# Transcription expert 1

Duration: 82 minutes

X: Dan begin ik met de eerste vraag van het interview. Kan je mij vertellen wat een VPN is?

Y: Wat een VPN is? Eh, wat is de gewenste doelgroep voor deze uitleg?

X: Ja, het is de bedoeling dat je zo veel mogelijk vertelt wat jij van VPN weet, dus, eh, ja, mij uitlegt wat een VPN-verbinding is.

Y: Oké, voor mij is een VPN-verbinding- Het staat voor Virtual Private Network. Eh, virtueel betekent softwarematig. Eh, wat het doet is, het legt een verbinding eh, van een endpoint, ofwel een startpunt, dus een endpoint kan betekenen of jouw computer, of jouw eh, mobiel, of een tablet, een veilige verbinding te kunnen maken met een netwerk. En vaak noem je dat dan een intern netwerk. He, dus wat het doet, je legt eigenlijk een tunnel tussen iets wat normaal gesproken niet binnen het netwerk ligt, he, doordat je niet verbonden bent met het netwerk, eh, tot een netwerk, eh, ja, een intern netwerk, een intern onderdeel van het netwerk. Want meestal heb je, eh, vanuit een computernetwerk heb je eh, een, een, extern facing netwerk en een intern netwerk, he, dat zijn segmenten van een netwerk. Eh, het externe netwerk is vaak verbonden met het internet. Daar kun je vanuit elk punt van de wereld, he, zolang je het adres weet, het uiteindelijke adres weet, kun je daarop inloggen. Eh, maar op het moment dat jij, bij resources of, he, de, de dingen, dingen, servers noemen we het op andere computers, websites wil met een privé IP adres zeg maar, moet je dat doen via ofwel connecten via het netwerk zelf, dat is vaak als jij binnen het kantoor bent of wat dan ook, dan maak je direct verbinding met het interne netwerk, he, dan kun je praten met alles binnen in ieder geval binnen dat segment van het netwerk. Maar bij een VPN laat je iemand toe die niet in de buurt is van het netwerk, om via het internet eigenlijk, eh, een andere lijn te leggen naar die interne netwerken. Eh, ja, dat is hoog over wat een VPN is. Een VPN is eigenlijk, ja, ze noemen het niet een end-to-end encrypted beveiligd, he, dus je maakt eigenlijk een beveiligde verbinding, maar die beveiliging die begint pas, he, die begint bij het apparaat tot aan waar je binnenkomt aan de andere kant van die lijn. He, dus op het moment dat je aan de andere kant zit, is je, is je, eh, is je netwerk, of je, ja, je traffic, je verkeer is dan niet meer beveiligd. Die beveiliging kun je dus op verschillende manieren doen, daar worden verschillende protocollen bij gebruikt, dat kun je zelf instellen. Dus, dat zijn, eh, bepaalde, eh, cryptografische, eh, ja, handshakes noemen ze dat, maar dat zijn protocollen, he, waar punt A met punt B praat, eh, en punt B weer terugpraat met punt A, om te zeggen, om te verifiëren wie je bent. En dat doe je door middel van bijvoorbeeld in te loggen met een wachtwoord eh, of een username en een password. Eh, en de meeste VPN-oplossingen die gebruiken ook een tweede vorm van verificatie, dus een hardware of een software token, die je toevoegt aan je gebruikersnaam en wachtwoord. Omdat het ontzettend gevoelig is om, om ineens vanuit een onvertrouwd punt in de wereld kunnen inloggen op een vertrouwd punt. Die zou je goed dicht moeten gooien. Eh, verder bestaan er ook verschillende vormen van VPN. Dus, waar je, eh, ja, ook een volledige, ja, ik noem het volledig en split, split tunnel. Dus je kunt al het verkeer door een VPN leiden en wat er dan vaak gebeurt, is dat je al het verkeer naar het datacenter stuurt, die je dan vervolgens weer doorstuurt naar het juiste punt. Of je hebt een gedeelde of een split, he, en dan bepaald een organisatie welke endpoints, oftewel welke IP-adressen door een VPN-tunnel moeten en welke niet. En daarmee kun je de hoeveelheid data die je door je datacenter heen leidt eh, verminderen. Heel veel mensen hebben niet door dat dat zo werkt. Dus een voorbeeld is dat een organisatie kan zeggen, oké, ik wil al het verkeer naar [social media platform], [social media platform], [social media platform], [social media platform], allerlei social media en [social media platform] bijvoorbeeld, die laat ik gewoon via het internet verlopen. En al het andere verkeer, of al het verkeer dat naar een intern object is gericht, dat laten we door de VPN heenlopen. Eh, ja, dus dat zijn verschillen daarin. Eh, dan zijn de verschillen ook, ja, wat ik ook van VPN weet is dat er natuurlijk veel verschillende aanbieders zijn van VPN. He, dat is zoals ik al eerder zei, het is virtueel, dus het is software gedreven. Eh, en wat mensen ook vaak niet beseffen, is dat die, eh, dat die software ook, ja, eigenlijk, je kunt heel veel software gebruiken om tot een VPN-verbinding te komen, daar hoef je niet, eh, niet alle organisaties hebben dat dichtgezet, voor één, of he, wordt dat opengezet voor één specifieke VPN-aanbieder, maar kunnen ook meerdere zijn, zolang je het wachtwoord maar weet. Zolang je de juiste credentials hebt om in te loggen. Eh, ja, ik denk dat dit wel redelijk gecovered is, in ieder geval. Ja, is dit in de richting van wat je, wat je zocht?

X: Ja. Je zegt een endpoint, bijvoorbeeld noemde je een computer en een mobiel. Gebruik jij ook een VPN op jouw computer en jouw mobiel?

Y: Eh, ik gebruik alleen eh, actief VPN op mijn eh, computer. Eh, en ik gebruik, even kijken hoor, geen actieve VPN op mijn eh, mijn mobiel. Dat is afhankelijk van welke service ik gebruik hoor, want als ik de mobiele app gebruik dan doet die dat volgens mij automatisch. Eh, en hetzelfde met alle links die ik aanklik vanuit mijn e-mail, die gaan naar een beveiligde browser, dus er zit een soort van sandboxing in, die volgens mij automatisch leidt naar eh, een VPN-verbinding. Maar mijn computer, ja, dat is afhankelijk ook, he, want je merkt gewoon, er is wel snelheidsverlies. Toen ik inlogde op eh, dit interview, de Big Blue Button, eh, toen zag ik ook dat ik connected was met [the VPN of the professional services firm], ja, die heb ik uitgezet, want je merkt gewoon, ja, daar zit wat vertraging in. En daarbij merk ik dus dat, waarschijnlijk gebruikt [the professional services firm] een volledige VPN en niet een split tunnel.

X: En je noemde eerder over de beveiliging en encryptie, kun je daar meer over vertellen?

Y: Oeh, ja, je gebruikt natuurlijk, eh, ja, dat hangt er een beetje van af wat je, wat je, welk protocol je gebruikt, want er zijn natuurlijk meerdere protocollen, maar eh, volgens mij maken ze gebruik van, volgens mij zijn daar ook weer verschillende stromen in. En als ik het niet fout heb, en pin me daar niet aan vast, gebruiken ze een block cypher, dus AES-265 en daarbinnen een handshake, eh, dus met ook een certificaat. En dat certificaat wordt dan gebruikt om de data te encrypten. Dus je zegt eigenlijk ik ben deze partij, dat is eigenlijk je verificatiestap he, als je inlogt, dan zegt de server, oké, ik geloof dat, want zo ben je geregistreerd, dan kom je terug en volgens mij komt er dan eh, een certificaat op je computer te staan. En met dat certificaat, eh, dat gebruik je dan om stukken van je data, he, dat wordt opgesplitst in pakketjes eh, en die pakketten worden dan versleuteld met dat certificaat en aan de andere kant hebben ze een versie van het certificaat waarmee ze de data kunnen eh, ja, terugdraaien, dus unencrypten, ontsleutelen.

X: Aan de andere kant?

