# Transcription expert 11

Duration: 51 minutes

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

Y: VPN, of Virtual Private Network, is een eh, eh, een verbinding waarmee je met een eh, eh, een enduser of een enddevice, net hoe je het wilt noemen natuurlijk eh, over he, ze zeggen over een beveiligde verbinding toegang maakt tot het netwerk. Dat kan een bedrijfsnetwerk zijn of bijvoorbeeld het netwerk van een webapplicatie. Eh, in ieder geval dat.

X: Oké. En je zegt dat de verbinding beveiligd is-

Y: Ja.

X: Op wat voor manier is deze verbinding beveiligd?

Y: Ik neem dat het altijd gaat over een eh, eh, gebruik maken van versleuteling van eh, van de communicatie en dat die communicatie versleuteld is op een eh, asynchrone manier, dus door middel van een eh, eh, private key of public key infrastructure. Dat is mijn aanname, maar dat- Dat is een aanname, ja. Ik neem aan dat het over een PKI gaat.

X: Oké-

Y: Versleuteld. Ja.

X: En waarvoor gebruik jij de VPN?

Y: Eh, de VPN dat he, je refereerde aan het begin van het interview naar het gebruik van VPN binnen [the professional services firm], dus in dit geval zou de VPN zou dan zijn om van mijn thuiscomputer of vanuit mijn thuisnetwerkverbinding te maken met het [the professional services firm] netwerk, zodat ik bijvoorbeeld bepaalde zaken kan benaderen die alleen maar werken als je op het lokale netwerk zou zitten of via de VPN-verbinding maakt met het lokale netwerk.

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

Y: Binnen [the professional services firm] of?

X: Ja.

Y: Persoonlijk. O, binnen [the professional services firm] zou dat zeg maar verbinding met het eigen netwerk eh, ja, dus verbinding maken met toepassingen die daarvoor geschikt zijn. Eh, op die manier. Eh, dat zijn de enige redenen, het [the professional services firm] netwerk zelf geeft me niet het gevoel nou dat ik nou zeg maar anoniem op het internet browse. Integendeel, het is natuurlijk het bedrijfsnetwerk, dus nee. Puur voor verbinding maken met het netwerk, zodat ik toegang heb tot de shares en de applicaties die alleen werken met die verbinding.

X: Ja, duidelijk. En je noemt wel anoniem browsen-

Y: Hmhm.

X: Hoe werkt dat?

Y: Ja, het hele idee natuurlijk he, van een VPN is dat je verbindt met een ander netwerk. Nou, vanuit dat andere netwerk kan je verschillende dingen doen. Net alsof je op een fysiek netwerk aangesloten bent. En een van die dingen die je kan doen is natuurlijk weer verbindingen opzetten naar anderen netwerken. Stel dat je bijvoorbeeld browsed naar een website. Nou ja, als je nou persoonlijk gebruik maakt of eh, ja, vanuit je werk kan natuurlijk ook eh, van een VPN, dus ook bijvoorbeeld een webserver die communicatie maakt met een he, een apparaat dat dan vanuit die VPN een verbinding maakt, dat is natuurlijk wel een voorwaarde. He, dat de verbinding ook opgesteld wordt vanuit het netwerk van de VPN. En die ziet dan enkel als eh, als zender eh, dat netwerk van de VPN en niet het netwerk waar je misschien zelf in zit. Nou ja, op die manier eh, heb je een soort van eh, geanonimiseerde verbinding als in eh, men praat tegen die VPN aan en weet eigenlijk niet eh, wat jouw thuisnetwerk is. Nou als je het natuurlijk een paar keer achter elkaar doet he, dan krijg je een onion of een tor netwerk en ja dan, dan weet men eigenlijk niet wie nou het endpoint is. He, dus op die manier kan bijvoorbeeld een webserver, weet wel met welk netwerk die praat, maar dat is niet het netwerk waar jij zit. Dus op die manier weet die minder waar je vandaan komt en nou ja, dan kan je natuurlijk bijvoorbeeld bedenken aan dat de grote landen IP-reeksen toch wel vaak in brokken zijn uitgedeeld, dus daarmee kan je best wel wat informatie over wij hebben ...(0:04:50), daar gaat het voornamelijk om eh, waar jij bent, ja, ontnemen van iemand. En bijvoorbeeld correlaties van andere logs die je achterhaald.

X: Ja, en-

Y: Daarvoor kan ik het [the professional services firm] netwerk niet gebruiken hoor, want aangezien al het netwerk natuurlijk gemonitord wordt, is het voor mij in dat geval alleen maar juist vervelender, maar het is een mogelijkheid.

X: En hoe bedoel je dat dat vervelender is?

Y: Nou ja, stel nou dat ik he, op het internet dingen wil doen waarvan ik eh, zou verwachten van het is beter dat men niet weet wie ik ben, dan zal het in dat geval ook waarschijnlijk niet beter zijn dat mijn eh, bedrijf he, waar ik werk, weet dat ik die dingen doe. Dus in dat geval zou ik de [the professional services firm] VPN nooit gebruiken.

X: En hoe zouden zij dan weten wat jij doet?

Y: Nou ja, de netwerkstromen die eh, he, ik weet natuurlijk niet precies hoe het bij [the professional services firm] ingericht is, maar er vindt ook gewoon verkeeranalyse plaats, en dat is zeer zeker wel eh, natuurlijk gelinkt aan he, wie achter hun verbinding zit. Want [the professional services firm] beheert natuurlijk uiteindelijk eh, het apparaat waar ik op werk. Dus als ik voor een reden anoniem moet blijven, dan kan ik dat beter natuurlijk niet doen via het netwerk van het bedrijf waar ik werk.

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

Y: Eh, nou, vanuit [the professional services firm] is het zo ingericht dat natuurlijk de VPN-adapter geheel geconfigureerd is, dus de software eh, die eh, weet met wie die moet communiceren, tegen wie het, he, het endpoint toe moet gaan, is allemaal geconfigureerd. Het enige dat aan mij wordt gevraagd is mijn wachtwoord in te voeren, dus eh, binnen het netwerksegment van de omgeving klik ik op connect to this he, tot dit netwerk, dan krijg ik een pop-up veld en dan wordt mij gevraagd om eh, met twee-factor authenticatie in te loggen eh, en een gedeelte daarvan is een eigen persoonlijke identificatienummer en het tweede is een eh, een tweede factor, in dit geval een apparaat he, dat ik heb, mijn telefoon, en die geeft mijn code via door middel van de [access token provider] app die erop staat. En dan samen dat eh, dan worden mijn credentials gecheckt en als dat klopt, dan wordt de verbinding opengezet.

