KLANTVERHAAL

Avantage
MAKES IT SIMPLE

JE MOET HET GEWOON DOEN!

cybersecurity is bij thuiscorporatie Elkien niet vrijblijvend

De Friese thuiscorporatie Elkien biedt mensen met bescheiden inkomens betaalbare, duurzame en passende woningen in een leefbare omgeving. Elkien wil een corporatie zijn waar huurders, medewerkers en partners zich welkom en gewaardeerd voelen. Het hoofdkantoor van Elkien staat op een steenworp afstand van het Abe Lenstra Stadion in Heerenveen. Verder heeft de thuiscorporatie vestigingen in Leeuwarden en Sneek. Bij Elkien zijn ruim 200 medewerkers dagelijks bezig met het woon- en leefklimaat van de huurders.

“Het eerste contact tussen Elkien en Avantage? Dat is begin 2017 geweest”, vertelt Projectmanager & Security Officer Everdina Groen. Gedetacheerd door een gespecialiseerd bureau werkte zij toen op projectbasis voor Elkien om de verhuizing van delen van de IT-omgeving naar de cloud te managen. “De bestaande IT-partner kon door de beperkte omvang niet voldoen aan de toekomstige behoeftes en innovatiewensen van Elkien. Na een zorgvuldig selectieproces bleven er twee gelijkwaardige partijen over. Uiteindelijk hebben we heel bewust gekozen voor een IT-partner zonder achtergrond in de corporatiesector. Het idee was dat je dan makkelijker samen naar nieuwe kansen en mogelijkheden kunt kijken en verder kunt komen.”

Transitie naar de cloud

In de oorspronkelijke uitvraag was nauwelijks sprake van cybersecurity. “Digitale veiligheid stond in 2017 nog niet prominent op de kaart”, geeft Everdina als verklaring. “Basiszaken als inlogprocedures en wachtwoordbeleid waren trouwens wel geregeld. Net als een firewall en antivirussoftware. Bovendien werd in die tijd ook al gewezen op het gevaar van phishing. Er was alleen nog geen overkoepelend plan; geen structuur waarin cybersecurity kon worden ingebed. Dat zat toen overigens ook niet in mijn portefeuille. Ik was bij Elkien gedetacheerd om de transitie naar de cloud in goede banen te leiden. Dat heb ik dan ook gedaan.”

Geoliede projectorganisatie

“We hadden al snel een technische match met Avantage”, kan Everdina zich nog goed voor de geest halen. “Voor het afstemmen van de processen hadden we wat meer tijd nodig. Evengoed hadden we binnen een paar maanden een geoliede projectorganisatie opgetuigd.” De overgang naar de cloud verliep dan ook voorspoedig. “De medewerkers van Elkien moesten alleen even wennen aan de nieuwe servicedesk. Voorheen waren ze gewend om met hun vragen even binnen te lopen in de IT-ruimte, waar drie IT’ers hun werkplek hadden. Na de verhuizing naar de cloud werd de gebruikersondersteuning op afstand uitgevoerd door de servicedesk van Avantage. Maar ook die overgang ging redelijk geruisloos. De interne campagne die we daarvoor hebben gevoerd, heeft daar zeker bij geholpen.”

Vulnerability Scan

In 2019 werd het detacheringscontract van Everdina omgezet in een vaste aanstelling bij Elkien. “Sinds dat moment ben ik verantwoordelijk voor alle IT-zaken en dus ook voor cybersecurity. Een van mijn eerste acties was in gesprek gaan met Avantage om de kwetsbaarheden en potentiële kwetsbaarheden in onze IT-omgeving in beeld te brengen. De uitkomsten van de Vulnerability Scan - die toen werd uitgevoerd - hebben ons heel goed geholpen om te anticiperen op mogelijke problemen die dankzij de scan geen problemen zijn geworden.”

Ook kritisch gekeken naar het securitybeleid en de bedrijfsprocessen.

De Vulnerability Scan was niet alleen gericht op technische maatregelen. “Er zijn nog twee andere aandachtsgebieden die bij zo’n scan aan de orde komen. Zo wordt er ook kritisch gekeken naar het cybersecuritybeleid en de inrichting van de bedrijfsprocessen. En als derde element wordt het digitaal veiligheidsbewustzijn van de medewerkers in jouw organisatie onder de loep genomen. Je kunt kapitalen investeren in techniek en processen – en daar moet je zelf een zorgvuldige afweging in maken – maar het zijn uiteindelijk wel de mensen in je organisatie die digitaal veilig moeten werken.”

