Buyers guide

Awareness, gedrag en organisatiecultuur

CYBERVEILIG NEDERLAND

Inhoudsopgave

Introductie

Bij het verhogen van de cyberweerbaarheid van organisaties speelt de menselijke factor een belangrijke rol. Medewerkers van een organisatie werken dagelijks met digitale systemen en voeren daarbij handelingen uit die van invloed zijn op de veiligheid van uw organisatie. Het is daarom verstandig om een organisatiecultuur te ontwikkelen waarin deze veiligheid als vanzelfsprekend wordt gewaarborgd.

Voor het ontwikkelen van een cyberveilige cultuur is het goed om te werken aan twee aspecten:

- Het verhogen van awareness en kennis
- Het ontwikkelen van cyberveilig gedrag

U kunt verschillende maatregelen treffen om aan deze aspecten te werken. Ook is het mogelijk om een cybersecuritydienstverlener om ondersteuning te vragen. Het is belangrijk dat u maatregelen en diensten kiest die goed aansluiten bij uw organisatie en organisatiecultuur. Sommige maatregelen en diensten zijn effectiever dan andere. Dit hangt onder meer samen met de volwassenheid van uw organisatie op gebied van een cyberveilige cultuur. Ook moeten de maatregelen en diensten goed passen bij uw organisatiecultuur. Alleen dan zullen medewerkers makkelijker een doorvertaling maken naar hun eigen werkzaamheden en eerder geneigd zijn zich cyberveilig te gedragen. Als de aansluiting op uw cultuur goed is gemaakt, zullen medewerkers maatregelen minder snel zien als een verplichting waaraan moet worden voldaan, maar zorgen ze daadwerkelijk voor een vertaling naar gewenst cyberveilig gedrag en een positieve ontwikkeling van de organisatiecultuur. Dit is overigens vaak een groeiproces dat stap voor stap wordt doorlopen.
Dit document heeft als doel om u inzicht te geven in de aspecten die een rol spelen bij het ontwikkelen van een cyberveilige organisatiecultuur en de diensten die daarvoor in de markt beschikbaar zijn. Met deze informatie hopen we dat u een specifiekere uitvraag kunt doen in de markt als u behoefte heeft aan ondersteuning op dit gebied. Dit document geeft definities van de verschillende diensten en laat zien wat de huidige mogelijkheden zijn op dit gebied. Op deze manier kunt u scherper kiezen wat bij u past, maar u kunt met deze informatie bijvoorbeeld ook offertes eenvoudiger met elkaar vergelijken. Dit document zien wij als een aanvulling op het eerder gepubliceerde Cybersecurity Woordenboek (zie https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/) waarvan de definities als uitgangspunt zijn gebruikt.

We hebben deze buyers guide awareness, gedrag en organisatiecultuur primair geschreven voor securityverantwoordelijken zoals CISO's, maar bijvoorbeeld ook IT-managers, voor verantwoordelijken voor Learning & Development, zoals HR- en communicatieverantwoordelijken en voor inkopers van securityproducten en -diensten. Voor andere doelgroepen is dit document vanzelfsprekend eveneens bruikbaar. De keuze voor onderwerpen hebben we echter vanuit de primaire doelgroep gemaakt.

Het bereiken van een cyberveilige organisatiecultuur

Er is vanuit de psychologie veel onderzoek gedaan naar het verhogen van awareness en kennis, het beïnvloeden van gedrag en het ontwikkelen van een organisatiecultuur op gebied van veiligheid. Daarbij zijn modellen en theorieën ontstaan die helpen om te begrijpen waar je in een organisatie interventies kunt doen om de cultuur van een organisatie positief te beïnvloeden.

In al deze modellen en theorieën zien we gedragsaspecten terug die je wilt beïnvloeden, zoals beseffen en inzien, weten, willen, kunnen, doen en blijven doen of volhouden. De modellen en theorieën geven richting aan de samenhang en ook de volgorde van hoe je deze gedragsaspecten beïnvloedt. Die volgorde is namelijk van belang. Zo zijn sommige elementen een randvoorwaarde voordat mensen overgaan op ander gedrag.

Als een organisatie bijvoorbeeld graag wil dat de medewerkers vertrouwelijke documenten na gebruik vernietigen in een papierversnipperaar, dan is het van belang dat de medewerker...

- weet dat dit van hem wordt gevraagd (beseffen)
- begrijpt hoe de papierversnipperaar werkt (kennis)
- gefaciliteerd wordt door dat er een papierversnipperaar in de buurt staat van de werkplek (kunnen, gelegenheid)
- er tijd voor wil maken om papier te versnipperen (willen, motivatie)

Zodra medewerkers kennis en bewustzijn hebben over wat er van hen wordt gevraagd is het van belang om inzicht te krijgen in waarom bepaald gewenst gedrag (nog) niet optreedt. Vervolgens kunnen dan interventies worden uitgewerkt die in een bepaalde organisatorische context het gewenste gedrag laten ontstaan én onderdeel laten worden van de organisatiecultuur, zodat de gedragingen ook langdurig blijven bestaan.
Dit alles vat zich samen in de volgende vier stappen voor awareness, gedrag en organisatiecultuur:

- Bewustwording en kennisontwikkeling
- Inzicht in oorzaak van het ontbreken van gewenst gedrag
- Het doen van passende interventies voor gewenst gedrag
- Het bestendigen van het gewenste gedrag in de organisatiecultuur

Voorbeelden van deze modellen en theorieën zijn (zie bijlage voor details):

- Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)
- Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads (MacInnis, D. J., Moorman, C., & Jaworski, B. J., Journal of Marketing, 55, 32-53, 1991)
- Attitudes, personality, and behavior (Ajzen, I., 2nd Ed., Milton-Keynes, England: Open University Press, McGraw-Hill, 2005)
- Persuasive by Design, Behaviour Change Model (R. Renes, S. Hermsen , Draaiboek gedragsverandering, 2017)
- Self-Determination Theory (Deci & Ryan, 1985; 2000)
- Transtheoretisch model (Prochaska & Di Clemente, 1982)
- Het CASI-model (zie https://www.communicatierijk.nl/vakkennis/casi/documenten/publicaties/2019/03/08/handleiding-casi, 2020)

Volwassenheid op gebied van organisatiecultuur ontwikkeling

Voor wat betreft het ontwikkelen van een organisatiecultuur waarin veiligheid een vanzelfsprekend onderdeel vormt, is de mate van volwassenheid van een organisatie een belangrijk aspect. Deze volwassenheid blijkt uit de brede aanpak die een organisatie op gebied van cybersecurity heeft, waarin meerdere onderdelen een rol spelen zoals bijvoorbeeld risicomanagement, beleid, verantwoordelijkheid, technologie, compliance en gedrag.

Veel organisaties besteden in eerste instantie meestal aandacht aan het veilig maken van technologie en het inrichten van de bijbehorende processen, maar richten zich nog minder op de medewerkers. Het is echter van belang om over de hele linie (techniek, organisatie en mens) te groeien in volwassenheid op gebied van cybersecurity. De stappen zoals beschreven in de vorige paragraaf (bewustwording en kennisontwikkeling, inzicht in oorzaken van ontbreken van gedrag, maatregelen gericht op gedragsverandering, bestendigen in de organisatiecultuur) kunnen hierbij als leidraad dienen voor de achtereenvolgens te nemen stappen.

Om gedragsverandering gestructureerd aan te pakken is het ook mogelijk om een volwassenheidsmodel te hanteren om stap voor stap naar een hogere volwassenheid te groeien. Veel leveranciers gebruiken momenteel een door henzelf ontwikkeld volwassenheidsmodel dat hierin ondersteunend kan zijn. Vaak zijn deze modellen ontwikkeld op basis van een al bestaand volwassenheidsmodel.

