# Transcription non-expert 7

Duration: 41 minutes

X: Dan start ik met de eerste vraag van het interview. Kunt u aan mij uitleggen wat een VPN is?

Y: Ja, als ik het eh, heel simpel vertaal naar eh, Jip en Janneke taal, dan is het eigenlijk dat een gebruiker een soort masker op zet en daarmee eh, zich kan voordoen als iedereen op eh, op internet. Voordeel is dat eh, berichten versleuteld worden eh, tussen de gebruiker, tussen de laptop van de, de pc van de gebruiker en de, en de VPN server. En dat ook de locatie er eigenlijk ook niet meer toe doet. He, zo zie je dat mensen waar nogal censuur op het internetgebruik zit, zoals in sommige Aziatische landen, dat men daar vaak een VPN verbinding gebruikt om toch social media kanalen te kunnen gebruiken. Dat is een beetje het beeld wat ik er van heb. Eh, binnen de organisatie, [the professional services firm], wij gebruiken het ook, ik denk ook eh, vanwege dat eh, die global insteek eh, en, en uiteraard de versleuteling van de data. He, omdat-

X: En wat bedoelt-

Y: natuurlijk ook wel eens in hotels of op vreemde plekken op eh, op een openbare wifi zitten.

X: Oké. En wat bedoelt u met global insteek?

Y: Eh, nou ja, als je, ik heb bijvoorbeeld [0:02:08 till 0:02:10 has been omitted], dan moet je wel bij de Nederlandse servers kunnen. Ik kan me voorstellen dat er bepaalde locatievoorzieningen zijn, die zeggen waar zit jij, nou in mijn geval zat ik dan in [country] en ik moet iets benaderen in Nederland. Dan kan die verbinding niet worden eh, gemaakt, omdat ik dan buiten Nederland ben. Ik heb dat toevallig van de week gehad met Ziggo, ik weet niet of je Ziggo kent, maar dan start je die app op in Duitsland, dan zegt die ja je bent binnen, of je bent buiten Nederland, dus we kunnen die content niet laten zien. Je mag gewoon niet buiten eh, buiten het land, maar met een VPN verbinding kan je doen alsof je in Nederland bent eh, vanuit elke plek op aarde.

X: Oké. En u noemde ook een masker, wat bedoelt u daarmee?

Y: Nou, dat je min of meer incognito op eh, op het internet kunt eh, kunt surfen, omdat je IP-adres, waarmee je je op het, het internet surft van je PC, ja, die kun je iedere naam geven die je wilt, of ieder nummer geven die je wilt. Je kunt iedere IP-adres aannemen. En niet je vaste IP-adres waarmee je te herleiden bent naar je betreffende locatie.

X: Oké. En u zegt dat de berichten versleuteld worden tussen de gebruiker en de VPN server-

Y: Ja.

X: Hoe worden deze berichten versleuteld?

Y: Nou, hoe dat technisch precies gaat weet ik niet, maar het bericht wat je maakt wordt als het ware in een soort koker gestopt. En die koker eh, ja, die is, daar zit een sleutel op eh, en aan de andere kant eh, gaat die sleutel er weer af. Dus zou dat bericht onderweg ergens eh, of zou die koker onderweg ergens eh, geopend moeten worden, dan moet je die sleutel hebben om dat bericht dat erin zit te kunnen lezen. Dat is het voordeel, dat is eigenlijk het voordeel van een VPN verbinding. En dat is ook ja, ik zeg dat nu zo eh, het bericht gaat in een koker, dat is natuurlijk niet zo, maar eh, dat is eh, dat is eh, een beetje de visuele voorstelling die ik daarvan heb.

X: Ja, oké. En eh, dan noemde u ook nog VPN in verband met openbare wifi-

Y: Ja.

X: Wat is de relatie hiermee?

Y: Nou ja, als je, tenminste, dat is mijn beleving, als je via een openbare wifi in een of andere [example of restaurant] eh, voor je werk een bestand op wilt halen, dan gaat dat via die beveiligde verbinding, en omdat die eh, omdat dat internetverkeer versleuteld is eh, gaat dat toch op een veilige manier. Is mijn idee eh, he, normaal gesproken kun je vrij eenvoudig meelezen op een openbare wifi verbinding met eh, wat iedereen daar aan het doen is. En dat is natuurlijk eh, dat brengt natuurlijk een risico met zich mee.

X: Ja. Oké. En voor welke doelen gebruikt u VPN?

