# Transcription non-expert 5

Duration: 36 minutes

X: Wat is een VPN?

Y: Nou, VPN, dat is de connectie waarmee onze computer eh, jeetje, hoe moet ik dat, dan moet ik even, even uitleggen natuurlijk. De eh, de veiligheids eh, eh, connectie zeg maar, tussen, tussen mijn laptop en het [the professional services firm] netwerk. Eh, he, dus een soort schild he.

X: Oké. En wat bedoelt u met een schild?

Y: Nou ja, een soort, een soort eh, eh, veiligheids eh, ja, hoe noem je dat. Eh, veiligheidssysteem voor [the professional services firm]. He, dat we eh, veilig onze data heen en weer kunnen sturen. He, dat je daardoor op een veilige wijze kan inloggen eh, op, op alle systemen eh, van het [the professional services firm] netwerk. Nou, op het moment dat je geen connectie maakt met VPN, dan eh, dan, dan kom je niet verder.

X: Ja. En hoe bedoelt u dat u niet verder komt?

Y: Eh, nou ja, goed, dat is er veel data, de [the professional services firm] data, die is op dat moment niet eh, niet bereikbaar, niet beschikbaar.

X: Oké. En u zegt veilig data heen en weer sturen, op wat voor manier bedoelt u veilig?

Y: Eh, nou veilig in de zin van he, je bent op afstand verbonden met elkaar, eh, en eh, we willen niet dat data die [the professional services firm] heeft dat die bij derden terecht komt. Daarvoor eh, moeten wij in een veilige omgeving werken, dus waar, waar derden eh, geen toegang tot hebben. Daarvoor wordt, wordt VPN gebruikt.

X: Oké. En weet u hoe derden geen toegang kunnen hebben tot de verbinding? Tot de data?

Y: Eh, nou ja, het meest logische wat ik daarin kan bedenken is wij moeten een bepaalde code invoeren eh, en anderen hebben die code niet.

X: Ja. Oké. En waarom gebruikt u VPN?

Y: Eh, om in te kunnen eh, om, om bij de data eh, te komen waar wij toegang toe moeten hebben. Die ik nodig heb om mijn werk te kunnen doen.

X: Ja. Zijn er nog andere redenen waarom u een VPN gebruikt?

Y: Nee, voor mij niet. Eh-

X: Oké.

Y: Ik weet niet of die er zijn, maar-

X: Ja.

Y: Kennelijk wel, als je zo de vraagt stelt.

X: Niet per se hoor-

Y: Een aantal van mijn systemen die draaien enkel als ik ingelogd ben op het netwerk. Eh, dus he, onder andere via de Citrix omgeving, op het moment dat wij geen connectie hebben, dan eh, dan kan ik, dan kunnen wij ons werk niet uitvoeren. Daarnaast onze shared drive, die eh, die heeft ook eh, he, daar kom je ook niet op zonder VPN, zonder het netwerk.

X: Ja, oké. En als gebruiker, welke handelingen voer jij uit om een VPN verbinding te maken?

Y: Eh, nou, ik eh, ja, dat moet je natuurlijk heel gedetailleerd weten gok ik.

X: Ja, wat u kunt vertellen.

Y: Haha. Nou ja, rechtsonder klik eh, klik ik op zo een mooi icoontje en dan geef ik aan eh, mijn wifi icoontje zeg maar, en dan geef ik aan dat ik met [the VPN of the professional services firm] wil verbinden eh, he, dan open ik mijn eh, [access token provider] token, mijn [access token provider] [the professional services firm] software token, eh, nou dan vul ik mijn code in, ik zeg connect en vervolgens gaat het helemaal goed komen.

X: Oké. En u zegt uw software token, zijn hiervoor nog andere mogelijkheden?

Y: Ja, je hebt ook een hardware token. Eh, de ervaring leert dat dat eh, een mindere connectie geeft. En een deel van mijn team heeft daarmee te maken. En die hebben daardoor eh, veel, veel connectie issues.

X: Wat bedoelt u daarmee, dat het een mindere connectie geeft?

Y: Eh, dan wordt die, dan wordt die met enige regelmaat uitgelogd.

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

Y: Eh, enkel op mijn laptop. Op mijn telefoon eh, daar heb ik, daar raadpleeg ik enkel met name mijn mail. Eh, en dan, en [conferencing software] eh, he, de [conferencing software] omgeving en dan heb je geen [the VPN of the professional services firm] nodig.

X: Oké. En kunt u aan mij uitleggen hoe een VPN verbinding werkt? Als u wilt kunt u hiervoor het whiteboard gebruiken. Ik zal mijn tekeningen weghalen.