De meeste van deze modellen hebben 5 niveaus van volwassenheid die zich als volgt laten beschrijven:

- **Ad hoc.** Er worden op ad hoc-basis activiteiten ontplooid op gebied van awareness. Dit is vaak zeer beperkt en incident-gedreven.
- **Vastgelegd.** Er zijn diverse activiteiten op gebied van awareness, voornamelijk gedreven door compliance overwegingen (bijvoorbeeld vanuit een implementatie van de ISO 27001 standaard).
- **Herhaalbaar.** Er is sprake van een plan met heldere doelstellingen, gekoppeld aan de cyberrisico's van een organisatie, en er wordt structureel aandacht besteed aan awareness en kennisontwikkeling, met soms al enkele stappen gericht op gedragsverandering.
- **Gemanaged.** Er is inzicht in het gewenste gedrag in relatie tot de cyberrisico's die een organisatie loopt. Er wordt op basis van dit inzicht gestuurd op interventies die het gedrag veranderen.
- **Geoptimaliseerd.** Op dit niveau is het gelukt om een veiligheidscultuur te creëren waarin cyberveilig gedrag vanzelfsprekend is en medewerkers elkaar aanspreken op het (ontbreken van) gewenste gedrag.

In onderstaande tabel is de relatie tussen de bovenstaande volwassenheidsniveaus en de 4 stappen voor awareness, gedrag en organisatiecultuur en inzichtelijk gemaakt. Met andere woorden, ieder volwassenheidsniveau vraagt om andere maatregelen op gebied van awareness en gedrag.

VOLWASSENHEIDSNIVEAUS	4 STAPPEN VOOR AWARENESS, GEDRAG EN ORGANISATIECULTUUR
1. AD HOC	1. Bewustwording en kennisontwikkeling
2. VASTGELEGD	1. Bewustwording en kennisontwikkeling
3. HERHAALBAAR	1. Bewustwording en kennisontwikkeling 2. Inzicht in oorzaak van ontbreken van gewenst gedrag
4. GEMANAGED	2. Inzicht in oorzaak van ontbreken van gewenst gedrag 3. Het doen van passende interventies voor gewenst gedrag
5. GEOPTIMALISEERD	4. Het bestendigen van het gewenste gedrag in de organisatiecultuur

Tabel 1 Relatie tussen volwassenheidsniveaus en stappen voor awareness, gedrag en organisatiecultuur

Het toepassen van een volwassenheidsmodel kan een organisatie helpen om te bepalen wat de huidige situatie is. Hiervoor wordt vaak een (nul)meting uitgevoerd. Vervolgens kan een organisatie op basis van risico inschattingen enerzijds en beschikbaar budget anderzijds bepalen wat het gewenste niveau is en op welke termijn dit niveau bereikt zou moeten worden. Dat bepaalt uiteindelijk welke maatregelen er achtereenvolgens genomen worden.

Het gebruik van een volwassenheidsmodel kan voor een CISO ondersteunend zijn om de benodigde maatregelen op gebied van awareness en gedrag in de juiste context te plaatsen en gestructureerd aan te pakken. Deze context kan ook helpen bij het motiveren van de benodigde investeringen richting de budgethouder binnen de organisatie.

Op basis van de keuzes op gebied van volwassenheid kan voor een overzichtelijke periode een programma worden samengesteld om de awareness-, gedrag- en cultuurontwikkeling ten uitvoer te brengen. De interventies vormen idealiter een continue cyclus waarbij deze afwisselend worden ingezet. Dit heeft ook te maken met de manier waarop mensen leren.

Een programma zou er bijvoorbeeld als volgt uit kunnen zien:

WEEK	ACTIVITEIT
1-2	In kaart brengen van risico's vanuit menselijk gedrag
3	Workshop commitment management In kaart brengen gewenste gedragingen
4	Kick-off campagne cyberveilig gedrag voor alle medewerkers met VR-game
4-6	Awareness e-learning medewerkers
6-8	Gedragsmetingen: • Mailphishing test • Wachtwoordencheck
8-12	Analyse van huidig cyberveilig gedrag in de organisatie
12-37	Interventieprogramma gedrag
CONTINUE	Wekelijkse nieuwsbrief cyberveiligheid

Tabel 2 Fictief voorbeeld van een mogelijk ontwikkelprogramma

Een glossary met diensten voor een cyberveilige organisatiecultuur

In onderstaande paragrafen lichten we toe welke diensten er in de markt beschikbaar zijn in ieder van deze stappen. Dit is geen uitputtend overzicht, maar geeft een beeld van de actuele mogelijkheden die er zijn. De diensten zijn geordend in de volgende categorieën:

- Metingen over cyberveilig gedrag
- Workshops
- Communicatiecampagnes voor personeel
- Trainingen
- Analyses gedrag en cultuur
- Gedragsinterventies
- Cultuurprogramma
- Consultancy

Metingen over cyberveilig gedrag

Nulmeting

Bij een nulmeting wordt het huidige niveau van de organisatie gemeten op een bepaald aspect op gebied van cyberveilig gedrag binnen een organisatie. Het doel van de meting is om een startpunt te bepalen voor een in te zetten verandering op gebied van cyberveilig gedrag zodat na verschillende interventies het effect kan worden bepaald.

Er kan bijvoorbeeld gemeten worden op factoren als:

- **Kennis:** wat weten medewerkers al over cyberveilig gedrag?
- **De houding van medewerkers:** vinden zij veilig werken belangrijk?
- **De subjectieve norm:** wat denkt een medewerker wat er van hem of haar verwacht wordt?
- **De ingeschatte beheersing:** vinden je medewerkers dat ze voldoende kennis en hulpmiddelen hebben om cyberveilig te werken?
- Etc.

Effectmetingen

Idealiter wordt een meting jaarlijks herhaald zodat de organisatie inzicht krijgt in de groei en ontwikkeling van de volwassenheid op het gebied van awareness en gedrag. Een nulmeting kan gerichter plaatsvinden als de organisatie ook inzicht heeft in dreiging, risico's en maatregelen die zij willen/moeten nemen ten aanzien van cyberveilig gedrag.

Management dashboards

Omdat programma's gericht op gedragsverandering vaak langere tijd in beslag nemen is het verstandig om het management regelmatig te informeren over de voortgang van het programma. Op basis van de nulmeting en de gestelde doelen kan een management dashboard worden ingericht waarmee de voortgang overzichtelijk wordt weergegeven.

Workshops

Workshop management inzicht in problematiek en commitment. Om het management mee te krijgen in de beweging naar meer cyberveilig gedrag is het belangrijk dat ze ook het waarom achter het wenselijke gedrag begrijpen. Door in een workshop aandacht te besteden aan de grootste dreigingen, risico's en gewenste cyberveilige gedragingen in de context van hun eigen organisatie wordt de sense of urgency verhoogd en draagvlak gecreëerd ten aanzien van de noodzakelijke maatregelen.

Management commitment is een belangrijke voorwaarde voor een succesvol ontwikkelprogramma op gebied van bewustzijn en gedrag. Een workshop voor het management wordt daarom vaak aan het begin van een programma ingezet om voldoende draagvlak voor de veranderingen te bewerkstelligen.

