Security, Het Nieuwe

Wie in een organisatie verantwoordelijk is voor beveiliging, beleeft spannende tijden. En dan denken we eens niet aan terroristische dreigingen, hackers en ander dreigend onheil. Nee, wat deze tijd zo boeiend maakt, zijn de grote veranderingen in de manier waarop mensen werken. Die het vakgebied van security voor nieuwe uitdagingen plaatsen. Uitdagingen die van security managers vragen om met een brede blik te kijken naar wat zich in hun werkomgeving afspeelt. Paul Koedijk *

Aan de ene kant is de tendens zichtbaar om te komen tot een betere organisatie van tijd en plaats van arbeid en dienstverlening als vorm van sociale innovatie, zoals het SER-advies 'Tijden van de samenleving' constateert. Het zogenaamde Nieuwe Werken is daar een uiting van. Werken raakt steeds minder gebonden aan traditionele werktijden en het klassieke kantoor. Verhoging van effectiviteit en productiviteit vraagt echter meer dan dat. De mens achter de werknemer kan dan ook niet langer worden genegeerd. Persoonlijk functioneren en welbevinden spelen een belangrijke rol. Het gaat steeds meer om de vraag die organisatiedeskundige *Wessel Ganzevoort* stelt: hoe kunnen we een organisatie vormen waarin iedereen 'zin' heeft en de zin ervan inziet? Daarbij is de vooronderstelling dat een dergelijke organisatie beter presteert dan een waarbij die ingredienten ontbreken.
De cultuur van een organisatie en het gedrag van medewerkers vormen in die gedachtegang belangrijke ingrediënten in de mix die bepaalt of een onderneming gezond is: niet alleen in financieel-economische zin maar ook als het gaat om het functioneren en welbevinden van de werknemers. Een gezonde organisatie is productiever en creatiever. Welke graadmeters gelden voor die gezondheid? Een omgekeerde indicatie vormen de vijf kenmerken van niet-functionerende teams:
1. afwezigheid van vertrouwen;
2. angst voor conflicten;
3. gebrek aan betrokkenheid;
4. vermijden van het afleggen van rekenschap;
5. onverschilligheid ten aanzien van resultaten van het werk.

Spagaat

Organisaties die overgaan op Het Nieuwe Werken en die hun werknemers zingeving willen bieden, staan voor de vraag welke plaats controle daarbij inneemt. Als er al geen plek meer is voor de traditionele supervisie door de chef die zijn werknemers soms letterlijk op de vingers keek, wat betekent dat dan voor de security manager, die meestal op nog grotere afstand staat? Alles vastspijkeren in processen en procedures werkt niet, omdat daarmee alle dynamiek uit een organisatie verdwijnt: de organisatie verstart en dat brengt weer andere wezenlijke problemen met zich mee.
Vernieuwing kan niet ontstaan zonder risico's te nemen. Het draait juist om het vinden van een goede balans tussen regels en vertrouwen. Dat laatste wordt er echter niet gemakkelijker op in een samenleving die steeds meer de juridische beheersbaarheid van risico's zoekt. In de cultuur van indekken en afrekenen die daarmee gepaard gaat, ontstaat de neiging om verantwoordelijkheden af te schuiven. Compliance wordt dan al snel een dwangbuis die creativiteit en innovatie smoort. Maar juist die creativiteit en innovatie zijn hard nodig om optimaal te reageren op de economische en sociale uitdagingen van nu. In dat opzicht is er sprake van een spagaat. Enerzijds worden de teugels op allerlei manieren aangetrokken, terwijl aan de andere kant het besef groeit dat nieuwe manieren van werken veel meer gebaseerd zijn op vertrouwen dan op traditionele vormen van controle.

Onduidelijkheid bij samenwerken

Het Nieuwe Werken heeft vooral betrekking op de eigen medewerkers. Maar de situatie is gecompliceerder. Het ontwikkelen van nieuwe producten en diensten die aansluiten bij een steeds veeleisender en gecompliceerder markt, vraagt meer en meer om samenwerking met partijen van buiten. Het besef groeit daarbij dat optimale snelheid en het maximaal uitbuiten van creativiteit de sleutels vormen van dergelijke samenwerkingsprocessen. Maar het is voor traditioneel opererende ondernemingen moeilijk om die draai te maken. De zogenaamde open innovaties vragen om flexibele netwerken, terwijl er momenteel hoofdzake-

Bevlogenheid als component van effectieve security?

Werken en innovaties

Het Nieuwe Werken en open innovatie leggen een veel grotere nadruk op het vertrouwen in werknemers.

lijk sprake is van gesloten systemen. Bescherming van de eigen belangen door middel van controles en regels speelt in dat soort systemen een belangrijke rol. Die werken echter belemmerend op innovaties die een antwoord willen bieden op de snelle en soms grillige veranderingen in de markt.
Aan het alternatief zitten echter ook haken en ogen. Zoals *professor Elke den Ouden* van de TU Eindhoven in haar oratie uit 2009 over 'het ontwerpen van (meer)waarde' al opmerkte: Een van de problemen bij innovatie via flexibele netwerken is dat er geen contracten of afspraken zijn waarin beschreven staat wat ieders rechten zijn. In het verlengde daarvan geldt dat die onduidelijkheid ook geldt voor de security-aspecten van die vorm van samenwerken.

