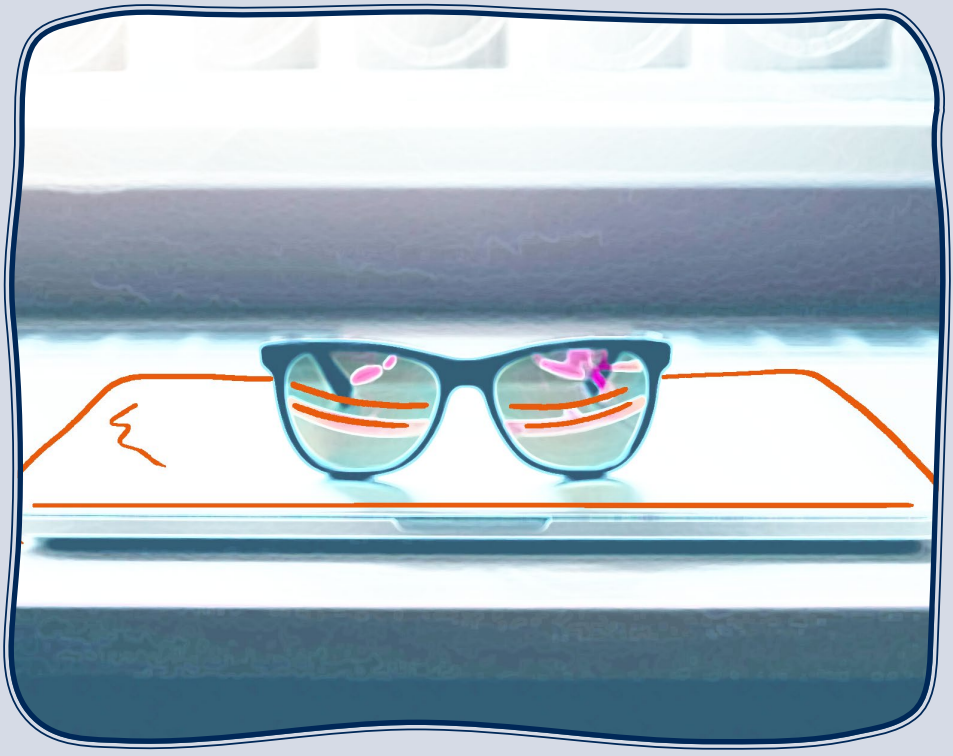
Gemeenten. Bewustzijn. Privacy.



Het handboek voor informatiebewustzijn bij de lokale overheid

Martine van de Merwe
Renco Schoemaker Erna Havinga

Gemeenten.
Bewustzijn.
Privacy.

Het handboek voor informatiebewustzijn
bij de lokale overheid

Martine van de Merwe
Renco Schoemaker
Erna Havinga

privacylab
IB&P
Dat gaat je niets aan

Inhoud

Waarom dit boek

In 2018 verscheen het boek “Zorg voor privacy”, geschreven door Martine van de Merwe. Dat boek hebben we beiden met veel belangstelling gelezen. Privacy is een belangrijk recht, alhoewel niet absoluut. Informatie geeft macht en dat geldt zeker ook in het overheidsdomein. Gemeenten verwerken op grote schaal persoonsgegevens voor de uitoefening van taken en zowel burgers als bedrijven moeten ervan op aan kunnen dat al die persoonsgegevens bij de overheid in goede handen zijn. Uitsluitend technische (beveiligings)maatregelen nemen is nooit genoeg. Uiteindelijk zijn en blijven het mensen die werken met persoonsgegevens. Het lukt dus alleen als medewerkers zich bewust zijn van hun rol in het veilig houden van al deze gevoelige informatie. Dit boek zal daar een bijdrage aan leveren.

Met de komst van de AVG is de aandacht voor privacy, of beter: gegevensbescherming, flink toegenomen. Dit is ook bij gemeenten het geval en het is nu zaak die aandacht vast te houden. Niet primair om een boete van de toezichthouder te voorkomen, maar omdat de bescherming van persoonsgegevens een fundamenteel onderdeel is van de publieke dienstverlening. Daarnaast zijn burgers mondiger geworden en weten zij hun privacyrechten beter uit te oefenen.
Tot slot dwingt ook de toenemende samenwerking in ketens gemeenten tot een zorgvuldige en veilige verwerking van persoonsgegevens. Allemaal redenen om als gemeente van harte transparantie na te streven met betrekking tot de verwerking van persoonsgegevens.

Medewerkers van gemeenten oefenen hun vak professioneel en gemotiveerd uit. Een goede dienstverlening aan burgers en bedrijven (en aan de medewerkers van de gemeente zelf) staat voorop.
Het goed en netjes regelen van de informatiebeveiliging en de privacy is een onderdeel van die goede dienstverlening. Het gedrag van mensen is een belangrijk onderdeel van een veilige omgang met gegevens. Over hoe je die mensen bereikt en kunt helpen om te kiezen voor veilig gedrag, gaat dit boek. Sommige medewerkers hebben op het eerste gezicht niet zoveel op met beveiliging en privacy. Dat is schijn. Onze ervaring is dat ze de privacy van de burger, en de eigen privacy, een belangrijk onderdeel van het vak vinden. En ze snappen best dat gegevens beveiligd dienen te worden. Toch is het niet altijd makkelijk om ze te bereiken.

Bij diverse gemeenten mislukten pogingen om te werken aan bewustwording. Zonde van de tijd en energie. Dat moet beter kunnen. Gemeenten hebben al erg veel te regelen om alle producten en diensten te faciliteren en om aan alle eisen en verwachtingen van de omgeving te voldoen. Je kunt niet verwachten dat gemeenten op alle terreinen experts in huis hebben. Daarom hebben we een stappenplan ontwikkeld om gemeenten zo te helpen dat hun inspanningen wél effect hebben.

Omdat het niet om eenmalige acties gaat, is het een cyclisch model. Het PrivacyLab-bewustwordingsmodel van Martine van de Merwe, maar dan toegespitst op gemeenten, staat beschreven in deel 2 van dit boek.

Dit boek is een handreiking voor die CISO, functionaris voor gegevens-bescherming (FG), privacy officer of wie dan ook, die de taak heeft aan de slag te gaan met veilig gedrag van medewerkers bij gemeenten.

