# Transcription non-expert 6

Duration: 35 minutes

X: Kunt u aan mij uitleggen wat een VPN is?

Y: Eh, dat hoop ik. Eh, voor zo ver ik weet is het een Virtual Private Network en wordt het gebruik om te zorgen dat je eh, binnen een netwerk eh, op in ieder geval op een veilige manier berichten kunt versturen door danwel versleuteling meestal toe te passen of eh, en in ieder geval de berichten eh, los van het onderliggende netwerk te kunnen versturen.

X: En wat bedoelt u met los van het onderliggende netwerk?

Y: Nou dat eh, het eh, de bedoeling is dat op het moment dat iemand een bericht verstuurd vanuit eh, [the professional services firm] bijvoorbeeld eh, over het internet. Dat eh, anderen op het internet de berichten eh, niet kunnen onderscheppen.

X: En waardoor kunnen zij die berichten niet onderscheppen?

Y: Eh, ja, dat is een goede vraag, want dat is heel technisch volgens mij. Eh, volgens mij komt dat omdat je de berichten eh, via bepaalde lijnen laat lopen waar eh, anderen niet eh, bij kunnen komen. Dus afgesloten.

X: Ja. Oké. Eh, om welke redenen gebruik jij een VPN?

Y: Eh, ik gebruik VPN omdat ik daarmee veronderstel dat eh, mijn berichten niet eh, of in ieder geval niet heel eenvoudig door eh, door derde partijen kunnen worden eh, onderschept en gelezen. Als ik gebruik maak van VPN eh, over een VPN over internet, ik weet dat VPN ook in een aantal gevallen gebruikt wordt binnen bedrijven, om in interne netwerken om meer beveiliging te krijgen. Maar ik gebruik het met name omdat ik ervan uitga dat de VPN die wij gebruiken ook de berichten versleuteld, dus als iemand al berichten zou kunnen onderscheppen, dan eh, dan zou die ze in ieder geval niet kunnen lezen, omdat die geen sleutel heeft om ze te ontsleutelen.

X: Ja, oké. En wat bedoelt u met eh, met het gebruik van VPN in interne netwerken?

Y: Nou ja, je kunt VPN natuurlijk ook binnen je eigen eh, organisatie gebruiken eh, zodat je dus eh, op het eigen netwerk, het lokale netwerk, eigenlijk op dezelfde manier berichten verstuurd. Waarbij je dus ook beveiliging maakt en ik neem aan dat je dat doet omdat als er iemand toch van buitenaf op jouw interne netwerk zou komen, dat die niet zomaar eh, gegevens kan eh, kan lezen.

X: En zijn er nog andere redenen waarom u een VPN gebruikt?

Y: Nee, dat is voor mij eigenlijk de belangrijkste reden, gewoon extra beveiliging, waardoor je in ieder geval geen risico loopt dat anderen jouw berichten kunnen onderscheppen. Of in ieder geval niet kunnen lezen als ze ze al onderscheppen.

X: Ja. Oké. Dan de volgende vraag. Als een gebruiker, welke handelingen voert u uit om een VPN verbinding te maken?

Y: Eh, dat eh, is in dit moment via een eh, het opstarten van eh, remote access en het gebruik op een mobiele telefoon van eh, van de, de access code. Dus ik log in via eh, op mijn eh, op mijn laptop. Dan moet ik een pincode invoeren en vervolgens een code die iedere minuut wijzigt. En daarmee leg ik de verbinding.

X: Oké. En hoe komt u aan deze code die iedere minuut wijzigt?

Y: Dat is een app op de telefoon. [access token provider] heet die geloof ik. En dat is een, een app die door eh, [the professional services firm] is verstrekt. Ter vervanging van voorheen eh, want hiervoor hadden we natuurlijk de mooie key waar die code op het schermpje kwam, dat ding dat je aan je sleutelbos bij je had. En dit is de digitale variant.

X: Oké. En op welke apparaten gebruikt u een [the professional services firm] VPN?

Y: Eh, ik gebruik hem alleen op de laptop van [the professional services firm]. [0:06:47 till 0:06:58 has been omitted].

