# Transcription expert 2

Duration: 30 minutes

X: Kan jij aan mij uitleggen wat een VPN is?

Y: Nou, van wat ik weet, een VPN is een Virtual Private Network en het beveiligd de verbinding als je bijvoorbeeld, eh, off-site werkt. Dat je toegang hebt tot, eh, bijvoorbeeld je bedrijfsgegevens of wat voor gegevens dan ook, maar op een beveiligde verbinding. Een beetje encrypted verbinding, waardoor je gegevens niet zomaar gelekt kunnen worden. Dat je toegang hebt tot eh, bepaalde webpagina's die gewoon via de internet niet eh, toegankelijk zijn.

X: En hoe zijn deze niet toegankelijk normaal?

Y: Hoe zijn ze niet toegankelijk normaal?

X: Ja.

Y: Eh, gezien het in het interne netwerk is van je bedrijf of waar je het ook opzet. Maar meestal- Ik ken het alleen in het bedrijfsleven. Gezien het in het bedrijfsleven in het interne netwerk bevindt, dan is het eh, afgesloten van eh, ja, het internet, dus de buitenwereld. En met een VPN kan je wel toegang krijgen tot eh, ja, alles wat in het interne netwerk is van je bedrijf.

X: Oké, en je zet dat het een beveiligde verbinding is. Kan je meer vertellen over deze verbinding?

Y: Nou, het enige wat ik weet is dat het geencrypt wordt, maar verder weet ik niet veel van VPN, dus het technische deel van hoe het precies in elkaar zit.

X: En wordt de hele verbinding encrypted?

Y: Dat hoop ik wel. Wat ik vermoed, niet zeker, maar wat ik vermoed is dat het eh, op het moment dat je het opzet dat alles wat eh, van jouw laptop, of jouw telefoon, of mobiele device, dat die dan geencrypt wordt naar het interne netwerk van je bedrijf.

X: En je zegt laptop en mobiele device. Gebruik jij ook op allebei deze apparaten een VPN-verbinding?

Y: Eh, ja en nee. Voor werk gebruik ik alleen op mijn laptop, eh, voor eh, voor mijn mobiele device, dus mijn telefoon, mijn mobiele telefoon daar zit het al, eh, ik weet niet hoe de applicatie heet, maar [example of mobile application], en ik vermoed dat dat ook eh, op een of andere manier beveiligd is.

X: Bedoel je ook beveiligd via een VPN-verbinding of op een andere manier?

Y: Dat weet ik eigenlijk niet. Is een beetje raar als security expert dat ik dat niet weer, maar je verwacht wel dat werk het goed geregeld heeft. Maar je krijgt wel dat dat ervoor zorgt dat je applicaties die je binnen de [example of mobile application] download, dus je [example of mobile application], je [example of mobile application], en al die, zulke, [example of mobile application], je krijgt wel een melding dat het geencrypt wordt. Dus ik verwacht wel dat het, ja, ik weet niet of het echt VPN is, maar ik verwacht wel dat ze het op een of andere manier eh, beveiligd is.

X: Op je mobiel dan bedoel je.

Y: Ja, mobiel.

X: En je zegt dat jij een VPN-verbinding off-site gebruikt. Op wat voor plaatsen gebruik jij een VPN?

Y: Eh, thuis. Of ja, waar ik mijn laptop ook gebruik eigenlijk. Want als ik [0:04:36 till 0:04:37 has been omitted], dan zet ik ook mijn VPN aan om gewoon bij [the professional services firm] dingen te komen, documenten of je mail of wat dan ook.

