INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

Verhogen bewustzijn informatiebeveiliging

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking verhogen bewustzijn informatiebeveiliging

Versienummer

1.01

Versiedatum

Mei 2021

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
1.0	November 2019	Definitieve versie
1.02	Mei 2021	Toevoeging beschikbaarheid toolkit

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy- / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

INFORMATIE
BEVEILIGINGS
DIENST

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is gemeenten een handreiking te bieden voor een structurele aanpak van het verhogen van het beveiligingsbewustzijn binnen de organisatie.

Doelgroep

Dit document is van belang voor de CISO, de Functionaris Gegevensbescherming, het management van de gemeente, de afdeling HRM/Personeelszaken, de communicatieadviseur en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligings- en privacybeleid van de gemeente
- Criteria borging AVG

Verwijzingen naar de Baseline Informatiebeveiliging voor de Overheid (BIO)

7.2.2 Alle medewerkers van de organisatie en - voor zover relevant - contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover dat relevant is voor hun functie.

Verwijzingen naar Criteria borging AVG, onder ‘Organisatorische inbedding’:

1.2 Er zijn voldoende middelen beschikbaar om privacybescherming te bevorderen in kennis, houding en gedrag van alle medewerkers in de organisatie.

Inhoudsopgave

1. Inleiding

Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatievoorziening. Ongewenste, onbewuste acties blijken een groter risico voor de privacy van burgers en de veiligheid van informatie dan bewuste en gerichte aanvallen[1]. Investeren in het verhogen van het besef bij medewerkers dat informatiebeveiliging belangrijk is, is dus een effectieve maatregel om dreigingen het hoofd te bieden. Organisatorische en technische maatregelen om informatie te beveiligen werken alleen als bestuur, management en medewerkers de noodzakelijke houding en gedrag vertonen. Hoe krijg je dit gewenste gedrag tussen de oren van mensen? Deze handreiking biedt gemeenten passende hulp door middel van een gestructureerde aanpak. Gedrag heeft te maken met iets ongrijpbaars als de 'organisatiecultuur'. Een gestructureerde aanpak maakt het ongrijpbare toch hanteerbaar. Maar het vereist wel een voortdurend proces, dat zijn basis vindt in een duidelijke strategie en een verdere uitwerking in een concreet stappenplan.

1.1. Waarom het verhogen van beveiligingsbewustzijn lastig is

Veel gemeenten hebben al de nodige maatregelen genomen om het bewustzijn binnen hun organisatie te verhogen, maar toch worden de meeste beveiligingsincidenten nog steeds veroorzaakt door menselijk handelen[2]. Hoe komt het dat het verhogen van beveiligingsbewustzijn zo lastig is?

De belangrijkste faalfactoren zijn:

- Het ontbreken van een integrale aanpak met een plan hoe het bewustzijn te verhogen. Inspanningen zijn vaak ad hoc gericht op incidenten en niet ingebed in een voortdurend proces.
- Men doet iets aan bewustwording alleen om te voldoen aan regelgeving, zonder na te denken over het uiteindelijke doel van de campagne.
- Bewustwordingscampagnes zijn te algemeen gericht op de organisatie en sluiten onvoldoende aan op de werkzaamheden van individuele medewerkers.
- De voortgang noch de waarde van activiteiten in het kader van verhogen van het bewustzijn voor de organisatie wordt gemeten, dus het effect van de inspanningen is onbekend. Er wordt ook niet bijgehouden wie wel en niet een training gevolgd hebben.
- Onrealistische verwachtingen over menselijk gedrag. Het hanteren van regels omtrent veilig gedrag betekent niet dat ze dan ook vanzelfsprekend worden nageleefd door medewerkers.
- Onrealistische verwachtingen over het effect van maatregelen om het bewustzijn te verhogen. Een jaarlijkse bijeenkomst over het belang van informatiebeveiliging heeft geen zin als daar in de praktijk niet de noodzakelijke organisatorische en technische maatregelen aan worden verbonden.
- De gebruikte instrumenten sluiten niet aan op de boodschap die men wil overbrengen of het tijdstip waarop de boodschap wordt gebracht. Bijvoorbeeld: je kunt een nieuwe medewerker op zijn eerste werkdag overspoelen met informatie over veilig gedrag, maar zijn focus zal op dat moment meer gericht zijn op vertrouwd raken met de nieuwe werkomgeving dan op informatiebeveiliging.

---

[1] Zie 'Dreigingsbeeld Nederlandse Gemeenten 2018'

[2] Het jaarrapport 2018 van de Autoriteit Persoonsgegevens geeft bijvoorbeeld aan dat 63% van de bij haar gemelde datalekken zijn veroorzaakt door het versturen van persoonsgegevens aan de verkeerde ontvanger.

- Herhaling van steeds dezelfde boodschap met hetzelfde instrument (bijvoorbeeld een plenaire bijeenkomst zonder interactie), waardoor de aandacht voor het belang van informatiebeveiliging verslapt.
- Bewustzijn van informatiebeveiliging wordt gezien als achtergrondruis, als iets wat vanzelfsprekend aanwezig is.

1.2. Waarom is beveiligingsbewustzijn belangrijk?

De toegenomen afhankelijkheid van internet in het maatschappelijke en zakelijke verkeer, de voortschrijdende digitalisering van de dienstverlening, het toegenomen gebruik van sociale netwerken en de opslag van informatie in de cloud creëren nieuwe beveiligingsrisico's voor de integriteit en vertrouwelijkheid van persoonsgegevens. De mens is een belangrijke schakel in het grotere geheel van informatiebeveiliging. De mate waarin medewerkers zich bewust zijn van de dreigingen die aan het cyberlandschap verbonden zijn en veilig gedrag vertonen, bepaalt de sterkte en zwakte van deze schakel. De meeste inbreuken op de vertrouwelijkheid en integriteit worden veroorzaakt door onbewust verkeerd handelen. Om het risico op dit onbewust en ongewenst verkeerd handelen te bestrijden, moet er binnen organisaties een goede veiligheidscultuur worden gecreëerd; een cultuur waar medewerkers risico's en bedreigingen meewegen als onderdeel van hun dagelijkse routine. Om een goede veiligheidscultuur binnen uw organisatie op te bouwen, is een structurele cultuurverandering nodig. Dit is niet gemakkelijk te realiseren, het is een langdurig proces waarvoor een integrale aanpak en veel deskundige inzet nodig zijn.

Een goede veiligheidscultuur is eveneens vereist voor een zorgvuldige omgang met persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG). Bij gemeenten komen veel gevoelige persoonsgegevens bijeen. Gemeenten hebben daarom een belang bij het beschermen van de privacy van hun inwoners. Informatiebeveiliging en privacy zijn onlosmakelijk met elkaar verbonden. Bovendien bevat de AVG vereisten die niet (rechtstreeks) terugkomen in de BIO, zoals grondslagen en bewaartermijnen. Daarom verdient privacy, zoals ingekaderd in de AVG en in meer specifieke wetgeving zoals de Wet basisregistratie personen (Wet BRP), aparte aandacht bij het verhogen van het beveiligingsbewustzijn.

1.3. Aanpak verhogen beveiligingsbewustzijn

Bij gemeenten is er behoefte aan duidelijke richtlijnen met betrekking tot een goede aanpak om het beveiligingsbewustzijn te verhogen. Gemeenten geven ook aan dat relevante tooling centraal geselecteerd op basis van de juiste kritische succesfactoren en beschikbaar gesteld door de IBD zeer welkom zou zijn. De IBD ontwikkelt hiervoor een module ‘Awareness’ als onderdeel van het project dat gericht is op het vergroten van de digitale weerbaarheid[3]. In dit document wordt een aanpak[4] gepresenteerd om structureel aandacht te geven aan het verhogen van beveiligingsbewustzijn. Deze aanpak kent de volgende fasen:

1) de ontwerpfase, waarin het te bereiken doel wordt bepaald en een strategie wordt ontwikkeld hoe de doelstelling wordt gerealiseerd;
2) de ontwikkelingsfase, waarin een plan wordt opgesteld om het bewustwordingsprogramma vorm te geven;
3) de implementatiefase, waarin uitvoering wordt gegeven aan het opgestelde plan;
4) de evaluatie- en onderhoudsfase, waarin het effect van het bewustwordingsprogramma wordt beoordeeld. Deze fase maakt van het gehele proces van de ontwikkeling van een bewustwordingsprogramma een cyclisch en zich herhalend proces.

[3] Zie voor meer informatie de website van de IBD: https://www.informatiebeveiligingsdienst.nl/project/digitaleweerbaarheid/

[4] Deze aanpak is gebaseerd op NIST Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" en de "Handreiking Security Awareness" van het Nationaal Adviescentrum Vitale Infrastructuur, 2008

1.4. Toolkit Behaviour by design

Bij deze handreiking is een toolkit “Behaviour by design” beschikbaar. Deze toolkit helpt gemeenten bij de ontwikkeling en uitvoering van een structureel bewustwordingsprogramma rond informatiebeveiliging. Er is bewust voor gekozen om de instrumenten niet van een IBD-ontwerp te voorzien, zodat iedere gemeente de eigen huisstijl kan toepassen op de documenten.

1.5. Verdere opbouw van dit document

In het volgende hoofdstuk wordt ingegaan op de invloed van de organisatiecultuur op het beveiligingsbewustzijn van medewerkers. Vervolgens wordt ingegaan op een integrale aanpak van het verhogen van het beveiligingsbewustzijn aan de hand van de hierboven beschreven fasering. Ten slotte wordt de integrale aanpak vertaald naar uitvoering in de praktijk aan de hand van een aantal persona, die invulling geven aan de verschillende leerbehoeften binnen een organisatie.

