



“Je gaat het pas zien als je het doorhebt”, zei een beroemde filosoof ooit. Misschien is dat de reden dat ik de indruk kreeg dat de berichten over cybercrime en cybersecurity elkaar de afgelopen tijd wel in een erg hoog tempo opvolgden. Saillant waren natuurlijk de nieuwsmeldingen over het hacken van politieke partijen in de VS, midden in een verkiezingstijd die toch al een historisch verloop heeft gekregen. Waarbij de verliezende kandidaat al veel langer onder vuur lag vanwege haar nogal onveilige gebruik van privé-e-mail voor overheidszaken. Over de herkomst van de hacks wordt – uiteraard – getwist, hoewel er enthousiast gewezen wordt naar de al net zo enthousiast ontkennde Russen. Maar duidelijk is dat Amerikaanse politici maar beter niet al te lichtzinnig met hun digitale veiligheid kunnen omgaan.

Dichter bij huis verscheen ‘Nederland digitaal droge voeten. De economische en maatschappelijke noodzaak van meer cybersecurity’, het adviesrapport dat onder auspiciën van PostNL-CEO Herna Verhagen tot stand kwam. Minister-president Mark Rutte en VNO-NCW-voorzitter Hans de Boer ontvingen het als eersten. Een zeer relevant stuk met concrete aanbevelingen voor zowel de overheid, het bedrijfsleven als de mensen thuis. Het maakt opnieuw duidelijk dat cybersecurity essentieel is voor onze economie en maatschappij, en dat de toenemende risico’s om forse investeringen vragen. Het is ontzettend belangrijk dat Verhagen met dit advies komt. Het laat zien dat we – met elkaar – hard moeten werken om onze bedrijven en samenleving beter te beschermen tegen cyberincidenten.

ALERT ONLINE: DREIGINGEN NEMEN TOE

Het publicatiemoment van het rapport-Verhagen was ook niet toevallig gekozen. Het viel precies in de periode van Alert Online, de tweewekelijkse campagne waarin overheid, bedrijfsleven en wetenschap aandacht vragen voor cybersecurity en cybersecure gedrag. De campagne van 2016 werd af-

gesloten met het Cyber Security Research Event, georganiseerd door onderzoekplatform dcypher.nl. De hoge opkomst maakt nog eens duidelijk dat cybersecurity een onderwerp van belang is. Ook het rapport ‘Cybersecuritybeeld Nederland’ toonde wederom helder aan dat de dreigingen toenemen en dat alertheid alleszins geboden is.

Nu heb ik al sinds lange tijd door dat cybercrime een groeiend fenomeen is, dat bijna inherent verbonden is aan de digitale transformatie waarvan we onderdeel uitmaken. Ik ‘zie’ de dreiging dagelijks in onze praktijk en ben automatisch gespitst op al het nieuws dat voorbij komt. Ik constateer ook dat er steeds meer aandacht wordt besteed aan dit onderwerp, wat ik alleen maar toejuich. Maar ik constateer tegelijkertijd dat we er met aandacht alleen niet komen. We zullen daadwerkelijk in actie moeten komen! We staan nog maar aan het begin van een steeds verdergaande digitalisering. Nederland heeft in de afgelopen jaren goede stappen gezet, maar het is hard nodig om door te pakken. Anders worden we ingehaald door de criminelen en door andere landen. Kijkend naar de gebieden waarop actie nodig is, wil ik hier inzoomen op twee punten: het Digital Trust Center en de kansen voor de Nederlandse economie.

DIGITAL TRUST CENTER

Het mkb moet beter worden beschermd tegen cybercrime. Het mkb is de banenmotor van onze economie en cybercrime heeft een steeds grotere economische impact op mkb-bedrijven. Enerzijds is er het gevaar beroofd te worden van bedrijfsgevoelige informatie of klantgegevens. Anderzijds worden bedrijven al maar vaker gegijzeld door ransomware. Dergelijke incidenten kosten ondernemers veel geld en belemmeren het succes van hun bedrijven. Voor velen, en dan met name binnen het mkb, is deze problematiek nog een ver-van-mijn-bedshow. Zij hebben het nog niet door. Tot ze zelf slachtoffer worden, dan zien ze de omvang van het probleem pas. Dat moet anders en dat kan ook anders. Op nationaal niveau moeten visie, beleid en investeringen gericht zijn op het behouden van onze koppositie als digitale en concurrerende economie. En daarbij vraagt het mkb specifieke aandacht. In dat kader wijs ik als bestuurslid van Nederland ICT graag op het manifest van Nederland ICT. Daarin

wordt gepleit voor het oprichten van een Digital Trust Center voor het mkb. Dit moet het mkb advies geven over cybersecurity en privacy. Op die manier versterken we de digitale economie en bevorderen we het ‘level playing field’. Uiteraard in een publiek-private samenwerking, want alleen dan kun je cybercrime oplossen.

STIMULANS

Security is ook een kans voor de Nederlandse economie. De sterke Nederlandse ict-sector kan nationaal en internationaal hoog scoren met het bieden van innovatieve securityoplossingen. Het cybersecurityspeelveld in Nederland biedt daarvoor een vruchtbare voedingsbodem, zo bleek tijdens het genoemde Cyber Security Research Event. De aangekondigde nieuwe subsidies die de overheid gaat verstrekken voor onderzoek en innovatie zijn een goede en welkome stimulans. Daarbij is mijn oproep wel om de

Security is ook een kans voor de Nederlandse economie

lat hoog te leggen. We hebben in Nederland immers de juiste industriële ingrediënten en opleidingen. Onderzoekers en overheid maken het mogelijk werkelijk onderscheidende oplossingen te ontwikkelen.

SCHERP HET VELD OPSTAPPEN

“Je gaat het pas zien, als je het doorhebt,” zo citeerde ik onze voetbalgrootmeester. Alle aandacht die cybersecurity de afgelopen periode kreeg, maakt hopelijk dat het tot iedereen in de Nederlandse samenleving – van overheid én bedrijfsleven tot de gewone burger – doordringt dat cybercriminelen hun ‘vak’ benaderen als topsport. Als iedereen dat doorheeft, kan het niet anders dat ook het besef komt dat je daarop alleen maar kunt reageren door net zo scherp het veld op te stappen. Geen kansen weggeven, maar ze zelf creëren: dat zou ons gemeenschappelijke doel moeten zijn. Ik wens u een prettige wedstrijd!

Ron de Mos is senior vice president en general manager van CGI in Nederland.