Het coronavirus verplicht bedrijven om halsoverkop over te schakelen naar thuiswerk. Die omschakeling houdt heel wat uitdagingen in, vooral op het vlak van cybersecurity. Telenet Business ondersteunt zijn professionele klanten hierbij, ook vanuit zijn eigen ervaringen.

THUISWERK vergt een nieuwe beveiligingsaanpak

Corona heeft onze manier van werken helemaal veranderd. Meer dan zes op de tien Belgen die tijdens de lockdown aan het werk waren, deden dat plots van thuis uit. Vier op de tien werknemers hadden dat voor de coronacrisis nog nooit gedaan.

Die overstap van de vertrouwde werkplek naar het thuiskantoor is een grote verandering. Dat ervaart ook Telenet, dat duizenden mensen tewerkstelt. Director security Mark Van Tiggel en chief technology officer Micha Berger leggen uit hoe zij omgaan met de nieuwe manier van werken.

Mark Van Tiggel: 'De coronacrisis was voor veel bedrijven een big bang. Werknemers werden plots verplicht om thuis te werken: voor veel ondernemingen was dit nieuw. Bij een bedrijf als Telenet lag dat anders: veel van onze medewerkers, waaronder onze consultants, werkten al regelmatig vanop afstand. Bovendien hebben we ook mensen aan het werk in India. Onze bedrijfsinfrastructuur was al grotendeels afgestemd op telewerk.'

'De gedwongen stap naar voltijds thuiswerk was wel ongezien. De overgang van 300 tot 500 mensen die gelijktijdig van thuis uit werken naar bijna 4.000 voltijdse thuiswerkers hield uitdagingen in. De manier van werken veranderde helemaal: vroeger werkte je thuis individueel en gefocust, vandaag zit je vaak in de ene videovergadering na de andere.'

'Aanvallers profiteren van de kwetsbaarheid van de geïsoleerde thuiswerker'

MICHA BERGER,
CHIEF TECHNOLOGY OFFICER TELENET

Die ommezwaai creëert wellicht allerlei nieuwe behoeften?

Micha Berger: 'Dat klopt. Niet elke werknemer heeft thuis een werkruimte, een bureaustoel, audio- en videofaciliteiten en voldoende internetbandbreedte. Maar daarnaast brengt thuiswerk natuurlijk ook heel wat veiligheidsaspecten met zich mee. Plots moet je de woning van al je medewerkers zien om te bouwen tot een beschermde omgeving die vergelijkbaar is met die op kantoor. Een policy inzake thuiswerk hadden we uiteraard al, maar die moest aangepast worden aan de nieuwe situatie.'

Mark Van Tiggel: 'Als werkgever verlies je bij telewerk gedeeltelijk de controle. Als thuiswerkers applicaties gebruiken die bedrijven zelf hosten in hun datacenter en alleen toestellen van de werkgever gebruiken, kan er niet veel fout gaan. In de praktijk gaat het meestal anders: medewerkers gebruiken ook eigen toestellen - zoals een tablet of een smartphone - voor het werk. Bovendien werkt iedereen tegenwoordig in de cloud. Daar hangen risico's aan vast.'

Zijn die risico's groter geworden? Zijn er meer cyberaanvallen dan vroeger?

Micha Berger: 'Jazeker. Tijdens de lockdown had iedereen meer vrije tijd. Hackers gingen op zoek naar nieuwe opportuniteiten. Bovendien zijn de eigen toestellen van werknemers makkelijkere doelwitten dan bedrijfstoestellen. Vooral phishingaanvallen kenden een sterke groei sinds de corona-uitbraak. De aanvallers profiteren van de kwetsbaarheid van de geïsoleerde thuiswerker. Die kan niet zomaar te rade gaan bij een collega in de nabije omgeving. Wij trainen onze medewerkers daarom in het identificeren van verdachte mails.'

Zo maak je van veiligheid een reflex. Is dit wat jullie verstaan onder 'security by design', een term die je vandaag steeds meer hoort?

Micha Berger: 'Security by design betekent dat je beveiliging niet langer als een laag bovenop de technologie beschouwt, maar als een noodzakelijk onderdeel van de systemen en processen die je als onderneming uitbouwt. In het verleden ging een technologiespeler als Telenet zo te werk: we ontwikkelden eerst een platform, lieten dat testen door beveiligingsexperts en deden vervolgens de nodige aanpassingen. Vandaag is het securityteam betrokken bij elke ontwerpfase. Samen met de ontwikkelaars evalueren onze veiligheidsexperts in elke stap van het design de mogelijke risico's.'


© Marco Mertens

'De gedachte "sluit de deur en er kan je niks meer gebeuren" houdt geen steek. Een holistische kijk op beveiliging is essentieel'

MARK VAN TIGGEL,
DIRECTOR SECURITY TELENET

Welke elementen mogen niet ontbreken in een goed veiligheidsplan?

Mark Van Tiggel: 'Een moderne firewall en goede beveiligingssoftware blijven belangrijke elementen in elke verdedigingsstrategie. Helaas garandeert geen enkele tool of oplossing honderd procent veiligheid. Vooral gerichte aanvallen zijn amper tegen te houden. De gedachte "sluit de deur en er kan je niks meer gebeuren" houdt geen steek. Een holistische kijk op beveiliging is essentieel.'

'Als bedrijf moet je voorbereid zijn op het feit dat je ooit zelf het slachtoffer van een cyberaanval bent. Hoe reageer je daar op? Welke processen kunnen de impact van een aanval inperken? Ligt er een actieplan klaar? Is dat getest en uitvoerbaar? Wie neemt wanneer de leiding? En hoe leer je je medewerkers omgaan met de gevaren? Al deze elementen samen maken een onderneming weerbaarder tegen cyberaanvallen."

Hoe helpt Telenet Business zijn klanten bij die holistische beveiligingsaanpak?

Micha Berger: 'Wij bieden bedrijven verschillende technische tools en oplossingen om indringers buiten te houden. Onze ervaren cybersecurity-experten ondersteunen organisaties bij het maken van de juiste keuze. Ze zorgen ook voor de implementatie. Voor klanten die dit wensen, nemen we het volledige veiligheidsbeheer in handen. Zo is de klant zeker van een correcte opvolging en expertise als er een incident plaatsvindt.'

'Naast die technologische component, focussen we sterk op het menselijke aspect. We helpen bedrijven bij het opstellen van een actieplan en informeren ze over actuele bedreigingen. Tot slot zetten we sterk in op bewustmaking. We voorzien opleidingen die medewerkers bewuster maken van de gevaren van thuiswerk. De expertise die we in huis hebben, delen we graag met onze klanten.'