Y: Nou, dat vind ik een hele leuke vraag. Even kijken hoor. Dus dan moet ik hier een tekeningetje gaan maken, oe. [start drawing 16\_1]. Eh, even kijken. Nou, dan hebben we, nou ja, allemaal verschillende gebruikers. He, ik teken er even een paar. Eh, en we hebben hier, hebben we zeg maar de router eh, van eh, [the professional services firm]. Ik had het wel dichterbij mogen tekenen. Eh, he, dus dan heb je eh, tweerichtingsverkeer. Hebben ze eh, nou ja, ik log in op, op, eh, op mijn laptop en dan gaat die heen en weer zenden. Eh, he, dus dit is de [the professional services firm] router, tja, schitterend mooi getekend. Eh, nou ja, goed, en op het moment dat ik de code heb ingevoerd eh, dan, dan heb ik uiteindelijk connectie. En tot dat moment heb ik geen connectie. [start drawing 16\_2]. Dus er zit hier zeg maar een soort eh, een soort schild voor. Dat is eh-

X: Ja.

Y: Even heel plat gezegd zo, zo kijk ik ernaar.

X: Ja, prima. En waar in deze tekening zouden wij de [the professional services firm] omgeving vinden, de interne applicaties waar u bij moet komen?

Y: [start drawing 16\_3]. Eh, hier. Dus hier, ja, jeetje. Eigenlijk zou ik hem dan overnieuw moeten tekenen. [start drawing 16\_4]. Maar hier heb je een soort eh, he, dit is dan je, je VPN. He, dat is een soort schild, noem ik het maar even. En hier heb je eh, alle data van [the professional services firm]. Eh, is natuurlijk een hele grote server. Volgens mij staat die in [country]. Eh, in ieder geval voor Nederland. En eh, op het moment dat je he, je logt in op VPN eh, en vervolgens he, op het moment dat het oké is, dan mag je door. En kan je bij de data.

X: En u noemt een server, wat is een server?

Y: Eh, ja, dat is een eh, ik ben zo IT onderlegd he, not. Eh, eh, ik zou dat omschrijven als een eh, een IT systeem waar eh, waar alle data opgeslagen wordt. Eh, en die gekoppeld kunnen worden met andere servers eh, waardoor je onderling data kan uitwisselen.

X: Ja. En waar ik deze tekening vinden we een server?

Y: Eh, ja, voor mij zit dat allemaal hierin. Maar misschien eh, zouden we dat wat groter moeten tekenen.

X: Ja, duidelijk. En wat is het verschil tussen een router en een server?

Y: Eh, een router, ja, voor mij zou dat zijn, een router is eh, datgeen waarmee je een connectie maakt tot het internet. He, dus dat staat bij mij hier thuis. Eh, en een server is he, dat is wat ik net zei, de, de eh, dat systeem he, waar eh, waar de gegevens van [the professional services firm] worden opgeslagen.

X: Ja. En dit is ook de router van [the professional services firm] zei u toch?

Y: Nee, dat heb ik nog niet gezegd. Maar eh, ik zou wel zeggen dat dat zo zou zijn. [start drawing 16\_5]. Dat dat hier, ja, weet je, ik denk dat je onderaan de streep zal er eh, he, dan heb je hier bij wijze van een serverpark eh, he, dus daar zit de connectie met eh, even kijken, dan heb je hier, nou ja, verschillende serverparken, ongetwijfeld. He, dus eh, zo zit het allemaal een beetje met elkaar verbonden.

X: En eh, als dit niet een router is, wat is dat dan?

Y: Eh, moeilijke vragen joh, voor mij als en IT-leek. Nou ja, dat zou prima, ik, ik zou zeggen van nou ja, goed, hier thuis heb ik een router. He, dus daarmee maak ik verbinding met het internet. Nou, in principe, [the professional services firm] maakt ook verbinding met het internet, dus dan zou er prima een router kunnen zijn. Eh, nou ja, goed, daarvoor zit die, zit die, database, of sorry, de VPN connectie, nou goed eh, er wordt hier onderling allerlei data wordt er uitgewisseld. Eh, dus dan zou dat prima ook een router kunnen zijn, ja.

X: Oké. En u tekent verschillende serverparken zei u, waarom tekent u verschillende serverparken?

Y: Eh, risico mitigerend.

X: Op wat voor manier mitigeren zij risico's?

Y: Eh, door elkaars back-up te zijn.

X: Hebben die serverparken nog een andere functie?