Y: Nou, volgens mij heb ik niet eens een keus. Wij zitten altijd via een VPN verbinding, maar ik denk, omdat wij nu vanuit huis werken, het extra belangrijk is dat eh, dat de data versleuteld wordt. Niet iedereen heeft zijn thuisnetwerk goed beveiligd. We gaan met onze [the professional services firm] laptop op ons thuisnetwerk wat ooit eens een keer een slimme buurman heeft aangelegd eh, ja, dan is het wel belangrijk dat de data, die vaak eh, vertrouwelijk is. He, omdat het over cliënten gaat he, of over de organisatie als [the professional services firm] zelf, dat dat eh, dat dat niet voor anderen zo maar leesbaar is. En voor zo ver-

X: Ja. En wat bedoelt u ermee, o, sorry?

Y: En voor zo ver ik heb begrepen geldt dat ook voor de telefoons die wij ter beschikking hebben gekregen. He, ik heb een eh, ik heb een [mobile phone], ja, daar zit je natuurlijk eh, te pas en te onpas op onbeveiligde wifi. En, en, ja, die neem je ook mee als je, als je de stad in gaat. Ik noem maar wat. He, dus het is wel belangrijk dat die data juist op de mobiele telefoon versleuteld wordt en niet voor iedereen toegankelijk is. Vooral omdat de apps waarmee we toegang krijgen tot de [the professional services firm] systemen steeds eh, steeds meer toeneemt. He, onze volgende tijd, tijdschrijfsysteem, zal een app hebben. Het verantwoorden van expenses, dat zal via een app kunnen. [0:06:37 till 0:06:42 has been omitted]. Ja, dan is het wel belangrijk, omdat je natuurlijk je expenses op een, en je time ook, op een engagementnummer boekt, dat niet al die engagementnummers zo maar beschikbaar zijn eh, op je mobiele telefoon.

X: Ja. Oké. En gebruikt u dan ook de VPN verbinding op uw [mobile phone]?

Y: Nou, je kunt niet zonder. Want zonder die VPN verbinding, werken die apps niet.

X: Oké. En u gebruikt dan ook de [the VPN of the professional services firm]?

Y: Ja. Nou, of ik dat gebruik weet ik niet, maar ik heb [e-mail], dat moet je, dat moet je binnen een bepaalde appstore halen, een [the professional services firm] appstore en die [e-mail] app en de andere apps, we hebben er nog meer, [conferencing software] is er ook zo een. Eh, en de expense app. Die eh, die gaan allemaal via die, via die VPN verbinding, anders werken die apps niet eens. Want in je instellingen moet je ook toestaan dat die VPN verbinding gebruikt wordt, daarmee worden ook een aantal security settings ingesteld die je niet kun omzeilen, althans ik heb dat niet echt geprobeerd. Maar je ziet dat je telefoon ook binnen een minuut eh, vergrendeld wordt. He, terwijl je als normale gebruiker, als je hem alleen eh, privé gebruikt, ja, kun je dat geloof ik instellen tot wel 15 minuten voordat het scherm automatisch vergrendeld wordt.

X: Ja. Oké. En dan zei u eerder nog eh, wij zitten altijd via VPN.

Y: Ja, volgens mij wel.

X: En op welk apparaat bedoelt u dit?

Y: Nou ja, op eh, op de PC, op de laptop, die eh, die ik gebruik van [the professional services firm] en op de telefoon. De apps die ik voor [the professional services firm] gebruik he, als ik gewoon naar mijn eigen bank ga op de telefoon van [the professional services firm], dan gaat dat niet via een VPN verbinding.

X: Oké. Moet u dan weer de VPN uitzetten of gaat dat automatisch?

Y: Nee, nee hoor, daar hoef je niets voor te doen, nee. Nee, het is ook niet zo dat ik op de laptop wel of niet kies voor een VPN verbinding.

X: Oké, dus eh-

Y: Volgens mij, volgens mij gaat dat via [the VPN of the professional services firm]. Als ik op de [the professional services firm] systemen wil, dan moet ik eerst via [the VPN of the professional services firm] een verbinding leggen, dan eh, dan kan ik bij de [the professional services firm] systemen zoals [conferencing software] eh, [conferencing software] kan, [conferencing software] of nee SharePoint bijvoorbeeld. Eh, de [the professional services firm] apps, zoals [an internal page], daar kun je alleen maar bij, die op het intranet zitten, daar kun je alleen maar bij als je via die eh, via die [the VPN of the professional services firm] bent ingelogd.

