Tussen stoel en toetsenbord

Hoe gedrag en cultuur bijdragen aan informatiebeveiliging

"Tussen de stoel en het toetsenbord zit de zwakste schakel" is een veelgehoorde uitspraak over de informatiebeveiliging in organisaties. Het is daarom des te opmerkelijker dat in de normenkaders voor informatiebeveiliging zo weinig aandacht wordt besteed aan de factor mensen. Dat hangt ongetwijfeld samen met de (veelal technische) achtergrond van de mensen die deze kaders hebben ontwikkeld, maar wellicht is daarom hier nog wel de meeste winst te behalen. Binnen InAudit werken specialisten op het gebied van informatiebeveiliging samen met gedragsdeskundigen. In onze analyses gaan we onder meer uit van de ZDT-theorie en in dit artikel willen we ingaan op hoe we deze theorie kunnen toepassen, om zo bij te dragen aan een betere beheersing van de risico's die samenhangen met 'de zwakste schakel': de mens.

Awareness is nog geen gedrag

De meeste normenkaders schrijven voor dat de organisatie moet investeren in programma's om de awareness voor wat betreft cybersecurity te verhogen en om de interne regels en procedures onder de aandacht te brengen. Maar awareness is nog geen gedrag. Het is overigens wel een eerste stap naar gewenst gedrag: mensen moeten weten wat van ze wordt verwacht. Dat betekent dat ze zich bewust moeten zijn van het signaleren van risico's en van hoe daarop te reageren. Stap 1 is dus het opstellen en communiceren van duidelijke voorschriften en procedures die bekend en toegankelijk zijn zodat iedereen weet hoe (en wanneer!) te handelen. De volgende stap is om deze wetenschap ook in gedrag te vertalen. Het MOA-model (motivation-opportunity-ability) leert ons dat gedrag kan worden gestimuleerd aan de hand van drie factoren: motivatie, gelegenheid en mogelijkheid. Hierna gaan we daar verder op in.

Dat kennis nog geen gedrag is werd in een bijdrage in het Informatiebeveiliging Magazine mooi geïllustreerd aan de hand van een goed voorbeeld, namelijk het voorschrift om een sterk wachtwoord te gebruiken. Je zou verwachten dat deze basale kennis algemeen bekend is, maar het onderzoek liet zien dat bij ca. 20% van de deelnemers de kennis afwezig of onvoldoende was. Waar 80% van de respondenten wel degelijk op de hoogte was van het voorschrift, bleek dat van deze 80% slechts 30% deze kennis ook daadwerkelijk toepaste. De helft van de respondenten beschikte dus wel degelijk over de benodigde kennis, maar paste deze uiteindelijk niet toe. Zowel vanuit het oogpunt van informatiebeveiliging als vanuit de gedragswetenschap is dit interessant terrein. InAudit heeft beide expertises in huis, wellicht dat wij u op dit vlak kunnen helpen.

Stel mensen in staat om veilig te werken

Voor wat betreft het bieden van de 'mogelijkheid' is het delen van kennis over veilig werken en het beschikbaar stellen van toegankelijke procedures een belangrijke eerste stap. Mensen moeten weten wat van ze wordt verwacht, wat ze moeten doen en waar ze het eventueel kunnen raadplegen. Maar dat alleen is niet voldoende. Zoals mijn vader ooit eens opmerkte: "Ook Messi moet trainen om zo goed te kunnen spelen". Het gaat dus ook om het automatiseren van bepaalde patronen en handelingen. Dat doe je niet alleen door procedures uit te leggen, maar met name door training. Zo kan bijvoorbeeld het melden van verdachte phishing mails en incidenten een automatisme worden. Daarvoor zijn inmiddels goede en aantrekkelijke tools beschikbaar. Wat opvalt is dat veel van deze tools ook elementen van beloning, spel of competitie in zich hebben. De 'homo ludens' laat zich nu eenmaal makkelijker verleiden om net iets meer te trainen als daar iets van beloning in zit. Al is het maar een digitaal schouderklopje.

Maak van de veilige keuze ook de gemakkelijke keuze

Als we het element 'gelegenheid' verkennen dan is het belangrijk om vast te stellen dat mensen bij voorkeur de gemakkelijke weg kiezen. Wanneer mensen worden belemmerd om de veilige keuze te maken, terwijl de onveilige keuze veel eenvoudiger is, dan laat zich voorspellen in welke richting het gedrag zal gaan. Hierin kan de ICT-afdeling een belangrijke rol spelen, door de veilige keuze te faciliteren (en eventueel het opwerpen van belemmeringen voor de ónveilige keuze). Denk hierbij aan het faciliteren van single-sign on procedures en/of wachtwoord-managers zodat het niet langer belastend wordt om complexe wachtwoorden te onthouden. Een ander voorbeeld is een 'report phish' button als add-on in de e-mailbox om verdachte emails eenvoudig te rapporteren. Als het als ingewikkeld wordt ervaren om bestanden van de ene gebruiker naar de andere gebruiker te verschepen maar medewerkers dit gemakkelijk doen met een USB-stick, dan zal het aantal USB-sticks dat rondslingert snel toenemen; met alle risico's van dien. Het is daarom belangrijk om belemmeringen die veilig werken in de weg staan te inventariseren. Het wegnemen van deze belemmeringen kan een belangrijke bijdrage leveren aan het stimuleren van veilig gedrag.