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

Y: Nou, in principe niet, in principe is het meer om je, ja, je weet eh, dan dat je gewoon bij alle gegevens kan komen. Als ik het niet nodig heb zet ik het ook niet aan. Maar dat is eh, als je buiten werkt is het eh, het handigste om dat te gebruiken, want dan weet je zeker dat het ook eh, beveiligd is. Dus voor het zekere voor het onzekere zet ik het altijd aan als ik, zeker als ik [0:05:14 till 0:05:15 has been omitted], eh, thuis zet ik het aan als ik bijvoorbeeld bij een [the professional services firm] applicatie moet zijn, maar dat moet, want anders kom je er niet bij. Maar e-mail, als ik alleen bij e-mail en [cloud software] moet zijn, dan laat ik de VPN uit, want dan is het niet nodig. Maar dat is alleen als ik thuis ben. Op het moment dat ik buiten zit bij een café of eh, ergens, dan zet ik altijd, ja, voor de zekerheid zet ik de VPN toch aan.

X: De VPN aan.

Y: Ja.

X: Waarom zet je dan de VPN aan?

Y: Dat geeft een gevoel van vertrouwen. Maar, in principe, ik weet weinig van VPN, maar het is gewoon een gevoel van vertrouwen dat je hebt, dat het eh, je communicatie die je op dat moment bezig mee bent, dat dat wel op een veilige manier gebeurt.

X: En op wat voor manier gebeurt dat veilig?

Y: Nou de encryptie die je toepast. Die ja, toegepast wordt door VPN.

X: De verbinding dan bedoel je?

Y: Ja, precies.

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

Y: Eh, de eh, [the VPN of the professional services firm] openzetten, nou, eerst mijn wifi van waar ik ook zit aan te eh, connecten. Daarna de [the VPN of the professional services firm], mijn zes-cijferige pincode invoeren en dan de eh, vier- of vijf-cijferige code van eh, [access token provider], en dan connect, dan heb je hem. Dus dat is simpel, maar daarom heb ik ook nooit achter gezocht van eh, wat allemaal precies doet op technisch niveau.

X: Je voegt een extra code toe naast je pincode, waar haal je die code vandaan?

Y: Van [access token provider] eh, [access token provider] is de token. Van [access token provider].

X: Oké, dat is een token. Wat voor een token?

Y: Het is een eh, software token dat je krijgt van [the professional services firm], de applicatie heet [example of mobile application] en daarop krijg je een zescijferige code is het en het heet een [the professional services firm] software token. Dus als je- En het verandert met de minuut krijg je een nieuwe code.

X: Zijn er nog andere manieren, eh, andere soort tokens?

Y: Eh, ja, je hebt zeg maar de ene die je in je hand gewoon al, ja het is echt een token, het lijkt op zo een klein dingetje, ovaal dingetje, en daarin, maar het is hetzelfde principe, dus het verandert de code om de minuut.

X: Zou je mij kunnen uitleggen hoe een VPN-verbinding werkt? Je kan hiervoor ook het whiteboard gebruiken als je dat fijn vindt.

Y: Ja, ik zou het wat kunnen tekenen, maar, oké. Eh, even kijken, hoe kan ik tekenen. Moet ik het naar mijn scherm, nee, ik kan het niet gebruiken. O, ja, ik heb hem. Dus stel je hebt hier je laptop, zo, ik ben niet heel goed met tekenen, maar oké. Denk dat het wel duidelijk is. Zo, je laptop, en dan heb je hier ergens de VPN. En hier heb je de server van eh, [the professional services firm]. En dan heb je zeg maar hierachter internet en dan is de VPN-tunnel, die loopt zo. En dat weet ik wel dat het een tunnel heet, maar dan gaat het via het internet, maar dan via een beveiligde verbinding naar de server van [the professional services firm].

X: Kan je dan meer specifiek uitleggen over de VPN die je hebt getekend?

Y: Dit?

X: Ja.

Y: Nee, nee, daar weet ik niet meer van inhoudelijk of technisch gebied.

X: Want de VPN zit dus in het internet?

Y: Nee, het is niet echt in het internet, maar het gaat over het internet heen via de tunnel. Maar ik zou niet weten hoe ik het anders moet tekenen. Maar niet dat het in het internet zit nee.

X: En wat bedoel je met een tunnel?

Y: Eh, ja, de tunnel is eigenlijk alles wat door de tunnel heen gaat, encrypted is. Dus alles wat hierdoorheen gaat is gescheiden van het echte internet.

