Tekst: Hans Eberson, Fotografie: Marcel Krijgsman

LAGARDE GROEP MAAKT THUISWERKEN VEILIG

‘CORONA LEVERT NIEUWE VEILIGHEIDS-VRAAGSTUKKEN OP’

Sinds de uitbraak van het coronavirus is thuiswerken normaal. Wat in eerste instantie begon als een strenge aanbeveling van de overheid werd voor menigeen al snel een gewoonte. Veel medewerkers ervoeren de voordelen van werken aan huis. Geen files of overbevolkt OV, je deelt je eigen dag in en je kunt zo gemakkelijker werk en privé combineren. Thuiswerken is efficiënt, thuiswerkers zijn zeer productief en dus is ook het bedrijfsmanagement inmiddels overtuigd van de meerwaarde. Maar er kleven ook nadelen aan, zoals veiligheid. Hoe zorg je ervoor dat thuiswerkers geen extra risico vormen voor de veiligheid van je IT-systeem en je data? Lagarde Groep heeft de oplossing.

Lagarde Groep is sinds 1991 het aanspreekpunt voor ICT, Communicatie en Beveiliging. De combinatie van deze aandachtsgebieden is niet toevallig, want IT is in alles wat er op deze terreinen speelt de rode draad. Lagarde Groep heeft met zo'n 110 medewerkers vestigingen in Putten, Ede en Hoevelaken. Het bedrijf heeft zich in bijna dertig jaar ontwikkeld tot een gewaardeerde partner voor bedrijfsleven, overheid en semi-overheid. Ook in tijden van corona, want thuiswerken levert nieuwe veiligheidsvraagstukken op.

PARTNERRELATIE

Eric Klomp is operationeel directeur. In zijn dagelijks werk is hij met name met klanten in gesprek. "Ik heb langdurige ervaring in de IT, maar mijn voorkeur gaat toch echt uit naar het bouwen van IT-netwerkstructuren. Zet mij bij een klant maar voor een whiteboard en ik ben in mijn element." Cornelis Vreeken is salesmanager ICT. "Onze vraag aan elke klant gaat altijd over de meerwaarde die we kunnen bieden, in innovatie, in efficiency en natuurlijk in veiligheid. Elke klant staat tegenwoordig in het vizier van kwaadwilligen, die 24/7 zoeken naar manieren om schade toe te brengen. Financieel via ransomware of bijvoorbeeld door diefstal of misbruik van data." Dat levert Lagarde Groep veel vaste klanten op. Eric Klomp legt uit: "Wil je in deze branche effectief kunnen samenwerken, dan moet je je klant van binnen en van buiten kennen. Hoe zit zijn organisatie in elkaar, hoe verlopen de processen en hoe heeft hij zijn backoffice ingericht. Als je dat weet, kun je meerwaarde bieden in bijvoorbeeld procesinrichting, administratieve netwerken of veiligheid. Het hangt namelijk allemaal met elkaar samen. Daarom zijn wij geen leveranciers voor onze klanten, maar partners", vertelt Cornelis Vreeken. "Daarom willen wij weten waar een klant over vijf jaar denkt te staan, wat dan gevolgen kan hebben voor de dingen die we vandaag voor hem doen."

VEILIGHEID

De wereld wordt steeds ingewikkelder, de nadruk op digitale systemen wordt steeds groter en netwerken worden steeds complexer. En ondanks alle media-aandacht gaat het nog veel te vaak mis. Dat landen als China, de Sovjet Unie en Noord-Korea stel-

selmatig pogingen doen om in te breken in westerse computersystemen is bekend. Maar ook de gewone hacker kan enorme schade aanrichten; bedrijfsinformatie vergaren, gegevens en ideeën stelen, chantage plegen, je netwerk gebruiken voor het verspreiden van spam, het is soms kinderlijk eenvoudig. De aanvallen worden niet alleen uitgevoerd op multinationals, ook MKB-ondernemingen en overheden moeten op hun hoede zijn voor een digitale inbraak op hun systemen en netwerken. Ze vormen nog steeds een makkelijker prooi voor die cybercriminelen: ze hebben vaak veel digitale waarde-elementen, maar nemen vaak minder beveiligingsmaatregelen dan een grotere organisatie. Eric Klomp: "Zeker op het gebied van veiligheid zijn nog grote slagen te maken. Als je kijkt hoe de digitale criminaliteit zich in vijf jaar heeft ontwikkeld, dan schrik je. Vroeger had je te maken met een nerd die het leuk vond om in je netwerk in te breken. Gewoon omdat het kon. Nu heb je te maken met criminele organisaties die op een heel professionele manier te werk gaan. Ze vinden elke week wel nieuwe manieren om het bedrijven en overheden moeilijk te maken. In feite lopen we daar voortdurend achteraan. Uiteraard zorgen we ervoor dat een systeem zo goed mogelijk is beschermd, maar er kan altijd iets fout gaan en de mens is helaas de meest kwetsbare factor. Daarom hameren we voortdurend op bewustwording; realiseer je dat je voortdurend risico's loopt en doe er alles aan om die risico's te minimaliseren."

THUISWERKEN

Het zijn bijzondere tijden met nieuwe vragen. Hoe blijf ik met medewerkers en klanten communiceren, nu ze vaker op afstand staan. Daarvoor moet soms een nieuw informatiesysteem in de juiste organisatiestructuur worden ontworpen. "Ook dat lukt eigenlijk alleen als je je klant goed kent en die kennen we. Corona is ook een moment om de interne veiligheid nog eens goed onder de loep te nemen. Zeker ook omdat mensen thuis vaak met eigen apparatuur werken en dat brengt nieuwe risico's met zich mee."