Het belang van privacy en goede, veilige dienstverlening aan burgers en bedrijven maken dat wij met volle inzet werken om gemeenten te helpen. Dit boek is bedoeld om daar ook een bijdrage aan te leveren.

Renco Schoemaker - IB&P
Erna Havinga - IB&P

Omdat de informatie in mijn boek “Zorg voor privacy, het handboek voor privacybewustzijn in de zorg”, breder toepasbaar is dan alleen in de zorg, heb ik Erna en Renco gevraagd het boek te bewerken.
Met hun diepgaande kennis van de lokale overheid hebben zij een waardevol boek samengesteld met informatie, speciaal gericht op gemeenten. Zo kan ook daar effectief aan bewustwording gewerkt worden en krijgt het handboek een groter bereik. De grote hoeveelheid gevoelige informatie bij gemeenten verdient een goede bescherming.

Martine van de Merwe - PrivacyLab

Mei 2019

Inleiding

Privacy is een grondrecht. Je hebt het recht om te leven zonder dat anderen van alles over je weten en om zelf te bepalen wie welke informatie over jou heeft. In de huidige tijd, waar je niet ziet of weet waar welke informatie over jou blijft, hebben mensen het gevoel dat privacy-schendingen onvermijdelijk zijn. Tegelijkertijd maken mensen zich zorgen over privacy. In Europa heeft dat geleid tot wetgeving die als doel heeft mensen in de gelegenheid te stellen hun grondrecht uit te oefenen: Algemene Verordening Gegevensbescherming (AVG), van toepassing sinds 2018.

Betrokkenen, bij gemeenten zijn dat met name burgers en medewerkers, hebben in de AVG meer rechten gekregen: het recht op informatie, inzage, correctie en verwijdering. Verder schrijven de AVG en andere wet- en regelgeving voor dat je informatie moet beveiligen. Je dient te waarborgen dat informatie vertrouwelijk blijft, juist is en beschikbaar wanneer nodig. De maatregelen hiervoor noemen we informatie-beveiliging. Dat is voor een deel een technisch verhaal, maar ook een verhaal waarbij het gedrag van mensen een grote rol speelt.

Deel 1 van dit boek vertelt wat er mis kan gaan en geeft meer achter-gronden van informatiebeveiliging en privacy. **Deel 2** van het boek beschrijft het PrivacyLab-model voor informatiebewustzijn bij gemeenten. Het model bestaat uit zes stappen die samen het kader vormen om effectief te werken aan bewustwording op het gebied van informatie-beveiliging en privacy bij een gemeente.

Mensen enthousiasmeren en motiveren is niet altijd makkelijk. Dat geldt zowel voor management en bestuur, als voor mensen die direct met burgers en bedrijven werken. *Het moet van de wet* is niet genoeg om collega's mee te krijgen. Dit boek geeft zowel inhoudelijke informatie als een stappenplan om een degelijk bewustwordingsprogramma op te zetten. Het wiel is tenslotte al uitgevonden. Met de informatie en het stappenplan kun je zelf efficiënt en effectief aan de slag.

Deel 1

Het belang van informatiebeveiliging en privacy bij gemeenten

6. Wat is een bewust-wordingsprogramma?

Continuïteit en samenhang zijn nodig om op langere termijn effectief aan bewustwording en een veiligheidscultuur te werken. Om resultaat te bereiken werk je daarom meestal in een bewustwordingsprogramma. We zien dat gemeenten vaak uit zichzelf wel weten dat ze iets aan bewustwording moeten doen, of dat een bepaalde leverancier of adviseur ze dat heeft verteld. Dan wordt er één activiteit uit de kast getrokken, bijvoorbeeld een e-learning voor alle medewerkers, en daarna blijft het stil. Dat zorgt misschien voor een korte opleving, maar heeft weinig blijvend resultaat. Om succes te hebben kun je beter een geheel van plannen maken, binnen een *programma*.

De mens in het proces van informatiebeveiliging

Het proces van informatiebeveiliging bestaat uit de stappen *voorkomen – detecteren – behandelen – leren*. Preventieve maatregelen zijn erop gericht te voorkomen dat zich incidenten voordoen.

Praktijkvoorbeeld

Neem als voorbeeldincident een brand in de serverruimte. Preventieve maatregelen zijn een rookverbod en onderhoud van kabels en apparatuur om kortsluiting te voorkomen. Als zich dan toch een incident voordoet, wil je dat zo snel mogelijk ontdekken. De maatregelen die je daarvoor treft noemen we detectieve maatregelen. In geval van brand is dat een rookmelder of temperatuuralarm. Daarna wil je de gevolgen van het incident zo klein mogelijk houden door middel van repressieve maatregelen. Bij brand kun je dan denken aan blusmiddelen en brandwerende deuren die verspreiding tegengaan. Daarna tref je herstelmaatregelen om de oude situatie terug te brengen, bijvoorbeeld de ruimte schoonmaken, nieuwe apparatuur installeren of back-ups terugzetten. De laatste stap is dan het leren van het incident. Hoe kunnen we voorkomen dat zoiets zich een volgende keer voordoet? Op basis daarvan breng je de informatiebeveiliging naar een hoger niveau.

Bewustwording bij medewerkers helpt met name om de stappen *voorkomen* en *detecteren* krachtiger te maken. Bewuste mensen veroorzaken minder incidenten. Ook hebben ze een belangrijke rol in het detecteren. Als CISO achter je bureau kun je niet weten wat er elders in de organisatie gebeurt. Neem de metafoor van een voetbalstadion met een heleboel doelen. Jij probeert al die doelen dicht te krijgen: bij de één zet je een muurtje neer, voor de ander hang je een net en de derde leg je plat op de grond. Een aanvaller weet waar alle doelen staan en kan rustig één voor één proberen te ontdekken waar nog ergens een gat zit. Denk aan een hacker die alle bekende kwetsbaarheden van systemen uitprobeert. Als het stadion nu vol zit met 50.000 mensen die de aanval zien aankomen en jou waarschuwen, dan wordt je taak stukken eenvoudiger! Zo kun je ook gebruik maken van de inzichten van alle medewerkers binnen jouw gemeente.

Onderdeel van het bewustwordingsprogramma is dus altijd om mensen te vragen een rol te spelen in de detectie-stap van het informatiebeveiligingsproces. Zodat de organisatie kan leren van incidenten of bijna-incidenten.

