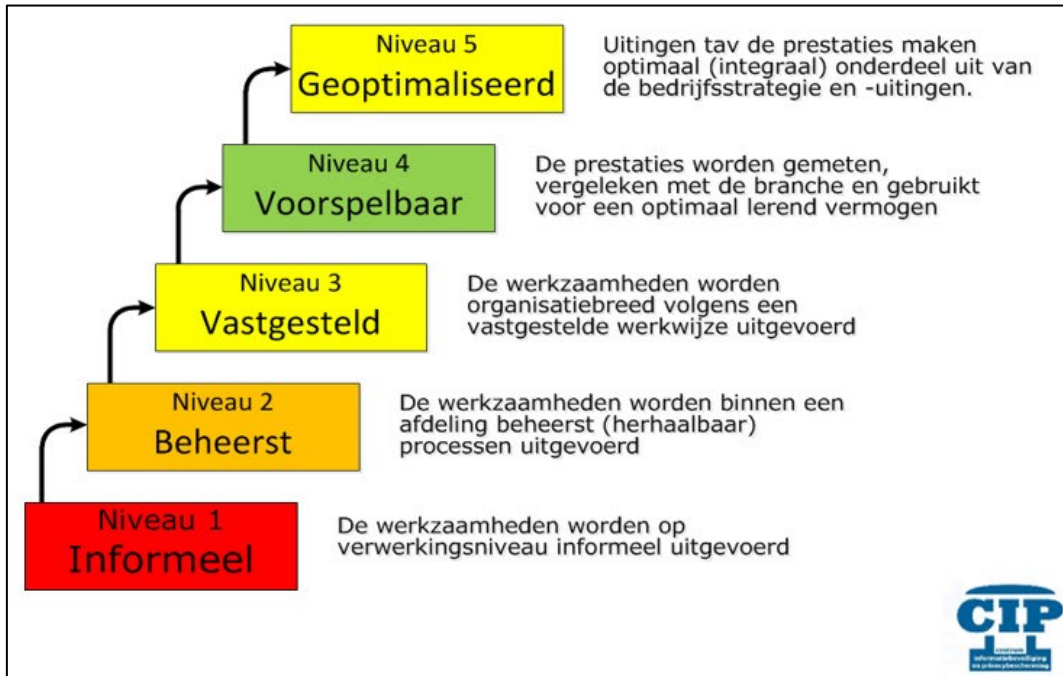
Inwoners mogen van de gemeente Beuningen verwachten dat ze zorgvuldig omgaat met persoonsgegevens en andere informatie. Daarnaast wil de gemeente Beuningen vanuit haar verantwoordelijkheid voor informatie een solide en betrouwbare partner zijn voor inwoners, bedrijven, ketenpartners en derden. Dit betekent dat de gemeente een inspanningsverplichting heeft om de processen en informatiesystemen zodanig in te richten en te beheren dat de betrouwbaarheid van de informatie gewaarborgd is. Dit doet de gemeente op basis van risicomanagement en hanteert hierbij de werkwijze van de BIO. De gemeente ziet dit niet als een eenmalige actie, maar als een continu proces, waarbij het beleid en de daarop gebaseerde wijze van werken voortdurend wordt aangepast en afgestemd op nieuwe ontwikkelingen. De omgeving waarin de gemeente haar werk doet verandert immers continu.

De gemeente wil daarnaast aantoonbaar ‘in control’ zijn op informatiebeveiliging. Dit betekent dat de gemeente weet welke processen en bijbehorende informatie(systemen) zij in huis heeft, welke passende technische en organisatorische beveiligingsmaatregelen er al zijn genomen en welke nog moeten worden ingericht. Ook betekent ‘in control’ dat de gemeente aan kan tonen dat de gegevensverwerking in overeenstemming met de geldende regelgeving wordt uitgevoerd en de beveiligingsmaatregelen toereikend en effectief zijn. Getroffen maatregelen dienen daarbij continu te worden geëvalueerd en indien nodig geactualiseerd. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de gemeentelijke organisatie (zie ook figuur 1).

Naast technische en organisatorische maatregelen zal de menselijke kant van informatiebeveiliging van blijvend belang blijven. Het beschermen van informatie is een verantwoordelijkheid van iedereen. Mensen kunnen echter pas verantwoordelijkheid nemen als ze weten wat er verwacht wordt en welke mogelijke gevaren er zijn. Het is daarom essentieel dat medewerkers adequaat getraind zijn en blijven op het gebied van informatiebeveiliging. De structurele bewustwording resulteert in een verhoogde weerbaarheid tegen de steeds veranderende dreigingen. Hiermee creëren we een sterke menselijke schakel in de informatiebeveiliging.

