ONDERNEMEN

Gabi Ouwerkerk

Het laatste nieuws over zaken die ondernemers raken. Tips en ideeën? Mail naar **ondernemen@dft.nl**

Groeigeld voor omscholingsplatform

Online onderwijsplatform Winc Academy heeft een investering opgehaald van $3 miljoen. De nieuwe financieringsronde wordt geleid door Rubio Impact Ventures en Dutch Founders Fund. Ook Vivid Ventures, het investeringsfonds van Heleen Dura-Van Oord dat in 2019 de eerste financieringsronde leidde, doet mee.

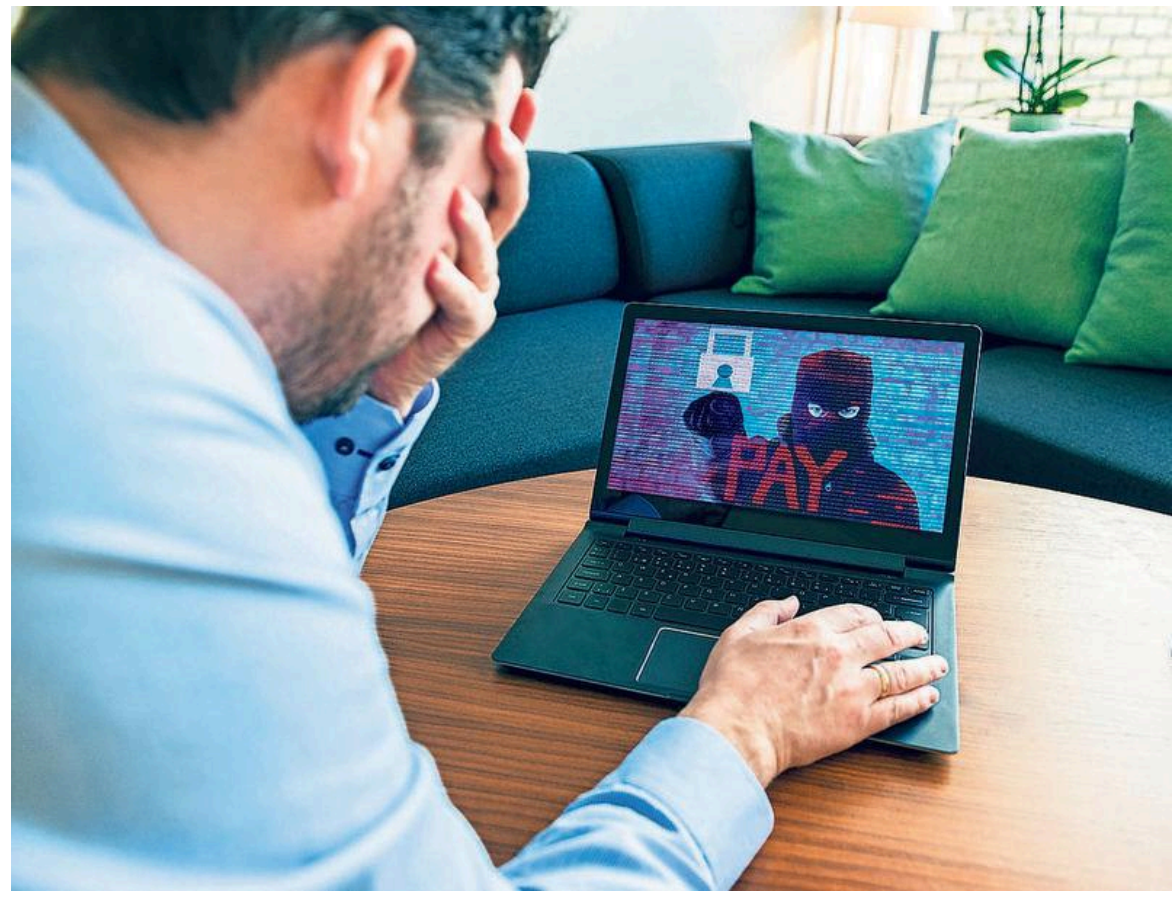
Met het groeigeld wil de Amsterdamse scale-up binnen een paar jaar 20.000 volwassenen voorbereiden op een baan als programmeur, data-analist of een andere techcarrière. Winc is in 2018 opgericht met als doel het personeelstekort in de technologie-industrie te bestrijden. In slechts zes weken tijd kan het platform studenten de basisbeginselen van het programmeren bijbrengen, waarna ze direct als junior bij een bedrijf aan de slag kunnen.

COMMUNITY-BOUWER

InSided nu Amerikaans

De Amsterdamse softwareontwikkelaar InSided is overgenomen door zijn Amerikaanse branchegenoot Gainsight. Een overnamebedrag is niet bekendgemaakt, maar naar verluidt gaat het om een bedrag van €75 miljoen.

Het eind 2010 door Robin van Lieshout en Wouter Neyndorff (foto) opgerichte InSided ontwikkelt software waarmee bedrijven zelf een online gemeenschap kunnen bouwen. Hoewel het bedrijf met klanten als T-Mobile, Zapier en Dyson de omzet en het klantenbestand nog steeds zag groeien, denkt het onder leiding van Gainsight het groeitempo te kunnen versnellen.



Vraag jezelf af hoeveel schade je oploopt als je een dag geen toegang hebt tot je voorraadbeheer, kassysteem of e-mail.
FOTO GETTY IMAGES

Cybercriminaliteit neemt toe, ook in het mkb

'Breng risico in kaart'

door **Gabi Ouwerkerk**

AMSTERDAM • Cybercriminelen die bedrijfsnetwerken platleggen en losgeld eisen om de boel weer aan de praat te brengen. Als kleine ondernemer lees je erover, maar menigeen denkt dat het hem of haar niet zal overkomen omdat er niets te halen valt. „Je hoeft geen doelwit te zijn om slachtoffer te worden", waarschuwt echter Petra Oldengarm, directeur van brancheorganisatie Cyberveilig Nederland.

Het zijn vooral aanvallen op grote bedrijven die in het nieuws komen, zoals de aanval vorig jaar op Bakker Logistiek. Hierdoor kwamen onder andere kaasleveringen aan distributiecentra van klanten stil te liggen, wat lege schappen in de supermarkt veroorzaakte. Dit soort aanvallen heeft grote economische impact, raakt meerdere ketens en krijgt veel aandacht. Een aanval op de bakker op de hoek is economisch gezien minder erg, maar raakt de getroffen ondernemer keihard.

Uit onderzoek van de Haagse Hogeschool blijkt dat één op de vijf mkb'ers slachtoffer is geweest van cybercriminelen en daar schade van heeft ondervonden. Oldengarm raadt elke ondernemer aan goed in kaart te brengen welke systemen aangesloten zijn op internet en dus een doelwit kunnen zijn. „Vraag jezelf af hoeveel schade je oploopt als je een dag geen toegang hebt tot je voorraadbeheer, kassysteem of e-mail en wat als je hele productieketen stil komt te liggen?"

Petra Oldengarm, directeur van Cyberveilig Nederland
FOTO ARENDA OOMEN

Vergissen

Het klopt volgens Oldengarm dat veel ransomware-aanvallen zich richten op grote bedrijven, omdat daar vaak meer te halen valt. Maar zij wijst er tegelijk op dat er ook veel kruimeldieven zijn naast professionele cybercriminelen. „Die blijven met hagel schieten tot ze een doel treffen." Bovendien vergissen ondernemers zich volgens haar als ze denken dat er bij hen niets te halen valt.

Cybercriminelen verhandelen databases met e-mailadressen en gelekte wachtwoorden op de zwarte markt. Die gegevens kunnen vervolgens gebruikt worden om in te breken op bedrijfsnetwerken van ondernemers. Veel mensen gebruiken namelijk nog steeds dezelfde inloggegevens voor meerdere systemen."

