(On)veilig gedrag geeft vaak de doorslag

Steeds meer organisaties slaan de weg van digitalisering in. Dat biedt grote kansen maar brengt ook nieuwe risico's met zich mee. SRA wil een inhoudelijke bijdrage leveren aan het versterken van uw kantoor en de relatie met uw klanten die deze transitie doormaken. Daarom hebben we de samenwerking gezocht met Northwave, een zeer gerenommeerde partij op het gebied van integrale informatiebeveiliging.

In dit tweede artikel kijken we naar de factor 'mens' bij het veilig werken met informatie. Dat doen we met Inge van der Beijl, gedragswetenschapper en Director Behaviour en Training van Northwave.

Datalek, digitale fraude en afpersing

"Bij Northwave staan we dagelijks organisaties bij die slachtoffer zijn geworden van hackers. Vaak gaat dat om een datalek in de zin van de AVG dat moet worden gemeld, maar we zien ook veel digitale fraude en afpersing. We weten zodoende dat criminelen gebruik maken van menselijke patronen, gewoontes en de zucht naar gemak. Om dat te voorkomen, is het belangrijk dat medewerkers in staat zijn hun werk veiliger te doen. Dat gaat veel verder dan inzetten op 'security awareness', oftewel meer bewustzijn. Wat nodig is, is een cultuur waarin veilig werken zit ingebakken. Daardoor is de werknemer waakzaam en veerkrachtig en juist in staat om de werkwijze van de hackers te doorbreken en tegen te werken."

Meer dan bewustzijn

Van der Beijl, die meer dan tien jaar voor TNO heeft gewerkt en daar in de laatste jaren de afdeling Human Behaviour & Organisational Innovations leidde, ziet dat veel organisaties wel met dit onderwerp bezig zijn, maar nog te vaak hun heil alleen zoeken in het verhogen van bewustzijn en kennisgerichte maatregelen, zoals standaard e-learning.

"Natuurlijk is het verstandig het bewustzijns- en kennisniveau van je mensen op peil te houden. Kennis over (actuele) bedreigingen,

Inge van der Beijl

Wat nodig is, is een cultuur waarin veilig werken zit ingebakken

Mensen bagatelliseren de gebeurtenis in hun hoofd

risico's en procedures is belangrijk. Wij mensen zijn echter gewoontedieren en het brein is idolaat van prikkels en snel reageren.

Zeker de huidige digitale informatiestromen en het continue aanbod van prikkels maakt dat we voortdurend 'aan' staan en steeds onmiddellijk willen reageren. Hierdoor is het logisch dat we snel e-mails beantwoorden, of op een toegestuurd linkje klikken. Ons patroon is niet: eerst even nadenken wat er nu werkelijk gevraagd wordt, met alle gevolgen van dien. Wat we vervolgens vaak in de praktijk zien, is dat mensen die achteraf toch gaan twijfelen of er wellicht iets niet in de haak was, daar niet adequaat op reageren. Mensen verwachten dat het niet direct consequenties heeft of kunnen de consequenties niet overzien. Dus bagatelliseren ze de gebeurtenis in hun hoofd en geven zo de aanvaller het voordeel van de twijfel. Dat is niet de schuld van de medewerker, maar het gevolg van hoe ons brein werkt en van de cultuur waarin medewerkers werken", aldus Van der Beijl.

Wat kunnen organisaties doen?

Alleen een kenniscampagne of e-learning is dus niet voldoende. Het gaat om het veranderen van de manier waarop mensen hun werk doen. Dat klinkt meteen als een onoverzichtelijk en abstract probleem. Wat kunnen organisaties doen?

"De kern van een cultuur van veilig werken zit in de openheid over incidenten en elkaar mogen aanspreken op gedrag. Incidenten zullen er namelijk altijd zijn. Je wilt dat je medewerkers met zelfvertrouwen handelen als er zich iets vreemds voordoet. In organisaties waarin wij die openheid bereiken met onze programma's, is er juist waardering voor een collega die op de rode knop drukt en zodoende openheid geeft over de incidenten. Dan zie je opeens hoeveel incidenten er eigenlijk zijn, want je mensen melden die nu wel. Met die meldingen leveren medewerkers zelf structurele en zichtbare verbeteringen van de beveiliging. Veilig werken ontstaat zo vanuit mensen zelf. Zo ervaren ze dat het zinvol is om verantwoordelijkheid te nemen."