X: Oké. En je zei dat het endpoint geconfigureerd is, wat bedoel je hiermee?

Y: Eh, ja, wat ik ermee bedoel is he, stel nou dat ik moet natuurlijk he, de VPN, als je het zo zou kunnen noemen, weet natuurlijk niet waar het de verbinding mee op moet zetten, dus de gegevens die nodig zijn eh, en ik denk dan he, dat het dus in de configuratie opgesteld is met oké he, verbind naar, ik noem maar wat, naar deze server, en voor ons staat volgens mij alles in [country] he, en daarop he, weet die server, als er verzoeken komen en ik neem aan, maar dat weet ik niet zeker, van he, dit apparaat, in mijn geval zal het waarschijnlijk een MAC-adres zijn of misschien nog wel op basis van andere gegevens, zoals mijn AD-account, mijn AD eh, gegevens, weet die van oké, he, bij een verzoek van deze verbinding hoort ook eh, deze credentials. He, want ook zij moeten natuurlijk controleren dat de hash die, of in ieder geval de wachtwoordgegevens die binnen komen, correct zijn. Dus ik denk dat dat met het configureren is. Dus zeg maar dat de verbinding die opgesteld wordt, ja, moet men weten waar naartoe, je kan geen lege envelop sturen. Of eh, je kan geen envelop sturen zonder eh, adresgegevens erop.

X: Ja. En hoe wordt bepaald waar het uiteindelijk naar toe wordt gestuurd?

Y: Hoe bedoel je?

X: Eh, je zegt adresgegevens-

Y: Ja, ja, dus in he, eh, he, ik wil een verbinding opzetten, ik doe dus een verzoek ergens over het internet he, dat ik wil gaan verbinden met het netwerk en daarvoor moet ik ergens over het internet ...(0:08:52) die verbinding maken, maar die verbinding moet ook weten dat ik die verbinding mag maken en welke gegevens zij nodig hebben. Dus in die configuratie eh, zal waarschijnlijk staan he, naar welk adres dat verzoek toe staat, dat is wat ik bedoel met de adresgegevens op de envelop.

X: Ja. En dan zei je voor wat je nodig hebt om je verbinding te maken-

Y: Ja.

X: Dat je je persoonlijke code hebt en daarnaast een code op je mobiel-

Y: Ja.

X: Zijn hier nog andere mogelijkheden voor, voor deze andere code?

Y: Eh, even kijken, voor zo ver ik weet bij ons niet. Eh, he, je zit of op het netwerk natuurlijk he, dan ben je fysiek aangesloten of he, fysiek als in eh, je zit op het eh, het bedrijfsnetwerk of je logt inderdaad in door middel van de VPN en dan voor zo ver ik weet moet dat altijd gaan via de twee-factor authenticatie. We hadden daar vroeger een eh, [access token provider] token voor, maar als het goed is worden die nergens meer gebruikt.

X: Oké. En op welke apparaten gebruik jij je VPN?

Y: Eh, ik gebruik mijn eh, de VPN waar wij het nu over hebben, zeg maar [access token provider] token(0:10:09) en geldt puur voor mijn laptop.

X: Oké. Gebruik je het nog op andere apparaten?

Y: Nou, we hebben, het schijnt dat we sinds kort een mogelijkheid hebben om met onze telefoon ook op een gedeelte van het bedrijfsnetwerk te komen en dan bepaalde webpagina's, maar a het is mij nog niet gelukt het werkend te krijgen en b dat zal via een andere manier ingesteld zijn dan dit. Dus ik denk alleen op eh, dit ik houd het op alleen de laptop.

X: Oké. En kun je aan mij uitleggen hoe een VPN-verbinding werkt? En hiervoor kan je het whiteboard gebruiken-

Y: Hmhm.

X: Ik zal mijn tekeningen weghalen.

Y: Ja, even kijken hoor. [start drawing 11\_1]. Even kijken, we hebben in ieder geval een paar toren he, en dat is in ieder geval- En onderaan, dan zeg ik even dat dit ...(0:11:05) zit. Dus dan zeg maar, he, de user, noem het even de user, hoe, ja, dan tekenen we het gewoon erin, ook goed. O, wacht, zo moet dat, kijk, zo, he, he, user. Ook fijn dat er zo een lange periode tussen zit met transcriberen zo meteen, waarvoor dank. Eh, user, dus we hebben een user he, die zet een verbinding op naar een bepaald adres, he, dat zou dan de, nou ja, ik noem het nu even de VPN-ontvanger zijn. Eh, ik weet niet of dat de juiste terminologie is, maar in ieder geval die zet een verbinding op naar dat adres en die stuurt mee eh, bepaalde gegevens he, eh, en een gedeelte daarvan, dat zijn dan die wachtwoord, het wachtwoord plus dan dat token en dat zal waarschijnlijk in een hash eindigen. He, dus we zeggen hier dat er een hash meegaat, o, wacht, hij staat nu op, zo, even kijken, even kijken hoe die tool precies werkt hoor, zo. He, die stuurt dan die hash mee, kan ik beter niet zo doen, o, he, he, nou, geen enkel probleem. Hup, we weten nu wat we moeten doen. User, zal vast niet de eerste zijn die hem helemaal kapot maakt.

X: Nee, het gebeurt een enkele keer inderdaad.

