# Transcription non-expert 2

Duration: 48 minutes

X: Wat is een VPN?

Y: Een VPN is een beveiligde tunnel waar je internet eh, verkeer overheen gaat zeg maar vanuit jouw eigen computer eh, gaat, gaat dat wat je over het internet verzendt via die tunnel naar een volgend punt. Maar goed, dat vanaf daar is het weer eh, die tunnel is natuurlijk wel beperkt tot je eigen computer. Het gaat niet door eh, zeg maar het is niet alsof je een email stuurt eh, en je hebt je VPN aanstaan dat dan de email door een hele tunnel van jouw computer naar de computer van eh, de server van degene die de email ontvangt gaat. Maar het is een stukje eh, beveiliging van jouw computer naar het internet, dan gaat het verkeer door die tunnel heen.

X: Oké. En je zegt dat de tunnel naar een volgend punt gaat, wat is dit volgend punt?

Y: Ja, dat weet ik ook niet precies. Ja, volgens mij, ik denk eh, tot het moment dat het echt zeg maar, ik denk tot aan de server.

X: Wat is een-

Y: De eerstvolgende server die je tegenkomt.

X: Wat is een server?

Y: Ja. Een server is eigenlijk gewoon een computer. Eh, en vaak is die server eh, volgens mij, nou, in dit geval sowieso zal het een server moeten zijn die verbonden is met het internet. Servers hoeven niet per se met het internet verbonden te zijn, maar in het kader van VPN eh, zou dat weinig zin hebben als dat niet zo is.

X: Ja.

Y: Eh, ja, een grote computer waarin data wordt verwerkt, opgeslagen en zo voorts.

X: Duidelijk. En u beschrijft de verbinding als een tunnel, wat bedoelt u met een tunnel?

Y: Ja. Ik zie het dan een beetje voor me als een soort beschermende hoes, die om de data heen gaat. Of ten minste, ja, dat, dat is, afgeschermd van eh, eh, ja, hoe ga ik dat eens even, eh, ik weet eigenlijk niet hoe ik dat beter moet, moet omschrijven als een tunnel. Ja, op de een of andere manier visualiseer ik het dan ook een beetje, maar-

X: Dat is geen probleem.

Y: Ja, als een soort beschermlaag, waardoor je die, waar zeg maar van buitenaf niet doorheen gekeken kan worden en waar die data dan doorheen gaat. In plaats van dat het gewoon open is. Op je computer. En ook het internet, nou ja, kijk, dat is natuurlijk wat betreft een- Als je een VPN gebruikt en je bent verbonden ... (0:04:15) naar je internetrouter en-

X: Ja.

Y: Daar op die internetrouter kan het anders worden ingezien, gaat alle data open doorheen, normaal gesproken. Maar als je het via een VPN tunnel stuurt, dan gaat het, dan is het vanuit die, vanuit die router niet toegankelijk. Dan is daar zeg maar die beschermende laag eromheen. Dus zeg maar degene die toegang hebben tot de router, kunnen dan niet zien welke data vanaf jouw computer daar overheen gaat, want daar zit die VPN tunnel dan omheen. En daar kunnen ze niet door.

X: Duidelijk. En op wat voor manier kunnen ze dat dan niet zien?

Y: Ik denk dat dat een vorm van encryptie is, maar zeker weten doe ik dat niet.

X: Oké. En waarom gebruik jij een VPN?

Y: Nou-

X: O, sorry?

Y: Nou, ik zit even te denken of het voor, ja. Een beschermde laag, het is niet zo dat de data die daar inzit dan geencrypt is, alleen die laag daaromheen. Maar ik weet niet of dat nou encryptie is of een ander soort techniek.

X: Ja. Oké. Waarom gebruik jij VPN?