2. Organisatiecultuur

2.1. Inleiding

Om het beveiligingsbewustzijn van medewerkers te verhogen is inzicht nodig in de organisatiecultuur: dat zijn de collectieve patronen die kenmerkend zijn voor de organisatie en waar medewerkers zich aan conformeren om onderdeel te worden of te blijven van de organisatie. De effectiviteit van regels en procedures is mede afhankelijk van de mate waarin zij in de organisatiecultuur worden verankerd.

Cultuur is een ongrijpbaar begrip. Cultuur bestaat uit de groepsnormen, rituelen en het gewoontegedrag die elke organisatie kenmerken. Het vertaalt zich naar bijvoorbeeld de gewenste kennis, houding en gedrag van alle medewerkers om bewust met privacy en informatiebeveiliging om te gaan, zodat de organisatorische en technische maatregelen die in dit kader getroffen worden het gewenste effect hebben.

Organisatiecultuur wordt voor een belangrijk deel bepaald door de boodschappen die de mensen denken te ontvangen over wat écht wordt gewaardeerd binnen de organisatie. Die boodschappen hebben in ieder geval vier bronnen:

- het voorbeeldgedrag van de leiding;
- de beslissingen die worden genomen over tijd, geld of andere schaarse middelen;
- de regels en procedures in de organisatie;
- het verhaal dat wordt verteld over wat belangrijk wordt gevonden.

In het kader van integriteitsbevordering binnen de overheid heeft het bureau BIOS[5] een integrale aanpak ontwikkeld om te komen tot een integriteitsbevorderende cultuur. Dit model benoemt de aspecten die een rol spelen bij het ontstaan van een goede veiligheidscultuur. Hieronder is dit model weergegeven.

Het model geeft inzicht in welke aandachtsgebieden bij het bevorderen van een veiligheidscultuur een rol spelen. Het is geen blauwdruk voor een stappenplan, maar het toont aan dat er sprake is van een integrale samenhang van deze aandachtsgebieden. Verhogen van het beveiligingsbewustzijn vereist een samenhangende aanpak op al deze gebieden.

[5] Naar een integriteitsbevorderende cultuur. Een integrale aanpak. Bureau Integriteitsbevordering Openbare Sector, december 2015

Commitment en visie

Het ontstaan van een veiligheidscultuur vereist dat het management informatieveiligheid een belangrijk onderwerp vindt en bereid is daarin te investeren en hiervoor voldoende budget en capaciteit vrijmaakt. Daarvoor is ook een heldere visie van belang, die antwoord geeft op vragen als: waarom willen we aandacht besteden aan informatieveiligheid, wat verstaan we eronder, wat is de strategische doelstelling en wat willen we bereiken? Door middel van informatiebeveiligingsbeleid wordt invulling gegeven aan dit aandachtsgebied. Het is van belang dat bestuur en management vanwege hun invloed op de organisatiecultuur zelf in houding en gedrag het belang van privacy en informatiebeveiliging uitdragen. Het hanteren van een duidelijke strategie helpt bij het uitdragen van de boodschap, die met behulp van de in dit document besproken aanpak moet zorgen voor de verankering van het gewenste bewustzijn in de organisatie.

Waarden en normen

Waarden en normen vormen het onderliggende gedachtegoed voor beveiligingsbewustzijn. Zij geven invulling aan de vraag wat binnen de organisatie als wenselijk of ongewenst gedrag wordt beschouwd. Een gedragscode maakt inzichtelijk waar de organisatie en de medewerkers voor staan en waar zij op aangesproken (kunnen) worden.

Regels en procedures

Maatregelen en afspraken worden vastgelegd in procesbeschrijvingen en formele afspraken en voorschriften, bijvoorbeeld het hanteren van het vierogen-principe of het toepassen van functiescheiding. Deze maken de ongeschreven waarden en normen concreet en maken duidelijk hoe medewerkers binnen de organisatie omgaan met informatie.

Personeelsbeleid

Aandacht voor beveiligingsbewustzijn en de betrouwbaarheid van medewerkers dient een onderdeel te zijn van het aannamebeleid (werving en selectie, screening en dergelijke). Informatiebeveiliging moet als onderwerp een rol spelen in diverse personeelsgesprekken (jaarplan, voortgangs- en beoordelingsgesprekken). Ook in het exitbeleid is informatiebeveiliging een aandachtspunt. Daarnaast zijn personele maatregelen in de vorm van introductiebijeenkomsten, werkoverleg en bewustwordingssessies aangewezen manieren om te werken aan het bevorderen van de veiligheidscultuur binnen de organisatie.

Incidenten en handhaving

Hoe binnen de organisatie wordt omgegaan met de melding en afhandeling van beveiligingsincidenten is van grote invloed op de veiligheidscultuur. De mogelijkheid om incidenten op een eenvoudige manier te melden en de adequate opvolging van deze incidenten geven het signaal af dat er aandacht is voor het aanpakken en leren van incidenten.

Monitoring en verantwoording

Monitoren van de inspanningen die gericht zijn op het verstevigen van de veiligheidscultuur en het beveiligingsbewustzijn van medewerkers is belangrijk om de doelmatigheid en uitvoering van maatregelen op dat gebied te kunnen beoordelen. Hiervoor is ondersteuning in de vorm van een leermanagementsysteem (LMS)[6] aan te bevelen, bij voorkeur een LMS dat aansluit op het bestaande personeelsmanagementsysteem.

Organiseren en borgen

De aandacht voor informatieveiligheid en voor de hiervoor genoemde elementen dient structureel binnen de organisatie te worden belegd. Daarbij is van belang wie het beleid coördineert (de CISO), welke actoren hierbij betrokken zijn en wat de rol van het management is. Activiteiten en actiehouders worden bij voorkeur vastgelegd in het Information Security Management System (ISMS) van de gemeente.

2.2. Invloed van dit model op beveiligingsbewustzijn

Een integrale aanpak van beveiligingsbewustzijn betekent dat elk instrument dat wordt ingezet voor het bevorderen van het beveiligingbewustzijn wordt verbonden aan de zeven hiervoor genoemde aandachtsgebieden. Het opstellen van een gedragscode bijvoorbeeld vereist:

- Commitment en visie van bestuur en management. De gedragscode moet antwoord geven op vragen als: waarom vinden we informatieveiligheid belangrijk en welke middelen stellen we beschikbaar om de informatieveiligheid te waarborgen?
- Gedeelde waarden en normen binnen de organisatie. De gedragscode moet duidelijk maken waar de organisatie en medewerkers voor staan en waarop ze aangesproken kunnen worden. Zo zullen er afspraken zijn om de privacy van burgers te waarborgen door vertrouwelijk met hun persoonsgegevens om te gaan.
- Regels en procedures. In de gedragscode wordt bijvoorbeeld vastgelegd hoe omgegaan wordt met vertrouwelijke documenten of toegangscodes en het melden van incidenten.
- Personeelsbeleid. In de gedragscode wordt bijvoorbeeld vastgelegd hoe de medewerker geacht wordt te handelen met door de gemeente beschikbaar gestelde mobiele apparaten.
- Incidenten en handhaving. Het melden van incidenten als virussen, malware en datalekken en de gevolgen van niet nakomen ervan zijn onderdeel van de formeel geldende afspraken binnen de organisatie. Hoe hiermee in de praktijk wordt omgegaan is van invloed op de organisatiecultuur.
- Monitoring en verantwoording. Een gedragscode moet voortdurend de spiegel zijn van de cultuur die binnen de organisatie in stand wordt gehouden. Regelmatig herijken van de gedragscode en het toetsen of deze nog voldoende aansluit op bestaande normen en waarden is belangrijk. Ook moet regelmatig gecontroleerd worden of elke medewerker in de organisatie kennis heeft genomen van de gedragscode. Bij voorkeur wordt hiervoor getekend. Niet alleen de eigen medewerkers, maar ook door de gemeente ingehuurde medewerkers moeten zich aan de gedragscode conformeren. Een voorbeeld van een gedragscode in relatie tot informatieveiligheid is opgenomen als bijlage bij deze handreiking.

[6] Een LMS is een softwarematige omgeving voor het administreren, beheren en faciliteren van opleidingsactiviteiten (bijvoorbeeld e-learningactiviteiten). Het LMS biedt niet alleen activiteiten aan, maar bewaakt ook de voortgang van de inspanningen op het gebied van leren binnen de organisatie.

3. Structurele aanpak verhogen beveiligingsbewustzijn

3.1. Inleiding

Een belangrijke reden waarom veel campagnes voor het verhogen van het beveiligingsbewustzijn niet het gewenste effect hebben, is dat er geen gestructureerde aanpak aan ten grondslag ligt. Veel campagnes zijn incidentgedreven en een duidelijke visie erachter ontbreekt. Vaak wordt het bevorderen van bewustzijn aan individuele personen overgelaten, terwijl een goede veiligheidscultuur het cement van de beveiligingsorganisatie dient te zijn. Het gaat iedereen aan en gaat verder dan een incidentele lunchbijeenkomst of het periodiek bespreekbaar maken van beveiligingsbewustzijn tijdens een beoordelings- of functioneringsgesprek. Het creëren en behouden van de gewenste veiligheidscultuur vraagt om een structurele aanpak, waarin het verhogen van het beveiligingsbewustzijn in een voortdurende cyclus aandacht krijgt en behoudt.