Kosten-batenanalyse

Cybersecurity kent dus drie bouwstenen: techniek, werkwijze en menselijk gedrag. “Dat klopt als een bus. Bij techniek moet je dan denken aan de IT-infrastructuur; het IT-platform; de inrichting van servers; veilige verbindingen; toegang tot de IT-omgeving en dat soort zaken. Er zijn namelijk genoeg technische maatregelen die je kunt nemen om het cybercriminelen moeilijk te maken. Tegelijk moet je ook beseffen dat 100 procent veilig een onhaalbaar ideaal is. Hoe ver je komt, hangt van zo enorm veel factoren af... En uiteindelijk is het niet jouw IT-partner die dat voor jou bepaalt. Je stelt zelf vast welke technische maatregelen je voor jouw organisatie neemt. Welke risico’s accepteer je en hoeveel heb je over voor het afdekken van de risico’s die je niet wilt accepteren. In feite praat je over een zakelijke kosten-batenanalyse.”

De omvang van de organisatie speelt daarbij geen rol. “Het maakt totaal niet uit hoe groot of klein jouw bedrijf of instelling is. Elke organisatie is tegenwoordig een potentieel slachtoffer”, weet Everdina. “Elke organisatie heeft namelijk ergens een plek in een supply chain. En als één organisatie in een keten wordt aangevallen of getroffen, lopen de andere organisaties in die keten ook gevaar. Zo is een warme bakker of zelfs een bedrijf in de supply chain van die bakker een potentieel doelwit wanneer de bakkersbond het uiteindelijke doel is. Cybercriminelen zoeken simpelweg de zwakste plek in de keten om van daaruit verder te werken en hun doel te bereiken.”

Verschillende data beschermen

De mate waarin privacygevoelige gegevens in een organisatie worden verwerkt, is een bijkomende factor bij het bepalen van de technische voorzorgsmaatregelen om een cyberaanval te voorkomen. “Dat is natuurlijk ook nog een punt, tot op zekere hoogte. Want aan de ene kant heb je te maken met privacygevoelige gegevens van anderen - in onze situatie bijvoorbeeld van huurders - maar aan de andere kant moet je ook de bedrijfsdata van je eigen organisatie beschermen.

Cybercriminelen zoeken simpelweg de zwakste plek in de keten.

Dan komt meteen de Algemene Verordening Gegevensbescherming in beeld, die zaken voorschrijft. En voor een directie speelt vooral de continuïteit van de bedrijfsprocessen een belangrijke rol. Die moeten altijd door kunnen gaan. Je hebt dus meerdere soorten data om te beschermen en ook verschillende belangen waarmee je rekening moet houden.”

Device Management

Over voorzorgsmaatregelen gesproken: uit het cybersecuritybeleid komt voort dat iedereen bij Elkien uit een beperkt aantal modellen smartphones kan kiezen en met hetzelfde type laptop werkt. Want? “Dat maakt het beheer met Device Management heel eenvoudig, ook al omdat we het aantal te gebruiken applicaties tot een werkbaar minimum beperken. Daarbij staan we geen schaduw-IT toe in onze IT-omgeving. Wat we daarbovenop ook nog doen, is regelmatig toetsen van de integriteit van onze systemen en data. Dat soort zaken hebben we of in het beleid of in de bedrijfsprocessen verankerd. Maar net als bij techniek geldt: ook in dat opzicht is 100 procent veilig een utopie. En op zich is dat ook helemaal niet erg. Waar het om gaat, is dat je de risico’s zo goed mogelijk minimaliseert.”

Risico’s minimaliseren en afdekken, dat is dus de crux. “En waar het vooral om draait, is dat je jouw mensen bewust maakt van wat cybersecurity eigenlijk is en hoe ze daar zelf een bijdrage aan kunnen leveren. Je kunt technisch en organisatorisch van alles bedenken; de menselijke factor is doorslaggevend. De grootste uitdaging is daarbij dat je jouw medewerkers bewust moet zien te maken van onbewust gedrag. Dat is geen eenmalige activiteit of een uniek project, maar een continu proces dat je moet blijven voeden. En dat is niet eens zo ingewikkeld. Voor de cybersecuritytrainingen hanteren wij verschillende spelvormen, waardoor het voor onze medewerkers leuk blijft om mee te doen aan het verhogen van de security awareness in onze organisatie.”

Je moet jouw medewerkers bewust zien te maken van onbewust gedrag...

Veiligheid en gemak

De speelse security awareness trainingen zijn niet alleen bedoeld voor de medewerkers op kantoor. “Security awareness is voor iedereen. Ook voor onze vakmensen die reparaties op locatie uitvoeren. Zie zo’n laptop of smartphone maar als een stuk gereedschap waar je goed voor zorgt omdat het onmisbaar is bij wat je doet. Maak de vertaalslag naar het device waarmee je werkt en je snapt meteen waarom je daar ook goed voor moet zorgen. Als organisatie moet je alleen wel de balans tussen veiligheid en gemak goed in de gaten houden.”

