BMC
YACHT GROUP

Bewustwording:

De essentie voor veilige informatie

Partners in verbetering

Beleid, procedures, audits en regelgeving zijn niet genoeg om de informatieveiligheid op het gewenste niveau te brengen en te houden. De mens is de cruciale factor: het menselijk handelen is de essentiële schakel in de werkprocessen waarin informatieveiligheid in het geding kan komen.

Bewustwording is geboden, voor medewerkers, management en bestuur, dus in alle lagen van de organisatie. Het is van groot belang dat zij zich bewust zijn van de risico's die zijzelf, hun organisatie, en de inwoners voortdurend lopen.

BMC helpt u ervoor te zorgen dat medewerkers, management en bestuur zich bewust worden van deze risico's, door middel van een planmatige aanpak en praktische tips.

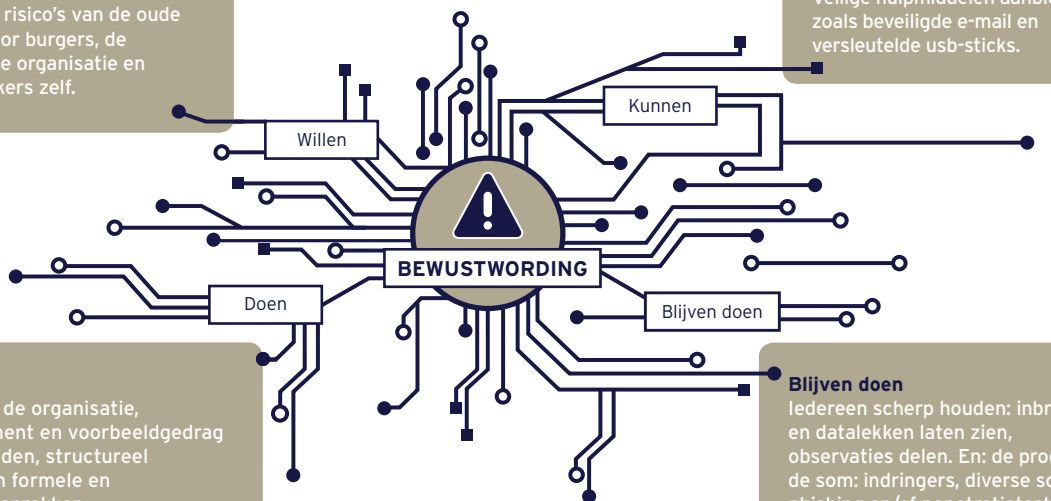
BMC maakt uw medewerkers niet alleen bewust van de risico's op het gebied van informatie-veiligheid, maar kan ook helpen de praktische vertaalslag te maken naar processen en werk-wijzen binnen specifieke vakgebieden. BMC is immers het bureau voor ondersteuning van gemeenten en heeft de expertise in huis op alle terreinen waar de gemeentelijke organisatie werkzaam is. Door deze meerwaarde leert uw organisatie er in de breedte voor te zorgen dat gegevens bij haar in veilige handen zijn.

BMC biedt u het programma **Bewust van veilige informatie** aan met thema's die het risicobewust-zijn rondom informatieveiligheid bevorderen. Samen met u richten wij een continu proces in van 'leren en doen' en we zorgen dat dit geborgd is in het dagelijks handelen. **Bewust van Veilige Informatie** is praktisch en maakt de vertaalslag naar uw dagelijkse realiteit. Uw medewerkers, managers of bestuurders worden begeleid om in hun rol en op hun werkterrein op juiste wijze met informatie om te gaan.

Wij ondersteunen u bij het creëren van een inclusieve cultuur, waar iedereen meedoet en waar men elkaar kan aanspreken op houding en gedrag. In deze cultuur is het nuttig en leerzaam om eventuele incidenten of ongewenste werk-wijzen aan de orde te stellen, zonder dat dit negatieve spanningen veroorzaakt.

Willen
Belichten van het 'waarom': de mogelijke risico's van de oude werkwijze voor burgers, de gemeentelijke organisatie en de medewerkers zelf.

Kunnen
De medewerkers in staat stellen om zich verantwoordelijk te gedragen. Risico's kennen en kunnen vermijden, omgaan met hindernissen en dilemma's. Veilige hulpmiddelen aanbieden, zoals beveiligde e-mail en versleutelde usb-sticks.



Doen
Inbedding in de organisatie, via commitment en voorbeeldgedrag leidinggevenden, structureel onderwerp in formele en informele gesprekken.

Blijven doen
Iedereen scherp houden: inbreuken en datalekken laten zien, observaties delen. En: de proef op de som: indringers, diverse soorten phishing en/of penetratietests.

Het proces van Bewustwording Informatieveiligheid kan gaande worden gehouden door:

- workshops informatieveiligheid en privacy
- trainingen veilig handelen met wachtwoorden;
- trainingen bevordering van de meldcultuur bij incidenten;
- onderzoek naar de zorg om persoonsgegevens in werkprocessen;
- trainingen clean desk en clean screen beleid (opstellen, implementeren en toetsen);
- onderzoek naar de veiligheid van het gebouw ter bescherming van informatie.