3.2. Meten is weten

Een gestructureerde aanpak van het verhogen van het beveiligingsbewustzijn begint met de vaststelling van hoe het in de huidige situatie met het bewustzijn van medewerkers is gesteld. Hoe stel je die bestaande situatie vast? Een manier is om een enquête uit te zetten onder medewerkers[7]. Dat kan veel inzicht opleveren, maar het vereist ook veel tijd voor het beantwoorden en verwerken van de vragen. Een andere manier om de bestaande situatie vast te stellen is wanneer hiervoor gebruikgemaakt wordt van een concrete actie, zoals het versturen van een phishingmail of de inzet van een mysteryguest. De resultaten van zo'n actie geven inzicht in de bestaande situatie binnen de organisatie en maken houding en gedrag van medewerkers bespreekbaar, bijvoorbeeld tijdens plenaire bijeenkomsten met de medewerkers. Als het bij een eenmalige actie blijft, is het effect ervan slechts tijdelijk. Dat geldt ook voor een enquête. Het regelmatig herhalen van dezelfde actie maakt veranderingen in het gedrag zichtbaar. Maar hoe maak je die veranderingen in het kader van beveiligingsbewustzijn concreet? Hieronder een paar voorbeelden van indicatoren die inzicht geven in de mate van bewustzijn van medewerkers en van de organisatie:

- het aantal datalekken dat wordt gemeld;
- het aantal beveiligingsincidenten in een bepaalde periode;
- het aantal keren dat geklikt wordt op een link in een (georganiseerde) phishingmail;
- het aantal keren dat een phishingmail als beveiligingsincident wordt gemeld;
- het aantal aan gebruik van mobiele apparatuur gerelateerde incidenten;
- het aantal verzoeken om wijziging van wachtwoorden;
- het aantal medewerkers dat geen geheimhoudingsverklaring heeft ondertekend;
- het aantal door malware geinfecteerde computers;
- het aantal apparaten (laptops, smartphones, USB-sticks) dat als verloren of gestolen is gemeld;
- het aantal computers waarvan bij een verlaten werkplek het scherm niet vergrendeld is;
- het aantal medewerkers dat aan het eind van de werkdag een 'clear desk' achterlaat.
- de resultaten van kwetsbaarheidscans die uit structurele netwerkmonitoring voortkomen.

[7] Zie voor een voorbeeldvragenlijst de Handreiking Communicatieplan Informatiebeveiliging BIO van de IBD

3.3. Hoe 'volwassen' is de aandacht voor beveiligingsbewustzijn in uw gemeente?

De aandacht die vanuit de organisatie wordt gegeven aan het verhogen van beveiligingsbewustzijn kan in grote lijnen worden onderscheiden in de niveaus ‘laag’, ‘midden’ en ‘hoog’.

Niveau ‘laag’

Er is binnen de gemeente geen strategisch beleid en dus ook geen structureel budget voor een bewustwordingsprogramma. Er is slechts incidenteel aandacht voor bewustwording en de drijfveer is vooral het voldoen aan regelgeving. De verantwoordelijkheid voor het bevorderen van beveiligingsbewustzijn is niet centraal belegd bij een daarvoor aangewezen medewerker. Door het ontbreken van een strategie en budget is er geen opvolging van activiteiten en ontbreekt de samenhang tussen de verschillende activiteiten. Registratie van incidenten speelt geen rol.

Niveau ‘midden’

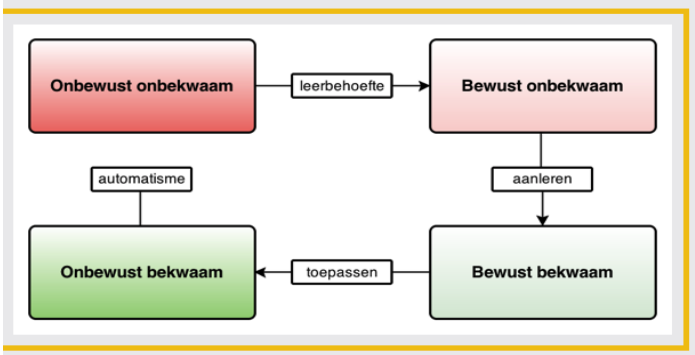
Er is binnen de organisatie besef aanwezig dat er beleid en budget moet zijn om aandacht te geven aan het verhogen van het beveiligingsbewustzijn. Hiervoor is een medewerker aangewezen en de aanpak is gebaseerd op een analyse van beveiligingsincidenten, die veroorzaakt worden doordat medewerkers niet beveiligingsbewust handelen. Maar voortdurende aandacht geven is lastig, omdat er geen structureel budget is. De relatie naar een verlaging van het aantal incidenten is onduidelijk en er is niet voldoende creativiteit om het beveiligingsbewustzijn door inzet van verschillende instrumenten vast te houden.

Niveau ‘hoog’

Er is structureel aandacht voor informatiebeveiliging in het strategisch beleid van de gemeente en er is jaarlijks budget voor de uitvoering van bewustwordingsprogramma's. De verantwoordelijkheid hiervoor is belegd bij een medewerker. Over de stand van zaken wordt periodiek gerapporteerd aan het management, dat zich ook bewust is van de eigen rol in relatie tot informatiebeveiliging. Er vindt incidentregistratie plaats en er worden analyses op de incidenten uitgevoerd. De organisatie is zich bewust van de risico's die het gevolg zijn van niet beveiligingsbewust handelen van medewerkers. In de bewustwordingsprogramma's wordt gebruikgemaakt van vernieuwende en creatieve middelen en ze zijn daardoor in staat de aandacht voor bewustwording vast te houden. Medewerkers begrijpen waarom maatregelen nodig zijn en passen deze onbewust toe bij hun werkzaamheden.

Deze handreiking richt zich op gemeenten die zich qua ‘volwassenheid’ op de niveaus ‘laag’ en ‘midden’ bevinden, en dus willen starten met een structurele aanpak van het beveiligingsbewustzijn. Deze aanpak is erop gericht om medewerkers onbewust bekwaam te maken, dat wil zeggen dat beveiligingsbewustzijn onbewust ertoe leidt dat beveiligingsmaatregelen automatisch worden toegepast.

Om dit niveau van bekwaamheid te bereiken doorlopen medewerkers een aantal fasen, zoals weergegeven in onderstaande figuur.



Figuur 1 Leerfasen van Maslow

Het doel van de structurele aanpak van het beveiligingsbewustzijn is om vanuit onbekendheid met na te leven regels en gewenst gedrag medewerkers zich ervan bewust te maken dat zij een leerbehoefte hebben om fouten te voorkomen. Kennis van regels en de juiste houding leidt tot aangeleerd gedrag. In de hoogste mate van bewustzijn is het veilig handelen van de medewerker onbewust onderdeel van zijn of haar dagelijks functioneren.

3.4. Samenhang tussen bewustzijn, training en opleiding

De aanpak van beveiligingsbewustzijn moet gebaseerd zijn op de beveiligingsorganisatie van de gemeente en aansluiten bij de belevingswereld van de medewerkers. Het programma moet zich niet alleen richten op de medewerkers op de werkvloer, maar ook op het bestuur en management van de gemeente. Van hen wordt voorbeeldgedrag verwacht. De effectiviteit van een bewustwordingsprogramma is in grote mate afhankelijk van de bereidheid en uitstraling van bestuur en management om zelf de veiligheidsregels na te leven.

Veiligheidsvoorschriften en procedures zijn vaak wel beschikbaar op het intranet of als handboek in de kast, maar de instructie over nut en noodzaak en het hanteren van deze voorschriften wordt vaak achterwege gelaten. Dan kan van een nieuwe medewerker niet worden verwacht dat deze prioriteit aan de naleving geeft. Een bewustwordings-, opleidings- en trainingsprogramma is essentieel in de verspreiding van noodzakelijke informatie die medewerkers en management nodig hebben om hun werk veilig te kunnen uitvoeren.

Doel van een bewustwordingsprogramma is om gedrag te veranderen en kennis van beveiligingsmaatregelen en procedures te vergroten. Een goed bewustwordingsprogramma richt zich op alle relevante psychologische componenten: kennis (door interne of externe opleidingen), houding (bewustzijn en competenties) en gedrag (door herhaalde oefening en training). Er moet te allen tijde aandacht aan al deze componenten worden besteed om tot een succesvol bewustwordingsprogramma te komen. Kennisoverdracht vereist het gebruik van meerdere technieken, waarbij onderstaande wijsheid vanuit het perspectief van de leerling aangeeft hoe de boodschap het best blijft hangen:

"Vertel het me en ik zal het vergeten"
"Laat het me zien en ik zal het onthouden"
"Laat het me doen en ik zal het begrijpen"

4. Ontwerpfase

4.1. Inleiding

In de ontwerpfase worden de te beveiligen belangen en behoeften vastgesteld, de hiervoor relevante onderwerpen en prioriteiten geïdentificeerd en vervolgens draagvlak, betrokkenheid en budget gezocht. In dit hoofdstuk gaan we achtereenvolgens in op:

- de strategie die gevolgd gaat worden in het bewustwordingsprogramma;
- de structuur van het bewustwordingsprogramma;
- het bepalen van de inhoud van het programma;
- het opstellen van een plan;
- het stellen van prioriteiten;
- de budgettering;
- commitment en draagvlak;
- rol van HRM en Communicatie.

4.2. Strategie

Het informatiebeveiligingsbeleid van de organisatie geeft invulling aan de door de organisatie beoogde veiligheidscultuur en het hierbij passende gewenste gedrag van medewerkers. De strategie kan gericht zijn op het creëren van een omgeving waarin de eigen verantwoordelijkheid van medewerkers voorop staat, of op het inrichten van een in hoge mate gestructureerde omgeving waarin normen en regels strikt worden gehandhaafd. De strategie bepaalt dus op welke wijze het raamwerk verder wordt ingericht.

Gemeenten zijn organisaties die regels uitvoeren. In het kader van het verhogen van het beveiligingsbewustzijn is dan ook de meest gangbare benadering om een set van regels en richtlijnen aan medewerkers over te brengen, met als doel dat medewerkers zich hieraan houden. De vraag is of dat werkt in een omgeving die voortdurend in beweging is en vraagt om zelfstandig denkvermogen om die ontwikkelingen bij houden. Te star vasthouden aan regels werkt ontwijkend gedrag in de hand, waarbij medewerkers op zoek gaan naar alternatieve ‘shortcuts’ om te omslachtige beveiligingsprocedures te omzeilen. En omdat regels in het algemeen volgend zijn op de praktijk, is het formeel handhaven van voorschriften lastig in overeenstemming te brengen met een dreigingsbeeld dat voortdurend verandert.

