# Transcription expert 7

Duration: 48 minutes

X: Dan de eerste vraag voor het interview. Kun je mij uitleggen wat een VPN is?

Y: Eh, ja. Hangt ervan af hoe technisch je het wilt. Eigenlijk de meest eenvoudige vertaling daarvan is een eh, ja, eigenlijk een privé lijn wat je hebt richting een bepaalde locatie, richting een server, voordat je verbinding hebt met eh, bijvoorbeeld het internet, maar dat kan ook een VPN zijn, een lijn zijn naar een bepaalde server voor je verbinding hebt met een andere server. Dus eigenlijk he, om een privé lijntje die eh, op een manier beveiligd is.

X: Wat bedoel je met een privé lijn?

Y: Dat gaat dus al echt om een virtuele verbinding, dus eh, een eh, connectie he, tussen jouw eigen device en een eh, en een server. Dat gaat dus wel over het internet, maar he, je bent niet direct initieel verbonden met het internet. In de vorm van je zit niet op het publieke netwerk, je zit in een afgescheiden kanaal.

X: Waar zit je dan niet in het publieke netwerk bedoel je?

Y: Sorry. Je maakt wel gebruik van eh, eh, van natuurlijk dezelfde techniek, maar je zit niet direct in het publieke netwerk. In het gedeelde netwerk. Dus je bent altijd met een beveiligde verbinding direct naar een eh, een doellocatie, naar een server.

X: Hoe is de verbinding beveiligd?

Y: Sorry?

X: Hoe is de verbinding beveiligd?

Y: Eh, met encryptie.

X: Oké. En wat is encryptie?

Y: Eh, encryptie is versleuteling van data. En dat gaat via specifieke, oeh, eh, ja, ik denk dat je het het best kan omschrijven als tunnels. Dus eigenlijk een soort van eh, van poortje. Eh, en dan om die eh, om die te kunnen lezen, wat erin staat, heb je een bepaalde sleutel nodig. En als je die sleutel niet hebt, dan kan je daar dus niet in.

X: Duidelijk. Eh, wat bedoel je met een tunnel?

Y: Een datatunnel zeg maar. Een poortje, kan het ook een deur noemen of eh, een transportkanaal, laten we het zo noemen.

X: Oké, en eerder noemde je dat de verbinding gaat naar een server. Hoe gaat deze verbinding naar een server?

Y: Kan op verschillende manieren, he. Een private line kan je ervoor hebben of je kan een VPN hebben wat gewoon valt over het eh, over het reguliere netwerk gaat. Dus je wordt altijd via een he, of via een internetverbinding direct of een private line betekent eigenlijk een privéverbinding daarvoor richting een server.

X: En wat is een server?

Y: Een server is een device, ja, eigenlijk je, je, net als je je computer hebt, een client, is dat een device voor het regelen van, in dit geval, een eh, een dataverkeer. Dus de server kan zijn in eh, specifiek in dit geval een router vanuit de VPN, maar achterliggend zit daar een he, een basisplatform.

X: Dankjewel. Waarom gebruik jij een VPN?

Y: Waarvoor ik het gebruik vanuit mijn werk of waar ik het gebruik persoonlijk of algemeen waarvoor iemand een VPN gebruikt?

X: Ja, waarom jij de VPN gebruikt binnen [the professional services firm].

Y: Waarvoor ik hem binnen [the professional services firm] gebruik, oké. Binnen [the professional services firm] eh, gebruik ik hem om diverse eh, authenticaties met diverse eh, applicaties. En denk hiervoor aan eh, even kijken, [an internal page] is volgens mij nu niet meer, maar [an internal page] bijvoorbeeld, zit ook nog achter een VPN. Dus als ik in, bij [an internal page] wil komen, kan dat alleen maar via een specifiek eh, punt, dus moet ik eerst VPN naar zo een eh, locatie gaan, naar zo een server, en daarvandaan kan ik de omgeving, in dit geval eh, [an internal page] benaderen. Maar dat is ook voor-

X: En wat-

Y: Sorry, wat zei je?

X: Je kunt je zin afmaken.