Een management commitment sessie kan diverse doelen dienen:

- Inzicht in de problematiek bieden
- Nut en noodzaak van management commitment bespreken
- Nut en noodzaak van security awareness aantonen, vastleggen en laten uitspreken
- Rollen en verantwoordelijkheden van management vastleggen en laten uitspreken
- Invloed van voorbeeldfunctie bespreken
- Taken bespreken

Tabletop workshop

Een tabletop workshop is gericht op een fictieve simulatie waarmee de capaciteiten van de organisatie op het gebied van cybersecurity worden getest. In de meeste gevallen wordt de aandacht gericht op incident response en crisismanagement.
Een organisatie wordt tijdens zo'n workshop geconfronteerd met een (soms op maat gemaakt), fictief scenario van een cyberaanval. Op deze manier wordt getest in hoeverre de organisatie effectief weerstand kan bieden tegen een cyberaanval. Er ligt een nadruk op het testen van (bestaande) procedures op het gebied van crisismanagement en incident response. Afhankelijk van de doelgroep is het ook mogelijk om de dilemma's af te stemmen op de eigenschappen van deze doelgroep.

Mogelijke dilemma's & leerdoelen die aan de orde komen zijn:

- Of deelnemers voldoende procedures hebben opgesteld om de continuïteit van de operaties van de organisatie zo veel mogelijk te waarborgen tijdens het voordoen van een cybercrisis.
- Of deelnemers zich tijdens het voordoen van een cybercrisis ook houden aan de voorgeschreven procedures om de continuïteit van de organisatie te waarborgen.
- Of deelnemers zich houden aan hun zorg- en meldplicht richting bijvoorbeeld het NCSC, het ministerie van Justitie & Veiligheid, en de verantwoordelijke toezichthouders binnen de sector van de getroffen organisatie.
- Of deelnemers interne communicatie naar medewerkers tijdens een cybercrisis voldoende op orde hebben.
- Of deelnemers communicatie met partners binnen de sector tijdens een cybercrisis voldoende op orde hebben. Denk hierbij aan partners binnen de sector waarmee wordt samengewerkt op het gebied van productie en levering en andere organisaties binnen de sector die eventueel door een cyberaanval kunnen worden getroffen.
- Of deelnemers externe communicatie tijdens een cybercrisis voldoende op orde hebben. Denk hierbij aan: journalisten, politici, bestuurders, klanten, burgers en bedrijven.

Communicatiecampagnes voor personeel

Awareness campagnes

Er zijn vele vormen van awareness campagnes denkbaar waarmee een organisatie de aandacht kan vestigen op het belang van cyberveilig gedrag.

Voorbeelden zijn:
Nieuwsbrieven. De kracht van communiceren zit in diversiteit en herhaling. Een nieuwsbrief besteedt aandacht aan actuele security onderwerpen en kan bijvoorbeeld positieve voorbeelden vanuit de organisatie belichten.
Blogs/vlogs. Om een ontwikkelprogramma goed te laten werken, moet deze aansluiten op de cultuur van de organisatie. Daarbij kunnen ook blogs en vlogs worden ingezet. In blogs kunnen ambassadeurs vanuit een organisatie aan het woord komen en in vlogs kunnen op een eigentijdse manier relevante security onderwerpen onder de aandacht worden gebracht.
Posters, stickers en andere zichtbare verwijzingen. Het is belangrijk dat medewerkers het gewenste gedrag ontwikkelen en daarna blijven doen. Daarvoor kunnen kleine reminders en aansporingen ondersteunend zijn (nudging). Alleen als het nieuwe gedrag vaak en zonder na te denken wordt uitgevoerd, wordt het een automatisme. Prikkelende posters, stickers en andere zichtbare verwijzingen kunnen hierbij ondersteunend zijn.

Algemene presentaties door security experts

Leren over bepaalde onderwerpen die relevant zijn voor een specifieke doelgroep kan goed in de vorm van een algemene presentatie door een security expert. Daarin kan de aandacht worden gericht op onderwerpen zoals het belang van informatiebeveiliging of recente beveiligingslessen op basis van marktonderzoek of bedreigingen voor een bepaalde afdeling (bijv. financiën of HR), of praktische lessen voor veiliger werken (bijv. over wachtwoorden).

Ook is het mogelijk om middels een live hackdemo te laten zien hoe bijvoorbeeld wachtwoorden gekraakt worden met behulp van bepaalde aanval strategieën of hoe kan worden binnengedrongen in de IT systemen van een organisatie. Het is belangrijk om de presentatie goed af te stemmen op het niveau van de doelgroep.

Een publiek zonder technische kennis heeft meer baat bij een presentatie in begrijpelijke taal met voorbeelden die aansluiten bij de eigen werkomgeving, terwijl IT-experts juist gebaat kunnen zijn bij een technische presentatie over de eerste incident response stappen bij een ransomware aanval.

Challenges/funactiviteiten

Om voor een breed publiek awareness campagnes aantrekkelijker te maken wordt steeds vaker een funfactor ingebouwd. Het leren wordt dan gecombineerd met een leuke ervaring om zo op een positieve manier het gewenste gedrag aan te leren. Voorbeelden van dit soort activiteiten zijn:

VR game. In een virtuele wereld worden de spelers van de game blootgesteld aan allerlei spannende uitdagingen en moeten ze daarin verstandige keuzes maken.
Escaperoom. Spelers moeten zien te ontsnappen uit een benarde situatie, bijvoorbeeld door proberen te voorkomen dat een fictieve cyberaanval op hen wordt uitgevoerd.
(Pub)quiz. In een borrelsetting wordt in teams gestreden om de meeste punten met betrekking tot kennisvragen over digitale veiligheid.
Phishing battle. Teams van medewerkers mogen in de huid van een aanvaller kruipen en zelf phishing acties initiëren richting de andere teams om daarmee zoveel mogelijk punten te verzamelen. Op deze manier krijgen de deelnemers meer inzicht in de aanpak van een aanvaller én in gewenst gedrag om phishing tegen te gaan.

Vaak gaan dit soort activiteiten gepaard met een nabespreking waarin de geleerde lessen worden samengevat.

Trainingen

Digitale trainingen

Er zijn verschillende digitale trainingen denkbaar om het kennisniveau van medewerkers op gebied van cyberveiligheid te verhogen. Veel aanbieders hebben een grote digitale bibliotheek beschikbaar met digitale trainingen.

Bij de keuze van een passende digitale training kunt u rekening houden met diverse elementen:

Taal. Het is van belang dat de beschikbare talen aansluiten op de talen die leidend zijn binnen uw organisatie.
Cultuur. De wijze waarop mensen leren is gerelateerd aan de regio waarin zij zijn opgegroeid, leven en werken. Sommige trainingen zijn primair ontwikkeld vanuit één land of regio. Andere hebben een breder aanbod van content op dit gebied.
Trainingsvorm. Sommige trainingen kennen hun invulling met tekst, andere met infographics en animaties en weer andere met video's waarin acteurs herkenbare werksituaties naspelen. Het is goed om inzicht te krijgen in de aangeboden vormen en hierin te kiezen wat het beste bij uw organisatie past.
Expertise. Elke organisatie die trainingen ontwikkelt, zet daarbij zijn eigen experts in, zoals leerexperts, psychologen en game designers en beschikt over eigen expertise. Het is goed om na te gaan wat de belangrijkste inhoudelijke principes zijn die ten grondslag liggen aan het lesmateriaal en welke (type) experts zijn ingezet bij de ontwikkeling van de digitale trainingen.
Omvang aanbod. De omvang van het aanbod varieert. Het is dus van belang om na te gaan of het beschikbare aanbod op bepaalde onderwerpen voldoende aansluit bij de gewenste leerdoelen van uw organisatie.
Opbouw van het aanbod. Sommige aanbieders hebben alleen één type training beschikbaar (bijvoorbeeld animaties over basisonderwerpen). Andere aanbieders hebben een breed aanbod, variërend van microlearnings en korte introductievideo's tot verdiepingsprogramma's.