Ongeacht hun kennisniveau kunnen alle medewerkers en bestuurders aan dit programma deelnemen. In het programma **Bewust van veilige informatie** zorgen wij ervoor dat houding en gedrag van de medewerkers meetbaar zijn. De effecten van het programma worden daarmee zichtbaar voor de hele organisatie.

Als management en bestuur krijgt u inzicht in knelpunten en risico's in de houding en het gedrag van de medewerkers.

Risicobewustzijn meten

De mate waarin mensen zich bewust zijn van risico's voor de informatieveiligheid valt te meten.

Het bewustzijnsniveau wordt op alle niveaus gemeten via onder andere:

- online kennistoets
- GAP-analyse bewustwording
- interviews
- phishing test (via email en telefoon)
- mysteryguest

Activiteitenplan

De analyse toont voor elke afdeling in een oogopslag de knelpunten en risico's. Met deze inzichten formuleren we een activiteitenplan, dat volledig is toegespitst op de risico's en het beveiligingsbewustzijn van uw organisatie. Dit actieplan kunnen wij in overleg met u implementeren.

Via dit activiteitenplan leren alle medewerkers het juiste gedrag aan jegens informatieveiligheid. De adviseurs van BMC kunnen u helpen bij de praktische implementatie van de aangescherpte werkwijze. Zij helpen u, met hun veelzijdige expertise, de eventuele knelpunten per vakgebied of afdeling op te lossen.

Voorbeelden van activiteiten:

- workshops
- cursus ethical hacking
- games (online, offline)
- bevordering i-bewustzijn, met gebruikmaking van overheidstools
- posters, flyers
- afdelingsoverleggen

De medewerker die zich bewust is van zijn verantwoordelijkheid:

✓ vergrendelt zijn/haar beeldscherm
✓ spreekt de collega aan die zijn beeldscherm niet vergrendelt
✓ deelt individuele wachtwoorden en accounts niet met anderen
✓ verstrekt geen vertrouwelijke (persoons) gegevens via email of telefoon
✓ behandelt dossiers van medewerkers en burgers vertrouwelijk
✓ herkent aanvallen zoals phishing, spam en hacks

Elke leidinggevende geeft het goede voorbeeld!

Uw resultaat voor de hele organisatie

Met behulp van het programma **Bewust van Veilige Informatie** ontstaat een sterke samenhang tussen alle geledingen: van B&W tot het MT en de vakafdelingen. Praktische problemen rond informatieveiligheid worden opgelost. Iedere medewerker gaat op de juiste manier om met informatieveiligheid en privacy en is tegelijkertijd ambassadeur voor de informatieveilige organisatie. Het is van groot belang om het bewust omgaan met de veiligheid van informatie voortdurend te stimuleren, te sturen en te meten. Communicatie over informatieveiligheid, in allerlei vormen en in alle geledingen en vakgebieden, verdient blijvende aandacht.

De bijdrage van BMC

De adviseurs van BMC hebben een brede kennis van en ervaring in overheidsorganisaties. Zij weten vanuit alle vakgebieden, zoals ICT, het sociaal domein, of HRM de verbinding te leggen met informatieveiligheid en privacy. Zij staan naast de medewerkers vanuit hun ervaring met het dagelijks werk binnen de gemeente. Altijd pragmatisch en resultaatgericht.

Meer informatie en contact

Voor meer informatie over het programma **Bewust van Veilige Informatie** of om een vrijblijvende afspraak te maken kunt u contact opnemen met:

Harm Timmerman
adviseur
06 - 10 38 42 79
harm.timmerman@bmc.nl

Lisanne van Boekel
accountmanager
06 - 12 97 26 14
lisanne.van.boekel@bmc.nl

Kijk voor meer informatie ook eens op onze website **www.bmc.nl**

Kostenoverzicht

Risicobewustzijn meten

Cursussen, audits en regelgeving alleen zijn niet genoeg om de informatieveiligheid op het gewenste niveau te brengen en te houden. De mens is de cruciale factor: het menselijk handelen is de zwakste schakel in de werkprocessen waarbij informatieveiligheid in het geding kan komen.

Bewustwording is geboden in alle lagen van de organisatie, voor medewerkers, management en bestuur. Het is van groot belang dat zij zich bewust zijn van de risico's die zij zelf, hun organisatie, en de inwoners voortdurend lopen. BMC helpt u ervoor te zorgen dat medewerkers, management en bestuur zich bewust worden van deze risico's, door middel van een planmatige aanpak en praktische tips.

BMC biedt diverse activiteiten aan om bewustwording binnen uw organisatie tot een hoger niveau te krijgen en dit niveau te borgen (PDCA-cyclus). Hieronder worden deze activiteiten weergegeven met een korte toelichting en een prijsindicatie.

