

Bijlage A - Wat beschermen we, waarom, hoeveel bescherming is nodig

Achterliggende motivatie om te beveiligen

Informatie, processen en documenten van een gemeente zijn van groot belang voor de maatschappij. De impact kan groot zijn als bijvoorbeeld informatie niet beschikbaar is, als informatie niet klopt, als vertrouwelijke informatie op straat ligt, of als personen worden verwisseld. Deze impact raakt primair burgers en bedrijven die van de gemeente afhankelijk zijn, maar als incidenten regelmatig plaatsvinden dan gaat dat ten koste van het vertrouwen in de overheid en zet dit uiteindelijk vraagtekens bij de legitimiteit van het bestuur.

Hierbij komt dat het openbaar bestuur zelf controleerbaar moet zijn. In voorkomende gevallen moeten burgers en bedrijven zich ook beschermd weten tegen de overheid zelf.

Het maatschappelijk belang en de controleerbaarheid van de overheid zijn intrinsieke redenen waarom informatiebeveiliging bij een gemeente robuust en op een hoog niveau moet zijn gerealiseerd.

Daarnaast gelden diverse externe kaders waaraan een gemeente moet voldoen en zijn er diverse toezichthouders. Deze externe kaders ankeren uiteindelijk allemaal in het maatschappelijke belang en in de controleerbaarheid van de overheid, en sluiten daarmee aan bij de eerdere intrinsieke redenen om goed te willen beveiligen.

Concretiseren van de behoefte aan beveiliging

Om informatiebeveiliging concreet te kunnen maken wordt vaak gewerkt vanuit drie kwaliteitsaspecten, samengevat als BIV:

- Welke eisen stel je aan **B**eschikbaarheid?
- Welke eisen stel je aan **I**ntegriteit, oftewel: hoe weinig inhoudelijk foute informatie of foute uitkomsten van een proces kun je je veroorloven?
- Welke eisen stel je aan **V**ertrouwelijkheid?

Bij hoge Beschikbaarheid kunnen maatregelen genomen worden als het dubbel uitvoeren van systemen, frequente backups, het testen van herstelplannen, voorbereiden van werkprocessen waarmee een periode zonder ICT zou kunnen worden overbrugd.

Bij hoge Integriteit kunnen maatregelen genomen worden als strakke toegangsrechten, Multi-Factor authenticatie, vier-ogen principe, review van loggings, verbandscontroles binnen applicaties, audits.

Bij hoge Vertrouwelijkheid kunnen maatregelen genomen worden als strakke toegangsrechten, Multi-Factor authenticatie, een afgescheiden netwerk, fysieke afscherming van werkplekken, blinderen van ramen, beperking van mogelijkheden om te printen, versnipperaars op de gang, beperken van toegang op afstand, versleutelen van bestanden, screenen van personeel

Het grondig uitvoeren van een classificatie naar aspecten B, I en V is veel werk. Omdat alle gemeenten in essentie dezelfde processen hebben, is hieronder teruggegrepen op werk dat de IBD voor alle gemeenten heeft uitgevoerd. Het document van de IBD is toegevoegd als Bijlage B, als vertrekpunt dient de tabel op pagina 16 van dat document die zijn oorsprong heeft in 2007.

Sinds 2007 heeft de wereld niet stil gestaan. Er zijn inhoudelijke veranderingen geweest waardoor namen zijn veranderd, er zijn taken verschoven, maar de essentie van de tabel staat nog steeds overeind.

Een grotere verandering is dat het werken met ICT veel dieper is doorgedrongen in de processen dat en het werken met / delen van data enorm is toegenomen. Als het digitale aandeel groter wordt, dan krijgen de digitale risico's een groter gewicht en verschuift de classificatie mogelijk naar een hoger niveau.

Hieronder staat de tabel uit het document van de IBD gekopieerd, waaraan in lichtgroen een aantal regels is toegevoegd die te maken hebben met de andere manieren van werken met ICT en data.

