# Transcription expert 6

Duration: 29 minutes

X: Dan begin ik met een hele open vraag. Kan jij aan mij vertellen wat een VPN is?

Y: De afkorting staat voor Virtual Private Network als ik het goed heb. Eh, een VPN is in principe, ja, is een mechanisme om een soort van veilige verbinding te maken tussen eigen laptop en een externe omgeving. Dat is hoe ik het zie. En daar zit dan een VPN-verbinding tussen om het ja, meer beveiligd eh, te maken. Eh, en dat is dan ook wat op alle [the professional services firm] laptops eh, uiteindelijk ook staan met die eh, die code, die je ook- Die [access token provider] code, die ik moet invoeren anders kom je niet op het netwerk van [the professional services firm]. Dus dat is hoe ik een VPN zie, dus eigenlijk een soort van, zoals ik zei, een beveiliging om, om te zorgen voor een veilige verbinding tussen je eigen standalone laptop die je gebruikt en tot een extern netwerk. Dat is hoe ik het zie.

X: Kan jij vertellen hoe deze verbinding beveiligd is?

Y: Oeh. Eh, ja, ik neem aan door middel van, ja, hoe, en dan het je het in de zin van technische zin, of-

X: Ja, of op een andere manier. Je zegt dat het een veilige verbinding is, wat bedoel je daarmee?

Y: Nou ja, dat je slechts, doordat je dus een app hebt op je telefoon met daarin dat je een code krijgt, die niet iedereen zomaar kan krijgen, dat je slechts op die manier in kan loggen op het netwerk. Dus in die zin dat het technisch wordt afgedwongen dat je eerst een code, of een software token code, nodig hebt, voordat je überhaupt op het netwerk kan komen.

X: En je maakt verbinding met een externe omgeving, wat bedoel je daarmee?

Y: Eh, daar bedoel ik mee de [the professional services firm] omgeving. Dus inzicht krijgen in de [the professional services firm] portal tot de [the professional services firm] documentatie die wij vastleggen op bijvoorbeeld [an internal page], daar zit gevoelige eh, informatie in en daar kan je alleen maar toegang toe krijgen als je eerst met je VPN verbonden bent.

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

Y: Eh, nou ja, ik gaf al aan, beveiliging van documentatie, privacy. Verder, ja, ja, wat een vraag, ja, ik denk dat is het.

X: Welke handelingen voer jij uit als een gebruiker om een verbinding te maken? Want je zegt al net dat je de [access token provider] code invult-

Y: Hmhm. Ja, dat klopt. Dus welke handelingen ik moet verrichten, of-

X: Ja.

Y: Is je vraag. Oké. Ja, allereerst als je bij [the professional services firm] komt werken heb je die app nodig, zonder die app krijg je ook geen toegang. Dus je hebt ook sowieso een [the professional services firm] mobiel nodig. Of in ieder geval je moet [the professional services firm] medewerker zijn. Dus ik heb een, naast dat het een app kan zijn kan het ook een token zijn, en daar eh, dan krijg je daar die code op. Je moet eerst zelf een persoonlijke code instellen, weet ik nog. Eh, aan het begin van mijn dienstverband. Die wijzigt overigens geloof ik niet, die hoef je niet periodiek te wijzigen en dan eh, ja, om echt toegang te krijgen moet je eerst je eigen persoonlijke code dus instellen, zodra je die hebt ingesteld kun je verbinding maken met de, je eigen code dus samen met dan de [access token provider] code, die je ja, standaard krijgt vanuit ofwel die app ofwel de token, de fysieke token.

X: En op welke apparaten gebruik jij een VPN?

Y: Alleen op mijn laptop.

X: En maak jij ook verbinding met het interne netwerk van [the professional services firm] op jouw mobiel?

Y: Eh, nou, ik heb het wel eens gedaan, maar ik heb eigenlijk, bijvoorbeeld ik heb mail en al dat soort dingen heb ik eigenlijk niet meer op mijn werktelefoon staan, dus nee. Ik heb dat dus ook niet echt meer nodig, omdat ik die apps er ook niet op heb, op heb staan.

X: Gebruikte je daarvoor dan destijds een VPN-verbinding voor?

Y: Phoe. Goede vraag. Ik geloof voor sommige apps wel, maar niet voor allemaal. Ik weet even niet meer helemaal uit mijn hoofd voor welke wel, welke niet eh, to be honest. Het is al een hele lange tijd geleden dat ik die op mijn mobiel had, had staan.