Afhankelijk van uw leerdoelen zal een specifieke opbouw van het aanbod gewenst zijn.

Vernieuwing. Het is goed om na te gaan hoe frequent de aangeboden content wordt vernieuwd. Het domein van digitale veiligheid is voortdurend aan verandering onderhevig en het is van belang dat nieuwe inzichten tijdig in de trainingen worden opgenomen. Ook is het belangrijk dat het aanbod blijft passen bij de uitstraling van uw organisatie.

Sectorspecifieke content. Sommige aanbieders hebben content beschikbaar die gericht is op specifieke sectoren.

Live trainingen

Naast digitale trainingen, worden er ook live trainingen gegeven in het kader van awareness en gedrag. Dit zijn trainingen die gegeven worden door trainers, soms op locatie en soms op afstand (via een digitale leeromgeving).

In veel gevallen betreffen dit trainingen waarin maatwerk wordt geleverd. Afhankelijk van de specifieke uitdagingen of risico's die een organisatie heeft, kunnen bepaalde thema's in zo'n trainingen verder worden belicht. De meeste live trainingen worden in groepsverband gegeven en zijn aanvullend op al beschikbare digitale trainingen.

Bijkomend voordeel van live trainingen is dat de interactie binnen de groep tot bruikbare inzichten en/of nieuwe oplossingen voor organisatie kan leiden.

Serious games

Steeds vaker wordt bij het leren gebruik gemaakt van serious games. Dit zijn spellen die als primair doel hebben om te onderwijzen en de leerervaring leuk maken. Zo'n spel kan bijvoorbeeld een bord- of kaartspel zijn, maar ook een digitaal spel. In het spel zijn lessen opgenomen ten aanzien van awareness en veilig gedrag. Afhankelijk van de invulling van het spel worden bepaalde facetten hiervan benadrukt.

Analyses gedrag en cultuur

Social engineering testen

Dit soort testen richten zich op het onderzoeken van het gedrag dat medewerkers vertonen als zij te maken krijgen met een fictieve dreiging. Onderzocht wordt op welke gebieden medewerkers op dit moment kwetsbaar zijn, zodat op basis van de uitkomsten passende maatregelen kunnen worden genomen. Voorbeelden van social engineering testen zijn:

Phishing. Bij een phishing test wordt een medewerker verleid tot het verstrekken van vertrouwelijke gegevens. Dit kan bijvoorbeeld via mail gebeuren, maar ook via de telefoon of chat. Voor phishing testen via de mail hebben veel dienstverleners digitale platformen beschikbaar waarmee uzelf of zij voor u fictieve mails kunnen versturen naar uw medewerkers. In geval van phishing via telefoon of chat wordt er een medewerker van de dienstverlener ingezet die zich voordoet als iemand anders en de medewerkers probeert te overreden om vertrouwelijke gegevens te delen.

- Mystery guests. Bij de inzet van een mystery guest probeert iemand een organisatie binnen te dringen, zonder dat hij daarvoor geautoriseerd is. Het gaat bijvoorbeeld over het ongezien passeren van de beveiliging en het betreden van ruimten die voor gasten niet toegankelijk zouden moeten zijn.
- Red teaming. Bij een red teaming test probeert het red team zo dicht mogelijk bij de 'kroonjuwelen' van een organisatie te komen. Vaak betekent dit een gecombineerde aanpak waarbij enerzijds geprobeerd wordt om fysiek een pand te betreden zonder de juiste autorisaties én om digitaal in te breken in de systemen van de organisatie. Doel is om te laten zien op welke punten de organisatie kwetsbaar is voor een digitale aanval.

- Wachtwoordencheck. Helaas maken veel mensen nog altijd gebruik van makkelijk te 'raden' wachtwoorden. Men realiseert zich vaak niet dat hackers op basis van veel voorkomende patronen wachtwoorden sneller kunnen kraken dan met de inzet van een brute force methode (waarbij alle mogelijke opties voor een wachtwoord worden geprobeerd. Als medewerkers in hun wachtwoord woorden gebruiken die voorkomen in het woordenboek of bijvoorbeeld de bedrijfsnaam en dan bepaalde letters wijzigen in cijfers, is een wachtwoord eenvoudig te kraken. Bij een wachtwoordencheck wordt onderzocht hoeveel wachtwoorden snel te kraken zijn en welke patronen in de wachtwoorden vaak voorkomen, zodat op basis hiervan adviezen kunnen worden gegeven voor het verbeteren van de wachtwoorden die binnen een organisatie worden gebruikt.

Onderzoek doen naar cyberveilige gedragingen in een organisatie

Om het huidige cyberveilige gedrag van medewerkers in een organisatie te meten, zijn er grofweg twee methoden:

- Kwalitatief onderzoek
- Kwantitatief onderzoek

Kwalitatief onderzoek richt zich op beschrijvingen en wordt gebruikt om gedachten en ervaringen van medewerkers te begrijpen. Een voorbeeld van kwalitatief onderzoek is het afnemen van interviews of het opzetten van focusgroepen. Kwalitatief onderzoek is vooral geschikt om verkennend onderzoek te doen en dieper in te gaan op de persoonlijke ervaring van mensen. De interpretatie van kwalitatieve data is echter subjectief en de data kan beïnvloed worden door ongewenste factoren, zoals wie de interviewer is en in hoeverre er wordt doorgevraagd tijdens een interview. Ook is kwalitatieve data vaak beperkt, doordat maar een klein deel van de doelgroep wordt bevraagd. Antwoorden die deze groep geeft, zijn niet per se representatief voor de hele doelgroep. Toch geeft een kwalitatief onderzoek wel een eerste indruk van wat er speelt binnen een doelgroep en kunnen er door de persoonlijke aanpak belangrijke issues naar boven komen die anders wellicht onderbelicht blijven.

Kwantitatief onderzoek richt zich op cijfers en wordt gebruikt om een zo objectief mogelijk beeld te krijgen van een situatie. Een voorbeeld van kwantitatief onderzoek is een vragenlijstonderzoek. Kwantitatief onderzoek is minder gevoelig voor subjectieve interpretatie van data, is makkelijk af te nemen onder een grote doelgroep, en is makkelijk te repliceren wanneer je opnieuw hetzelfde onderwerp in kaart wil brengen. Kwantitatief onderzoek biedt echter beperkt informatie over de ervaring van een individu, en er is specialistische, statistische kennis nodig om kwantitatieve data te analyseren. Wanneer het gaat om factoren die moeilijk te meten zijn, zoals kennis, motivatie

en gedrag, vereist dat bovendien specialistische kennis over psychometrie.
Een combinatie van de twee onderzoeksmethodes, een mixed methods aanpak, combineert de voordelen van beide methodes en heeft daarom vaak de voorkeur.

Bij het opzetten van (kwalitatief en kwantitafief) onderzoek is het verstandig om stil te staan bij de volgende vragen:

- Wat wil je meten? Cyberveilig gedrag bestaat uit verschillende thema's. Sommige aanbieders focussen specifiek op het in kaart brengen van één thema, zoals phishing. Anderen kijken breder naar bijvoorbeeld email gebruik, wachtwoord management en incident rapporteren. Hoe meer thema's er in een onderzoek worden meegenomen, des te breder het beeld is dat ontstaat over het cyberveilige gedrag in een organisatie. Ook is het belangrijk om na te denken over welke gegevens waardevol zijn, bijvoorbeeld over het daadwerkelijke huidige gedrag, het kennisniveau op bepaalde onderwerpen, wat medewerkers belangrijk vinden, etc.