Y: Ja, precies. Dan we noemen het even he, de VPN-ontvanger, maar ik heb geen idee wat de daadwerkelijke terminologie is. Zo, gaan we eerst een verbinding opzetten. Dus ik heb he, met mij is geconfigureerd he, naar wie ik iets moet sturen. Anders, ja, ik kan natuurlijk niet ...(0:13:06) iets sturen. Zo, zetten we een lijntje op zo, wat daaruit komt he, dus we sturen de gegevens mee die nodig zijn eh, he, om te verifiëren dat ik ik ben en dat ik überhaupt mag inloggen, dus in dit geval zal dat usergegevens zijn. Plus dan he, het password. En he, laten we ervan uitgaan dat is een hash. Kan ik dit nog groter maken, nee, jij misschien wel later in je tekening, in ieder geval je weet dat het er staat. Nou, he, die gegevens die komen daaraan en dat wordt gecontroleerd he, dus zij eh, hebben een manier om te controleren van he, de hash klopt met de hash die zij kunnen genereren. Eh, nou ja, en als dat allemaal goed is dan wordt mij toegang verleend. Nou he, dan zorgt de VPN-ontvanger, of de VPN-ontvanger staat misschien al in een netwerk, van het netwerk waar ik naartoe wil verbinden. Laten we daar op dit moment even vanuit gaan dat dat gewoon een gedeelte van het segment is. Die zegt dat klopt, die verbinding mag worden opgesteld. He, die stuurt dus weer de gegevens terug die nodig is om onze eigen communicatie eh, eh, te versleutelen. [start drawing 11\_2]. Ja, als dat allemaal werkt, dan ja, heb ik feitelijk, o, wacht, verkeerde, toegang tot het netwerk. He, laten we zeggen, laten we dit even [the professional services firm] noemen, tekst, [the professional services firm] netwerk, en nou, om toegang tot dat netwerk te bereiken eh, voor of over bepaalde protocollen of voor bepaalde services of diensten. He, het hoeft natuurlijk niet per se zo te zijn dat voor alle verbindingen die ik straks naar buiten open stel dat die altijd via het [the professional services firm] netwerk gaan. Dus om een voorbeeld te noemen, mijn [e-mail] gegevens he, hoeven niet per se over het, over de VPN te gaan he, dus als ik browse op internet of een verbinding op stel, dan bepaalt mijn computer ten eerste oké, mag het naar de VPN toe of niet of gaat het over de VPN of niet en alle gegevens die erover gaan die gaan erover en alle gegevens die er niet over gaan, die gaan gewoon via het netwerk waar ik dan daaronder verbonden ben, in dit geval gewoon mijn thuisnetwerk. Nou ja, en dat blijft gewoon gaan tot een sessie termineert.

X: Oké. Eh, dus in dit geval in deze tekening staat de VPN-ontvanger in het [the professional services firm] netwerk.

Y: Ja, maar, ja, maar ik zal je niet durven te zeggen, het zou ook kunnen zijn dat die eh, in ons geval ergens anders staat en zeg maar alleen maar als een soort van PKI eh, fungeert om te zeggen oké he, hij mag die verbinding opstellen en zet de verbinding op, dat weet ik echt niet. Ik weet niet of we dat op die manier intern hebben of niet. En dit is allemaal natuurlijk wel gesegmenteerd he, dat is wel natuurlijk sowieso zo.

X: Wat bedoel je daarmee, dat het gesegmenteerd is?

Y: Nou ja, he, eh, dus het is sowieso een eigen eh, virtueel netwerk binnen dan wat van [the professional services firm] is. He, de VPN-ontvanger zal natuurlijk nooit op die manier vrije verbindingen naar het gehele netwerk open kunnen stellen, maar er alleen voor kunnen zorgen dat ik verbinding kan maken met het netwerk of gedeeltes van het netwerk. Zoals dat met een normale verbinding ook zal gelden.

X: Oké. En je noemde kort even protocollen in het verhaal-

Y: Hmhm.

X: Wat is de rol van een protocol?

Y: Ja. De protocollen he, eh, of in dit geval ook services, en dan denk ik van hoe het geconfigureerd is he, dus de manieren waarop de verbindingen en de diensten voor die verbinding gebruikt kunnen worden. Eh, over een in dit geval, over een eh, over een netwerk of over een verbinding. En het kan heel goed zijn dat je bijvoorbeeld een VPN hebt die jou eh, toegang geeft tot het netwerk of tot een segment van het netwerk, maar alleen maar voor het uitvoeren van bepaalde diensten of voor verkeer over bepaalde eh, protocollen. He, en het meest gemakkelijke geval zal men bijvoorbeeld die als onveilig beschouwd worden niet accepteren, dat een, of eigenlijk biedt die niet aan. Maar voornamelijk voor diensten kan het heel goed zijn dat bepaalde diensten eh, misschien helemaal niet over het VPN gaan, dus ook niet over het netwerk gaan. He, dat, dat, kan ik weten, ik heb echt geen idee hoe dat bij ons van toepassing is. En ik weet bijvoorbeeld dat voorheen het voor eh, ons mailverkeer het noodzakelijk was om verbinding te maken met het [the professional services firm] netwerk, en dat tegenwoordig niet meer zo is. Dus ik neem daarmee ook aan dat eh, zeg maar het mailverkeer, [e-mail] is dat volgens mij, dat weet ik niet zeker, dat dat niet meer over een VPN loopt en ook niet meer over een VPN dus hoeft te lopen. Zoals als je de VPN-verbinding hebt en je stuurt een mail en hij is er op die manier uitgesloopt, dan zal die mail ook niet over de VPN lopen in dat geval.

X: Ja. En als die mail niet over VPN loopt, hoe gaat het dan naar je toe?

Y: Dan loopt het gewoon over mijn eigen netwerk. Dus als we hier ergens het internet zouden kunnen tekenen. [start drawing 11\_3]. He, dus ik zit he, de user zit ook in dit geval in zijn eigen netwerk, zo. Hij, mijn teken skills zijn niet de allerbeste, zoals je waarschijnlijk al ziet. Maar he, usernetwerk, nou ja, en mijn mail, waar die voorheen dus waarschijnlijk eerst naar het [the professional services firm] netwerk ging en daar dan een mailserver stond en dan he, verder naar destination toe ging, gaat het nu naar de mailserver en die kan of in het [the professional services firm] netwerk liggen of eh, wat mijn vermoeden is bij [example of softwareprovider], aangezien we [an internal page] hebben. [start drawing 11\_4]. Zo he, en dan voor de eenvoudigheid gewoon o, wacht, eerst even noteren. He, dus als ik die verbinding op moet stellen, dan zal die ongeacht of VPN aanstaat of niet, naar die mailserver toegaan, die ja, eigenlijk niets met eh, de VPN te maken heeft. En dan ja, naar de bestemming whatsoever.

X: Oké. En als deze VPN-ontvanger niet in het [the professional services firm] netwerk zit, hoe ziet dat er dan uit?

Y: Stel dat die niet in [the professional services firm] he, er zijn een paar dingen, maar he, dus voor mij, op die manier kom ik niet echt veel mee in aanraking mee. Eh, he, maar netwerk technisch gezien zou ik denken dat het mogelijk zou zijn dat je bijvoorbeeld echt een VPN hebt die geheel extern is, he. Die zal dan twee dingen kunnen doen. Ik kan het niet wegnemen he, dit of wel, met het handje misschien, kijken, nee. Oké. Was te proberen. [start drawing 11\_5]. Eh, dan zou je bijvoorbeeld wat zou kunnen zijn, maar ik weet niet of dat bestaat of dat het werkt, dat je een dienst hebt die gewoon puur hier eh, verifieerd of nou deze user deze user is en deze user nou die verbinding wel mag stellen. En he, indien dat zo is eh, die verbinding doorzet. He, zeg maar een soort van handshake verricht. En sommige partijen die het bijvoorbeeld ook doen voor authenticatie met eh, overheden eh, wat ook heel misschien zou kunnen zijn, maar dat weet ik ook niet zeker, of misschien is dat wel gebruikelijk, maar eh, dat je ook zo een partij hebt die controleert dat, die verifieert dat he, die voorziet misschien van de credentials. En met die credentials kan ik dan direct zeg maar contact opnemen met het netwerk en dan gewoon het normale netwerkverkeer eh, employen. Maar dat is voor mij gewoon een beetje gokken hoor, ik heb geen idee waar de VPN host, als je hem zo zou kunnen noemen, specifiek staat. Of het in het netwerk moet staan of niet.

X: Ja. En je had het eerder over versleuteling-

Y: Ja.

X: Welke van deze verbindingen zijn versleuteld?

Y: Nou ja he, wat natuurlijk in dit geval he, eh, van alles wat, kijk, verbinding met de VPN dus nadat de VPN sessie is opgesteld he, zijn inherent versleuteld. Dat is het hele idee natuurlijk van het private, van het gedeelte en virtueel staat natuurlijk voor het feit dat je niet daadwerkelijk verbonden bent met het netwerk via een kabel. Eh, he, dus de eerste uitwisseling kan gaan op een op, op, een type versleuteling, maar zal waarschijnlijk enkel gebruikt worden voor het overeenkomen eh, eh, van hoe er versleuteld gaat worden. He, dat je een pre-key gaat definiëren. Eh, daarna zal al het verkeer, nou ja, het hangt ervan af eh, he, als de VPN inderdaad in het netwerk staat dan zal al dat verkeer versleuteld blijven, in het geval eh, dat de VPN verbinding alleen maar wordt gebruikt als een hub, dan blijft dat ook gewoon heen en weer versleuteld hier, en in het geval dat er alleen maar voor wordt gezorgd dat mijn credentials kloppen en dat er zeg maar via een externe partij of een externe host de verbindingen opgezet worden, dan zal daarna al dit verkeer versleuteld lopen. En met [example of software provider] neem ik ook aan dat het versleuteld loopt, maar ja, dat is buiten de, buiten de scope van het onderzoek. Eh, het hele idee natuurlijk van VPN zelf is om versleuteld verkeer mogelijk te maken. Ten minste, verkeer mogelijk te maken tussen netwerken en nou ja, dat moet gewoon versleuteld zijn. Zou wel heel slecht zijn als dat niet versleuteld is, zou vast mogelijk zijn natuurlijk, maar, binnen [the professional services firm] denk ik niet, maar zeg maar in de rest van de wereld. Eh, ja, het idee is natuurlijk dat je op een beveiligde manier versleuteld bent, omdat je niet weet wie het is.

X: En voor deze tekening maakt het nog uit op welke locatie jij bent?

Y: Eh, nou ja, laten we eens naar het beginscenario toegaan. Dus he, dus maakt eigenlijk voor deze tekening maakt het voor de user niet uit of die nou in het usernetwerk zit of in een, weet ik veel, best friend netwerk als je het zo zou kunnen noemen, of een ander netwerk. Het kan wel zijn, maar he, he, dan gaan we weer even terug naar de scope voor het [the professional services firm] netwerk, maakt het volgens mij niet uit uit welk netwerk het verzoek komt. Dus het maakt niet uit in welk netwerk het userapparaat zich bevindt. He, maar het kan wel voor, ik kan me heel goed voorstellen dat je ook met whitelisting natuurlijk kan werken en kan zeggen ik wil alleen maar mensen, apparaten met deze gegevens correct, die correct aansluiten, die ook uit het netwerk komen. Maar dat is voor [the professional services firm] niet geldig, in ieder geval niet geldig op een manier dat ik alleen maar vanuit mijn huisnetwerk, thuisnetwerk een verbinding op kan zetten. Dat is niet zo.

X: Oké. En stel je voor dat je op een andere locatie bent, in dit geval bijvoorbeeld een café-

Y: Hmhm.

X: Verandert er dan iets aan deze tekening?

Y: Nee.

X: Oké.

Y: Nee.

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

Y: Definieer computerbeveiliging.

X: In een hele brede manier. Heeft VPN invloed op jouw computerbeveiliging?

Y: Eh, nou ja, eh, stel dat ik eh, hangt eraf, laten we even de makkelijke aanname nemen dat de aanname is dat al het verkeer als ik een VPN-verbinding heb, al het verkeer via de VPN gaat. Dus eh, verbindingen naar mij toe of verbindingen van mij af die ik opzet, komen altijd van het VPN-netwerk af. In dat geval, he, omdat het VPN-netwerk natuurlijk beschikt over meer beveiligingsmaatregelen dan ik thuis he, denk dan aan geavanceerde firewall, denk aan eh, analyse, de IDS en IPS, voegt dat toe aan de beveiliging van mijn netwerkverkeer. Eh, maar dat maakt het zeg maar niet onmogelijk ofzo om virussen op te lopen. Misschien moeilijker omdat er packetinspection kan plaatsvinden op de verbindingen die dan via de VPN via het [the professional services firm] netwerk naar buiten gaan, wat misschien niet beveiligd is. Eh, dus ja, het voegt zeker he, in het breedste zin van het woord, voegt het eh, iets toe, positiefs, aan de beveiligingsaspecten van mijn werklaptop.

X: Oké. En je noemde even kort een firewall, waar in deze tekening zouden we een firewall kunnen vinden?

Y: Nou ja, he, het zal eerst bij het usernetwerk zijn in dit geval. [start drawing 11\_6]. Dus dat kunnen we ook wel tekenen hierzo bij het usernetwerk he, want de meest elementaire firewall namelijk zit gewoon bij mij in de router met vastgestelde zaken van de IPS. Dan zal de he, de VPN-ontvanger zit natuurlijk in het [the professional services firm] netwerk en alle verbindingen uit het [the professional services firm] netwerk gaan ook over een firewall heen, zou hier zitten. En alle verbindingen die naar buiten gaan, gaan waarschijnlijk ook over dezelfde firewall. Of in ieder geval over hetzelfde firewallsegment heen. En eh, nou ja, dat geldt natuurlijk indien hier een derde partij is, als hier een derde partij is he, alles wat in het netwerk zit in dit geval zal achter een firewall zitten.

X: Oké-

Y: Of een vorm van firewall, he, ja.

X: Zijn er nog meer manieren waarop een VPN invloed heeft op jouw computerbeveiliging?

Y: Even kijken, mijn communicatie is versleuteld he, dus zeg maar man in the middle, dus waar je enerzijds op doelt, iemand die tussen zit zou niet met mij kunnen meelezen. Eh, enerzijds is verkeer dat enerzijds loopt he, naar anderen toe. [start drawing 11\_7]. Dus stel dat hier weer een andere webserver is he, dat, teken even heel lelijk dat het via [the professional services firm] netwerk gaat. Ja, he, en dit is niet versleuteld bijvoorbeeld he, en dat zet ik hier de maatregelen die wij gesteld heb, stel aan blacklisting eh, eh, verkeeranalyse, ook allemaal gelden voor eh, die verbinding. [start drawing 11\_8]. Terwijl als ik hem misschien zelf direct doe, dat niet zou gelden. Dus dat voegt op die manier toe, ja.

X: Oké. En je zegt verkeeranalyse, maar ook dat het netwerk versleuteld is, hoe hangt dat samen?

Y: Sorry, ik verstond het eerste gedeelte van je vraag niet. Kan je dat herhalen?

X: Ja, je noemde verkeermonitoring-

Y: Ja.

X: En ook versleuteling, hoe hangt dat samen?

Y: Ja. Eh, he, het zijn natuurlijk- Kijk, stel dat ik hier een verbinding met het netwerk opzet en dat verkeer is versleuteld he, dan moet het op een gegeven moment ergens ontsleuteld worden, want anders weet men niet he, wat er moet gebeuren. Stel dat ik hier tegen een webserver aan loop te praten en die krijgt alleen maar voor hem zeg maar gibberish binnen, ja, dan weet die natuurlijk niet welke zaken er eh, moeten plaatsvinden. Dus dat moet je ergens gaan eh, ontsleutelen he, offloading. Eh, he, op het moment dat je het offload, betekent dat alles in te zien is. Eh, betekent ook dat je analyse kan uitoefenen op dat verkeer, he, dat gaat geautomatiseerd. Dus dat gaat met apparaten en met software he, die analyseert wat voor dingen er gevraagd worden, wat eroverheen loopt eh, waar de verbindingen naar toe gaan. Eh, he, en dat doet het op verschillende manieren. Wat natuurlijk ook nog kan, he, er was vroeger een bedrijf van, dat is failliet gegaan helaas, dat analyseerde bijvoorbeeld hoeveel verbindingen erop werden gesteld en hoeveel foutmeldingen er kwamen eh, naar DNS-verzoeken, die ja, eerst niet werkten. En het idee erachter was dus dat als men bijvoorbeeld eh, een grote eh, DDoS aanval wilde gaan raadplegen, moet je dus eerst allerlei apparaten infecteren en je wil eh, he, die aansturen, dus een soort van command and control center gaan bouwen. En je wilt ervoor gaan zorgen dat die op een gegeven moment natuurlijk actief worden, maar niet allemaal gelijktijdig, want dat valt op, of in ieder geval niet allemaal buiten moment van infectie, want dan heb je niet een groot genoeg kritische massa. Dus wat deden die apparaten, die zaten in het netwerk, of dat kon je laten implementeren eh, die zochten nou vaak nou ineens eh, eh, niet bekende of bijna niet bestaande eh, DNS-verzoeken kwamen naar eh, webservers en als dat heel vaak ineens naar onbekende omgevingen waren, dan was dat waarschijnlijk dus een webserver die eh, door eh, malware werd aangevraagd, maar die nog niet actief was. Derhalve he, kreeg je die eh, kreeg je die foutmelding, dat is ook een vorm van beveiliging natuurlijk. Maar dan hebben we het over zeg maar hele geanalyseerde netwerken eh, of hele geavanceerde analyses. Eh, het meest elementaire is gewoon de automatische packetinspection op het verkeer, na ontsleuteling. Als je naar versleuteld verkeer kijkt, kan je ook nog wel wat doen, bijvoorbeeld het aantal eh, het aantal verbindingen dat opgesteld wordt, het aantal requests dat binnen komt of he, de sources, maar ja, dat, ja, is feitelijk een beetje waardeloos als je het vergelijkt met wat je kan eh, geautomatiseerd als je het verkeer in kan zien.

X: Ja. Oké. En dan een hele brede vraag. Met wat voor digitale dreigingen heb jij op een normale dag te maken?

Y: Haha. Even kijken, ik denk dat eh, als thuisgebruiker mijn digitale dreiging er niet anders uitziet dan eh, voor iedereen anders en dat afhankelijk van wat voor bedrijf je werkt, en [the professional services firm] zou dat kunnen zijn he, een bedrijf waar je denkt hé, daar valt een hoop geld te halen of dat is leuk om het om te leggen en je ook nog eens in getarget kan worden. En nou dreigingen ja, die zijn ook ultrageneriek. Dus wij zullen vast wel geen beveiliging hebben blootstaan aan alle vormen van eh, van malware en dan kan je natuurlijk ja, denken aan alles, mensen die verkeer proberen af te luisteren, mensen die eh, proberen informatie te extraheren, mensen die proberen eh, toegang te krijgen tot systemen, tot applicaties, tot eh, de laptop in dit geval eh, mensen die dingen versleutelen om daarvoor geld te halen, ransomware, eh, ja, alles. Op die manier specifiek.

X: Oké-

Y: Om een heel breed antwoord terug te geven op je vraag.

X: Ja. En hoe verandert de soort dreiging door een VPN-verbinding?

Y: Nou ja, kijk, de soort dreiging he, we hebben natuurlijk te maken over de threat actors of threats, en we hebben natuurlijk te maken met kwetsbaarheden. Eh, ja, he, gebruik of geen gebruik eh, van VPN verandert niets aan mijn threats. He, dus als dat geautomatiseerd gaat of men wil doen, dat blijft bestaan. Het is niet dat ik een VPN-verbinding heb en ineens alle malware uit de wereld is. Eh, wat wel zo natuurlijk is dat eh, heel veel kwetsbaarheden die ik misschien zou hebben, bijvoorbeeld he, dat iemand een manier heeft gevonden om het verkeer tussen mij en in dit geval mijn ISP, waarschijnlijk een webserver ergens anders, en dan [the professional services firm] in te zitten, eh, ja, die kwetsbaarheid of die threat verandert niet, maar dat zij verkeer kunnen luisteren of meenemen of inzien wel. Omdat de VPN-verbinding het versleutelt in dit geval. Eh, dus dat verandert op die manier.

X: Oké. En heeft de VPN-verbinding nog meer invloed op de soort dreiging?

Y: Even kijken. Heeft de VPN-verbinding- Ja, wat, nou ja, wat je nog zou kunnen zeggen, stel dat ik maak gebruik van een bepaalde type VPN, stel nou dat andere mensen weten dat wij gebruik maken van die bepaalde type VPN, dat voor dat bepaalde type VPN een kwetsbaarheid bekend is eh, ja, dan zouden wij natuurlijk specifiek getarget kunnen worden. En alsnog steeds de vraag als het alternatief geen VPN is he, dan is het natuurlijk om het even. Dus theoretisch gezien op die manier wel, maar praktisch gezien vervang je dan natuurlijk de ene dreiging voor de andere.

X: Ja. Oké. En dit ging dan over digitale dreiging, heb jij ook op een normale dag te maken met een sociale dreiging?

Y: Ja, nou ja, voorheen meer dan nu natuurlijk, ik zit nu voornamelijk thuis. Dus mensen die met mij meelopen naar binnen heb ik niet echt heel erg. Mensen die mij afluisteren eh, en dat ik toevallig zeg of kunnen overhoren wat ik zeg maar zeg, heb ik natuurlijk ook niet meer, want ja, ik zit op die manier in een afgesloten en gecontroleerde omgeving. Eh, mensen die mij misschien proberen informatie te ontfutselen of iets dergelijks, ja, nee, ook niet. Eh, nee, ik denk het niet nee. Sociale dreigingen, nee, niet van threat actors zo ver ik weet en ook niet intentioneel. Zo ver ik weet.

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

Y: Ik denk niet dat de VPN-verbinding invloed heeft op deze sociale dreigingen.

X: Oké.

Y: Behalve, ja, ik wil nog wel een ding opperen. Eh, als dat niet erg is. Stel nou, dit is natuurlijk niet het geval. Maar stel dat ik op een openbare locatie ben he, [0:35:03 till 0:35:04 has been omitted], in ieder geval niet thuis of bij [the professional services firm] kantoor en eh, iemand bemachtigd mijn laptop en op een of andere manier kan hij binnen komen en eh, dan zorgt de VPN natuurlijk wel voor dat eh, alles wat hij in kan zien beperkt is tot de gegevens die op mijn laptop staan. Aangezien door de twee-factorauthenticatie hij de VPN nog niet kan opzetten en dus ook geen informatie kan verschaffen tot gegevens die op het [the professional services firm] netwerk staan. Als dat de bedoeling was van de vraag.

X: Ja, dat was de bedoeling van de vraag.

Y: Oké. Ja.

X: Bedankt. Als we kijken naar deze digitale en sociale dreigingen-

Y: Ja.

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

Y: Ja, dat zal natuurlijk he, eh, eh, heel verschillend kunnen zijn. He, als je kijkt naar het landschap, dan heb je helemaal bovenaan heb je zeg maar nation states he, in de film altijd afgebeeld als [country], nou dat is het zeer zeker natuurlijk ook, maar he, natuurlijk ook een [country], [country] en eh, ja, met een zekerheid grenst er waarschijnlijkheid aan onze eigen buren en onze vrienden. He, dus door overheid eh, getraind en geleide eh, gespecialiseerde omgevingen. Nou, ik verwacht niet dat ik als persoon daar onderdeel van ben, ik verwacht wel heel stiekem dat [the professional services firm] daar misschien een klein beetje een target van is. Dat is een. Dan heb je nog gespecialiseerde hackersgroepen die dingen tegen betaling doen. Die vinden zich vast plaats in [country]. Denk ook niet dat wij daar onder zitten. Dan heb je een groep daaronder, dat zijn zeg maar hackercollectivism eh, ja, groepen. He, mensen die om wat voor reden dan ook eh, eh, vinden dat eh, wie dan ook eh, iets niet goed doen, daarvoor gestraft moet worden, op een miljard manieren kan dat natuurlijk. Daarvan denk ik wel dat wij als [the professional services firm] onderdeel eh, zeg maar ook een target van zijn. He, dat zou je dan kunnen benaderen aan het feit natuurlijk dat onze [role] schandalig veel geld verdienen, maar dat we waarschijnlijk ook wel prominentere klanten hebben eh, die sowieso op hun lijstje staan. En derhalve zeg maar, medeschuldig zijn. Mij persoonlijk denk ik niet. Nou daaronder heb je dan gewoon losstaande hackers zeg maar he, daar kan je natuurlijk wel verschillende gradaties in vinden eh, van echt zeg maar scriptkiddies en mensen die misschien ook professioneel doen. Nou ja, daar zullen we vast wel ook een target van zijn, maar he, eh, niet op de manier dat echt eh, belangrijk is. En natuurlijk andere organisaties. Met andere organisaties bedoel ik eh, concurrenten of andere partijen. Eh, ja, he, die, die zullen allemaal het wel op [the professional services firm] gemunt hebben ergens op de wereld. Hebben natuurlijk meer dan [number] medewerkers. Nou, ik verwacht eigenlijk zelf niet dat ik daaronder val. Het enige waar ik wel verwacht misschien onder te vallen zijn eh, he, wanneer een van die actoren besluit gewoon om geautomatiseerd een beetje te scannen om te kijken wat open is. Zeg maar eh, he, dan toevallig ergens op uitkomt. Even kijken, we hadden het over dreigers he, over threat actors toch nu?

X: Ja.