Y: Nou ja, wisselend eh, voor mijn eigen gebruik is dus inderdaad om die data af te schermen voor eh, mensen die per ongeluk toegang zouden hebben tot eh, tot de router. He, tot dezelfde internetomgeving. [0:05:43 till 0:05:54 has been omitted], dus daar heb ik geen zin om mijn data onbeveiligd overheen te sturen, daarom doe ik dat zelf. Voor [the professional services firm] geldt, speelt die reden natuurlijk ook eh, voor zo ver he, als je gebruik maakt van een openbare internetverbinding. Overigens is het dan ook als ik het goed begrijp afgeschermd voor de internetprovider, die kan dan ook niet zien wat je doet eh, online, als je dat via een VPN verbinding doet. Eh, en verder praktisch gezien doe ik het ook vanuit [the professional services firm] omdat ik op die manier toegang tot [an internal page] enzovoort. Zeg maar een aantal functionaliteiten binnen [the professional services firm] werken alleen maar als je via de VPN verbinding hebt gemaakt. Die [the VPN of the professional services firm].

X: Ja. En je noemde kort ook een openbare internetverbinding, wat is-

Y: Ja.

X: De rol van de VPN hierin?

Y: Eh, zorgen dat eh, het internetverkeer eh, dat wat jij over die internetverbinding doet niet zichtbaar is voor anderen, gewoon het afschermen, in de tunnel houden, waar anderen niet bij kunnen. Want eh, nou ja, goed, je, je kan het ook wel zien als er demonstraties worden gegeven van eh, ik heb wel ook eens een demonstratie gezien in het theater dat eh, dat er werd gekeken naar hoe veilig iedereen met zijn dingen omging en dat dat gewoon eh, konden onderscheppen wat er eh, wat er allemaal eh, voor berichtjes, voor websites werden bekeken- Berichtjes verstuurd weet ik even niet zeker, maar in ieder geval de websites die werden bekeken en door wie en wat, wanneer eh, van mensen die op de eh, mensen die op de wifi hadden ingelogd eh, van de locatie. ...(0:07:48).

X: Ja.

Y: Ja, digitaal dan.

X: Zijn er nog andere redenen waarom jij de [the professional services firm] VPN gebruikt?

Y: Ja, praktisch dus, om de systemen eh, omdat dat een voorwaarde is voor toegang voor een deel van de systemen. Maar verder gewoon veiligheid, afschermen.

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

Y: Eh, binnen [the professional services firm] is dat eh, eh, de god hoe heet het, o, nou heb ik mijn password incorrect ingetikt, zo, nou kan ik even kijken hoe het ook alweer heet. Eh, dan ga ik naar de [the VPN of the professional services firm], daar vul ik dan mijn eigen wachtwoord in eh, dan pak ik mijn token daarbij, [access token provider] token, en dan eh, het nummer wat op dat moment op die token staat dat vul ik daarachter in en dan enter.

X: Duidelijk. Kun jij meer vertellen over deze token?

Y: Ja. Deze token eh, die verandert elke 5 minuten geloof ik, geeft die een nieuwe code eh, dus dat is dynamisch. Eh, het is daarom ook belangrijk dat de batterij vaak wordt vervangen, want als die een beetje achterloopt met het genereren van die code, dan klopt de code niet en krijg je geen toegang meer. Eh, het is natuurlijk in het kader van de veiligheid dat er steeds een andere code verschijnt, dat dat niet dezelfde code is steeds. Dus eh, op het moment dat iemand ook eh, je wachtwoord zou kennen, zonder die token daarbij is het waardeloos en andersom ook. Met alleen de token zonder het wachtwoord eh, ja, kan je niet eh, die VPN verbinding eh, kraken of eh, gebruiken. Want nou ja, goed, zodra je die VPN verbinding open hebt staan heb je natuurlijk gewoon toegang tot meer [the professional services firm] informatie dan je anders hebt. Dus dat is eh, dat is vanuit dat oogpunt ook heel belangrijk, met name vanuit dat oogpunt voor deze computer.

X: Zijn er verschillende soorten tokens?

Y: Eh, ja, ik heb een eh, fysieke token, maar je kan ook eh, je kan ook een token generator op je telefoon zetten.

X: Oké, beide opties zijn beschikbaar binnen [the professional services firm] ook.

Y: Ja.

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

Y: Alleen op mijn laptop. [0:10:43 till 0:10:45 has been omitted].

X: Oké. En kun je aan mij uitleggen-

Y: ...(0:10:53)

X: Sorry?

Y: Ik weet ook niet of het via de smartphone of daar überhaupt ook dezelfde functionaliteit voor beschikbaar is, maar goed. [0:11:00 till 0:11:04 has been omitted].