Y: Ja, aan de andere kant. Dat zijn de, zeg maar, ja, je logt natuurlijk in via het internet en dat heeft een plek waar dat aankomt. Dus er is data, eh, die je versleuteld, dat wordt verstuurd naar een server, of dat wordt verstuurd naar een eh, computer aan de andere kant, het netwerk dan noemen we dat. Maar dat komt natuurlijk niet aan op he, dat komt niet direct in het netwerk via eh, een server aan de andere kant, daar zitten stappen tussen. En of dat nou een load balancer is of dat nou een eh, ja, vaak wordt dat via een load balancer gedaan of een firewall of een ja, web application firewall, en die hebben vaak, die hebben vaak een, eh, manier om een certificaat te gebruiken. Die hebben dan het certificaat aan de andere kant om de data te ontsleutelen, zodat die data dan verstuurd kan worden naar de server in kwestie.

X: Oké. En wat is een load balancer?

Y: Een load balancer is eigenlijk een netwerk eh, ja, appliance noemen ze dat, ja, vroeger was het een hardware stuk, maar dat is het tegenwoordig niet meer, ja, eigenlijk ook weer wel, maar goed, daar gaan we maar niet op in. Eh, en die- Tegenwoordig is het veel software gedreven allemaal, he, ook de cloud en zo. Eh, en een load balancer is eigenlijk een stukje eh, netwerkapparatuur waarin data wordt eh, ja, gedistribueerd, dus eigenlijk wordt gekeken van welke servers eh, kan dit verzoek aan. He, er is altijd een verzoek binnen het HTTP protocol, eh, of HTTPS protocol, of any protocol ook, maakt niet uit welk protocol je gebruikt. Eh, en die load balancer, die is eigenlijk om ervoor te zorgen dat de server niet overbelast raken met allerlei request of verzoeken. En die verzoeken worden dus verdeeld over de servers ofwel de apparaten die eh, waar het om gaat. Soms, soms zit er geen load balancer tussen hoor, maar dat is in de nieuwe vorm is dat wel een heel veel gebruikt stukje hardware of software.

X: Als er geen load balancer tussen zit, wat zit er dan tussen?

Y: Wat zei je?

X: Als er geen load balancer tussen zit, wat zit er dan wel tussen?

Y: Ofwel een firewall, ofwel geen firewall. Maar er zit vaak een type bescherming, een beschermingslaag tussen. Dus wat er ook wel eens in zit is dat je eerst een firewall raakt, dan kijkt die mag dit eigenlijk wel, dan gaat die naar een server, en soms zit daar nog een firewall achter, of een stuk bescherming tussen eh, en daarna ga je pas naar de server.

X: En je beschreef het eerder als een tunnel, wat bedoel je met een tunnel?

Y: Een tunnel. Voor mij, kijk, het is meer dat dat beeldspraak is, een tunnel. Je maakt eigenlijk gewoon een verbinding. Eh, en, en dat is, ja, dat wordt een soort van, he, door de ja, mensen die dat proberen te omschrijven, wordt dat als een tunnel weergegeven, wat je legt eigenlijk alsof je een fysieke verbinding neerlegt, eh, naar een, eh, een type netwerk. Dus je graaft eigenlijk een soort van een verbinding onderlangs, dus het is eigenlijk niet een normaal, een normaal type verkeer. Maar het is bedacht zodat je gewoon direct in een beschermd stukje kan komen, dus alsof je een tunnel graaft. Maar is het echt een tunnel? Nee, het is geen tunnel. Het is gewoon een verbinding. Je zegt gewoon, oké, mag A met B praten, ja dat mag onder bepaalde eh, omstandigheden. En die omstandigheden, die eh, die geef je, he, die geef je, die configureer je eigenlijk. Dus is het een tunnel? Nee, het is gewoon een verbinding.

X: En je noemde ook servers in het verhaal. Wat zijn servers?

Y: Servers. Servers zijn, eh, eigenlijk zijn het een soort van computers, zoals jij en ik ook een computer gebruiken, alleen die servers hebben maar een, een select, selecte functionaliteit. Ze doen eigenlijk he, ze zijn niet gemaakt om gebruikers eh, eh, ja, te helpen om hun werk te doen, he, maar het zijn eigenlijk apparaten die iets binnenkrijgen, een verzoek, het verzoek om content te leveren, bijvoorbeeld even een makkelijk voorbeeld is als je een website hebt en die zet je op een server eh, en, en iemand gaat naar een website toe, he, dus www.nu.nl bijvoorbeeld , dan is er bij nu.nl is er een server waar de inhoud van die website op dat moment staat. Eh, en wat die doet is op het moment dat jij nu.nl intypt, dat is eigenlijk een verzoek voor die website, en een server verwerkt dat eigenlijk. He, dat, dat kan door andere verzoeken intern te sturen, maar dat kan ook door gelijk de inhoud terug te sturen. Maar het is- Simpel gezegd is het niet meer dan dat.

X: Oké. En je maakte eerder onderscheidt tussen een intern en extern netwerk. Hoe wordt dat onderscheidt gemaakt?

Y: Eh, er is een eh, conventie, eh, voor IP-adres reeksen. Eh, dus er zijn eigenlijk maar heel- Ja, vroeger toen het IP, het Internet Protocol, bedacht werd, toen dachten ze oké dit aantal zal genoeg zijn. Dus ze hadden een schatting gemaakt van hoeveel IP-adressen er zullen zijn, eh, nou weet ik niet het exacte nummer, volgens mij iets van RFC9812 ofzo, zoiets, denk ik. Nou, eh, hebben ze gezegd we nemen drie, eh, vier octetten, zeg maar. He, dus een IP-adres bestaat uit vier getallen, eh, tussen vier puntjes, of drie puntjes. Dus je begint met een getal punt getal punt getal punt getal punt, dus A B C D noemen ze dat, vier octetten, eh, die geven eigenlijk aan, eh, dat, dat is hun adres eigenlijk, een internetadres van een endpoint, daar hadden we het eerder over. Dus alle endpoints hebben eigenlijk een IP-adres. Dus dat kan zijn, eh, voor ja, jouw, jouw computer heeft een IP-adres, jouw telefoon heeft een IP-adres, een tablet heeft een, en servers hebben ook een IP-adres, net als alle netwerkapparaten hebben ook een IP-adres. Je kunt je voorstellen, zeker met de komst van Internet of Things, dat IP-adressen opraken. Want je hebt maximaal iets van, ja, wat is het, twee, ja, het gaat dus van nul, het zijn dus octetten he, dus nullen tot enen, dus acht keer een binair getal, nul tot een, dus twee tot de macht acht, en dan maal twee tot de maal acht, maal twee tot de maal acht, maal twee tot de maal acht, en volgens mij is dat iets van 6,5 miljoen of zo. Of, eh, aantal IP-adressen, dus dat is natuurlijk nooit eh, genoeg om alle eh, internet apparaten te, te huisvesten. Nou, daar hebben ze iets slims op bedacht. Ze hebben een deel hebben ze gereserveerd voor een eh, publiek domein, he, dat zijn eigenlijk alle IP-adressen die eh, ja aangeroepen kunnen worden vanuit het internet. He, dat zijn bepaalde reeksen, die weet ik niet precies uit mijn hoofd, maar volgens mij iets van 192 reeks, eh, ja, volgens mij 192, want als je zelf volgens mij ook je IP-adres zoekt zit je ook in 192. En dan zijn er een paar anderen, die zijn publiek, dat zijn er best wel veel. En er zijn er een aantal die zijn gereserveerd voor interne, intern gebruik. Dus elk bedrijf kan weer zijn eigen interne gebruiken en die kunnen dus ook overlappen. Dus elk bedrijf kan een tien reeks hebben bijvoorbeeld, een 172 reeks, een 192 reeks, et cetera. Dus, ja, elk bedrijf kan dat weer herhalen. Elk netwerk kan zijn eigen dingetje hebben, zolang endpoints maar niet hetzelfde IP-adres hebben, want ja, dan weet je ook niet meer waar je de data heen moet sturen. Eh, nou zo wordt onderscheidt gemaakt, even helemaal terugkomen naar je vraag, tussen intern en extern netwerk. Eh, dus als jij, bijvoorbeeld binnen [the professional services firm] naar [een interne pagina] gaat, die heeft een intern IP-adres, die heeft een IP-adres die je niet kan bereiken via het internet, dus daar heb je VPN voor nodig om daarop te komen. Maar, [the website of the professional services firm], die heeft een publiek IP-adres, daar kun je vanuit overal komen.

X: Oké. En je noemde ook een hardware en een software token. Hoe past dit in dit verhaal?