Ambitie

Het is een wettelijke verplichting en een maatschappelijk plicht, om de juiste maatregelen te nemen binnen de organisatie en in de techniek. Dit wordt uitgedrukt in volwassenheidsniveaus.



Figuur 1 : Volwassenheidsniveaus informatiebeveiliging en privacy

De beveiligingsvolwassenheid geeft aan hoe volwassen de gemeente Beuningen in de borging van beveiliging is. We hanteren het model van het Centrum Informatiebeveiliging en Privacybescherming (CIP) dat de volwassenheid in vijf volwassenheidsniveaus uitdrukt. De vijf niveaus worden gedefinieerd aan de hand van de mate waarin voldaan wordt aan de beveiliging. Het CIP vertaalt de wetgeving op het gebied van informatieveiligheid en privacy naar concrete, hanteerbare normen die duidelijk aangeven waar organisaties wat moeten regelen in hun beveiligingsbeleid, de uitvoering en de controle erop.

Het huidige volwassenheidsniveau van informatieveiligheid en privacy van de gemeente Beuningen ligt op basis van het Regionaal rekenkameronderzoek naar informatiebeveiliging en privacybescherming¹ ruwweg tussen niveau 1 en 2. De basis is op orde, maar de BIO en de Algemene Verordening Gegevensbescherming (AVG) vragen meer. Om de komende jaren naar het noodzakelijke niveau 3 toe te groeien is een gecoördineerde en gestructureerde aanpak noodzakelijk. In het tweede kwartaal van 2024 is hiervoor het plan van aanpak met uitvoeringsprogramma gereed. Het bevat een planning om stapsgewijs naar niveau 3 door te groeien. Zodra dat niveau bereikt is, heeft de organisatie informatieveiligheid geborgd binnen haar werkprocessen. Zij voldoet dan aan wet- en regelgeving én heeft voldoende kennis om proactief op ontwikkelingen te anticiperen.

¹ Rapport Weten wat je moet weten, juli 2022.

1.5 Speerpunten van beleid

De speerpunten die voor informatieveiligheid de komende jaren hoog op de agenda van de gemeente staan zijn:

1. **Dataclassificatie:** door aan informatie waarde toe te kennen, kunnen we het niveau van bescherming bepalen. In het verleden baseerden we de classificatie voornamelijk op de dataclassificatie van de gemeente Nijmegen en werd zo'n beetje alle informatie op hetzelfde (hoge) niveau ingedeeld. Hier hebben we onze maatregelen op aangepast. Met een eigen dataclassificatie kunnen we meer variëren in de beveiliging. Dit heeft als voordeel dat niet alles op het hoogste niveau beveiligd hoeft te worden. Maatregelen kunnen namelijk een verstorend effect hebben op het proces. Verder helpt de dataclassificatie om de risicobereidheid van de managers helder te krijgen. Zij kunnen dan beter inschatten welke risico's zij bereid zijn te accepteren en voor welke risico's er toch aanvullende maatregelen nodig zijn. Naast het verstorende effect dat maatregelen kunnen hebben, vergen ze namelijk ook tijd en geld om te implementeren en verwezenlijken.
2. **Risicomanagement:** het tweede speerpunt is risicomanagement. In het beschermen van de informatie speelt risicomanagement een essentiële rol. Wanneer we op gestructureerde wijze risico's in kaart brengen en evalueren, zijn we beter in staat om gerichte maatregelen te treffen. Daarom zal risicomanagement steeds meer geïntegreerd worden in het inrichten en uitvoeren van processen. Vanuit de accountant en interne controle/juridische kwaliteit maken we nu al risicoprofielen. Het risicomanagement informatiebeveiliging sluit hierbij aan.
3. **Bewustwording:** het derde speerpunt in het informatiebeveiligingsbeleid 2024-2027 is bewustwording. Ondanks dat medewerkers gemotiveerd zijn om veilig met gegevens om te gaan, gaat het soms mis. Criminelen worden steeds beter en succesvoller in het verkrijgen van toegang tot systemen en data via social engineering (alle trucs en technieken die criminelen gebruiken om mensen te verleiden om op links te klikken of gegevens achter te laten). Voortdurende training is daarom nodig om de bewustwording en kennis op peil te houden.
4. **Beleidsdocumenten:** het vierde speerpunt voor het informatiebeveiligingsbeleid 2024-2027 is het vaststellen en effectueren van aanvullende beleidsdocumenten en procedures. Dit informatiebeveiligingsbeleid zal samen met het privacy beleid dienen als kapstok voor deze aanvullende beveiliging- en privacy beleidsdocumenten, procedures en standaarden van de gemeente (voor schema zie samenvatting). De BIO schrijft deze documenten voor en ook uit de ENSIA-audit komt naar voren dat we de impact van dataclassificatie, risicomanagement en de gekozen maatregelen meer beleidsmatig moeten formaliseren.

