

Van cybersecurity tot drones

# 6 TRENDS IN BEVEILIGING

Welke trends houden de Nederlandse beveiligingswereld bezig? Een overzicht van de hoofdpunten, met onder meer de instroom van jonge, hoogopgeleide security professionals, de integratie van fysieke en cybersecurity, de angst en roep om maatregelen na terroristische aanslagen en het toenemend besef dat preventie belangrijker is dan repressie. En natuurlijk drones, want 'gadgets' blijven hoe dan ook leuk.

DOOR ERIC DE VRIES CPP

**O**p gebied van beveiliging spelen de nodige trends. Hieronder een aantal op een rij.

## TREND 1. ROEP OM MAATREGELEN NA TERRORISTISCHE AANSLAGEN

De angst voor aanslagen zoals in Parijs heeft de Westerse wereld in zijn greep. Dat leidt tot angst en onzekerheid en vaak ook tot een roep om meer beveiliging. Maar hoe moet je je als bedrijf of organisatie (de Rijksoverheid blijft hier buiten beschouwing) daar nu tegen beveiligen? Kan dat wel, en is dat eigenlijk wel nodig? Dat zijn lastige vragen, vooral omdat het om perceptie gaat. Statistisch gezien is de kans op een verkeersongeval vele malen groter dan de kans slachtoffer te

worden van een aanslag. Maar het zit niet in onze aard om risico's rationeel te beschouwen. We willen maatregelen, want dat geeft een veilig gevoel.

Belangrijk is te zorgen voor een goede balans tussen risico en maatregel. Daarbij is essentieel een adequate respons gereed te hebben, en geen maatregelen te stapelen. Bij dit soort extreme dreigingen is veerkracht het belangrijkste. Weten hoe je moet handelen. Vandaar ook de Amerikaanse slogan over (school)shootings: 'run, hide, fight'.

Het heeft vooral zin om medewerkers te trainen in 'hoe' te handelen. Focus op veerkracht dus. Dat laat onverlet dat terroristische risico's – ook binnen uw organisatie – serieus en professioneel gewogen moeten worden en waar nodig tot beveiligingsmaatregelen horen te leiden. Maar wel rationeel.

## TREND 2. GROTERE VRAAG NAAR PARTICULIERE BEVEILIGING

Die trend houdt ook de beveiligingswereld bezig. Enerzijds leidt dat tot meer technische oplossingen (denk aan beveiligingscamera's) maar ook tot

**'DE INSTROOM VAN HOOGOPGELEIDE JONGE TALENTEN ZAL TOT VERDERE VERNIEUWING EN INNOVATIE LEIDEN'**



Cybersecurity kan niet bestaan zonder een gedegen fysieke basis. Wat is per slot van rekening het nut van een firewall als je zomaar de serverruimte in kunt lopen?

een vrij plotselinge vraag naar beveiligingsmedewerkers. Particuliere beveiligingsbedrijven kunnen de vraag nauwelijks aan. En dat terwijl ze nu juist vele jaren van krimp, reorganisatie, bezuinigingen en overleven achter de rug hebben. Het is typisch een voorbeeld van hollen en stilstaan. Want het is niet alleen de vraag om beveiligers vanwege de terreurdreiging, ook de vluchtelingenstroom en de aantrekkende economie leiden tot een grotere vraag. Dat is commercieel een goede ontwikkeling voor particuliere beveiligingsbedrijven, maar zet wel grote druk op het hoger en middenmanagement, waarvan er vele de laatste jaren noodgedwongen zijn afgevoerd. Qua aanbieders is er weinig veranderd, want de top 4 (Trigion, G4S, Securitas, NVD - (\* Fair Groep is in maart 2015 overgenomen door G4S) is al jaren min of meer gelijk.