Y: Ja. Eh, ja. Je hebt dus binnen, eh, je identity, je hebt een identiteit, en die identiteit, he, het gaat om wie jij bent zeg maar. En als jij praat met een computernetwerk, dan hebben we het over eh, verificatie. Dus jij zegt eigenlijk dat jij Veroniek bent, maar dat computernetwerk dat gaat vragen oké, laat maar zien dat jij Veroniek bent. He, dat kun je op verschillende manieren doen, he, dus eh, je hebt verschillende factoren die je kunt gebruiken. Dus iets, he, dus iets, je kunt dan laten zien iets wat je bent, he, bijvoorbeeld je, je vingerafdruk, je iris, je DNA, of weet ik veel, noem maar op. Iets wat je hebt, he, dus ofwel dat token, eh, of iets dat je weet, dat is het wachtwoord. Als je naar dat token gaat, dus iets wat je hebt, dan gaat het erom dat jij iets hebt dat, he, iets hebt dat niemand anders heeft. Dus iedereen heeft een token, maar die van jou is specifiek voor jou. He, en, eh, wat voor VPN heel veel gebruikt wordt is eh, een token dat om de 60 seconden geeft die een nieuwe, eh, een nieuwe, eh, ja, binnen [the professional services firm] is dat een zes-cijferig getal, dat je kunt toevoegen aan jouw wachtwoord. Die combinatie die wordt, die wordt, die, die, dat is dan zeg maar een sterkere combinatie dan alleen je wachtwoord, he bijvoorbeeld. Nou, je hebt dus daarin verschillende vormen, he, je hebt een, eh, hardware vorm, he, dan heb je echt een dingetje dat om de 60 seconden jou een nieuw getal geeft. Of je hebt een applicatie, he, een stukje software dus op jouw mobiel bijvoorbeeld, die hetzelfde doet, he, in principe niets anders, behalve dat het fysiek, he, dus hardware versus digitaal wat software is.

X: Deze opties zijn allebei beschikbaar binnen [the professional services firm]?

Y: Eh, volgens mij de laatste tijd niet meer. Want, eh, er zijn natuurlijk wat problemen met hardware tokens. Eh, dus vroeger had je wel zo een hardware token en dat hebben ze volgens mij afgelopen jaren eh, ja, eigenlijk gemigeerd naar een software token. Dus ik denk, ja, je kunt natuurlijk je mobiel kwijtraken, he, maar met alle herstel mogelijkheden eh, kun je precies dezelfde software token terugkrijgen. En je mobiel raak je toch iets minder snel kwijt dan zo een klein dingetje. He, je mobiel gebruik je natuurlijk voor veel meer dingen dan alleen je, je verificatie. Terwijl dat hardware tokentje, dat was alleen daarvoor gebruikt. En dat, ja, dat was gewoon een klein ding dat je kwijtraakt. Daarnaast kan de batterij opgaan, hij kan beschadigd raken, hij kan gestolen worden. He, al die dingen, die, ja, dat helpt natuurlijk niet voor de veiligheid. En software klinkt makkelijker, maar er zit wel meer, als je je mobiel goed inricht, zit er wel meer beveiliging op. He, je kunt dus, je moet inloggen op je mobiel eh, om, om bij dat software token te komen. En je hebt ook meer pushberichten, he, die zijn er ook. Dus als je inlogt dat je gewoon een bericht krijgt van he, jij bent, er is iemand die inlogt op jouw identiteit, kun je dat bevestigen, nou, druk je op bevestigen. En dan krijg je als je op ja hebt geklikt, krijg je toegang tot, eh, tot de omgeving waar je recht toe hebt.

X: En je zei eerder ook dat er verschillende aanbieders zijn van VPN, hoe zit dit binnen [the professional services firm]?

Y: Volgens mij heeft [the professional services firm] maar een aanbieder, en dat is, ja, ik weet niet of ik dat mag noemen vanuit veiligheidsperspectief. Eh, maar er is in ieder geval een aanbieder, en daar gebruiken we het stukje software voor. Eh, en, ja, volgens mij wordt alleen verkeer vanuit die servers, vanuit die aanbieder eh, worden toegelaten tot het interne netwerk. Als het goed is, dat is een aanname.

X: En waarom gebruik jij een VPN?

Y: Eh, ik gebruik eigenlijk alleen een VPN als ik, als ik toegang moet hebben tot [the professional services firm] interne dingen.

X: En waar gebruik je VPN?

Y: Eh, waar?

X: Ja.

Y: Ja, kijk, in principe gebruik ik mijn computer nooit op onveilige netwerken, dus dat is niet eens een ding voor mij. Ik gebruik gewoon geen onveilige netwerken, punt zeg maar. Dus als ik ergens ben, bijvoorbeeld een vliegveld of een eh, nou, noem maar op, [example of restaurant], dan gebruik ik gewoon mijn telefoon, dat is een 4G netwerk, he, dat is mijn eigen netwerk, dus niemand kan daar, in ieder geval, niemand kan daarop insnoepen, meeluisteren. Eh, dus ik gebruik eigenlijk alleen mijn VPN als ik eh, diensten wil gebruiken van [the professional services firm]. He, ik weet dat zeg maar, op het moment dat je het onveilige netwerk gebruikt, je een VPN moet gebruiken, eh, en dat doe ik dan ook op het moment dat het echt moet. Er zijn natuurlijk situaties waar het echt moet. Dus ik kijk, eh, ik zal nooit inloggen of gebruik maken van een netwerk waar je geen wachtwoord in moet voeren. Dat je in ieder geval weet dat er in ieder geval beveiliging is en dan gebruik je nog VPN daar bovenop.

X: Waarom gebruik je VPN als je gebruik maakt van een onveilig netwerk?

Y: Omdat, ja, dan komt het beveiligingsstukje om de hoek. Want in principe is het heel onveilig om, eh, ja, onbeveiligde netwerken te gebruiken. Dat klinkt, ja, op zich klinkt dat heel logisch allemaal, maar hoe het werkt is natuurlijk dat verkeer wordt versleuteld. Eh, ja, in ieder geval je gaat ervan uit dan verkeer wordt versleuteld. Maar in principe kun je, als je controle hebt over een stukje netwerk. Dus stel ik ben bij de [example of restaurant], dat is het al bekende voorbeeld, daar zit geen netwerk op, dus je kunt gewoon in zeg maar. Op het moment dat iemand, eh, één controle heeft over het netwerk, dan kan die ook inlezen op jouw verkeer, dat is één. Eh, en ten tweede op het moment dat iemand zich voordoet als hetzelfde netwerk, eh, en controle heeft over dat netwerk, wat logisch is, eh, dan kan iemand jouw verkeer inlezen. En dat, dat kan gevolgen hebben voor, ja, je wilt natuurlijk dat data niet op straat komt te liggen. En je beschermt natuurlijk de, de, de, zowel de, he, dat zijn de drie, de triad van informatiebeveiliging, dat zijn ook de drie doelen, he, confidentiality, integrity en availability. En vooral confidentiality en vertrouwelijkheid, he, dus mag alleen iemand inzien die, he, de data inzien die de data in mag zien. Dat is een principe en de tweede is integriteit, is de data nog steeds de data, die, he, is het juist, is het goed, is het volledig, et cetera, je wilt weten dat niemand aan die data heeft gezeten. En een VPN, maar ook eigenlijk alle beveiliging die überhaupt is, even losstaand van een VPN. Encryptie in het algemeen, die zorgt er gewoon voor, eh, dat, eh, dat, dat die data of die vertrouwelijkheid en integriteit wordt bewaakt.

X: En je zei dat jij dan in publieke ruimtes gebruik maakt van 4G, wat is dan het verschil tussen een onveilig netwerk en 4G?

Y: 4G is een, eh, een op zichzelf al beveiligd, eh, ja, vooral als die je eigen is, he, want dat is gewoon verbonden aan jouw, eh, telefonie, eh, abonnement. En je mobiel zorgt ervoor dat, dat die data, ja, beveiligd is. En dan wordt het naar een satelliet gestuurd of een zendmast of whatever. Eh, en dan weer doorgezet naar het internet. He, dus er zijn, voor mij is dat, heeft, je kunt niet zeggen dat het volledig veilig is, dat weet je nooit. Alleen de drempel van veiligheid is een stuk hoger. En dus de controle over dat netwerk wordt beter bewaakt dan, eh, die bij de [example of restaurant], bij wijze van spreken. Daar zit ofwel een telecomprovider, ofwel een netwerkprovider, ofwel zelfs een overheid. En dan is ook maar de vraag, oké, waarvoor, he, waarvoor ben je bang. Eh, maar in ieder geval, dat 4G netwerk, die levert in ieder geval een zekere mate van eh, vertrouwen voor mij in ieder geval. Eh, dat ik weet dat, dat, eh, dat daar niet gekke dingen mee gebeuren, eh, op het allerlaagste niveau. Klinkt een beetje paranoid, maar goed.