X: Oké. En kunt u aan mij uitleggen hoe een VPN verbinding werkt? U kunt hiervoor het whiteboard gebruiken-

Y: Hmhm.

X: Ik zal mijn tekeningen weghalen.

Y: Ja. Eh, hoe die werkt. Hoe ik hem opstart en hoe dan vervolgens mijn berichten gaan volgens mij, of-

X: Ja.

Y: [start drawing 17\_1].Oké. Ik heb dus mijn eh, mijn laptop. Dit moet mijn laptop voorstellen. Eh, die maakt verbinding met de VPN van [the professional services firm], even kijken hoor, kon ik tekst erin zetten makkelijk, o, die moet ik niet hebben. Even kijken hoor, kon ik de tekst selecteren.

X: Door op de pen te klikken en dan op een T te klikken-

Y: O, ja, ik heb hem.

X: En dan ook een vierkant te tekenen en daarin kunt u typen.

Y: O, oké. En- Even kijken hoor, dan moet ik weer tekenen. [start drawing 17\_2].En de VPN gaat dan terug en die vraagt dan een, ja, mijn mobiele telefoon, nou dit moet mijn mobiel voorstellen.

X: Ja.

Y: Eh, die vraagt dan de code op, en die code eh, die tik ik hier in en dat is de code die dus iedere minuut wijzigt en die geeft dan, laat ik even een ander kleurtje kiezen, en die geeft dan die code op. Dan is de VPN eh, verbinding wordt geopend. Even lastig om even snel te tekenen met dat ding. [start drawing 17\_3]. En dan eh, dan wordt zeg maar de VPN verbinding open gezet. Eh, ik heb aan mijn kant een sleutel. Volgens mij heet dat de private key als ik het goed heb. Nou, het vakje moet wat groter, maar- De private key, dus het bericht wordt dan hier ingezet en dan wordt die versleuteld en dan wordt die eigenlijk de VPN verbinding ingezet. En aan de andere kant heb ik dan hier ergens de ontvanger, wie dat dan ook is. Iemand die ook op het [the professional services firm] netwerk zit. En die krijgt dan eh, die heeft ook de, uiteraard, een key. Met het bericht gaat dan de public key mee als ik het goed heb. En dan kan degene die aan de andere kant zit, die krijgt dan het berichtje binnen, of in ieder geval eh- [start drawing 17\_4]. Volgens mij wordt het zelfs opgeknipt in verschillende pakketten. En die kan dan die pakketten via die, door die keys aan elkaar te koppelen, weer ontsleutelen. En lezen.

X: Ja.

Y: Ik kan hem geloof ik niet aanpassen, of wel. Nou, je begrijpt wat ik bedoel.

X: Ja, zeker.

Y: En die VPN verbinding die zorgt er in ieder geval voor volgens mij ook dat die pakketten worden gecreëerd en dat de pakketten weer ergens op, weer bij elkaar worden gevoegd.

X: Oké.

Y: Zo is ongeveer hoe ik het begrijp.

X: Ja. Oké. Een vraag hierover-

Y: Hmhm.

X: Voor de duidelijkheid. Is het eh, de bedoeling dat dit apart staat?

Y: Nou, dit is eigenlijk de tool, het tooltje dat ik opstart.

X: Oké.

Y: [start drawing 17\_5]. Het tooltje wat opgestart wordt om deze verbinding te openen en die verbinding maakt dan gebruik, ja, misschien moet ik, is het handig om nog even een pijltje inderdaad erbij te zetten. Dus eigenlijk zorgt deze ervoor eh, zal ik het er even bij zetten in tekst, zo.

X: Ja, ik kan het nog lezen.

Y: Ja. Dus die zorgt voor het openen van de verbinding en op het moment dat ik dan ga versturen, zorgt die verbinding ervoor dat die pakketten worden verstuurd en versleuteld zijn en aan de andere kant weer ontsleuteld kunnen worden.

X: Ja. En u zei dat de [the professional services firm] ontvanger iemand is die ook op het [the professional services firm] netwerk zit-

Y: Hmhm. Ja.

X: Wat betekent dit?