Activiteit	Omschrijving	Kostenindicatie
Plan (nul-meting)		
Kennistoets (game)	Met een kennistoets wordt vastgesteld wat medewerkers al weten over informatieveiligheid en risico's met betrekking tot het werken met informatie. De kennistoets wordt vormgegeven als een online spel.	In overleg, afhankelijk van wensen
Phishingtest	Er wordt een fictieve phishingmail in de organisatie verspreid. Gemeten wordt hoeveel medewerkers in de fout gaan en welke informatie wordt prijsgegeven.	251 – 500 medewerkers: € 2.750,- 501 – 750 medewerkers: € 3.250,-
Mystery guest	Een mystery guest brengt een bezoek aan het gemeentehuis en onderzoekt of en hoe ver deze onbevoegd het gebouw kan binnenkomen. Daarbij wordt tevens de naleving van clean desk clear screen getoetst.	€ 2.195,-
Mystery caller	Een mystery caller probeert op verschillende manieren onbevoegd informatie te vergaren via de telefoon.	€ 1.395,-
Interviews	Met diverse medewerkers uit verschillende lagen van de organisatie worden gesprekken gevoerd over informatieveiligheid. Hierbij komt aan bod wat zij mis zien gaan op de werkvloer ten aanzien van informatieveiligheid.	€ 1.600,-
Communicatieplan	Er wordt een communicatieplan opgesteld met de doelstellingen ten aanzien van bewustwording en met een beschrijving en planning voor de uit te voeren activiteiten.	€ 3.500,-

Do		
Workshops	Voor het college, de gemeenteraad en het MT worden workshops georganiseerd over informatieveiligheid en de verantwoordelijkheden die de betrokkenen hieromtrent hebben. Doordat BMC-adviseurs binnen alle vakgebieden en lagen van overheidsinstanties werkzaam zijn, beschikken zij over brede kennis van gemeentelijke organisaties. Workshops worden dan ook sterk toegespitst op de dagelijkse praktijk van de doelgroep.	€ 1.600,- (3 workshops)
Train de trainer	Een selectie medewerkers wordt getraind in het ambassadeur zijn voor informatieveiligheid en in het zelf organiseren en uitvoeren van bewustwordingsactiviteiten. Verdeeld over het jaar worden 4 trainingssessies georganiseerd.	€ 1.000,- (voor de eerste sessie) Daarna € 500,- per dagdeel
Werkoverleggen	Er wordt aangesloten bij werkoverleggen van de afdelingen. Hierbij wordt op interactieve wijze informatieveiligheid besproken met een sterke link naar de werkzaamheden op de desbetreffende afdeling. Doordat BMC-adviseurs binnen alle vakgebieden en lagen van overheidsinstanties werkzaam zijn, beschikken zij over brede kennis van gemeentelijke organisaties. Workshops worden dan ook sterk toegespitst op de dagelijkse praktijk van de doelgroep.	€ 1.600,- voor de eerste 5 werkoverleggen, daarna € 500,- per extra werkoverleg
Berichtgeving	Op intranet maar ook door middel van flyers en posters wordt aandacht besteed aan informatieveiligheid op de werkvloer. Centraal staan de 10 gouden regels voor informatieveiligheid. 1 keer per maand wordt berichtgeving verzorgd.	€ 1.800,-
Datalekkenspel	Er wordt een spel rond het thema datalekken georganiseerd voor medewerkers. Op een ludieke wijze wordt men bekend met het fenomeen datalek en leert men hoe hiermee om te gaan. Een spel duurt ongeveer een dagdeel inclusief voorbereiding).	€ 800,- (per spel/dagdeel)
Check		
Kennistoets (game)	Met een kennistoets wordt opnieuw gemeten hoe het is gesteld met de kennis van medewerkers. De kennistoets wordt vormgegeven als een online spel. Het resultaat wordt vergeleken met de kennistoets in de beginfase.	In overleg, afhankelijk van wensen.
Phishingtest	Er wordt opnieuw een fictieve phishingmail in de organisatie verspreid. Gemeten wordt hoeveel medewerkers in de fout gaan en welke informatie wordt prijsgegeven. Het resultaat wordt vergeleken met het resultaat uit fase 1.	251 – 500 medewerkers: € 2.750,- 501 – 750 medewerkers: € 3.250,-
Mystery guest	Een mystery guest brengt opnieuw een bezoek aan het gemeentehuis en onderzoekt of en hoe ver deze onbevoegd het gebouw kan binnenkomen. Daarbij wordt tevens de naleving van clean desk clear screen getoetst. Het resultaat wordt vergeleken met het resultaat uit fase 1.	€ 2.195,-
Mystery caller	Een mystery caller probeert opnieuw op verschillende manieren onbevoegd informatie te vergaren via de telefoon. Het resultaat wordt vergeleken met het resultaat uit fase 1.	€ 1.395,-
Act		
Vervolgacties definiëren	Op basis van de resultaten uit de “check”-fase wordt bepaald welke vervolgactiviteiten wenselijk zijn om in een volgende campagne uit te voeren. Dit resulteert in een bondig en concreet advies.	