Zoals in hoofdstuk 4 nog verder wordt toegelicht spelen het college, de gemeentesecretaris en het management een cruciale rol bij deze speerpunten. Het college is bestuurlijk verantwoordelijk en de gemeentesecretaris is samen met het management verantwoordelijk voor de uitvoering.

Met deze speerpunten groeien we toe naar een gemeente die informatieveiligheid zodanig organiseert dat steeds de afweging wordt gemaakt tussen enerzijds kans, dreiging, gevolgschade en anderzijds de kosten van de beschermingsmaatregelen voor het beperken van schade en de draagkracht van medewerkers. De gemeente zorgt ervoor dat binnen de gehele gemeentelijke organisatie verantwoordelijkheid wordt genomen voor informatieveiligheid met duidelijk ingevuld eigenaarschap. Ook zorgt de gemeente dat informatieveiligheid altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt (security by design). Verder is de gemeente aantoonbaar in control doordat ze informatieveiligheid verankert in de reguliere planning en control cyclus en zorgdraagt voor het periodiek uitvoeren van onafhankelijke onderzoeken en zelfevaluaties om het geheel voortdurend up-to-date te houden.

2. Het beleid

2.1 Doel

Het doel van dit beleid is om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente Beuningen te waarborgen en te verbeteren. Dit informatiebeveiligingsbeleid dient als kapstok voor aanvullende beleidsdocumenten en procedures, zoals voorgeschreven door de Baseline Informatiebeveiliging Overheid (BIO).

Hieronder enkele specifieke doelstellingen en ambities:

- Het implementeren van een effectief en efficiënt beveiligingsbeleid, rekening houdend met zowel technologische als menselijke aspecten.
- We streven ernaar aantoonbaar 'in control' te zijn op het gebied van informatiebeveiliging. Dit betekent weten welke processen en bijbehorende informatie(systemen) er zijn, welke beveiligingsmaatregelen zijn genomen en deze continu evalueren en actualiseren.
- We hebben de ambitie om naar volwassenheidsniveau 3 te groeien, zoals gemeten volgens het vijfpuntsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP).
- Dit beleid benadrukt het belang van een zorgvuldige omgang met persoonsgegevens, rekening houdend met de complexiteit van privacyvraagstukken in een gedigitaliseerde samenleving.
- Dit beleid erkent het belang van bewustwording en training van medewerkers op het gebied van informatiebeveiliging. Dit omvat het begrip van verantwoordelijkheden en bewustzijn van mogelijke bedreigingen.

De uitwerking van dit beleid in concrete acties en maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 Baseline Informatiebeveiliging Overheid

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de organisatie nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afweegt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Het BIO-normenkader is eind 2022 geëvalueerd. In oktober 2024 zal op basis van deze evaluatie BIO 2.0 worden geïmplementeerd.

2.2.2 Network and Information Security 2 en Wet beveiliging netwerk- en Informatiesystemen

De Europese Unie heeft een nieuwe richtlijn vastgesteld voor cyber security, namelijk de Network and Information Security directive (NIS2). Deze moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cyber security bij organisaties en bedrijven. In Nederland is de voorloper van deze richtlijn (NIS/NIB) opgenomen in de Wet beveiliging netwerk- en Informatiesystemen (Wbni). Naar

verwachting van de VNG zal het Ministerie van Binnenlandse Zaken op grond van NIS2 de gemeente aanwijzen als essentiële entiteit in de Wbni. Dit houdt onder meer in dat de gemeente een wettelijke zorgplicht krijgt voor informatieveiligheid plus een wettelijke meldplicht voor informatiebeveiligingsincidenten. Ook zal formeel toezicht worden gehouden op deze zorgplicht. Daarom is het cruciaal dat de gemeente door blijft gaan met de cyclus van plannen, uitvoeren, controleren en bijstellen rondom de complete BIO.