Die uitspraak licht Everdina graag toe. “Kijk; schermbeveiliging die na twee seconden inactiviteit op de laptop meteen inschakelt, is uit het oogpunt van cybersecurity een goed plan. Alleen is het niet praktisch omdat je het mensen op die manier erg lastig maakt om hun werk te doen. Cybersecurity moet je bij mensen niet door de strot duwen en je moet ook niet alles willen voorschrijven. Je hebt er veel meer aan dat mensen snappen waarom ze dingen wel of niet moeten doen en daar uit zichzelf rekening mee houden. Je moet medewerkers dus helpen om veiliger te werken en niet alleen zeggen dat ze dat moeten doen. Uitleggen waar de risico’s zitten en dan ook uitleggen wat de gevolgen kunnen zijn. Inzicht geven. Aandacht voor de drie O’s: onverschilligheid, onvoorzichtigheid, onwetendheid. Dat helpt.”

Cybersecurity regel je niet met beleid of procesbeschrijvingen op papier. Die conclusie kan intussen veilig worden getrokken. “Je moet het gewoon dóen. En voor alle duidelijkheid: we hebben wel degelijk een aantal regels waar iedereen zich aan moet houden. Denk alleen maar even aan de schaduw-IT die ik al eerder noemde. Als medewerkers regels overtreden, heeft dat consequenties; ook als het om cybersecurity gaat. Daar moet je transparant in zijn. Cybersecurity is bij ons niet vrijblijvend.”

In Avantage heeft Elkien een IT-partner gevonden die dat uitgangspunt van harte onderschrijft. “Het Security Advisory Center, de podcastserie Hack van de Dam… Avantage is ook op het gebied van cybersecurity een partner die bij ons past. We snappen van elkaar hoe we zaken met elkaar willen doen en het is fijn om dat in de praktijk bevestigd te zien. Tegelijk zou ik elke organisatie met een IT-partner willen adviseren om van tijd tot tijd te controleren of die partner de benodigde controles op tijd uitvoert. Dat doen wij ook en dat vinden zowel Avantage als wij heel normaal.”

Samen verder komen

“Wanneer je bij een betrouwbare webshop artikelen bestelt, kijk je toch ook voor de zekerheid of die compleet worden aangeleverd? Vertrouwen is mooi, maar dat vertrouwen moet altijd bewezen kunnen worden. Dat is niet negatief en het is ook niet bedoeld om met een vinger te kunnen wijzen als er iets misgaat. Die steekproeven zorgen er juist voor dat we samen de lat hoog blijven leggen. Samen verder komen; dat is het uitgangspunt. Sinds 2017 hebben we in onze samenwerking al heel veel veranderingen en IT-ontwikkelingen meegemaakt, maar aan die insteek is niets veranderd. En dat bevalt ons allebei uitstekend.”

Dat mensen snappen waarom ze dingen wel of niet moeten doen en daar uit zichzelf rekening mee houden.

In dit klantverhaal heb je kunnen lezen hoe thuiscorporatie Elkien actief omgaat met cybersecurity en medewerkers bewust maakt van digitale dreigingen. In andere klantverhalen gaan we in op andere thema's. Die verhalen kun je direct downloaden door op het betreffende thema te klikken.

Stichting Vluchteling
Intune en AutoPilot

Pré Wonen
De moderne werkplek

Nebest
Outsourcing van IT

Harmony
Een eigen online startportal

Versa Welzijn
Microsoft Teams als uitgangspunt

Wijdezorg
Het samenwerkingsproces

Oceanco
Digitale volwassenheid

Thuiscorporatie Elkien
Cybersecurity en bewustzijn

Over ons

Wij geloven dat IT altijd en overal voor jou moet werken. Daarbij maakt het niet uit op welke van de laatste woorden je de klemtoon legt. IT móet gewoon voor jou wérken. Dat betekent dat wij zorgen voor een betrouwbare en veilige IT-omgeving, die 24/7 voor jou beschikbaar is en waarin je gegevens eenvoudig kunt vinden. Bovendien moet IT vóór jóu werken. Dat bereiken we door verschillende applicaties en data met elkaar te verbinden. Dat zorgt ervoor dat je relevante inzichten en stuurinformatie op een presenteerblaadje krijgt aangereikt. Daardoor kunnen jij en je collega's productiever (samen)werken.

Wil je meer weten over onze dienstverlening en onze manier van werken? Neem contact op met Jasper Glaser. Dan is een kennismakingsafspraak snel gemaakt.

jasper@avantage.nl
06 26 52 01 40