



De Opiniepagina's zijn een platform voor debat. De verhalen mogen bij voorkeur niet langer zijn dan 700 woorden.



Lezersbrieven (maximaal 200 woorden) naar: redactie.secretariaat@bndestem.nl of Redactie BN DeStem, Postbus 488, 4870 AL Etten-Leur

► Wereldwijde cyberaanvallen kosten Nederland nu al jaarlijks ruim 8 miljard euro

Cybercrime, voor de bakker? Nee, het is juist 'een nooit gelopen race'

Voor veel burgers en mkb'ers is cybercrime een ver-van-ons-bed-show. Maar **we moeten juist samen alert zijn** en digitaal weerbaarder worden.

Ben Kokkeler en Roel de Beer

GASTOPINIE

Ruim een week geleden ging het als een schokgolf over de wereld: een wereldwijde cyberaanval veroorzaakte grote verstoringen in meer dan 150 landen. In Engeland werden ziekenhuizen korte tijd gesloten. In Nederland leek het allemaal mee te vallen. Het ging hier zijn gangetje na het weekend, ondanks ernstige waarschuwingen.

U hebt vast gedacht: cyberaanvallen, cybercrime, da's voor de bakker toch? De overheid regelt het voor mij?

De overheid, duizenden professionals in publieke organisaties, zijn inderdaad dagelijks in de weer met uw digitale veiligheid. Denk dan niet alleen aan defensie of politie, maar ook aan het openbaar vervoer, onderwijs, zorg, drinkwater- en energievoorziening, gemeenten. Overal waar gebruik gemaakt wordt van ict en internet is weerbaarheid tegen cyberaanvallen aan de orde van de dag.

Jaarlijks kosten cyberaanvallen in Nederland ruim 8 miljard euro, 1,5 procent van ons gezamenlijke bruto nationaal product. En dan rekenen we niet eens mee welk leed er berokkend wordt. Want bij cyberaanvallen denkt u natuurlijk – terecht – aan groot-schalige internationale aanvallen waardoor bijvoorbeeld telebankieren onmogelijk wordt, treinen niet meer rijden, of via zogeheten *ransomware* geld wordt afgeperst.

Maar dan vergeet u dat aloude vormen van pesten, bedreiging en afpersing ook moderne vormen hebben aangenomen. Onder ogenschijnlijk hippe Engelstalige



Het komende kabinet moet volgens experts veel meer doen aan digitale dijkverzwaring

woorden als *phishing* of *sexting* gaat een hoop ellende schuil. Denk aan ouderen die geld ontfutseld wordt of jongeren die via *fake* foto's seksueel bedreigd worden.

De waakhond van de Tweede Kamer voor nieuwe technologie, het Rathenau Instituut, spreekt niet voor niets in een recent rapport over 'de nooit gelopen race'. Voor elke 'slimme' oplossing die de overheid inzet, zijn er cybercriminelen die – vaak sneller – met een 'next generation'-aanval komen.

Er ligt zeker een taak voor onze Rijksoverheid. Nederland heeft een vooraanstaande

positie in wereldwijde internetknooppunten. Onze welvaart en ons welzijn hangen in hoge mate af van internettechnologie. Zoals vele experts momenteel betogen, moet het komende kabinet veel meer doen aan digitale dijkverzwaring. Onze open samenleving moet – ook digitaal – weerbaarder gemaakt worden om grootschalige aanvallen te kunnen weerstaan.

Daarin staan we niet alleen: de Europese Unie gaat strengere eisen stellen aan grote platformorganisaties zoals Google of Apple. En een buurland als Duitsland maakt van 'Datenschutz' veel werk.

Is daarmee, ook voor ons in Brabant, de cyberveiligheid voor de bakker? Nee. Ook de 'gewone burger' en 'de bakker op de hoek' moeten aan de slag. Zorg dat uw wifi thuis of in uw zaak, en dat uw apparaten goed beveiligd en *up-to-date* zijn. Denk na waar u waardevolle data opslaat, zorg voor *backups*. En denk ook vooral na over wat u via social media wel of niet deelt. Zo gek is dat toch niet? Wij willen graag leven in een open samenleving waarin we zelf beslissen hoe we samenleven, denken en doen, wonen en werken?

Onze Veiligheidsregio, de politie en burgemeesters in onze regio pakken de handschoen op. Zo ontwikkelt het aan de Veiligheidsregio gelieerde Dutch Institute for

Technology in Safety & Security innovatieprojecten. Gemeenten en politie werken samen in de opzet van nieuwe cybercrime teams. Kennisinstellingen slaan de handen ineen in het JADS instituut in Den Bosch dat big data-toepassingen ontwikkelt. Zorginstellingen werken samen om de digitale bestanden en de uitwisseling ervan beter te



Door bewust bezig te zijn met ons digitale rijgedrag kunnen we veilige digitale snelwegen benutten

beveiligen. Er zijn grote innovaties op til door verdere digitalisering in het openbaar vervoer en door introductie van zelfrijdende auto's. Ook in de telezorg worden in de komende jaren grote stappen gemaakt. Huishoudelijke apparatuur en kinderspeelgoed 'praten' via internet. Belangrijke ontwikkelingen voor een zelfredzame, 'groene' en duurzame samenleving die maken dat we dagelijks met digitale technologie zullen werken. Avans Hogeschool is in dit soort ontwikkelingen een belangrijke kennispartner.

GEVAARLIJKE RANSOMWARE



▲ ILLUSTRATIE JEAN GOUDERS

U als burger of als mkb'er kunt de kans grijpen digitaal weerbaar te worden. Ook daarin biedt Avans de helpende hand. Samenwerking is daarbij de sleutel. Een goed voorbeeld is Regio in Bedrijf, dat voor mkb'ers uit allerlei branches in juni een praktische studiedag belegt om goede tips uit te wisselen over het online gedrag van medewerkers. Het behoort inmiddels tot 'goed werkgeverschap' ervoor te zorgen dat medewerkers zichzelf digitaal weerbaar maken. Ook scholen hebben een belangrijke rol. Avans zelf, als grote werkgever en als gemeenschap van ruim 30.000 (jonge) mensen, heeft een belangrijke voorbeeldfunctie te vervullen. We moeten vroeg beginnen, praktisch en dichtbij de eigen leefwereld. Voor basisscholen en ouders is digitaal oefenmateriaal beschikbaar via Ouders Online, Alert Online, maar ook door inzet van grote internetproviders die verantwoordelijkheid nemen. Onze overheid zorgt voor veilige digitale snelwegen. Het is aan ons Brabanders die veiligheid en vrijheid goed te benutten, door bewust bezig te zijn met ons eigen digitale rijgedrag.

■ **Ben Kokkeler** is lector Digitalisering & Veiligheid bij Avans Hogeschool

■ **Roel de Beer** is docent Integrale Veiligheid bij Avans Hogeschool