X: En bedoelt u dan dat VPN automatisch opstart of wat bedoelt u met wij zitten altijd in VPN-

Y: Dat vermoed ik wel ja, want ik start, ik start het niet zelf op. Volgens mij gaat dat op de achtergrond van zelf. Dat vermoed ik hoor, ja dat eh-

X: Ja. Oké. En eh, als je dan de [the VPN of the professional services firm] opstart, welke handelingen voert u daarvoor uit?

Y: Nou, ik druk op een icoontje onderin mijn taakbalk, want die heb ik daarin gezet. Eh, nou ja, dan vul ik mijn persoonlijke wachtwoord in plus de eh, wat zijn het, vijf cijfers die eh, die op de [the VPN of the professional services firm] app verschijnen. En die samen eh, maken verbinding met het intranet van [the professional services firm]. Ik start niet specifiek VPN op. Maar mijn vermoeden is dat dat erachter zit. Dat die intranet toepassing allemaal via een VPN verbinding eh, worden benaderd en dat je dat automatisch met [the VPN of the professional services firm] opstart.

X: Oké. En is er ook als eh, [the VPN of the professional services firm] nog niet opgestart is, kunt u ook een VPN verbinding maken?

Y: Ik heb dat nooit geprobeerd. Maar dat ja, technisch eh, moet dat lukken. Want je kunt, je kunt als privé persoon ook gewoon een VPN verbinding aanvragen. Sommige zijn zelfs gratis.

X: Ja. Oké. En-

Y: Maar kijk, ik heb daar geen ervaring mee. Sorry.

X: Geen probleem. Gebruikt u naast uw mobiel en laptop nog andere apparaten voor de [the VPN of the professional services firm]?

Y: Eh, nee, nee. Ik heb wel een tablet, maar die gebruik ik nooit.

X: En kunt u aan mij uitleggen hoe een VPN verbinding werkt? Ik zal hiervoor een nieuwe dia pakken, dan kunt u het whiteboard gebruiken als u dit wilt.

Y: Oké. Ik ben wel mijn icoontjes kwijt om mee te tekenen.

X: O, ja. Nu niet meer.

Y: O. Eh, eens even kijken hoor. Ik zie hier- [start drawing 18\_1]. Je hebt de gebruiker die via een firewall het internet opgaat, een verbinding maakt. Ja, nou dat tekenen, dat eh- Pak alleen het potlootje anders maar even hoor.

X: Oké.

Y: En daar ben ik niet best in hoor, in tekenen.

X: Prima.

X: Via internet maak je verbinding met een- Ik lijk wel een kind van twee dat voor het eerst een tekening maakt. Nee, wacht even, die- He, dus je hebt hier firewall, hier ben je, dit is de laptop van de gebruiker hier links, dat rondje. Nou, dan ga je door een firewall heen, nou, dat is gewoon de firewall die ik hier he, geïnstalleerd heb op mijn eh, op mijn thuisnetwerk. He, dat anderen niet op mijn thuisnetwerk kunnen. Daarmee ga ik het internet op en maak ik verbinding met eh, dit moet dan een VPN server voorstellen van [the professional services firm]. [start drawing 18\_2]. En daarmee eh, ja, ga ik naar de verschillende websites. Is mijn beleving hoor, maar ik ben geen eh- Want het gaat over experts en eh, en onwetenden, nou ik ben geen expert in ieder geval als het gaat om VPN, misschien is dat eigenlijk ook maar goed, want dat blijkt dat dat het achter de schermen wellicht allemaal zo veel vanzelf sprekend is, dat je daar als gebruiker ook niet heel veel last van hebt.

X: Nee, dit zie je natuurlijk niet aan de voorkant wat er allemaal gebeurt.

Y: Nee, je ziet aan de voorkant niet wat er eh, wat er allemaal gebeurt, nee.

X: Oké. En kunt u aan mij uitleggen wat een server is?

Y: Nou ja, wat een server is eh, een server die verzorgt het eh, die verzorgt de verbinding tussen de gebruiker en eh, het internet en de systemen binnen [the professional services firm]. He, dat is eigenlijk een soort eh, ja, een soort draaideur, naar de eh, naar de verschillende, naar de verschillende websites en de eh, en de systemen van [the professional services firm].

X: Ja. Oké.