2.2.3 De 10 bestuurlijke principes voor informatiebeveiliging (zie bijlage 1)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de raad en het college zichzelf opleggen. De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen hen bij het (laten) uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.2.4 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

Het IBD-dreigingsbeeld 2023-2024 laat het volgende beeld zien:

- meer ransomware met destructievere gevolgen
- steeds meer en ernstiger kwetsbaarheden in software
- gevaren toenemende ketenintegratie; minder zicht op veiligheid

2.2.5 Informatie uit incidenten en inbreuken op de beveiliging

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid. Hierbij werkt de gemeente samen met iRvN en gemeenten in de regio.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.

Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek² in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook worden praktische operationele handreikingen uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan.

De inhoud en structuur van deze nota zijn afgestemd op die van de International Organization for Standardization (ISO) en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Dit zijn systemen die zorgen voor de besturing van apparaten door middel van Proces Automatisering (PA), zoals bij gemalen, gebouw alarmering en verkeerslichten. Onder het beveiligingsbeleid valt ook de ruimte van PA; het beleid treft dan ook beleidsafdelingen die zich met PA bezighouden.

2.4 Plaats van het beleid

Dit beleid wordt gebruikt om de basis te leggen voor de beleidsplannen en daarmee richting te geven aan de verdere invulling van informatiebeveiliging.

2.5 Scope informatiebeveiliging

De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit gemeentelijk informatiebeveiligingsbeleid is een algemene basis en dekt samen met het privacy beleid de aanvullende beveiligingseisen uit wetgeving af zoals voor de Basisregistratie Personen (BRP), Waardedocumenten, de beveiligingsnorm DigiD, de Basisregistratie Adressen en Gebouwen (BAG), de Wet politiegegevens (Wpg), de Algemene Verordening Gegevensbescherming (AVG) en de Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI). Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI, Wpg en gemeentelijke basisregistraties). Deze worden in aanvullende documenten geformuleerd. Bewust wordt in het beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar dit beleid gelegd.

² De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

2.6 Uitgangspunten

Het managementteam speelt een cruciale rol bij het uitvoeren van het informatiebeveiligingsbeleid. Het managementteam schat het belang in van informatievoorziening voor verschillende afdelingen van de gemeente, is zich bewust van de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het managementteam dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.6.1 Doelen

De doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- Het college is eindverantwoordelijk voor de informatiebeveiliging.
- Het informatiebeveiligingsbeleid is van toepassing op alle gemeentelijke processen, onderliggende informatiesystemen (waaronder Suwinet en BRP), procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. En omvat daarmee niet alleen op de verwerking, uitwisseling en opslag van digitale informatie, maar ook op de informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip of de gebruikte apparatuur.
- De bescherming van Proces Automatisering (PA) valt ook onder dit beveiligingsbeleid en daarmee ook (beleids)afdelingen die zich met PA bezighouden.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het managementteam. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Beuningen hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de

informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
- Informatiebeveiliging richten we in door een slimme combinatie van technische en organisatorische maatregelen. We kiezen daarbij bij voorkeur voor veilig faciliteren in plaats van verbieden, waar nodig schermen we informatie af. Techniek faciliteert een verantwoorde informatiebeveiliging, maar mag niet onnodig belemmerend werken.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Verantwoord en bewust gedrag is essentieel voor informatieveiligheid. We verwachten dat medewerkers bewust en verstandig omgaan met de informatie die ze nodig hebben voor hun werk, zij worden daarbij ondersteund door hun leidinggevende. Waar medewerkers zich niet aan afspraken houden worden ze hierop aangesproken.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het college stelt het informatiebeveiligingsbeleid vast.
- Het managementteam stelt jaarlijks het informatiebeveiligingsplan vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke beleidsregels die aanvullend zijn op het informatiebeveiligingsbeleid.
- Het managementteam is verantwoordelijk voor het vragen om informatie aan vakspecialisten en kwaliteitsmedewerkers en neemt adequate maatregelen voor de bescherming van de informatie, informatiesystemen en procesautomatiseringssystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het managementteam, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken is aandacht voor de informatiebeveiliging uit de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, worden opgenomen in de auditplannen.
- De managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De managers zijn verantwoordelijk voor het oefenen met informatiebeveiligingsincidenten en bedrijfscontinuïteit.
- Hoewel de basiskernregistraties (zoals BRP, PUN, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de gestelde doelen.
- De gemeente traint alle medewerkers in het gebruik van beveiligingsprocedures.
- Medewerkers gaan verantwoord om met persoonsgegevens en andere informatie.
- Managers zien toe op de regelmatige uitvoering van controle op het verwerken van persoonsgegevens, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.