Y: Ja, er zijn dus ook overige applicaties die draaien eh, ten minste die alleen toegankelijk zijn vanuit VPN-locatie binnen [the professional services firm].

X: En wat bedoel je met authenticatie met applicaties?

Y: Authenticatie eh, betekent he, dus het toegang krijgen tot, dus het hele proces omtrent het eh, identificeren en toegang krijgen tot een omgeving of applicatie.

X: Zijn er nog andere redenen waarom jij een VPN gebruikt?

Y: Binnen [the professional services firm] momenteel-

X: Ja.

Y: Hebben we het over, he, de scoping. Eh, ik zit even te kijken op welke applicaties dit nog van toepassing is. We hadden het over voorheen ook op [an internal page] natuurlijk, voor een stukje veiligheid, want het is vanuit authenticatie zit natuurlijk daarachter een stukje beveiliging. Nee, ik weet niet over welke je het nu precies eh, specifiek naar opzoek bent.

X: Welke handelingen voer jij uit om een VPN-verbinding te maken?

Y: Wat ik uitvoer persoonlijk is eh, ik moet zowel eerst in mijn eh, in mijn laptop moet geconfigureerd zijn het adres van de VPN-server, als die geconfigureerd is en dat staat over het algemeen al gedaan vanuit IT staat dat in je device. Dan moet je inloggen met jouw gebruikersnaam met een eh, een authenticatiecode en die authenticatiecode is onderdeel, een code die eh, die je zelf bepaalt, een vaste pin en het tweede deel van die code wordt gegenereerd via een soft token. Dat betekent dus he, een token die op jouw mobiel device wordt gegenereerd.

X: En die soft token, zijn er nog andere mogelijkheden naast een soft token?

Y: Voor zo ver ik weet is er een eh, kan een tijdelijke soft token worden gegenereerd vanuit helpdesk, eh, voorheen hadden we hardtokens, die zijn als het goed is geheel uit gefaseerd, maar dat zal vast nog wel he, [the professional services firm] kennende zullen die ook nog wel in de omloop zijn.

X: En waarom zijn die uit gefaseerd, weet je dat?

Y: Een keychain is natuurlijk minder veilig dan een, een token op je eh, mobiel device waar nog eens een wachtwoord op zit. Eh, maar je houdt ook het hele stukje beheer daarvan- Het is makkelijker om eh, keygenerators te beheren dan de fysieke eh, tokens die mensen bij zich dragen. Het is ook makkelijker om een token te verliezen wat dat betreft, dan een mobiele telefoon. En als die token is verloren, dan heeft iemand gelijk toegang tot die code en op je mobiele telefoon zit dan altijd nog en een wachtwoord plus je device kan ook vanaf afstand worden gecleared, dus leeggehaald. Dus als je aangeeft dat jouw telefoon gestolen is bijvoorbeeld, dan eh, zal daar niet eh, niet zo snel misbruik van gemaakt kunnen worden.

X: En op welke apparaten gebruik jij een VPN?

Y: Ik gebruik het persoonlijk alleen nu op mijn laptop, maar ik kan dat natuurlijk ook gewoon op mijn telefoon gebruiken of elk ander willekeurig device, als ik daarvoor eh, richting [the professional services firm] apps zal benaderen. Momenteel eh, is dat niet ingeregeld.

X: Je kan eh, meerdere apparaten gebruiken om verbinding te maken met [the VPN of the professional services firm]?

Y: Volgens mij kan dat ook vanuit eh, de omgeving, ik weet even niet zo goed hoe die omgeving nu heet, dat is een paar keer van naam veranderd, maar we hebben [example of mobile application] hadden wij op de telefoon. Eh, maak ik nu even geen gebruik meer van. Waar wij uiteindelijk dus ook via een VPN-verbinding eh, bent verbonden.

X: En kan jij aan mij uitleggen hoe een VPN werkt? Het meer technische waar je het over had. Je kunt als je wilt het whiteboard daarvoor gebruiken.

