



## Het verslag van het seminar 'SecurityNext' - de beveiligingsomgeving van de toekomst

### SecurityNext: Het oog op de bal

*Op donderdag 3 oktober 2013 organiseerde Croon GBBS bij Universiteit Nyenrode in Breukelen het seminar 'SecurityNext'. Ongeveer tachtig beveiligingsexperts discussieerden over de invloed van maatschappelijke en technologische ontwikkelingen op de beveiligingsomgeving van vandaag, morgen en de toekomst. Wat betekenen big data en cybersecurity voor hen en voor u? What's next? SecurityNext!*



Waar gaan we naar toe met security? Waar staan we nu en wat is de volgende stap? Croon's accountmanager Security Jan Kouwenhoven bijt het spits af. "Elke achttien maanden verdubbelt de rekenkracht van computers. In 2029 zijn ze even slim als de mens", begint hij. "Al ruim voor die tijd beschikken we over bionische lenzen en kunnen we iemand identificeren aan de hand van zijn hartslagritme. Sterker nog: dat kan nu al. Wat een paar jaar geleden nog science fiction leek, is vandaag realiteit." In de realiteit van morgen krijgen we te maken krijgen met FMS en Business Intelligence, stelt Kouwenhoven: "Daarna wacht de uitdaging van kunstmatige intelligentie. Hoe gaan we daarmee om? Eén ding is zeker: hoe verschillend ons vertrekpunt ook is, de toekomst is voor iedereen gelijk."

### Wie is verantwoordelijk?

Cyber crime staat hoog op de agenda van de security manager, zegt Kouwenhoven. "Hoe beheers je de risico's voor je organisatie, wanneer medewerkers informatie in een dropbox stoppen, usb-sticks mee naar huis nemen of hun computer thuis open laten staan als de buurman langskomt? Wie is er verantwoordelijk voor de veiligheid: de afdeling IT of security? Te vaak nog zie ik verzuiling in de beveiliging." Een ander hot topic vormt Big Data: "Er is enorm veel informatie beschikbaar. Hoe vis ik daar precies de informatie uit die voor mij relevant is? En hoe combineer ik die data om iets te bereiken of juist te voorkomen?" Kouwenhoven geeft het voorbeeld van de Navy Yard Shooting in Washington, VS, september 2013: "Er vielen dertien slachtoffers. De dader, een voormalig werknemer van de Marine, werkte bij een onderaannemer van Hewlett-Packard en had een toegangspasje. In zijn tijd bij de Marine was hij herhaaldelijk op wangedrag aangesproken. Daarbuiten was hij betrokken bij verschillende incidenten waar vuurwapens aan te pas kwamen. In 2004 was hij al eens gearresteerd. Hij had geestelijke problemen en gebruikte antidepressiva. Een betere screening had naar alle waarschijnlijkheid veel ellende kunnen voorkomen."

## Ondersteunen

Een derde hot topic is het beheersen op afstand. “We willen met minder mensen situaties beter kunnen beheersen. Dat doen we vanuit centrale ruimten, op afstand. Daarvoor hebben we intelligente oplossingen nodig, zodat we de juiste procedure in gang kunnen zetten bij een dreiging.” Het laatste onderwerp dat Kouwenhoven agendeert is systeemintegratie en sensorfusie.

Croon GBBS ondersteunt organisaties bij hun beveiligingsvraagstukken. “Ons Innovatieteam is voortdurend bezig om antwoorden te formuleren op nieuwe uitdagingen. Onze wetenschappers vertalen de theorie naar de praktijk: waar is echt behoefte aan en welke oplossing is realistisch? Ze zijn er bijvoorbeeld in geslaagd software voor gezichtsherkenning te ontwikkelen en software te ontwerpen die laat zien dat er iets wordt ontvreemd uit een ruimte. Zo ondersteunen ze de security manager bij zijn vak.”

## De keerzijde van beveiliging

Na Kouwenhoven zet filosoof en hoogleraar Bas Haring veiligheid in een ander perspectief. “Wat is



veiligheid eigenlijk? Is dat een totale controle van je omgeving? Is dat het uitsluiten van ieder risico? Moeten we daar wel naar streven? Wat mij betreft: je kunt het ook overdrijven, er moet een balans zijn tussen beheersing en vrijheid.”