In de strategie om het bewustzijn te verhogen moeten de medewerkers en de dreigingen waartegen zij aanlopen in het dagelijks functioneren centraal worden gesteld. Het centraal stellen van de medewerker leidt ertoe dat er meerdere doelgroepen moeten worden onderscheiden, die vanuit hun specifieke werksituatie een andere benadering vereisen. Programma’s om het bewustzijn te verhogen worden vaak generiek ingericht, alsof iedereen binnen de organisatie geconfronteerd wordt met dezelfde beveiligingsrisico’s. Maar een baliemedewerker loopt tegen andere risico’s aan dan een medewerker van de afdeling financiën. Het hanteren van één en dezelfde aanpak om beveiligingsbewustzijn van alle medewerkers te verhogen heeft minder kans van slagen dan een aanpak, die is gebaseerd op de dagelijkse werksituatie van individuele medewerkers of teams. Bovendien leert niet iedereen op dezelfde manier, dus inzet van hetzelfde middel voor alle medewerkers zal niet voldoende effect hebben op het collectieve bewustzijnsniveau van de organisatie.

4.3. De structuur van het bewustwordingsprogramma

In de ontwerpfase moet worden gekozen of er centraal of vanuit de afzonderlijke domeinen van de gemeentelijke organisatie uitvoering wordt gegeven aan het programma. Wie krijgt de regie over het programma? De keuze die gemaakt wordt moet aansluiten bij de reguliere bedrijfsvoering van de organisatie. In veel gemeenten zijn lijnmanagers integraal verantwoordelijk voor de bedrijfsvoering. Aandacht voor beveiligingsbewustzijn is hier onlosmakelijk onderdeel van, maar de kans dat die aandacht structureel gegeven wordt is bij een decentrale opzet niet groot. Daarom is het aan te bevelen om de CISO een coördinerende rol te geven bij de uitvoering van het programma. De CISO moet vanuit deze rol erop toezien dat de lijnmanager afspraken in het kader van informatiebeveiliging naleeft, dus ook de afspraken die in het kader van verhogen van het beveiligingsbewustzijn worden gemaakt.

4.4. Risicoanalyse als basis

De basis voor een goed bewustwordingsprogramma is een risicoanalyse, waarin bepaald wordt tegen welke dreigingen de organisatie zich moet beschermen. Vanuit deze analyse wordt bepaald in hoeverre het beveiligingsbewustzijn van medewerkers van invloed is op het ontstaan van risico's en in welke mate een bewustwordingsprogramma kan bijdragen aan het mitigeren van deze risico's. Zie voor het uitvoeren van een diepgaande risicoanalyse de handreiking van de IBD. In het kader van een bewustwordingsprogramma is het van belang risico's te mitigeren door een combinatie van maatregelen te kiezen, die gericht zijn op kennis, houding en gedrag en daarbij rekening te houden met de individuele (start)situatie van de medewerker. Een onbewust onbekwame medewerker moet vooral kennis aangereikt krijgen om te weten wat hem wordt verwacht, terwijl een onbewust bekwame medewerker vooral geprikkeld moet worden met instrumenten om het gewenste gedrag te tonen.

4.5. Opstellen van een plan

Nadat de behoeftebepaling heeft plaatsgevonden kan het plan worden opgesteld waarmee het eigenlijke bewustwordingsprogramma vorm kan krijgen. Het plan bevat de basiselementen voor de te volgen strategie en bevat ten minste de volgende onderwerpen:

- de formele basis voor het programma, bestaande uit in wet- en regelgeving vastgelegde eisen, het strategische beveiligingsbeleid en de richtlijnen die gelden binnen de organisatie;
- de wijze waarop het programma wordt aangestuurd en ingebed in de organisatie;
- de scope van het programma;
- de bepaling van doelgroepen voor bepaalde onderdelen van het programma (denk aan nieuwe medewerkers, medewerkers van het KCC, medewerkers op vitale functies (systeembeheer, applicatiebeheer en dergelijke);
- de verplichte en optionele onderdelen van het programma voor iedere doelgroep en de frequentie van deelname;
- leerdoelen en te behandelen onderwerpen voor afzonderlijke onderdelen van het programma;
- documentatie, terugkoppeling en registratie van deelname;
- hoe evaluatie en onderhoud van het programma gaat plaatsvinden.

4.6. Stellen van prioriteiten

In het programma moeten belangrijke en urgente zaken voorrang krijgen. Kennis die voor alle medewerkers van belang is, zoals de regels over het gebruik van wachtwoorden of het omgaan met vertrouwelijke informatie, krijgt voorrang boven zaken die alleen voor medewerkers in specifieke functies een rol spelen. Generieke onderwerpen krijgen in de fasering van de aanpak prioriteit boven specifieke onderwerpen.

4.7. Budgettering

Nadat de strategie is bepaald en de prioriteiten zijn vastgesteld, moet het benodigde budget worden bepaald. Aan de hand van het opgestelde plan zal een berekening gemaakt moeten worden van de kosten die betrekking hebben op het ontwikkelen van materiaal, de productie en verspreiding ervan en de kosten die gemoeid zijn met het daadwerkelijk uitvoeren van het programma. Een exacte berekening van het budget is lastig te maken. In plaats daarvan kan een andere benadering worden gekozen, bijvoorbeeld door de budgettering te baseren op een bepaald percentage van het gehele trainings- en opleidingsbudget van de organisatie, of dit als onderdeel van de totale personeelskosten per medewerker op te nemen.

4.8. Commitment en draagvlak

Een bepalende succesfactor voor een bewustwordingsprogramma is dat dit wordt gedragen door bestuur en management van de gemeente. Dat moet zichtbaar worden gemaakt door aanwezig te zijn op belangrijke momenten in het programma, zoals de startbijeenkomst en de eerste presentatie. Als de 'baas' niet uitstraalt dat hij het bewustwordingsprogramma belangrijk vindt, is geen draagvlak bij de medewerkers te verwachten.

Wat is de rol van bestuur en directie in het kader van het beveiligingsbewustzijn van medewerkers?

Bestuur en directie (hoger management) van de gemeente staan aan de basis van een sterke beveiligingscultuur in de gemeentelijke organisatie. Zij zijn opdrachtgever voor een bewustwordingscampagne en moeten hiervoor de middelen beschikbaar stellen. Bestuur en directie moeten de noodzaak zien om aandacht te besteden aan informatiebeveiliging en bewustwording en in houding en gedrag het belang van informatieveiligheid uitdragen. Binnen het bestuur hoort een portefeuillehouder informatieveiligheid aanwezig te zijn. Deze is vanuit het bestuur de belangrijkste sponsor van het bewustzijnsprogramma. In het kader van risicomanagement heeft de bestuurder een direct belang bij het verhogen van het beveiligingsbewustzijn van de medewerkers.

De belangrijkste taak van de directie is het verstrekken van de middelen, in de vorm van geld en capaciteit, die structureel benodigd zijn om tot verhoging van het beveiligingsbewustzijn te komen en te zorgen dat de aandacht hiervoor niet verdwijnt. En uiteraard speelt op dit niveau voorbeeldgedrag ook een belangrijke rol.

Wat is de rol van de lijnmanager in het kader van het beveiligingsbewustzijn van medewerkers?

Lijnmanagers moeten in de aansturing van medewerkers in houding en gedrag uitdragen dat informatieveiligheid een kernwaarde is van de organisatie. Zij moeten de noodzaak zien om aandacht te besteden aan informatiebeveiliging en bewustwording en hun medewerkers tijd en ruimte geven om aan bewustwordingssessies en trainingen deel te nemen. Uiteindelijk is de lijnmanager de drager van de risico's voor de bedrijfsvoering die voortkomen uit ontbrekend beveiligingsbewustzijn.

5. Ontwikkelingsfase

5.1. Inleiding

Nadat het bewustwordingsprogramma is ontworpen, moet het ondersteunende materiaal worden ontwikkeld. Het aandachtspunt hierbij is dat dit materiaal moet aansluiten bij de belevingswereld, het kennisniveau en de functie van de medewerker. Een deel van het materiaal moet voor iedere medewerker toepasbaar zijn, maar een deel zal ook gericht zijn op specifieke doelgroepen. Bij de ontwikkeling van het materiaal spelen onderstaande vragen een rol:
- Welk gedrag willen we versterken?
- Welke vaardigheden willen we aanleren en laten toepassen?

5.2. Ontwikkelen van materiaal

Het tijdens de ontwerpfase geschreven plan zal een lijst bevatten met onderwerpen die behandeld moeten worden. Voor de wijze waarop invulling wordt gegeven aan kennisoverdracht staan allerlei vormen ter beschikking. De keuze van de vorm hangt af van het type en de complexiteit van de boodschap. Onderstaand overzicht kan een hulpmiddel zijn bij de keuze van de wijze waarop de onderwerpen gecommuniceerd kunnen worden:

- boodschappen op dagelijks gebruiksmateriaal, zoals pennen, muismatjes, keycords en dergelijke;
- posters met informatie wat te doen of juist niet te doen;
- screensavers met wisselende teksten;
- nieuwsbrieven;
- e-mailberichten;
- videoberichten;
- mondelinge instructies of presentaties;
- securitydagen;
- dagelijkse 'tips van de dag' op het opstartscherm;
- e-learning, trainingen, opleidingen;
- pubquiz;
- enzovoort.