- Wie wil je meten? Wie gaat deelnemen aan het onderzoek? Om een zo compleet mogelijk beeld te krijgen van het gedrag binnen een organisatie, is het verstandig om alle (groepen) medewerkers mee te nemen in het onderzoek. Hoe meer mensen uit een doelgroep deelnemen, des te accurater het beeld is dat het onderzoek geeft.

- Hoe wil je meten? Bij een kwantitatief onderzoek naar cyberveilig gedrag van medewerkers, is objectieve data (zoals het aantal downloads van illegale software) vaak beperkt beschikbaar. In plaats daarvan kunnen er vragenlijstitems worden geformuleerd, zoals stellingen en meerkeuzevragen. Meestal zijn dit zogeheten self-report items: mensen geven zelf aan hoe ze zich gedragen, voelen bij of denken over bepaalde onderwerpen. Wanneer een aanbieder voldoende expertise over psychometrie in huis heeft, zijn self-report items een goed alternatief voor objectieve data.

- Waarom wil je meten? Het is belangrijk om vooraf te bepalen waarvoor de onderzoek data wordt ingezet. Als het als nulmeting wordt gebruikt is het goed om dit vooraf met de aanbieder te bespreken zodat bij de onderzoeksopzet hiermee rekening wordt gehouden. De opzet van het onderzoek bepaalt in grote mate wat de bruikbaarheid van de data na afloop is.

Aanbieders van diensten op dit gebied hebben ervaring met al deze aspecten en kunnen adviseren over een passende insteek en voorbeelden geven van effectieve metingen die ze eerder hebben uitgevoerd.

Gedragsinterventies

Interventieprogramma gedrag op basis van organisatiecontext

Weten wat je zou moeten doen, betekent niet per se dat je dat ook doet. Daarom is het belangrijk om eerst te begrijpen op welke factoren van gedrag je als organisatie kunt sturen. Vanuit de psychologische theorie bestaat gedrag uit drie factoren:

- Capaciteit – heeft iemand voldoende kennis om het gevraagde gedrag te tonen?
- Motivatie – wil iemand het gewenste gedrag vertonen?
- Gelegenheid – is iemand in staat om het gewenste gedrag te vertonen?

Om gedrag te veranderen moeten de interventies die worden ingezet medewerkers activeren op deze drie factoren: door te leren, motiveren of te faciliteren. Belangrijk is dat elke interventie wordt afgestemd op de specifieke behoeften van een doelgroep. Om hetzelfde gewenste gedrag te bereiken kan het daarbij nodig zijn om voor verschillende doelgroepen verschillende interventies in te zetten. Als bijvoorbeeld een tekort aan kennis wordt geïdentificeerd als barrière voor het gewenste gedrag van een bepaalde doelgroep, kan een lezing worden ingezet waarin de nadruk ligt op kennisoverdracht. Als het gaat om een gebrek aan motivatie kan de insteek van diezelfde lezing eerder motivatie zijn, of een heel andere interventie die medewerkers motiveert. Of er kan gekozen worden voor een interventie die het gedrag als het ware afdwingt zodat medewerkers geen keuze meer hebben.

Voorbeelden van mogelijke interventies gebaseerd op de organisatiecontext zijn:

- Social engineering
- Roadshow
- Lezing
- Ambassadeurschap
- Serious Game
- Educatieve sessie
- Hack Demo
- Intervisiegroepen
- Event met een competitie element
- Escape room

Cultuurprogramma

Analyse van veiligheid in relatie tot de bestaande organisatiecultuur

Voordat gewerkt kan worden aan een veilige organisatiecultuur is het nodig inzicht te krijgen in de huidige organisatiecultuur en identiteit van de organisatie. Denk hierbij aan belangrijke onderliggende normen en waarden, het (voorbeeld)gedrag en de visie van medewerkers en management.

Hierin kan inzicht worden verkregen door middel van een vragenlijstonderzoek binnen de hele organisatie, interviews met medewerkers, veldonderzoek (het observeren van gedrag in de praktijk) en/of deskresearch.

Interventieprogramma t.b.v. cultuurverandering

Op basis van een analyse van de huidige cultuur is het van belang dat wordt vastgesteld wat de gewenste cultuur is en wat er nodig is om deze te bereiken. Dit kan worden uitgewerkt in een interventieprogramma voor cultuurverandering. Elementen die hierin kunnen worden meegenomen zijn:

- Herhaling van belangrijke boodschappen, zodat de noodzaak van cyberveilig gedrag beter beklijft.
- Bevorderen van doelgedrag door het aanspreken van sociale invloed. Doelgedrag is bijvoorbeeld dat medewerker bezoekers zonder begeleiding of badge aanspreken, een beeldscherm vergrendelen bij het verlaten van een werkplek of collega's aanspreken op zichtbaar ongewenst gedrag. Door sociale invloed te stimuleren wordt een cyberveilige cultuur versterkt.
- Gebruik maken van informeel/formeel leiderschap bij het communiceren en uitdragen van het belang van een cyberveilige organisatiecultuur.
- Werken aan zichtbaarheid en toegankelijkheid van security binnen organisatie. Denk bijvoorbeeld aan de zichtbaarheid van cybersecurityteam, de wijze waarop de helpdesk over dit onderwerp communiceert, betrokkenheid van management, etc.

Activiteiten ter bestendiging van de veiligheidscultuur.

Er zijn verschillende activiteiten denkbaar voor het bestendigen van de cultuur. Naast het belang van herhaling van de boodschap, kan gedacht worden aan:

- Communicatietraining voor doelgroepen die actief en reactief bezig zijn met cybersecurity (IT-helpdesk, communicatie, management, HR afdeling) en hoe dit onderdeel te maken van het dagelijkse werk.
- Campagnes voor het bevorderen van een veilige meldcultuur
- Communicatie over gewenst doelgedrag (vb: infographics, korte filmpjes met uitleg, artikelen op intranet, nieuwsbrieven) en het aanspreken van collega's.
- Technische ondersteuning van doelgedrag (vb: meld phishing knop, wachtwoordmanager).
- Security ambassadeur trainingen/opleidingen die blijvend ondersteuning biedt.
- De CEO/bestuurder in communicatie uitingen voortdurend aandacht laten besteden aan het onderwerp, soms meer impliciet, andere keren expliciet.

Consultancy

Advies over organisatie specifieke vraagstukken

Afhankelijk van een specifieke context van een organisatie kunnen er vragen ontstaan die maatwerk vereisen. In dat geval kunnen dienstverleners advies geven waarbij de kennis van de dienstverlener in de context van een organisatie wordt toegepast.