X: Ja. En kun je aan mij uitleggen hoe een VPN verbinding werkt? Ik kan mijn tekeningen hier even weghalen. En dan kunt u het whiteboard gebruiken als u dit wilt.

Y: Hmhm. [start drawing 13\_1]. Nou, ja, hoe ik het een beetje in mijn hoofd visualiseer, maar goed, of dat klopt, dat weet ik dus niet. Hallo. Nou. Eh, nee. Heb ik ook een gum?

X: Er is een mogelijkheid om eerdere handelingen ongedaan te maken door op het pijltje te klikken, alleen is de laatste lijn die je dan tekent het eerste dat-

Y: Ja, dat schiet niet op. Oké. Eh. Ja, ik denk dat dit dus dan de router is. Nou, die tools, dingen, is niet heel responsive.

X: O, oké, goed om te weten.

Y: ...(0:12:54) lijntjes blijf zitten.

X: Het is niet mogelijk om op een ander vakje te klikken?

Y: Nou ja, ik heb het nu eh, o. a. Nee, ik zit nou, a, oké. Ik denk dus dat dit de router is. Router, of de server, dat weet ik niet zeker. O, dit zijn colors, nee. O, dus je moet niet, juist niet op dat pijltje gaan lopen klikken in dat vakje, maar op het dingetje zelf. [start drawing 13\_2]. Eh, nee, o. Eh, eh. O, nee. Zoiets.

X: Oké. En kun je mij uitleggen wat alle onderdelen van de tekening zijn?

Y: Nou ja, het begint dus eh, op je eigen device. De PC heb ik die maar even genoemd.

X: Ja.

Y: En eh, dat wat je daar doet zoals dit he, we zitten nou in een online eh, omgeving. Eh, dus alles wat he, wat je dus online doet vanaf je computer, dat gaat niet open over je eh, richting het, richting de router en richting het internet, dat stukje is afgeschermd, dat gaat dus door die tunnel. Eh, zodat dat van buitenaf niet zichtbaar is voor anderen mensen die op die internetverbinding eh, op die router of eh, anderszins op die internetverbinding zitten. Ja, want er is natuurlijk ook dus de internetprovider die die toegang tot het internet verstrekt, die kan er evenmin bij. Dus dan is het waarschijnlijk tot de server van de internetprovider. Eh, waar die tunnel toe loopt, dat dat laatste punt is. En ja, op dat moment dat het het internet opgaat, dan eh, ja, dan, dan zijn die data niet meer afgeschermd. Volgens mij. Is dat zeg maar waar de bescherming ophoudt, daar ben je gewoon weer op het internet. En eh, afhankelijk van natuurlijk he, dan ben je weer afhankelijk van het platform of dat een eh, HTTPS heeft of iets dergelijks, dan gaat de bescherming verder, maar dit gaat alleen maar op dat stuk. Dacht ik.

X: Oké. En stel dat je nu verbinding maakt, of je wilt toegang tot een interne applicatie, hoe zou dat in deze tekening eruit zien?

Y: Eh, ja, dan gaat de tunnel misschien tot die interne applicatie. [start drawing 13\_3]. Dus dan zou hierbij komen, de interne applicatie. Dat dat ook gewoon op het eigen netwerk is, op de eigen server.

X: Ja. Oké. Zijn er verder nog dingen eh, die je weet van hoe een VPN werkt?

Y: Nou, denk het eigenlijk niet, haha.

X: En wat is de rol van een router?

Y: Eh, die, jemel, dat is het internetkastje. Eh, die dus de signalen vanaf jouw computer omzet denk ik op een manier dat ze het internet opgestuurd kunnen worden. Ja, of die die verbinding eh, het is het toegangspunt, nou ja, goed, eerst gaat er natuurlijk nog een stukje kabel richting het kastje in de straat vanaf je eigen router, daar gaat het dan de systemen van de internetserviceprovider op. Eh, en vanaf daar naar het wereldwijde web, het netwerk van computers. Waar we alles overheen sturen.

X: Dan nu een hele andere vraag. Wat is de invloed van een VPN verbinding op jouw computerbeveiliging?