5.3. Selecteren van onderwerpen

Zonder uitputtend te zijn volgt hieronder een overzicht van mogelijke onderwerpen die tijdens het bewustwordingsprogramma aan de orde kunnen komen:

- implementatie van beveiligingsbeleid, regels en richtlijnen;
- hoe om te gaan met wachtwoorden;
- het up-to-date houden van virusscanners;
- e-mailgebruik en omgang met bijlagen;
- opslaan en verwijderen van gegevens;
- 'clean desk - clear screen';
- social engineering;
- Mobile Device Management;
- installeren van updates;
- omgang met bezoekers;
- enzovoort.

5.4. Bronnen voor materiaal

Op internet zijn verschillende bronnen beschikbaar voor materiaal dat tijdens een bewustwordingsprogramma kan worden gebruikt. Specifiek voor de overheid is er de website www.digitaleoverheid.nl, waarop campagnemateriaal is terug te vinden voor het vergroten van het besef welke handelingen in privé- of werksituaties wel of niet uiting geven aan beveiligingsbewustzijn. Andere voorbeelden zijn de website van Alert Online (www.alertonline.nl) en de website www.veiliginternetten.nl. Daarnaast is veel informatie te halen uit de maandmonitor van de IBD. En uiteraard zijn de media een belangrijke bron van informatie over informatieveiligheid.
De Informatiebeveiligingsdienst houdt een overzicht bij van alle activiteiten die in het kader van bewustwording door gemeenten en niet commerciële organisaties worden ondernomen (https://www.informatiebeveiligingsdienst.nl/overzicht-bewustwordingscampagnes/).

5.5. Zelf doen, samen doen, uitbesteden?

Niet alleen de ontwikkeling, ook het onderhoud van een bewustwordingsprogramma kost veel tijd, energie en geld. In de ontwerpfase is het een belangrijke afweging of je het als individuele gemeente allemaal zelf moet gaan bedenken, of dat dit aan de markt wordt overgelaten, dan wel samen met andere gemeenten wordt opgepakt. Vragen die bij deze afweging kunnen helpen, zijn de volgende:

- Hebben we binnen de organisatie voldoende kennis en capaciteit beschikbaar?
- Is het kosteneffectiever om het programma zelf op te zetten of uit te besteden?
- Is de organisatie in staat om ontwikkelde of aangeleverde programma's zelf te onderhouden?
- Past zelf ontwikkelen in het beoogde tijdsplan?

Vanuit de gedachte van samen organiseren neemt de IBD het initiatief voor een partnerschap met gemeenten voor de verdere uitwerking en het onderhoud van een op gemeenten gericht bewustwordingsprogramma.

6. Implementatiefase

Na de fasen Ontwerp en Ontwikkeling moet het bewustwordingsprogramma binnen de organisatie uitgelegd en gecommuniceerd worden. Het doel is begrip en ondersteuning te realiseren voor de uitvoering van het programma en de bijdrage die van medewerkers verwacht wordt in het programma. In deze implementatiefase worden de stakeholders en ambassadeurs betrokken bij de uitrol van het programma.

6.1. Betrekken van stakeholders en ambassadeurs

Waarom is betrokkenheid van stakeholders en ambassadeurs belangrijk?

Een integrale aanpak om het beveiligingsbewustzijn te verhogen gaat de hele organisatie aan, niet alleen de CISO of de communicatieadviseur. Zonder instemming of betrokkenheid van bestuur en management bij een programma om het beveiligingsbewustzijn te verhogen, is dit programma tot mislukken gedoemd.

Bestuurders

Privacy en informatiebeveiliging zijn in het algemeen geen onderwerpen die op veel aandacht vanuit het bestuur kunnen rekenen. Bestuurders beschouwen informatiebeveiliging en het bijbehorende beveiligingsbewustzijn over het algemeen als een vanzelfsprekende randvoorwaarde voor de bedrijfsvoering en niet als iets wat bestuurlijke betrokkenheid vereist. Maar bestuurders vertegenwoordigen wel de waarden waarvoor de organisatie staat. Een bestuurder moet dan ook zelf het goede voorbeeld geven hoe je verantwoordelijk omgaat met informatie. Een belangrijke verantwoordelijkheid van een bestuurder is ook het bevorderen van een veilige cultuur in de organisatie, waarin iedereen zich vrij voelt om dreigingen waar te nemen en te melden, zodat de bijbehorende risico's kunnen worden aangepakt.

In het kader van de BIO wordt de rol van de bestuurder belangrijker. De BIO positioneert de bestuurder sterker dan voorheen in de rol waarin hij of zij risicogebaseerd stuurt op het gebied van informatieveiligheid. De bestuurder moet hierover met de CISO afspraken maken[8].

Binnen het bestuur hoort een portefeuillehouder informatieveiligheid aanwezig te zijn. Deze is vanuit het bestuur de belangrijkste sponsor van het bewustwordingsprogramma. In het kader van risicomanagement heeft de bestuurder een direct belang bij het verhogen van het beveiligingsbewustzijn van de medewerkers.

Directie of managementteam

De belangrijkste taak van de directie is het verstrekken van de middelen, in de vorm van geld en capaciteit, die structureel benodigd zijn om tot verhoging van het beveiligingsbewustzijn te komen en te zorgen dat de aandacht hiervoor niet verdwijnt. En uiteraard speelt op dit niveau voorbeeldgedrag ook een belangrijke rol.

[8] Om het gesprek over informatiebeveiliging en privacy met bestuurders te voeren, heeft de VNG een mindmap informatiebeveiliging opgesteld (‘Eigen huis op orde’, juni 2019). Daarnaast kunnen de ‘Tien bestuurlijke principes voor informatiebeveiliging’ door de CISO worden gebruikt als leidraad voor dit gesprek.

Lijnmanagement

Het bevorderen van beveiligingsbewustzijn wordt meestal als een taak van de CISO en/of de FG beschouwd binnen de gemeentelijke organisatie. Deze moeten er inderdaad op toezien dat er binnen de organisatie maatregelen worden getroffen om het beveiligingsbewustzijn te verhogen. Maar de werkelijke actiehouder is de lijnmanager. In de praktijk blijkt het vaak lastig om de lijnmanagers in de rol te plaatsen die van hen verwacht wordt. Verhogen van bewustzijn wordt niet altijd gezien als onderdeel van de lijnverantwoordelijkheid, maar beschouwd als een impliciet onderdeel van de houding en het gedrag van medewerkers.
Van lijnmanagers wordt verwacht dat zij:

- Inzicht hebben in de dreigingen en risico's die zich binnen hun afdeling en werkprocessen voordoen. De maatregelen die hier tegenover staan moeten zij helder kunnen uitleggen aan hun medewerkers.
- Weten welke houding en gedrag noodzakelijk zijn bij de medewerkers om de organisatie en werkprocessen veilig te houden.
- Zorgen dat de medewerkers de juiste opleiding en training volgen om in hun werkzaamheden bewust met privacy en informatiebeveiliging om te gaan.
- Het beveiligingsbeleid en wijzigingen die zich daarin voordoen onder de aandacht van de medewerkers brengen.
- Een beveiligingsbewuste cultuur helpen bevorderen door informatieveiligheid onderdeel te laten zijn van de manier van denken van medewerkers.
- Een voorbeeldfunctie vervullen.
- Uitstralen dat ze veilig en privacybewust werken net zo belangrijk vinden als snel en klantgericht werken.

ICT-medewerkers

ICT-medewerkers dienen ervoor te zorgen dat de basis op orde is. De basis op orde betekent de inrichting van een aantal kritische IT-beheerprocessen, zoals weergegeven in de mindmap Maatregelen en Processen van module 1 Verhogen Digitale Weerbaarheid en de bijbehorende filmpjes[9]: incidentmanagement, wijzigings-, configuratiebeheer, patch- en bedrijfscontinuïteitsmanagement (waaronder back-up en recovery). ICT-medewerkers moeten inzien dat er niet alleen beheer van deze processen moet plaatsvinden, zodat ze zorgdragen voor een actueel beeld van het ICT-landschap, maar dat ze ook bedoeld zijn om veilig gedrag van medewerkers te ondersteunen. Opvolging van beveiligingsincidenten zorgt voor een lerende organisatie. ICT medewerkers moeten worden meegenomen in de doelstelling van een lerende organisatie, waarin privacy en informatiebeveiliging onderwerpen zijn van een voortdurende leercyclus.

HRM/Personeelszaken

De afdeling HRM/Personeelszaken speelt een belangrijke rol in het kader van personele beveiligingsmaatregelen. Die rol wordt uitgebreid beschreven in het BIO-OP product 'Handreiking personeelsbeleid'. [10] In dit document volstaan we met het benoemen van deze afdeling als een belangrijke stakeholder. Gedurende de hele HR-cyclus is aandacht voor het verhogen van beveiligingsbewustzijn van medewerkers noodzakelijk. Dat begint al voor de indiensttreding van medewerkers door middel van screening en strekt zich uit tot aanstellings- en wijzigingsprocedures en uiteindelijk tot een adequate uitdiensttredingsprocedure.

[9] Verhogen Digitale Weerbaarheid, module 1: Maatregelen en processen, Informatiebeveiligingsdienst
[10] Handreiking Personeelsbeleid, Informatiebeveiligingsdienst

De rol van HRM/Personeelszaken is met name formeel ingestoken, maar de wijze waarop personele maatregelen worden getroffen en bewaakt heeft ook grote invloed op de beveiligingscultuur van de organisatie. Zo dient HRM/Personeelszaken ook te bewaken dat bij de periodieke beoordelingsgesprekken beveiliging voldoende aandacht krijgt.

Afdeling Communicatie

De afdeling Communicatie is voor de CISO en FG een belangrijke partner bij het verhogen van het beveiligingsbewustzijn van medewerkers. Het is de primaire sparringpartner van CISO en FG om per leerfase te bepalen op welke wijze en met welke middelen het beste resultaat behaald kunnen worden. De IBD heeft een voorbeeld van een communicatieplan informatiebeveiliging opgesteld[11], om gemeenten te ondersteunen bij hun inspanningen om de informatiebeveiliging naar een hoger niveau te brengen door de inzet op het verhogen van het beveiligingsbewustzijn en de daarbij horende communicatie(middelen).