Y: Ongetwijfeld. Eh, weet je, de, de systemen draaien daarop, je zal er een, een stukje data storage hebben he, waar alle gegevens eh, en, en, van [the professional services firm] staat opgeslagen. Eh, nou, ik weet voor een van de systemen die wij gebruiken he, daar eh, daar hebben we ook een server en een back-up server. He, dus, nou ja, die lopen synchroon met elkaar, gaat het mis met de een he, dan hebben we de ander nog om eh, om daar eh, vanuit te kunnen werken. Eh, dus onderaan de streep eh, voorkomen we daarmee dat we data, gegevens kwijt kunnen raken. En eh, heb je dat wel nodig.

X: Oké. En stel we gaan nu naar een andere locatie eh, stel je bent bijvoorbeeld in een café, verandert er dan iets aan deze tekening?

Y: Eh, wauw, eh, nou, misschien wel, maar hetgeen wat, kijk, in een café, als je in een café inlogt, eh, he, formeel gezien he, moet je goed checken of dat je eh, of dat je een veilige verbinding hebt. [start drawing 16\_5]. Eh, nou zit ik even te twijfelen he, stel je voor he, dan, dat dit eh, je laptop is he, dus dan eh, dan is dit de vraag van normaal gezien is dit de router thuis. Eh, en op het moment dat dat in ene keer de café eh, router gaat worden, geeft dat dan een veiligheidsissue. Als het goed is niet. Eh, want je hebt nog steeds die VPN connectie eh, waardoor je eh, waardoor je veilig kan eh, kan internetten. Anders zou je bijvoorbeeld ook niet op een Schiphol of waar dan ook eh, connectie kunnen maken.

X: Ja. En je zegt dat je moet controleren of het een veilige verbinding is, wat bedoel je daarmee?

Y: Nou, ja, heb ik altijd gehoord. Goed eh, nou, kijk, als ik kijk bij mijn thuissituatie dan eh, dan wordt er eh, dan heb ik meerdere, ten minste, heb ik maar een persoon die daar op inlogt zeg maar, eh, he, die wachtwoord heeft tot de betreffende router. Eh, bij een café verbinding of nou, Schiphol, whatever, eh, dan heb je eh, meer mensen die op eh, op hetzelfde netwerk inloggen. Eh, ik weet niet of dat per definitie of dat, dat eh, eh, veilig is of niet. Ik ga ervan uit dat op het moment dat je je VPN gebruikt, dat dat veilig is.

X: En wat is dan het verschil tussen de situatie dat je geen VPN gebruikt en dat je wel VPN gebruikt?

Y: Nou, op het moment dat ik wel VPN gebruik, dan kan ik bij al mijn eh, mijn systemen en programma’s. Op het moment dat ik dat niet doe, dan kom ik daar niet bij. Dus dan heb ik geen eh, geen toegang tot de beveiligde gegevens van [the professional services firm].

X: Ja, en als je dan denkt op het gebied van de veilige verbinding-

Y: Ja, waar doel je op?

X: Wat is dan het verschil tussen een verbinding met VPN en zonder VPN?

Y: Eh, zonder VPN heb je eh, vermoedelijk niet altijd een veilige verbinding. En met eh, ja, voor de, voor de programma’s eh, en gegevens van [the professional services firm] heb je dat wel. Maar is dat ook maar weer net hoe je er mee omgaat.

X: Ja. Oké. Dan ga ik door naar de volgende vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Wat de invloed is van een VPN op mijn computerbeveiliging. Eh, eigenlijk verschrikkelijk. Op het moment dat ik, dat ik, dat mijn VPN uitvalt he, en, en, nou neem even wat ik eerder al aangaf, een deel van het team werkt met een, een hardware token eh, he, als dat uitvalt, dan heb je geen connectie tot de programmatuur die wij gebruiken. Nou, dat kost tijd en zorgt voor een inefficiënte geheel. He, dus vanuit dat perspectief heeft dat invloed.

X: Ja, oké. En heeft de VPN op een andere manier ook nog invloed op jouw computerbeveiliging?

Y: Eh, niet dat ik weet.

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

Y: Met wat voor digitale dreiging.

X: Ja.

Y: Eh, nou, eigenlijk best nog wel wat, zegt de theorie. Eh, wij hebben de mogelijkheid op eh, eh, [0:19:49 till 0:20:31 has been omitted]. Wij hebben eh, te maken met een stuk databreach he, op het moment dat eh, dat we per ongeluk met de verkeerde partij communiceren. Eh, nou ja goed, en er is altijd een risico he, we hebben eh, pak en beet zo een paar honderd e-mails per dag die er binnen mijn team worden behandeld eh, en er zit altijd een risico, een behoorlijk risico op, dat je, dat je toch een eh, een soort van paard van Troje binnenhaalt.