Y: Eh, ik denk vrij weinig. Eh, ja, ik heb wel eens de illusie dat dat me dan ook een beetje beschermt eh, van buitenaf, nou ja, tegen hacken en dergelijke beschermt het niet. Op het moment dat iemand toegang heeft tot mijn computer en dat kunnen ze zich verschaffen of ik nou met een VPN of niet zit, nou ja, dat is afhankelijk van hoe goed ze kunnen hacken en de beveiliging op je computer zelf. Oe, wacht, mijn batterij is wel bijna leeg, momentje.

X: Ja.

Y: Eh, maar goed, ik hoop, ik heb dan wel een beetje de illusie dat er op het moment dat ik met het internet communiceer via een VPN tunnel, dat het dat dan ook iets lastiger maakt voor iemand van buitenaf die toch immers via het internet op jouw computer zal moeten komen. Eh, dat het dat wel lastiger maakt. Want hoe komen zij dan die tunnel weer in als zij geen eh, authenticatie daarvoor hebben en is die tunnel dan inderdaad de enige, op dat moment de enige toegangspoort tot jouw computer, nou ja, het is in ieder geval voor eh, maar misschien dat dat ook weer afhangt van of je netwerkblock hebt en of je dat aanhebt of niet. Maar goed, dat, dat zijn meer dingen dat ik hoop dat het ook iets doet, maar weten geen.

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

Y: Eh, ja, volgens mij moet je ook iets eh, verandert het ook nog iets aan je proxy-instellingen, maar dat weet ik niet precies. Maar ik heb in ieder geval wel eens gezien dat er iets was met een proxy en dat dat weer anders moest vanwege de VPN. Maar hoe dat eh, hoe dat precies zit, geen idee.

X: Wat is een proxy?

Y: Ja, dat weet ik eigenlijk ook niet, haha.

X: Oké. Nog een vraag over de tekening. Wat zijn deze lijnen hier, aan de bovenkant. En de onderkant.

Y: Ja, eh, dat zijn invloeden van buitenaf. Eh, mensen die willen kijken eh, ja, of ten minste, indringers. En die dan afketsen.

X: Oké.

Y: Ik ben denk ik een beetje geïnteresseerd door wasmiddelreclames en dat soort dingen, haha.

X: Haha, oké. En dan een andere vraag weer. Met wat voor digitale dreiging heb jij op een normale dag te maken?

Y: Ja, daar merk ik gelukkig heel weinig van. Eh, dus eh, nou ja, goed, je hebt natuurlijk wel eens phishing mails die je ontvangt. Eh, ik krijg ook wel eens een melding, maar eigenlijk is het bijna altijd een false positive dat er iets van een programma, dat mijn malware beveiliging me ergens voor waarschuwt. Maar vaak is dat gewoon eh, in het kader van een update van een programma wat ik gewoon gebruik en eh, wat eh, betrouwbaar is. Eh, ja, heel af en toe raakt mijn eh, mijn malwarebeveiliging ook wel echt eh, echt iets op. Ik heb wel eens iets voorbij zien komen van een eh, een cryptocoin-achtige scam. Ik weet niet meer precies wat dat was. Maar eh, dat dat in quarantaine werd gezet door mijn malwarebescherming, dacht ik dacht nou dat lijkt me wel heel goed.

X: Ja, zeker. En hoe verandert de soort digitale dreiging door een VPN verbinding?

Y: Eh, ja, je hebt dan minder, je hebt dan minder te maken met dreiging eh, qua eh, zeg maar, de dreigingen die, die op dat stukje waar de tunnel lopen spelen, daar heb je dan gewoon minder last van. Want normaal gesproken kan je daar dan ook gewoon worden bespioneerd en dat gaat dan niet meer. Dat is een van de makkelijkste eh, manieren om te hacken als ik het goed heb begrepen, dat je het internet eh, verkeer afvangt. Dat je gewoon eh, doet, dat een hacker doet alsof hij de, de router is, het wifi access point, en dat die gewoon het verkeer naar zijn eigen access point eh, omleidt en daar alles kan inkijken. En ja, daar heb je dan, nou goed, dan gaat je verkeer daar misschien wel overheen, maar het zit in die tunnel, dus dan kan de hacker er alsnog niet inkijken. Tenzij die daar weer bijzondere manieren voor heeft, maar goed, dat eh, daar moeten we maar op hopen van niet.

X: Verandert de dreiging ook nog op een andere manier door de VPN verbinding?

Y: Eh, niet dat ik weet. Nou ja, wat natuurlijk wel zo is, is een VPN, dat hangt er een beetje vanaf, een VPN verbinding is natuurlijk wel iets wat ook weer een dienst is van een derde partij. Eh, dus als die niet betrouwbaar blijkt, ja, dan heb je dus je afgeschermde internetverkeer altijd aan zo een derde partij beschikbaar gesteld en eh, je moet natuurlijk ook een beetje, ja, je moet daar dan ook weer een stukje vertrouwen hebben. Maar goed, als dat eh, onterecht blijkt te zijn, heb je dus je e-mailverkeer aan een onbetrouwbare derde partij ter beschikking gesteld. Dat is een potentiele dreiging.

X: Oké. Tot zo ver digitale dreiging. Heb jij ook te maken met een sociale dreiging op een normale dag?

Y: Nou ja, die phishing e-mails zijn natuurlijk een soort van social eh, hacking. Krijg ik niet vaak overigens. Eh, ja, als je in een openbare plek eh, zit, dan zou je mensen kunnen hebben die proberen mee te kijken op je scherm. Eh, ja, sociale dreiging, ja, als je je computer ongegrendeld achterlaat, is natuurlijk ook een stukje sociale dreiging voor de beveiliging. Eh, ja, ik ben heel eh, dwangmatig met eh, met het, het windowsknopje L, als ik een seconde wegloop van mijn computer. Eh, ja, dat zijn denk ik wel de grote sociale dreigingen. Ja, je kan natuurlijk zelf eh, meer sociale dreigingen creëren door allerlei dingen te gaan doorsturen naar je Hotmail of je Gmail of whatever. Eh, of via WeTransfer en als dat soort eh, appjes(0:28:05). Maar ik weet niet of dat onder sociale dreiging valt. Dat is meer gewoon je eigen eh, dat je zelf beveiligingsrisico’s creëert.

X: Ja, zeker. En hoe verandert de sociale dreiging door de VPN verbinding?

Y: Ja, niet. Eh, ten minste niet de voorbeelden die ik net noemde, wat dat eh, als iemand dan op die manier op je eh, op je device kan, ja, op de device is het allemaal aanwezig, daar verandert die tunnel niks aan. Eh, op het moment dat je het via een VPN tunnel op eh, op zo een filesharing platform gooit, ja, eenmaal op dat platform, is het gewoon daar en aldaar aan allerlei dreigingen onderhevig. Dus dat eh, nee, daar zie ik niet echt eh, hoe de VPN verbinding moet helpen. Het enige is misschien dat je, op het moment dat je, je moet actief die verbinding maken met VPN, misschien dat je daar een momentje zelf een beveiligingsawareness momentje ontstaat. Maar eh, verder zie ik het niet helemaal, beïnvloedt.

X: En wat bedoel je dat er een beveilingingswareness moment bestaat?

Y: Nou ja, je gaat toch eh, die handelingen ondernemen om met een VPN te verbinden eh, hoeveel mensen ook weten van VPN, of hoe weinig, iedereen weet toch wel dat het ...(0:29:45) beveiliging. Eh, dus dat dan zeg maar actief bezig bent met een beveiliging op je eh, op je computer voor je dataverkeer en dat je dan dus misschien ook wat meer eventjes van o ja, beveiliging is belangrijk achtig, onderbewust momentje hebt.

X: Oké. En als we nadenken over deze verschillende soorten dreigingen, wie of wat is dan de aanvaller die de dreiging veroorzaakt?

Y: Welke dreigingen? De sociale dreigingen of de dreigingen waartegen VPN beschermt of eh-

X: Alle dreigingen.