X: Maakt het voor deze tekening nog uit waar je bent als fysieke locatie?

Y: Nee. Nee, maakt niet uit. Zo lang je een mobiele device hebt en je verbindt met de VPN dan gaat alle gegeven die je hier hebt heen en weer.

X: Stel je voor dat je dan een e-mail stuurt, hoe zou dat in dit proces verlopen?

Y: Dat weet ik niet. Ik vermoed gewoon dat alles wat je hier doet, via de VPN gaat hiernaartoe. Maar, technisch weet ik niet meer dan dat.

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

Y: Een goede vraag. Ik denk eh, als je verbindt met een VPN of eh, als je computer verbonden is met een VPN van [the professional services firm] bedoel je.

X: Ja.

Y: Kan ik me zoiets voorstellen dat er dan eh, bijvoorbeeld automatisch updates uitstuurt. Nee, ik heb eh, eerlijk gezegd eh, weinig idee over hoe het allemaal technisch gaat.

X: Oké. En hoe zouden de automatische updates gestuurd worden?

Y: Dat wordt als het goed is gepushed naar je laptop via de admin. Dus dat zou- Waarschijnlijk gaat dat ook via VPN, want zolang je geen VPN aanzet, heb ik meegemaakt toen [0:11:54 till 0:11:55 has been omitted], dat er ook geen updates gebeurt. Dus je moet een keer per week ongeveer moet je VPN even verbinden en dan krijg je ook die eh, worden die updates automatisch gepushed en ook automatisch bijgewerkt. Daar hoeven wij als medewerkers weinig mee te doen.

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

Y: Ik denk de meest voorkomende zijn sms’jes. Ik heb weinig last van spam e-mails, maar sms’jes die krijg ik wel van een of andere partij die zegt bijvoorbeeld je [company] krediet wacht op je goedkeuring, log hier in. Of je, je krijgt een sms’je van CJIB dat je een boete nog moet betalen. Maar voor werk heb ik zelf nog niet meegemaakt dat ik eh, een spam email krijg waar klik op een link of iets dergelijks.

X: Heb je met nog meer digitale dreigingen te maken?

Y: Eh, voor mij niet. Eh, enige waar ik gewoon zorg eh, als ik bijvoorbeeld klaar ben met een klant, dat ik die gegevens ook van mijn harde schijf verwijder, zodat ze echt op het interne netwerk van [the professional services firm] zitten. Maar nee, ik heb geen dreiging meegemaakt eh, in mijn carrière.

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

Y: Eh, ik denk het wel. Zou wel logisch moeten zijn. Want op het moment dat je een encrypted verbinding opzet, dan is het niet, of ik kan niet zeggen niet mogelijk, maar het is minder moeilijk, of minder makkelijk om bij je interne gegevens te komen.

X: Hoe bedoel je dat?

Y: Wat zeg je?

X: Hoe bedoel je dat?

Y: Nou, gezien de gegevens geencrypt gaan via de VPN, dan vermoed ik dat het onmogelijk is, of bijna onmogelijk is om bij die gegevens te komen. Voor een externe persoon. Dus ook al heeft die toegang tot jouw internet of tot jouw laptop, op eh, op een slechte manier. Dan vermoed ik dat alles toch wat je communiceert via de VPN wel veilig blijft.

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

Y: Eh, weinig, omdat ik eh, geen social media gebruiker ben. Ik heb wel accounts maar eh, ja, er is weinig te halen eruit, omdat ik niet echt eh, gebruik van maak.

X: En heb je nog te maken met andere sociale dreigingen?

Y: Ik de enige die ik te maken mee zou kunnen hebben is het hacken. Dat als iemand mijn laptop hackt of mijn mobiele device hackt, maar that's it. En zelfs als dat gebeurt dan heb ik eh, op afstand dat ik alles kan verwijderen. Dus als ik eh, zie dat iets gebeurt, kijk dat heb je sowieso met de werklaptop, vanuit je mobiele telefoon eh, kan je zowel met de eh, kan ik de IT-service desk bellen verwijder alles en ook eh, ook van mijn eigen [mobile phone], omdat ik mijn privé [mobile phone] gebruik voor werk, kan ik het ook zelf verwijderen. Dus het enige wat ik kan bedenken wat een dreiging voor mij is dat mijn laptop of mijn mobiele device gehackt wordt, maar er is niet veel te halen eruit.