6.1. Totstandkoming van het PrivacyLab-model

Marktonderzoek is de basis geweest voor de ontwikkeling van het PrivacyLab-model. Martine, auteur van ‘Zorg voor privacy’, heeft vele organisaties bezocht om met IT-managers, informatiemanagers, CISO’s, interne auditors, privacy officers, juristen en anderen te praten over wat werkt en wat niet op het gebied van bewustwording. Naast deze interviews heeft ze een literatuurstudie gedaan in boeken, tijdschriften en andere publicaties. Ook bezocht ze diverse conferenties in binnen- en buitenland. Alles gericht op bewustwordingsprogramma’s, gedragsbeïnvloeding, risicomanagement, training en wat er nog meer bij komt kijken. Dit heeft geleid tot dit model met zes fases. Per fase zijn activiteiten gedefinieerd die kunnen bijdragen aan het bereiken van de doelen van die specifieke fase. De resultaten van al deze werkzaamheden kun je teruglezen in de komende hoofdstukken van dit boek.

John P. Kotter is een autoriteit op het gebied van verandermanagement. Hij schreef de bestseller ‘Leiderschap bij verandering’[12], waarin hij acht stappen benoemt die zorgen voor succesvolle verandering in organisaties. Meestal gaat het om grote cultuur- of organisatie-veranderingsprocessen.

Het onderwerp van dit boek is van een andere orde. Toch hebben we ervoor gekozen de theorie van Kotter te laten terugkomen in het model. De acht stappen van Kotter zijn beschreven in de verschillende fases van het bewustwordingsmodel, omdat je bij cultuurverandering op het gebied van informatiebeveiliging en privacy veel kunt leren van de lessen van Kotter.

Gouden driehoek: people – processes – technology

Gouden driehoek is de term die gebruikt wordt voor de mix van elementen: mensen, processen en technologie (ook wel: mens, techniek en organisatie). In de informatiebeveiliging is de afgelopen decennia veel geïnvesteerd in technische maatregelen, die veel vruchten afwerpen. Laat er geen misverstand over bestaan dat deze technische maatregelen nuttig en noodzakelijk zijn. Maar als mensen er niet op de juiste manier mee omgaan, of er zijn onvoldoende processen ingericht om de techniek zijn werk te laten doen, dan is de beveiliging niet effectief. En is het niet zo dat veel technische maatregelen worden ingeregeld door mensen, die daarbij keuzes maken, en misschien zelfs vergissingen? Als mensen in een organisatie weerbaar en alert zijn, is dat waardevol in combinatie met techniek en processen. Het PrivacyLab-model is bedoeld om die weerbaarheid en alertheid te vergroten, en via steeds veiliger gedrag te komen tot een veiligheidscultuur.

6.2. Randvoorwaarden voor een succesvol bewustwordingsprogramma

Er is meer nodig dan een enkele training

Praktijkvoorbeeld

Veel auditors vinken het onderwerp 'bewustwording' af als je eenmaal per jaar iets doet voor alle medewerkers, hoe beperkt ook. Of er resultaat is, wordt niet echt bekeken. En zelfs als je een perfecte, interessante training aflevert, dan nog zal het effect beperkt zijn als het blijft bij een eenmalige activiteit. In de drukte van alledag, waar de aandacht vooral uitgaat naar dienstverlening, verdwijnt het onderwerp weer naar de achtergrond. Dat is logisch en kun je medewerkers niet kwalijk nemen. Het blijft nu eenmaal een onderwerp dat bij de meeste ambtenaren niet vanzelf hoog op de agenda staat.

1. Werk volgens een structuur

Hersenen zijn goed in het filteren van informatie. Als je steeds hier en daar een losse activiteit lanceert, zien mensen de samenhang niet. Werkend in een programma kun je zorgen voor herkenbaarheid waardoor die samenhang wel helder wordt. Je doelgroep kan de achtergronden oppikken en daardoor wordt de informatie en motivatie beter vastgehouden. Structuur helpt veel mensen en het is goed als je die kunt bieden. Probeer daarom al je activiteiten met elkaar in verband te brengen.

2. Periodieke en continue activiteiten

Om nieuwe gewoontes te verankeren, is veel meer nodig, namelijk een consistent, herkenbaar bewustwordingsprogramma dat organisatiebreed wordt ondersteund. Om niet te verslappen is herinnering in de vorm van het telkens in aanraking komen met het onderwerp, gecombineerd met het erover praten met collega's, noodzakelijk. Een schokkende presentatie kan als start een gevoel van urgentie creëren. Maar om effectief te zijn, moet je meer doen.

Praktijkvoorbeeld

Eenmalig vertellen helpt niet voldoende om gewoontes te veranderen. Je kunt zeker gebruik maken van een presentatie waarin mensen schrikken van de risico's die ze lopen. Kort daarna letten ze misschien beter op. Maar ja, we zijn allemaal maar mensen, en we vallen snel terug op ingesleten patronen. Volgens diverse theorieën is er een langere periode nodig. De ene theorie zegt 21 dagen, de andere 100 dagen. En dan gaat het om dagelijkse handelingen of activiteiten die je dus tot 100 keer anders moet hebben uitgevoerd voordat het nieuwe gedrag een gewoonte is geworden. De gewoontes waar we het bij veilig gedrag over hebben, zijn meestal niet dagelijks, waardoor terugval eerder zal optreden.

Periodieke en continue activiteiten zijn nodig. Bij periodieke activiteiten kun je denken aan trainingen, zodat de medewerkers eens in de zoveel tijd met het onderwerp informatiebeveiliging en privacy in aanraking komen. Parallel hieraan zijn er doorlopende activiteiten, zoals posters met een aandachtspunt, continue informatie op intranet, en iedere zoveel weken een nieuwsartikel. Als je hiervan een mix realiseert, zet je een grote stap naar verder bewust gedrag. Het is wel belangrijk om dit in samenhang uit te voeren; planmatig en met de juiste accenten. Dan kun je het geheel uitwerken in een programma, dat ervoor zorgt dat inhoud en timing van activiteiten je doelen goed ondersteunen.

