TECHNOLOGIE

Mkb achilleshiel bij cybercrime, meer hulp overheid en bedrijfsleven nodig

- **Cyberveiligheid blijft voor mkb te veel bijzaak**
- Strengere regels dwingen orde op zaken te stellen
- Ketenaanpak belangrijk voor vestigingsklimaat

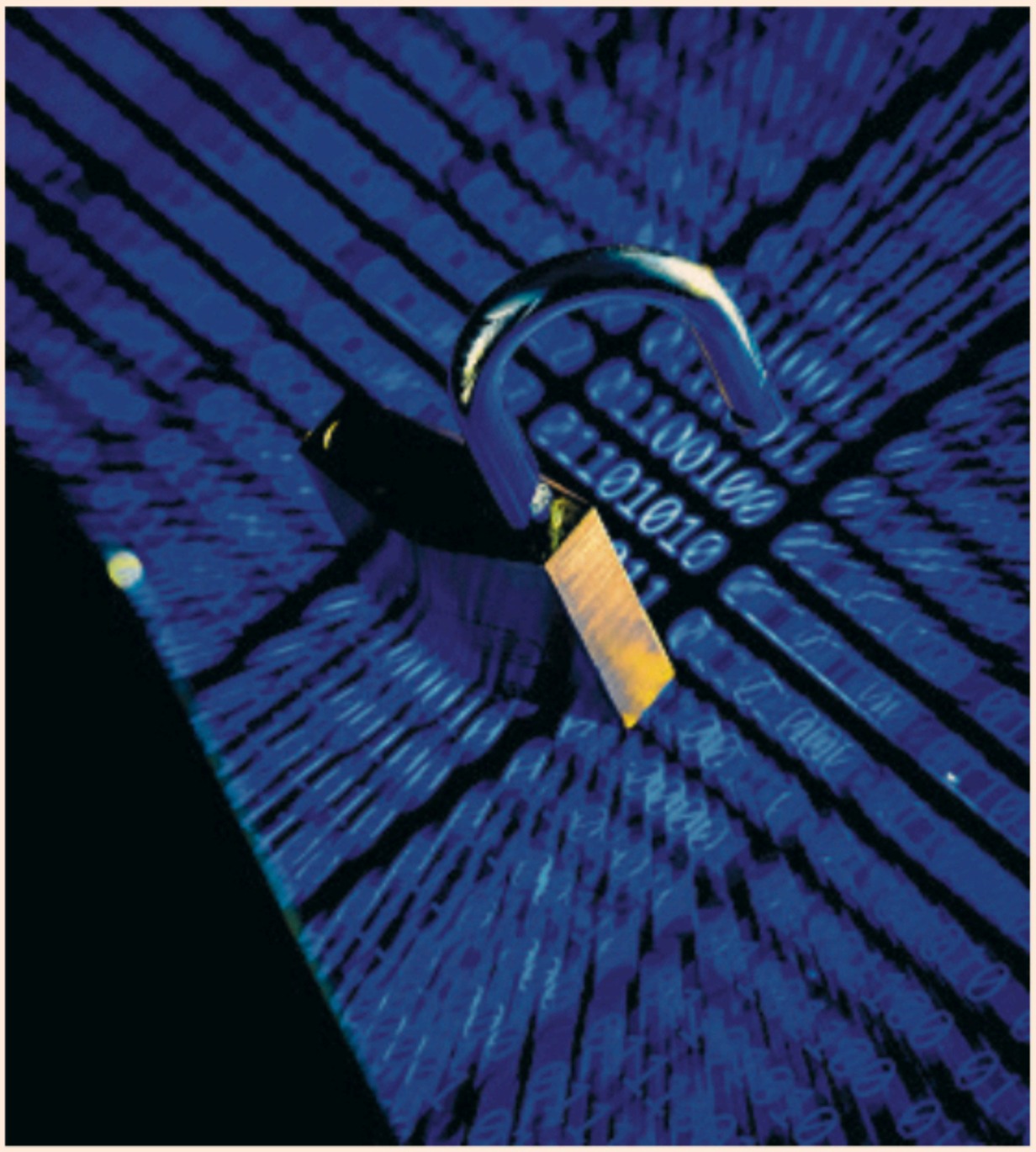
Ardi Vleugels
Amsterdam

Kleine en middelgrote bedrijven lopen achter met hun cyberveiligheid, zegt de Cyber Security Raad (CSR). Vaak weten ze niet wat ze moeten doen of waar ze moeten beginnen. Informatie over veilig werken bereikt hen onvoldoende en is te versnipperd. De raad adviseert het Rijk in te grijpen met meer praktische hulp, zoals een overheidsloket voor ondersteuning. Ook moet er een keurmerk komen voor ICT-leveranciers, zodat duidelijker is wat veilig te gebruiken producten of diensten zijn.

Deloitte onderzocht voor de CSR welke obstakels binnen het mkb spelen, waardoor er veel achterblijvers zijn. Mkb'ers blijken zich minder bewust van de risico's en zien soms door de bomen het bos niet meer, staat in het rapport. Het gevolg is dat ze minder risicoanalyses uitvoeren en minder maatregelen nemen.

'Het mkb vormt de ruggengraat van onze economie', zegt CSR-covoorzitter Theo Henrar. 'Tegelijk zien we dat het mkb nadrukkelijk doelwit is van cybercriminelen. Onvoldoende cyberweerbaarheid is een risico voor het voortbestaan van het bedrijf zelf, maar door de onderlinge verbondenheid van bedrijven ook voor de hele bedrijfsketen en daarmee voor het functioneren van onze samenleving.'

> **'Als jij niet veilig werkt, kiest jouw opdrachtgever sneller voor een ander die dat wel doet'**



Mkb-bedrijven lopen achter met cyberveiligheid. FOTO: KOEN VAN WEEL/ANP

Bart Groothuis is medebedenker van nieuwe Europese richtlijnen voor cyberweerbaarheid NIS2, die in Nederland in 2025 ingaan. NIS2 zal gelden voor alle bedrijven met minimaal vijftig medewerkers en €10 mln omzet die essentiële diensten verlenen. Per sector komt er een cybertoezichthouder en een meldingsplicht en NIS2 stelt besturen verantwoordelijk voor cyberincidenten, met sancties als zij onvoldoende bijsturen.

Groothuis steunt het pleidooi dat de overheid ondernemers gerichter moet helpen. 'Door NIS2 moeten ondernemers meer werk maken van cyberveiligheid, met als ultiem middel dat er boetes volgen. Maar de geest van die wet is óók dat bedrijven daarbij een helpende hand krijgen.' Zo moet wie onder NIS2 valt een informatiepakket kunnen krijgen. Nu is het aan de bedrijven zelf om uit te zoeken welke verplichtingen ze straks hebben.

Hij voegt daaraan toe dat de overheid ook infrastructuur kan bouwen die ondernemers ontzorgt. Nederland kan daarvoor afkijken bij andere landen. De Belgen krijgen bijvoorbeeld een rood scherm te zien als ze op een website klikken waarmee malware dreigt te worden geïnstalleerd. Dat heeft de overheid gebouwd en met internetserviceproviders uitgerold. En in Canada tekenden 850.000 bedrijven en overheden vrijwillig in op een overheidsprogramma dat op de systemen meekijkt naar ransomware en statelijke actoren.

Volgens de raad zijn kleine bedrijven zich ook minder bewust van cyberrisico's voor anderen in de digitale keten waarin ze werken. Terwijl grotere partijen met de komst van de scherpere Europese NIS2-regels wel vaker van hen gaan eisen dat ze hun cyberveiligheid op orde hebben, om zich voor incidenten en sancties te behoeden.

Rodrique Engering van de raad van bestuur van de Kamer van Koophandel (KvK) constateert dat dit besef nog niet is ingedaald. 'Wij bieden ondernemers online informatie en hebben bedrijfsadviseurs die we hebben opgeleid in cyberveiligheid. Maar we zien geen extra verkeer naar die hulp.' Dat baart hem zorgen. 'Veilig werken wordt straks *your license to operate*. Het helpt je om zaken te kunnen blijven doen. Als jij niet veilig werkt, zal jouw opdrachtgever sneller voor een andere partij kiezen die dat wel doet.'

De CSR adviseert om partijen als de KvK en brancheorganisaties in te zetten om kleine ondernemers gerichter te bereiken. Engering vertelt dat zij die rol al op zich nemen: er zijn onlinestappenplannen en offline-informatiesessies en de KvK overweegt landelijke spotjes. 'We wachten met smart op de Nederlandse uitwerking van de NIS2-regels, zodat wij ondernemers nog beter kunnen informeren.' Engering denkt dat bestuurders van kleinere ondernemingen vaak wel weten dat cyberveiligheid van belang is. 'Maar als een ondernemer alles in het bedrijf zelf wil regelen, is het toch een onderwerp dat snel op de lange baan wordt geschoven. Terwijl het enorme schade kan opleveren, ook aan klanten en leveranciers.' Cyberveiligheid hoort bij gezond ondernemerschap, benadrukt Engering. 'Als je in Nederland gaat ondernemen, moet je partijen kunnen vinden in een betrouwbaar handelsregister en je moet ervan uit kunnen gaan dat je veilig zakendoet met deze partijen.' Die garantie is nodig om buitenlandse ondernemingen en investeringen aan te trekken. 'Cyberveiligheid is net zo'n belangrijk thema voor ons vestigingsklimaat als lage belastingen.'