Y: Eh, ja, je hebt dan de dreigingen van hackerachtige dreigingen, mensen die echt op zoek zijn of een bot, whatever, die echt op zoek zijn naar informatie of naar eh, he, toegang tot eh, die zijn natuurlijk ook vaak eh, op zoek naar toegang tot betaalgegevens en dergelijke. Dus ja goed, kwaadwillenden die op zoek zijn naar eh, data die zij kunnen exploiteren. Eh, en andere dreiging is eh, het internet eh, service provider en wat die allemaal, een nieuwsgierige internet service provider die eh, die interessante dingen wilt doen met de data die over zijn netwerk gaan. Nou is dat, nou mogen ze dat inmiddels niet meer echt analyseren, niet deep packet inspection wat ze in het verleden hebben geprobeerd(0:31:36), maar misschien dat ze alsnog toch iets er mee doen, willen doen. Dan zijn er ook de eh, de dreiging van eh, van autoriteiten die eh, toegang willen tot die data en toegang afdwingen tot data via de internet service providers. Eh, he, of die dingen opvragen. Eh, trouwens VPN geeft vaak ook een ander IP-adres dacht ik. Tenminste, veel VPNs doen dat. Dus dat maakt ook weer eh, dat zorgt er voor dat de herleidbaarheid, dat er minder herleidbaarheid is van je, van je acties op het internet.

X: En wat is het gevolg ervan? Als de herleidbaarheid minder is?

Y: Eh, nou ja, dan kan je beter eh, dat wat, dat wat alleen jezelf aangaat tot jezelf houden. Of als mensen op jouw persoon willen gaan zoeken of willen gaan kijken wie een bepaalde actie eh, willen achterhalen wie een bepaalde actie op een platform eh, website, whatever heeft eh, eh, heeft verricht, kunnen ze dat niet zo makkelijk achterhalen wie dat dan is. Dus je bent eh, je bent anoniemer op het internet. Totdat je er een gebruikersnaam en weet ik veel wat er aan koppelt, dan eh, wordt het een ander verhaal.

X: En als we dan terugkijken naar de tekening, op wat voor manier eh, valt het stukje herleidbaarheid er dan in?

Y: Ja, dat is natuurlijk, dat heb ik er nog niet in verwerkt want dat bedacht ik me net pas. [start drawing 13\_4]. O, dus dan hebben we ook die PC eh, hallo, heeft de PC een IP-adres, en de router heeft ook een IP-adres, hallo, en dan geeft de VPN- Eh, o wacht, nee dat kan ik wel hier doen he. Hallo, nee. Dus eh, iemand die dan eh, hier naar kijkt, naar een van deze eh, datastroompjes wat jij doet op het internet, die ziet dan dit IP-adres, wat een IP-adres is dat is uitgegeven door de VPN en niet deze of deze. Dus die kan niet zien waar dat verkeer dan he, waar die handelingen dan vandaan kwamen. Ja, die komen dan uit bij een IP-adres van een eh, VPN dienstverlener en eh, daar loopt het dan dood.

X: Oké. En heeft de VPN dienstverlener in deze tekening een plaats?

Y: Nee, ja, die zit natuurlijk hier. Die maakt, die, die, die creëert die tunnel. [start drawing 13\_5]. Dus dat- Geen idee of het, of de VPN bij [the professional services firm] in eigen beheer is.

X: Oké. En we kwamen op dit onderwerp door te praten over hoe, of wat voor aanvaller achter een dreiging zit.

Y: Hmhm.

X: Hoe verandert de soort aanvaller door een VPN verbinding?

Y: Eh, dan verandert met name, ja, de locatie van de aanvaller. Dan gaan de aanvaller meer hier op het internetdeel zich richten, alleen werkt, nou ja, goed, afhankelijk van hoe goed je daar herleidbaar bent, kunnen ze dan nergens heen. Of ze gaan zich direct richten op jouw computer, maar ze richten zich niet meer op dat stuk eh, zeg maar dat stuk internet, router, internet toegangspunt en jouw computer. Zeg maar dat stuk daartussen dat eh, daar kunnen ze dan weinig meer uithalen. Dus de, de met een auto rondrijden en wifi signalen onderscheppen en proberen in die wifi eh, apparaten te komen, dat heeft dan geen zin meer.

X: En verandert de soort aanvaller nog op een andere manier door een VPN verbinding?

Y: Geen idee, ja, dan moeten ze de tunnel in zien te komen waarschijnlijk.

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

Y: Eh, ja, meestal eh, geldelijk gewin uiteindelijk denk ik dan echt, denk ik. Je hebt natuurlijk, ja, geen idee of bijvoorbeeld dingen als plaatsen van eh, eh, hoe noem je die eh, van bots die miningbots of iets dergelijks, of dat ook nog door een VPN wordt beïnvloed of dat dat wel gewoon kan. Moeten ze toch echt op je systemen komen. Eh, sorry, wat was de vraag ook alweer?