Y: Ja, oké, dat is even basisconcept, he. Even kijken. [start drawing 7\_1]. Basisconcept is ik heb een device, ik heb een mediating server en, nou laten we het noemen, heb ik een, o, gaat niet, wat doe ik verkeerd, eh, een device, een server en tekenen, je hebt het internet, laten we het zo even noemen. Nou, dit is mijn eh, mijn client, tekst had ik hier ook ergens. Mijn client, dit is- Server noemen. En dan voor eh, even kijken hoor, hoe ga ik terug. Dus het idee is, o, wacht, hier nog even internet bij, dit het eh, het internet, publiek noemen of algemeen internet, is wel goed denk ik voor dit doel. [start drawing 7\_2]. Het idee is dat je voordat je echt hierzo, voordat je, o, hoe verwijder ik.

X: Je kunt op undo, het pijltje, klikken.

Y: [start drawing 7\_3]. Dit is het basisidee, dat ik hier, als ik vanuit mijn client verbinding wil maken hier ergens met een device X, ga ik eerst naar de server, hiervandaan wordt die, ga ik door vanuit die server naar het publieke deel van het internet of naar het, een, eh, wordt verkeer gemanaged. Het kan ook zijn dat een eh, een doel waar ik heen ga op dezelfde server staat, in dezelfde omgeving als de VPN-omgeving. [start drawing 7\_4]. Dus ik heb hierzo mijn client, die staat ergens willekeurig. En deze server staat binnen het netwerk van eh, van [the professional services firm]. [start drawing 7\_5]. Nou, om een voorbeeld te noemen van [an internal page], die staat volgens mij hier ergens he, dus dan heb je hier eh, een [the professional services firm] app, laten we het zo even noemen. Die staat dan binnen de omgeving van [the professional services firm], waardoor ik dus niet door hoef weer terug het internet op. Initieel is dit dus, deze lijn, dit is die private line waar ik het over had. Wat dus eigenlijk een soort van encrypted tunnel is eh, richting de ontvangende server.

X: En waar begint en eindigt de encryptie?

Y: Dit deel, dus van je client tot aan de server is encryptie. Tot aan je VPN-

X: Daarna niet meer.

Y: Daarna he, in principe op het moment als je daarna eh, hangt ervan af waar je naartoe gaat in je [the professional services firm] netwerk. Je zou in principe ook encryptie verder nog kunnen hanteren eh, maar in principe als je hiervan uitgaat, na je VPN nog even terug, naar je publieke internet op, dus naar een willekeurige website, dan heb je natuurlijk niet meer een encryptie daarop zitten. Want een encryptie werkt tussen twee partijen die allebei de sleutel hebben. Duis als je hier nar een willekeurige omgeving gaat op het internet, die heeft he, die heeft niet een sleutel, die heeft he, die kan nooit, kan geen gebruik maken van die encryptie.

X: Maakt het voor deze tekening nog uit eh, wat je fysieke locatie is?

Y: Nee, die client dat is dus overal. He, fysieke locatie van je client is niet gebonden. Dus ik kan eh, net, ik zit nu ergens op een access point, als ik nu aan de andere kant van de wereld ga zitten is het natuurlijk precies dezelfde situatie.

X: Duidelijk. Dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Eh, ja, is een goede natuurlijk. Want aan ene kant, al het verkeer wat via die verbinding gaat he, wordt natuurlijk getunneld, dus dan zou je zeggen dat voor dat verkeer veiliger is, ten minste beveiligd is laten we het zo nu even noemen. Het werkt ook twee kanten op, dat betekent wel dat verkeer dat je binnen krijgt via de tunnel vanuit de andere kant eh, dat dat potentieel een eh, zwakte punt is, want het gaat door je beveiliging heen van je systeem. Een voorbeeld stel he, die server hier die gaat zo meteen eh, allemaal malicious berichten versturen, die VPN-verbinding die gaat beide kanten op, dus van mij naar die server, maar ook andersom. Dus dat is potentieel een poort die vatbaar is voor beveiligingsincidenten.

X: Ik snap niet helemaal wat je bedoelt. Eh, wie zou dan, waarvandaan zou dat verstuurd worden?

Y: Sorry?

