# Transcription expert 10

Duration: 40 minutes

X: Dan begin ik met de eerste vraag van het interview. Kun je aan mij uitleggen wat een VPN is?

Y: Haha. Nou ja, kijk, ik denk dat een VPN heel lastig woordelijk eh, uit te leggen is, maar het komt erop neer dat het een soort van tunnel is naar een andere computer. Eh, waarbij jij vanaf jouw eigen device een eh, nou ja, als het ware een tunnel opzet die versleuteld is, die verkeer naar de andere eh, eh, server of eh, toestel versleuteld. En vanaf dan acteer je eigenlijk als het ware vanaf dat andere eh, toestel of server, hoe je het wilt noemen. Eh, en nou ja, dat heeft allerlei voordelen, maar in feite is de VPN dus de, de verbinding naar, zo zou ik hem omschrijven.

X: Oké. En kan je iets meer uitleggen wat je bedoelt met een tunnel?

Y: Eh, ja, eh, ik zou zeggen dat is een verbinding, zoals eigenlijk eh, iedere verbinding er een is. Maar deze versleuteld eh, het verkeer vanaf jouw eigen device tot en met eh, de server. En daardoor kun je als het ware als buitenstaander niet eh, het verkeer nou ja, lezen, of eh, nou, onderscheppen kan wel, maar je kunt er in ieder geval niets mee zonder het sleutelmateriaal. Eh, en omdat het dus om een afgeschermde eh, eh, verbinding gaat op die manier, spreken veel mensen van een tunnel.

X: Oké. En op wat voor manier is het versleuteld?

Y: Eh, uit mijn hoofd via public-private-key.

X: Oké. En je zegt dat de tunnel loopt tot de server, wat is een server?

Y: Haha. O god. Eh, een computer, haha.

X: Oké. En wat gebeurt er daarna met de verbinding? Na de server?

Y: Eh, hoe bedoel je?

X: Is de server het eindpunt van de verbinding?

Y: Volgens mij wel.

X: Oké. Kan je iets meer vertellen over deze server?

Y: Eh, anders dan dat die VPN moet ondersteunen, nee.

X: Oké. Prima. Dan de volgende vraag, waarvoor gebruik jij een VPN?

Y: Eh, binnen [the professional services firm] gebruik ik een VPN om eh, een verbinding op te zetten naar het [the professional services firm] netwerk. Eh, zodat eh, ja, mensen zeggen altijd zodat je verkeer veilig is, he. Eh, zodat ik veilig kan eh, eh, mijn email kan checken. Ik denk dat dat ook wel klopt, want in feite maak ik verbinding met de server van [the professional services firm], waarop al mijn applicaties draaien en eh, daar staat eigenlijk alle data op van [the professional services firm], dus als het eh, als het erop aankomt dat ik eh, nou stukken van [the professional services firm] wil inzien, en die zijn ook maar enigszins vertrouwelijk eh, dan gebruik ik een VPN, want dan heb ik inzage of dan heb ik de mogelijkheid om die stukken te bekijken. Eh, dat is eigenlijk waarom ik de VPN gebruik.

X: Ja, zijn er nog andere redenen waarom jij de VPN gebruikt?

Y: Eh, nou ja, waarom ik het gebruik niet. Ik denk dat [the professional services firm] een VPN afdwingt eh, omdat ze daarmee ook gemakkelijker kunnen inregelen dat ik bijvoorbeeld niet naar bepaalde websites ga waar ik helemaal niets te zoeken heb.

X: En hoe hebben ze dat ingeregeld?

Y: Dat hebben ze ingeregeld op die server waar ik verbinding mee maak, want als ik die VPN-verbinding niet opzet vanaf mijn laptop, dan kan ik wel bijvoorbeeld naar alle websites die ik wil. Nou, dat is niet helemaal waar, maar laten we even voor het gemak zeggen dat het kan. Eh, maar als ik die VPN opzet, dan maak ik dus als het ware verbinding eerst met die andere server van [the professional services firm] en acteer ik vervolgens als het ware als die server en dan heb ik ineens wat extra restricties.

X: Oké-

Y: Maar ook de voordelen van de eh, vertrouwelijkheid en de integriteit.

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

Y: Het meest basale antwoord is denk ik eh, ik maak een internetverbinding, vervolgens eh, start ik een programmatje op dat eh, dat de VPN-verbinding voor mij opzet en daarvoor maar ik gebruik van een gebruikersnaam, wachtwoord en eh, tokencombinatie. Nou, als dat goed lukt, dan wordt de verbinding voor mij automatisch opgezet.

X: Oké. En kan je meer vertellen over deze token?

Y: Ja, die token dat is eh, een token die via een RSA-algoritme wordt gegenereerd en eh, ik heb dat op mijn telefoon heb ik een app hiervoor geïnstalleerd, daar heb je uit mijn hoofd, iedere zestig seconden wordt die eh, token vernieuwd en eh, nou ja er zit wel wat latency op, op het moment van token op mijn app versus wanneer kan ik hem nog invoeren. Dus nou ja, wat ik daarmee bedoel is ik moet die token invoeren op mijn laptop, nou kan het in theorie zijn dat die token op mijn app net even vervallen is, nou dan kan ik hem nog wel eh, invoeren en wordt die als geldig gezien. Ik denk dat dat een seconde of tien is ofzo, dat durf ik niet met zekerheid te zeggen.

X: Ja. En je zegt dat het een app is, is er ook een andere mogelijke manier?

Y: Eh, ik meen dat de eh, hardware token nog steeds wordt ondersteund. Eh, eigenlijk is het principe dan hetzelfde. Je hebt een eh, ja, wat is het, een soort kastje, of een soort sleutelhanger eigenlijk. Eh, waarop eenzelfde soort token iedere zestig seconden denk ik wordt weergegeven. En dan wordt die vervangen door een andere token via ik denk hetzelfde RSA-algoritme eh, ik weet echt niet welke dat het precies is. Maar het is in ieder geval RSA en ja, verder werkt het mechanisme hetzelfde. Je moet wel aangeven of in die applicatie of ergens anders, dat weet ik niet eens meer, welke token je gebruikt. Eh, dus je moet wel ergens je token koppelen aan eh, nou, jouw laptop en jouw gebruikersaccount, anders zou je een willekeurige token kunnen gebruiken natuurlijk.

X: Ja. En op welke apparaten gebruik jij de [the professional services firm] VPN?

Y: Ik gebruik hem alleen op mijn laptop.

X: Zijn er andere mogelijkheden?

Y: Nee, dat is niet waar trouwens. Ik gebruik ook een VPN-connectie op mijn eh, op mijn telefoon. Maar dat werkt net even wat anders. Eh, volgens mij kun je ook eh, en dat is via dezelfde VPN-connectie, via eh, IPad, tablet, kun je ook VPN-verbinding opzetten. Die VPN-verbinding via telefoon die werkt op een andere manier trouwens, dat werkt via Citrix. Eh, ik weet niet uit mijn hoofd of dat technisch een VPN-verbinding is eerlijk gezegd.

X: Oké. En hoe werkt een VPN? Als je wilt kun je hiervoor ook het whiteboard gebruiken. Ik zal mijn tekeningen weghalen.

Y: Hmhm.

X: En zou je mij dan kunnen uitleggen hoe een VPN werkt?

Y: Eh, nou laten we eh, ik ga gewoon een poging doen. [start drawing 10\_1]. Laten we zeggen, o, je kon ook typen, he. Even kijken. Werkt dat zo, nee. Even wat dingen aan de kant zetten. Bij mij werkt het typen van de tekst niet.

X: Als je op de T drukt, dan is het ook als het ware alsof je een vierkant moet trekken en dan kan je daarin typen.

Y: O, nu doet die het wel. Nou, oké. Eh, nu doet die het weer niet en nu weer wel. Oké. De VPN server. Eh, dus eh, je zit als het ware eerst een eh, nou, je hebt eerst verbinding nodig met het internet. Kunnen we het internet ook nog intekenen toevallig. Ja, dat kunnen we. Wolkje, ofzo. Eh, dus wat je doet is eh, je zet een verbinding op eerst met het internet, dat is eigenlijk tot hier. En vervolgens eh, benader je de VPN server met eh, jouw inloggegevens. Dus in mijn geval is dat een gebruikersnaam een eh, wachtwoord en een token. Eh, even kijken hoor. Ik doe dit niet dagelijks. Eh, even kijken. Goed. Je meldt je aan eh, vervolgens eh, heb je hier een soort van eh, nou ja, een bibliotheek waarin mijn gegevens dus ook staan, en heb je datzelfde RSA-mechanisme dat kan controleren van goh, is het [me] wel in dit geval. [start drawing 10\_2]. En als dat oké is, dan eh, gaat die gewoon weer terug, dan zegt die joh, je bent aangemeld. [start drawing 10\_3]. En vanaf dan eh, heb je een succesvolle VPN-verbinding en gaat eigenlijk alles zo, via de server, en kun je vanuit daar doen wat je wilt.

X: Oké-

Y: Nou zit er een stap tussen. Eh, ik weet niet precies, ik heb hem er niet ingetekend, want ik weet niet precies waar die zit, maar je moet ook nog ergens een handshake maken van goh, welk certificaat gaan we nou eigenlijk gebruiken, welke versleuteling, welke versleuteling. He, want een verbinding is eh, deze initiële verbinding is natuurlijk als wel versleuteld eh, want anders zou ik mijn eh, inloggegevens direct over het internet versturen en dat lijkt me ook niet handig. Volgens mij zit er vooraf, zit er nog ergens een soort van eh, pingetje van mijn device naar de VPN server die dan zegt van hoi, ik wil verbinding gaan maken. Dan komt er volgens mij eerst nog een signaaltje terug van nou, dat is goed. Ik ondersteun deze versleutelingstechnieken. Laten we zeggen TLS 1.2 of whatever, en deze eh, cijferpers, noem maar op. Nou, vervolgens zegt mijn device volgens mij is goed eh, ik ondersteun ook deze eh, versleuteltechnieken. Ik eh, ik stel voor dat we deze techniek gebruiken en omdat dat er dus eentje is dat de VPN server ook is, stuurt die direct de publieke sleutel mee. Eh, vervolgens wordt er een berichtje teruggestuurd vanuit de VPN server eh, hoewel, nee, ik denk andersom. Ik denk dat de VPN server de publieke key terugstuurt eh, en vervolgens wordt er een eh, wordt mijn bericht, en dat is dus die eerste pijl, eh, met die publieke sleutel versleuteld, kan de VPN server het ontsleutelen, controleren en bericht terugsturen met goh, het klopt. En ook dat bericht is dan waarschijnlijk versleuteld. Eh, en vanaf dan heb ik dus een eh, dezelfde beveiligde eh, eh, verbinding en heb ik mezelf geautoriseerd tegen die VPN server.

X: Oké. En welke verbinding is dan eh, versleuteld?

Y: Welke verbinding is versleuteld. Eh, uiteindelijk alle zou ik zeggen, behalve dan de verbindingen die ik niet heb ingetekend. Dus he, waar het echt gaat om hoi, ik wil VPN-verbinding opzetten eh, dat is goed ik heb deze certificaten, dat zijn niet versleutelde verbindingen.

X: Dus alle lijnen, deze en deze-

Y: O, ja, en deze die eh, deze hangt ervan af. Maar dat, ik denk dat die niet onder de VPN-verbinding valt. Eh dit is eh, als het ware van goh, ik maak verbinding naar een andere website en als die andere website eh, geen versleuteling behoeft. Laten we zeggen dat het een HTTP eh, eh, protocol voor nodig, benodigd heeft, dan hoeft die verbinding niet versleuteld te zijn. Maar dan is het verkeer van VPN server naar die website en terug niet versleuteld, maar het verkeer van VPN server naar mijn device weer wel.

X: Duidelijk, prima, dankjewel. Dan een andere vraag. Wat is de invloed van een VPN-verbinding op jouw computerbeveiliging?

Y: Invloed van een VPN-verbinding op mijn computerbeveiliging. Eh, ik zou zeggen dat het mijn eh, beveiliging vergroot. Eh, omdat eh, nou ja, eh, ja, hoe zeg je dat, eh. Kijk, als ik vanaf een VPN-verbinding, maak ik verbinding met die VPN server. En vanaf dan lijkt het alsof ik eh, niet meer mijn device gebruik, maar lijkt het alsof ik de VPN server alleen maar gebruik. Dus is, dus denkt eh, nou ja, het andere eind van dit laatste pijltje denkt van goh, eh, een VPN server maakt verbinding met mij, terwijl eigenlijk doe ik dat. Eh, dus in die zin is alles wat aan eh, aanvallers en aanvalsvectoren op dit lijntje zit, eh, ja, die zijn eigenlijk gevaarlijk voor die VPN server. Maar voor mijn device direct niet. Nou, ik denk dat als je die VPN server uiteindelijk weet te hacken, dan is mijn device ook niet meer helemaal veilig. Maar ik denk in eerste instantie he, dus het direct eh, eh, voordeel is dat mijn device zelf wat meer beveiligd is.

X: En daarmee bedoel je dan dat jouw device meer beveiligd is, omdat je uiteindelijk het doel niet jou ziet maar de VPN server.

Y: Correct.

X: Oké. En hoe ziet het uiteindelijke device dan de VPN server in plaats van jou?

Y: Eh, o, sorry, ik krijg even een rare melding in beeld. Eh, hoe ziet het uiteindelijke device, ja, die ziet hier dan achter he. Die, ja, die kan gewoon kijken welke IP-adressen hebben verbinding met mij. Eh, en eh, die zal niet mijn eigen eh, device zien, maar die zal de VPN servers eh, IP-adres zien. Dus, ja, die, die gaat mijn device nooit zien. Tenzij eh, hij op slinkse wijze die VPN server weet te hacken en ziet dat er een VPN-connectie vanuit mijn device is onder andere eh, en dan zou die wel mijn device kunnen zien. Maar ik denk dat dat een scenario is dat eh, dat buiten beschouwing dient te worden gelaten. Eh, want dan is die VPN server gewoon niet meer veilig.

X: Ja-

Y: En dan is het hek van de dam zeg maar.

X: Ja, oké. En je zei eerder dat een VPN er ook voor zorgt dat je niet naar bepaalde websites kan gaan-

Y: Ja, maar dat is dan ingeregeld op de VPN server, als daar eh, bepaalde websites geblacklist zijn, dan wordt dat op die manier geregeld. Maar het is niet zo dat omdat ik deze drie lijntjes heb dat ik dan daardoor niet bepaalde websites kan benaderen. Dat heeft puur en alleen configuratie te maken van die VPN server.

X: Prima. En stel je voor dat je op een andere fysieke locatie bent-

Y: Hmhm.

X: Heeft het dat invloed op de, deze tekening? Op jouw VPN-verbinding?

Y: Eh, volgens mij niet. Eh, ik- Wat ik zeg, je maakt verbinding met het internet. Dat kun je eigenlijk vanaf overal doen. Eh, en dan kun je een, een verbinding aanmaken met een VPN server die ook overal op de wereld eh, staat. Eh, dus zodoende zou ik nu vanuit mijn huis in Nederland een VPN server in eh, nou noem eens een land, in [country] kunnen eh, zoeken. Eh, en, en, ja, dan kan ik vanuit daar verbinding maken met nou ja, wat vanuit [country] toegankelijk is. Eh, andersom kan ook. Ik denk ook dat ik vanuit [country] een VPN server, nou laat ik geen [country] zeggen, maar in eh, in [country] kan benaderen. Eh, en, en vice versa. En ja, vervolgens he, dat van die websites net dat moet je niet te letterlijk nemen he, want je kunt als websitehouder kun je natuurlijk ook zeggen van joh, ik wil geen verkeer toestaan vanuit IP-adressen vanuit [country]. Eh, dus tuurlijk kun je vanaf de VPN server kun je bepaalde websites blacklisten, maar je kunt als website kun je ook bepaalde IP-adressen blacklisten. Dus dat moet je altijd wel even meenemen. En andersom is ook het verhaal eh, misschien kan ik vanaf mijn persoonlijke device niet bij een bepaalde website eh, maar kan ik juist omdat ik met een VPN-verbinding connecteer eh, eh, kan ik wel weer bij bepaalde websites. Zowel intranet als eh, sorry- Zowel internet als intranet.

X: Ja, oké. En als je dan bijvoorbeeld in een openbare ruimte zit zoals een café, maakt het dan nog uit?

Y: Hoe bedoel je? Wat maakt dan nog uit?

X: Of, ja, verandert er dan iets aan deze tekening bijvoorbeeld? Of heeft dat invloed op je VPN-verbinding?

Y: Nou ja, kijk, ik denk dat het voor de tekening op zich niets uitmaakt. Eh, maar, kijk, op zo een internetcafé, daar heb je gewoon heel veel mensen die op hetzelfde netwerk zitten. Eh, dus, ja, ik zou er eigenlijk nog wat dingen tussen moeten tekenen wil het echt helemaal kloppen, maar daar is het whiteboard of te klein voor, of mijn teken skills zijn echt niet goed genoeg. Maar er zitten nog wat stappen tussen. Kijk, mijn device is op dit moment geconnecteerd met mijn eigen eh, eh, wifi-omgeving, met mijn eigen router. En in zo een internetcafé, dan heb jij eigenlijk hetzelfde. Dan verbind je met zo een router op een internetcafé. Eh, en is het maar de vraag of al dat verkeer binnen dat eh, ja, binnen het netwerk van het internet beveiligd is of niet. Kijk, hier thuis geloof ik het wel, want ik ben de enige die het wachtwoord weet en noem maar op. Maar op zo een internetcafé is het vaak wat anders, zitten veel mensen op hetzelfde netwerk, is het misschien wel of misschien niet een beveiligd netwerk. Eh, maar bovenal kan die eigenaar van die router of degene die die router heeft gehackt, whatever, die kan al het verkeer eh, heel zwart-wit gezegd, die kan het inzien. Eh, dus in dat geval is het wel handig als je zegt van nou, weet je eh, allemaal prima, dat mag die inzien, maar ik wil wel even een VPN-verbinding opzetten, want dan weet ik in ieder geval zeker dat eh, het verkeer vanaf die VPN server naar mijn device, dat is versleuteld. Want die versleuteling dat vindt plaats van device naar server en niet op router naar router zeg maar, of van firewall naar firewall, of eh, eigenlijk de verbinding zelf eh, ja, die is versleuteld, maar niet omdat het een versleutelde verbinding is, maar omdat de versleuteling plaatsvindt op het device en VPN server.

X: Ja. Oké, duidelijk. Eh, even kijken. Dan een hele brede vraag. Met wat voor digitale dreigingen heb jij als [the professional services firm] medewerker op een normale dag te maken?

Y: Eh, voor zo ver ik zie heel weinig. Eh, dus laat ik mij daar dan ook op beperken, anders moet ik echt gaan gissen. Eh, ik denk dat de digitale dreigingen die voor ons het grootst zijn eh, de phishing mails zijn. Eh, ik werk zelf niet vanuit eh, publieke eh, netwerken. Het enige wat ik doe is een persoonlijke hotspot opzetten eh, [0:22:52: till 0:22:54 has been omitted] en dan zelf alsnog een VPN eh, connectie direct opzetten. Eh, dus daar zie ik eigenlijk weinig risico's verder, omdat ze al gemitigeerd worden door de maatregelen. Eh, een ander risico dat ik zie is ja, verlies van eigendommen zeg maar, dus dat ik mijn laptop ergens laat liggen, of mijn telefoon of eh, wat dan ook. Eh, denk dat dat wel de meest reële dreigingen zijn op dit moment eh, waar wij direct last van zouden kunnen hebben. En, en ik geloof best dat eh, dat er nog verschillende partijen zijn die het [the professional services firm] netwerk bijvoorbeeld proberen te hacken of aan te vallen. Al dan niet via phishing. Maar daar zie ik zelf niets van. Op de phishing mails na dan.

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

Y: Nou, op het laten liggen van eh, spullen niet. Eh, ik bedoel dat doe ik zelf en nou ja, dan raken we data kwijt. Eh, maar ja, met of zonder VPN is dat sowieso het geval. Eh, ik denk dat eh, ja, omdat ik dus eigenlijk nooit met publieke netwerken verbinding maak eh, anders dan mijn eigen wifi eh, denk ik dat dat risico door VPN eh, ja, met of zonder VPN er ook nauwelijks is. Eh, als ik [0:24:28 till 0:24:34 has been omitted], ja, dan heb je wel datzelfde risico ook wat je ook in het internetcafé hebt, dus dat iemand gewoon mee zit te lezen op je, op je lijntje. Eh, ik weet niet of VPN daar nou eh, het grote verschil maakt. Eh, maar dat is meer, dat heeft meer te maken met de aard van de werkzaamheden die ik doe zeg maar. Eh, omdat dat over het algemeen toch al over een beveiligde connectie gaat. Dus ja, dan is het verkeer van mijn laptop naar eh, eh, [0:25:08 till 0:25:10 has been omitted] dat is eh, via een beveiligde eh, of een versleutelde eh, eh, verbinding. Het is anders als ik intern naar het [the professional services firm] netwerk wil vanaf een [0:25:21 till 0:25:21 has been omitted]. Maar daarvoor heb ik sowieso al een VPN-verbinding nodig, anders kan het niet.

X: Ja. En wat bedoel je ermee dat je over het algemeen al via een veilige verbinding werkt?

Y: Nou, eh, dat eh, de verbindingen die je legt die zijn vaak niet via een HTTP eh, verbinding maar een HTTPS-verbinding. Dus dan heb je al een versleutelde verbinding. We leggen geen FTP connectie, maar een SFTP of een FTPS verbinding. Eh, ja, zelfde heb je met telnet en SSH, telnet doen we niet, SSH wel, maar dat zijn allemaal al(0:26:03) direct al direct versleutelde verbindingen. Dus in die zin denk ik dat het eh, het risico beperkt is. Eh, en dat de VPN-verbinding eh, het risico wel enigszins zou kunnen mitigeren of nog meer mitigeren, maar eh, ja aan het eind van de rit, ja, zou het alleen denk ik echt een groot verschil maken eh, met zaken die van het [the professional services firm] intranet afkomen eh, naar eh, mijn device zeg maar. Maar wat ik zeg, daar heb je sowieso een VPN-verbinding voor nodig, omdat ik ja, het intranet zegt het al, het is een intern netwerk van [the professional services firm]. Daar kom ik vanaf het internet niet bij.

X: Ja. Oké. En dan zeg je dat je een persoonlijke hotspot gebruikt-

Y: Ja.

X: Als je- In plaats van een publiek netwerk-

Y: Klopt.

X: Gebruik je op een persoonlijke hotspot ook nog steeds een VPN-verbinding?

Y: Ja.

X: Oké-

Y: Al is het dan- Als is het maar omdat ik dan met het intranet van [the professional services firm] verbinding kan maken.

X: Ja. En wat is het verschil tussen je persoonlijke hotspot en het publiek netwerk?

Y: Hele goede vraag. Durf ik niet te zeggen eh, en, en misschien dat ik daarom ook wel eh, een VPN altijd alsnog opzet. Better-

X: Oké. Sorry?

Y: Better safe than sorry zullen we maar zeggen.

X: Ja. Oké. En dan als we nadenken over de verschillende dreigingen die je net opnoemde. Wie of wat is de aanvaller die de dreiging veroorzaakt?

Y: Werkelijk geen idee. Ja, goed, ik zelf als ik mijn spullen laat liggen, maar wie er dan wat mee doet durf ik niet te zeggen. En eh, ja, wie [the professional services firm] aanvallen, ja, ik heb daar wel mijn ideeën bij, maar nee, dat kan ik beter niet zeggen, want dat zou echt gissen zijn. Dat zijn resultaten waar je voor je onderzoek niets mee kunt.

X: Oké. En ik ga toch vragen, wat voor ideeën heb jij erbij?

Y: Nou goh, laten we dan eens concurrenten noemen eh, klanten wellicht eh, misschien een eh, een verdwaalde student die is afgewezen op een stage of op een eh, op een baan eh, ik denk niet dat de grote eh, statelijke actoren nou, die misschien ook wel trouwens, ons willen hacken. Ik denk dat statelijke actoren voor hele gevoelige dossiers misschien ook nog wel wat willen doen. Eh, maar ja, de, de, eh, hoe zeg ik dat, je komt niet zomaar bij eh, de dossiers eh, waarbij staatsgeheimen stukken worden opgeslagen. Daarvoor heb je weer extra beveiligingsmaatregelen die helemaal losstaan van een VPN-verbinding.

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

Y: Ja eh, ik zou het, het gebruikelijke zeggen. Concurrentie eh, denk ik, omdat ze willen kijken wat [the professional services firm] doet. Hoe wij bepaalde stukken aanpakken, wat we hebben gezien, wat onze strategie is, ja, de verdwaalde student of de scriptkiddie uit wraak eh, omdat het leuk is, verveelt zich, kan van alles zijn, wilt gewoon wat vandalisme eh, doen, beetje gekkigheid. Eh, statelijke actoren omdat ze staatsgeheimen van andere eh, landen willen eh, ontdekken eh, of gewoon kijken waar zwakheden zijn binnen andere staten eh, criminele organisaties wellicht omdat er geld te halen valt eh, ja, het kan van alles zijn. Maar ik durf echt niet in te schatten hoe groot per actor de dreiging is.

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

Y: Als in eh, studie of hoe bedoel je?

X: Ja, is er een soort basisniveau van kennis dat een aanvaller heeft?

Y: Eh, ja, weetje, het zal best wel iemand met een beetje technische affiniteit moeten zijn eh, wat ik al zeg, ik ben geen hacker eh, dus ik heb zelf niet de kunde om het te doen. Het is sowieso niet handig als ik het doe in mijn functie, maar toch. Eh, ik denk voor het meeste is wel wat technische achtergrond nodig en eh, ja, afhankelijk van eh, nou, hoe je omschreven wordt he, ben je de scriptkiddie of ben je de statelijke actor dan, dan is die bagage dat je meedraagt wat meer. Ik weet wel dat iedere type aanval eh, wordt steeds gemakkelijker om uit te voeren zeg maar. He, dus he, nou ja, waar het dertig jaar geleden onmogelijk was voor iemand op een zolderkamertje een DDoS aanval te doen eh, zou het er nu binnen vijf minuten kunnen initiëren. Zonder dat ik er de technische kennis ervoor heb. He, dus in die zin is de achtergrond die je nodig hebt, de technische achtergrond die je nodig hebt wordt wel steeds kleiner.

X: En waardoor is dat nu steeds kleiner?

Y: Eh, omdat die technieken eh, nou ja, door de komst van het internet eigenlijk publiekelijk bekend raken eh, dan heb je nog het eh, het darknet of het darkweb eh, waar, waar ja, aanvallen te koop zijn. Dus ja, het is gewoon makkelijker om aan een aanval te komen zeg maar.

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

Y: Eh, verandert de soort aanvaller door een VPN-verbinding. Dus als ik een VPN-verbinding heb, dan heb ik andere aanvallers wanneer ik dat niet heb, is dat wat je vraagt?

X: Ja. Of eh, ja.

Y: Ja, weet ik niet. Eh, ik denk dat je de scriptkiddie misschien wat meer uitvlakt. He, dus de, de, de huis en tuin hacker zeg maar. Eh, aan de andere kant eh, zo een persoon kan ook gewoon op [social media platform] kijken wie bij [the professional services firm] werkt eh, op basis van onze syntax voor emailadressen, die echt bijzonder simpel is, kun je echt naar verschillende mensen een mailtje sturen en kun je op die manier alsnog eh, eh, malware verspreiden binnen het netwerk. En daar doet de VPN-verbinding verder niets aan. Dus ja, weet je, ik denk het niet eerlijk gezegd. Ik denk niet dat het veel verschil maakt.

X: Oké. Maar maakt de VPN-verbinding in zichzelf, heeft dat wel invloed op de soort aanvaller?

Y: Eh, ja, ik zit even te denken of ik je vraag dan goed begrijp. Ik denk van niet, tenzij je dus in een internetcafé ofzo zit. Eh, of misschien zelfs [0:33:38 till 0:33:39 has been omitted]. Eh, kijk, je, je verkleint wel je, je exposure zeg maar. He, als je in een internetcafé zit, dan is iedereen in dat internetcafé is een mogelijke aanvaller, want iedereen zou in theorie met wat technische kennis mee kunnen kijken in jouw eh, verkeer als jij eh, geen versleutelde verbinding eh, gebruikt. Eh, en zet jij een VPN-verbinding op, ja, dan heb jij die exposure niet. Eh, he, maar dat ja, dat is dan ook het enige wat je er mee wint.

X: Minder exposure. Oké.

Y: Ja.

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

Y: Als ik een VPN-verbinding gebruik of niet?

X: Ja, of niet inderdaad.

Y: Ja-

X: Impact voor [the professional services firm] dan.

Y: Eh, de impact voor [the professional services firm], nou, dat zou kunnen zijn dat eh, dat er malware eh, binnen het netwerk wordt geïnstalleerd en dat kan dan weer leiden tot eh, tot downtime, dat kan leiden tot eh, eh, lekken van dossiers of persoonlijke data, dat kan leiden tot financiële eh, schade, dat kan leiden tot reputatieschade. Wat, wat langer doordreunt dan die eenmalige afkoopsom zeg maar. Eh, ja, ik denk dat eh, ja, de impact die kan echt verschillend zijn. En die kan afhankelijk van wat de aanval is kan die bijzonder groot zijn en kan eh, kan ook best wel eens wat meevallen.