Y: Dat dat iemand is die dus eh, maar dat weet ik dus niet zeker, maar daar ga ik eigenlijk vanuit, dat die ook de VPN eh, verbinding heeft met [the professional services firm], maar dat hoeft trouwens, nee, dat is trouwens niet waar wat ik nu zeg, want volgens mij kan iemand gewoon de berichten lezen, ook al is die niet via VPN ingelogd. Maar dat weet ik niet zeker.

X: Ja. En hoe zou het werken als iemand die niet is ingelogd op de VPN wel de berichten kan lezen?

Y: Dan zou het volgens mij niet goed werken. Dus ik, ik denk dat als deze berichten via VPN verzonden worden, dat dat dan wel, want de [the professional services firm] ontvanger kan ook een systeem zijn he, in dit geval. Eh, want ik gebruik VPN bijvoorbeeld om verbinding te maken met Citrix en ik kan niet in Citrix als ik geen VPN verbinding heb. Dus de [the professional services firm] ontvanger, zit blijkbaar op het VPN netwerk, want anders kan die ook niet zeggen dat ik eh, dat die geen verbinding kan maken.

X: Ja. En zijn er nog meer voorbeelden waarbij de [the professional services firm] ontvanger een systeem is?

Y: Eh, ja, er zijn meer eh, meer systemen eh, ja, er zijn heel veel systemen die alleen maar via VPN benaderbaar zijn, bijvoorbeeld [an internal page] omgeving, waar je [0:15:44 till 0:15:48 has been omitted], kun je alleen maar via VPN benaderen.

X: Ja. En een [the professional services firm] ontvanger, kan dat ook een persoon zijn?

Y: Ja, dus dat zou ook een persoon kunnen zijn, alleen dat, dat is even voor mij een beetje onduidelijk nu, omdat ze heel veel dingen voorheen achter de VPN hadden staan en eh, bijvoorbeeld mail kon je alleen maar benaderen als je op het eigen netwerk zat of via een VPN was ingelogd, alleen dat hebben ze eh, ertussenuit gehaald vanwege de corona ellende. Waardoor blijkbaar de eh, de bandbreedtes enorm werden belast, dus ik weet dat dat in het begin, dat daar bepaalde dingen bij VPN weggehaald zijn, [conferencing software] is ook zo een voorbeeld.

X: Ja.

Y: Dus die zitten niet in het VPN netwerk, dus daar kan, zou in theorie dus iedereen gewoon mee kunnen kijken.

X: Ja. Oké. En eh, stel we wisselen van locatie, we gaan met de eigen laptop bijvoorbeeld in een café zitten-

Y: Hmhm.

X: Verandert dat iets aan deze tekening?

Y: Nee, in principe niet, want de VPN verbinding eh, die leg ik via het internet. Dus in deze maakt het natuurlijk niet uit of dat het internet is bij mij hier of eh, op een wifi eh, ergens bij een café. Ik zal alleen wel weer een VPN verbinding op moeten zetten om te zorgen dat ik in ieder geval eh, veilig ben. Het enige wat ik me kan voorstellen, maar ik weet dus niet waar de VPN ergens start, is dat er iemand tussen jou eh, ergens jouw wifi kan eh, kan omzeilen of kan afluisteren.

X: Ja.

Y: Maar dat weet ik niet of dat kan.

X: Oké. En dan ga ik door naar een volgende vraag.

Y: Hmhm.

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

Y: Eh, ja, wat, wat versta je onder computerbeveiliging?

X: In de brede zin.

Y: Oké. Mijn computer op zich wordt niet beveiligd door VPN. Dus als ik mijn computer eh, aanzet en ik doe niets met, en ik zet VPN aan, dan kan iedereen nog steeds op mijn computer als die wil. Dus in die zin is het beveiliging alleen maar als ik eh, berichten ga versturen, dus mijn computer zelf wordt niet beveiligd door VPN. Dus als iemand hier binnenstapt en die zou mijn wachtwoord kunnen eh, ontcijferen of eh, iets, dan kan die nog steeds op mijn computer, dus daar heeft de VPN geen enkele waarde voor. VPN is alleen maar voor het berichtenverkeer. Dus die beveiliging is er wel, maar niet voor de computer op zich.