X: Ja. Oké. En hoe veranderd de soort dreiging door een VPN verbinding?

Y: Eh, niet.

X: Duidelijk. Oké. En dan een andere vraag. Met wat voor sociale dreiging heb jij op een normale dag te maken?

Y: Eh, sociale dreiging. Wat verstaan jullie daar normaal gezien onder?

X: Alle dreigingen die niet digitaal zijn en die eh, waar jij op een normale dag te maken hebt als een [the professional services firm] medewerker.

Y: Eh, nou ja, goed, onze, wij zijn een communicerend team he, dus wij eh, wij eh, hebben veel contact met klanten, [0:22:11 till 0:23:05 has been omitted]. Maar goed, daar nemen wij, in beiden gevallen nemen wij daar specifiek actie op, om te voorkomen dat dat nog een keer gebeurt en he, dat collega's of wij zelf onheus worden bejegend.

X: Ja. Oké. En heeft een VPN verbinding invloed op deze sociale dreigingen?

Y: Eh, nee, geen enkele.

X: Oké. Wel vervelend om te horen, dat wel. Ik kan me voorstellen dat dat niet leuk is.

Y: Nou ja, weet je, dat is eh, tegelijkertijd, aan de ene kant is dat het spel dat we spelen en eh, het werk dat we doen. Eh, tegelijkertijd, ja, blijft het het minst nette kant van de andere kant. Gelukkig komt het, het is net niet dagelijks dat je ermee te maken hebt, maar eh, ja, weet je, dat, het is, soms zijn mensen ook gewoon bang [0:24:12 till 0:24:19 has been omitted]. Ja, weetje, dat eh, daar hebben we gewoon mee te maken. Covid helpt daar niet bij, zeg maar.

X: Nee, dat kan ik mij voorstellen. Dat is vervelend. Oké. En dan terugkijkend naar de digitale dreiging die je eerder noemde, verandert eh, daarbij de soort aanvaller- Of wie of wat is de aanvaller die de dreiging veroorzaakt, bij de digitale dreigingen?

Y: Eh, digitaal. Dat is eh, nou ja, zowel klant als [the professional services firm] medewerker, maar met name klant. Eh, en nee sorry, digitale dreiging dat is even, excuus, nee dat is eh, ja, netjes gezegd de hacker die eh, die bijvoorbeeld een klantsysteem over heeft genomen of daarin heeft ingebroken. Dat kan zijn, een tijd geleden hebben we te maken gehad met [0:25:24 till 0:25:40 has been omitted]. He, dus dat zou een optie kunnen zijn. Maar ja, digitaal, digitale dreiging is voor mij wat meer de boefjes en de, he, dat ze echt eh, inbreuk maken op onze systemen, danwel op de systemen van de klant. En op basis daarvan gewoon [0:26:05 till 0:26:18 has been omitted].

X: Ja, oké. En wie of wat is dan de aanvaller die de dreiging de veroorzaakt? De boefjes?

Y: Ja, die ken ik niet persoonlijk. Maar je hoort tegenwoordig, je leest veel over eh, Russische, Chinese hackers, maar goed, dat gaat wat mij betreft meer over, over landen level. Ik zou eh, ik zou eh, gewoon zeggen iemand die slim is eh, met IT en eh, denkt hiermee op een goede manier weg te kunnen komen.

X: Ja. En wat is de motivatie van een aanvaller?

Y: Eh, ja, dat kan meerdere zijn. He, dat kan bijvoorbeeld zijn om eh, eh, zelf geld binnen te halen. [0:27:09 till 0:27:14 has been omitted]. Dat is eh, misschien wel om een bedrijf eh, schade toe te brengen. Kan zijn dat ze, dat ze bijvoorbeeld een systeem hacken he, of een hele computer, of een range computers eh, en eh, die vrijgeven op het moment dat er losgeld wordt betaald. Eh, dat.

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

Y: Eh, weet ik niet. Dat kan eh, dat kan van iedere klasse zijn. Ik denk niet dat ik eh, dat ik die aanvaller op dit moment kan identificeren.

X: Wat bedoel je ermee dat die van iedere klasse kan zijn?

Y: Je hebt meerdere sociale klasses. Ik heb eh, ik heb geen idee van eh, wie de, wie de uiteindelijke aanvaller van eh, van eh, voor een [the professional services firm] zou kunnen zijn.