Ambassadeurs

Ambassadeurs worden gekozen, of dienen zich vanzelf aan. Iedereen binnen de organisatie die in houding en gedrag uitstraalt dat hij of zij beveiligingsbewust is, kan een ambassadeur zijn. Ambassadeurs snappen het belang van privacy en informatieveiligheid en ondersteunen als vanzelfsprekend de regels die binnen de organisatie hiervoor zijn opgesteld. Een ambassadeur aarzelt niet om collega's aan te spreken op hun ongewenste gedrag. Hoe groter het draagvlak van een ambassadeur is onder de medewerkers, hoe groter het effect is van dit aanspreken op gedrag. Ambassadeurs kunnen helpen om maatregelen die door de organisatie worden 'opgelegd' aanvaardbaar te maken als collectief belang, dus niet alleen voor de organisatie belangrijk maar ook voor de medewerker zelf. Een goede ambassadeur is de medewerker die:

- niet uitlegt dat maatregelen moeten worden nageleefd, maar uitlegt waarom ze getroffen worden;
- de boodschap niet via de hiërarchie laat lopen, maar communiceert dwars door de organisatie heen;
- niet alleen zijn verhaal vertelt, maar ook luistert naar de ander;
- zich richt op verbinding in plaats van op controle.

Als niemand zich als ambassadeur aanmeldt, kan de incidentenregistratie wellicht uitkomst bieden. De medewerker die het initiatief heeft genomen een datalek te melden, kan zo maar een goede ambassadeur zijn.

[11] Handreiking Communicatieplan informatiebeveiliging, Informatiebeveiligingsdienst

7. Evaluatie- en onderhoudsfase

In deze fase wordt beoordeeld of de uitvoering van het bewustwordingsprogramma in overeenstemming is met het gedefinieerde ontwerp en of het behaalde resultaat voldoet. Deze fase maakt van het gehele proces van de ontwikkeling van een bewustwordingsprogramma een cyclisch en zich herhalend proces.

Gedurende de uitvoering van het bewustwordingsprogramma dient informatie verzameld te worden over de deelname aan het programma. Hieronder een paar voorbeelden van indicatoren die inzicht geven in de mate van bewustzijn van medewerkers en van de organisatie:

- het aantal datalekken dat wordt gemeld;
- het aantal beveiligingsincidenten in een bepaalde periode;
- het aantal keren dat geklikt wordt op een link in een (georganiseerde) phishingmail;
- het aantal keren dat een phishingmail als beveiligingsincident wordt gemeld;
- het aantal aan gebruik van mobiele apparatuur gerelateerde incidenten;
- het aantal verzoeken om wijziging van wachtwoorden;
- het aantal medewerkers dat geen geheimhoudingsverklaring heeft ondertekend;
- het aantal door malware geinfecteerde computers;
- het aantal apparaten (laptops, smartphones, USB-sticks) dat als verloren of gestolen is gemeld;
- het aantal computers waarvan bij een verlaten werkplek het scherm niet vergrendeld is;
- het aantal medewerkers dat aan het eind van de werkdag een ‘clear desk’ achterlaat.
- de resultaten van vulnerabilityscans.

Voor het beoordelen van leerresultaten wordt bij voorkeur gebruikgemaakt van een Leer Management Systeem (LMS), waarin de volgende informatie wordt vastgelegd:

- cursus- en opleidingsdata;
- inhoud van de opleiding;
- deelname, zowel percentages per afdeling als totaal voor de organisatie.

De meetgegevens kunnen worden gebruikt voor rapportages aan het management over de mate van compliance, de kwaliteit en volwassenheid van het bewustwordingsprogramma, de bereidheid van lijnmanagers om deelnemers af te vaardigen en kwaliteitsverbetering. De deelnamegegevens geven een rechtvaardiging van beschikbaar gesteld budget en geven in detail aan of medewerkers hebben deelgenomen aan het programma. Aan niet deelnemen kan een sanctionering worden verbonden, bijvoorbeeld in de vorm van een beperking van gebruiksrechten binnen een bepaalde functie.

7.1. Evaluatie en feedback

Voortdurende verbetering van een bewustwordingsprogramma kan niet plaatsvinden als het ontbreekt aan informatie hoe een programma werkt. Vanaf de ontwikkelfase van het programma moet worden nagedacht over de manier waarop de kwaliteit van het programma op een objectieve manier kan worden vastgesteld. De meest gangbare manieren voor evaluatie en feedback zijn:

- Gebruik van evaluatieformulieren. Gebruik daarbij zoveel mogelijk voorbedrukte teksten en normeringen, zodat de informatie op eenvoudige wijze verwerkbaar is.
- Selectieve interviews met deelnemers waarin 1-op-1 de onderwerpen van de evaluatie besproken worden.
- Onafhankelijke observatie door een derde partij die kan zorgen voor een gedegen onafhankelijk oordeel.
- Formele statusrapporten door managers van deelnemers.

7.2. Veranderingen doorvoeren

Een bewustwordingsprogramma is geen statisch iets, maar een dynamisch proces dat onder invloed van nieuwe technieken en veranderingen in kennis en gedrag van medewerkers voortdurend aanpassing vereist. Ook veranderingen in het strategisch beleid van de organisatie of wijzigingen in wet- en regelgeving kunnen aanleiding zijn om veranderingen door te voeren.

7.3. Verhogen van het niveau

Zoals eerder besproken zal een bewustwordingsprogramma moeten starten met een focus op generieke beveiligingsaspecten die de hele organisatie raken. Als het beoogde niveau gehaald is, zal de volgende stap gezet moeten worden om het niveau te verhogen. Dit kan door differentiatie aan te brengen in doelgroepen, die ieder een op hun niveau of functie passend programma gaan volgen. Op deze wijze zal het programma groeien in volwassenheid. Het verdient aanbeveling om deze doorgroei in het ontwerp van het programma mee te nemen en te baseren op meetbare gegevens, zoals die hierboven zijn weergegeven.

8. Uitvoering

8.1. Inleiding

Aan de hand van een aantal persona maken we de in de voorgaande hoofdstukken voorgestelde aanpak om het beveiligingsbewustzijn te verhogen concreet. We volgen hen in de ontwikkeling van onbewust onbekwame medewerkers naar onbewust bekwame medewerkers, waarbij we kijken naar in te zetten instrumenten en leermiddelen om deze ontwikkeling te ondersteunen.

Hester, Bas, Paula en Frits zijn onlangs als nieuwe medewerkers begonnen bij de gemeente Meerstad. Hester is medewerkster van het Klant Contact Centrum en heeft via de telefoon, mail en receptie eerstelijns klantcontacten. Bas werkt op de afdeling WMO als consulent Jeugdzorg en wordt verantwoordelijk voor het indiceren van hulpbehoeften van jongeren. Paula is tijdelijk ingehuurd als afdelingshoofd Externe Dienstverlening en Frits is functioneel beheerder van de BRP-applicatie.

8.2. Fase 1: onbewust onbekwaam

Na de afronding van hun sollicitatie hebben de nieuwe medewerkers van de afdeling HRM/Personeelszaken een introductiemap ontvangen met informatie over de gemeente en een korte toelichting op hun eerste werkdag, die start met een gezamenlijke introductiebijeenkomst. De afdeling HRM heeft na afronding van de sollicitaties de komst van de nieuwe medewerkers op het intranet van de gemeente bekendgemaakt en de naaste collega's en leidinggevenden apart via een persoonlijke e-mail geïnformeerd over hun komst.

In de introductiemap is naast de algemene informatie over de gemeente een overzicht van de huisregels en een gedragscode opgenomen en een overzicht van de veiligheidsvoorschriften. Onderdeel van die voorschriften is een instructie hoe wordt omgegaan met beveiligingsincidenten binnen de gemeente. Een ander onderdeel is de klokkenluidersregeling, die zorgdraagt voor een veilige meldcultuur in de gemeente. De introductiemap bevat ook een geheimhoudingsverklaring, die ondertekend moet worden meegenomen op de eerste werkdag. Daarnaast ontvangt elke nieuwe medewerker een e-mail met de mededeling dat voor hem of haar een Verklaring omtrent Gedrag (VOG) is aangevraagd, gericht op hun specifieke functie. Door met DigiD in te loggen op Justis wordt hun aanvraag in behandeling genomen. De medewerkers wordt verzocht om de VOG op hun eerste werkdag mee te nemen, dan wel deze zo snel mogelijk in te leveren bij de afdeling HRM.

Op de eerste werkdag van de nieuwe medewerkers staat een introductiebijeenkomst gepland. Zij worden ontvangen door een medewerker van de afdeling HRM, die met de nieuwe medewerkers een checklist doorneemt van activiteiten die uitgevoerd zijn om een vloeiende start te kunnen maken binnen de gemeente. Daarnaast wordt een eerste begin gemaakt met het opstellen van een personeelsdossier. De checklist wordt na controle op uitvoering van de activiteiten door elke nieuwe medewerker ondertekend en opgenomen in het personeelsdossier. Op de checklist staan de volgende activiteiten:

- aanwijzen werkplek
- verstrekken bedrijfstelefoon en nummer
- autorisatie tot netwerk en intranet
- aanmaken email-adres
- autorisatie voor systeemapplicaties
- verstrekken toegangspas (en eventuele parkeerkaart)

Het personeelsdossier bevat na deze introductiebijeenkomst de volgende documenten:

- een ondertekende arbeids- of opdrachtovereenkomst
- een ondertekende geheimhoudingsverklaring
- een Verklaring Omtrent Gedrag
- een exemplaar van de bovenstaande checklist
- een kopie van het door de medewerker overgelegde ID-bewijs
- een bruikleenovereenkomst voor de telefoon en eventuele laptop
- een bruikleenovereenkomst voor de toegangspas

De gemeente Meerstad hecht eraan om bij de introductie van nieuwe medewerkers direct aandacht te geven aan de beveiligingsvoorschriften binnen de organisatie. Zo mogelijk is de burgemeester of een wethouder aanwezig bij de introductiebijeenkomst om de missie en waarden van de gemeente toe te lichten. Een directielid zorgt voor de vertaling van de missie en waarden naar de huisregels van de organisatie en de rol die medewerkers spelen in een veilige organisatie. De CISO geeft een toelichting op de informatiebeveiligingsvoorschriften. HRM gaat in op een aantal personele aspecten in relatie tot informatiebeveiliging, zoals de gedragscode en de geheimhoudingsverklaring.