Stimuleer veilig gedrag

Bij het derde element, namelijk 'motivatie' komen we op één van de belangrijkste pijlers onder de visie die wij als InAudit centraal stellen in onze advisering: namelijk het stimuleren van intrinsieke motivatie. Wij hangen hierbij de inzichten aan die voortkomen uit de Zelfdeterminatietheorie (ZDT) van de wetenschappers Ryan en Deci. Naast intrinsieke motivatie kan echter ook extrinsieke motivatie een rol spelen bij het stimuleren van gewenst gedrag, bijvoorbeeld in de vorm van beloningen (positief) of sancties (negatief). Ook dit kan effectief zijn, denk maar aan de invloed van de trajectcontrole op sommige wegen. Toch achten wij het stimuleren van de intrinsieke motivatie op de lange termijn als het meest effectief in het bereiken van doelstellingen. Bij intrinsieke motivatie gaat het om drie elementen. Het eerste element is de betrokkenheid bij de organisatie en haar doelstelling, zoals bijvoorbeeld de zorg voor het bewaken van de vertrouwelijkheid van de toevertrouwde gegevens. Het tweede element is de verantwoordelijkheid die men ervaart en de autonomie om daar invulling aan te geven. Het derde element is de ervaren mate van vaardigheden waar men over beschikt om de taak goed uit te voeren. Als mensen intrinsiek gemotiveerd zijn om informatiebeveiliging serieus te nemen, zal men eerder geneigd zijn om 'kennis' te vertalen in gedrag. Niet omdat het moet, maar omdat het kan.

Het goede voorbeeld

Hiervoor hebben we geschreven over 'gedrag', maar er is ook nog iets als 'cultuur'. Het voorbeeldgedrag van de bestuurder, het aanspreekgedrag van collega's en de professionele sfeer die ervoor zorgt dat we ons werk serieus nemen zijn allemaal uitingen van de cultuur van een organisatie. Om de effectiviteit van informatiebeveiliging te verhogen moet er ook een effectieve risicocultuur bestaan. De mens is immers een sociaal wezen. Het gaat te ver om hierover nu al te veel uit te weiden, maar wellicht helpt een korte illustratie: We kennen waarschijnlijk allemaal wel afbeeldingen met zogenaamde olifantenpaadjes, 'shortcuts' die mensen nemen omdat ze ofwel het nut niet inzien van de maatregelen, ofwel de 'koninklijke route' te belastend vinden, ofwel om andere redenen. Deze komen ook volop voor in de wereld van de informatiebeveiliging. Helaas is de veiligste weg vaak niet de meest gebruikersvriendelijke en toch willen we dat de veilige procedure wordt toegepast: Als eindverantwoordelijken in hun gedrag laten zien dat zij kiezen voor de makkelijke weg ('scherm niet afsluiten', geen tools gebruiken voor email die moet worden beveiligd, etc.) of als een groot deel van de collega's procedures negeert, dan zal dit niet bijdragen aan een effectieve informatiebeveiliging. Het niet vertonen van voorbeeldgedrag biedt medewerkers een eenvoudige manier om procedures in de wind te slaan met als rationalisatie: de baas doet het ook niet.

Op weg naar steeds betere volwassenheid
In de wapenwedloop met de (veelal goed) georganiseerde partijen die onze informatiebeveiliging bedreigen, is het goed om te beseffen dat de bedreigingen niet alleen in de techniek zitten, maar met name ook in het menselijk gedrag. De verschillende normenkaders schrijven wel maatregelen voor gericht op het verbeteren van de 'awareness' (het bewustzijn), maar naar onze mening veel te weinig als het gaat om 'gedrag' zelf. Zoals aangegeven leidt bewustzijn niet altijd automatisch tot gedrag. Er is meer voor nodig. Ook over het stimuleren van een effectieve risicocultuur wordt in de meeste normenkaders niet gesproken; bovendien is dit lastig te toetsen. Daarom is het goed om regelmatig een 'gap-analyse' uit te voeren om de kennis en de toepassing van de regels te toetsen. Omdat vreemde ogen dwingen kan een auditor, een CISO of een gedragsdeskundige u op basis van objectieve waarnemingen helpen om met gerichte interventies stappen voorwaarts te maken. We zullen nooit helemaal gereed zijn om volledige weerstand te bieden tegen alle dreigingen die op de loer liggen, maar als we informatiebeveiliging 'belangrijk en leuk' weten te maken zijn we alweer een stukje verder. Uiteraard zijn wij graag bereid om u hierbij met onze kennis en competenties te ondersteunen !

Tussen stoel en toetsenbord