'HET GAAT ALTIJD OVER DE MEERWAARDE DIE WE KUNNEN BIEDEN, IN INNOVATIE, IN EFFICIENCY EN NATUURLIJK IN VEILIGHEID'

Uiteraard kun je als bedrijf investeren in laptops en smartphones voor medewerkers. Dat maakt het instellen van toegang en veiligheid misschien eenvoudiger, maar dat vergt een behoorlijke investering, dus gebruikmaken van bestaande capaciteit ligt voor de hand. Vrijwel elke Nederlander beschikt immers over een eigen laptop en die kunnen met toestemming van de medewerkers prima worden gebruikt voor professionele doeleinden. Dat heet Bring Your

Own Device (BYOD). Door het gebruiksgemak – elke medewerker kent zijn eigen laptop - is BYOD populair in bedrijfsomgevingen. Er kleven ook nadelen aan, niet alleen waar het gaat om beveiliging van bedrijfssystemen en –geheimen, er kunnen juridische complicaties optreden. Wie is bijvoorbeeld verantwoordelijk voor verlies, diefstal of schade bij een geslaagde virusaanval en er zullen afspraken over de kosten moeten worden gemaakt. En dan denk je dat je het als bedrijf goed hebt geregeld, maakt een medewerker tijdens een tussenstop gebruik van een onbeveiligd wifi-netwerk. Dat valt dus weer onder het hoofdstuk bewustwording. Er treden rond thuiswerken meer problemen op die goed moeten worden getackeld. Cornelis Vreeken: “Neem beeldbellen, bijvoorbeeld Teams, een must voor thuiswerkers. Maar hoe stroomlijn je de informatie die tijdens zo’n sessie wordt gedeeld? Hoe houd je het beheer onder

‘WE ZORGEN DAT KLANTEN IN GEVAL VAN EEN CALAMITEIT ZO SNEL MOGELIJK, MET ZO WEINIG MOGELIJK SCHADE VERDER KUNNEN’

controle, zodat niet elke gebruiker zijn eigen stukje bedrijfsinfo in een of ander bestand opslaat dat voor zijn collega’s onbereikbaar is? En hoe integreer je telefonie (VoIP) in je systeem? Daar heb je dus nu een mooie kans voor met bellen via Microsoft Teams. ‘Ja maar ik heb net een nieuwe centrale gekocht’, zegt je klant dan. Dan koppelen we die toch aan Teams, zodat de centrale gewoon zijn werk blijft doen.”

EAT YOUR OWN DOGFOOD

Natuurlijk maken de mensen van Lagarde Groep zelf uitgebreid gebruik van de veiligheidssystemen die ze ook aan klanten adviseren. “Bewustwording is bij ons volop aanwezig, omdat we weten wat er mis kan gaan. Onze medewerkers werken ook thuis met Microsoft 365 en alle apparatuur is met onze security-systemen verbonden. Daarnaast werken we met multifactor authenticatie, dus het is niet zo eenvoudig om een wachtwoord te stelen. Alle ongeautoriseerde toegang wordt automatisch geblokkeerd. We werken ook met zogeheten ‘conditional access’, waarbij je op grond van bepaalde condities, die je zelf kunt regelen, toegang krijgt tot het systeem. Daarnaast gebruiken we onze zelf ontwikkelde software. Eat your own dogfood heet dat. Neem bijvoorbeeld Blue Socks. Dat is een systeem dat uitgaand netwerkverkeer scant en eventuele afwijkingen constateert. Er kan namelijk op de een of andere manier een virus in je systeem zijn gedrongen dat zich maanden slapende houdt en dan opeens actief wordt en data gaat versturen. Onze software constateert dat onmiddellijk, slaat alarm en sluit het apparaat af. Ten slotte hebben we onze eigen security-afdeling die alle systemen 24/7 monitort. Zij zijn voortdurend op zoek naar gaten in ons systeem, want laten we eerlijk zijn, je bent nooit voor 100% klaar, dus er valt altijd iets te verbeteren. Een minstens zo’n belangrijke taak is het assisteren van klanten die door een virus worden aangevallen of met een hack hebben te maken. Zorgen dat ze zo snel mogelijk, met zo weinig mogelijk schade verder kunnen. Dat is de opdracht.”

KLANTTEAMS

De mensen van Lagarde Groep steken veel energie in klantrelaties. “We denken dat we ons werk optimaal kunnen doen als we een klant van haver tot gort kennen. Daar investeren we in, daar hebben we onze dienstverlening via abonnementsvormen op afgestemd en ook onze organisatie is door onze klantteams zo ingericht dat we elke klant maximaal kunnen bedienen. Elke klant heeft met één klantteam te maken, zij staan hem in alles bij. Zo’n team gaat veel verder dan accountmanagement, er zitten specialisten in die samen alle terreinen van onze dienstverlening bestrijken. Het voordeel? Ze kennen de klant, ze kennen de contactpersonen en dat maakt dat ze op elk moment, bij ieder project of calamiteit onmiddellijk kunnen reageren. Ik werd ’s ochtends in de auto een keer gebeld door een klant met een brand. Ik wilde het klantteam op de hoogte brengen, bleek dat drie teamleden al onderweg waren. ’s Middags hadden we die klant weer online en bereikbaar. Dat kun je alleen realiseren als je investeert in een diepe klantrelatie. En dan krijg je de klanten die dat weten te waarderen, bij overheid, in de zorg, het onderwijs, dienstverlening en MKB en MKB+. We hebben de laatste jaren meer dan 6.000 projecten bij onze klanten succesvol gerealiseerd, dat zegt wat ons betreft genoeg. Meer weten? Kijk op lagarde.nl.”