X: Ja, maar, op wat voor manier is dat dan veiliger?

Y: Oeh. Voor, ja, vanuit perspectief is die vraag?

X: Nou, je zegt, je noemde eerder allemaal beveiliging die er wel is als je gebruik maakt van een VPN en waarom je dan een VPN gebruikt op een onveilig netwerk. Maar, dan zeg je ook als je wel in een publieke ruimte bent, dat je gebruik maakt van 4G.

Y: Ja.

X: Is er dan nog een verschil in het beveiligingsniveau van 4G en VPN?

Y: Ja. Kijk, het ding is dat, hoe je het moet voorstellen is dat het bedrijf heeft natuurlijk gewoon een internetverbinding. He, dus bijvoorbeeld een, een [example of restaurant], eh, die heeft dan routers of die gebruikt, he, die gebruikt acces points noemen we dat dan, noemen we de routers. Of in ieder geval die gebruikt apparaten, modems, om een connectie te leggen met het internet. Daar zitten dus tussen jouw, bij wijze van spreken computer als je die gebruikt bij de [example of restaurant], tot aan die modem, nou daar heb je al een stukje, eh, ja, stukje dataverkeer. En dan dat apparaat naar het internet toe. Nou, moet je voorstellen dat, op het moment dat iemand, eh, dus, he, dat kun je ook zelf zijn, dat kan ik ook zelf zijn. Maar als iemand dus die data, of die apparaten manipuleert die tussen dat dataverkeer inzitten, eh, dan, ja, is dat, ja, dan is dat natuurlijk onveilig. En de vraag is natuurlijk oké, wat maakt het dan minder veilig? Ik denk gewoon dat de drempel, eh, lager is. Dus, ja, je hebt gelijk, we kunnen niet uitgaan, we kunnen niet 100% zeker zijn dat 4G netwerken veilig zijn, daar zitten ook kwetsbaarheden in. Eh, he, dus dat heb je ook altijd. He, je hebt ook, eh, partijen die malafide kunnen zijn of kwade bedoelingen hebben, maar ik vind de drempel, is een stuk, stuk, stukken lager. Dus ik weet in ieder geval dat als ik mijn eigen mobiel gebruik, dan ben ik eigenlijk de persoon tussen de computer en het internet. In plaats van dat iemand anders dat is. En ik heb controle over in ieder geval het stukje tussen mijn laptop, mijn mobiel en daarna, eh, het internet. En daar kan iemand tussen zitten, dat klopt.

X: Heb je nog het whiteboard voor je?

Y: Eh, ik heb het whiteboard voor mij, als het goed is. Ja.

X: Zou je dan voor mij kunnen tekenen hoe deze situatie eruitziet als je een VPN-verbinding maakt?

Y: Met. Dus als ik, als ik bijvoorbeeld, eh, VPN, eh, op VPN inlog?

X: Ja.

Y: [start drawing 1\_1].Oké. Even kijken. Ik heb alleen een pen, he. O, nee, ik heb meer. Eh, ja, dat kan ik. Dus als ik bijvoorbeeld. O, doet die iets. Wat ik doe, o, dit is wel heel dik. Laten we zeggen, dit is, eh, dit is het netwerk. Kan ik dit verplaatsen of niet. Dit is het interne netwerk. [start drawing 1\_2]. Dan is er ook nog een, he, wat ik noem, externe netwerk, he, dat hoort nog steeds bij dat bedrijf, he, noem het een DMZ, dat is een heel vaak gebruikte, ja, term voor het publieke, het publieke deel van je netwerk, demilitatrized zone. Nou, in principe betekent dat gewoon, nou, het heeft een lagere mate van vertrouwen. [start drawing 1\_3]. Als jij als endpoint, jij bent, eh, het poppetje. Dat is je endpoint. Eh, even kijken, een poppetje. Nou, dat poppetje, dat wil eigenlijk naar een van de resources die hierin zit. [start drawing 1\_4]. Dus een server die, ik teken nog een netwerk erbij, want je hebt natuurlijk meerdere segmenten. Je hebt A, B, C, D, als een bedrijf dat goed doet, heb je gewoon meerdere segmenten. En dat, dat zorgt voor extra beveiliging. [start drawing 1\_5]. Nou, als jij verbinding wil maken, dan zeg je eigenlijk oké, ik wil verbinding maken met een server die hier staat bijvoorbeeld, dus een ander endpoint. Jammer dat ik geen tekst kan toevoegen, maar dat maakt op zich niet uit.

X: Je kunt tekst toevoegen.

Y: Ja, hier.

X: Als je-

Y: O, dat kan wel, oké, nou. Hoe doe ik dat.

X: Op de pen klikken, en dan staat er een T.

Y: [start drawing 1\_6]. He, dus dit is DMZ bijvoorbeeld, external. Ik weet niet hoe lang ik hier over mag doen.

X: Zo lang als je wilt.

Y: Oké. Kan ik dit, kan ik dit klikken? Hier eigenlijk, eh. Dus dit is de DMZ, external facing network. Heb je hier nog internal facing network. [start drawing 1\_7]. Wat ik ga toevoegen is bijvoorbeeld, dit zijn allemaal servers die in de- Laten we zeggen dat dit allemaal endpoints zijn. Hier zitten allemaal endpoints, is allemaal leuk en aardig, maar hier wil je heen. [start drawing 1\_8]. Dit is je laten we zeggen, je, je target. En wat je doet op het moment dat je VPN aanzet, dit is eigenlijk de, de situatie op het moment dat je, dat je VPN eh, hebt eigenlijk, daar komt het op neer. Dus op het moment dat je het wilt vastleggen, he, dan stuur je eigenlijk een- Dan zorg je voor een, ja, hoe noem je dat, dan stuur je eigenlijk een verzoek. Dus je begint eigenlijk door het eerst te, vast te stellen zeg maar- [start drawing 1\_9]. En vaak is er wel nog een derde partij, dat is afhankelijk, heel afhankelijk van hoe je het ziet. Dus de inrichting is wel belangrijk, dus ik ga even van een situatie uit. Dus je hebt extern, intern, de VPN-aanbieder heeft dan ook een server waar die mee praat. Wat er zou kunnen gebeuren, dus dat is even hypothetisch he, want het zou ook hier kunnen gebeuren, maar wat ik, even voor het gemak, en ik denk een beetje in [the professional services firm] terms zeg maar. [start drawing 1\_10]. Wat die doet, op het moment dat jij VPN aan, start zeg maar, dan zeg je hé, doe mij een VPN-verbinding. Dat is eigenlijk een eerste verzoek. Nou, dan komt er een respons, zal ik even in rood doen. [start drawing 1\_11]. He, en als dat allemaal heen en weer goed is, want eigenlijk zeg je gewoon al bij zo een VPN, want die heb je al op je computer staan, die, dan stuur je al je credentials mee met het verzoek, he, dus dat doe je al meteen, nou dan komt er een connectie hier terug van ja, dat mag. [start drawing 1\_12]. En vaak gaat dat ook via, zou het zo kunnen, he, dus dat je zegt er is een respons naar een server in de DMZ die weet wie jij bent. [start drawing 1\_13]. He, en dat dit ding dan weer terugpraat, eh, van hé, het is goed. Of het gaat direct zo, boem, hiernaartoe. [start drawing 1\_14]. Er is nu ergens een server die dus met jou zeg maar zo een verbinding maakt. Dus dit is dan, een soort van, ja, afhankelijk van, dus je begint in ieder geval deze connectie ofwel deze connectie voor [the professional services firm] bijvoorbeeld het netwerk die, eh, ja, DMZ is. Dus dit kan allebei zijn, dat is even afhankelijk van de situatie. Dan heb je een verbinding met de, dat is zeg maar deze rode lijn. En die rode lijn zorgt er eigenlijk voor dat je dit stuk, kan, eh, overslaan, nou, doet die natuurlijk niet. Maar wat die dan wel doet, en dan gebruik ik hem even in groen bij wijze van spreken, dus de connectie is gelegd. [start drawing 1\_15]. En dan kun je hier doorheen, he, dan word je toegelaten. En je hebt een IP-adres, dat dit IP-adres is zeg maar, dus hier wil je heen. [start drawing 1\_16]. En deze zorgt er dan voor dat je deze verbinding kunt maken, he. [start drawing 1\_17]. En die verbinding zorgt er ook voor, he, dus met alle informatie van dien die je daarbinnen hebt, laten we paars gebruiken, die stuurt het allemaal terug naar hetzelfde punt en die stuurt dat dan weer terug naar jou. En zo heb je eigenlijk verkeer. Dus die groen, groen-paarse, is op het moment dat je een VPN hebt. En zwart-rood is eigenlijk om, om te valideren wie jij bent. En als je een split tunnel gebruikt, eh, dat ook zou kunnen gebeuren, he. Is dat stukje software, dat is afhankelijk van wat het doet, he, want daar hebben we het niet eens over gehad. [start drawing 1\_18]. Dat stukje, er kan ook een stuk software tussen zitten, dat is dan op je endpoint, die zorgt dat jij gewoon naar een endpoint gaat die helemaal niet in de buurt is van dat netwerk. [start drawing 1\_19]. Dus dat, dat als jij een split tunnel gebruikt kan dat stukje netwerk eigenlijk gewoon zeggen van nee we gaan niet via [the professional services firm], nee we gaan gewoon naar een publiek stukje netwerk, en dan is het verkeer ook gewoon tussen die twee dingen in. He, dus deze lijnen, die gaan allemaal via dat stukje software. [start drawing 1\_20]. En ook, kijk naar, ik denk dat ik nu te veel uitleg, maar hier heb je natuurlijk ook weer verbindingen tussen elkaar, dus die kan weer dit netwerk, zo lang deze grenzen dat toelaten. Dus zo zie ik VPN een beetje.