X: Waarvandaan zou ja, malicious eh-

Y: Nee, kijk, wat ik bedoel is, je krijgt hier een open poort die dan ontstaat, he, dus tussen je client en je server. Dat betekent dat voor al het verkeer dat vanuit die server he, dat zal een, dat gaat dus buiten je beveiliging laag om die je hierzo aan je clientside hebt voor overig verkeer. Dus hier bestaat zeg maar een trusted connection tussen.

X: Heeft een VPN-verbinding verder nog invloed op jouw computerbeveiliging?

Y: Eh, nou vast wel, maar ik zal het nu even niet weten eerlijk gezegd. Weet niet welke kant je daarmee bedoelt.

X: Of er nog meer invloed is. Dan een hele brede vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Digitale dreiging vanuit scoping nu ik ben aan het werk op mijn [the professional services firm] laptop. En dan de dreiging voor [the professional services firm], die bedoel je denk ik, of niet.

X: Ja.

Y: Oké. Nou, de grootste dreinging die ik heb dat eh, direct zie ik als alles wat door klanten wordt aangeleverd, of alles wat door collega’s wordt aangeleverd via onofficiële kanalen. Altijd een, een, eh, grootste dreiging zit bij mensen op dit gebied. Dus de, je kan nog zo mooi je systemen hebben ingericht he, dat, dat je allemaal beveiligingslagen hebt ingebouwd, maar als vervolgens de eh, ik noem maar even wat, een collega die eh, die krijgt een mail, een mail door en in die mail staat salarisinkomsten of bonussen van [role] en die klikt erop en die stuurt dat vervolgens ook door naar jou, ja, of eh, vanuit de klant krijg je bestanden door die eh, laten we zeggen niet eh, niet heel schoon zijn en die gaan via onze, buiten de formele kanalen waar bestanden gescand worden, worden die met ons gedeeld.

X: Wat bedoel je met ze gaan buiten de formele kanalen?

Y: Sorry?

X: Wat bedoel je daarmee, dat ze buiten de formele kanalen gaan die gescand worden?

Y: Nou je he, natuurlijk hebben wij vanuit [the professional services firm], vanuit het netwerkverkeer wordt he, wordt gescand, maar ook vanuit mail en vanuit een eh, [an internal page], zit ook bepaalde scanning op. Maar als iemand ik noem maar wat via WeTransfer wat binnen haalt of op een andere manier eh, waarbij die maatregelen dus niet meer van toepassing zijn, dan is dat een eh, eh, een gemis in je, in je defensie.

X: Duidelijk. En als je nadenkt over verschillende soorten digitale dreiging, verandert de soort dreiging dan door een VPN-verbinding?

Y: Je bedoelt in een situatie waarin je alleen maar op VPN werkt? Of?

X: Ja, als je via VPN werkt, heeft dat invloed op de digitale dreiging, op een digitale dreiging?

Y: Ja, oké, stel he, we zouden alles alleen maar via VPN werken he, dus ik ben nu met VPN he, stel ik zal altijd via VPN verbonden zijn en al het verkeer gaat over VPN, dan krijg je dus dat in dit gebied hierzo, deze kant, dat het makkelijker te monitoren wordt. Dus je krijgt minder kanalen waarin data eh, richting het publieke netwerk gaat. Dus je krijgt he, wel dat dit, deze kant hier rechts belangrijker wordt, dus je gaat je kanalen beperken, dus dan wordt het wel he, krijg je een bottleneck daarop zitten. Maar het is wel beter te beheersen. Aan de andere kant, het heeft dermate veel performance dat dat vraagt, dat ik niet zie een situatie waarin [the professional services firm] op kort termijn alles via VPN te laten verlopen. Juist zijn er nu bewegingen gemaakt om zaken zoals [an internal page] niet via VPN te hebben.

X: Wat bedoel je met kanalen beperken?

Y: Eh, met je lijntjes. Dus een lijntje kan zijn als ik hier mijn data altijd via deze server laat verlopen, dan weet ik dat alles eh, he, eh, hierzo ook binnen gaat komen. Als ik eh- [start drawing 7\_6]. Dus of ik nou hier naar dit punt ga, hierzo ga, hierheen ga, of daarheen ga, he, dat gaat altijd via deze server in plaats van eh, dat ik vanuit de client direct daarheen kan benaderen. In plaats van dat je al die lijntjes zo he, dus al die dreigingen zou moeten afvangen, heb je dat nu vanuit een centraal punt.