Omdat introductiebijeenkomsten niet altijd in te plannen zijn op een moment dat bestuur en directie schikt, is door de gemeente een introductievideo gemaakt, waarin aandacht voor informatiebeveiliging en privacy wordt gevraagd en toegelicht door een vertegenwoordiger van HRM, de CISO, een bestuurder en een directielid. Zo wordt gezorgd dat elke nieuwe medewerker dezelfde informatie krijgt bij aanvang van het dienstverband of de opdracht.

Alle nieuwe medewerkers krijgen van de afdeling HRM een toegangscode tot een e-learningomgeving, die onderdeel is van een persoonlijke leeromgeving. Eén van de modules die iedereen moet doorlopen is de module ‘Informatiebeveiliging en privacy’. Hierin worden de beveiligingsmaatregelen behandeld die de beschikbaarheid, integriteit en vertrouwelijkheid van de gemeentelijke informatie, met name de persoonsgegevens, moeten waarborgen. Onderdelen van deze module zijn de generieke maatregelen ten aanzien van:

- logische toegangsbeveiliging: gebruik van wachtwoorden, autorisatie tot bedrijfssystemen en applicaties, Mobile Device Management, incidentenprocedure en dergelijke;
- fysieke toegangsbeveiliging: toegang tot het gebouw en zonering van ruimten, omgang met bezoekers, dragen van badges, sleutelbeheer en dergelijke;

- dreigingen: social engineering, (spear) phishing, misbruik van bevoegdheden en vertrouwen en dergelijke.

Via het Leer Management Systeem houdt HRM van elke medewerker bij welke e-learning, training of opleiding wordt gevolgd.

In de fase onbewust onbekwaam zijn de nieuwe medewerkers zich niet bewust van ontbrekende kennis. Inzet van leermiddelen is er dan ook op gericht om het inzicht bij de medewerkers te laten ontstaan dat er regels en voorschriften zijn die in elke functie als randvoorwaarde in acht moeten worden genomen om als nieuwe medewerker binnen de organisatie te kunnen functioneren.

8.3. Fase 2: bewust onbekwaam

In de eerste vier weken van het dienstverband of de opdracht krijgt elke nieuwe medewerker een mentor aangewezen die hem of haar begeleidt in de nieuwe functie. Bij voorkeur is dit iemand met kennis, ervaring en aanzien binnen het team, die voldoende vrijgemaakt is om zijn of haar mentorrol te vervullen. Voor Hester is dat een naaste collega, die dezelfde functie al een aantal jaren vervult. Omdat die haar mentorrol vooral richt op het vertrouwd maken van Hester met de KCC-applicatie en de bezoekersregistratie, krijgt Hester via e-learning een training om haar alert te maken op de gevaren van social engineering. Deze is aanvullend op de training die zij in het kader van haar introductie als nieuwe medewerker heeft gevolgd en is speciaal gericht op de dreigingen waar zij in haar specifieke functie mee te maken krijgt. Zo leert zij dat ze niet zomaar het e-mailadres mag verstrekken van een medewerker als een klant daarom vraagt en zich ook niet moet laten overrompelen door iemand die belt en zich voordoet als goede bekende van de burgemeester. Ze leert de grenzen kennen van het eerstelijnscontact en de afspraken die er zijn om klantvragen over te dragen naar de tweede lijn.

Bas heeft niet het geluk dat hij kan worden ingewerkt door een naaste collega, maar hij heeft dezelfde functie al in een andere gemeente uitgevoerd en kan dus terugvallen op zijn ervaring. Het is voor hem wel nieuw dat de gemeente Meerstad cliënten niet naar het gemeentehuis laat komen, maar ze in hun eigen omgeving opzoekt om de hulpbehoefte te bepalen. Daarvoor krijgt hij de beschikking over een laptop, een bedrijfstelefoon en een token waarmee hij kan inloggen op het gemeentelijke netwerk om gespreksverslagen rechtstreeks in te voeren in de Jeugdhulp-applicatie.
Bas moet in zijn werksituatie rekening houden met welke informatie wel en niet kan worden gedeeld met zijn cliënten, maar ook welke informatie van de cliënt mag worden vastgelegd in relatie tot het doel van de hulpverlening. Omdat deze informatie van geval tot geval kan verschillen, is een training over toepassing en voorschriften van de AVG het aangewezen instrument om Bas te laten groeien in zijn rol als consulent. Welke voorschriften gelden ten aanzien van gebruik van mobiele apparatuur zijn hem bekendgemaakt via de e-learning in het introductieprogramma.

Paula wordt als externe medewerker niet anders behandeld dan de interne medewerkers. Zij volgt hetzelfde introductieprogramma en moet aan dezelfde voorwaarden voldoen als de interne medewerkers. Dus tekent zij ook de geheimhoudingsverklaring en de aanvraag VOG. Als externe krijgt zij geen laptop of telefoon van de gemeente, maar ze krijgt wel toegang tot het gemeentelijke netwerk om af en toe vanuit huis te kunnen werken. Ze krijgt een aparte instructie van de systeembeheerder hoe ze toegang kan verkrijgen en welke beveiligingsmaatregelen ze in haar privéomgeving moet treffen om beveiligingsrisico's weg te nemen. Omdat haar voorganger tijdelijk met ziekteverlof is, is er geen warme overdracht van taken geregeld, maar als interimmer heeft Paula voldoende ervaring om zich taken snel eigen te maken. Wat wel nieuw is voor haar, zijn de huisregels en de gedragscode van de gemeente Meerstad.

Als mentor krijgt zij een collega uit het managementteam toegewezen, die haar wegwijs kan maken in de bedrijfscultuur van de gemeente Meerstad.

Frits is nog niet bekend met het BRP-systeem dat hij als functioneel beheerder onder zijn hoede krijgt. Dat was bekend bij zijn sollicitatie, maar de gemeente Meerstad heeft hem een opleiding aangeboden om zich de specifieke kennis van het systeem eigen te maken. Naast een cursus bij de leverancier van het systeem, heeft de gemeente Meerstad haar buurgemeente bereid gevonden om de daar werkzame functioneel beheerder van het BRP-systeem als mentor te laten fungeren tijdens de inwerkperiode. Voor Frits is het vooral belangrijk te weten welke afspraken en procedures er zijn tussen de gemeente en de leverancier van de BRP-applicatie. Deze draait in een cloudomgeving. Alle afspraken en procedures zijn terug te vinden in de dienstverleningsovereenkomst die de gemeente Meerstad met de leverancier heeft afgesloten.

In de fase bewust onbekwaam ontstaat het inzicht bij de medewerkers dat zij vanuit hun rol of functie binnen de gemeente behoefte hebben aan kennis van specifieke maatregelen die toegepast moeten worden in het kader van informatiebeveiliging. Bij HRM is deze leerbehoefte in relatie tot de specifieke rol of functie in beeld, zodat hier adequaat op kan worden ingespeeld. Hiervoor wordt het eerder genoemde LMS gebruikt: per rol of functie wordt aangegeven welke training of opleiding op het gebied van informatiebeveiliging en privacy moet worden gevolgd en dit wordt actief bijgehouden.

8.4. Fase 3: bewust bekwaam

Hester heeft in de eerste vier weken van haar dienstverband veel klantcontacten gehad en een redelijk inzicht ontwikkeld in de contacten waar ‘een luchtje aanzit’. Waar zij twijfelt aan de oprechtheid of betrouwbaarheid van de informatie die klanten haar verstrekken, raadpleegt zij nog wel haar collega’s of die twijfel gedeeld wordt. Bas raakt ook steeds meer vertrouwd met de contacten in het kader van Jeugdhulp. Hij weet inmiddels dat er vooral door externe ketenpartners meer informatie wordt opgevraagd dan voor het bepalen van de hulpbehoefte noodzakelijk is. Bij twijfel valt hij terug op zijn kennis van de grondslagen voor gegevensverwerking die hij in de AVG-cursus heeft geleerd. Hij merkt wel dat hij vaak terugvalt op zijn theoretische kennis, die niet altijd makkelijk te vertalen is naar de specifieke situatie waar hij in zijn werk tegenaan loopt. Paula heeft haar interimopdracht inmiddels beëindigd, omdat haar voorganger eerder dan verwacht van ziekteverlof is teruggekeerd. Ze is blij verrast met de zorgvuldigheid van de exitprocedure die de gemeente Meerstad hanteert. Niet alleen krijgt zij een exitgesprek met haar opdrachtgever over de inhoudelijke kant van haar opdracht en de lessen die Meerstad uit haar ervaring kan leren, ze doorloopt bij HRM ook een soort ‘omgekeerde introductie’: aan de hand van de bij de start van haar opdracht opgestelde checklist wordt haar token ingenomen en haar toegangspas. Zij ziet dat vanuit HRM een mail verzonden wordt aan de netwerkbeheerder dat haar toegangsrechten beëindigd kunnen worden en dat er een aantekening wordt gemaakt wanneer haar P-dossier kan worden vernietigd. Ook krijgt zij een ontvangstbewijs voor de door haar ingeleverde token en toegangspas.
Frits is duidelijk gegroeid in zijn rol van functioneel beheerder van de BRP en weet inmiddels waar de grens ligt tussen zijn taken en die van de leverancier. Als er onduidelijkheden zijn valt hij terug op de afspraken die vastgelegd zijn in de dienstverleningsovereenkomst.