X: Oké. En je maakt dus verbinding via die demilitarized zone met de internal facing network?

Y: Ja, dat is eigenlijk het stukje, ja, je kan, je kan niet direct naar het stukje netwerk. Dat bestaat gewoon niet. Er zit iets tussen, he, er moet gewoon iets zijn wat, eh, wat, eh, wat, ja, eh, de logica heeft zeg maar, de beslissing kan maken of dit goed is of niet zeg maar, of het mag of niet. Dat doet een firewall ook, het zijn eigenlijk een beetje domme apparaten, want ze zeggen van mag dit, ja of nee. Onder welke voorwaarden.

X: Wat zijn dan die segmenten?

Y: Welke segmenten? Deze? Bij internal facing? Wat, eh, wat bedoel je?

X: Wat zijn de functie van die segmenten?

Y: Die segmenten. Ja, dus dat is eigenlijk een extra stukje beveiliging. He, want in principe kun je- Een netwerk kan plat zijn, noemen we dat. Dan kan alles met elkaar praten. [start drawing 1\_21]. Dus wat je vaak ziet, gaan we even naar zwart toe, is dat er gewoon meerdere endpoints in een segment zitten. Wat vaak ingeregeld is, dus het is ook afhankelijk van hoe je het inregelt he, het is allemaal afhankelijk van, van, van de architectuur, eh, is dat deze direct met elkaar kunnen praten. Dus, dat er altijd verbinding gemaakt kan worden tussen al deze endpoints binnen het segment. [start drawing 1\_22]. Maar he, dat, eh, even kijken, dat bijvoorbeeld dit is niet, niet bij voorbaat mogelijk. He, dat is alleen mogelijk als zeg maar, een firewall dit toelaat. Dus stel een endpoint zegt ik wil praten met dit apparaat en er staat nergens- En je hebt besloten om segmenten te nemen, eh, en er wordt niet specifiek gezegd dat punt A met punt B mag praten, dan komt dat ook niet tot stand. En zo voeg je eigenlijk een beetje extra lagen van beveiliging toe. Dus wat ik hier teken is eigenlijk een soort van eh, multi-tier architecture. Is wat, eh, eerst bijvoorbeeld een client, internet facing stuk hebt, dan heb je een webserver bijvoorbeeld, he, dus de meeste website zijn zo ingericht. Dan heb je een, eh, website en die website heeft weer een database erachter. Alleen wat je niet wilt is dat eh, een endpoint direct praat met een database, want dan heb je echt, dan heb je, ja, het heet niet voor niets informatiebeveiliging. Nou waar staat informatie, die staat natuurlijk in databases. Eh, en als je direct toegang kan hebben tot de database kan je aardig wat schade aandoen. He, dus je wilt zo veel mogelijk stukken beveiliging inrichten voordat je bij die databases aankomt. He, en wat ook vaak gebeurt is dat iemand binnen het gebruikersnetwerk direct wel, he, wel direct toegang heeft tot die database, maar iemand vanuit een, een external facing netwerk dat niet kan. He, dat is heel afhankelijk van hoe dat is ingericht. Dus daar zijn- Deze grenzen worden allemaal bepaald door middel van regels of, eh, door middel van, eh, van, ja, omgevingsfactoren. Dus [example of softwareprovider] is daar heel erg mee bezig, is dat eh, he, zero trust noemen ze dat. Dus als ik het zo teken, dan is er wel een mate van vertrouwen. Als je eenmaal hier bent, dan mag je hiernaartoe, dat is een mate van vertrouwen. He, je voegt dan minder vertrouwen toe op het moment dat je meerdere segmenten toevoegt. En je hebt al helemaal geen vertrouwen op het moment dat jij een medewerker bent die in het interne netwerk zit. Dus bijvoorbeeld, [0:47:51 till 0:48:18 has been omitted] en je hebt zero trust, he, het model zero trust, dan, eh, kijken ze eerst naar oké, wie ben jij, ben jij ingelogd, heb jij de juiste, eh, permissies, bla bla bla. Je kunt nog verder gaan door te zeggen ja, log jij normaal gesproken op dit tijdstip met dit apparaat in, he, dat zijn die omgevingsfactoren die je kan inbouwen, en dat is iets waar [example of softwareprovider] heel erg sterk mee bezig is, omdat zij natuurlijk, ja, de grootste aanbieder zijn van, van, eh, ja, hoe heet dat, werkstations. [0:48:53 till 0:48:55 has been omitted], he, dus zij kunnen ook via software kunnen ze dingen toevoegen waardoor ja, per netwerksegment, per vierkantje hier kan worden bepaald, oké, op basis van welke van deze factoren mag iemand worden toegelaten. En dat zie je dus ook steeds meer met dat single sign-on verhaal, he, VPN speelt een heel grote rol in single sign-on, en eh, dat het lijkt alsof je alles mag, maar daar zit heel veel complexiteit achter en heel veel, ja, management achter. En dat zijn eigenlijk die stukken, he, dus stel dit is [een interne pagina], die mag je alleen onder bepaalde voorwaarden inzien.

X: Oké. En hoe wordt bepaald wat je in mag zien?

Y: Dat is allemaal configuratie. He, dus iemand met de rol, ja, noem het manager, noem het eh, supervisor, noem het lead, die heeft de verantwoordelijkheid gekregen om het netwerk in te richten. He, dat is vaak een, eh, nou ja, dat is vaak geen architect. Een architect bepaald eigenlijk meer, he, wat de toekomstplannen zijn. En op welke principes de plannen zijn gebaseerd, eh, en eh, eh, hoe alles verbonden moet worden. Maar uiteindelijk is er ook een soort van lopend proces, he, dus iemand heeft management, eh, ja, power zeg maar om te bepalen op basis van welke, eh, voorwaarden dat wordt, eh, toegang wordt gegeven. Dus iemand is wel in de lead, er zal ook een security, eh, of een chief information security officer zijn binnen [the professional services firm], die dus bepaalt hoe, eh, hoe dat, eh, hoe dat moet verlopen. He, dat is echt een mensenstukje. Dus je kunt niet alles met techniek afdekken. Je kunt veel met techniek afdekken, zeker tegenwoordig. En zeker nu de grenzen van he, diensten, eh, met de cloud weet je wel, dat die overal staan, overal en nergens weer in Nederland staan. He, dus hoe krijg je meer controle over, he, dus niet alleen dit stukje aan de rechterkant, maar ook dat paarse bolletje, dat is niet een ding, dat zijn meerdere dingen. Dus, eh, makkelijke voorbeelden zijn natuurlijk [social media platform], ja, andere social media, maar wat als je [example of external software] gebruikt, wat als je een bestaande oplossing gebruikt, [example of external software] gebruikt, ja, dat staat niet altijd in het interne netwerk van [the professional services firm]. Dus het is vaak goedkoper, en eh, ja, je kunt gewoon van schaalvoordelen genieten op het moment dat jij een Software as a Service gebruikt, he. Met, eh, de, de, het inleveren van beveiliging die daarbij komt kijken.