Y: Oké, ja, ja. Eh, nou ja, voor alle aanvallen die zij gebruiken, want ik ga vast vervolgvragen beantwoorden. Eh, denk ik dat de VPN mij beschermt op de manier die we hiervoor al zijn uitgelegd.

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

Y: Eh, de motivatie van een aanvaller kan natuurlijk verschillend zijn. He, eh, he, zoals we net al eh, eh, bespraken, hebben we natuurlijk de nation states, die zouden dingen doen om diplomatieke eh, eh, economische en militaire belangen eh, dan laat het eh, daaronder hadden we net ook alweer gezegd, hadden we de getrainde doelen, die doen het voor geld, eh, de hackers eh, groepen, die doen het vanuit een morele slash ethische eh, omgeving eh, vinden zij. Eh, die andere organisaties zouden het doen vanuit een commercieel belang. Scriptkiddies vanuit een intrinsiek belang. Volgens mij heb ik dan iedereen benoemd die we net benoemd hebben. En natuurlijk kan het gecombineerd zijn he, dus een goede ransomware aanval om een voorbeeld te noemen geleid vanuit een eh, een nationstate of een door een nationstate geleide groep, met als doel om eigenlijk een land plat te leggen en als bijkomend voordeel om heel veel geld op te halen, is natuurlijk een valide combinatie op die manier.

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

Y: Ja. Nou ja, hij of zij zal natuurlijk wel eh, eh, op die manier goed moeten kunnen zijn met de techniek en de kwetsbaarheden en de beheersing van bepaalde tools. En de achtergrond voor de rest zeg maar he, waar je het hebt over demografieën of overtuigingen of iets ja, zou afhangen van in welke threat actor hij of zij zit.

X: Oké-

Y: Dan hebben we het over het technische verhaal, he. En het sociaal verhaal is natuurlijk eigenlijk hetzelfde, alleen dan ja, is het eh, he, als iemand natuurlijk met je mee wil lopen en ik hoor hem overduidelijk [country] praten of in ieder geval over duidelijk iets praten waarvan ik denk dat het [country] is en ik vind dat die heel verdacht dicht achter mij loopt, eh, he, dat is natuurlijk dan anders. Eh, maar voor de rest, ja, dat is qua achtergrond wat ik denk zeg maar. Zullen wel ja, attacksavvies zijn. Hoeft niet per se hoog- of laagopgeleiden te zijn of iets dergelijks.

X: Oké. En eh, over deze aanvaller, verandert de soort aanvaller door een VPN-verbinding?

Y: Ik denk niet dat de soort aanvaller verandert door de VPN-verbinding, wel dat de pogingen die het soort aanvaller doet door de VPN-verbinding verandert. He, dus eh, iemand met weinig kennis of iemand die denkt hé, het is wel grappig om even te kijken, eh, zo stuiten op die VPN-verbinding en door gaan naar een klant die makkelijker is. He, of een omgeving die makkelijker is. Eh, ja, he, een echt getargete aanval he, eh, he, dus zeg maar die eerste paar threat actors die ik benoemde, ja dat zou toch niet veranderen want die zijn he, niet gemotiveerd vanuit een perspectief dat ze even aan het kijken zijn zoals een scriptkiddie met een hé, wat is leuk om te doen he, dat is een hele andere motivatie. Dus die zullen niet ophouden. Of in ieder geval, die zullen niet weggaan omdat de VPN-verbinding er is. He, misschien dat ze niet eh, niet slagen in hun poging he, maar ja, dat zou niet betekenen dat ze niet ophouden of dat ze geen andere manier vinden.

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

Y: Nou ja he, in ons geval zou dat eh, zou de impact van een aanval op verschillende manieren kunnen uitwerken. Denk aan eh, commercieel belang he, dus in dit geval zou dat bijvoorbeeld het niet kunnen gebruiken van bepaalde middelen kunnen zijn eh, waardoor wij ons werk niet kunnen uitoefenen. Het zou ook een ...(0:42:33) belang kunnen zijn he, dus wij kunnen het niet gebruiken maar we zijn bijvoorbeeld gegevens kwijt. Eh, he, allemaal economische verhalen eh, he, we zouden data kunnen verliezen van klanten of het kan openbaar worden, zijn ook allemaal nog economische verhalen. Eh, ja, in ons eigen geval he, mensen zouden misschien een beetje bangig(0:42:54) kunnen worden, maar de impact denk ik bij [the professional services firm] zal altijd zijn economisch eh, aangezien wij geen ziekenhuis zijn waar daadwerkelijk mensen van afhankelijk zijn. Dus ik denk dus economisch en afhankelijk van hoe je het ziet kan het het verlies zijn van he, eh, het gaat natuurlijk een stuk verder. He, je hebt natuurlijk improductiviteit(0:43:14) of verlies van data of het weggaan van data, maar ja, als wij natuurlijk geen werk kunnen uitoefenen, zullen klanten als onprofessioneel zien en misschien niet meer bij je komen et cetera. Dat kan natuurlijk door blijven lopen. He, eh, wat nog wel kan schelen, kan gelden overigens, is ook het verlies van integriteit, eh, want als het hen lukt om bijvoorbeeld allemaal persoonsgegevens openbaar te maken eh, ja, dan hoeft het niet per se natuurlijk een economisch probleem te zijn he, commercieel probleem, maar zorgt het het er ook voor dat de privacy van mensen aangetast kunnen worden.

X: Ja-

Y: Kan natuurlijk ook wel weer een commercieel probleem hebben, dat je dan eh, als je het een beetje slecht gedaan hebt, terecht de AVG aan je broek op hebt, aan je broek hebt. Maar he, dat dan zeg maar, dan hebt je niet iets wat op die manier direct in geld uit te drukken is, wat wel echt een probleem is.

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

Y: Ja.

X: Hoe veilig is een VPN-verbinding?

Y: Eh, nou er, ervan uit gaande zeg maar dat he, dat alles wat men doet, men goed doet. Dus je zou vast een miljard instellingen hebben eh, die je moet kunnen uitvoeren. Dat is de beveiliging van de VPN-verbinding zelf he, dus dan hebben we het niet over het feit dat je met een ander netwerk verbonden bent, maar echt de VPN-verbinding zelf eh, is eh, even sterk als de manier van versleuteling. Dus maak jij of een fout met het versleutelen aan het begin waardoor iemand dus kan achterhalen eh, hoe je kan versleutelen of iemand zich kan voordoen als dat die jij hem bent eh, he, dus dan ontvang je alle informatie. Eh, is natuurlijk veel kwalijker als jij een manier van versleutelen hebt die eh, mathematisch te kraken is, waardoor dus iemand wel kan meelezen en je dus oorspronkelijke eh, eh, oorspronkelijke gevaar of oorspronkelijke dreiging weer terug hebt, namelijk dat alle informatie die je hebt ingelezen kan worden. Dus het hangt allemaal af van die twee factoren, dus implementatie en werking. Eh, in hoeverre je daarin kan variëren en natuurlijk daadwerkelijke eh, eh, rekenkundige sterkte van de versleuteling zelf.