In de fase bewust bekwaam zijn de gewenste kennis, houding en gedrag ten aanzien van informatieveiligheid binnen de eigen functie aangeleerd. Er is nog geen sprake van automatismen, maar wel van beveiligingsbewustzijn.

8.5. Fase 4: onbewust bekwaam

Na het doorlopen van de introductiefase en de voor de specifieke functies van Hester, Bas en Frits noodzakelijke opleidingen en trainingen, wordt informatieveiligheid onbewust voortdurend gewaarborgd in de uitvoering van de dagelijkse werkzaamheden. Er is sprake van routine in de toepassing van beveiligingsvoorschriften en -maatregelen. Tegelijk ontstaat door deze routine afstand tot het doel van deze voorschriften en maatregelen. Het is in deze fase van belang om vanuit de organisatie voeding te blijven geven aan de aandacht die medewerkers moeten behouden voor informatiebeveiliging. Het ontstaan van rituelen moet worden voorkomen. Door middel van postercampagnes, screensavers en gebruik van persona op het intranet wordt de onbewuste aandacht voor informatieveiligheid telkens weer even bewust gemaakt. Om op een speelse manier invulling te geven aan het beveiligingsbewustzijn wordt regelmatig een pubquiz georganiseerd, waarbij medewerkers in competitie met andere afdelingen strijden om de prijs van meest beveiligings- of privacybewuste afdeling van de gemeente Meerstad.

8.6. Evaluatie en monitoring

Elke twee maanden is er in de gemeente Meerstad een overleg tussen de CISO en FG, de afdeling HRM, de netwerkbeheerder en de afdeling Communicatie. Doel van dit overleg is om te bepalen of de personele maatregelen en de in te zetten leermiddelen moeten worden bijgesteld. Basis voor dit overleg is de incidentenregistratie. Aan de hand van de geregistreerde incidenten wordt nagegaan of er interventies nodig zijn op het gebied van kennis, houding en gedrag. Suggesties voor aanvullende trainingen en opleidingen worden doorgegeven aan de lijnmanagers. De geconstateerde incidenten vormen daarnaast input voor de afdeling Communicatie om voorschriften via Intranet nog eens te verduidelijken en eventueel extra te ondersteunen met postercampagnes, nieuwsbrieven en dergelijke.

Bovenstaande fictieve weergave van de wijze waarop in de gemeente Meerstad wordt gewerkt aan het verhogen van het beveiligingsbewustzijn is erop gericht duidelijk te maken dat beveiligingsbewustzijn geen vanzelfsprekendheid is, maar het resultaat van voortdurende aandacht vanuit de organisatie voor de samenhang tussen in te zetten instrumenten en de effectiviteit daarvan in verschillende stadia van bewustwording en de rol van medewerkers in de organisatie. Om die samenhang te behouden is er een samenspel nodig van meerdere actoren in de gemeentelijke organisatie. Beveiligingsbewustzijn is geen onderwerp dat vanuit één specifieke functie moet worden benaderd, het resulteert juist uit het inzicht dat het voor iedereen in de organisatie een onderdeel is van de rol die in de organisatie wordt vervuld.

INFORMATIE
BEVEILIGINGS
DIENST

Bijlage 1 Voorbeeld gedragscode

Gedragsregels informatiebeveiliging en privacy

Het is belangrijk dat er zorgvuldig met informatie van de gemeente omgegaan wordt. Daarom heeft de gemeente hiervoor regels opgesteld. Informatie kent vele vormen: gesprekken, papieren documenten, digitaal opgeslagen informatie, dvd's, foto's, et cetera. Digitale informatie kan op allerlei plekken zijn opgeslagen: pc's, laptops, telefoons, servers, websites, netwerken, USB-sticks et cetera
Informatie vertegenwoordigt een waarde voor onze gemeente. Daarom is bescherming van de informatie noodzakelijk. Informatiebeveiliging omvat alle maatregelen die ervoor zorgen dat:

- informatie beschikbaar is;
- informatie juist is;
- vertrouwelijke informatie niet in verkeerde handen valt.

Informatiebeveiliging draait zeker niet alleen om technische maatregelen. Het gedrag van iedereen die met informatie omgaat, is het belangrijkste onderdeel.
Binnen de gemeente gelden de volgende informatiebeveiligingsregels:

1. Houd u altijd aan de wet en de gedragscode.
2. Behandel informatie met zorg.
3. Draag zorg voor toegangsbeveiliging en mobiele apparatuur.
4. Houd uw wachtwoorden en pincodes geheim.
5. Weet met wie u handelt.
6. Ga zorgvuldig om met internet, e-mail en social media.
7. Meld incidenten zoals virussen, diefstal en verlies.

Houd u altijd aan de wet en de gedragscode

- Houd u aan de gedragscode.
- Respecteer de (privacy)wet- en regelgeving die voor uw werk van toepassing is.
- Houd u aan de afspraken over informatieuitwisseling.
- Spreek collega's aan op het niet naleven van de regels.

Behandel informatie met zorg

- Berg informatie op bij het verlaten van de werkplek. Vertrouwelijke informatie hoort achter slot en grendel (clean desk).
- Breng geen vertrouwelijke informatie naar buiten.
- Behandel gegevens waarvoor geheimhoudingsplicht geldt, als geheim.
- Verwijder documenten onmiddellijk van printers, kopieerapparaten en faxen.
- Voer vertrouwelijke documenten af in de daarvoor bestemde afgesloten afvalcontainers of de papiervernietiger.

Draag zorg voor toegangsbeveiliging en mobiele apparatuur

- Leen uw toegangstoken niet uit! Dit is een strikt persoonlijke toegangssleutel.
- Laat onbevoegden niet meelopen bij het naar binnen gaan.
- Meld bezoekers vooraf aan en begeleid ze bij het komen en gaan.
- Laat mobiele apparatuur niet onbeheerd achter.

Houd uw wachtwoorden en codes geheim

- Gebruik moeilijk te raden wachtwoorden en codes en verander ze regelmatig.
- Deel wachtwoorden en codes niet met anderen.
- Vergrendel uw computer bij het verlaten van uw werkplek.

Weet met wie u handelt

- Wees u ervan bewust dat iemand kan meekijken naar documenten (ook op beeldscherm) of kan meeluisteren bij (telefoon)gesprekken.
- Weet met wie u communiceert via telefoon, fax, internet of e-mail.
- Gebruik uw professionele oordeel wanneer u informatie krijgt: niet alles is waar.
- Geef bij verstrekking van informatie aan waarom en door wie deze gebruikt mag worden.

Ga zorgvuldig om met internet en e-mail op het werk

- Gebruik internet en e-mail hoofdzakelijk voor uw werk.
- Open geen e-mail van onduidelijke afzenders en wees zorgvuldig wanneer u informatie (bijlagen) downloadt.
- Verstuur vertrouwelijke informatie via e-mail alleen met beveiligde mail. Bedenk vooraf of verzenden van deze vertrouwelijke informatie echt noodzakelijk is.
- Benader, download, bewaar of verzend geen illegale of aanstootgevende gegevens.

Als u buiten het gemeentehuis werkt gelden onderstaande aanvullende regels

- Volg altijd de regels die zijn vastgelegd in het beleid met betrekking tot mobiel werken van de gemeente ten aanzien van:
    - de op het mobiele apparaat van toepassing zijnde beveiligingseisen;
    - het actueel houden van de virusscan en eventuele andere beveiligingssoftware die op het mobiele apparaat is aangebracht.
- Open vertrouwelijke informatie niet via webmail.

Via webmail is het mogelijk om, overal waar een internetverbinding is, uw e-mail te bekijken. Het is ook mogelijk om bijlages te openen die in de mail staan. Doe dit echter niet met vertrouwelijke informatie. Op het moment dat een document uit de mail wordt geopend, wordt het opgeslagen in een tijdelijke map op de pc. Daar blijft het ook staan na het afsluiten van het document. Wanneer uw thuis-pc niet goed genoeg beschermd is, zal een hacker dus toegang kunnen krijgen tot deze informatie. En wanneer u het document bijvoorbeeld in een internetcafé hebt geopend, zal een gebruiker na u het document kunnen vinden en gebruiken.

- Het is niet toegestaan gemeentelijke informatie op te slaan op de harde schijf van uw laptop.
- Het is niet toegestaan vertrouwelijke gemeentelijke informatie op te slaan op een USB-stick. Deze kan kwijtraken en virussen bevatten.
- Als u voor de gemeente werkt, logt u altijd in via de VDI-omgeving zodat u veilig werkt.
- Vermijd het gebruik van USB-ticks. Deze kunnen kwijtraken en makkelijk virussen bevatten.
- Het is niet toegestaan om (standaard) zakelijke mail door te sturen naar een niet-gemeentelijk account.
- Het is niet toegestaan om gemeentelijke informatie op te slaan in de cloud (zoals Dropbox, OneDrive, Google Drive, et cetera.)

INFORMATIE
BEVEILIGINGS
DIENST

Meld incidenten zoals virussen, verlies, diefstal en datalekken

- Meld verdachte activiteiten op uw pc of verlies of diefstal ervan onmiddellijk bij de servicedesk en uw leidinggevende.
- Meld (vermoedelijke) datalekken bij de servicedesk en/of uw CISO.

INFORMATIE
BEVEILIGINGS
DIENST

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie