Be safe
IT Local zorgt voor een veilige werkplek

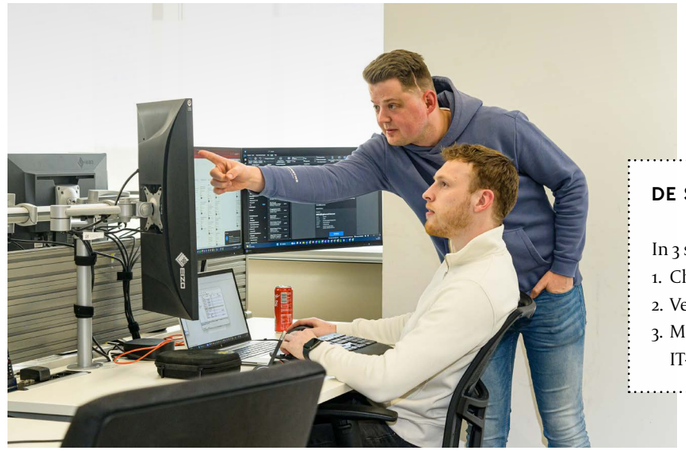
TEKST: KOPPIE COPY | FOTOGRAFIE: JAN ADELAAR

Met een kleine 40 medewerkers werkt **IT Local**, gevestigd op Industriepark Kleefse Waard in Arnhem, dagelijks aan het ontwerpen, leveren en beheren van veilige cloudwerkplekken. En dat is zeker in deze tijd, waarin succesvolle hackpogingen aan de orde van de dag zijn, geen overbodige luxe. Directeur **Remko Kleij** en marketing- en communicatiemanager **Theo Kroon** vertellen over hoe zij er met hun team voor zorgen dat de werkplek die zij inrichten bestand is tegen kwaadaardige aanvallen.

"Wij werken vanuit het PPT Framework, daar vertelden we in een eerdere editie van Arnhem en Nijmegen Business al over," aldus Remko. "People, Process, Technology, daar draait het om. Daarin staat de mens centraal. Technologie staat enkel in dienst van de mens en het optimaliseren van processen. Ook in de security-roadmap die we hebben ontwikkeld is de mens het startpunt: wie is jouw medewerker, welk type mens, als we dat zo mogen zeggen, is hij of zij en is er wellicht al enige IT-kennis aanwezig? Als we daar een beeld bij hebben gaan we verder."

DE ROADMAP-GEDACHTE

"Alles begint met bewustwording," vult Theo aan. "Het risico wordt steeds groter. Steeds vaker zijn bedrijven het doelwit van hackpogingen. En die pogingen worden almaar gehaaider. Met de mogelijkheden die ChatGPT biedt bijvoorbeeld worden mails opgesteld die er zo echt uitzien dat je al snel verleid raakt om de mail te openen. Met alle gevolgen van dien. Je moet echt heel goed uitkijken. Zelfs de professional, de medewerker die zich heel bewust is van de gevaren die er zijn, kan er intuinen."
"We zeggen dan ook nog weleens gekscherend dat het grootste veiligheids-



DE SECURITY JOURNEY

In 3 stappen naar een veilige werkplek:
1. Check: hoe veilig is jouw IT-omgeving
2. Verbeter: aanpassen van de IT-omgeving.
3. Monitoring en gedrag: hou de IT-omgeving veilig.

> "Het grootste gevaar zit tussen het toetsenbord en de stoelleuning"

risico tussen het toetsenbord en de rugleuning van de bureaustoel zit, aldus Remko."

"We beginnen met een inventarisatie: waar sta je nu en waar zou je met het type bedrijf dat je hebt moeten staan qua veiligheidsmaatregelen? Als we dat helder hebben maken we in nauwe samenwerking met de ondernemer een plan om te komen tot waar je zou moeten zijn. Oplossingen hoeven daarbij zeker niet altijd duur te zijn. Soms doet een eenvoudige 2-stapsverificatie al heel veel."

PERSOONLIJKE AANSPRAKELIJKHEID

"Met de geüpdate versie van de Europese security-maatregelen, de NIB2, die dit jaar is ingegaan, zijn er strengere eisen rondom netwerk- en informatiebeveiliging ingegaan. Die gelden op dit moment nog alleen voor bepaalde organisaties, maar de scope aan bedrijven die hieronder gaan vallen wordt steeds groter. Belangrijk om te weten is dat, mocht je slachtoffer worden van een datalek of iets dergelijks, je niet zomaar jouw IT-partner daar verantwoordelijk voor kunt stellen. Jij, als eigenaar van het bedrijf, bent voortaan persoonlijk aansprakelijk."

WEES JE BEWUST VAN DE GEVAREN

"Alles staat of valt met het bewust zijn van wat er kan gebeuren. We steken dan ook veel tijd in de bewustwording van de medewerkers en geven daarbij eenvoudige tips als: noteer nooit wachtwoorden, zorg dat je je computer lockt als je even van je plek gaat en laat geen usb-sticks slingeren. Je zult versteld staan hoe vaak dit soort simpele zaken nog voorkomt. Naast bewustwording monitoren we ook. Met de test-app die we ontwikkeld hebben bijvoorbeeld, waarmee we mails rondsturen om te zien of er ongeoorloofd toch op geklikt wordt. Is dit het geval dan gaan we opnieuw het bewustwordingsproces in."

DATA VEILIGSTELLEN

"Wij zorgen ervoor dat de werkplek veilig is. Mocht het alsnog voorkomen dat er iets mis gaat – en ga ervan uit dat we allemaal een keer aan de beurt komen – dan zorgen wij ervoor dat je zo snel mogelijk weer operationeel bent met zo min mogelijk dataverlies. Als het nodig is, schakelen we daar onze partners bij in die gespecialiseerd zijn in het blussen van digitale brandjes. Door de samenwerking met externe partijen blijven we scherp en kunnen we de veiligheid van de werkplek continu optimaliseren. Het is toch een soort van wedloop: aan de ene kant staan wij, aan de andere kant de hackers. Wij staan klaar en testen met professionele ethische hackers regelmatig ons platform om te zien of en hoe snel zij binnen kunnen komen. En nemen we waar dat nodig is maatregelen. In de hybride wereld waarin we leven en werken zorgen wij voor een gestandaardiseerde werkplek waarbinnen alles veilig kan draaien. We werken daarbij op profielbasis: op basis van de functie in kwestie wordt de werkplek ingericht. Zo voorkom je dat er onnodig dure werkplekken worden ingeregeld en ben je veilig tegen zo laag mogelijke kosten." ■

Meer weten over hoe IT Local jouw werkplek veilig houdt?
www.itlocal.nl