



*Peter Borghaerts*

## Computers vertellen hoe mensen moeten werken

**B**ij de start van 2017 hadden we een nogal roerig jaar achter de rug. Een jaar waarin hackers met gedurfde acties de show stalen. Zijn de Amerikaanse verkiezingen gemanipuleerd? Iedereen houdt zijn mond, maar de geruchtenmachine draait op volle toeren. Ook Nederland heeft gestemd, maar niet digitaal! Er speelt, achter de politieke schermen, dus duidelijk meer. Security kon niet worden gegarandeerd. Genoeg om er voor te zorgen dat wij allemaal het rode potlood ter hand moesten nemen.

Security is naar de top van de internationale prioriteitenlijst gestegen variërend van politiek tot defensie en van smart homes gekoppeld aan onze wereldwijde economische systemen. Met de nieuwe drones, kunstmatige intelligentie, New Media websites, robots, autonome auto's, slimme stadsinfrastructuren, en een overvloed aan Internet of Things (IoT) apparaten die dagelijks op de markt komen, rijst de vraag of we ons wel op de volgende generatie cyberaanvallen kunnen voorbereiden. Wat staat ons nog te wachten?

Er zijn verschillende trends zichtbaar of zoals de industrie zelf aangeeft 'projecties', want wie heeft de juiste glazen bol? De komende tijd, in een klein overzicht, kunnen we onder meer verwachten dat ransomware zal de cloud aanvallen en drone-jacking de terroristische bedreiging zal doen toenemen. Hacktivisten, jawel ze hebben een doel, zullen privacy issues aan de kaak blijven stellen. Met de komst van IoT-machines wordt de cyber-achterdeur vooral thuis, maar zeker ook bij bedrijven, wagenwijd opengezet. Ook worden digitale mobiele betaalsystemen steeds belangrijker, maar ook uitdagender voor fraude.

Maar tegen welke risico's lopen de gemiddelde werknemers aan op de New Media-kanalen? Bijvoorbeeld scammen. Oplichters maken fake accounts en sturen berichten naar jouw vrienden. Ongetrainde werknemers liken, delen en reageren en lopen met een aangemelde company telefoons zo de bedrijfsvloer op inclusief schadelijke apps, spyware en virussen. Door hen goed te trainen in goede social mediagewoonten voorkomt u een hoop ellende. Zorg ook voor een goed en duidelijk New Media beleid. Het consumentenvertrouwen zal verder worden aangetast door een explosieve groei aan nepberichten/advertenties en gekochte 'likes'. Tot slot zullen nepberichten de publieke opinie verder ondermijnen. In deze ChannelConnect staan een aantal prachtige bedrijven die dagelijks om moeten gaan met deze bedreigingen. Ik benijd ze niet en wens ze veel wijsheid en succes.

Ik vind de huidige mogelijkheden van New Media onder het motto 'vrijheid, blijheid' inspirerend en dynamisch. Ik juich het gebruik van alles met of zonder draadje toe. Maar het lijkt wel of mensen, net als baby's die net de nieuwe wereld aan het ontdekken zijn, eerst alles stuk moeten maken. We staan nog maar aan het begin van alle technologische ontwikkelingen, maar als ik de verwachte bedreigingen zie, gaan mijn haren overeind staan.

De mens vertelt de computer wat het moet doen, maar... zou het niet ethisch prachtig zijn, als computers ons zouden vertellen, hoe wij eigenlijk met hen moeten omgaan?

*Peter Borghaerts is Manager New Media  
Reageren? [peter@channelconnect.nl](mailto:peter@channelconnect.nl)*