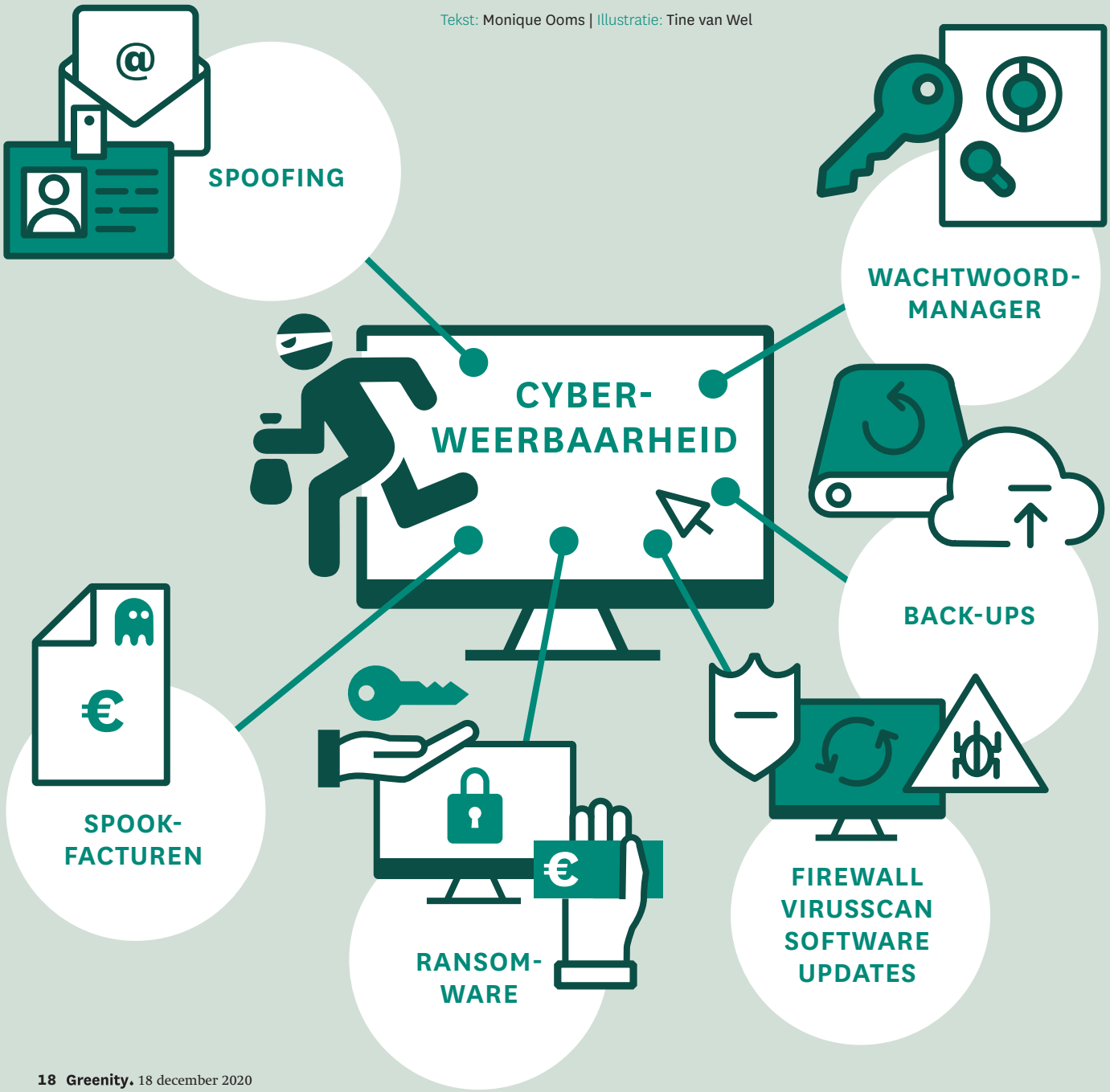
‘Ook kleine kwekers interessant voor hackers’

De gemiddelde ondernemer doet van alles om zijn bedrijf te beveiligen, ook in de groensector. Hekken om de bedrijfsterreinen, goede sloten, een alarmsysteem en bewegingssensoren op het bedrijfspand en het perceel. Maar de bescherming van digitale gegevens is voor verbetering vatbaar. Veel ondernemers lijken te denken dat ‘het niet zo’n vaart loopt’. Misschien omdat de cyberdief onzichtbaar is. Maar hij is er wel degelijk en loert ook op kleine ondernemingen.