Y: Die zegt van wie ben jij en waar moet je naartoe en heb jij daar toegang. Nee, niet waar, heb jij daar toegang, want dat weet die server niet. Dat komt, dat komt dan terug vanuit eh, vanuit de toepassing zelf. Maar eh, die regelt dat verkeer.

X: Oké. Eh, dan zei u eerder ook dat er versleuteling wordt gebruikt van de berichten-

Y: Ja.

X: Waar in deze tekening vinden we de versleuteling terug?

Y: [start drawing 18\_3]. Nou de versleuteling die vindt volgens mij pas plaats vanaf de VPN server.

X: Ja, VPN. Dus dan bedoelt u, o sorry?

Y: Je gaat naar de websites, maar misschien heb ik het gruwelijk mis hoor, maar dat is mijn beleving bij een eh, bij een VPN. He, dus hier vindt de versleuteling plaats, hier doe ik een aanvraag voor de website he, [an internal page], nou, die draait op een [the professional services firm] server. [start drawing 18\_4]. En deze, deze verbinding is eh, is dan versleuteld. He, daar kan dan dus een ander niet op meelezen. Of dat ook geldt tussen de gebruiker en de VPN verbinding zelf, die ook over het internet loopt, dat weet ik niet. Ik kan wel gokken, maar nee, dat weet ik niet.

X: Oké. En dan een andere vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Nou, het is niet echt merkbaar, maar het kan niet anders dan dat het allemaal iets trager verloopt, omdat dat versleutelen nou eenmaal tijd kost. En dat zal ongetwijfeld heel intelligent zijn tegenwoordig, maar het kost gewoon tijd. En eh, ja, wat dat komt de performance over het algemeen niet ten goede. Maar omdat ik de keuze niet heb, kan ik niet zien hoe snel mijn verbinding is met en zonder VPN.

X: En wat bedoelt u, dat u niet de keuze heeft?

Y: Nou volgens mij kan ik niet naar [an internal page] om te kijken hoe snel het is zonder VPN verbinding. Want dan werkt het gewoon niet, dan krijg ik gewoon geen toegang.

X: Oké. En heeft een VPN verbinding nog op een andere manier invloed op jouw computerbeveiliging?

Y: Nee, voor zo ver, nee, volgens mij niet, nee.

X: Oké. Dan een hele brede vraag-

Y: Nou ja-

X: O, sorry.

Y: Nou ja, in zoverre dat iemand die mijn laptop steelt he, er wordt ingebroken in mijn huis, mijn laptop, of neemt de [the professional services firm] laptop mee, die kan niet zomaar op de [the professional services firm] systemen, omdat je dan weer door die beveiliging heen moet.

X: Ja. En wat bedoelt u dan met beveiliging?

Y: Nou de beveiliging van eh, van eh, wat is het, [the VPN of the professional services firm]. He, ze hebben dan alleen maar de hardware, je hebt alleen maar de PC en je kunt niet bij onze klantenbestanden en dergelijke en bij onze rapportagesystemen. Bij alle systemen waar de gebruiker van [the professional services firm] toegang toe heeft.

X: Ja. Oké. En dan nog een vraag over deze tekening. Zijn deze verbindingen dan ook versleuteld, geldt dat voor alle verbindingen achter de lijn?

Y: Ja, volgens mij wel, ja.

X: Ja, oké. Dan een hele brede vraag. Met wat voor digitale dreigingen heb jij op een normale dag te maken als [the professional services firm] medewerker?

Y: Digitale dreigingen. Eh, nou ja, je, je email adres dat vind ik een eh, ja, dat is, dat is een sleutel tot eh, tot [the professional services firm] die vrij makkelijk eh, ja, ik krijg, ik krijg tegenwoordig ook spam binnen op mijn [the professional services firm] mailbox. En misschien wordt er nog een hoop tegen gehouden. Eh, de andere dreiging is toch de, de mobiele telefoon, hoewel die ook steeds beter wordt met beveiliging, met gezichtsherkenning en dat soort dingen. Eh, ja, de, de dreiging, kijk, de, de VPN verbinding volgens mij is die maar twee uur actief he, dus zou mijn PC, mijn [the professional services firm] laptop in die twee uur gestolen worden, ja, dan kan men alles doen wat men wil. Als ik nu even boodschappen ga doen, en ik kom terug, mijn PC is gestolen, ja, dan kan in die twee uur kan iedereen alles doen wat men wil. Want ik sluit niet af.

X: En moet u dan na die twee uur weer op niet de [the VPN of the professional services firm] opstarten?