X: En wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Sorry, kun je de vraag herhalen?

X: Ja. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Wat is de invloed ervan? Hm. Ik weet niet of ik, of ik, of ik die vraag kan beantwoorden, he, wat is de invloed van- Kan je die anders stellen?

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

Y: Ja, dat heeft zeker invloed op mijn computerbeveiliging. Dus eigenlijk alles wat ik nu genoemd heb, vooral vanuit vertrouwelijkheid en integriteit weet ik dat, eh, dat, eh, in ieder geval, ik heb het niet vastgesteld, maar dat is ook nog belangrijk. Eh, het bedrijf heeft gekozen voor deze oplossing, eh, en het bedrijf heeft ook vertrouwelijkheid en integriteit hoog in het vaandel. Eh, dus ik denk, denk dat dat zeer belangrijk is om te gebruiken, maar niet voor alles. He, dus ik zie het niet als de oplossing voor alle computerbeveiliging, er is zo veel meer in computerbeveiliging. He, malware kan ook via een VPN verlopen, maar, eh, ook heel veel impact hebben op jouw computerbeveiliging. He, het is dus een van de tools [0:53:25 till 0:53:30 has been omitted] voor informatiebeveiliging.

X: En met wat voor een digitale dreiging heb jij op een normale dag te maken?

Y: Persoonlijk bedoel je?

X: Ja.

Y: Ik vind dreiging wel echt een heel groot woord. Eh, bij dreiging denk ik gelijk aan [0:53:51 till 0:53:54 has been omitted]. Eh, ja, wat ik zie langskomen is bijvoorbeeld spam, met, eh, ja, advertenties erin of weet ik veel wat erin. Of links die leiden tot eh, malafide websites. Ja, phishing is natuurlijk echt een ding. Eh, ik denk dat dat vanuit een persoonlijk perspectief, of bedoel je vanuit een klant perspectief? Wat ik eh, ik zie-

X: Ja, of vanuit [the professional services firm] perspectief?

Y: Ja, kijk, ik kan alleen maar gissen, wat daadwerkelijke dreigingen zijn, worden niet door mij gemeten, die worden niet door mij ingezien. Ik krijg ook geen bericht van oké, jij bent slachtoffer geweest van. He, dus heel veel wordt natuurlijk al uitgefilterd door email systemen of door eh, ja andere dingen van [the professional services firm]. [The professional services firm] heeft natuurlijk heel veel software die ons helpen, om, om veiliger te zijn. Dus, ja, ik kan eigenlijk geen goed beeld geven van de dreigingen die ik op dagelijkse basis zie. Behalve dan dat ik kan raden wat het is. He, als je, als je zelf een server hebt, eh, en die zet je op het internet en die zet je op je external facing netwerk, ja, geheid dat jij constant rare verzoeken krijgt. He, dus daar wordt wel constant scanning op gedaan, op het moment dat jij publiek beschikbaar bent op het internet. He, want dat is natuurlijk geen ingang voor eh, aanvallers om op het netwerk te komen. Daar zie je het wel heel duidelijk. Als je het eenmaal open zet voor het internet, wat er allemaal voor gespuis langskomt om te kijken hoe het allemaal zit.

X: En verandert de soort dreiging dan door een VPN-verbinding?

Y: Ik denk niet dat de soort dreiging verandert, maar dat je de maatregelen in ieder geval neemt om de dreiging af te dekken. Dus je hebt onveilig, he, verkeer over het internet heen. Ja dat, daar geef je iets meer zekerheid over. He, dat jij kan internetbankieren bijvoorbeeld is toch, ja, fijn als je een VPN-verbinding gebruikt, maar dat hoeft niet. Kijk, als ik [the professional services firm] gebruik voor internet bankieren, eh, ja, dat doe ik dus niet. Maar dan weet ik ook dat de data gaat gewoon via [the professional services firm] resources, nou dat wil ik ook niet. He, dus er zit ook een stukje zelfbescherming in. He, maar, eh, kijk op persoonlijke basis gebruik ik geen VPN voor internetbankieren. Ik vertrouw wel op HTTPS protocollen, he, TLS, om een beveiligde verbinding te maken met mijn bank. Daar gebruik ik geen VPN voor.

X: Dit ging dan over digitale dreiging. Maar heb jij ook nog te maken met een sociale dreiging?

Y: Sociale dreiging, wat bedoel je met sociale dreiging?

X: Eigenlijk alles wat niet digitaal is.

Y: Eh. Wat is niet digitaal tegenwoordig.

X: Eerder bijvoorbeeld had je het over internet bankieren en dergelijke. Dus dat is dan allemaal duidelijk digitaal, maar zit hier ook nog een sociaal aspect aan?

Y: Eh, ja, ik kan die twee dingen bijna niet los van elkaar zien tegenwoordig. He, dus, kijk, als je het hebt over bijvoorbeeld advertenties ontvangen, of als je het hebt over de overheid kan eh, inzien op wat jij doet, of wat dan ook, ja, die impact is er zeker. Als je daar om drukt maakt, dan moet je andere maatregelen nemen.

X: Heeft een VPN-verbinding hier invloed op?

Y: Eh, nee. Helemaal niet. Ik heb juist het idee dat ik ook een beetje gevaar loop als ik een VPN-verbinding gebruik. He, want ja, je dekt misschien wat verkeer af. Het gaat nog steeds via je VPN-verbinding, he, daar moet je maar vertrouwen in hebben, dat is een. Eh, het tweede is, ja, als een overheid op, he, dat is, wat mij betreft is dat het allerhoogste niveau van, eh, van persoonlijke dreiging, eh, zijn overheden. Nou, ik vertrouw de overheid op zich wel, maar ik weet ook wel waartoe ze in staat zijn. En daar gaat een VPN niet bij helpen. He, als zij willen dat jouw VPN-verbinder of aanbieder toegang geeft tot data, dan vraag ik mij af of zij hun poot stijf houden. Ik geloof dat eigenlijk niet eens.

X: Biedt een VPN dan in enige vorm wel bescherming? Want je zegt als ze data vrijgeven, wat bedoel je daarmee?

Y: Nou ja, kijk, een VPN-verbinding heeft, he, zo lang zij hun werk doen, zo lang zij doen wat zij beloven, dan ben je veilig. Voor in ieder geval je netwerk, eh, je verkeer. Dus hetgeen wat jij verstuurt tussen A en B en weer terugkrijgt van punt B naar A. Eh, ja dus dat is de bescherming die ze bieden. Eh, maar, zoals alles, nou alles, veel in beveiliging is het toch heel erg afhankelijk van, eh, het vertrouwen dat je hebt met de aanbieder. Dus als de aanbieder, kijk, als jij een gratis VPN gaat gebruiken, nou dan, dan doe je dat waarschijnlijk niet omdat je echt iets beschermt wilt hebben. Dan doe je dat waarschijnlijk om binnen [company] Amerikaanse series te kunnen kijken of eh, een ander land. He, dat is de kracht van VPN natuurlijk ook. Je maakt verbinding met eh, een ander netwerk of een ander apparaat in een andere regio, he, zodat je kunt doen alsof je in Amerika zit. He, dus als je zegt ik ben privacy aware en ik wil eh, eh, he, ik wil via andere punten connecten, zodat ze in ieder geval een, of twee, of drie stapjes meer moeten nemen zodat ze bij mij komen, eh, dat kan. Maar dan zou ik eerder een ander mechanisme gebruiken.

X: Op wat voor manier draagt een VPN bij aan privacy?