X: Oké. En je zei al dat je niet heel veel van VPN van de technische kant weet, maar zou je mij kunnen vertellen hoe een VPN-verbinding werkt? Hiervoor kan je het whiteboard gebruiken als je dat fijn vindt.

Y: Ja, ja, eens even kijken. Nou, laten we eens even kijken. [start drawing 6\_1]. Eh, als dit, kan je ook, dit kan niet he, nee, o, ja, kan wel. Als dit je- Moet ik gewoon zo, ja. Ik dacht misschien kan je ook schrijven, maar dat kan niet.

X: Je kan typen.

Y: Toch wel?

X: Door een vierkant ook te tekenen, dan kan je daarin eh-

Y: Misschien eh, nee. O, eens even kijken. Hmhm. O, zo ja. Als dit je laptop is, dan- Ik weet niet of ik het zo goed omschrijf hoor, misschien doe ik het ook wel helemaal fout. Maar je gaf al aan er zijn niet echt foute antwoorden.

X: Maakt niet uit.

Y: Wat zei je?

X: Maakt niet uit of het goed of fout is, het gaat erom hoe jij denkt dat een VPN-verbinding werkt.

Y: O ja, dit moet de cloud voorstellen, maar oké. Cloud eh-

X: O.

Y: Sorry. Andere kleurtjes. Zo, hmhm. Dan is dit eigenlijk je, ja, maar misschien dat ik het verkeerd omschrijf hoor. Eh, het is nu wel iets te klein, kan ik het groter maken. Hij heeft eigenlijk iets meer als een firewall, maar oké. Eh, hmhm. Nee. Ik weet niet een beetje hoe ik het zou uittekenen, dus dat je hier je toegang moet maken met je eh, VPN. [start drawing 6\_2]. Als je geen signaal terugkrijgt, dan kun je ook niet toegang krijgen. En zodra je pas een signaal krijgt, krijgt je pas toegang tot het netwerk. Hoe ik het zou uittekenen.

X: Wat bedoel je met een signaal terugkrijgen?

Y: Eh, nou, een signaal terugkrijgen bedoel ik mee dat je altijd een code nodig hebt. Zonder dat je een code hebt, kun je ook niet toegang krijgen. Als je je code foutief invoert, dus stel ik heb code, een persoonlijke code, dus ik zeg iets, 00887766, en je vult daar een andere code in, dan krijg je een foutmelding. Dus dan krijg je geen toegang.

X: Daarmee bedoel je dan je pincode? Je persoonlijke code dus zeg maar, die niet veranderd.

Y: Ja, klopt.

X: Oké, duidelijk. En kan je meer vertellen over de gele lijn?

Y: Deze? De oranje?

X: Ja.

Y: Oké, eh. Wat kan ik vertellen. Ja, dat zal een soort van, een, ja, ik weet niet helemaal hoe ik het moet omschrijven. Vind ik wel moeilijk. Een soort van een, ja, ik weet niet helemaal of je het kan noemen zo, maar een firewall is in principe ook een soort van een tunnel of het is een bepaalde zone waar je in principe doorheen moet. Eh, ja, voordat je er doorheen komt. Eh, ik weet niet helemaal of het een zone, ja, een soort van versleutelde zone waar je eerst doorheen moet, zonder dat je er daadwerkelijk echt doorheen kan komen. Ik weet niet of dat het toelicht, deze lijn, een versleutelde zone.

X: Wat bedoel je dan met versleuteld?

Y: Ja, dat je er slechts doorheen kan als je de juiste toegang krijgt.

X: En je omschrijft het ook als een tunnel, wat bedoel je daarmee?

Y: Ja, een tunnel omgeving. Er zal iets zitten in je laptop waarmee die bepaalt of je er wel of niet doorheen komt. Dus er zal wel een iets van een tunnel of een soort van kluis, die pas open gaan als je dus de juiste codes invoert.

X: Oké, dankjewel.

Y: Zodoende een tunnel.

X: Eh, dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: De invloed van VPN op mijn computerbeveiliging, is dat je vraag?

X: Ja.

Y: Eh, nou ja, dat je dus niet zomaar bij gegevens kan van eh, van, van klanten die eigenlijk in principe op de [the professional services firm] eh, netwerk staan, of [the professional services firm] gegevens staan. Dus vanuit die zin heeft VPN een positieve invloed, omdat je eigenlijk alleen maar erbij kan als je VPN, met VPN verbonden bent.

X: Oké. En zijn er nog meer invloeden van VPN op jouw computerbeveiliging?