- De gemeente bepaalt de beveiligingsmaatregelen op basis van risicomanagement. Managers laten quickscans informatiebeveiliging uitvoeren door vakspecialisten of kwaliteitsmedewerkers op basis van de BIO om risico-afwegingen te kunnen maken.
- Informatiebeveiliging maakt deel uit van de beoordelingssystematiek tijdens het gesprek tussen manager en medewerker.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- De gemeente bevordert en borgt actief de kennis en het bewustzijn van informatiebeveiliging en het omgaan met persoonsgegevens binnen de organisatie.
- Jaarlijks laat de Chief Information Officer (CIO) een informatiebeveiligingsplan opstellen, gebaseerd op:
 - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
 - Het dreigingsbeeld gemeenten van de IBD;
 - De door de managers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een rekenkamerrapport.

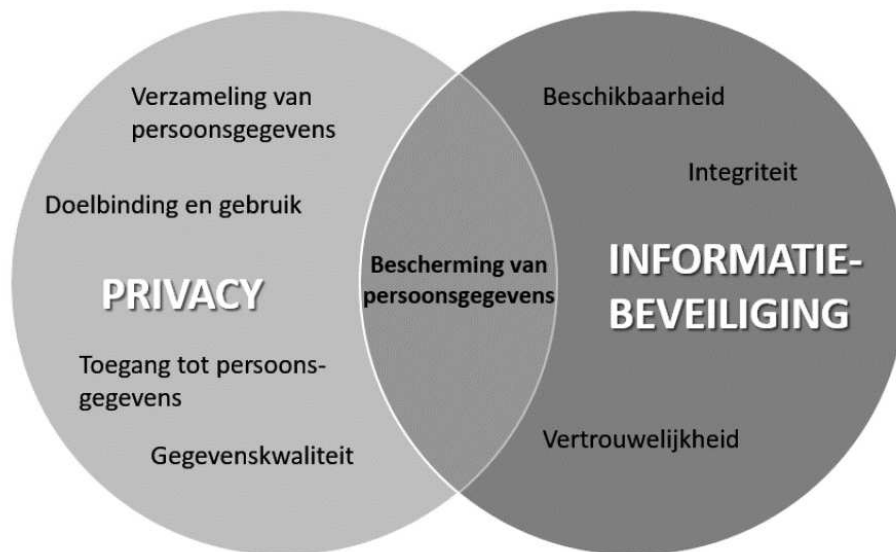
Door de snelle ontwikkelingen van de techniek verouderen maatregelen voor informatiebeveiliging snel. Het beleid wordt daarom jaarlijks - of eerder als zich significante veranderingen voordoen - beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.

3 Samenhang privacybescherming en informatiebeveiliging

Er is een nauwe samenhang tussen privacybescherming en informatiebeveiliging. Het zijn twee verschillende begrippen, maar wel met een gemeenschappelijk raakvlak. Privacybescherming gaat over het vertrouwelijk omgaan met persoonlijke gegevens en deze voldoende beschermen. Informatiebeveiliging gaat over de beschikbaarheid, integriteit en vertrouwelijkheid van alle (gevoelige) informatie. Zowel informatiebeveiliging als privacy vragen om een risico gedreven aanpak.

Privacybescherming en informatiebeveiliging zijn twee terreinen die met elkaar verbonden zijn. In de bescherming rond persoonsgegevens hebben beide een eigen en een gezamenlijke taak.

Dit blijkt ook uit de AVG (art. 5, lid 1, f) waarin staat dat persoonsgegevens op een veilige manier verwerkt moeten worden door het nemen van de juiste technische en organisatorische maatregelen. Maatregelen die ervoor zorgen dat het verwerken van persoonsgegevens op een passende beveiliging kan rekenen. Op het bijgevoegde plaatje is de overlap duidelijk aangegeven.