Andere eisen aan beveiliging

Het onderhouden van contacten buiten de eigen organisatie en het uitwisselen van ideeën en kennis binnen een flexibel netwerk stellen aanvullende en andere eisen aan beveiliging. Sommige zaken spreken natuurlijk voor zich. IT-security springt meteen in het oog en het is niet voor niets dat in de discussies over security en Het Nieuwe Werken vooral dat aspect op de voorgrond staat. Het is nu eenmaal eenvoudiger om meer concrete zaken te bespreken. Maar waar mensen samenwerking zoeken en aangaan, gaat het natuurlijk om meer dan alleen het beveiligen van digitale communicatie. Zijn de partners in het netwerk betrouwbaar? Met wie zit je eigenlijk aan tafel? Maar ook in het proces zelf. Hoe open mag je zijn tegenover je gesprekspartners? Waar is terughoudendheid in de uitwisseling van informatie op zijn plaats? Wanneer moet je een einde maken aan vrijblijvendheid?

Dat zijn slechts een paar van de vragen die security raken, maar die lastig zijn te beantwoorden voor degenen die vol enthousiasme in het creatieve proces zitten. Wanneer netwerken steeds spontaner ontstaan en zich pas verdichten wanneer ook de ideeën zich meer beginnen uit te kristalliseren, is het moeilijk om te bepalen op »

In de discussies over security en Het Nieuwe Werken staat vooral IT-security op de voorgrond.

welk moment de security manager en de jurist instappen. Wanneer een samenwerking vanuit het wit langzaam het grijs inschuift, breekt het meest lastige moment aan. Het doet denken aan de tv-campagnes over veilig vrijen. Bijna alle spotjes concentreren zich op de vraag wie daarover als eerste begint. Bij innovatieve samenwerking gaat het er niet om wie als eerste het moment bepaalt om een voorbehoedsmiddel uit broekzak of tas tevoorschijn te halen, maar wie het eerst het woord '*non disclosure agreement*' in de mond neemt. Dat is het moment waarop het perspectief voor een langdurige samenwerking een reele optie begint te worden – en tegelijkertijd perspectieven en risico's ontstaan.

Voordat de juristen binnenstappen, komt het echter vooral aan op de sociale vaardigheden en inzichten van de deelnemers aan het netwerk om te bepalen of zij – in casu hun onderneming – geen onverantwoorde risico's lopen. Dat is niet eenvoudig. Creatieve ontwikkelaars omzeilen doorgaans het liefst de securityafdeling, omdat die vooral als een sta-in-de-weg wordt gezien. Het is ook moeilijk om de fases in het samenwerkingsproces en de daaraan verbonden risico's helder in kaart te krijgen, omdat ze zich onttrekken aan de traditionele manieren van productontwikkeling.

Vernieuwing kan niet ontstaan zonder risico's te nemen

Cultuurverandering

Het Nieuwe Werken en open innovatie leggen een veel grotere nadruk op vertrouwen in werknemers. Maar hoe bewerkstelligt een onderneming dat zijn werknemers te vertrouwen zijn? Een grotere nadruk op pre-employment screening – bekender terrein voor de security manager – is niet afdoende. Van cruciaal belang is dat medewerkers gemotiveerd zijn en zich met het bedrijf verbonden voelen. Bevlogenheid als component van effectieve security? Daarmee komt de security manager op een terrein waar hij of zij traditioneel weinig mee van doen heeft en waar het aan zekerheden en handvatten ontbreekt. Het vraagt van de security manager dat hij de cultuur van zijn bedrijf als het ware tot in de haarvaten kent. Zijn adviezen moeten aansluiten bij die cultuur, maar kunnen ook een pleidooi bevatten om in die cultuur noodzakelijke veranderingen aan te brengen; iets wat overigens niet eenvoudig is.
In algemene zin vormen cultuurveranderingen een grote opgave, zowel gezien vanuit de functie als vanuit de persoon van de security manager zelf, die traditioneel toch minder op heeft met de 'zachte kant'. Hij of zij kan dat ook niet alleen voor elkaar krijgen. Het vereist een veel vanzelfsprekender integratie van security in alle aspecten die te maken hebben met de manier waarop een organisatie of bedrijf zich probeert aan te passen aan de eisen van de tijd; eisen die niet alleen voortvloeien uit snelle veranderingen in de markt maar ook uit het streven naar een organisatie die in alle opzichten gezond is.

De belangrijkste bijdrage van security managers aan dergelijke processen bestaat eruit om bij de deelnemers besef te kweken voor wat ze vooral *niet* moeten doen. En om hen te stimuleren bij het nadenken over de vraag of er iets is wat om bescherming vraagt en wanneer het moment daarvoor is aangebroken. Boven dat laatste zweeft steeds nadrukkelijker de grotere en principiële discussie over de vraag of er nog steeds zaken moeten worden gedaan vanuit gesloten systemen of dat *open source* (waarbij alle informatie vrij is) de weg vormt naar innovatie. Dat is nog een brug verder, met nog grotere uitdagingen voor alle betrokkenen. De spannende en boeiende tijden voor de security manager zijn voorlopig niet voorbij. «

* *Paul Koedijk (met dank aan Elke den Ouden). Koedijk is partner bij Integis BV, een kantoor van forensisch accountants en andere onderzoekspecialisten, en tevens betrokken bij IFOH (Inspirational Forum on Organisational Health).*