X: Eh, en dan was dit omtrent digitale dreigingen, maar heb jij op een normale dag ook te maken met sociale dreigingen binnen [the professional services firm]?

Y: Bedoel je dan wederom heeft dat nog een relatie tot eh, VPN, of bedoel je algemeen sociale dreigingen in de vorm van social engineering op kantoren en dergelijke?

X: Ja, algemeen.

Y: Natuurlijk heb je op he, op kantoren heb je sociale dreigingen. En ik weet niet in hoeverre je op de hoogte daarvan bent, maar we hebben binnen [the professional services firm] [0:23:58 till 0:24:06 has been omitted]. En je kan ook zien dat mensen eh, toegang tot kantoor verkrijgen middels social engineering door gewoon met iemand mee te lopen. Dat is mogelijk. En dat is ook een van de, van de he, van de grote mensaspect waar ik net op doelde van awareness. Weet wat je aan het doen bent, dus als iemand achter je aanloopt, of je ziet iemand [0:24:26 till 0:24:27 has been omitted], spreek die erop aan. Maar hetzelfde, [0:24:30 till 0:24:31 has been omitted] en je gaat zelf niet fatsoenlijk om met je wachtwoorden of je eh, met je laptop open laten staan he, ongelogd of überhaupt je laptop onbeveiligd, niet aan een eh, niet op slot achterlaten.

X: Heeft een VPN-verbinding invloed op deze sociale dreigingen?

Y: Eh, ja in, ja en nee. Ja, als jij, hangt ervan af hoe je er mee omgaat. Als je, op het moment dat jij zo meteen nog steeds altijd alle ...(0:25:15) doet opnieuw moet authentiseren bij die VPN-omgeving, dus iemand heeft toegang tot je laptop, maar vervolgens kan die nergens bij omdat die niet binnen die, die authenticatie laag heen gaan, dan kan dat bijdragen aan je beveiliging.

X: Oké, en je zei ja en nee. In welke zin bedoel je dan nee?

Y: Eh, dat eh, het grote deel, momenteel, het is als ik een VPN-verbinding op start, start ik nu een keer een VPN-verbinding op en ik blijf gewoon de rest van de dag blijft die draaien. Of een x aantal uur blijft die draaien, dan steun je nog steeds vooral op de toegang tot je laptop zelf. Het is dus niet dat ik elke keer opnieuw die verbinding moet initiëren.

X: Oké. Eh, en als je nadenkt over deze digitale en sociale dreigingen, wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Als [the professional services firm] zijnde eh, ja, dat kan he, dat kan divers zijn. Het kan zijn dat ze op zoek zijn naar specifieke financiële data, want we kunnen natuurlijk bij zeer gevoelige klant data. Het kan zijn dat het he, direct een target is op eh, voor [the professional services firm] als organisatie, dan is het doel de organisatie is diskrediet brengen. Het kan verschillende dingen zijn.

X: Kan je voorbeelden bedenken van aanvallers?

Y: Voorbeeld, nou ja, iemand die eh, bijvoorbeeld eh, [0:27:00 till 0:27:05 has been omitted] zal een motivatie kunnen zijn. Gezien dat wij natuurlijk heel veel [0:27:11 till 0:27:16 has been omitted]. Daar kan significant veel geld mee verdiend worden. Ik denk dat dat cruciaal is. Aan de andere kant hebben we ook heel veel persoonsgegevens, direct, indirect. Maar als specifiek [the professional services firm] wordt getarget, zal mijn inschatting zijn dat dat of gaat om een stukje eh, financieel gewin [0:27:37 till 0:27:39 has been omitted] of reputatieschade.

X: Dat is meer motivatie beschrijven eh-

Y: Sorry?

X: Dat is meer motivatie beschrijven, maar wie of wat is dan echt de aanvaller zelf?