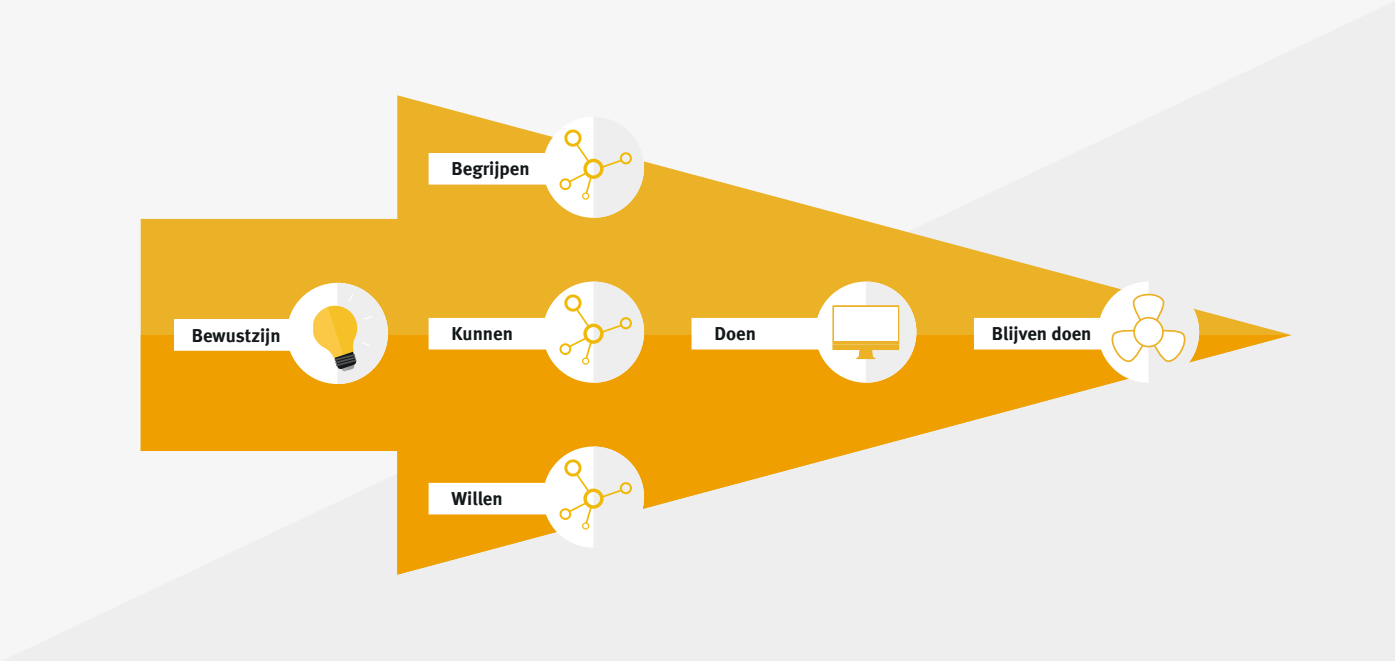
Bijlage

Balm model

Verwijzing:

- Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)

Het Balm model legt uit hoe mensen tot cyberveilig gedrag komen. Dat begint met bewustzijn: 'waarom is cyberveiligheid voor onze organisatie belangrijk?'. Medewerkers moeten vervolgens begrijpen wat dit betekent voor hun eigen gedrag ('welke kennis, vaardigheden heb ik nodig'?). De organisatie moet cyberveilig gedrag faciliteren, ook technisch. En uiteindelijk moeten mensen zelf ook cyberveilig gedrag willen vertonen, hierin speelt leiderschap en voorbeeldbeeldgedrag van belangrijke en zichtbare spelers, zoals bijvoorbeeld management, een grote rol. Als aan deze vier randvoorwaarden wordt voldaan zullen mensen ook bewegen naar cyberveilig gedrag. Vervolgens dient de organisatie dit gedrag ook te onderhouden, om een cyberveilige cultuur langdurig te waarborgen.



Gedragstheorie van MacInnis, Moorman en Jaworski

Verwijzing:

- Exercise Therapy and Behavioural Change (Balm, M.F.K., Purdue University Press, 2002)
- Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads (MacInnis, D. J., Moorman, C., & Jaworski, B. J., Journal of Marketing, 55, 32-53, 1991)

De gedragstheorie van MacInnis, Moorman & Jaworski (1991) stelt dat gedrag kan worden gezien als resultaat van drie factoren: motivatie, capaciteit en gelegenheid. Met andere woorden: wíl iemand het doen, is hij in staat om het te doen en krijgt hij de kans om het te doen?

- Capaciteit. De mate waarin iemand in staat is om bepaald gedrag te vertonen, gegeven zijn eigenschappen, vaardigheden, kennis en instrumenten.
- Motivatie. Wil iemand het gedrag vertonen; welk doel vindt iemand eigenlijk belangrijk?
- Gelegenheid. De mate waarin de omstandigheden het gedrag bevorderen of belemmeren. Bijvoorbeeld fysieke omstandigheden, sociale omstandigheden en technologie.

Als deze drie factoren allemaal in voldoende mate aanwezig zijn, zal gedrag plaatsvinden. Als één van deze factoren (deels) ontbreekt, is de kans op gedrag een stuk kleiner. Het verdelen van gedrag in deze drie componenten vergroot het inzicht in de maatregelen die een organisatie kan nemen om bepaald gewenst gedrag te laten optreden. Het inzicht dat gedrag uit meerdere componenten bestaat, maakt inzichtelijk waarom awareness programma's vaak niet tot het gewenste resultaat leiden. Awareness gaat over kennis en capaciteit. Dat gedrag niet optreedt vanwege een gebrek aan kennis erover is namelijk een aanname. Het kan net zo goed ontbreken aan motivatie of aan gelegenheid om het gedrag te vertonen. Daarom is het relevant om, voorafgaand aan het bedenken of implementeren van een interventie, te onderzoeken waarom bepaald gedrag niet of minimaal optreedt.

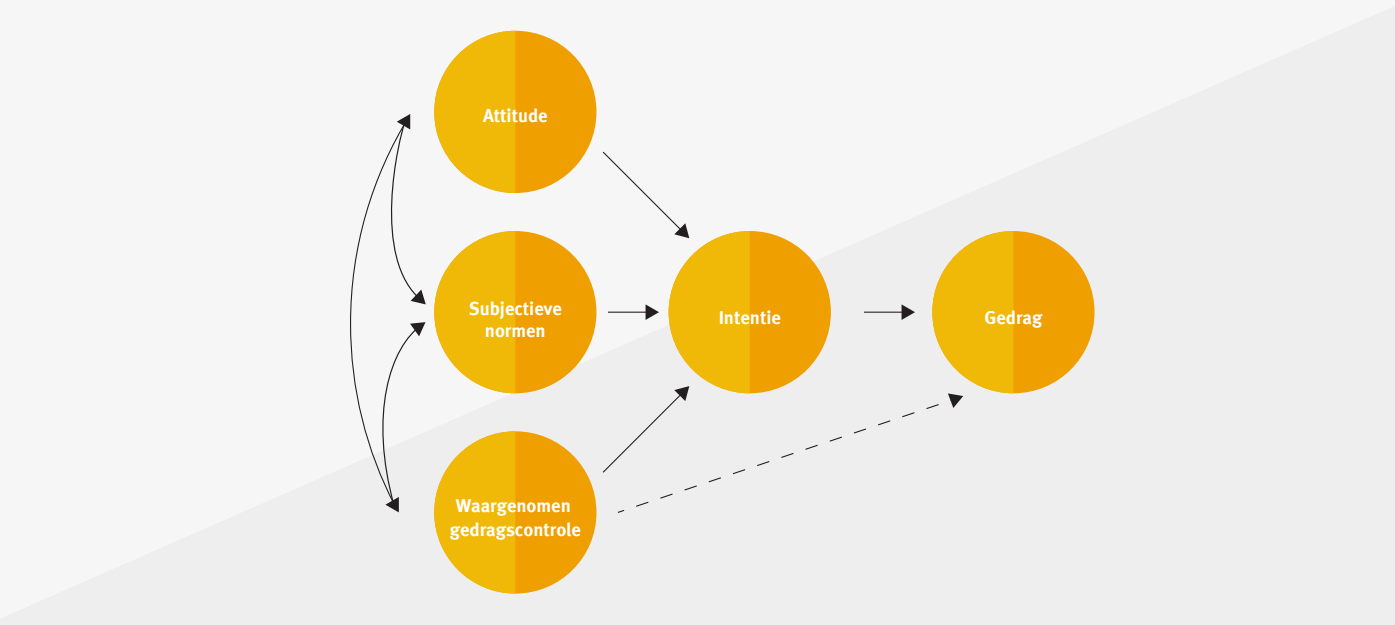
Theorie van Ajzen

Verwijzing:

- Attitudes, personality, and behavior (Ajzen, I., 2nd Ed., Milton-Keynes, England: Open University Press, McGraw-Hill, 2005)

De theorie van Ajzen (theory of planned behaviour) stelt dat bewust gedrag direct voortkomt uit de intentie om het gedrag te vertonen. De intentie wordt volgens Ajzen bepaald door drie elementen:

- Attitude. De attitude gaat over de houding van een persoon ten opzichte van het gedrag. Wanneer de persoon een positieve houding ten opzichte van het gedrag heeft, is de kans groter dat de persoon het gedrag bewust zal vertonen.
- Subjectieve norm. De subjectieve norm gaat over datgene wat de persoon denkt dat anderen – in zijn directe omgeving – vinden van het (uit te voeren) gedrag en hoe zij hierover oordelen. Wanneer de persoon denkt dat anderen het gedrag als normaal of goed beschouwen, is de kans groter dat de persoon het gedrag bewust zal vertonen.
- Waargenomen gedragscontrole. De waargenomen gedragscontrole gaat over de mate waarin de persoon gelooft dat het gedrag eenvoudig uit te voeren is. Dit gaat zowel om de eigen vaardigheden als om de omgevingsfactoren die het gedrag bevorderen of belemmeren. Wanneer de persoon gelooft dat gedrag eenvoudig is uit te voeren, is de kans groter dat de persoon het gedrag bewust zal vertonen.



Persuasive by Design Behaviour Change Model

Verwijzing:

- Persuasive by Design, Behaviour Change Model (R. Renes, S. Hermsen , Draaiboek gedragsverandering, 2017)

Hoe zorg je dat je campagne het beoogde gedragsveranderende effect heeft? Gedrag is complex en kent vele aspecten. Door vragen te stellen tijdens het ontwerpproces en ideeën aan te reiken voor interventie strategieën in je ontwerp, helpen de gedragslenzen je scherp te focussen op het gedrag van je doelgroep. De verschillende 'lenzen' geven onder andere inzicht in hoe je automatische facetten van gedrag kunt beïnvloeden, hoe je doelgroep tegenover het doelgedrag staat en wat de motivatie van de doelgroep is.

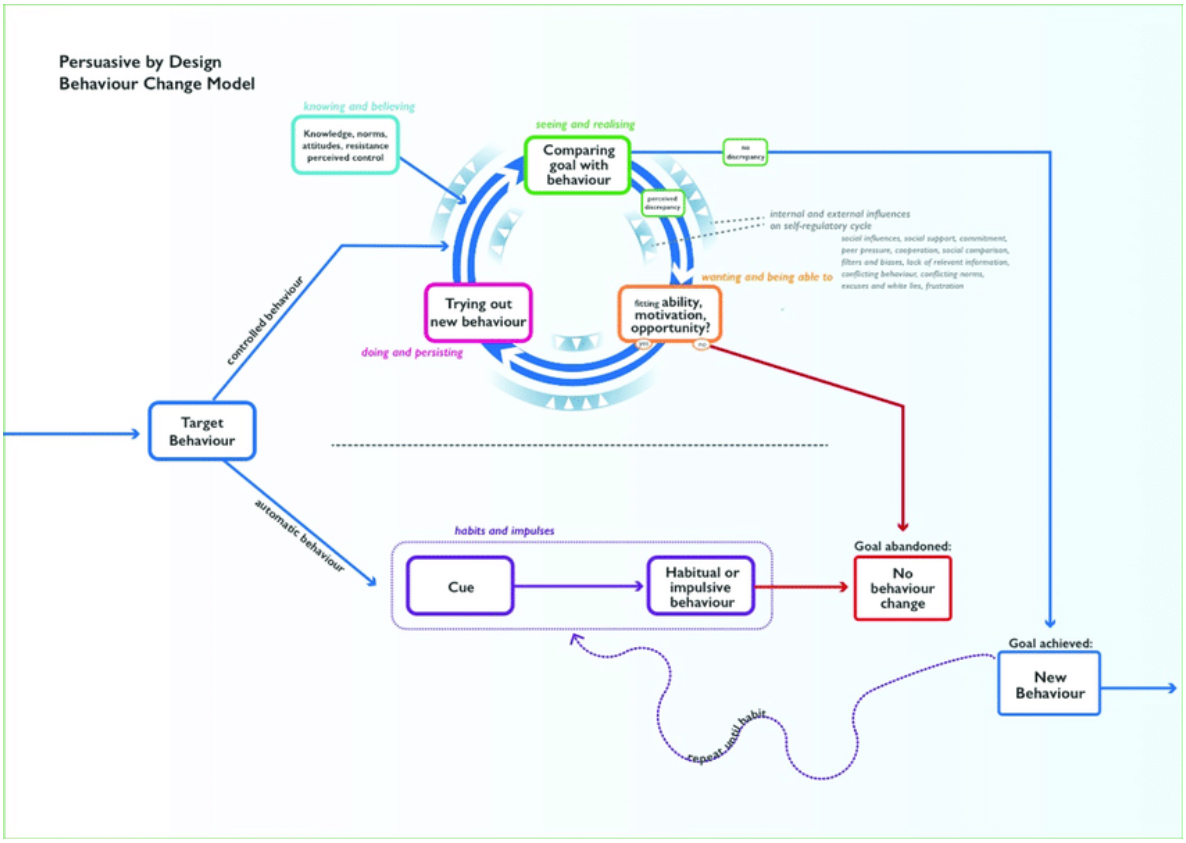
- Gewoontes en impulsen. Een groot deel van ons gedrag is automatisch. We denken er niet bij na. Het kan bestaan uit reflexmatige impulsen, maar ook uit meer of minder diep ingesleten gewoontes. Bekijk met deze lens of het doelgedrag van je doelgroep automatische aspecten kent en hoe je die kunt beïnvloeden.

- Weten en vinden. Het gewenste gedrag komt niet altijd overeen met de wil en de mogelijkheden van de doelgroep. Bekijk met deze lens welke kennis de doelgroep heeft van het doelgedrag. Onderzoek wat de doelgroep van het doelgedrag vindt, bijvoorbeeld of ze er weerstand tegen voelt.

- Zien en beseffen. Doelgroepen zijn niet altijd even goed in het waarnemen van het eigen gedrag. Bekijk met deze lens of je doelgroep goed in staat is om het verschil tussen het eigen gedrag en het doelgedrag waar te nemen. Onderzoek ook of zij daar hulp bij nodig heeft.

- Willen en kunnen. Gedragsverandering is pas echt mogelijk als er voldoende motivatie aanwezig is en de juiste vaardigheden voorhanden zijn. Bekijk met deze lens of de doelgroep voldoende gemotiveerd is om het gedrag te veranderen, of ze daartoe de juiste vaardigheden bezit en of ze de kans krijgt om het nieuwe gedrag uit te voeren.

- Doen en blijven doen. Om tot nieuw gedrag te komen, is het nodig het gewenste gedrag in haalbare stappen uit te proberen en te blijven toepassen. Bekijk met deze lens hoe makkelijk en aantrekkelijk het is om het nieuwe gedrag uit te proberen, te herhalen en onder de aandacht te houden.