Figuur 2: Samenhang Privacybescherming en Informatiebeveiliging

Informatiebeveiliging maakt daarmee een onderdeel uit van de bescherming van persoonsgegevens. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Normenkaders als de BIO helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. Hoe de gemeente omgaat met privacybescherming en de AVG is beschreven in het privacy beleid van de gemeente Beuningen.

4 Organisatie, taken en verantwoordelijkheden

Dit hoofdstuk beschrijft welke taken en verantwoordelijkheden inzake informatiebeveiliging horen bij welke afdeling en manager. De hiervoor gebruikte aanpak volgt het Three Lines of Defence (3LoD). In dit model is in de eerste lijn het management verantwoordelijk voor de eigen processen. De tweede lijn (CISO) ondersteunt, adviseert, coördineert en bewaakt of het management haar verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn voorziet een (interne) auditor het geheel van een objectief oordeel met mogelijkheden tot verbetering.

4.1 Aansturing: managementteam

Het managementteam zorgt dat alle processen en systemen en daarbij behorende middelen onder de verantwoordelijkheid van een manager vallen. Het managementteam legt verantwoording af over de beveiliging van de informatie. Het managementteam informeert de eindverantwoordelijke portefeuillehouder binnen het college gevraagd en ongevraagd over de mate van informatiebeveiliging in het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het managementteam stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het managementteam draagt zorg voor het uitwerken van informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. De gemeente Beuningen ziet het onderwerp informatiebeveiliging als een integraal onderdeel van risicomanagement.

4.2 Uitvoering: managementteam

Informatiebeveiliging valt onder de verantwoordelijkheid van het managementteam. Om deze verantwoordelijkheid waar te maken krijgen zij goede ondersteuning vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal één eigenaar hebben. Er is dus altijd iemand verantwoordelijk. Het managementteam rapporteert aan het college over de door hen uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken.

Taken die de managers in het kader van informatiebeveiliging (laten) uitvoeren, zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wetgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wetgeving bedacht is.
- Het binnen de eigen afdeling(en) uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

4.3 Controle en verantwoording

Dit beleid is een verantwoordelijkheid van het bestuur van de gemeente Beuningen. De raad, het college en het managementteam van de gemeente Beuningen geven volgens de 10 principes voor informatiebeveiliging richting en sturing aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

Het managementteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan respectievelijke portefeuillehouders. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van beleidsonderwerpen die aanvullend zijn op dit informatiebeveiligingsbeleid.

4.3.1 ENSIA

De gemeente verantwoordt zich over informatiebeveiliging via de ENSIA-systematiek. De CISO is als ENSIA-coördinator aangewezen. Deze haalt de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA op bij de verantwoordelijke managers. De managers leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Een bij NOREA geregistreerde IT-auditor controleert de collegeverklaring voor de domeinen DigiD en Suwinet en stelt een Assurancerapport op dat wordt gevoegd bij de verantwoordingsstukken.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college aan in hoeverre de gemeente voldoet aan de gemaakte afspraken voor de ENSIA-verantwoording Informatiebeveiliging. Ook zijn verbetermaatregelen vermeld die de gemeente gaat treffen.

Met de collegeverklaring informatiebeveiliging informeert het managementteam het college en de raad van de gemeente Beuningen. De betrokkenheid van het college en de raad is essentieel en laat zien dat

de gemeente Beuningen informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Bijlage 1. De 10 Principes voor informatiebeveiliging volgens VNG

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren, zowel binnen de eigen organisatie, maar ook daarbuiten. Als professionele organisatie past hierbij dat de gemeente ook de beveiliging van informatie adequaat organiseert. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moet de gemeente te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid heeft om de gegevens van de inwoners onder alle omstandigheden te beschermen.

Bestuurlijke aanvulling op de normen en regels

De principes gaan over waarden die de bestuurders en managers zichzelf opleggen. Deze waarden zijn verbonden aan de waarden van de organisatie. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1. Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium. Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als de organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunnen we adequaat reageren op dreigingen en samenhangende risico's.

2. Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement. Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik de Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen de organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3. Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten. Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak managers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Managers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4. Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is 'chefsache'. U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee

te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6. Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7. Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8. Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt. Verbetering komt voort uit leren en ervaring.

9. Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed de informatiehuishouding ook beveiligd is, incidenten blijven altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10. Het bestuur controleert en evalueert

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp.

Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.