X: Oké. Dan de volgende vraag. Het is een brede vraag-

Y: Hmhm.

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

Y: Eh, heel veel denk ik. Eh, een is je eh, spam. En eh, phishing. Ook binnen [the professional services firm] zie je dat eh, het komt niet heel vaak voor, maar een hele enkele keer zie je toch nog wel eens een mail binnenkomen die eh, die phishing bevat. Eh, daarnaast heb je natuurlijk altijd het risico dat iemand eh, je password kan achterhalen. Als je een niet zo heel sterk password gebruikt, dan loop je het risico dat iemand jouw computer in kan en dus heb je altijd het gevaar dat ze op jouw computer kunnen en dan vervolgens al jouw bestanden kunnen benaderen. Dus als er zaken zijn waar je niet via VPN bij zou kunnen, volgens mij zijn die er niet als ik mijn bestanden op netwerken van [the professional services firm] zet. Maar als dat al zou kunnen, dan zou iemand daar dus gewoon bij kunnen. Nou ja, op je telefoon de bekende eh, whatsapp fraude en eh, hackers die proberen jou eh, software eh, naar binnen te schuiven om jouw computer over te nemen, of om je telefoon te hacken of- Nou ja, daarnaast eh, bankverkeer, waar je altijd risico's loopt. Eh, ja, je telefoon is natuurlijk eh, het uitlezen van je eh, wat is het, je RFI ofzo he, is dat RFI, het chipje, waarmee je je betaling kan doen en dergelijke.

X: Oké.

Y: Ja, dat zijn denk ik wel een beetje raken(0:21:03).

X: Ja. En als we nadenken over deze dreigingen-

Y: Hmhm.

X: Heeft een VPN verbinding hier invloed op?

Y: Eh, deels. Want eh, op het moment dat ik natuurlijk een VPN verbinding opzet en eh, ik heb software op mijn computer staan die eh, malware die eh, uiteindelijk alles kan meelezen of al mijn toets combinaties eh, kan opnemen, ja, dan heeft een VPN natuurlijk maar beperkt effect. Want mensen kunnen dan dus gewoon lezen wat ik doe. Kunnen waarschijnlijk niet alle berichten ontsleutelen en dat soort dingen, maar ze kunnen wel zien als ik aan het typen ben bijvoorbeeld. Dus het VPN is niet een, niet absolute veiligheid, als die er al zou zijn.

X: Ja. Heeft een VPN op nog meer manieren invloed op deze dreigingen?

Y: Eh, nou, in ieder geval is het een extra laag. Dus het is een stuk toegevoegde beveiliging.

X: Ja. Oké. En dan waren dit digitale dreigingen-

Y: Hmhm.

X: Heb jij daarnaast op een normale dag ook te maken met sociale dreigingen?

Y: Nou, nee, ja, wat, wat versta je onder sociale dreigingen? Social media berichten die eh, bijvoorbeeld verkeerd eh, kunnen uitpakken als je ze opent of iets dergelijks. Bedoel je zoiets of?

X: Ja, ik bedoel alle dreigingen die eh, niet digitaal zijn en waar jij mee te maken hebt als werkende voor [the professional services firm].

Y: Nou, ik zou, buiten het feit dat mensen je misschien een bericht sturen dat, waar een gevaar in zou kunnen zitten, niet echt eigenlijk nee.

X: Oké. En heeft een VPN verbinding op eh, ja, dat soort berichten?

Y: Nee, dat denk ik niet nee. Daar voegt VPN niet veel aan toe.

X: En als we dan kijken naar deze digitale dreiging en de sociale dreiging-

Y: Hmhm.

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

Y: Waarvan ik denk dat dat degene is die dat zou veroorzaken?

X: Ja.

Y: Ja, ik denk dat degene die die dreiging veroorzaken dat dat eh, hackers zijn die uiteindelijk op eh, op data of op financiële gegevens eh, dat die daarnaar op jacht zijn. Voorbeeldje waar wij werken met [0:24:00 till 0:24:42 has been omitted]. En dat gebeurt in de praktijk.