Y: Eh, ja, een individu, een persoon. Ik zal verwachten he, dat dat niet intern is vanuit een [the professional services firm] bijvoorbeeld. Want wij hebben daarvan steun je natuurlijk een deel op het stukje integriteit van überhaupt mensen die bij [the professional services firm] werken en eh, stukje eh, [0:28:21 till 0:28:29 has been omitted]. Ik denk dat [the professional services firm] he, eerder een target is van een specifieke hacker wat dat betreft dan, social engineering he, kan ook een manier van hacking zijn. Maar niet zo zeer van hacktivisten.

X: Duidelijk. En eh, wat voor achtergrond heeft een aanvaller?

Y: Eh, ja, die zal zelf ook een [0:28:59 till 0:29:08 has been omitted] of eh, aan de kant van social engineering, als het eh, op een andere manier technisch vlak, dan zal het, zal het, ja, haast een whizzkid zijn. Dus of een hacker gewoon met heel veel he, ervaring of iemand die persoons gedreven erop uit gaat om [0:29:32 0:29:32 has been omitted] data te ontvreemden. Alleen heb je natuurlijk wel specifieke kennis nodig om het eh, om het verder nog toe te passen. Het is niet zoals een willekeurig persoon een [0:29:45 till 0:29:55 has been omitted].

X: Eh, heeft een VPN-verbinding nog invloed op de soort aanvaller?

Y: Eh, ja eh, nu specifiek voor [the professional services firm] in de situatie waar we dan alleen gebruik zouden maken van VPN bedoel je? Of in de huidige situatie?

X: Ja, als je gebruik maakt van de VPN altijd ten opzichte van de huidige situatie.

Y: Oké, dus de situatie waarbij we altijd gebruik maken van VPN. Eh, ja, dan heb je een eh, wellicht een hele andere ingangshoek inderdaad. Eh, specifiek eh, de techniek voor dat hacken daarvan zou ik niet weten. [0:30:44 till 0:30:54 has been omitted].

X: En je zegt wel eh, dat waarschijnlijk de soort aanvaller verandert, op wat voor manier verandert de aanvaller?

Y: Dat he, als je vanuit de techniek probeert dan aan te vallen, kijk eh, je krijgt dan wat grootschaliger ja, je krijgt een specifieke VPN-verbinding die, dus vanuit een centraal punt waar je een ingang moet vinden. En niet aan de kant van heel veel clients die allemaal potentieel een ingang hebben. Al die he, weer het verschil tussen een centrale situatie waar je je verkeer monitort ten opzichte van diverse eh, eh, gedecentraliseerde kanalen die je zou moeten monitoren en beveiligen uiteraard.

X: En wat zou de impact van een aanval kunnen zijn voor [the professional services firm]?

Y: Eh, grootste impact reputatieschade. He, dus impact dat klantgegevens worden ontvreemd, persoonsgegevens worden ontvreemd en je hebt natuurlijk [0:32:05 till 0:32:39 has been omitted], als [the professional services firm] lek jij die gegevens uit, dan krijg jij een behoorlijke dreun in je reputatie. [0:32:46 till 0:33:00 has been omitted]. Een situatie waarin dus klantdata of eigen data wordt ontvreemd, nou dan heeft het een gigantische impact.

X: Zou je nog meer voorbeelden van impact kunnen bedenken?

Y: Ja, het kan natuurlijk ook interne verstoring zijn van de processen binnen [the professional services firm]. Maar ik denk dat de grootste is vanuit [the professional services firm] zelf, is een stukje reputatieschade.

X: Duidelijk, oké. Dan over de VPN-verbinding zelf, hoe veilig is een VPN-verbinding?

Y: Eh, dat hangt uiteindelijk vanaf hoe die verbinding beveiligd is. In de vorm van he, de ene VPN-verbinding is niet even goed beveiligd als een andere VPN-verbinding. En hier moet ik heel eerlijk in zeggen, ik weet dat hier verschillende concepten van zijn, maar ik ken die niet in detail.

X: Oké, en kan jij kwetsbaarheden in de VPN-verbinding bedenken?

Y: Ja, een van de grootste is natuurlijk je, je encryptie.