Y: Eh, nou het enige wat mij wel opviel is dat ...(0:12:27) dat we eerder gebruikte we, of gebruikte ik eigenlijk altijd eh, Firefox, zeg ik dat goed. Nee, Explorer, Explorer gebruikte ik altijd. En nu gebruiken we ook, sinds kort gebruik ik Edge of Chrome en ik geloof in ieder geval voor Edge in het begin had je soms niet een VPN-verbinding nodig tot eh, tot bepaalde [the professional services firm] tools te komen, dus dat vond ik wel interessant hoe dat dan werkt.

X: En was dat nog locatieafhankelijk?

Y: Eh, nee, ik geloof dat maakte in principe toen niet per se uit. Als je op [the professional services firm] netwerk zit, dan ben je er sowieso al in, dus dan heb je ook niet meer de VPN eh, code nodig. Dan zit je op het [the professional services firm] netwerk, dus dan herkend die blijkbaar al dat je geautoriseerd bent. Maar vooral namelijk vanuit andere locaties dan een [the professional services firm] kantoor kon je gewoon al standaard er al inkomen, in ja, [an internal page] heet dat in ieder geval, dat is de omgeving die ik hiermee, waar ik zelf gebruik van maak. Dus dat vind ik wel interessant, eerder had je altijd een code nodig, anders kom je [an internal page] niet eh, in principe niet in.

X: Een verbinding nodig hebt om eh, binnen [an internal page] te komen.

Y: Ja, en in [an internal page] leggen wij eigenlijk alle, ja, dat is ons dossier om onze ja, werkzaamheden in vast te leggen, dus daar liggen best wel veel gevoelige, gevoelige informatie in.

X: Dan een andere vraag. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Eh, voornamelijk phishing e-mails. En zelf heb ik ja, ik denk voornamelijk phishing e-mails, maar die krijg ik niet naar mijn werkemail hoor. Meer naar mijn privé email.

X: Kan je nog een andere digitale dreigingen bedenken?

Y: Nou eh, niet waar ik zelf mee te maken heb. [the professional services firm] breed zal er wel mee te maken hebben. Zoals eh, ik zeg maar iets, ransomware of eh, DDoS attacks, maar dat heb ik zelf niet een eh, reguliere dag basis. Ja, we hebben natuurlijk wel, ja, digitale dreigingen, ik weet niet of je het dan ook hebt over fysieke dreigingen, fysieke digitale dreigingen, maar dat is misschien anders.

X: Ja, bijvoorbeeld.

Y: Nou, bijvoorbeeld, ik heb, stel dat [0:15:02 till 0:15:04 has been omitted] en ik heb eh, mijn code, ik heb een token, die heb ik nog, maar die moet ik eigenlijk al heel lang inleveren, dus dat moet ik nog even doen. Maar stel dat iemand die pakt en ik laat mijn laptop open staan, dus ik lock mijn laptop niet. Ja, dan kan iemand zo maar even meekijken met mijn eh, gegevens op mijn laptop of eh, überhaupt meekijken op mijn scherm. Dus daarvoor heb je ook die privacy screen setting op je laptop, moet je eigenlijk wel altijd aan hebben [0:15:33 till 0:15:37 has been omitted] zou kunnen meekijken. Dus dat soort ja, misschien iets minder dus echt een digitale dreiging, maar wel een-

X: Meer een sociale dreiging is dat dan.

Y: Ja, misschien dat dat het is ja.

X: Kan je nog andere sociale dreigingen bedenken?

Y: Eh, ja, nou ja, maar dat is meer, stel dat ik probeer in te breken bij een ander bedrijf, stel dat ik in het pand probeer te komen met een eh, pasje van iemand anders en dat ik zo ook toegang krijg tot bepaalde informatie, maar ik denk dat dat iets te veel afwijkt van het onderwerp, maar dat kan ik me nog bedenken. Eh, ik bedenk even niets, misschien wel dat ik er zo op kom.

X: Dit zijn al voorbeelden. Eh, heeft de VPN-verbinding nog invloed op deze dreiging?

Y: Wat zei je, sorry?

X: Verandert de soort dreiging door een VPN-verbinding?

Y: Ligt eraan wat je dreiging is. Eh, VPN-verbinding kan best een goed mechanisme zijn, alleen als de mens het eh, een beetje laat slingeren, dan heb je er alsnog niks aan. Dus stel dat ik mijn code, mijn token overal laat slingeren, ja dan is het heel leuk dat je een VPN kan eh, verbinden, of in ieder geval met je code, maar als iedereen toegang heeft tot die code dan heb je er alsnog weinig aan. Eh, als je het echt hebt over die phishing mails die ik aan het begin zei, dan denk ik niet dat VPN daar invloed op heeft, maar dat is misschien mijn technische, niet onderbouwde, hoe noem je dat, niet onderbouwde technische kennis. Naar mijn eigen inschatting zou VPN daar geen invloed op moeten hebben.