X: Ja, en wie zouden deze hackers zijn?

Y: Ja, als we dat wisten was het makkelijk he. Ik eh, dit zullen mensen zijn die eh, uiteindelijk een criminele achtergrond hebben over het algemeen, zeker degene die op financiële gegevens uit zijn. Eh, omdat die gewoon puur geld ermee willen verdienen. Mensen die echt op, op data van [the professional services firm] uit zijn, ja, het zou eh, bijvoorbeeld een concurrent kunnen zijn.

X: Oké. En is er naast het verkrijgen van financiële gegevens nog meer mogelijke motivaties?

Y: Nou ja, wat ik zeg, de data over bijvoorbeeld klantenbestanden. Prijzen die wij afspreken met leveranciers zou interessante informatie kunnen zijn voor anderen. Ja, personeelsgegevens, persoonsgegevens, het liefst natuurlijk voorzien van eh, van, van gegevens als adressen en hoe heet het, BSN ofzo. Ik kan me voorstellen dat dat data is waar mensen naar eh, naar opzoek zijn.

X: Oké. En wat voor achtergrond heeft een aanvaller?

Y: Ja, dat kan heel divers zijn. Dat kunnen jongens zijn van twaalf, dertien jaar, die het spannend vinden om proberen te hacken ergens. Tot aan eh, criminelen die gewoon op geld uit zijn en proberen je computer of het netwerk plat te leggen en daarvoor ransomware eh, te installeren en uiteindelijk losgeld vragen. Dus ik denk dat hackers in allerlei geledingen voorkomen.

X: Ja. Oké. En wat zou de impact van een aanval kunnen zijn?

Y: Eh, afhankelijk van het type aanval kan dat lopen van nou ja, goed, een vervelend dingetje dat je misschien software hebt die rare dingen op je computer doen, maar niet schadelijk zijn. Tot aan het volledig platleggen van je netwerk en daardoor loop je natuurlijk financiële schade, dat is een. Maar veel belangrijker denk ik zeker voor [the professional services firm] is natuurlijk reputatieschade. Als jij als [the professional services firm] door hackers platgelegd wordt, dat geeft niet echt een professionele indruk. Dus ik denk dat die schade nog vele malen groter zou zijn.

X: Oké. En als we an gaan kijken naar de VPN verbinding zelf-

Y: Hmhm.

X: Hoe veilig is een VPN verbinding?

Y: Ja, eh, durf ik niet te zeggen. Dat zal afhankelijk zijn van, van wat voor soort VPN verbinding, want ik heb ooit begrepen dat je ook een VPN verbinding kunt leggen maar zonder versleuteling. Ja, dan is dat eh, denk ik minder veilig dan eh, dan op het moment dat je ook nog aanvullend daarop bepaalde versleutelingen toepast en dan ligt het er ook nog aan wat voor versleuteling. Hoe geavanceerder je versleuteling, hoe groter eigenlijk de veiligheid is.

X: Ja. En zijn eh- Worden VPN verbindingen zonder versleuteling voor andere doeleinden gebruikt dan een VPN met versleuteling?

Y: Eh, dat, dat denk ik wel dan ja. Als je al zou kiezen voor het niet versleutelen, dan is dat waarschijnlijk omdat je alleen wilt voorkomen dat, dat niet willekeurig iedereen kan eh, je berichten kan onderscheppen. Alleen ja, op het moment dat iemand toch toegang krijgt en op de een of andere manier de berichten weet te onderscheppen, dan kan die ze dus wel gewoon lezen. Nou, kan me voorstellen dat je dat doet met minder gevoelige data, bijvoorbeeld niet-financiële data of eh, of iets dergelijks. Kijk, op het moment dat ik een mail naar een collega stuur, nou zit dat niet achter VPN, maar stel dat ik dat in VPN zet, dat ja, dat is wat minder spannend dan dat ik [0:29:12 till 0:29:25 has been omitted].

X: Ja. Oké. En als je nadenkt over deze mogelijk verschillende vormen en mogelijk verschillende niveaus in veiligheid dan ook-

Y: Hmhm.