X: Oké-

Y: Of de he, dus he, als je encryptie, we draaien nu eigenlijk volledig op steunt (0:34:34), als die eh, als je daar niet meer, als je niet meer kan steunen op een stuk vertrouwelijkheid van die data, ja, dan is eigenlijk het hele concept weg natuurlijk.

X: En als je nadenkt over deze onveiligheden, maar ook wat je eerder noemde, veranderen jouw handelingen hierdoor?

Y: Welke handelingen bedoel je nu? Of hoe je acteert richting het eh, richting externe bronnen of?

X: Jouw omgang met VPN.

Y: Mijn omgang met VPN, nee, ik gebruik VPN-verbinding binnen [the professional services firm] he, nu, in de huidige situatie alleen maar om naar eh, bepaalde applicaties toe te gaan. Verder zet ik hem uit. Dat ook vanwege een stukje eh, capaciteitsproblemen die we hebben binnen [the professional services firm]. Terwijl wij hebben he, ik kan wel continu via VPN werken, maar dat heeft ook impact op de eh, capaciteit van de VPN-server, aangezien we wereldwijd nu allemaal aan het thuiswerken zijn. Het is niet zo dat ik bewust meer via VPN zal gaan werken. Maar ik ben wel van mening dat als [the professional services firm] zijnde breed, moet je wel goed nadenken over welke verantwoordelijkheden je bij je eindgebruikers he, dus hierzo bij je clients allemaal neerlegt, want niet iedereen is even, heeft dezelfde awareness van risico’s van buitenaf en kan daarin dus ook zelf de juiste eh, inschatting maken of ze wel of niet bijvoorbeeld zo een WeTransfer moeten gaan gebruiken.

X: En gebruik jij nog wel eens een VPN-verbinding op een andere locatie dan thuis?

Y: [0:36:33 till 0:36:36 has been omitted]. Eigenlijk alles wat niet op kantoor is. En op kantoor heb je eigenlijk ook een VPN-verbinding he, op de kantoren hebben ze een interne verbinding. Dus je maakt verbinding met het kantoor netwerk en daarvanuit zitten hun, zit je met een centraal VPN-netwerk zit je verbonden. ...(0:36:56). Dus het is niet als je op een kantoorlocatie zit eh, dat er dan totaal geen gebruik is van VPN, alleen maak je er zelf dan geen eh, merk je er zelf op dat moment niets van.

X: Zou je nog andere situaties kunnen bedenken waarin je een VPN-verbinding gebruikt op een andere locatie?

Y: Eh, je bedoelt op het moment als je op een onveilige locatie zit extern. Dat zal-

X: Ja, bijvoorbeeld.

Y: Dat zal kunnen, maar als je op een onveilig netwerk zal zitten dan zou ik eerder mijn mobile device gebruiken voor eh, mijn mobiel kanaal. Niet zo zeer dan op een onbeveiligd netwerk.

X: Op je mobiel kanaal?

Y: Ja he, een hotspot op je mobiel, dus dat je via het mobiele netwerk gaat.

X: En dan gebruik je daarbij geen VPN-verbinding?

Y: Nou, hangt er vanaf he, wederom he, als ik op mijn mobiel gebruik als een hotspot en ik ga naar services waarvoor ik geen VPN-verbinding nodig heb, dus ik hoef niet van specifiek [the professional services firm] services gebruik te maken, waar, die afhankelijk zijn van VPN, dan zou ik daar niet een VPN-verbinding voor gebruiken, nee.

X: Waarom gebruik je een mobiele hotspot in plaats van een openbaar netwerk?

Y: Omdat ik van mijn mobile hotspot weet ik zeker dat het dan direct via de eh, internetprovider verloopt en vanuit een openbaar, onbeveiligd hotspot heb je altijd het man in the middle risico. Stel dat al je data he, potentie voor je data om onderschept te worden, in ieder geval gemonitord te worden.

X: Heeft een VPN-verbinding hier impact op?

Y: VPN-verbinding zal dat risico zeker beperkter. Dus als jij op een onbeveiligd eh, eh, ten minste op een slecht beveiligde access point zit en je hebt een VPN-verbinding, dan pak je een directe tunnel he, met de server. Waardoor je dus weer, vanwege de encryptie, een beveiliging laag toevoegt.