‘Belangrijk is te zorgen voor de juiste balans tussen risico en maatregel’

Naam	Omzet (mln euro)	Fte
Trigion	375.0	6197
G4S	364.8	5028
Securitas	301.8	5076
NVD	32.5	470
Fair Groep *	17.0	222

Voor de complete top 10: zie Facto online van 7 juli 2015 <http://facto.nl/top-10-particuliere-beveiliging>

### TREND 3. CYBER EN FYSIEK, EEN NOODZAKELIJKE RELATIE

De cyberdreiging is niet meer weg te denken. Elke dag is er in het nieuws iets te vinden over DDoS-aanvallen, diefstal van persoonsgegevens en cyber warfare. Dat duidt niet alleen op een risicoverschuiving van fysiek (wat valt er – behalve infor-

matie – nu nog te stelen in het gemiddelde kantoor?) naar cyber. Het is ook een wake-upcall voor organisaties hoe kwetsbaar ze kunnen zijn. En dat is tegelijk een stimulans om fysieke beveiliging serieus te nemen. Want cybersecurity kan niet bestaan zonder een gedegen fysieke basis. Wat is per slot van rekening het nut van een firewall als je zomaar de serverruimte in kunt lopen? Maar een gezonde en begripvolle samenwerking tussen IT en beveiliging is niet vanzelfsprekend en gemakkelijk. Daar is nog een lange weg te gaan, en dat verdient de aandacht van het management. Dankzij de trend van analoog naar IP is trouwens geen enkele technische beveiligingsoplossing nog mogelijk zonder IT. De samenwerking kan dus van twee kanten groeien.

#### **TREND 4. VAN PASSIEF NAAR PROACTIEF BEVEILIGEN**

Veel menskracht en techniek inzetten om vervolgens te wachten op een incident was al nooit erg efficiënt. Dankzij de digitalisering en in het bijzonder 'big data' is het ook steeds minder nodig. De mogelijkheid om uit open bronnen informatie te verzamelen (denk aan sociale media) om te kunnen anticiperen op dreigingen heeft de weg geopend naar wat proactieve beveiliging wordt genoemd. Het is mogelijk om beveiligingsmedewerkers (maar zeker ook anderen) te trainen in het herkennen van afwijkend gedrag om op die manier te kunnen anticiperen op (bijna) incidenten. Deze werkwijze wordt onderwezen in cursussen zoals 'predictive profiling'.

Een vergelijkbare ontwikkeling is ook waar te nemen op tactisch en strategisch niveau. Daarbij richt de afdeling security zich veel meer op het anticiperen dan op repressie. Er is dan sprake van 'intelligence driven security'. Daarbij worden processen en technieken gebruikt voor het verzamelen en analyseren van informatie die afkomstig is uit de inlichtingenwereld. Dat klinkt misschien eng, maar dat is het niet. Het is een kwestie van je informatiepositie verbeteren. In het Engels klinkt het mooier. Als het goed wordt toegepast leidt het tot meer veiligheid voor minder geld, omdat de focus op de juiste prioriteiten ligt. Een ontwik-

**'Een gezonde en begripvolle samenwerking tussen IT en beveiliging is niet vanzelfsprekend en gemakkelijk'**

**'Elke security manager breekt zich het hoofd over hoe om te gaan met drones'**

keling die ook tot de broodnodige organisatorische innovatie in beveiliging zal leiden.

#### **TREND 5. DE GEVOLGEN VAN DRONES**

O ja, en natuurlijk breekt elke security manager zich het hoofd over hoe om te gaan met de dreiging van drones. Bij hoogrisico-objecten is dit zeker van belang. En voor beveiliging van evenementen is het een serieuze uitdaging. Maar het 'toys for boys'-gevoel is bij deze trend toch wel aanwezig.

#### **TREND 6. VERJONGING SECURITY PROFESSIONALS**

De 'boys' geven overigens nog steeds de toon aan in deze typische mannenwereld. Gelukkig zijn er veranderingen gaande. Zo is het aantal vrouwelijke security professionals in vakvereniging ASIS International Benelux Chapter de laatste jaren verdubbeld, maar het blijft een minderheid. Wel is er een sterke verjonging van de security professional te zien. Aanzienlijke groepen hbo'ers studeren af in integrale veiligheid, en recent werd de eerste lichte hbo'ers Security Management verwelkomd aan Saxion Hogeschool.

Die instroom van goed opgeleide jonge talenten met een gedegen theoretische kennis, zal tot verdere vernieuwing en innovatie leiden.

Want echte innovatie is nog steeds de meest opvallende afwezige trend. Innovatie die verdergaat dan meer van dezelfde slimme techniek, maar die echt bijdraagt aan het bedrijfsproces, is nu juist wat nodig is om positieve aandacht in de boardroom te krijgen. <<



Erik de Vries CPP is directeur/eigenaar van DutchRisk bv en Regional Vice President van ASIS International. ([www.DutchRisk.nl](http://www.DutchRisk.nl) en [www.ASISonline.org](http://www.ASISonline.org))