Y: Ja, dat moet ik opnieuw [the VPN of the professional services firm]. Ik zeg kan iedereen alles doen, maar dat is natuurlijk niet zo, want je scherm wordt wel beveiligd, of je laptop. Dus je moet wel die code invoeren, die pincode, dus dat valt qua dreiging denk ik nog wel mee.

X: Ja. Dus op een normale dag moet u ook meerdere keren opnieuw verbinding maken?

Y: Ja. Ja, heel veel eh, applicaties, zoals [e-mail] en [conferencing software] wat je tegenwoordig eh, wat ik tegenwoordig het meest gebruik, dat werkt ook zonder eh, [the VPN of the professional services firm]. Eh, dus ja, dat eh, ik start het soms niet eens op, maar dan ga ik naar een intranetsite en die werkt dan niet. Dan denk ik o ja, even een [the VPN of the professional services firm] verbinding maken. Eh, en dan merk ik soms ook, als ik dan later op de dag, als ik dat nog een keer heb, he, dat die weer verbroken is.

X: Ja. Oké. En heeft u op een normale dag met nog meer digitale dreigingen te maken?

Y: Eh, nou ja, kijk, digitale dreigingen, die zitten natuurlijk op het thuisnetwerk, en het thuisnetwerk is over het algemeen niet zo goed beveiligd he, en ook niet zo sterk als een eh, een kantoornetwerk. He, en ik moet altijd door mijn privé netwerk heen. Ja, daar, als ik, als ik van binnen naar buiten kan, dan is het wellicht ook mogelijk dat iemand van buiten naar binnen gaat. He, dus inbreekt op mijn eh, privé netwerk, ik heb hier ook een NAS. Ik weet niet of je- Een NAS, zo een netwerkdrive, ja, die heeft ook verbinding met buiten, dat gaat ook via een cloudoplossing, kan ik er overal ter wereld bij. Hartstikke handig. Maar daarvoor moet je wel bepaalde deuren openzetten in je, in je router. Die zeggen nou voor dit apparaat mag er van buitenaf verbinding worden gelegd. He, want die zit natuurlijk aan de binnenkant van je netwerk. Nou, dat, dat is natuurlijk een potentieel risico. Als je dat niet goed doet is het een potentieel risico.

X: Ja. Oké. En heeft een VPN verbinding invloed op deze soorten digitale dreigingen?

Y: Eh, ja, dat denk ik wel. Denk wel dat eh, dat als iemand een VPN verbinding gebruikt vanuit het buitenland, ten eerste is die dan niet meer terug te traceren, terwijl iemand eh, ja, een hacker die eh, die zonder VPN verbinding probeert in te breken, die is te herleiden aan zijn IP-adres, en zijn IP-adres is weer te herleiden naar een locatie eh, en uiteindelijk de bezitter van die, van die laptop. Eh, maar in ieder geval de locatie. Met een VPN verbinding is dat onmogelijk, dan kan het overal vandaan komen. Dan lijkt het iemand misschien uit Appelscha te zijn, terwijl die ergens op de Filipijnen zit.

X: Ja, en is dit ook mogelijk met de [the professional services firm] VPN?

Y: Dat weet ik niet. Dat weet ik niet. Maar ik mag hopen dat ze dat goed beveiligd hebben. Nou ja, mag ik allemaal wel hopen, maar vorige week zijn er natuurlijk weer een hoop Twitter accounts gehackt. En ik mag aannemen, maar daarvan zien we het tegendeel, dat Twitter zijn zaakjes ook niet echt goed op orde hadden. He, omdat medewerkers van intern daar eh, eh, hebben, aan mee hebben geholpen. Ja, als medewerkers hebben binnen [the professional services firm], die eh, die VPN servers beheren, eh, en het op een akkoordje gooien met hackers, ja, dan is eh, dan houdt het op natuurlijk. Je hebt altijd nog die menselijke factor.

X: Ja, oké. En over deze menselijke factor gesproken, heeft u naast digitale dreigingen ook nog te maken met sociale dreigingen op een normale dag?