X: Ja. Oké. En als we nu naar de VPN-verbinding zelf kijken, hoe veilig is een VPN-verbinding?

Y: Ja, die is net zo veilig als het eh, het algoritme dat gebruikt wordt om de verbinding te beveiligen.

X: Oké. En zijn er andere manieren waarop een VPN mogelijk niet veilig is? Of onveiliger?

Y: Eh, nou, wat ik al zei. Als je VPN server gecompromitteerd is dan heeft het weinig zin om zo een VPN-verbinding op te zetten, omdat je dan in de illusie leeft dat het een veilige verbinding is. Want uiteindelijk heb je alsnog een, ja, iemand die gewoon meekijkt in je verkeer. Eh, ik zit te denken van ja, als je eigen device ook gecompromitteerd is of niet ook, maar als je eigen device gecompromitteerd is, dan heeft het ook al weinig zin meer om, om een VPN-verbinding op te zetten, omdat je vanuit je eigen device dan het onversleutelde verkeer of al het binnenkomende verkeer onversleuteld alsnog kunt laten doorsluizen naar eh, iemand anders.

X: Oké. En kan je nog meer van dit soort voorbeelden bedenken?

Y: Wanneer is een VPN-verbinding nog meer niet meer veilig. Eh, nee, ik denk dat dit het eh, wel is. We kijken altijd alles redelijk simpel, he. Eh, een verbinding opzetten doe je tussen een initiator, in dit geval mijn device, als dat niet meer veilig is dan is het niet meer veilig. Je zet hem op met een doel, dat is de VPN server, als die niet veilig is, dan is ook niks meer veilig en als de verbinding niet veilig is, wat er tussenin zit, dan is het ook niet meer veilig. Dus eigenlijk heb je drie zaken waarop het mis kan gaan. Eh, en volgens mij is dat het.

X: Oké. Duidelijk. Even kijken. Eh, dan waren dit tot zo ver mijn vragen. Zijn er nu nog dingen eh, van VPN, die niet naar voren zijn gekomen?

Y: Eh, nou, nee, ik denk dat- VPN is een toepassing, een maatregel eh, maar ik denk dat het samenspel van maatregelen altijd ertoe leidt dat iets wel of niet veilig is. He, kijk, alleen een VPN-verbinding eh, nou, dat kan veilig zijn, maar wat ik al zeg, er hoeft maar een van die drie puzzelstukjes zeg maar, niet goed te zijn en, en je hebt er al niet zo veel meer aan. Eh, dus het gaat er altijd om welke maatregelen zijn er nou nog meer om eventuele restrisico's ook te mitigeren. En ik denk dat dat eh, met name van belang is. En ja, dat, dat is misschien het laatste wat ik erover kwijt wil zijn.

X: Ja, en dan zeg je restrisico’s, bedoel je dan de risico’s die overblijven na een VPN-verbinding al?

Y: Eh, ja, of, of risico’s dat eh, op het moment dat eh, he, het is een maatregel en als die maatregel niet meer goed is, ja, dan wil je niet dat je direct eh, bloot wordt gesteld aan het volledige risico dat die maatregel eh, beoogt af te dekken eh, dus daarom is dat goed om nou ja, in de ...(0:38:54) zeggen joh, per risico minstens twee maatregelen, ik denk dat het in cybersecurity niet per se opgaat en dat je nog meer maatregelen hebt. Maar in ieder geval iets wat preventief werkt nou, dat is een VPN-verbinding, maar ook in ieder geval wat detectief of reactief werkt, dat op het moment dat er iets niet goed gaat, dat het in ieder geval gesignaleerd kan worden en dat daar direct op geacteerd kan worden. Eh, en daarnaast, maar goed, dat is dan op het moment dat eh, dat als er sowieso een VPN-verbinding is, want wat ik al aangaf, een VPN-verbinding op zich is niet zaligmakend voor alle risico’s eh, zou je ook nog andere maatregelen moeten nemen.

X: Oké. Duidelijk. Zijn er verder nog dingen over VPN-verbindingen die niet naar voren zijn gekomen?

Y: Volgens mij niet.