De risico's kunnen voorspellen is belangrijk om ze te kunnen beheersen. Maar dan nog is de vraag: hoe ver mag je gaan? Moet je preventief actie ondernemen om ellende te voorkomen? Mag je mensen arresteren omdat je denkt dat ze iets gaan doen? “Die vraag moet u zich stellen”, daagt Haring het publiek uit. “Aan beveiliging zit ook een keerzijde en die is niet per se positief.” Hij illustreert dit met een fragment uit de film 'Minority Report'. Die schetst een toekomst waarin een bijzondere politie-eenheid moordenaars kan arresteren voordat ze hun misdaden plegen. Uiteindelijk wordt een lid van het team zelf beschuldigd

van een toekomstige moord. “Het gaat altijd anders dan je verwacht”, betoogt Haring. “Meer camera's betekent niet per se dat de veiligheid toeneemt of dat je je veiliger voelt.” Een aanwezige reageert: “We dichten duizend gaten, maar een crimineel heeft er aan ééntje genoeg. Dat maakt ons vak zo oneerlijk, maar ook leuk.”

Het is een prachtig bruggetje naar het volgende punt van Haring: ook het beste protocol garandeert geen ultieme veiligheid. Als je weet wat je doet en de situatie vraagt erom, dan moet je een protocol ook terzijde kunnen schuiven. Ook dit illustreert hij met een filmfragment. “Gelukkig”, besluit hij, “is 100% controle ook helemaal niet nodig. Zoals één keurig paadje in een woeste tuin van Mien Ruis de suggestie van beheersing kan wekken, kan één maatregel de veiligheid vergroten. Het gaat erom dat het de juiste maatregel is.”

## Overdrijven is ook een kunst

Theo Stevens krijgt het woord. Hij is security manager van ING Insurance & Investment Management. “Ik geef hier mijn persoonlijke visie”, steekt hij van wal, “en ik zie het zó!” Als oud marine-man is Stevens op een gegeven moment de beveiliging in gegaan, een eigen bedrijf gestart en via verschillende opdrachtgevers in 2011 bij ING Insurance & Investment in dienst getreden als security manager. “In tien jaar tijd is niet alleen de wereld veranderd, maar ben ik dat ook. Vroeger was mijn motto 'security first' en kon er aan het protocol niet getornd worden. Inmiddels weet ik dat overdrijven ook een kunst is. Het gaat erom dat je de essentiële zaken beveiligt in een wereld vol bedreigingen en veranderingen. Houd je ogen op de bal.”

Hij noemt als voorbeeld van actuele bedreigingen het Nieuwe Werken, het ontslag van werknemers en de vlucht die het social media-gebruik heeft genomen. “We moeten kunnen omgaan met onbekwame medewerkers, groeiende inkomens- en cultuurverschillen, identiteitsdiefstal, cybercrime, bedrijfspionage en terrorisme. Als security kunnen we ons daarbij niet beperken tot óf de personele óf de fysieke beveiliging óf de IT: we moeten de uitdaging integraal oppakken, want we zijn zo sterk als de zwakste schakel.”



### **Ontzorg mij**

Totale controle is onrealistisch, zegt ook Stevens. “De ontwikkelingen dwingen ons richting risk-based beveiliging. We hoeven niet alles te weten, maar we moeten wel beseffen welke incidenten ons pijn kunnen doen - en waaróm ze dat doen. We gaan naar 'smart remote guarding' van onze panden, leggen meer nadruk op screening van werknemers en bevorderen de eigen verantwoordelijkheid van onze mensen. Dat noemen we 'awareness training'. We geven de BHV meer handen en voeten.”

Wat verwacht hij daarbij van zijn leveranciers? “Zij kunnen onze partner zijn. We moeten hen uitdagen om met slimme, betere en efficiëntere oplossingen te komen. Want uiteindelijk willen we geen product, maar een oplossing: ontzorg mij.”

### **Croon GBBS**

Croon GBBS, onderdeel van Croon Elektrotechniek, verzorgt beveiligingsoplossingen bij grootschalige organisaties, bedrijven en instellingen met een complex beveiligingsvraagstuk en/of een verhoogd risicoprofiel. Croon GBBS ondersteunt de professionalisering van het beveiligingsvak en de groeiende behoefte aan managementinformatie. Croon GBBS ontzorgt.