X: Oké. En verandert de soort aanvaller door een VPN verbinding?

Y: Eh, nou ja, we maken het in ieder geval een stukje moeilijker. Dat de persoon of, of het type verandert. Eh, ja, dat eh, dat weet ik niet.

X: Oké. En op wat voor manier wordt het moeilijker gemaakt?

Y: Nou ja, je creëert een soort schild om, om in te loggen op het [the professional services firm] netwerk. En eh, daarmee maak je het moeilijker om, om aan de gegevens van [the professional services firm] te komen.

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

Y: Nou ja, de impact zou kunnen zijn dat ze een heleboel gegevens van [the professional services firm] eh, sorry, dat ze die eh, bloot kunnen leggen eh, eh, kunnen verspreiden, dus je hebt een gigantisch datalek. Eh, het zou kunnen zijn dat ze diverse systemen, eh, ...(0:29:40) of weet ik veel wat he, dat ze die kunnen hacken en, en lamleggen en eh, vele collega's hun werk niet kunnen doen. Het zou kunnen zijn dat eh, ook specifieke collega's daardoor bijvoorbeeld geraakt worden. Persoonsgegevens, data breach, had ik al genoemd. Dat eh, dat eh, nou goed, het ransomware he, dat er een stukje of een deel van [the professional services firm] gegijzeld wordt. Eh, maar onder aan de streep, ja goed he, eh, het is ook een heel groot imagoschade wat er mee te maken heeft. Of waar je dan mee te maken hebt.

X: Ja, oké. En als we dan kijken naar de VPN verbinding zelf, hoe veilig is een VPN verbinding?

Y: Dat weet ik niet.

X: Zijn er redenen die je kan bedenken waarom een VPN verbinding mogelijk niet veilig is?

Y: Eh, ja. Eh, simpel voorbeeld. [0:30:50 till 0:31:34 has been omitted]. En goed, vanuit dat perspectief ben ik eh, ben ik dingen gaan benaderen, van ja goed, alles is te hacken, alles is te kraken. Eh, maar je zal er continue eh, eh, als bedrijf mee bezig te moeten zijn om dat, om dat eh, om dingen veilig te houden en lekken te voorkomen.

X: Ja, zeker. En heeft encryptie zelf nog iets te maken met de VPN verbinding?

Y: Eh, dat weet ik niet precies.

X: Oké. Zijn er nog andere redenen waarom jij kan bedenken dat een VPN verbinding mogelijk niet veilig is? Of minder veilig?

Y: Eh, nou ja, weet je, je hebt, je hebt zelf een eh, het is de combinatie van een eigen password met een eh, random eh, random getal van zes cijfers eh, ja, ik weet niet of dat onder aan de streep, daarmee creëer je een heleboel combinatiemogelijkheden, ik weet niet of dat voldoende is, of dat daar nog over nagedacht moet worden. He, ik heb ook wel eens gehoord dat je daar bijvoorbeeld een dubbele eh, eh, he, codering in zou moeten gebruiken, om het nog veiliger te maken. Eh, maar daar weet ik het fijne niet van verder.

X: Ja. En wat bedoel je met een dubbele codering?

Y: He, dat je, dat je eigenlijk twee keer een eh, verschillende VPN moet openen.

X: Oké, ja. En wat voor eh, effect zou dan hebben?

Y: Dat je eh, het eh, nou ja goed, je, je maakt het iemand die kwaad wilt maak je het verschrikkelijk veel moeilijker, doordat je de keuze, de keuze van eh, ten minste, dat veel eh, je hebt twee lagen waar je doorheen moet zeg maar. Nou goed en als eh, [the professional services firm] IT goed oplet dan eh, dan kan men een keer door de eerste heen komen, maar zeker niet door de tweede.

X: Ja. En wat bedoel je dan met deze lagen?

Y: Met die lagen, dat je twee verschillende eh, VPN eh, connecties opbouwt. Eh, he, en je zou dus ook twee keer een password moten invoeren om bij de gegevens te komen eh, en daarmee zou je het veiliger maken. Maar goed, verder weet ik daar ook eh, de details, of het exacte verhaal niet van.

X: Ja, oké. Dan waren dit tot zo ver mijn vragen. Heb jij vragen voor mij? Of zijn er nu nog dingen van VPN die je denkt zijn belangrijk om te noemen, maar komen niet ter sprake?

Y: Eh, nee. Maar zat ik een beetje goed?

X: Ja, nee, zeker. Ik zal de opname even stopzetten.