Gestolen inloggegevens kunnen de sleutel vormen voor een ransomware-aanval. Als cybercriminelen eenmaal binnen zijn op een netwerk, kunnen ze vaak ongestoord rondneuzen, op zoek gaan naar vertrouwelijke informatie of onderzoeken hoe ze systemen plat kunnen leggen. Uit onderzoek van veiligheidsbedrijf Sophos blijkt dat hackers in de eerste maanden van 2021 gemiddeld 264 uur of elf dagen in een aangevallen netwerk zaten voordat zij werden ontdekt. De langst onopgemerkte inbraak duurde wel vijftien maanden.

'Firewall en virusscanner niet meer voldoende'

Basismaatregelen, zoals een firewall, virusscanner, multifactorauthenticatie en back-ups, zijn door de veranderde dreigingen niet meer voldoende om een netwerk te beschermen. „Alleen een slot op de deur voldoet niet meer. Je hebt ook een inbraakdetectiesysteem nodig", duidt Oldengarm, die benadrukt dat beveiligingsbedrijven meer moeten doen om het mkb hierbij te helpen. „De oplossingen zijn nu nog vaak complex en de kosten zijn veelal hoog. Het ontbreekt nog aan gestandaardiseerde beveiligingspakketten die zich specifiek richten op kleine mkb-bedrijven."

Risicoklasse

Bovendien verschillen de risico's die mkb-bedrijven lopen enorm per bedrijf en sector en daarmee ook de maatregelen die zij moeten treffen. Een goede eerste stap voor ondernemers die risico's in kaart willen brengen is volgens Oldengarm de risicoklasse-tool op de website van het Digital Trust Center (DTC) van het ministerie van Economische Zaken en Klimaat.

Deze bij ondernemers nog relatief onbekende overheidsinstelling is in het leven geroepen om bedrijven weerbaarder te maken tegen hackers. Waar het Nationaal Cyber Security Centrum (NCSC) zich richt op de bescherming van vitale organisaties als energiebedrijven, banken en de Rijksoverheid, daar richt DTC zich op bedrijven van groot tot klein.

„Zodra je als ondernemer weet welke risico's je loopt, kun je de afweging maken of je wilt investeren om het risico te verminderen", aldus Oldengarm die ondernemers op het hart drukt te allen tijde te zorgen voor het nemen van basismaatregelen zoals een goede back-up: „En bewaar die niet alleen digitaal, maar ook fysiek in bijvoorbeeld een kluis."

'Kruimeldief blijft met hagel schieten'

VRAAG & ANTWOORD

Doorlopend contact met de Belastingdienst

Ik las over horizontaal toezicht door de Belastingdienst? Wat is het voordeel hiervan? En hoe kom ik hiervoor in aanmerking?

HANS BIESHEUVEL
OPRICHTER ONDERNEMERSORGANISATIE ONL

Bij horizontaal toezicht verandert de relatie met de Belastingdienst. In plaats van een controle volledig achteraf vindt er lopende een periode contact met de Belastingdienst plaats over verplichtingen en onduidelijkheden. Je krijgt één aanspreekpunt en je hebt sneller duidelijkheid over je aangiften en fiscale positie.

Er zijn in principe geen naheffingsaanslagen achteraf en je kunt in gesprek over veranderingen die er altijd wel zijn in een bedrijf. Je bent niet afhankelijk van de interpretatie van de controlemedewerker, maar kunt in gesprek met de klantmanager van de Belastingdienst. Loopt het allemaal anders dan verwacht? Dan zoek je samen een oplossing. Ook als het, zoals nu door corona, gaat om een betalingsregeling voor de komende jaren. Het idee is dat je er altijd samen uit probeert te komen.

De eerste ervaringen zijn positief. De Belastingdienst heeft convenanten gesloten met individuele bedrijven, fiscaal intermediairs en brancheorganisaties.

De Belastingdienst meldt zelf dat 'wederzijds vertrouwen' de basis voor horizontaal toezicht is. Transparantie en elkaar begrijpen zijn daarbij belangrijk. Horizontaal toezicht geeft je beter inzicht in je eigen administratie en als je het goed aanpakt, heb je er zelf baat bij.

Ook een vraag voor Hans Biesheuvel? Vragen@dft.nl