Risico's bestaan, gebruik dus je verstand

We leven steeds meer in een risicomijdende maatschappij. En denken al gauw dat iemand anders wel over onze veiligheid heeft nagedacht. Maar je moet natuurlijk ook gewoon je gezonde verstand gebruiken en je bewust zijn van risico's. Samenwerking en informatie-uitwisseling tussen bedrijfsleven en overheid zijn dan wel een voorwaarde.

Erik de Vries, CPP
Chairman ASIS International Benelux Chapter

"Of het nu om de burger, het bedrijfsleven of de overheid gaat, je moet er natuurlijk op kunnen vertrouwen dat je veilig bent omdat regels zijn nageleefd. Zeker als het veiligheid is die je zelf niet zomaar kunt beoordelen. Maar we moeten ook durven accepteren dat je niet alle risico's kunt uitsluiten. Soms gaat het nu eenmaal mis. En dat laatste lijken we maar niet meer te willen inzien, sterker nog, bij een incident geven we al gauw een ander de schuld.

DE EERSTE STAP IS ALTIJD om de risico's te kennen. Dat geldt op alle terreinen van veiligheid, en dat zijn er veel. Veiligheid (safety & security) beslaat een zeer breed terrein; van brandpreventie, beveiliging, arbeidsveiligheid en crisismanagement tot IT-security. En daar begint ook de verwarring en het kolomdenken. Want het vraagt om moed om over je eigen muren heen te kijken en te erkennen dat risico's van IT-security soms dezelfde zijn als die van fysieke beveiliging.

OP ELK TERREIN VAN veiligheid zijn kennis en inschatting van risico's het uitgangspunt. Daarop baseer je je maatregelen, maar dat betekent ook dat je soms op basis van je risico-inschatting niets doet. Dat is prima, als het maar een bewuste keuze van de organisatie is.

IN DE PRAKTIJK ZIEN we vaak het tegenovergestelde. Organisaties nemen soms geen maatregelen omdat ze niet de tijd nemen risico's te kennen en begrijpen. Of men redeneert risico's weg: 'Hier gebeurt nooit iets' of 'Een incident overkomt een ander, niet mij'.

OF DE MAATREGELEN zijn juist aanbodgestuurd en niet gebaseerd op de risico's. Er worden bijvoorbeeld camera's opgehangen zonder stil te staan bij het doel ervan. Soms nemen organisaties slechts maatregelen om zich in te dekken. Dat

'Alleen via samenwerking kan een cultuur van veiligheidsbewustzijn ontstaan'

geeft minder gezeur dan onderbouwen waarom niets doen gewoon een kwestie van gezond verstand was.
Een serieuze security aanpak richt zich op organisatorische, fysieke en mensgerichte maatregelen. De organisatorische kant is van deze drie de belangrijkste. Je kunt nog zo'n veilige deur hebben, als je niet bewaakt dat hij dicht gaat, heb je geen maatregel.

ORGANISATORISCHE MAATREGELEN kunnen niet zonder veiligheidsbewustzijn binnen een organisatie. Dus betrek zoveel mogelijk mensen (medewerkers, omwonenden, toezichthouders) bij het waken over die veiligheid. Dat vraagt om samenwerking, voorlichting en herhaling. Want veiligheidsbewustzijn en eigen verantwoordelijkheid zakken snel weg. Na de terroristische aanslagen in Madrid in 2004 lette iedereen op onbeheerde koffers. Merkt u daar nu nog wel eens iets van?

ER IS AL LANGER EEN TREND om meer een beroep te doen op de eigen verantwoordelijkheid. Dat is alleen maar toe te juichen op voorwaarde dat regels worden gecontroleerd en er een gedegen handhaving is. Dat mag zowel door de overheid als het bedrijfsleven, bijvoorbeeld via keurmerken. Maar dan moet wel duidelijk zijn wie dat doet en moet er krachtig ingegrepen worden als dat nodig is. Een situatie zoals recent bij tankopslagbedrijf Odfjell in de Botlek is dan natuurlijk geen goed voorbeeld.

VAKORGANISATIES VORMEN een schakel tussen partijen op het gebied van veiligheid. Voor ons is dan ook een belangrijke rol weggelegd om de samenwerking en informatie-uitwisseling tussen overheid en bedrijfsleven te bevorderen."