Zeker in het mkb is er vaak beperkt inzicht in hoe je dit nu slim en vooral pragmatisch aanpakt. Bij ondernemers en accountants groeit weliswaar het bewustzijn over het belang van cybersecurity, maar het doorvertalen naar concrete en vooral effectieve stappen in het bedrijf wordt vaak nog als lastig ervaren. Veel ondernemingen blijven dus hangen in vooral technische maatregelen. De kwetsbaarheid voor 'social engineering' en gerichte phishingaanvallen blijft dan bestaan. We vragen Van der Beijl daarom waaraan ondernemers moeten denken als ze zo'n programma voor veilig werken willen opzetten.

Welke stappen zijn er?

"De eerste stap is dat je duidelijk benoemt welk veilig gedrag je eigenlijk wilt zien. Welke concrete risico's ben je aan het beperken en moet je beperken? En voor welke groep medewerkers geldt dan welk type gedrag? Het heeft geen zin heel algemeen of abstract te blijven over beveiliging als je dat niet koppelt aan concreet handelen van elk individu. Stap twee is beseffen dat je bezig bent om aan cultuur en het ingesleten gedrag van mensen te sleutelen. Dat komt echt alleen vanuit henzelf. Er is geen afstandsbediening voor je medewerker. Hoeveel vragen iemand ook goed kan beantwoorden, het gaat er om wat ze daadwerkelijk doen. We zorgen ervoor dat er geen obstakels zijn om goed te handelen, bijvoorbeeld procedures of techniek die dat belemmeren of een gebrek aan voorbeeldgedrag vanuit het management, en we zorgen dat er altijd een constructieve reactie is. Dus bij zowel 'goed' als 'fout' gedrag is de response van de organisatie positief en opbouwend. Dat bevordert dat mensen elkaar aanspreken en zich laten aanspreken. Het derde aspect is dat we vormen van monitoring kunnen inbouwen. We kunnen niet alleen vertrouwen op het signalerende en corrigerende vermogen van de mensen zelf. Deze monitoring (inhouse of uitbesteed) zorgt ervoor dat er altijd nog een volgende laag van bescherming is die kan ondervangen dat iemand toch een fout heeft begaan. Bovendien geeft die monitoring ook inzicht in gedrag dat we niet willen, zoals het gebruik van IT-middelen die niet zijn toegestaan; zogenaamde 'shadow IT'."

Belangrijkste tip voor accountants

Tot slot vragen we Van der Beijl om haar belangrijkste tip voor accountants die hun klanten willen bijstaan bij het aanscherpen van een cultuur van veiligheid.

"Verbeter de wereld en begin bij jezelf. Een goede eerste stap is om eens te denken vanuit de werkelijke risico's van je eigen kantoor en concreet te formuleren welk veilig gedrag daar bij zou passen. Maar kijk wel breder dan dat. Een structureel slimme aanpak van informatiebeveiliging en privacy vraagt altijd om inzicht in de totale uitdaging. Wij hebben het vaak over business, bytes en behaviour; ofwel de organisatie, de techniek en de mens. Dat is een aanpak die goed werkt, omdat je dan vanuit een totaalaanpak kunt werken aan de effectiviteit en samenhang van je beleid. Maar het allerbelangrijkste blijft dat beveiliging de business moet kunnen volgen. Mensen moeten hun werk kunnen doen. Beveiliging is niet leidend maar dienend. Als je denkt vanuit die optiek, dan maximaliseer je ook de medewerking van je eigen medewerkers."

Meer informatie

Kijk voor meer informatie over cyber security op www.sra.nl of stel uw vraag via automatisering@sra.nl.