X: De vraag was wat de motivatie is voor een aanvaller.

Y: O, ja. Nou ja, uiteindelijk dus bijna altijd geldelijk gewin, ja, nieuwsgierigheid zou ook wel eens voorkomen. Eh, maar uiteindelijk is het gewoon een business. Denk ik.

X: Oké. En heeft een motivatie nog andere- Of heeft een aanvaller nog andere motivaties?

Y: Ja, dat hangt ervan af. Kijk, als het gaat om de ex die eh, haha, dat soort hacks heb je natuurlijk ook wel, mensen die eh, dus dat uit wrok of he, gewoon omdat je iemand persoonlijk wilt treffen. Ik denk dat dat wel echt een veel minder groot aantal is. Eh, ja, ja, er zijn, je hebt natuurlijk ook de aanvallers die simpelweg willen laten zien van he, dit is niet op orde. Je hebt ook ongetwijfeld ook hobby aanvallers, die gewoon willen kijken wat is er allemaal niet op orde en misschien dat ze dat vervolgens ook ...(0:38:59), maar misschien ook niet je hebt natuurlijk de white hat hackers, die hebben ook een ander motief. Eh, he, meer om aan de kaak te stellen, beveiligingsproblemen. Ja, en dan, en dan weet ik even niet of je eh, overheids eh, instanties die toegang willen ook als aanvaller moet zien, want die gaan meestal wel via de juridische route en niet via een aanval. He, er zijn wel enige terughack eh, rechten, maar ja, dan moet je ze eerst wel hacken. Of dan moet je eerst een hacker zijn om zeg maar teruggehackt te mogen worden. Dus ja, dat zie ik dan niet direct als een aanvaller. Dan een overheids eh, instantie die eh, eh, een autoriteit, justitieachtige autoriteit die toegang verzoekt. Via meestal de internetprovider.

X: En wat voor achtergrond heeft een aanvaller?

Y: Ja. Geen idee. Ze kunnen zichzelf eh, het een en ander hebben aangeleerd. Er zijn ook allerlei tools die je kunt eh, downloaden om allerlei hacking acties te kunnen uitvoeren. Eh, dus het hoeft niet per se een hoogopgeleid iemand te zijn. Het hoeft niet per se de, de grootste computerwhizzkid op aarde te zijn. Al zullen de echte goede hackers dat waarschijnlijk wel zijn. En qua achtergrond, ja, kijk eh, de Nigeriaanse prinsen die allemaal eh, die via allerlei email scams, via phishing prachtige erfenissen uitdelen, ja, dat zullen ongetwijfeld mensen zijn die zelf van een, ja, minder goede afkomst zijn zeg maar, van een vrij arme achtergrond komen. Maar goed, dat weet ik ook niet eh, weet ik eigenlijk niet. En hoogopgeleid ook niet per se. Het zijn gewoon slimme, dat zijn de slimme, manipulatieve mensen, maar dat zijn dingen waarmee ze zijn geboren, haha. Vaardigheden, als je het zo mag noemen. En eh, ja, en, en de hackers dat zijn eh, he, die echt op systemen proberen in te breken, qua achtergrond ja, dat kan van alles zijn. Ik denk, maar goed, ik kan me voorstellen dat, dat je je eerder geneigd bent om tot dat soort acties over te gaan, of zo een richting te kiezen als je zelf minder goed af eh, bent. Dus dan toch van een armere en meer uitzichtloze afkomst bent. Al kan het ook natuurlijk zijn dat je het gewoon leuk vindt en makkelijke manier eh, om eh, een makkelijke om interessante manier om aan geld te komen en dat je dat gewoon verkiest boven een regular job. He, dus achtergrond van die mensen, ja, kan van alles zijn denk ik. Maar het zullen geen mensen zijn denk ik met een goede baan, want eh, dat slokt dan al je tijd op en dan heb je geen tijd om daarnaast nog eventjes te gaan zitten hacken.

X: Oké. En wat zou de impact voor [the professional services firm] van een aanval kunnen zijn?