X: En als je het dan hebt over phishing mails of eh-

Y: Hmhm.

X: [0:17:46 till 0:17:49 has been omitted], wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Eh, wij zelf. ...(0:18:01).

X: Sorry?

Y: Moet ik nog iets toelichten? Ik weet niet hoor.

X: Sorry, wat zeg je?

Y: Moet ik nog iets toelichten? Of niet?

X: O, ja.

Y: O, ik hoorde de laatste vraag niet denk ik.

X: Oké, eh, als je het hebt over die verschillende soorten dreigingen-

Y: Ja.

X: Wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Ja, oké. Nee, ik dacht dat ik daarop antwoord gaf. Ja, wij zelf, vaak initieert een phishing mail, dat is iemand die, een soort van een outsider, die probeert in te breken in eh, in de omgeving natuurlijk. Maar dat wordt altijd geïnitieerd door een mens, dus een persoon. Dus daarmee zijn wij zelf eigenlijk de initiator van zo een dreiging.

X: Als je het dan hebt over die outsiders, wat voor outsiders zijn dat?

Y: Ligt eraan wat hun intenties zijn, dus het kan een outsider zijn, bijvoorbeeld een eh, ja, ik weet niet of- Ik kom niet helemaal op het woord, maar een soort van een rookie, een rookie, zo een woord. Dus het kan zijn een, gewoon een gast, een jonge gast die denkt nou ik ga haha, ik ga voor de lol even proberen in te breken, maar het kan ook zijn dat het echt gaat om een outsider die meer ja, politieke bepaalde dreigingen te veroorzaken. Eh, dus dan kijk je, dan is het een heel ander motief waarom iemand zo een dreiging zou initiëren. Eh, andere outsiders, ja, het kan hacktivists, maar het kan ook gaan om, dus die politieke redenen gaf ik aan, het kan ook zijn iemand die echt schade aan wil richten, dus iemand die eh, ja, wat is het woord nou daarvoor, [0:20:13 till 0:20:15 has been omitted], vijf van die typen outsiders. Maar ik weet even niet meer de naam van zo een, echt iemand die dus echt schade wil aanrichten, dus niet om politice, politieke redenen of eh, maar echt bewust bepaalde gegevens op straat wil geven. Maar ik komen even niet op de term van zo een outsider.

X: Ik ben niet op zoek naar specifieke termen per sé, maar meer gewoon omschrijvingen. Dus je noemt al verschillende motivaties die er zijn, kan je nog meer motivaties bedenken?

Y: Even kijken, ik zei dus politieke redenen, ik zei om gewoon grapje uit te halen, ik zei om ja, dus echt eh, schade aan te richten vanwege zeg maar iets eh, nou, hoe heet het nou, ik kom er gewoon even niet op, he. Eh, redenen. Nee, ik denk het niet, misschien dat ik er zo nog even op kom. Ik ben nog heel even aan het malen in mijn geheugen.

X: We kunnen naar een volgende vraag doorgaan.

Y: Ja, misschien na een volgende vraag. Misschien kom ik er zo wel op terug.

X: Ja, prima. Als je bedenkt wat voor achtergrond een aanvaller heeft, wat zou dat kunnen zijn?

Y: Eh, denk ik ook, licht er wel aan, die mensen zijn best wel, ze zullen vast wel een technische, technische achtergrond hebben, anders weten ze echt niet hoe ze zo daarbinnen kunnen komen. Dus de achtergrond zal vaak zijn, of het is iemand die- Ik weet niet helemaal wat je bedoelt met achtergrond, in de zin van opleidingsachtergrond of in de zin van waarom zou iemand een dreiging willen veroorzaken.

X: Ja, opleidingsachtergond, dan wel formeel of informeel.

Y: Oké. Ja, ja, ik denk dus inderdaad eh, qua opleidingsachtergrond zal het echt wel een technische studie zijn, dus ik denk iets van business informatics ofzo, of iets van computer science, waarvoor je eh, ja, echt wel de skills nodig hebt eh, om zo een dreiging te kunnen veroorzaken. Ik denk niet dat je dat zo maar kan als je nou, zoals ik [me] heb gestudeerd. Maar dat is mijn eigen inschatting. Maar het hoeft niet altijd te zijn door middel van een opleiding, maar ook gewoon mensen die gewoon slim zijn eh, met computers an sich, dus die hebben dat op de een of andere manier aangeleerd of die hebben er gewoon affiniteit mee.