X: Veranderen jouw handelingen hierdoor?

Y: Eh, ja, zeker. Op het moment dat ik weet dat een VPN niet gebruik maakt van versleuteling, dan ben ik me in ieder geval bewust van het feit dat ik daar dus geen hele gevoelige data overheen moet sturen. Omdat dat risico daarvan dus groter is, als iemand dat al kan onderscheppen, dat ook de data dus bekend is. Dus nog wel, ja, weer even als voorbeeld het mailtje naar een collega met een vraag ja, is dan wat minder eh, spannend dan eh, [0:30:18 till 0:30:23 has been omitted]. Wat je niet versleuteld zou versturen.

X: Oké. En weet jij of de [the professional services firm] VPN versleuteling gebruikt?

Y: Volgens mij wel. Ik ga daar overigens ook wel een beetje vanuit dat dat gebeurt. Ik heb het nooit opgezocht, maar ik ga ervan uit dat dat versleuteld is.

X: Oké. En zijn er nog andere manieren waarop jouw handelingen veranderen?

Y: Nou niet zo zeer door VPN, ik denk meer door een algemeen besef dat als je gebruikmaakt van internet, dat je altijd risico's loopt. Dus dat betekent dat je op je laptop eh, op je [the professional services firm] laptop geen pagina’s moet gaan openen waar eh, of zaken moet gaan downloaden waarvan je niet weet wat eh, wat de oorsprong is. Gratis programmatjes en dergelijke of eh, bepaalde websites gaan bezoeken waar je risico's loopt. Dat zijn dingen die je denk ik in zijn algemeen moet doen, los van of je nou wel of niet een VPN gebruikt.

X: Ja, zeker. Oké. Dit waren tot zo ver mijn vragen-

Y: Oké.

X: Zijn er nu nog dingen waarvan jij denkt dit is belangrijk om te vertellen over een VPN, maar is niet ter sprake gekomen?

Y: Nou, de vraag die je stelde van of [the professional services firm] gebruik maakt van versleutelde VPN, het feit dat ik het eigenlijk niet weet, geeft dus aan dat dat blijkbaar niet, eh, en ik denk dat meer mensen dat niet weten. En dat mensen misschien ook niet altijd de risico's eh, overzien, die gebeuren. Kijk het hacken van een website of de DDoS aanvallen en dergelijke, je hoort daar natuurlijk nooit, nooit heel veel over en dat hoeft ook niet. Maar, maar mensen weten niet of dit gebeurt. [0:32:38 till 0:33:06 has been omitted]. En ik vraag me dus ook af of binnen [the professional services firm] daar voldoende aandacht aan wordt besteed, behalve dat mensen natuurlijk wel altijd weer zo een berichtje krijgen van nou doe dit niet, doe dat niet, maar je krijgt zo verschrikkelijk veel e-mails, dat mensen lezen dat gewoon niet meer. En het risico wordt gewoon iedere dag groter, want ook de hackers stil natuurlijk.

X: Nee zeker niet.

Y: En ook niet alleen de digitale, maar ook de wat je zei, ja, noem het sociale dreiging, de bekende e-mailtjes met eh, [0:33:49 till 0:33:56 has been omitted]. Of een LinkedIn berichtje van iemand eh, bunnen je netwerk, maar blijkt dat het geen LinkedIn is, maar een nagemaakte site, waardoor er binnen no-time allerlei vervelende software op het netwerk staat, ja, dat, dat zijn wel risico's waar volgens mij niet heel veel aandacht aan besteed wordt. Althans niet zichtbaar, laat ik het zo zeggen.

X: Ja. Oké. En zijn er daarnaast-

Y: En meer eigenlijk niet.

X: Oké. Prima, dan tot zo ver het interview gedeelte. Ik wil je heel erg bedanken voor je deelname, wat dit helpt mij heel erg. En heb jij nog vragen voor mij?

Y: Nou, ik ben even benieuwd wat, wat ga je hier precies mee doen, wat is uiteindelijk je doel van je opdracht.

X: Ja, dat snap ik, ik zal de opname even stoppen.