Proces	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Burgerzaken (klantbegeleiding, afspraken)	Noodzakelijk	Absoluut	Vertrouwelijk
Basisregistratie persoonsgegevens	Essentieel	Absoluut	Geheim
Overige basisregistraties	Essentieel	Absoluut	Openbaar
Indienen en behandelen beroep en bezwaarschriften	Belangrijk	Absoluut	Openbaar/ vertrouwelijk
Registratie ingekomen post burgers en bedrijven	Belangrijk	Hoog	Bedrijfsvertrouwelijk
Beheren gevonden voorwerpen	Belangrijk	Beschermd	Openbaar
Bedrijvenloket	Belangrijk	Beschermd	Openbaar
Publicatie van ruimtelijke plannen	Belangrijk	Absoluut	Openbaar
Grootschalige Basiskaart Nederland (GBKN)	Belangrijk	Absoluut	Openbaar
Kenbaarstelling Publiekrechtelijke Beperkingen (WKPB)	Belangrijk	Absoluut	Openbaar
Registratie risico's gevaarlijke stoffen (risicokaart)	Essentieel	Absoluut	Bedrijfsvertrouwelijk
Bodembeheer	Belangrijk	Hoog	Openbaar
Aanvraag en verlening vergunning	Belangrijk	Absoluut	Vertrouwelijk
Bouw- en woningtoezicht	Belangrijk	Absoluut	Vertrouwelijk
Financieel beheer (betalingen leges, et cetera)	Belangrijk	Hoog	Vertrouwelijk
Aangifte en heffing gemeentelijke belastingen/ heffingen	Belangrijk	Hoog	Vertrouwelijk
Waardebepaling Onroerende Zaken (WOZ)	Belangrijk	Hoog	Bedrijfsvertrouwelijk
Sociale Zaken — Uitvoering / verstrekking voorzieningen	Essentieel	Hoog	Geheim
Sociale Zaken — Handhaving en controle	Belangrijk	Absoluut	Geheim
Openbare orde en veiligheid (brandweer, preventie, rampbestrijding)	Essentieel	Absoluut	Geheim
Handhaving en toezicht gemeentelijke verordeningen / regelgeving	Belangrijk	Absoluut	Vertrouwelijk
Gezondheidszorg — GGD taak / ambulancedienst	Noodzakelijk	Absoluut	Geheim
Camera's, communicatie en andere voorzieningen waarmee veiligheid van publiek en handhavers wordt bewaakt	Essentieel	Absoluut	Vertrouwelijk
Ondersteuning en aansturing van Verkeersregel Installaties, Bruggen, Sluizen, Pollers en dergelijke	Essentieel	Absoluut	Basis
Sensoren, Smart City ontwikkelingen afhankelijk van de rol en het proces	Belangrijk - Essentieel	Beschermd - Absoluut	Openbaar – Geheim
In meer domeinen:			
Datagedreven werken, inclusief uitwisselen met derden en het combineren van gegevens waardoor deze gevoeliger worden	Belangrijk	Hoog	Geheim
Onderzoeken en evalueren van de effectiviteit van beleid in samenwerking met derde partijen	Belangrijk	Hoog	Vertrouwelijk
Beleid en besluiten in de fase voordat de inhoud ervan algemeen bekend is, en voorkennis erover van waarde kan zijn	Belangrijk	Beschermd	Vertrouwelijk
Geheime stukken	Belangrijk	Hoog	Geheim

De termen worden als volgt vertaald:

Vertaling	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Hoog	Essentieel	Absoluut	Geheim
Midden	Noodzakelijk	Hoog	Vertrouwelijk
Basis	Belangrijk	Beschermd	Bedrijfsvertrouwelijk

Relatie met het Beveiligingsplan

In het Beveiligingsplan staan twee activiteiten opgenomen waarin prioriteitstelling / volgorde wordt vastgesteld aan de hand van de classificatie op aspecten B, I en V.

Het betreft hier activiteit 2 (Formaliseren van eigenaarschap) en activiteit 6 (Uitvoeren van Risico Analyses)