Y: Ja, enorm natuurlijk. Omdat er gewoon heel veel vertrouwelijke eh, gegevens binnen de systemen van [the professional services firm] aanwezig zijn. De eh, ja, alle cliëntdossiers, alle e-mailcorrespondentie, zo veel vertrouwelijke informatie. Dat zou echt, dat kan desastreus zijn. Als daar toegang tot wordt verkregen. Ja, dan is het vertrouwen, dat heb je allerlei confidentiality obligations waar je, waar je problemen mee hebt. Dus contractuele aansprakelijkheden eh, buiten het feit dat je reputatie naar de haaien is en eh, en alle klanten waarschijnlijk weglopen. Want op het moment dat je informatie niet veilig is bij [0:43:12 till 0:43:17] eh, maar goed, betrouwbaarheid en vertrouwelijkheid is natuurlijk ook een eh, heel belangrijk element. Ja, dat, afhankelijk van hoe ver de aanval gaat he, tot waar de aanval eh, weet te doordringen, desastreus.

X: Oké. En kan eh- Als we naar de VPN verbinding zelf gaan kijken, hoe veilig is een VPN verbinding?

Y: Ik heb geen idee hoe veilig deze VPN verbinding is of hoe veilig een VPN verbinding in het algemeen is. Het wordt altijd verkondigd dat dat de manier is om eh, om je internetverkeer eh, af te schermen, maar of dat nou helemaal ondoordringbaar is, dat weet ik niet.

X: Oké. En zijn er manieren waarop je kan denken waardoor een VPN verbinding niet geheel veilig is?

Y: Nou ja, net zoals dat je op andere systemen kunt eh, kunt inbreken, kan je waarschijnlijk ook op een VPN tunnel inbreken. Ik bedoel overal zijn zwakheden, dus waarschijnlijk ook in die, die schil die daarom heen zit.

X: En als je nadenkt over deze onveiligheden, veranderen jouw handelingen hierdoor?

Y: Eh, nee, want dit is vooralsnog het enige wat ik voorhanden heb hiervoor. Dus ja, als er geen ander alternatief is, eh, ja, dan ga ik ook niet eens op zoek naar eh, van goh, is het allemaal wel 100% veilig, want ik kan niet, niets anders doen.

X: Ja.

Y: Behalve ja, behalve al je verkeer eh, apart nog een encrypten, maar goed, dan weet ik ook niet waar ik moet beginnen. Behalve dat je altijd dan via HTTPS eh, moet werken, maar dan heb je nog steeds dat stukje zwakheid van jouw computer. Want dat HTTPS begint natuurlijk pas op dat platform. Daar moet je dan eerst nog heen. Of nou, nee, HTTPS gaat misschien wel verder dan dat. Nou ja, dus dat eh. Ja, dat is het lastige, ja, dan ga je misschien meer focussen op HTTPS, zorgen dat je alles eh, op die manier ook afschermt. Dus dat je dus, nou goed, nou zullen de meeste online platforms hebben dat ook wel, meestal is het toch op het platform veilig, afhankelijk van de aanbieder die daarachter zit.

X: Oké. Dit waren tot zo ver mijn vragen.

Y: Hmhm.

X: Heb jij nu nog dingen van een VPN verbinding waar we het niet over hebben gehad?

Y: Nee, er schiet me nou niet direct iets te binnen. Ja, ik vroeg me nog af dat ik dacht van goh, is er ook een risico dat die VPN verbinding, dat die hele tunnel wordt verlegd, dat het ergens anders heen gaat. Maar eh-

X: En hoe bedoel je dan dat die ergens anders heen gaat?

Y: Nou, dat het eindpunt hier verandert. Oftewel dat het alsnog via, ja, als je dit weet te, weet te kapen, dan kan je ook de data die eruit komt misschien naar je eigen punt, naar je eigen internet access point leiden, en het daar alsnog aflezen. Dat weet ik niet hoor, maar goed dat eh, is iets wat ik me ineens bedacht.

X: Duidelijk. Zijn er verder nog andere dingen?

Y: Nee.

X: Oké. Eh, dan waren dit dus tot zo ver mijn vragen en dit gedeelte van het interview. Heb jij nog vragen voor mij?

Y: Eh, ja natuurlijk, het antwoord op alle vragen wat jij, die jij mij gesteld hebt, haha. In plaats van mijn gissingen.

X: In kan eh, in eerste instantie zal ik even de opname stoppen.