X: Zijn er naast de versleuteling nog andere manieren waarop een VPN mogelijk niet veilig is?

Y: Eh, we hebben het natuurlijk al, we hebben het natuurlijk gehad he, we hebben het over de pure verbinding zelf gehad, we hebben het gehad over eh, andere configuratiezaken he, dus eh, he, als een VPN verbinding eh, ik noem maar wat, om wat voor reden dan ook vanuit meerdere apparaten gelijktijdig opgezet kan worden vanuit verschillende omgevingen en dat wordt niet gezien als iets vreemds bijvoorbeeld he, dan, dan, dan eh, zou dat iets kunnen zijn. Maar dan zitten we eigenlijk weer in een configuratie, dus ik kom terug he, geconfigureerd, dus op de manier dat eh, het alleen voor bekende users, bekende apparaten he, eh, werkt eh, op een manier waarop die initiële eh, wachtwoorduitwisseling goed gaat met een beveiligde verbinding, denk ik niet dat er andere manieren zijn waarop een VPN-verbinding veiliger of onveiliger ingericht kan worden.

X: Oké. En eh, je hebt enkele manieren genoemd waarop een VPN-verbinding mogelijk onveilig is, of minder veilig-

Y: Hmhm.

X: Veranderen jouw handelingen hierdoor?

Y: Nee, want ik heb als eindgebruiker eh, weinig invloed op. He, stel dat, dat eh, he, laten we beginnen met het meest voor zichzelf sprekende, dat eh, de type versleuteling van een VPN-verbinding slecht is he, mathematisch te kraken, ja, dan kan ik nog steeds niet niet gebruik maken van die VPN, want ik heb hem nodig om het werk uit te oefenen. Wat natuurlijk wel kan zijn is he, stel, dat tweede, stel dat ik weet dat het op ons van toepassing is, zal ik gezegd van oké, he, dan ga ik ook niet meer mijn eigen mail bijvoorbeeld benaderen vanuit eh, [the professional services firm] he, vanuit mijn werklaptop, want ik weet niet of iemand dat kan meelezen. Maar ik kan er zelf weinig tegen doen natuurlijk. Eh, als ik geen controle heb. Het enige wat ik kan doen is mijn wachtwoord invoeren. Eh, dus ja, als eindgebruiker zal ik waarschijnlijk wat ander gedrag vertonen, omdat ik dan he, puur alleen eh, eh, het verkeer eh, hoe noem je het, het verkeer beperk tot het hoogstnoodzakelijk, hoogste hoogstnoodzakelijke he, en indien er geen andere manieren zijn. Eh, maar voor de rest blijf ik gebonden aan het feit dat ik moet kunnen werken, aangezien mijn werkgever dat ja, op prijs stelt. Laten we het maar zo noemen.

X: Ja, en doe jij dat ook? Maak jij alleen gebruik van het hoogstnoodzakelijke dingen met VPN-verbinding?

Y: Eh, nou ja, dat gaat om twee aannames in. Ja, er zijn zaken die ik he, en dan he, het klinkt misschien heel deur opener, is helemaal niet zo, maar die ik gewoon überhaupt niet doe op mijn werklaptop. Eh, he, bepaalde sociale websites en dergelijke, eh, en dat heeft misschien niet iets per se met de beveiliging te maken, maar omdat ik het gewoon onprofessioneel vindt dat je ook een klein beetje die brandbreedte moet beperkt moet houden. Mocht ik nou weten bijvoorbeeld dat de verbinding niet veilig genoeg is, dan zou ik bijvoorbeeld ook niet meer snel even paar mailtjes van mijn eigen eh, eh, via het internet benaderbare mails beantwoorden en dergelijke. Eh, maar voor de rest, ja, ik gebruik hem op die manier niet voor het hoogstnoodzakelijke, ook omdat het bijna eh, niet te doen is. Want je moet gewoon soms dingen regelen en je moet soms dingen opzoeken. Eh, anderzijds gebruik ik hem niet als een vrije verbinding, dus ik zit er tussenin. Wat ik wel gedaan heb-

X: Oké. Ja.

Y: En zeker toen aan het begin van de coronacrisis, he, toen was het ook zo dat onze capaciteit niet zo heel erg groot was, toen heb ik wel eigenlijk een VPN alleen maar gebruikt echt op het moment dat ik met het [the professional services firm] netwerk verbonden moest zijn. Dus in dat eigenlijk een gouden zet gevonden dat eh, eh, onze mailserver geen VPN meer nodig had en daardoor hoef je ook dus niet constant verbonden te zijn met de VPN-omgeving. Eh, en nu nou ja, we zeggen het eigenlijk wel, maar als ik erover nadenk moet ik eigenlijk toch terugkomen, want ik zet nu de VPN eigenlijk ook alleen maar aan als ik echt specifiek intern systeem nodig heb. Dus ik gebruik het eigenlijk wel voor het hoogstnoodzakelijke, ja. Haha, bedenk ik mij nu, want eh, ik heb hem vandaag nog niet aangehad.

X: Oké. Eh, dan waren dit tot zo ver mijn vragen-

Y: Hmhm.

X: Zijn er dingen over VPN die wij niet besproken hebben nu?

Y: Eh, even kijken, ja, er zullen vast wel dingen zijn. Er zullen vast ook een miljard dingen zijn die ik niet weet over VPNs. Eh, ja, ik denk het eigenlijk niet, het is geconfigureerd, het is ingesteld, we loggen in, we maken een verbinding, we gebruiken het ergens voor, we hebben gesproken over mogelijke aanvalsvectoren, factoren, wie het kunnen zijn, welke kwetsbaarheden zouden kunnen eh, eh, misbruiken en hoe we het zouden kunnen oplossen. Ik denk het niet, denk ik.

X: Oké. Dan was dit tot zo ver het interview.