Y: Sociale dreigingen. Nou, nee, ik heb daar niet mee te maken. Nee, ik heb daar niet mee te maken, maar ik, op [social media platform] bijvoorbeeld, ik heb een [social media platform] account, ik zal even een voorbeeld geven. Ik heb een [social media platform] account, nou ja, bij [social media platform] vragen ze ook eh, wat je doet, nou ik vul daar gewoon in [role] bij [the professional services firm], prima. Eh, maar wat ik op [social media platform] zet, ja, dat is over het algemeen natuurlijk zijn dat privé dingen. He, en die privé zaken, tegenwoordig is het natuurlijk allemaal heel zwart-wit wat er op eh, zijn hele zware discussies gaande. Je moet dan natuurlijk ook wel uitkijken wat je zegt. He, eh, wat je als privé persoon zegt, of schrijft op [social media platform]. En nou doe ik daar geen gekke dingen op, maar ja, dat kan altijd weer terug te herleiden zijn naar de organisatie waar je voor werkt.

X: Ja, oké. En heeft u daarnaast nog met andere sociale of niet-digitale dreigingen te maken?

Y: Nou ja, je hebt altijd te maken met inbraken natuurlijk. He, mogelijke inbraak. Je ziet dat tegenwoordig steeds meer zaken via de cloud gaan. Voor mijn privé, ik heb zelf privé een laptop, ja, daar zit ik nu op, heb ik nu met jou die verbinding. Ja, die eh, alle wachtwoorden die ik gebruik voor websites, en dat zijn er inmiddels [number], die gaan via de cloud naar mijn [mobile phone], naar mijn tablet, en naar de [mobile phone] van mijn [partner]. Die zijn gewoon daar leesbaar, die, die je ziet daar de login naam staan als je, als je in instellingen naar wachtwoorden en accounts gaat, dan zie je daar gewoon de inlognaam en het wachtwoord staan. Nou, ik krijg het niet voor elkaar om dat af te schermen. Dat vind ik, vind ik een dreiging waarbij je, bij de [the professional services firm] hardware zie ik dat niet. En nogmaals, het wordt steeds beter versleuteld, want ik heb net een nieuwe laptop en de, die werkt alleen maar met een vingerafdrukscanner en de [mobile phone] tegenwoordig met gezichtsherkenning, maar daarvoor de, de ouder [mobile phone] van mijn [partner], dat was een [mobile phone], ja, die had het allemaal niet. Die had ook geen code, want dat vond [partner] vervelend. Eh, dus [partner] zette hem aan, en dan zag je gewoon die [number] wachtwoorden staan. Als je wist waar je moest kijken. Nou, dat vond ik nou niet bepaald prettig.

X: Nee, dat kan ik mij voorstellen.

Y: Maar dat is, ja, dat, dat heeft niet betrekking op de [the professional services firm] organisatie.

X: Ja. En heeft u vanuit uw rol in [the professional services firm] wel te maken met sociale dreigingen?

Y: Nee. Nee. Dat idee heb ik niet. Ja, wat, kun je daar een voorbeeld van geven, wat ik, waar ik dan aan zou moeten denken.

X: Ja, dat zou van alles kunnen zijn. U noemde eerder bijvoorbeeld inbraken.

Y: Ja.

X: Dat kan ook. Maar dan gaan we terug naar de digitale dreigingen. En wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Ja, dat kan iedereen zijn. Dat kan iedereen zijn eh, die, die baat heeft bij eh, het inbreken op het [the professional services firm] netwerk. En dat kan zijn bijvoorbeeld om onze clientgegevens buit te maken. He, we zijn daar natuurlijk heel zorgvuldig mee, en terecht. Maar als grote organisatie zoals, zoals [company] en dat soort bedrijven gehackt kunnen worden, ja, dan, dan durf ik niet te zeggen dat het bij [the professional services firm] niet lukt. Nou zit er bij bedrijven als [company] altijd nog een financieel gewin achter als je [0:28:14 till 0:28:14 has been omitted] kunt buitmaken, bij [the professional services firm] hebben we dat minder. Maar toch eh, ja, uiteindelijk is het altijd een wedloop tussen je beveiliging vanuit je organisatie en eh, en de boze buitenwereld die daar toegang toe wil krijgen.

X: Ja, oké. En wat zou de motivatie van een aanvaller kunnen zijn?

Y: Nou ja, de motivatie zou kunnen zijn het buitmaken van, van clientgegevens he, van onze cliënten. He, of daar ...(0:28:50) zeggen, nou ik heb jullie, wat is het [number] cliënten op een USB stick staan, eh, wat heb je ervoor over. Het zou eh, ja, dat, de motivatie is meestal geld. En heel slecht gedacht, ja, zou het ook nog een eh, zou het ook nog een concurrentie eh, ding kunnen zijn. He, om te weten welke cliënten wij allemaal hebben. [0:29:23 till 0:29:46 has been omitted].