X: Als je nadenkt-

Y: Zal wel een soort van bètastudie zijn.

X: Sorry, wat zei je?

Y: Ik denk vooral mensen met een bèta achtergrond, bèta, bèta.

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

Y: Voor [the professional services firm] denk ik relatief, licht eraan waar ze toegang tot krijgen. Eh, maar als ik het weer heb over bijvoorbeeld stel dat een hacker toegang krijgt tot eh, tot [an internal page], dus tot die omgeving, dan kan dat best wel veel eh, schade verrichten, want daar zit gewoon allemaal klantgevoelige informatie in, in ons dossier. [0:23:44 till 0:24:20 has been omitted]. Dus dan heeft het zowel impact ons onze reputatieschade [0:24:24 till 0:24:26 has been omitted]. Dus dat heeft echt wel een hele grote impact. Maar als ze alleen toegang krijgen tot bijvoorbeeld het, ik zeg maar iets, intranet ofzo en daar staat alleen op dat eh, ik zeg maar iets hoor, dat [role] verspreidt hoe wij omgaan met coronavirus, ja, dan denk ik nou dat is misschien iets minder spannend als dat op straat komt, maar ligt er dus ook aan waar ze toegang tot krijgen.

X: Deze verschillende soorten impact, zou daar nog verschil in zijn?

Y: Ja, ja, dus ik denk wel inderdaad echt toegang tot ons [an internal page] dossier zou een heel grote impact hebben, maar toegang tot een intranetwebsite zou misschien minder impact hebben.

X: Oké. Dan gaan we terug naar de VPN-verbinding zelf-

Y: Ja.

X: Hoe veilig is een VPN-verbinding?

Y: Ja, nou, dat eh, ik zag dat al dat dat een van je vragen was, maar dat vond ik al een lastige vraag, want ik geloof dat je best wel makkelijk kan inbreken in een VPN, maar zoals ik zei, ik ben niet heel technisch onderlegd, dus ik weet het niet helemaal. Dus dat weet ik eigenlijk niet. Wat zei je?

X: Zei je dat je wel of niet kan inbreken in een VPN?

Y: Nee, nee, ik zou het niet weten. Ik weet niet of je daarop kan inbreken, ik denk dat je, dat het wel moet kunnen ofzo, maar ik zou niet weten hoe.

X: Oké. Ik zou ook niet weten hoe hoor, als je dat-

Y: Haha, ik denk dat het vast allemaal kan allemaal, vast, maar-

X: En houd jij nog op een bepaalde manier rekening met mogelijke onveiligheden van VPN? Zijn er bepaalde handelingen die jij uitvoert?

Y: Nee, nee, eerlijk gezegd niet. Ja, goed, ik houd me token houd ik altijd in mijn etui, zeg maar iets, ik laat hem niet- Mijn etui heb ik eigenlijk altijd eh, dicht zitten, want ik haal er alleen maar een pen uit en dan doe ik hem weer dicht, dus daar let ik wel op, maar voor de rest ben ik er niet heel bewust mee bezig, to be honest. Het is meer een handeling geworden, een automatische handeling als je je laptop opstart, want je vult gewoon zo een code in, maar ik heb daar niet echt specifieke beveiligingsmethodes voor ofzo.

X: Jij, eh, iedere keer als jij je laptop opstart, maak je direct verbinding met de VPN?

Y: Ja, ja, als ik thuis werk wel ja.

X: En ga je dan alleen naar het [the professional services firm] netwerk?

Y: Eh, ja, ja. [0:27:22 till 0:27:22 has been omitted].

X: Oké. Zijn er nog dingen van VPN die jij wel weet die niet ter sprake zijn gekomen, waar ik niet naar gevraagd heb?

Y: Eh, even nadenken hoor. Nee, denk het niet.

X: Dan waren dit tot zo ver mijn vragen, heb jij zelf nog vragen?

Y: Ja, ik vraag me af waar dit dan uiteindelijk op uitkomt, laat maar zeggen, want jij, op het einde ging het er natuurlijk wel even over, van denk je dat VPN ja, moet ik heel even nadenken hoe ik het duidelijk weer- Dus helpt, is VPN, kan dat, is dat secure genoeg om die dreigingen laat maar zeggen te eh, nou ja, tegen te houden of te voorkomen, ja, ik vraag me af wat daar dan uitkomt laat maar zeggen, waar jouw, wat jouw resultaat is van jouw onderzoek, maar dat weet jij nu ook nog niet, want je bent nu nog volop bezig met interviews natuurlijk.

X: Ik zal even de opname stopzetten.

Y: Ja.