Y: Nou het draagt zeker bij aan privacy tot op zekere hoogte. He, dus het zorgt er in ieder geval voor dat als jij bijvoorbeeld eh, veel eh, wil inloggen, eh, in ieder geval gewoon browsed of internet gebruikt, weet ik veel wat, en eh, dan, dan kunnen ze niet direct zien wie jij was. Dus zij zien dan niet een IP-adres, dat, dat kan op een server namelijk, dat wordt gewoon allemaal gelogd. He, dat wordt gewoon, ja, keihard wordt daar gewoon opgeschreven wie toegang probeert te krijgen op jouw eh, resources. He, als je technisch aangelegd bent, kun je de logs inzien en dan kun je zien dat jij of ik dat gedaan heeft. Niet op persoonlijke basis, maar wel jouw computer. Dus in ieder geval kun je heel erg pinpointen. Kijk als jij in een huishouden zit met, eh, vier personen en je weet het IP-adres, ja, dan kun je dus met redelijke mate van zekerheid vaststellen wie het is. Tot op vier personen. Je kunt natuurlijk gasten hebben, familieleden, wat dan ook, maar daar gaat het niet om. En, eh, een VPN kan daar hulp bij bieden om, om, om in ieder geval te doen alsof je vanuit een ander punt komt. He, want zij zien natuurlijk het laatste punt dat probeert, geprobeerd heeft te connecten. En natuurlijk gaat dat ook altijd- Kijk, hoe het technisch werkt, je hebt natuurlijk hops he, dus tussen jou en mij zitten denk ik minstens vier hops. Dus ik, eh, ga naar mijn, eh, een kastje hier en het kastje hier gaat naar het internet, en dat internet dat wordt een beetje gescrambled, of er komen meerdere dingen bij elkaar en dat komt weer bij jouw internetprovider terecht en dat komt weer bij jouw modem terecht. Dus uiteindelijk zitten er best wel wat hopjes tussen. En wat jij dan, stel je zou onze verbinding inzien, dan zie je een paar laatste, he, dat laatste stapje zie je. Maar wat je ook zelf kan doen is ping trace. He, dat is gewoon dat jij als pakketje volgt. Dus dan zie je precies welke hops ertussen zitten, met uitzondering van een paar private die ertussen zitten. Dan zie je dus ook bijvoorbeeld, ja, dat je zes stappen hebt genomen voordat je bij eh, je eindpunt eh, komt. Het is niet allemaal- Ik zeg maar- Ik simplificeer heel veel dingen hoor, er zit toch best wel wat complexiteit tussen. Dus, ja, eh, helpt het echt met privacy, ligt eraan hoe veel vraagtekens je hebt. Als je veel vraagtekens hebt, dan is het vaak nee. In de vorm van hoeveel kritische vragen stel je voordat jij tevreden bent met je privacy. Als jij een vraag hebt, dan ja. Als jij vijftien vragen hebt, dan is het hoogstwaarschijnlijk dat die niet gaat bieden wat jij wilt.

X: En je zegt het laatste punt die ziet dat dan, wat ziet die?

Y: Sorry, kun je dat herhalen?

X: Ja. Je zei dat je springt naar allemaal hops, en het laatste punt ziet dan alleen het laatste, of alleen het een na laatste punt. Wat ziet dat laatste punt?

Y: Wat dat laatste punt is?

X: Nee, zeg maar, jou naar mij, dan gaat het via allemaal punten-

Y: Ja.

X: En met een VPN-verbinding zie je alleen het laatste punt, zei je.

Y: Nee, nee, dan verander je het laatste punt natuurlijk. He, dan in je log-

X: En wat verander je dan?

Y: Ja, bijvoorbeeld je locatie, of je server, of wat, eh, je verandert niets aan de feitelijkheid, alleen eh, waarom het ook zo traag is, is dat er hops tussen zitten. He, er zitten dus dingen, als we weer teruggaan naar de tekening bijvoorbeeld, dan eh, is er hoogstwaarschijnlijk deze externe aanbieder of wat dan ook, dan, he, is dan een stap tussen, he, tussen jou, het moet eerst naar het internet komen, dus jouw modem, het internet, dan naar de externe VPN-aanbieder, die heeft waarschijnlijk ook allemaal servers, he, en die zorgt ervoor dat je weer naar DMZ gaat, en alles gaat weer terug, he. Dus alles stapjes worden teruggenomen, omdat elk pakketje wordt eigenlijk uitgepakt, he, dus eh, hm, het internetprotocol is opgebouwd uit meerdere lagen zeg maar, segmenten, zeven volgens mij in totaal. Nou, elk stukje zorgt eh, die verpakt, eh, dat vorige stukje en voegt een stukje, eh, toe. Dus wat er gebeurt is dat steeds meer data wordt toegevoegd aan een pakketje. En dat pakketje wordt, eh, bij het doorsturen wordt die dus weer ja, krijgt het weer een afzender en een, eh, target. Target blijft redelijk hetzelfde, omdat je altijd weet waar je uiteindelijk naar toe wilt. Er zit er eentje tussen, maar de, maar als die uitpakt dan ziet die, oké, hij kwam van dit punt, dus daar moet die ook weer naar toe. He, en zo onthoud je de hele tijd, eh, he, dus er hoeven geen actieve verbindingen te blijven bestaan om die connectie te laten, eh, leven zeg maar. Dus die data zit eigenlijk in het pakketje. Dus doordat de data in het pakketje zit, weet hetgeen wat het ontvangt of verwerkt of wat dan ook, waar die weer naar toe moet ofwel naar teruggestuurd moet worden.

X: En we hadden het eerder dan over digitale en sociale dreigingen en je noemde het al kort even, maar wie of wat is de aanvaller die achter een eventuele dreiging zit?

Y: Hm, wat is zijn motief bedoel je? Ik hoorde niet helemaal het laatste stukje.

X: Wie of wat is de aanvaller die achter een dreiging zit?

Y: Ja, dat is heel afhankelijk van eh, waar je bent in de wereld. Ik denk overal eigenlijk wel, maar eh, ja, je hebt gewoon verschillende vormen van, van, ja, actoren zogezegd, en, eh, die kunnen heel erg verschillen. Het kan je buurman zijn, maar het kan ook een, een kwaadwillend bedrijf zijn. Of het kan ook een bedrijf zijn die geld wil verdienen over jouw rug heen, denk aan [social media platform] bijvoorbeeld. Eh, maar het kan ook een lokale of eh, een wat grotere overheid zijn. Eh, of een criminele bende. Dus dat zijn echt verschillende vormen die, die dreiging kunnen geven.

X: Verandert de soort aanvaller ook door gebruik te maken van een VPN-verbinding?

Y: Hm, nou de soort verandert niet, maar ik denk dat eh, eh, dat het niveau, he, de kennis en kunde van de aanvaller, moet hoger zijn. En dat, dat geldt denk ik voor alles binnen informatiebeveiliging, alle maatregelen die je treft, verhogen de drempel voor een aanvaller om het effectief uit te voeren. He, en hoe moeilijker je het maakt, hoe meer middelen je nodig hebt, hoe meer tijd je nodig hebt en de kunde die je nodig hebt om een aanval uit te voeren.

X: Kan je daar een voorbeeld van geven?

Y: Eh, nou ja, je, stel je zou dus, en ik ga weer terug naar het [example of restaurant] voorbeeld, voor het gemak, omdat ook VPN als onderwerp hebben, eh, stel je zou geen VPN gebruiken en je maakt gewoon direct gebruik van het netwerk van [example of restaurant] dat onbeveiligd is, ja, dan is het voor iedereen mogelijk om jouw data in te zien. Dat kan ik, ik loop nu naar de [example of restaurant] ik kan dat. En ik kan jou dat uitleggen in een uur en dan kun je dat. Niet dat ik jou wil aansporen, dat zeg ik niet. Eh, maar het is redelijk makkelijk. Gebruik je VPN, he, dan heb je die dreiging, dan heb je die actoren al uit het veld. Nou, heb je echt goede mensen die snappen hoe het internet werkt, ja, dan wordt het al, dan is je bescherming toch wel iets minder. He, en stel je zou vanuit je thuisnetwerk gebruik maken van [the VPN of the professional services firm] om je diensten, eh, ja, om het internet te gebruiken. Ja, dan heb je toch wel echt meer, meer kennis en kunde nodig, kijk en misschien wel meer macht. He, dus wat heb je dan nodig? Misschien een kwetsbaarheid in de VPN-oplossing, of, of toegang bij de VPN-aanbieder, of weet ik veel wat. Ja, daar heb je echt wel wat macht voor nodig. En dat zijn wat mij betreft vaak de, de nationale overheden die dat eh, die dat gewoon kunnen. Zij kunnen ons nu ook afluisteren denk ik. Eh, ja, dat denk ik qua mogelijkheid is dat zekerheid. Of ze dat doen, dat is weer een andere vraag.

X: En wat zou de motivatie van een aanvaller kunnen zijn?