X: Ja, oké. En wat voor achtergrond heeft een aanvaller?

Y: Nou, dat is meestal een technische achtergrond. Dat, dat is vrijwel altijd een IT achtergrond. Die in opdracht werkt van eh, van iemand die daar financieel gewin uit haalt, maar zelf niet zo slim is om eh, om in te breken. Maar nou heb ik misschien, heb ik misschien een ouderwets beeld van een hacker hoor.

X: Ja. En wie zou dan de opdracht geven?

Y: Ja, wie is de opdrachtgever, dat, dat kunnen allerlei criminelen zijn natuurlijk. Ik kan niet zo specifiek een iemand aanwijzen he, of een groep aanwijzen die eh, die bij voorbaat verdacht, verdenk van eh, een potentiele inbraak op onze systemen, nee.

X: Er zijn er bepaalde ja, meer abstractere groepen in dit geval die je wel zou kunnen bedenken?

Y: En dan heb je het over [the professional services firm] specifiek?

X: Ja.

Y: Ja, nou, dat zou concurrentie kunnen zijn. Maar ook groepen, ook groepen die losgeld vragen he, data is tegenwoordig business. He, dat zien we aan bedrijven zoals [social media platform]. En dat zien we ook aan eh, gratis VPN eh, diensten. He, die jouw data he, want niks is gratis, maar het verdienmodel is dan jouw data, de websites die jij bezoekt. He, die kunnen allemaal verkocht worden eh, die gegevens. Eh, dus ja, data dat eh, dat is geld waard. En ik kan me voorstellen dat, dat er mensen zijn die interesse hebben in het klantenbestand van [the professional services firm]. En ik zeg nou steeds klantenbestand, maar ik kan me ook voorstellen het personeelsbestand wat wij hebben. Als je alle namen en adressen van onze medewerkers eh, op een USB stick hebt staan, ik, ik zou persoonlijk niet weet wat je er mee moet, maar ja, wellicht dat mensen daar iets in zien.

X: Ja. En het risico dat u noemt bij gratis VPN, speelt dat ook bij [the professional services firm] VPN?

Y: Nee. Nee, dat eh, nou ja, ja, nee is altijd zo zwart-wit, maar eh, dat vermoed ik niet. Als er niet mensen van binnenuit eh, onze IT-ers die binnen onze organisatie werken, dat serververkeer op een USB stik en te koop aan bieden, nee dan denk ik dat eh, dat dat risico minimaal is. En ik zeg minimaal, want nul is het nooit. Als iemand kan inbreken op die VPN server, ja, dan eh, dan hebben we alsnog een probleem. Maar van binnenuit verwacht ik dat niet nee.

X: En als we dan kijken naar al deze aanvallen, wat zou de impact van een aanval kunnen zijn?

Y: De impact van de aanval is dat eh, dat de vertrouwelijkheid naar je cliënten toe geschaad wordt en daardoor kunnen cliënten weglopen. Wat natuurlijk vervolgens een eh, een financieel verlies voor ons zal betekenen. He, als wij een client als [0:33:08 till 0:33:12 has been omitted] waarmee wij werken, waarvoor we werken, naar buiten lekken, ja, dan zal [company] waarschijnlijk naar een andere [0:33:20 till 0:33:22 has been omitted] op zoek gaan. En ik zeg nou [company], maar dat geldt voor iedere, voor iedere klant die we hebben.

X: Ja, zeker. Oké. En als we dan gaan kijken naar de VPN verbinding zelf, hoe veilig is een VPN verbinding?

Y: Ja, op een schaal van 0 tot 100 ofzo, of eh, wat, hoe veilig, ja, ik denk dat het op dit moment het meest veilige is eh, wat je eh, wat je als organisatie kunt inzetten.

X: Ja, en zijn er redenen wat u kunt bedenken waarom een VPN verbinding mogelijk niet veilig is? Of minder veilig?