3. Werk op langere termijn

Cultuur verander je niet van de ene op de andere dag. We raden je aan om met langetermijndoelen te werken en die op te breken in doelen voor een jaar. Die zijn overzichtelijk genoeg om je activiteitenplan op te baseren. Houd wel in gedachten dat het een kwestie is van de lange adem. Steun van het management (en idealiter ook van het bestuur) is onontbeerlijk om het op deze manier aan te kunnen pakken. Werk aan kleine stapjes met de grotere doelen als leidraad. Het uiteindelijke doel is cultuurverandering, maar dat bereik je pas als nieuwe en veilige gewoontes over een langere periode zichtbaar resultaat opleveren. Dat het resultaat zichtbaar moet zijn om te motiveren, geldt overigens niet alleen voor het management, maar voor alle medewerkers.

4. Houd rekening met de cultuur

Praktijkvoorbeeld

Behulpzaamheid is een kenmerk van de cultuur bij gemeenten. Mensen die bij gemeenten werken willen graag van maatschappelijke betekenis zijn en anderen helpen. Daar ligt hun focus. Dat anderen daar misbruik van maken, is soms moeilijk voorstelbaar. Wie wil er nu handel drijven met kopieën van paspoorten van kwetsbare burgers die zorg krijgen? Helaas is dat wel de realiteit en dienen ook ambtenaren hier alert op te zijn, zonder de dienstbaarheid en klantvriendelijkheid op de tocht te zetten.

Bij gemeenten zijn er relatief veel medewerkers die hun werk al lang doen, soms zelfs tientallen jaren. Zij hebben hart voor hun werk en voor de daarbij betrokken burgers, bedrijven en collega's. Tegelijkertijd zijn sommige medewerkers niet zo vaardig met computers. Ambtenaren zijn gevoelig voor hoe we met elkaar omgaan en voor het centraal stellen van de burger. Dit is onderdeel van de cultuur in de gemeente. Wat voor cultuur er ook is in jouw gemeente, je dient er rekening mee te houden als je gaat praten over informatiebeveiligings- en privacyrisico's.

5. Motiveer – extrinsiek en intrinsiek

Kennis alleen is onvoldoende om gedrag te veranderen.

Praktijkvoorbeeld

Herken je deze situatie? Je houdt een enquête over informatie-beveiliging en je krijgt allemaal positieve antwoorden, zoals 'ik geef nooit mijn wachtwoord aan een collega'. Terwijl dit niet is wat je om je heen ziet gebeuren. Je hebt sociaal wenselijke antwoorden gekregen. Het positieve daarvan is dat mensen blijkbaar heel goed weten 'hoe het hoort'.

Met de kennis zit het wel goed. Maar ze dóen het niet! Dat kan verschillende redenen hebben. Intrinsieke motivatie is als mensen dingen doen, prestaties leveren, omdat ze dat zelf willen. Het gaat om hun eigen drijfveren. Ze beleven er plezier aan, ze vinden het interessant of het helpt hen hun doelen te bereiken. Bij extrinsieke motivatie vertonen mensen gedrag op basis van externe invloeden. Straffen en belonen zijn middelen om via extrinsieke motivatie gedrag te beïnvloeden (zie ook hoofdstuk 12). Dit kun je zeker gebruiken bij het bevorderen van veilig gedrag. Proberen om mensen intrinsiek gemotiveerd te krijgen voor informatiebeveiliging is namelijk best lastig.

Er is ook nog een andere vorm van motivatie: geïnternaliseerde motivatie. Daar spreken we van als mensen dingen doen omdat ze het belangrijk vinden, ergens het nut van inzien, en het past bij de eigen waarden. Als je glas in de glasbak gooit, doe je dat omdat je er het nut

van inziet, niet zozeer omdat je intrinsiek gemotiveerd bent. Je kunt op geïnternaliseerde motivatie aansturen in verband met informatie-beveiliging en privacybescherming. Bijna iedereen vindt privacy belangrijk, ook mensen die in eerste instantie zeggen dat ze niets te verbergen hebben. Als je met hen in gesprek gaat, blijkt dat ze wel degelijk het belang ervan inzien. Het vergroten van de geïnternaliseerde motivatie is een doel van je bewustwordingsprogramma.

6. Beloon

Bestaande gewoontes zijn in de loop van de tijd ontwikkeld. Als je deze wilt veranderen, bied dan alternatieven aan die de medewerkers hetzelfde, of meer, opleveren. Je kunt ook medewerkers vragen te kiezen tussen verschillend gedrag en het veilige gedrag belonen. Soms is het zinvol om alleen al de inspanning te belonen. Dit gaat niet om het strooien met materiële zaken; een compliment, positieve aandacht in een werkoverleg of nieuwsbrief werkt ook. Zo creëer je een cultuur waarin het gebruikelijk is dat mensen vrijuit spreken, elkaar helpen, vragen stellen en antwoorden geven.

Het is het beste om niet te veel tegelijk te willen. Als je mensen overlaadt, dan creëert dat weerstand en afstand. In het taalgebruik kan het helpen om het te hebben over gewoontes, en niet over gedrag veranderen. Dat is minder bedreigend en wordt vaak eerder geaccepteerd.

7. Maak het makkelijk, toegankelijk en begrijpelijk

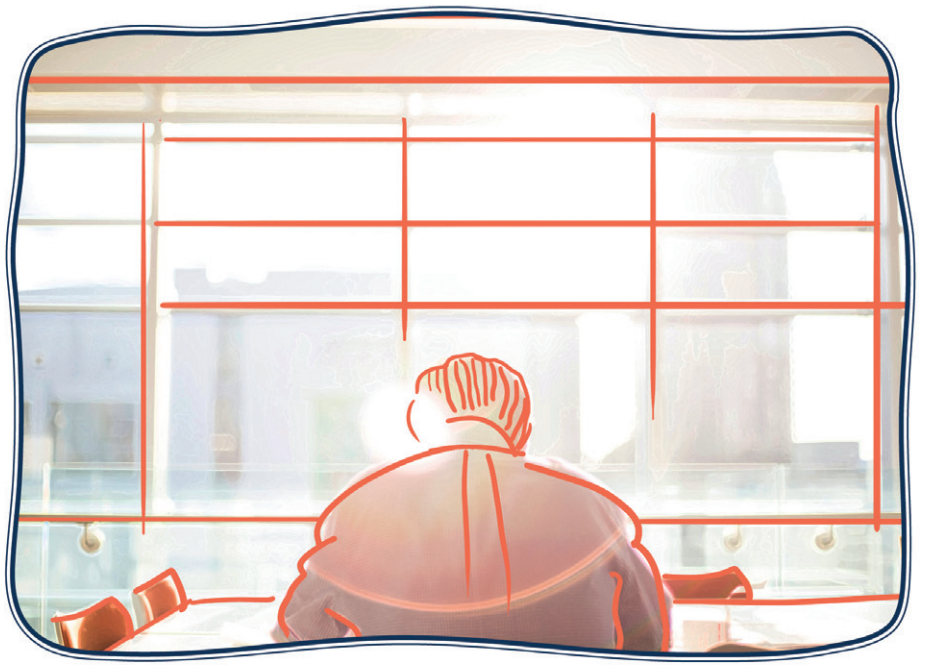
Veilig gedrag makkelijk maken helpt. Vaak wordt informatiebeveiliging geassocieerd met omslachtig en tijdrovend. Een dergelijk imago zorgt ervoor dat er weerstand ontstaat. Onderdeel van je bewustwordings-programma is dus niet alleen onderzoeken waarom mensen onveilige gewoontes hebben, maar ook hoe je een eenvoudig en veilig alternatief kunt bieden. Als het makkelijk te begrijpen en makkelijk uitvoerbaar is, dan is de acceptatie groter. Soms kun je de omgeving aanpassen om veilig gedrag te stimuleren. Enkele voorbeelden:

1. Implementeren van single-sign-on: eenmalig inloggen waardoor je maar één wachtwoord hoeft te onthouden. Bij gebruik hiervan kun je mensen er wel op attenderen dat dat ene wachtwoord dus belangrijker is. Als het bekend wordt, heeft een ander dus toegang tot álles.
2. Implementeren van follow-me-printen: het afdrukken start pas als je een printer activeert met een pasje of code. Hiermee voorkom je dat stukken per ongeluk op een verkeerde printer komen of blijven liggen omdat iemand vergeet de documenten op te halen.
3. Beschikbaar stellen van meer papiervernietigers. Als iemand ver moet lopen om zijn document door de vernietiger te halen, dan zal hij dat eerder uitstellen of vergeten.
4. Beschikbaar stellen van voldoende overlegruimtes om vertrouwelijke gesprekken te voeren.

8. Zorg voor zichtbaarheid

Zichtbaarheid, herhaling en opvallen – dat is nodig voor een effectief bewustwordingsprogramma. In de overvolle agenda en werkdag van veel mensen is het een strijd om aandacht. Als je niet terug blijft komen, zakt je boodschap weg in de dagelijkse drukte. Jouw rol is zorgen voor die zichtbaarheid. Je dient alle kansen die je tegenkomt om je verhaal te vertellen te grijpen, en steeds te zoeken naar aansluiting. Nodig jezelf uit bij overleggen, van managementteam tot werkgroep, en van werkoverleg tot informatiemarkt. Eén keer een presentatie (laten) geven is geen kunst; terugkomen met een verhaal dat resoneert met ambtenaren is dat wel.

Dit boek helpt je om stap voor stap tot dat verhaal te komen en om het uit te dragen, zodat bewustere medewerkers bijdragen aan informatiebeveiliging en privacybescherming.



9. Gebruik de juiste taal

Je bewustwordingsprogramma heeft pas effect als je de mensen echt weet te bereiken. Zoals al eerder besproken staan de onderwerpen informatiebeveiliging en privacy in de beleving van veel ambtenaren wat verder bij ze vandaan. Als je echt in gesprek gaat, zijn veel medewerkers wel betrokken bij het onderwerp, vooral als je ze aanspreekt op een manier die ze appreciëren. In de taal van de gemeente met de voorbeelden uit de gemeentewereld. Mensen werkzaam in de publieke sector worden in het algemeen minder geraakt door commerciële, financiële of wettelijke argumenten en voorbeelden.

10. Oorzaken van gedrag achterhalen

Vragen en luisteren is een goede manier om de beweegredenen van mensen te achterhalen als zij onveilige gewoontes hebben. Schijnbaar irrationeel gedrag heeft vaak een goede reden.

Er zijn wel een paar categorieën van redenen te benoemen.

1. Het kan liggen aan de motivatie: ‘Weer iets erbij wat moet; laat me lekker mijn werk doen, het waait wel over.’
2. Beïnvloeding door groepsdruk, niet willen afwijken van het gebruikelijke gedrag onder collega’s. Voorbeeldgedrag van management, maar ook van ambassadeurs en collega’s is echt van belang.
3. Wordt veilig gedrag wel beloond? Dat hoeft niet direct een financiële bonus te zijn, waardering van burgers, collega’s of de organisatie werkt ook.
4. Hoeveel moeite kost het om het veilige gedrag te vertonen? Vaak vinden mensen het gewoon een hoop gedoe. Van informatiebeveiliging ervaren ze niet direct positieve effecten op hun werk. Daarom zijn ze beperkt bereid om er tijd en moeite in te investeren. Ze hebben het gevoel dat ze minder van hun eigenlijke werk gedaan krijgen. De afweging wat belangrijker is, de dienstverlening (het primaire proces) of het voldoen aan beveiligingseisen, zal naar de dienstverlening neigen. Daarom dienen mensen die beveiligingsmaatregelen bedenken, zoals de CISO, zich goed bewust te zijn van het effect van hun maatregelen op de manier waarop medewerkers hun primaire taken kunnen vervullen. Ook dient het besef te groeien dat informatieveiligheid en privacybescherming onderdeel zijn van een goede dienstverlening. Het is niet iets wat daarnaast ook nog even moet gebeuren omdat het nu eenmaal in de wet staat. Neem nu zoiets als identiteitsfraude, een (soms jarenlange) nachtmerrie voor de slachtoffers ervan. Voor identiteitsfraude zijn

persoonsgegevens nodig, gegevens waarover gemeenten de beschikking hebben. Goede dienstverlening aan burgers betekent ook dat gemeenten alles doen om te voorkomen dat die gegevens in verkeerde handen vallen.

5. Het ontbreken van kennis en vaardigheden. Weten medewerkers eigenlijk wel wat veilig of onveilig gedrag is? En daarbij: kunnen ze het veilige gedrag ook uitvoeren? Je kunt wel weten dat je bestanden moet versleutelen, maar ja, hoe doe je dat dan? Hoe mail je veilig?

Het spreekt voor zich dat de manier waarop je gaat werken aan de overgang van onveilige naar veilige gewoontes afhankelijk is van de oorzaken van onveilig gedrag. Soms moet je werken aan de motivatie, soms help je mensen om nieuwe vaardigheden te verwerven, soms kan het helpen om veilig gedrag simpeler te maken. Dat laatste is overigens altijd een goed idee. Veilig gedrag dient makkelijk en vanzelfsprekend te zijn.

11. Betrek collega's bij het bepalen van de toon

Collega's betrekken bij het ontwikkelen van teksten en materialen kan helpen om te bepalen of je de juiste toon te pakken hebt. Zorg dat je veelvuldig contact hebt met mensen waarvan je het gedrag wilt beïnvloeden. Let op hun taalgebruik, welke voorbeelden geven ze, waar lopen ze tegenaan? Hoe meer je aansluit bij de belevingswereld, hoe beter de oplossingen die je kunt bedenken en hoe effectiever de communicatie daarover.

Als je in je bewustwordingsprogramma gebruik wilt maken van bestaande communicatiematerialen, mogelijk van andere leveranciers, let hier dan goed op. De effectiviteit van je programma gaat met sprongen omhoog als je bij selectie en gebruik zorgt voor wat past bij jouw gemeente. Zelfs voorbeelden uit een andere overheidslaag maken dat het bij de medewerkers al moeilijker binnenkomt. We adviseren je om de details aan te passen en alles in een proeftuin te testen bij je collega's.

12. Fouten mogen maken

Goed werk leveren doet iedereen graag. Maar hoe je omgaat met fouten is een belangrijk onderdeel van je cultuur. Worden fouten afgestraft of positief begroet als kans om te leren? Als je zicht wilt krijgen op wat er in alle hoeken van de organisatie gebeurt, dan is het nodig dat mensen weten dat ze fouten mogen maken. Dat ze fouten en onveilige situaties melden is een voorwaarde om als organisatie te kunnen verbeteren. Je kunt dit niet vaak genoeg benadrukken in je bewustwordingsprogramma.

6.3. Veiligheids- en organisatiecultuur

Het creëren van een veiligheidscultuur is je uiteindelijke doel.

Een cultuur is volgens het Van Dale-woordenboek het geheel van geestelijke verworvenheden van een land, volk. Onder meer dus de gewoontes en gebruiken van een groep mensen. Veiligheid is: vrij van gevaar, van bedreigingen zijn. Als je dit samenvoegt kom je erop uit dat een veiligheidscultuur is: de gewoontes en gebruiken van een groep die hen helpen vrij te zijn van gevaar en bedreigingen.

Hoe je op dit gebied omgaat met bedreigingen en met elkaar, is onderdeel van de veiligheidscultuur; samen eraan werken om veilig te zijn. Het gedrag van ieder lid van de groep heeft invloed op de rest.

Elementen die de veiligheidscultuur van een organisatie kenmerken zijn bijvoorbeeld:

- De houding en het gedrag van het bestuur, management en van de medewerkers.
- De prioriteit die het krijgt tussen alle andere zaken die belangrijk zijn.
- Hoe men ermee omgaat als er iets is misgegaan.
- Hoe de gemeente zelf de status op het gebied van veiligheid meet.
- Of er ruimte is voor opleidingen op dit gebied.
- Hoe de aanspreekcultuur is.

Voor meer achtergronden over veiligheidscultuur verwijzen we graag naar het werk van Kai Roer van CLT.re.[13] Hij voert al jarenlang het gesprek over informatieveiligheidscultuur.

Elke gemeente zijn eigen cultuur

Gemeenten hebben allemaal hun eigen cultuur, hun eigen kenmerken. Binnen een gemeente gelden normen en waarden die in stand blijven, ook bij wisseling van personeel. Over het algemeen is er continuïteit doordat de cultuur wordt overgedragen op nieuwkomers.

Een organisatiecultuur kan zich kenmerken door bijvoorbeeld:

- interne of externe focus
- een hiërarchische of platte organisatie
- centrale aansturing of meer zeggenschap op lagere niveaus
- besluitvaardigheid of niet
- open of gesloten
- risico's durven nemen of niet
- bureaucratisch of meer ad hoc
- formeel of informeel
- innovatief of behoudend
- hoe er wordt gereageerd op veranderende omstandigheden

Dit soort elementen maken een organisatie tot wat zij is. De organisatie is doordrenkt van de eigen waarden, iedere gemeente is daarbij anders. Het veranderen van een cultuur is niet eenvoudig, het is zelfs een heel vakgebied geworden: verandermanagement. Dit boek beperkt zich tot het onderdeel informatiebeveiliging en privacy. Mocht je interesse hebben in een breder perspectief op verandermanagement, dan raden we het werk van de hier vaker geciteerde Kotter aan.

Bewustzijn of cultuur?

Bewustzijn of cultuur, welk woord gebruiken we? Bewustzijn alleen is niet genoeg, daar zijn we het over eens. Iedereen weet dat die vette hap eten ongezond is en rijden met alcohol op onverstandig (en een misdrijf). Betekent dat, dat niemand het doet? Zeker niet! Ook op het gebied van informatiebewust gedrag zie je dit verschijnsel. Veel mensen weten wel dat ze hun wachtwoord niet mogen delen, en geen papieren moeten laten slingeren, maar toch gebeurt het. Kennis en bewustzijn alleen zorgt er dus niet voor dat de organisatie veiliger wordt.
Om gedrag te veranderen dienen mensen ook op emotioneel niveau geraakt te worden en ervan overtuigd te zijn dat het nodig is. Anderzijds moeten ze het alternatieve gedrag ook *kunnen* uitvoeren.

Bewustzijn is de eerste stap

Kortom, bewustzijn alleen is niet voldoende. Toch gebruiken we meestal deze term, omdat het nu eenmaal een ingeburgerde term is. En bewustzijn is wel de start, de eerste stap.
Ook Kotter noemt dit in zijn boek 'Het hart van de verandering' (The heart of change)[14] een heel belangrijk punt: bij verandering komt cultuur als laatste, niet als eerste. Hij zegt dat cultuur pas echt verandert als een nieuwe werkwijze over een periode heeft laten zien succesvol te zijn. Normen en waarden veranderen voordat je een nieuwe werkwijze hebt gecreëerd, werkt niet, volgens hem.

We beginnen dus met bewustzijn en gedrag, en daarna kunnen we het over cultuur gaan hebben.

Ook cultuur kun je meten

Als het meten van bewustzijn soms al op praktische bezwaren stuit, hoe zit het dan met het meten van de veiligheidscultuur? Ook dat is wel mogelijk als je concrete aspecten benoemt om te onderzoeken en te rapporteren. Het van oorsprong Noorse bedrijf CLTRe heeft in samenwerking met de Universiteit van Ljubljana een methode ontwikkeld voor het meten van de informatieveiligheidscultuur. Door een enquête uit te voeren onder alle medewerkers van een organisatie ontstaat een beeld op zeven dimensies van veiligheidscultuur:

- houding van de medewerker
- normen van de organisatie
- gedrag van de medewerker
- naleving van veiligheidsprocedures
- kwaliteit van communicatie
- kennisaspecten van veiligheid
- individuele verantwoordelijkheid

Uit onderzoek van CLTRe blijkt dat het werken aan de zeven dimensies risicovol gedrag significant verlaagt. Dit komt tot uitdrukking in de metingen. Een uitgebreid rapport kun je downloaden op hun website.[15]

6.4. Waar kan het misgaan zonder model?

Zonder model voor informatiebewustzijn wordt er geen of incidentele aandacht besteed aan bewustwording. Als er geen aandacht is, leidt dat tot onveilige gewoontes bij medewerkers, maar ook tot onvoldoende aandacht voor informatiebeveiliging en privacybescherming in het algemeen. Als degenen die de budgetten en jaarplannen vaststellen het onderwerp niet in gedachten hebben, zal er ook weinig tijd en geld zijn voor technische en procedurele maatregelen. Incidentele aandacht, zoals een enkele presentatie, af en toe een bericht op het intranet, of een poster aan de muur, leidt tot een klein beetje attentie voor een korte periode. Effectief verandert er niet veel.

Praktijkvoorbeeld

Bij een gemeente wordt er erg op cijfers gestuurd. Korte doorlooptijden van aanvragen zijn belangrijk. Er is incidentele aandacht voor informatie-beveiliging en privacy: iemand krijgt privacybescherming in zijn taken-pakket en hij mag naar een cursus. Vervolgens krijgt deze persoon van het management de volgende waarschuwing: 'Prima, maar val ons er niet mee lastig!'

Vragen aan de lezer

1. Wordt er bij jullie incidenteel, planmatig of helemaal geen aandacht besteed aan bewustwording op het gebied van informatiebeveiliging en privacy?
2. Bekijk eens of en op welke wijze de interne communicatie in jouw gemeente specifiek is voor de doelgroep. Niet alleen over informatiebeveiliging of privacy, maar ook over andere onderwerpen.
3. Welke beelden en woorden passen goed, welke beelden en woorden kun je beter vermijden? Bedenk dit niet alleen zelf achter je bureau, maar check bij collega's van andere afdelingen, met name die collega's die werkzaam zijn in het primaire proces van dienstverlening.
4. Hoe omschrijf je de cultuur in jouw organisatie op de volgende aspecten:
    - Wat zijn houding en gedrag van het bestuur, management en van de medewerkers?
    - Welke prioriteit krijgen informatiebeveiliging en privacy tussen alle andere zaken die belangrijk zijn?
    - Hoe gaat men ermee om als er iets is misgegaan?
    - Hoe meet de organisatie zelf de status op het gebied van informatieveiligheid?
    - Is er ruimte voor opleidingen op dit gebied?
    - Hoe typeer je de volgende kenmerken: aanspreekcultuur, interne of externe focus, een hiërarchische of platte organisatie, centrale aansturing of meer zeggenschap op lagere niveaus, besluitvaardigheid of niet, open of gesloten, risico's durven nemen of niet, bureaucratisch of meer ad hoc, formeel of informeel, innovatief of behoudend?
    - Hoe wordt er gereageerd op veranderende omstandigheden?
5. Wat betekent dit voor de opzet van je bewustwordingsprogramma?

Nawoord

Security fatigue is de term die we gebruiken voor mensen die moe zijn van alles wat met beveiliging te maken heeft, die het te ingewikkeld vinden en geen keuzes meer kunnen maken. Dat heeft ook te maken met de privacy-paradox: mensen vinden privacy wel belangrijk, maar hebben het gevoel er geen grip op te hebben.

Je wilt voorkomen dat jouw collega's terechtkomen in een staat van *security fatigue*. Dat wil niet zeggen dat je ze met rust moet laten, maar meer dat je het makkelijk kunt maken. Als zij het moeilijk vinden om te kiezen voor veilige gewoontes, waarom kies jij dan niet?

Uit onderzoek volgen drie dingen die helpen om *security fatigue* te verminderen:

1. Verminder het aantal keuzes dat mensen moeten maken.
2. Maak het kiezen van de veilige optie eenvoudig.
3. Zorg er bij het ontwerp van systemen voor dat, overal waar mogelijk, consistente, veilige keuzes gemaakt kunnen worden.

Voor een bewustwordingsprogramma is het dus relevant om in gesprek te blijven met de medewerkers om tekenen van *security fatigue* te signaleren, deze te onderzoeken en het programma en andere maatregelen waar nodig aan te passen.

Afstand tussen de CISO en medewerkers

Dikke kans dat degene die verantwoordelijk is voor het bewustwordings-programma een security-professional is (waarschijnlijk de CISO).

Afhankelijk van de omvang van de gemeente kan de afstand tot de medewerkers groot zijn. Gevolg is dat je dingen bedenkt die niet aanslaan, of zelfs worden ervaren als 'weer iets dat wordt opgelegd, we willen gewoon ons werk doen!'

Om een beter bewustwordingsprogramma te kunnen maken, is het belangrijk te weten wat voor werk je collega's doen en onder welke omstandigheden. We raden je met klem aan om regelmatig in gesprek te gaan en ook echt rond te lopen op de verschillende afdelingen. Zodat je gevoel krijgt voor welke zaken daar spelen, voor welke dilemma's de medewerker zich geplaatst ziet. Pas als je dat begrijpt, kun je passende veilige maatregelen bedenken en adviseren. En doe dit vooral samen met de medewerkers. Zij zien echt wel waar zaken beter kunnen. Als je samen nadenkt over oplossingen, heb je grotere kans op een gedragen voorstel dat ook echt past bij de organisatie.
Nogmaals: onderschat dit niet, het is een van de pijlers onder je succes. Of niet.