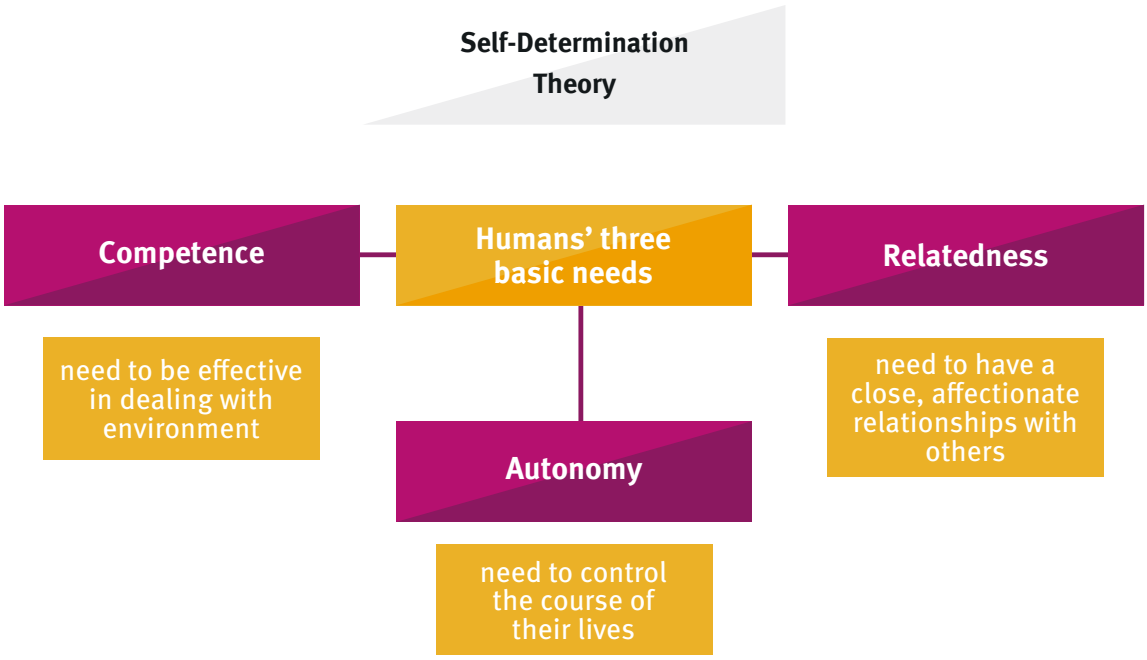


Self-Determination Theory

Verwijzing:

- Self-Determination Theory (Deci & Ryan, 1985; 2000)

Deze theorie stelt dat drie aangeboren en universele psychologische behoeftes de intrinsieke motivatie kunnen verhogen, waardoor mensen willen groeien en veranderen. Als er wordt ingespeeld op de drie psychologische basisbehoeften autonomie, competentie en relatie, zal dit een positief effect hebben op de intrinsieke motivatie.



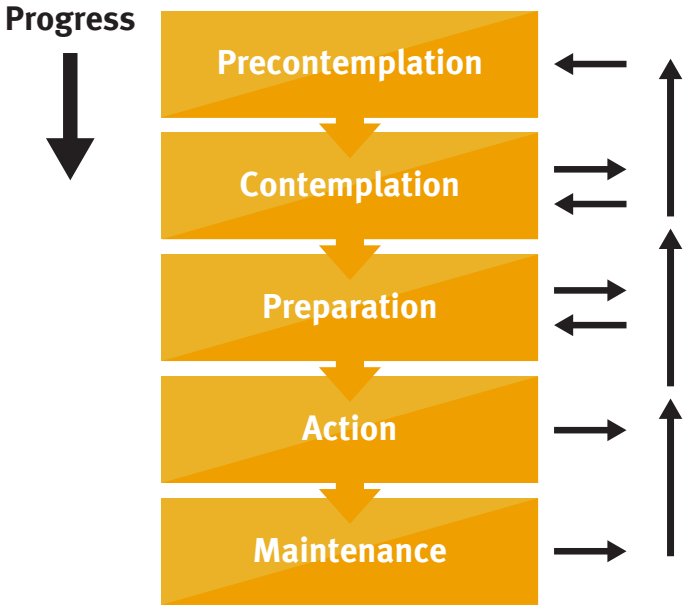
Transtheoretisch model

Verwijzing:
- Transtheoretisch model (Prochaska & Di Clemente, 1982)

Het transtheoretisch model, ook wel de cirkel van gedragsverandering, maakt inzichtelijk welke stappen er doorlopen worden in een veranderingsproces. Het veranderingsproces wordt in een cirkel van zes stappen weergegeven. De theorie stelt dat gedragsverandering geen linieair proces is (met een duidelijk begin- en eindpunt), maar een circulair proces. Tijdens elke fase kan de persoon terugvallen in een vorige fase of oud gedrag.

De zes stappen op een rij:

- Voorbeschouwing (precontemplatie): op dit niveau bestaat er (nog) geen intentie tot verandering. De persoon is zich vaak niet bewust van het probleem.
- Overpeinzing (contemplatie): hier is de persoon zich bewust dat er een probleem is. De motivatie om er iets aan te doen is aanwezig, maar er wordt door de persoon nog geen actie ondernomen.
- Besluitvorming (voorbereiding): op dit niveau maakt de persoon echt plannen om iets aan het gedrag te gaan doen.
- Actie: hier onderneemt de persoon daadwerkelijk actie om het gedrag te veranderen.
- Volhouden of consolidatie: op dit niveau probeert de persoon de bereikte verandering te bestendigen en niet terug te vallen. Het nieuwe gedrag moet een plaats vinden in het leven en geïntegreerd worden met andere activiteiten.
- Terugval: in de meeste gevallen is de persoon niet in staat om de bereikte situatie van bij de eerste poging volledig vast te houden. Terugval komt geregeld voor en het proces begint dan opnieuw.



Communicatie Activatie Strategie Instrument

Verwijzing:
- Het CASI-model (zie https://www.communicatierijk.nl/vakkennis/casi/documenten/publicaties/2019/03/08/handleiding-casi, 2020)

Het Communicatie Activatie Strategie Instrument (CASI) model is ontwikkeld door de Dienst Publiek en Communicatie van het ministerie van Algemene Zaken en wordt onder andere gebruikt door ministeries om effectieve interventies te ontwikkelen voor gedragsverandering. CASI is een stapsgewijze methode om inzichten uit recent wetenschappelijk onderzoek toe te passen in de praktijk van gedragsverandering.

Het belangrijkste onderliggende principe van CASI is dat je begint met een duidelijke analyse voordat je een oplossing of interventie verzint. In deze analyse bepaal je wat het gewenste gedrag is, wie de doelgroep is en hoe de huidige situatie eruitziet.

Je verdiept je analyse vervolgens door te onderzoeken welke factoren invloed hebben op het gewenste gedrag, de zogeheten 'gedragsbepalers'. Gedragsbepalers zijn factoren die het gewenste gedrag makkelijker of moeilijker maken. Dit kunnen bijvoorbeeld factoren in de (digitale) omgeving zijn (zoals de user interface), factoren in de sociale omgeving (zoals normen en voorbeeldgedrag), factoren rondom kennis en kunde, maar ook psychologische factoren (zoals weerstand of risicoperceptie).

Op basis van deze analyse selecteer je de meest kansrijke strategieën om, gegeven je doelgroep en bijbehorende gedragsbepalers, het gewenste gedrag onder je doelgroep te stimuleren.

Naast deze stapsgewijze methode biedt CASI een checklist met tien concrete, evidence-based tips voor gedragsverandering:
- Houd het simpel
- Maak het persoonlijk relevant voor mensen
- Maak iets wat mensen graag willen zien
- Laat het goede gedrag zien
- Laat mensen en situaties zien die herkenbaar zijn
- Geef je doelgroep concrete aanwijzingen
- Voorkom weerstand
- Zet de sociale omgeving van je doelgroep in
- Communiceer daar waar het gedrag plaatsvindt
- Houd het lang vol en herhaal

CYBERVEILIG NEDERLAND

Contactgegevens
E-mail: info@cyberveilignederland.nl
Telefoon: 088 - 118 25 10