Y: Nou ja, we maken natuurlijk steeds meer beschikbaar van clouddiensten. En die clouddiensten, daarvan zie je dat de servers eh, beheerd worden door externe organisaties. He, daar gaat dus ook onze data naartoe. He, onze nieuwe [an internal page] bijvoorbeeld, ja, die draaien op [company] servers, ik dacht in [country], maar dat weet ik niet helemaal zeker, maar ik dacht in [country]. Die data, die gaat dus tussen die VPN verbinding en die eh, [company] server. Ja, wat er bij de [company] en natuurlijk zijn daar allerlei eh, afspraken over en eh, liggen daar eh, contracten aan ten grondslag, maar uiteindelijk hebben wij geen zicht op eh, op de infrastructuur binnen die externe organisatie. En dat heb je met clouddiensten natuurlijk steeds vaker. Het is niet meer alleen binnen je eigen netwerk. He, dus als ik ergens een gevaar eh, zie, dan is het binnen die clouddiensten, die niet door ons beheerd worden. En we vertrouwen het allemaal wel, maar ja, we zullen niet de eerste zien die eh, waarbij toch blijkt dat het minder veilig is dan we denken.

X: Ja. En zijn er nog andere redenen die je kunt bedenken waarom een VPN verbinding mogelijk niet veilig is of minder veilig?

Y: Eh, nee. Nou, nee, ja, ik, kijk, ik kan me voorstellen dat een gebruiker die weet dat die een VPN verbinding gebruikt misschien wat minder zorgvuldig is. He, in het gebruik, wat die doet. Die onzorgvuldigheid, ja, dat is natuurlijk een potentieel risico. Eh, he, je kunt denken van nou ja, ik ben toch niet te traceren, dus eh, ga maar weet ik veel, op websites waar ik normaal eh, op mijn privé laptop niet naar toe ga. Wat zoals ik nu reclame krijg binnen, op mijn, op mijn [e-mail] scherm, of binnen [e-mail], ik heb geen idee waar ik ooit die eh, die zakelijke eh, he, dat zakelijke e-mailadres achter gelaten heb. Ik ben daar toch wel heel zorgvuldig in, maar kennelijk eh, is het toch ergens een keer binnen gekomen. Krijg nu allemaal elke dag reclame voor thermometers, neustrimmers en dat soort troep.

X: Dat is vervelend ja.

Y: Ja, dat is vervelend ja. Dat krijg ik om mijn privé laptop ook, maar goed, ja, op mijn zakelijke laptop wil ik dat niet.

X: Nee, zeker. En als we naar deze tekening kijken. Zou je mij kunnen uitleggen hoe het werkt als je verbinding maakt met dan een [company] clouddienst?

Y: Ja. Dat gaat, dat gaat volgens mij ook via die VPN server. [start drawing 18\_5]. Als gebruiker maak je contact met die [the professional services firm] VPN en die maakt eh, contact met eh, cloudservers van ja, ik zeg nou [company], nou [company]. Daar zit natuurlijk ook gewoon een eh, een server achter. He, die aanvraag die ik hier doe, via die VPN server leidt eh, en die zegt van he, [me], mag die toegang hebben tot die server, wat mag die dan en dat, dat verkeer loopt hier. [start drawing 18\_6]. Ja, dit verkeer is versleuteld. He, dus iemand die hier op inbreekt, die kan niet lezen wat ik daar doe. He, want deze informatie gaat natuurlijk twee kanten op, ik doe hier een aanvraag voor bijvoorbeeld [0:38:10 till 0:38:11 has been omitted] he, die gaat die kant op. Maar daar gaat de informatie over die [0:38:16 till 0:38:17 has been omitted], die gaat eh, die gaat uiteraard eh, weer terug naar mij toe. Want ik zie het uiteindelijk op mijn PC. Het wordt wel een eh, wordt wel een drukke tekening.

X: Ja, maar nog steeds heel duidelijk.

Y: Ja, misschien zit ik er helemaal naast hoor. Maar goed, jij vraagt mijn begrip van eh, van een VPN verbinding, en dat is wat ik ervan heb.

X: Ja, zeker. Oké. Dit waren tot zo ver mijn vragen. Zijn er nu nog dingen over een VPN die niet ter sprake zijn gekomen?

Y: Nee, volgens mij niet. Ja, nee. Nee, als het gaat om de [the professional services firm] organisatie, hebben we denk ik alles wel, wat ik weet eh, of denk te weten, laat ik het goed zeggen, hebben we alles wel gehad.

X: Ja. Oké. Dan eh, tot zo ver het interview. Ik wil u heel erg bedanken voor uw deelname, want dit helpt mij heel erg. En-

Y: Alsjeblieft.

X: Heeft u nog vragen ook voor mij?

Y: Eh, nou, ik ben wel benieuwd hoe je op een gegeven moment dat spectrum definieert van experts en eh, mensen die totaal niet, die niet eens weten wat VPN betekent.