Y: Hm. Ja, dat, ik denk dat dat verschillend is. Als jij- Je hebt natuurlijk persoonlijk motief, he, dus dat jij, ja, stel je bent een publiek figuur en iemand wilt jou eh, iets aandoen. Of je hoeft niet eens- Iemand wilt jou gewoon iets aandoen, dan is dat al een motief op zichzelf denk ik. Als je buurman boos is en die weet iets van computers af, dan zou die jou best kunnen targeten. Eh, dat geldt voor een overheid, als die jou in de smiezen wilt houden of wat dan ook, dan eh, dan, dan kan die jou targeten. Eh, als een criminele organisatie iets in jou ziet, qua geld, he, dat kan ook, dat is vaak meer een wat bredere approach, dan ben jij waarschijnlijk niet de enige, ja, dan ben jij gewoon of makkelijk te vinden, dat kan, of je hebt gewoon- Ze hebben gewoon een bepaalde specifieke interesse. Bijvoorbeeld als je directeur bent van een bedrijf met macht over geldstromen bijvoorbeeld.

X: En vanuit het perspectief van [the professional services firm]?

Y: Wat zei je?

X: Als je denkt vanuit het perspectief van [the professional services firm].

Y: Ja, dat kunnen ook heel veel dingen zijn, bedrijfsspionage bijvoorbeeld. Eh, concurrenten, eh, overheden willen misschien in de gaten houden wat je afspreekt met een klant. Eh, of je, ja, iemand waar je zaken mee doet. Ik denk dat er wel veel dingen zijn. Ik denk dat we niet helemaal onze zeg maar, dat, eh, dat, dat je helemaal de beveiligingen naar beneden moet stellen omdat je denkt dat dat niet gaat gebeuren.

X: Wat zou de impact van een aanval kunnen zijn?

Y: De impact van een aanval. Hebben we het dan over [the professional services firm] specifiek?

X: Ja.

Y: Ik denk, het is echt reputatie in dit geval. Zeg maar, feitelijk, dus stel iemand he, een derde partij leest of ziet iets gevoeligs van een ja, van [the professional services firm], op zichzelf is dat niet zo boeiend. Eh, alleen wat je wilt voorkomen is dat er dingen uitlekken die ervoor zorgen dat je geen bedrijfsvoering meer kan doen. He, en we gaan er natuurlijk altijd vanuit dat, dat, he, we doen gewoon altijd iets goeds, he, we gaan er gewoon vanuit dat wij altijd goed handelen, he, maar wat voor de ene partij goed handelen is, is voor de andere partij misschien helemaal niet goed. He, zo zijn er natuurlijk veel belangen die spelen. He, en op het moment dat jij [1:13:40 till 1:13:49 has been omitted]. En aan de andere kant, als een overheid eh, ziet dat er iets, ja, niet volgens, eh, eh, ja, een bepaalde interesse heeft zeg maar, je wilt natuurlijk altijd spelen volgens het boekje en dat soort dingen, dus dat doe je dan ook. Maar eh, stel iets komt op straat wat, eh, ja, misschien niet helemaal eh, goed is voor hun, naar hun mening, dan kan dat ook gevolgen hebben voor de licenties die je hebt, he, dat je je bedrijfsvoering niet mag doen. En dat is natuurlijk, he, op het moment dat er iets fout gaat, maar ook denk ik dingen die binnen de regels goed zijn en niet binnen de publieke opinie vallen bijvoorbeeld, weet je, [1:14:40 till 1:14:53 has been omitted]. He, en ook al blijven we binnen de boekjes van de wet, we overtreden daarmee soms helemaal geen wetten, kan dat soms nog steeds verkeerd vallen bij de publieke opinie. En dat soort dingen wil je niet op straat hebben liggen.

X: Is dit ook wat je bedoelde met gevoelige informatie?

Y: Ja, absoluut, ja. Ja, en kijk ik heb het niet eens over de GDPR he, ik heb het echt eigenlijk alleen over puur confidential informatie. Tussen ons en de klant. He, we hebben ook gewoon, eh, onze verplichtingen om de, de vertrouwelijkheid te bewaken.

X: En je zei er eerder al iets over, maar hoe veilig is een VPN-verbinding?

Y: Eh, een VPN-verbinding is zo veilig als je het maakt. En dat is een heel vaag antwoord, maar in principe hangt het er heel erg van af hoe je hem inricht. Hoe richt je hem in en wat is punt A, wat is punt B, welke, eh, eh, protocollen gebruik je, welk beveiligingsalgoritme gebruik je, en heb je vertrouwen in je aanbieder, eh, waar heeft de aanbieder zijn server staan, wie heeft er allemaal toegang toe, he, wat, en dat hele stukje vertrouwen is heel belangrijk hierin. Is, he, wie heeft controle over het bedrijf, eh, ja, wie is de uiteindelijke eigenaar, wie, ja, hoe hebben zij hun interne beveiligingsmaatregelen getroffen. Er zijn heel veel vragen die je moet beantwoorden en waar je due diligence op moet doen, voordat je besluit op welke VPN je gaat gebruiken. En veel van dat soort IT-beslissingen op zichzelf zijn niet zo moeilijk. He, zijnde, we gaan een VPN gebruiken, maar daadwerkelijk het idee hebben dat je, dat je iets goed, he, neemt of koopt, daar gaat best wel wat werk, moeite en due diligence inzitten.

X: Als je deze onveiligheden opnoemt, veranderen jouw handelingen dan ook daardoor?

Y: Ik heb hier natuurlijk minder directe invloed op he, omdat [the professional services firm] als groot bedrijf hebben zij gekozen voor een bepaalde oplossing, om welke redenen dan ook. Eh, en hierbij ga ik er echt vanuit dat [the professional services firm] de juiste stappen heeft genomen om een partner in de hand te nemen. Eh, mijn handelingen veranderen daarom niet, maar ik heb natuurlijk zelf wel een soort van basis, basisprincipes van privacy en security en zeker als security professional, he, noem het maar zo, dan, ja, dan, dan, weet je in ieder geval hoe het in elkaar zit. En kun je niet blindelings vertrouwen op eh, keuzes die gemaakt zijn. He, dus ik zou niet 100% vertrouwen op keuzes die [the professional services firm] altijd maakt.

X: Als je dan basismaatregelen treft, kan je een voorbeeld geven van deze maatregelen?

Y: Die ik tref?

X: Ja.

Y: Ja, ik scheid bijvoorbeeld privé en werk scheid ik echt. Dus ik, ik gebruik geen, ik heb bepaalde apparaten voor bepaalde doeleinden, dat klinkt heel panisch, maar goed, ik ken nog, ik ken nog wel gevallen waarin mensen bijvoorbeeld een hele operating system in een USB-stick met zich meedragen, zodat er geen hardware bij betrokken is, nou dat vind ik te ver gaan. Eh, en ja ik kijk wel uit, he, in dat opzicht, ik weet in ieder geval wat, eh, wat ik wel en niet met de apparaten moet doen van [the professional services firm]. He, wetende ook bijvoorbeeld dat je e-mailbox eh, ten alle tijden kan worden geconfisqueerd, maar ook worden ingezien door alles en iedereen, nou, niet alles en iedereen, maar in ieder geval- Je zou denken van niet, maar iemand heeft natuurlijk toegang tot jouw e-mailbox, dus als er, dus als iemand zeg maar de wil heeft om erin te kijken, dan kan die dat, he, dat moet je altijd weten. En dat is, dat is natuurlijk van belang om in je achterhoofd te houden. Dus dat jij niet dingen erin zet waarvan jij denkt oké, dat hoeft mijn bedrijf niet te weten. Persoonlijke zaken moeten dus weggelaten worden uit je professionele e-mailbox. Zelfde voor [Softwareprovider], he, zelfde voor [Softwareprovider], maar je verlaagt natuurlijk het risico door dingen te spreiden. Dus niet al je gegevens op straat liggen op het moment dat een e-mailbox wordt gecompromitteerd.

X: Zijn er nog andere maatregelen die jij treft?

Y: Hm, ja, ligt eraan waarvoor. He, wat is het doel, weet je wel.

X: Ja, maatregelen die jij treft vanwege eventuele onveiligheden in de VPN.

Y: Nee, ik tref verder geen eh, maatregelen.

X: Dan waren dit tot zo ver mijn vragen. Heb jij nog iets wat niet ter sprake is gekomen over VPN?

Y: Oeh. Ik heb het idee dat ik heel veel heb gezegd over VPN. Ik denk jij ook. Eh, ik heb verder niet echt vragen.