X: Oké, duidelijk. Eh, dit waren tot zo ver mijn vragen. Heb jij dingen over VPN die nu niet naar voren kwamen?

Y: Eh, ja er zijn natuurlijk he- Nee, het gaat nu specifiek he, dat snap ik, je onderzoek gaat over VPN en in welke mate dat kan bijdragen aan je beveiliging. Dat is hoe je onderzoek is ingericht. Eh, dan heb ik hier niet specifiek nu nog toevoegingen over. Wel mijn vraag in hoeverre eh, vanuit oplossingen voor [the professional services firm], dus even buiten het onderzoek om, of het antwoord alleen maar vanuit VPN moeten zoeken.

X: Dan eh, over de [the VPN of the professional services firm] niet per se in eh, betrekking tot beveiliging, maar algemeen, is er dan nog iets dat niet ter sprake is gekomen?

Y: Nou ja, [the VPN of the professional services firm] an sich, kijk ik vertelde je dat wij een standaard key hebben die wij moeten invoeren, een persoonlijke key. Eh, nou die key die heb ik volgens mij eh, ten minste ik heb hem een keer toen ooit ingesteld, ik zou niet eens weten of ik die kan aapassen. Dus he, als het gaat om de maat van beveiliging hoe die nu is, voor [the VPN of the professional services firm] zie ik wel wat aandachtspunten. Een daarvan is een VPN-connectie kan gestart worden volgens mij vanuit iedereen die een eh, die over een username en uiteindelijk wachtwoord plus key beschikt. Maar dat betekent ook dat je meerdere sessies per persoon kunt hebben. Zit uiteindelijk dan wel gekoppeld aan je AD-gebruiker, dus het is wel mijn laptop die ik heb, waar ik ben ingelogd, die geeft, zorgt ook sowieso voor de authenticatie met de verschillende servers. In theorie zal dat dus betekenen dat als ik mijn eh, mijn mobiel niet heb en ik moet inloggen, dat ik op iemands anders inlognaam zou inloggen bij eh, op VPN, zijn code invul, of hij zijn code invult, zijn authenticatiecode invult en ik vervolgens wel verbonden ben met, met de VPN-server. Dus hoog over he, ja, als je op zoek bent naar nog verbeterpunten in de huidige VPN is dat misschien nog een aandachtspunt dat je VPN-connectie ook gekoppeld zit direct aan je AD-user. En eh, dat een standaarddeel van je wachtwoord he, wat er inzit, een deel van je code dat vaststaat, dat het wellicht wel handig is om dat ook met regelmaat te wijzigen. Dat niet statisch te laten voor onbeperkt.

X: Duidelijk. En eh, je noemde meerdere aanbevelingen, kan je nog meer aanbevelingen bedenken?

Y: Eh, ja sowieso he, je hebt he, dit is eigenlijke en soort van eh, je hebt ook VPN, ik weet deze techniek nog niet helemaal he, maar ik weet je hebt tegenwoordig ook een VPN by design, dus volgens mij een VPN-verbinding die eh, automatisch wordt geïnitieerd op het oment als dat je je laptop opstart. He, dus dat maakt dan gebruik uiteindelijk, dat steunt dan op de authenticatie die je hebt om op je eh, user in te loggen en vervolgens haalt die zelf automatisch al een VPN-verbinding op met de server waar verder geen handelingen meer nodig zijn.

X: Oké, zie jij dat als een voordeel of een nadeel?

Y: Eh, ik zal he, die techniek zal gezien kunnen worden als een voordeel. Dat zal he, gebruikt kunnen worden, maar dan zal ik wel zelf nog een eh, een notificatiesysteem bij hebben. Oftewel dat je een eh, bericht krijgt op je telefoon waarbij je nog op een knopje moet drukken van accept bijvoorbeeld. Maar nogmaals, ik ben niet helemaal thuis nog in die techniek.

X: Nee, dat is geen probleem. Oké, eh, ja, dus tot zo ver mijn vragen.