In control zijn

Veel gemeenten zijn niet *in control* op het gebied van informatie-veiligheid. Bestuur en management kennen de betrouwbaarheid van de informatievoorziening niet. Hebben de risico's niet in beeld, weten niet of ze onacceptabele risico's lopen, weten niet of getroffen maatregelen effectief zijn en of ze voldoen aan wet- en regelgeving en eigen beleid. Met de grotere afhankelijkheid van (digitale) informatie, die zich meer en meer buiten de gecontroleerde omgeving bevindt, die geïmporteerd en geëxporteerd wordt, met de grotere kwetsbaarheid van alle verbonden apparatuur, is het moeilijker om in control te zijn dan een paar jaar geleden. Bewuste medewerkers signaleren risico's en voorkomen incidenten. Natuurlijk, daarmee ben je er nog niet, maar het levert wel

een bijdrage aan een betere risicobeheersing. Dit boek is bedoeld om je daarbij te helpen.

Samenwerken of zelf het wiel uitvinden

Wat er bij verschillende gemeenten speelt op het gebied van privacy, is vaak in grote lijnen hetzelfde. Waarom zouden we dan allemaal alleen voor onszelf bezig zijn? Gelukkig zijn er al wel regionale samenwerkingsverbanden of hulpmiddelen vanuit de VNG. Als je hier nog geen deel van uitmaakt, kijk dan eens of er in de buurt gemeenten zijn waarmee je kunt samenwerken.

Natuurlijk zijn er verschillen, bijvoorbeeld in de steun die er is vanuit bestuur en management. De een moet daar veel harder aan werken dan de ander. Maar het ontwikkelen van plannen en materialen, het uitzoeken van hulpmiddelen en het organiseren van trainingen kun je prima samen doen. Iedereen legt daarbij wel de accenten die bij de eigen organisatie passen. Je kunt van elkaar leren wat werkt en wat niet, en je bespaart tijd.

Doe nooit neerbuigend over mensen die fouten maken

'*Ze snappen er echt helemaal niks van*', '*Je moet alles tachtig keer uitleggen*' (zucht) en '*Dat is toch een stelletje ongeleide projectielen!*' Soms kom je in de verleiding om zo over collega's te praten die wel eens iets onhandigs doen op het gebied van informatiebeveiliging en privacy. Is dat wel slim? Ook al zeg je dit niet letterlijk tegen de mensen over wie je het hebt, het gevoel kan doorklinken in alles wat je doet, zegt en communiceert. Al is het niet altijd makkelijk, met begrip en een open houding bereik je waarschijnlijk meer.

Hoe komt het dat mensen die dingen doen? De meeste collega's zijn hardwerkende professionals die gewoon hun werk willen doen. Zij hebben expertise op hun onderdeel, jij op het jouwe. In gesprek gaan is effectiever en mensen voelen het als je ze waardeert om hun kennis en kunde. Bijna iedereen wil graag goed werk leveren, en als jij ze kan helpen om dat nog een beetje beter te doen, dan staan ze daarvoor open. Het stimuleren van een cultuur waarin fouten maken mag, dat werkt. Het is natuurlijk wel de bedoeling er iets van te leren met zijn allen. Probeer dat uit te dragen en ga zelf ook positief om met adviezen die jij van anderen krijgt.

Aan zo'n proces komt geen einde

Zoals het PrivacyLab-model een cirkel is, zo heeft ook bewustwording geen einde. Een project of een programma misschien wel, maar als je het onderwerp niet actief op de agenda houdt, treedt er terugval op. Hoeveel je wilt blijven doen, hangt af van de volwassenheid van de gemeente. Bij een heel volwassen gemeente met een echte veiligheidscultuur is het onderwerp ingebed in de dagelijkse gang van zaken. Mensen spreken elkaar aan. Incidenten en risico's worden gemeld en behandeld. Maar de wereld verandert en dat blijft vragen om aandacht. Er komen nieuwe systemen en processen in de organisatie en er ontstaan nieuwe risico's waarover je mensen wilt informeren. En natuurlijk komen er ook nieuwe mensen de gemeente binnen, die je mee wilt nemen in de manier van werken. Nieuwe mogelijkheden voor activiteiten en communicatie. Dat bij elkaar maakt het leuk om steeds weer verder te gaan. Er komt geen eind aan... gelukkig niet!

Aan de slag!

Dit is het laatste hoofdstuk van dit boek. Misschien heb je het van A tot Z gelezen, misschien heb je gebladerd en hier en daar een stuk gelezen. We hopen dat het je inspireert om aan de slag te gaan,

dat je de bagage hebt gevonden om beslissers van de noodzaak ervan te overtuigen, en dat je nu voldoende handvatten hebt om te weten waar je kunt beginnen.
Voor ons was het zeker inspirerend om dit deel van onze kennis op een rijtje te zetten en op te schrijven. Tijdens het schrijven kregen we echt weer meer zin om met gemeenten verder te werken op het mooie terrein van informatiebeveiliging en privacybescherming.

Als het veel lijkt, begin dan gewoon klein. Iedere stap is er één en een bewustwordingsproces is vooral iets van de lange adem. Mocht je ideeën hebben die je even wilt toetsen, of als je verder nog hulp nodig hebt, neem gerust contact met ons op. We vinden het altijd leuk om mee te denken.

Reacties op de inhoud van het boek zijn ook van harte welkom, net als verhalen over wat je in jouw organisatie hebt opgezet, met of zonder hulp van dit boek. We hopen van je horen. En voor nu: aan de slag!

Gemeenten. Bewustzijn. Privacy.
Het handboek voor informatiebewustzijn bij de lokale overheid
Eerste druk 2019

Uitgever: PrivacyLab

ISBN: 978-90-828604-4-3
NUR-code: 982
NUR-omschrijving: Informatica & management

Trefwoorden: informatiebeveiliging gemeenten, privacybewustzijn, PrivacyLab-model

Illustraties, vormgeving en ontwerp omslag: De Merkbrouwerij, Yoeri Laros, www.demerkbrouwerij.nl
Redactie: Joke van Kampen
Foto Martine: Nooij Photography, Janneke Nooij
Drukwerk: www.pumbo.nl

www.privacylabnederland.nl | www.ibnpbv.nl