Tekst: Monique Ooms | Illustratie: Tine van Wel



Bedrijven anno nu doen er goed aan om hun cyberweerbaarheid op orde te krijgen, stelt Joris den Bruinen, directeur van stichting The Hague Security Delta (HSD), een netwerk van bedrijven, overheden en kennisinstellingen die samenwerken aan kennisontwikkeling en innovatie op het gebied van veiligheid. “Belangrijk is dat je voldoende bent uitgerust tegen de risico’s in het digitale domein. Dat geldt overigens voor alle ondernemingen, niet alleen voor de hele grote. Het is een misverstand om te denken ‘bij mij valt niks te halen, dus ik ben veilig’. Een inbreker kijkt namelijk altijd waar hij het makkelijkst kan binnenkomen. Naarmate banken en grote bedrijven hun cyberweerbaarheid beter op orde hebben en hacken lastiger wordt, verschuift de aandacht meer naar de vaak kleinere bedrijven die de veiligheid nog niet op orde hebben.” Om een beeld te geven: “Zo’n 50 procent van de mkb’ers is slachtoffer van een vorm van cybercrime.”

ALLES KWIJT

Alle data kunnen relevant zijn voor hackers. “Ze kunnen je bedrijfsgegevens gijzelen en alleen teruggeven tegen betaling van flinke bedragen, de zogenaamde ransomware. Bovendien kunnen hackers via jouw gegevens weer terechtkomen bij andere partijen waarmee jij zaken doet. Dus doordat jij jouw digitale veiligheid niet op orde hebt, kun je ook een ander duperen.” Den Bruinen kent diverse praktijkvoorbeelden van bedrijven die werden gehackt. “Een fotograaf was gehackt en raakte al zijn bestanden kwijt. Hij wilde de ransomware niet betalen en nam een IT-security bedrijf in de arm. Zij konden 80 procent van de data terughalen. Dat bleek uiteindelijk te gaan om 80 procent per foto, dus daar had hij alsnog niets aan. Uiteindelijk is hij failliet gegaan. Dit gebeurt vaker.”

De sierteeltsector kan hard worden geraakt door cybercriminelen, stelt Den Bruinen. “Je wilt je vanzelfsprekend richten op groeien en bloeien, maar zult ook je digitale risico’s moeten afdekken. In de sierteeltsector wordt veelal in ketens gewerkt. Een kweker werkt bijvoorbeeld samen met een installatiebedrijf, een kassenbouwer en een leverancier van gewasbeschermingsmiddelen. Er gaan bestellingen en betalingen over en weer, steeds meer digitaal. Via de kleine kweker kan de hacker bij die andere bedrijven binnenkomen. De cybercrimineel kan ook jouw identiteit overnemen en bijvoorbeeld namens jou aankopen doen op de veiling. Processen zijn enorm gedigitaliseerd en dat maakt ons ook kwetsbaarder. Belangrijk is dus dat je hierop actie onderneemt. Je ziet de digitale dief niet, maar hij is er wel degelijk. Dat is misschien ook de reden dat veel mensen het onderschatten.”

GIJZELEN OF STELEN

Den Bruinen zet op een rij wat er zoal mis kan gaan. “Cybercriminelen kunnen je data gijzelen, je identiteit stelen en vervolgens op jouw naam bestellingen doen, indringen in je systemen en apps waardoor ze bijvoorbeeld de temperatuur in je koelcel veranderen of je waterpomp kunnen overnemen. Ook kun je denken aan spoofing, waarbij hackers via een trucje proberen jouw digitale identiteit over te nemen. Ze sturen bijvoorbeeld een mail uit jouw naam naar een van jouw relaties met de opdracht om geld over te maken naar een rekening. Of ze doen zich voor als de bank en vragen om je gegevens. Ook gebeurt het steeds vaker dat mensen via WhatsApp gehackt worden. En dan kennen we natuurlijk nog de spookfacturen die bedrieglijk veel op de echte facturen kunnen lijken.”

Wilt u meer weten over cyberveiligheid, scan dan deze QR-code met uw telefoon.

Cyberweerbaarheid is dus belangrijk, maar hoe pak je dat aan? “Als bedrijf begin je met een inventarisatie van de risico’s. Je kunt hiervoor de basisscan cyberweerbaarheid gebruiken van het Digital Trust Center (DTC) dat valt onder het ministerie van Economische Zaken of een cyber security specialist inhuren. Hiermee kun je in kaart brengen welke acties je moet ondernemen om cyberweerbaar te worden.” Den Bruinen maakt daarbij onderscheid tussen technische voorwaarden, beleidsprocessen en personeel. “Bij technische voorwaarden kun je denken aan zaken als een firewall, een virusscan, wachtwoorden en software updates. Doe die updates vooral, de verbeterde softwareversies zijn namelijk beter bestand tegen hackers.” Over het proces vertelt hij: “Maak afspraken met je IT-leverancier over wie waarvoor verantwoordelijk is bij incidenten. Zorg dat er back-ups van je data worden gemaakt en check of dat ook echt gebeurt. Doe je het zelf of je IT- leverancier? Tref daar dan voorzieningen voor en/of regel het in. Zoek uit wie je kunt bellen als er problemen zijn, bij voorkeur 24/7. Criminelen zitten namelijk over de hele wereld en houden zich niet aan onze kantoortijden. Belangrijk is dat je de telefoonnummers van de benodigde hulplijnen in zo’n situatie in je telefoon hebt.”

DIGITALE KLUIS

Personeel is ook een belangrijke factor in cyberweerbaarheid. “Zorg ervoor dat zij zich bewust zijn van de risico’s. Dat ze bijvoorbeeld weten dat ze niet op links moeten klikken, dat ze spookfacturen herkennen, hoe ze moeten omgaan met wachtwoorden, enzovoort. Daarbij gaat het niet alleen om bewustzijn, maar vooral ook om bewust bekwaam zijn.” Een goed wachtwoord maken, blijkt nog niet eenvoudig. “Voor de hand liggend is de naam van je favoriete voetbalclub, je vrouw of je kinderen. Hackers komen daar eenvoudig achter door op jouw social media accounts te kijken. Dus kies voor een woord dat online niet aan jou te koppelen is, en kies voor een combinatie van cijfers en (hoofd)letters, of een zin die jij kunt onthouden. Een hulpmiddel hierbij is de wachtwoordmanager, een digitale kluis waarin je al je wachtwoorden kunt opslaan.”

Jezelf en je bedrijf cyberweerbaar maken is in de praktijk niet heel complex, benadrukt Den Bruinen. “Je moet het vooral gewoon doen. Als je ermee aan de gang gaat, blijkt het allemaal niet zo ingewikkeld te zijn.” Om de cyberweerbaarheid in de tuinbouw in de regio West-Holland te vergroten is HSD een samenwerking aangegaan met Greenport West-Holland. “Via een nulmeting brengen we de huidige cyberweerbaarheid in kaart. Vervolgens is ons doel om hierin via een actieprogramma rond bewustwording en handelingsperspectief stappen vooruit te zetten en over twee tot drie jaar opnieuw te meten waar we dan staan.” Dit idee is goed ontvangen door de sector. “Tegelijkertijd staan nog niet veel ondernemers te trappelen om aan de slag te gaan. Onbekend maakt onbemind. Daar gaan we dan ook op inzetten. Want dat het belangrijk is, is wel zeker. Uiteindelijk zit niemand erop te wachten om in de problemen te komen door digitale criminaliteit.”