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

Y: Eh, ja. Want als ik iets moet delen dan is het wel via een beveiligde verbinding. Dus dan is de kans dat het gebeurt veel kleiner dan als je zonder VPN iets gaat delen. Bijvoorbeeld [cloud software] zit niet verbonden aan de VPN. Daar kan je altijd iets uploaden en downloaden zonder VPN te gebruiken. Als je hele gevoelige gegevens moet gaan delen, dan niet via [cloud software], maar eh, alles wat wij delen met de klant dat gevoelig is, dat wordt eerst geencrypt eh, dus dat zit op de [cloud software], of eh [cloud software] niet, [an internal page] gebruikte ik altijd, dat is ook via met VPN te verbinden. Via [an internal page] wordt dat gedeeld met de klant. Dus we doen heel weinig delen via eh, e-mail als het heel gevoelige gegevens is.

X: Eh, en wie of wat is de aanvaller die de dreiging veroorzaakt?

Y: Eh, als ik kijk naar wat ik deel, dan zou ik me kunnen bedenken dat het een competitor is, dus iemand die graag die gegevens van een andere eh, partij in handen wil hebben om daar zijn eh, voordeel uit te halen. Misschien is het ook handig om wat achtergrond te geven daarbij. [0:17:12 till 0:17:25 has been omitted]. Dus als ik kijk naar wie die gegevens zou willen hebben, dan zou het een competitor zijn, maar that's it.

X: Zouden er nog andere aanvallers kunnen zijn?

Y: Ja. Het zou gewoon eh, een random persoon kunnen zijn ook, die gewoon zegt oké, laat me even kijken wat voor gegevens ik kan halen uit [the professional services firm]. Om financiële schade te eh, niet financieel maar, eh, hoe noem je dat. O, jee, ik ben het woord even kwijt. Een schade aan het bedrijf, dus eh, momentje. Even het woord opzoeken, sorry.

X: Geen probleem.

Y: O, wauw, ik ben het woord gewoon even kwijt.

X: Je kan het ook omschrijven anders.

Y: Eh, ja, schade aan je bedrijf, dus dat je in de krant of eh, in het nieuws met slechte naam komt.

X: Reputatie?

Y: Reputatieschade, precies.

X: Dus dat is ook de motivatie van een aanvaller dan, motivatie-

Y: Ik denk dat dat de grootste motivatie zou zijn om eh, als ik kijk naar mij specifiek, om mij specifiek aan te vallen, dan zou het echt reputatieschade of om eh, ja, om te zeggen ja kijk, [the professional services firm] beveiligd niet goed of eh, zo makkelijk is het om bij gegevens van [the professional services firm] te komen. Bij mij persoonlijk valt er niet veel te halen.

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

Y: Achtergrond, ja. Eh, ja, ik heb eerlijk gezegd eh, geen idee. Misschien moet ik breder denken dan alleen aan mij, wat ik op mijn laptop heb. Eh, nee. Ik kom even niet op een goed antwoord.

X: Want je noemde eerder een ander bedrijf of een random persoon-

Y: Ja.

X: Wat moet zo iemand kunnen om een aanval succesvol te laten zijn?

Y: In principe niet veel, want eh, wat ik heb meegemaakt is dat met social engineering al genoeg kan eh, uithalen. Dus dat qua technisch heb je misschien helemaal geen kennis nodig om bij alle gegevens te komen, maar als je social engineering goed kan toepassen en dan gewoon toegang krijgt bijvoorbeeld tot USB-sticks, kijk gelukkig gebruiken wij dat niet, of ik niet. Maar dat zou ook een eh, manier kunnen zijn om bij gegevens te kunnen komen van [the professional services firm].

X: Bedoel je-

Y: Maar als je gewoon goed wilt kijken naar eh, ja, dan heb je wel de technische kennis nodig om te kunnen hacken bijvoorbeeld.

X: Hoe bedoel je dan social engineering?

Y: Eh, social engineering is bijvoorbeeld dat je eh, via spam een link stuurt, dat ik dan op die link klik. Dan moet het wel een goed opgezette e-mail zijn die betrouwbaar overkomt. Eh, tweede is dat je eh, eh, persoonlijk eh, tot, toegang krijgt tot mijn laptop, maar dat is ook niet waarschijnlijk, maar als iemand bijvoorbeeld achter je rug staat, stel [0:21:23 till 0:21:25 has been omitted] en iemand staat achter mijn rug te kijken hoe ik mijn wachtwoord invoer, dan is dat ook een manier om bij mijn, bij [the professional services firm] gegevens te komen. [0:21:35 till 0:21:36 has been omitted], die persoon kijkt naar je wachtwoord, je gaat even lunchen, ja dan heeft die wel een half uurtje zeker de tijd om bij alle gegevens te komen, als die je wachtwoord weet. En dat heeft ook een beetje met VPN te maken, want stel die persoon krijgt toegang tot mijn wachtwoord en ik ga even lunchen, mijn VPN blijft aan, een VPN is voor de hele dag bijna geldig, je moet dat een keer in de ochtend aanzetten en dan is die voor de rest van de dag geldig als je op hetzelfde netwerk blijft, dus op dezelfde wifi blijft. Dus dan heeft die wel toegang tot alle gegevens.

X: Maakt het daarbij nog uit of je je computer in slaapstand zet bijvoorbeeld?

Y: Nee, want dat ene wachtwoord gebruik je voor alles. Dat is single sign-on.

X: Dan blijft je VPN verbonden.

Y: Ja. Als je met de VPN verbonden blijft, ja, dan heeft die toegang tot alle [the professional services firm] gegevens. [0:22:37 till 0:22:41 has been omitted]. Zeker als de VPN verbonden is.

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

Y: Eh, bij mij persoonlijk of bij iemand van [the professional services firm]?

X: Bij iemand van [the professional services firm].

Y: Ik denk dat het afhangt van hoeveel gevoelige gegevens je op je laptop hebt, maar dan zou het eh, best wel een financiële en reputatieschade kunnen brengen. Als iemand met heel veel, ja, we werken met heel veel gevoelige gegevens van klanten, [0:23:20 till 0:23:30 has been omitted], ja, dan, dan zit je echt in de hoogste risicoklasse.

X: Is er naast financiële schade en reputatieschade nog meer schade?

Y: Eh, ik denk dat eh, qua informatie, die twee wel het belangrijkste zijn.

X: En dan over de VPN-verbinding zelf, hoe veilig is een VPN-verbinding?

Y: Eh, ja, als je er goed mee omgaat dan denk ik wel dat het veilig genoeg is. Want eh, je hebt zeg maar de code die je moet invoeren en je [access token provider] token, dus het is een persoonlijke code en de [access token provider] token en dan pas kom je erbij. Dus ik vind het wel veilig genoeg. Het is ook een manier van two-factor authentication, want je hebt zowel eh, je persoonlijke code op je laptop en dan op je mobiele device een andere code, dus het is niet ook niet op hetzelfde eh, mobiele device dat je beiden hebt. Dus dan zou iemand eh, zo bij je laptop moeten hebben, je mobiele device, wachtwoord van je laptop, wachtwoord van je mobiele device en je persoonlijke code. Dus er is best wel veel die je tegenhoudt om bij de VPN te komen. Om de VPN op te zetten bedoel ik.

X: En de VPN-verbinding zelf, is die ook 100% veilig?

Y: Dat weet ik niet. Dit is het technische deel dat ik dus geen kennis over heb.

X: En je zegt als je er goed mee omgaat dat het dan veilig is, wat bedoel je daarmee?

Y: Nou, het is het voorbeeld dat ik net gaf, als je je VPN eenmaal verbonden hebt dat het de hele dag verbonden blijft, zolang je op dezelfde wifi blijft. Dus, ik vind dat je daarmee wel voorzichtig mee moet omgaan, vooral als je bij, ja, buiten kantoor zit. Eigenlijk ook op kantoor gewoon, zorgen dat je altijd je laptop locked en eh, dat mensen niet zomaar bij je gegevens kunnen komen. Dus je moet je wel voorstellen eenmaal staat die VPN aan dan kan iedereen die toegang heeft tot je laptop bij alle [the professional services firm] gegevens komen waar jij ook toegang toe hebt.

X: Maakt het dan nog uit of je zelf op [the professional services firm] kantoor bent?

Y: Kijk, [the professional services firm] kantoor is een vertrouwde omgeving, maar eh, het, we ontvangen ook klanten, we ontvangen ook bezoekers, dus je weet nooit wie daar rondloopt. Ik vind eerlijk gezegd thuis veiliger, omdat ik thuis hier alleen zit. [0:26:13 till 0:26:16 has been omitted]. Maar thuis is sowieso veiliger dan op kantoor. Bijvoorbeeld ik durf thuis gewoon naar de wc te gaan zonder mijn laptop eh, te locken, maar op kantoor zou ik dat nooit doen. En niet omdat ik mijn collega's niet vertrouw, maar omdat je nooit weet wie langs kan lopen.

X: Wat is de rol van een VPN-verbinding hierin?

Y: Eh, de rol van VPN hierin is dat eh, eenmaal krijgt iemand toegang tot je laptop dat die dan ook gelijk, als je VPN aanstaat, bij alle [the professional services firm] gegevens kan waar jij ook bij kan. Dan is de beveiliging dan niet meer wat het hoort te zijn. Dan heb je liever dat de VPN uitstaat op dat moment.

X: Dat geldt zowel thuis als op kantoor?

Y: Ja.

X: En veranderen jouw handelingen hierdoor?

Y: Hoe bedoel je?

X: Jouw handelingen, want je omschrijft mogelijke aanvallen, hoe je daar zelf rekening mee houdt, zijn er nog meer handeling die jij uitvoert om een aanval te voorkomen?

Y: Ja, zeker. Als ik bijvoorbeeld [0:27:39 till 0:27:50 has been omitted], eh, thuis eh, gaat mijn laptop ook altijd uit als ik hem niet gebruik. Dus, ja, en sowieso, [0:27:59 till 0:27:59 has been omitted], is het ook eh, een kwestie van als je laptop niet met slot achtergelaten kan worden, neem het gewoon mee met lunch.

X: Wat voor slot bedoel je?

Y: Wat zeg je?

X: Wat voor slot bedoel je?

Y: Eh, [0:28:27 till 0:28:29 has been omitted] en je gebruikt dezelfde kamer de hele dag, dan eh, als je gaat lunchen de kamer openblijft, ja, dan gaat mijn laptop mee. Maar als de kamer, eh, de deur op slot gaat, dan kan ik mijn laptop daar achterlaten, maar dan staat die wel uit.

X: Zijn er nog meer dingen die belangrijk zijn om te vertellen over een VPN-verbinding?

Y: Eh, voor mijn kennis niet nee. Ik zou graag meer willen weten over VPN hoe het technisch werkt, maar gezien dat niet mijn expertisegebied is of waar ik eh, technisch heel veel over hoef te weten dan eh, heb ik nooit iets eh, achter eh, verder over, heb ik nooit meer eh, achter eh, verder over gezocht. Wat ik moet weten erover vind ik eh, nu genoeg, maar het is altijd interessant om meer te weten.

X: Oké, eh, heb jij zelf nog vragen verder?

Y: Ja, ik vraag eh, ja, ik ben benieuwd, tenminste als je het kan beantwoorden, waarom dit eh, waarom VPN gekozen is als onderwerp.

X: Oké, ik zal eerst de opname uitschakelen.