# Transcription expert 5

Duration: 58 minutes

X: Could you explain to me what a VPN is?

Y: Okay. Eh, so, eh, I would not classify myself as an expert to know about VPN, but the way I understand VPN is like, a narrow, or more like secure tunnel to this internet traffic online, where the provider and the receiver of information have a secured connection. So, it is like shielding a que of tunnel through the rest of the internet traffic. That is how I understand VPN.

X: Okay. And could you explain what you mean with a tunnel?

Y: Sorry, I am having a bit of- Okay, so, eh, let me try if I can draw something. [Start drawing 5\_1]. What I mean for example is here is the receiver, eh, there is a secured connection established between the receiver and let's say an organization that is providing their IT landscape. So, the people that are from external eh, yeah, environment who do not have access to this tunnel or environment, will not be able to decipher what is being transferred through this channel. This is what I am referring to as a tube. Eh, but it, it's like a way of isolating yourself from the rest of the environment of internet, that we call like a broad entity where information is freely available. If you want to have a secure connection, then VPN is what most of the companies prefer to go for. But this is how I understand what a VPN should be. I am not familiar with the technical term, but I do understand how it works.

X: Okay. And you say it is secured. How is it secured?

Y: Eh, okay, that's quite a good question. So, I am not quite certain how it is secured in terms of technical terms. Eh, but I know that eh, for example the provider of VPN in this case is an entity, it identifies its provider based on certain parameters. [Start drawing 5\_2]. I don’t know. Like the credentials for example eh, or there is two-factor identification for example. Eh, so, that kind of things. But I do not know what kind of encryption for example works to keep it isolated from other eh, eh, yeah, other attack, well not attack, but other actors. But this is how I understand it. Sorry, I cannot fill in much eh, here.

X: This is quite a lot actually.

Y: Okay.

X: And in what way does the encryption work?

Y: Eh, so, well, there are numerous ways of encrypting, but one of the ways is to obscure the information, or replace them with meaningless eh, how do you say, but eh, yeah, set of letters. [Start drawing 5\_3]. Let’s say one, a, c, b, for example. Yeah, basically replacing a whole sentence with a short encrypted eh, 256-bit of this long strings of mindless characters. And then you have to have a key to decipher what this actually means. So, this is what I understand encryption is. So, if you want to transfer information, this would be one way of transferring to the tunnel.

X: Could you explain to me what this and this is in your drawing?

Y: So, in this case I will say this is me. Sorry I am very bad at writing in this. In this case this is [the professional services firm], who is offering let’s say our VPN, that we call [the VPN of the professional services firm]. Eh, if I want to connect to [the VPN of the professional services firm], I will have to first access eh, yeah, the remote connect application where I have to identify myself, say this is my credentials. I think, once I enter those credentials, it also validates that these credentials are valid, only then I get access to this secure channel that is eh, VPN.

X: Okay. And earlier you also mentioned the IT-landscape, what do you mean with an IT-landscape?

Y: Well, so, let’s say, [the professional services firm] has a bunch of applications in its landscape, let’s say [an internal page], for example. [0:07:24 till 0:07:29 has been omitted]. These applications are not really accessible without a VPN. So, I can use internet without connecting to VPN. So, I have a broader channel to the rest of the internet, but if I want to access [the professional services firm] infrastructure, which is basically these applications, our clients’ documents are there, [0:07:45 till 0:07:47 has been omitted], eh, mainly sensitive information. Then I have to access it through this channel. So, I was referring to this as the [the professional services firm] IT-landscape eh, where the applications offered by [the professional services firm] can only be accessed through this channel. If I am not located in [the professional services firm] network.

X: Are there purposes for which you use the VPN?

Y: Eh, I am not quite certain. While I personally do not use it for any other applications, because I only have eh, well, [the professional services firm] VPN, [0:08:21 till 0:08:31 has been omitted]. But I can imagine other applications, like yeah, if you want to access, let’s say, eh, if you want to eh, yeah, mask yourself as being someone in a different location eh, ...(0:08:44) applications, we can always do that eh, by replacing your eh, IP for example. Eh, I can imagine you can also use VPN for that purpose. Eh, by obscuring your location where you are located.

X: How would it work if you mask your IP?

Y: Eh, well, eh, okay, I do not know the specifics, but I will try. [Start drawing 5\_4]. So, if, let's say, if I am located here in the Netherlands, eh, I have a specific IP assigned to it. A VPN will allow me to rout my access to the internet to a different location, to let's say Malaysia, or to China, eh, I do not know if it's possible. Eh, to all these- And then I am able to access another connection, which I do not want them to track me back to The Netherlands, or I want to access eh, data, that is in this country specifically. Let's say [company] eh, in the US for example, it is only available to content in the US. An IP, then in that case, I might be able to access yeah, the network, or the content in the US, by masking an IP which is located in the US, or subsidiaries. But this is just in a very layman's term.

X: Thank you. And are there any other purposes for which you use the [the professional services firm] VPN?

Y: Eh, I am trying to think eh, no. So, that is the purpose, I do not use the [the professional services firm] VPN for any other purposes. I am not sure if you can use it for any other purposes though. Eh, so.

X: And is it location dependent or time dependent when you use VPN?

Y: So, it is not time dependent, but I think it can be location dependent, but not in a way that we might understand it. So, I think our [the professional services firm] server for Europe are located in [place]. So, generally when we connect to VPN, when you open Google, the first reference is [place], where our datacenter is located. So, I can imagine that the VPN is connecting us to the VPN in [place], and then we are able to access [the professional services firm], eh, [the professional services firm] infrastructure. Eh, but it doesn’t depend on the country I am located in if I am able to connect. If I have my credentials with me, so, we generally have a [access token provider] token on our phone, which is a multi-factor authentication mechanism that [the professional services firm] uses, if I have my phone, I should be able to connect it to the [the professional services firm] VPN, even if I am in North-Korea for example. So, it is not really location dependent or time dependent.

X: Okay. And could you tell more about that token?

Y: Token, yes. So, eh, it is eh, well, right now I have a software version, but you can also get a physical version. But all it does, it spits out a six-digit number eh, which eh, I forgot the English, but it replenishes itself every one minute eh, that number is specific to my ID. Eh, I am not sure what kind of algorithm they use in that number eh, I think some combinations makes it recognizable that [me] in this case is trying to log in. And this is a number, is this number valid, yes, then it allows me to enter. So, if I am to log in using let's say my colleague’s [access token provider] token, it will not work, because the user ID and the number that is entered using the [access token provider] token will not match. But I think this is, this is very specific for employee eh, that they configure the [access token provider] token per employee and the user ID.

X: And on what devices do you use [the VPN of the professional services firm]?

Y: Eh, I use [the VPN of the professional services firm] only on my laptop. Eh, if I have to access [the professional services firm] infrastructure like I said before, to my mobile phone, then we have a special application eh, yeah, I forgot the name, let me quickly look it up. Yeah, it's called [example of mobile application], [example of mobile application] is like a VPN for phone, but once you log into [example of mobile application], you are actually able to access [an internal page], etcetera, only to that portal. So, it doesn’t work through web browsers, but there are specified browsers in there that are installed and connected to [example of mobile application]. The [example of mobile application] is like, yeah, it validates your ID and it validates the device on which it is running. Whether it is [the professional services firm] provided device, or it is a device for your own. Eh, if everything goes well, you are able to access it through your phone. If not, if it cannot validate your identity, it will not run. And then we have to use [example of mobile application] to authenticate ourselves on our phones, but it is only one-time process.

X: Okay, eh-

Y: Eh-

X: Sorry, is there anything else you want to add?

Y: No, no, sorry.

X: If we go back to your drawing-

Y: Yes.

X: You say this is you and this is [the professional services firm], could you tell a bit more about how that connection is established?

Y: Eh, can you be a bit more specific? How do you mean how is the connection established? Eh, so, what exactly should I elaborate on?

X: So, if you establish a connection, you said you use software, where in this drawing would we find that software?

Y: Okay, okay. Eh, okay. So, maybe I can try, draw a little bit over here.

X: Or I can provide a new slide if you would like.

Y: Okay, that's also great. Okay, thank you for that.

X: We can go back to the previous slide if you'd like as well.

Y: Okay. Eh, I can't draw anymore, eh-

X: One moment.

Y: Okay, yeah. [Start drawing 5\_5]. So, yeah, this might be a very childish drawing, but let's say this is my laptop here eh, my laptop is connected to Wi-Fi that is in my house, eh, and [the professional services firm] is providing their services accessible to web- to a channel. In addition, I need to have my telephone, eh, the app is installed on the telephone. So, what I have to do is when I log into [the professional services firm] network, whenever I have to access the [the professional services firm] infrastructure. Eh, first I have to enter my user ID, after that I have to enter this token ID, that will be generated here, once I open the token it will give me a random number, the random number enters, presented here, and then the information is send over to the router, to [the professional services firm], saying this guy is [me], or whatever my ID is, and this is the token, [the professional services firm] performs some calculations or validates that the ID is correct, because it is the two-factor authentication and then it is send back he, this is okay. And then there is a message that pops up on my screen that says I am connected. And after that I should be able to access all the applications in here. So, this is how I am connecting myself. And this works, not just my home Wi-Fi, but also works with Wi-Fi at a cafe, or any other place. As long as I have an internet access, I should be able to connect to [the professional services firm] eh, through the same procedure. Or there is an alternate way if people don’t want it on their phone eh, or have dinosaur technology, it is also possible to have a token eh, this is a physical token. Eh, all it does, it has a small 16-bit display, like we used to have those in ...(0:16:36). And it would do the same thing, it will display random numbers that will keep changing every one minute. If you have this token as well, this token is assigned to your name, you can enter the name here, sorry, enter the number here and then it works the same way.

X: Clear, thank you.

Y: You're welcome.

X: And now on a different topic-

Y: Okay.

X: What is the influence of a VPN on your computer security?

Y: Eh, well, I think eh, I am a bit scared to use VPN from public places eh, like, if I am sitting in a barista café like, [example of restaurant] for example, I am quite worried to use VPN eh, to their Wi-Fi network. Eh, but I am not sure whether that has any impact on my computer security. Well, in a way I am worried that someone tries to target my system, just because I have sensitive information and I am connected to a publicly accessible network, which may or may not be very secure. So, those are my top. So, what I always prefer to do is, I try to use the mobile phone internet, that is provided by [the professional services firm], eh, to, by connecting to a hotspot. I think that calms my nerves a bit. Eh, I know there are a lot of hacks possible from a network which is not secure, especially when you're connecting VPN and that is eh, so, yeah, so, it influences my thinking and my mind and how much I am worried to access it through public eh, publicly available network.

X: Why are you scared to use VPN in a public space?

Y: Eh, yeah, because I am partially aware of the kind of attacks that are possible. Eh, I do not know if someone will try to listen or look at the traffic that is going through the channel, if the, if the internet that I am connecting to is not secure. I do not know how, for example, the cookie and the communication logs are stored. Eh, either way, I am not sure who the Internet Service Provider is for the café, how secure they are, what are their security measures, et cetera. So, all these things really make me worried a bit. I do not know the technical specifics of how a person can attack, but I know it is possible. And hence, the worry that, because I have sensitive information on my laptop, I prefer not to connect to a publicly available eh, network.

X: And then you connect to a hotspot you say.

Y: That is correct.

X: And what is the difference between a hotspot and a public network?

Y: Well, first, the hotspot is provided by eh, a network that is approved by [the professional services firm]. Eh, so, either way there are certain, let's say, contractual obligations, that are in place. I am not sure if for telecom providers it matters if they have a contract with let's say, [the professional services firm] or anyone else, the security will be different. Eh, but, yeah, so, the difference is, I have right now internet connection through [telecom provider]. So, [telecom provider] is the preferred service provider for [the professional services firm]. I can imagine [telecom provider] taking extensive measures to make sure their, the internet that they are providing through the phone is secure and it is not easily crackable. Because of their application and ...(0:20:08). I do not know if a small café in a corner uses an internet provider, a service provider that is not really very robust. They do not have proper architecture. Eh, are they, you know, just cheaping out and paying more, just to have a proper security and just making internet available to people who want to do it. So, those kinds of things.

X: Okay. So, you mean in general you do never use eh-

Y: Publicly available Wi-Fi. Eh, yes. So, if I find Wi-Fi- Well, I mean, in dire need, when there is really nothing that is left, I generally know when the times are bad and you really have to get something done, your data on your phone is gone, than you have no other way. But, if I have an option, I will always tend to avoid it.

X: And you would definitely not use VPN if you're connected to the public internet connection in that case?

Y: Eh, no. Then I will, well, in the past I have done that once or twice, when there was an emergency and my phone wasn't connecting properly. My internet wasn't stable, so, at that point I just connected to the internet, got some stuff done and immediately eh, I kept the amount of exposure time to eh, yeah, as less as possible.

X: Clear. Then for example, if you send an email when you are connected to the public network-

Y: Yeah.

X: Could you explain how that process would go and where they could listen in as you say?

Y: Eh, yeah, so, eh, okay, so, I am not quite certain if they can refer to the emails in this case. Eh, yeah, because most of our mails are stored in [email], we do not use web-based email services. I am not able to access [the professional services firm] email through web-based eh, or through browser services. If it was the case, then it is possible that some of the cookies are stored in the browser or yeah, somewhere different outside the [email] environment, that is protected by [software provider]. Eh, then it is possible. But a lot of data that is uploaded to and downloaded from [an internal page] is through web-based services. So, my concerns or the worry- I am not sure if it is irrational or it is rational, but if I am using something through my browser, I can imagine a lot of cookies are being installed by the browser, because the cookie management is quite hectic and crowded. And if I am accessing it through a publicly available network, I am not certain if someone can get access to those cookies or some kind of logs that are registered in the system. That kind of situation. But I would not be worried about [email], or at least that is my understanding, that it is secured in the portal, yeah, so ...(0:23:00) client, like we call it. Eh, there is a client that is installed on the laptop, that you open it, and only then can you access the emails. So, that is how I understand it.

X: Okay. And if you were to upload information, how would that work?

Y: [Start drawing 5\_6]. Eh, if I have to upload information eh, okay, I have to first connect to VPN, like this, once my ID has been validated, I go to internet browser, I type [an internal page] eh, the [an internal page] opens. There is a location where it says upload files, I click on it and then that establishes a connection between [an internal page] and my system. Where I have to look up the files that are located in a specific folder, I select that file and the file gets uploaded. So, there is, this is basically open, well, within the VPN, this is like an open connection, where you are uploading a file from the system to here. I can imagine that the browser through which I am accessing, the browser will store a cookie with certain files with certain information has been transferred, so it works properly, or some functionalities for this to work are stored in those cookies. Eh, if someone is able to access those cookies, then it would be possible to some extent to know what is transferred, not exactly everything, but I can believe this can be useful or information for some people

X: Clear, thank you. Then on another notion, what kind of digital threats do you deal with on a normal day?

Y: Eh, digital threats as in social media, or-

X: Yeah, as an [the professional services firm] professional.

Y: Okay. Eh, I think I have eh, on a daily basis, my main interaction with digital platforms eh, as [the professional services firm] professional is three or four instances. [Start drawing 5\_7]. I use [social media platform] eh, to keep in touch with people and I get all these messages. Eh, so this is one platform that I use through [the professional services firm] VPN. Second one is [an internal page], which is my daily driver where I have to work constantly 24/7. And the third portal is [an internal page], this is again a new portal that is being developed by [the professional services firm] [country] eh, to use this portal quite a lot and there is a lot of data that is uploaded to [an internal page] on a daily basis. [0:25:34 till 0:25:47 has been omitted]. So, this is the major digital portal interaction that I have on a daily basis. Yeah, of course, there is always a possibility that I can open eh, let's say [email] as well. Eh, I generally don't use [social media platform], I don't like it. So, I never tend to open it on eh, office or open it at all. Eh, other than that, I think I also open [social media platform], I am sorry, I can't type apparently. Eh, I am trying to think, [social media platform] is sometimes open in case I want to yeah, listen to music or someone sends me a link of eh, cat doing something, then yeah. So, these are the regular interaction that I do eh, on the digital platform.

X: And you use VPN for this purpose?

Y: Well, I need VPN only for these two applications, I do not need a VPN for all these purposes. But I do not keep switching on and off. Once it is the start of the day, once I connect my laptop to VPN, after that all of this is within VPN. Although I do not need VPN for this. I can do it without connecting. So, over the weekend, if I am using my laptop eh, for personal use, I never connect to VPN, because then my laptop is simply my private laptop. I do not have to access [the professional services firm] systems. I can just do with the internet by using my Wi-Fi and I don’t need any of the codes to work.

X: Clear, great. And how does this threat or what- Are these also digital threats you would say?

Y: Are you asking if these systems are threats to [the professional services firm] systems?

X: Yes, because eh, I asked what kind of digital threats do you deal with on a normal day- O, you thought of other threads. Eh, okay. I mean threats as in, well not so, okay, it is a bit strong word, but as in attacks.

Y: O, attacks. Okay, I am so sorry, I misunderstood.

X: No worries. I get the confusion.

Y: O, I am so sorry, okay.

X: No problem, no problem.

Y: Eh, okay. So, I think the major threat, I do not have to personally deal with, but something that I always have in the back of my mind, is eh, yeah, something let's call it eavesdropping. [Start drawing 5\_8]. Eh, I am not sure if you are aware of that term. Eh, eavesdropping is someone trying to eh, yeah, read over my screen or listening to my telephone, when I am talking to a client. Since I have sensitive information open on my laptop, I always tend to use a privacy screen eh, yeah, whenever I am in public. I am also I think, I potentially deal with something called a man-in-the-middle attack. [Start drawing 5\_9]. Eh, yeah, this is quite eh, this is quite a high risk for a situation like this, where there is a VPN connection. [Start drawing 5\_10]. I am sure if we run a pentest on a [the professional services firm] system, there can be some vulnerabilities that can be exposed to either this kind of attack or something, yeah, this was what I was referring to. And someone tries to snoop in and read some information by being, yeah, an invisible party and trying to act as a person they should not be. This is one of the digital threats I think all of us deal on a regular basis, when we're trying to connect to a Wi-Fi that's not secure. Eh, I think the other threat that we have to deal with on a daily basis is legacy systems. [Start drawing 5\_11]. [0:29:47 till 0:30:19 has been omitted]. Dealing with legacy systems is quite risky, especially to a VPN, some services don't even work. And they are not really built to send out these kinds of attacks. So, when dealing with these kinds of systems, it is always a worry what to do. [0:30:33 till 0:30:47 has been omitted]. Eh, o, yeah, there is an alternate possibility of phishing emails. And [the professional services firm] seems to get a lot of it, I think we get a lot of these eh, mindless emails saying please I just offer this course. I can imagine they are trying to add a worm to [the professional services firm] network that keeps multiplying through different devices, I am not sure if anyone opens the links what happens. But we get a lot of phishing emails to see if they can steal credentials, they can gain access to the network. I can imagine this can be easier if you're connected to a non-secure VPN. So, that is something that we have to actively keep an eye on. Eh, another digital threat is, well, I mean this is something that everybody has to take care of themselves, but eh, there are a lot of data leak incidents. Well, not a lot, but it is quite a serious issue, because we deal with four or five clients at the same time, and you can imagine the nightmare if you send data from one client to the other. You have to raise a data privacy incident and we know the recent AVG regulation, that makes it even more difficult to deal, time-consuming, you have to be extra careful who are you sending the data to. And that kind of stuff. So, these are the main digital threats that I worry about every day. Including VPN and excluding VPN.

X: Yes. And you say that using a VPN when you need to access legacy systems is an extra risk, could you explain why that is a risk?

Y: Eh, yes. So, I think eh, let's say, [0:32:25 till 0:32:46 has been omitted]. Accessing that application through VPN is quite secure, because the application itself has a robust eh, authentication mechanism first. [0:32:55 till 0:33:06 has been omitted]. But again, it is not possible to log into the legacy systems in this environment, for that purpose we have to be on-site. [0:33:13 till 0:33:30 has been omitted].

X: Clear. And you say you get a lot of phishing emails, do you mean phishing emails at your [the professional services firm] email?

Y: Yes. Eh, so, I think, I am not sure if you can answer this question, ...(0:33:46) people as well, but eh, I think I get a lot emails eh, from specific eh, training company from [country], but we get all this trainings platforms, please look at these others, they might also be interested in that. Eh, if you look that eh, organization up and eh, eh, on internet it kind of, it looks a lot like sham and it looks like a phishing email, that you wouldn’t click any links on it. Eh, that kind of stuff. I know one of my colleagues was also running after one of the companies to remove all of his personal data eh, stating the AVG, yeah GDPR regulations, saying he, I have the right to be forgotten, please delete all my data and I do not want to receive any information from you et cetera. So, I think I am sure that other colleagues that you interview will also agree to this point that they get a lot of phishing emails. There is at least one per day.

X: And this was about social threats-

Y: Yes.

X: Eh, or digital threats. Eh, how does the threat change because of the VPN connection?

Y: Okay. Eh, I am trying to think, I am trying to go into my technical knowledge to see if I can make a comment. Eh, so, I think, I know that eh, that an attack like MITM, a man-in-the-middle attack is possible eh, if you're using VPN. Someone can impersonate you and then try to access information, but I do not know how the threat landscape changes eh, because of using a VPN. Eh, specifically speaking, so, I am, because I am not really, technicalities for cybersecurity, I can just say that okay, it is possible to create an MITM attack eh, if you're using a VPN. But beyond that I am not able to add anything valuable. Eh-

X: No problem. Could you explain how a man-in-the-middle attack would work when you are using a VPN?

Y: Okay, so, the first thing any attacker would want to initiate an MITM attack eh, would be to gain credentials. [Start drawing 5\_12]. Eh, yeah, yeah, if you want to access the same portal, the only thing that recognizes me is my user ID for example. What is the user ID. If I have a password to the system, he would want to know what the password is. Eh, if it is not encrypted than it is a big problem. And then the second layer of security in this case is the [access token provider] token. So, if he is able to decipher how these number work, then he should be able to gain access to it. Eh, or, I, okay, and I am getting into technicalities, I am not sure if he can act as a silent listener in this case, but eh, this is how I understand it. He might have to phish out my details eh, from my services, when I enter these details in my browser for example. If there is eh, yeah I am not, I forgot the technical name for it, it is like a phase blocking, where all the information is collected eh, in a tile or sheet(0:37:17), like a tracing eh, that is how I can imagine he can eh, impersonate me and be connected to [the professional services firm] network.

X: Okay, thank you. So, this was around digital threats. Do you also have to deal with social threats in a normal day?

Y: Eh, no, on a normal day no. There are eh, I have eh, I have never had a situation where someone was trying to follow me or someone was trying to eavesdrop. It is eh, it can be a challenging situation if you are working on some sort of project and if they found out the information is clear that someone is working at this is a [the professional services firm] laptop that can hold information, then yes. But, on a regular basis eh, there are not so many social threats that we deal with except these phishing emails of course, but eh, yeah, so, yeah, that's the major challenge. I know a lot of people have their laptop stolen eh, when I say a lot, it is more like one or two percent eh, but well that can be attributed to general thievery. Just because people like stealing stuff eh, we're not specifically targeted because it is a [the professional services firm] laptop. That's how I understand the situation that would go down when people are sleeping in trains for example and the laptop is stolen eh, et cetera. But these are the social threats that we deal with on a regular basis.

X: Okay. And does the VPN connection have any influence on this?

Y: Eh, I think yes. It has a big influence. Even if someone is able to steal my laptop, they will not be able to connect to the [the professional services firm] systems without the [access token provider] token, which is on my phone. Or in this case- Or in the case where it is a physical token, this, the thief will have to steal both of them to be able to access [the professional services firm] systems. So, I think VPN is very useful in this case, because it is a secure connection eh, and one part of the token can still be with me, and that is my phone. And again, my phone has this secure two-factor eh, well, sorry, my [mobile phone] has a lock on it, right, so, no one can access the phone either way. So, no one can reach the digital data and security and [access token provider] token. Eh, however, if you have a physical token, if you are like most of the people, who keep their physical token also in the laptop bag, which means if your laptop is stolen, your secure token is also stolen. Then, the person only has to know your password and he will be able to log into all systems at one time. Which is quite risky. That is why I called it a dinosaur system in the first, I think everyone should switch to a phone-based [access token provider] token. Eh, it has an additional layer of security.

X: Okay. And if you think about these digital and social threats, who or what could be an attacker behind the threat?

Y: Eh, who or what could be behind the threat. So, people on the attack side, right? Who would want to do it? Is that what you mean? Eh, hallo? I'm sorry.

X: Sorry, that is what I mean.

Y: Eh, okay, so, to clarify the question once again, you want to know eh, who could be behind these kinds of attacks right, from my perspective.

X: Yes.

Y: Okay. well, eh, eh, okay, that's a good question, eh, well, eh, I would imagine some portion of people being eh, yeah, eh, doing it for the sake of adventure. I’m not particularly certain if someone is specifically trying to target and phish out important emails, to get some sensitive information from clients. But I think a very small portion of attackers can specifically be targeting that information, that they already know. So, the one thing that most of the people outside, they are not in [the professional services firm], they do not know what kind of sensitive information exists. So, the only idea that there is some sensitive information at [the professional services firm] for the clients [0:41:37 till 0:41:38 has been omitted], but they do not know what kind of information might exist. So, it can be a very blindfolded attack, let's see what we can get out of the system. However, there will be very small percentage of people who might have all this information and he precisely also what he wants from this kind of attack. In that case we would classify it as a high-risk attacker. Others are just, yeah, the technical term, scriptkiddie, who just want to see he, can we can we bring down someone like eh, the eh, the DDoS attack on eh, Ziggo, eh, I don't know. In 2015 or '16 they brought down the services for Ziggo, just because they weren't taking care of their customers. Something like that. But nothing very specific, like terrorist or eh, specific governments targeting [the professional services firm] specifically, nothing that bad.

X: And what could be an attacker’s intention?

Y: Eh, either cause disruption in the services, or eh, gain access to certain valuable information, to see what is important and what is not. So, I can imagine that with many points in time, especially a [role] email, mailbox or his communication with the clients, a [role] laptop is very valuable, because it contains all confidential information, like [0:42:57 till 0:43:03 has been omitted]. Now all this information will not be available with me, but it can possible be available to [role]. I am just guessing, I don't know. I think this is something they might be interested in, [0:43:13 till 0:43:44 has been omitted]. So, if you want to gain access to this world of data from which is very sensitive, then it can be a minefield. You can sell this data for quite a high value on the black market, so this could be something that the client might be interested in. O, sorry, not the client, the attacker.

X: And what would be an attacker’s capability?

Y: Eh, how do you mean capability?

X: What would they need to be able to do eh, to make an attack successful? Or what would an attacker’s background be?

Y: Eh, I would consider [the professional services firm] technical system to be quite eh, robust. We have lot of layers of security to prevent these kinds of attacks, we also have a special security eh, yeah you call it a SOC organization eh, which has all these alerts popped into the system. So, whenever you do some kind of fishy activity, you will immediately get a call from [country] team, there is a specialized team in [country], who does the monitoring on all these kinds of incidents. So, if you want to avoid all these, I call it a minefield, if you want to avoid this minefield, you have to a lot of expertise on how to navigate across a corporate environment. So, let's say if I read a book, let's say red hat or red teaming strategy, I will not be able to do it myself. I believe someone who is either a certified hacker or has a lot of experience dealing with complicated systems, who knows his way around all this security monitoring and incident monitoring eh, only then you are actually able to extract this information. Eh, of course you also have to be a social engineer, to be able to get this information, like the access information from employees. Like most, I can, I would, I pray that all other colleagues that you interview are also aware of these kinds of attacks. We do a lot of training eh, to keep yeah, be aware of your surroundings. Who is looking at this screen for example. So, I would expect everyone to be responsible and have this in the back of their mind. So, I think the person has to be quite smart, he has to be, have some technical background, that they can navigate across the environment, it is not that easy. Yeah.

X: And does the kind of attacker change because of the VPN connection?

Y: Okay, that's, well, I mean, I am not sure if it changes eh, because, well, I mean I do not know any company that does not well, there are companies that do not offer VPN, but a sophisticated attacker would be ready to attack a VPN louder than attacking [the professional services firm] network directly, because doing that is quite impossible going into the datacenter for example, trying to crack into the [the professional services firm] office network in the offices, which is quite a difficult eh, strategy. I think the easiest way for an attacker to do is to attack the VPN, because it is remote and it highly depends on how the VPN is connected, how secure the Wi-Fi to which it is connected. So, that is how I believe an attacker might change. Yeah, it is easy to use a smart intelligent attack rather than use a brute force and break into the datacenter or crack open eh, the [the professional services firm] network inside the offices.

X: Thank you. And what could be the impact of an attack? The impact for [the professional services firm]?

Y: O jeez. Okay. Eh, I think it would be quite significant. Eh, if, well, if the attacker is successful to attack our network, it would not result in a public humiliation, unless the incident becomes public. However, if there is a data leak incident, if the attacker is able to steal private information, [the professional services firm] is obligated to report this incident to the data officer, who is within our firm or who is external I don’t know, within 72 hours what that impact, what impact it has on our clients, [0:48:04 till 0:48:22 has been omitted]. So, I think in that cases the consequences of these attacks will be quite higher. But, let's say, someone is able to crack into VPN and steal someone's personal ID or network, he might not be able to do much. So, this incident might not be reported outside, unless the attacker makes it public himself. The impact in that case again, like I said, there is security monitoring. So, if there is anything fishy going on, it might be sensed by this team in [country], and immediately they will try to block the account. Or, yeah, it happened, one of my colleagues eh, he was trying to eh, access a website, that website had a worm or some kind of pop-up, which was very malicious. After the pop-up opened, he got a call within a few second from the [country] team saying what the hell are you doing? We got a security alert and this is not okay, please close the website and restart the system. So, we have this kind of measure in place eh, but to prevent any further impact. But a data leak can have a significant impact eh, on our reputation. It results into eh, yeah, the attackers stealing something from us. It will not go down very well. It will result in financial losses, it will also result in a lot of reputational damage, there will be a lot of eh, extra work that needs to be put in after that, to make sure this kind of situation does not happen again. Eh, I can also tell you about recent measures. [0:49:47 till 0:50:18 has been omitted]. Eh, so, yeah, sorry, I am speaking to much, okay.

X: No, that's not a problem at all.

Y: Okay.

X: Could you think of any other possible impact of an attack?

Y: I am trying to think of an impact of an attack. Eh, I am not certain if the target, if the attacker would actually target employees individually to blackmail or something. Because most of us do not have any sensitive private information on our office laptop, I surely hope so, but I can imagine that if someone gets a hold of your laptop and is able to access your laptop and you lose all the sensitive information that is in the laptop, like your pictures for example, with your loved ones, et cetera. The attacker can use it to blackmail you eh, but certainly something like that. But other than that, I am not aware of any other impact that it can have on [the professional services firm] or on the personnel.

X: Clear, thank you. And you mentioned a bit about it already, but if we look at the VPN connection itself. How secure is the VPN connection?

Y: Eh, it depends how you measure it. So, eh, it depends what you call a very secure connection. Eh, I mean, I don’t know the technicalities, I don’t know if there is a scale to measure. But, if I am connected to my home Wi-Fi and I am connected to VPN, I would consider it a very secure connection. Eh, but I am sorry, I am not able to answer this question probably, because I don’t know what to measure it against.

X: Not necessarily on a scale, but more eh, for, could you think of reasons why the VPN connection is not 100% secure?

Y: Eh, yeah, well, I mean, so, eh, yeah, I am not quite certain why. But I can imagine when you are remotely connecting the system has to trust the person who is connecting is actually [me]. In this case it is me. Eh, when I am in [the professional services firm] office, if an unknown person is sitting on someone's floor, [0:52:40 till 0:52:46 has been omitted], trying to represent [me] for example, then it is a different situation. But I mean, VPN is only as secure as long as your credentials are with you and not with someone else. If the data, if I share all these details with [person], is also able to say [person] is [me] and [person] is connecting to and accessing all the information. So, it is only as secure as responsible people are with it. And the technicality, because you are using network that is not [the professional services firm] eh, that is one vulnerability in place. But I kind of touched upon that before. But I would not have anything to add beyond the points I already mentioned.

X: And you already mentioned a bit about it as well, how do your actions change because of these insecurities you mentioned?

Y: Eh, how would my what change, sorry?

X: How would your actions change?

Y: O, my actions, well, my interaction with [person] about my work is eh, well private. I sometimes, eh, yeah, so basically, first, we do not share the same laptop. [person] does not get to access the laptop eh, when we talk about work it is also very formal. It is nothing more details involved, because eh, if, if all the details are shared with your partner or anyone else, it is quite easy for an attacker to fish those details out from your partner for example. But, in the end, in this case for example, [person] does not know the password to my system, [person] cannot access it, [person] doesn’t have access to my phone, so [person] cannot know the [access token provider] token ID. All this information I mean, that is something that actively I try to do. I isolate the work environment away from the partner, so that the details are only limited to me. Eh, that is one type of action that I do. I actively avoid clicking on any other link, even if those links are sent by my colleagues in the email. Yeah, you can always copy a link and put in a, on these internet websites, where you can see is it fishy or not. But I just tend to avoid doing that in any situation. So, these are the measures I would take to eh, even give small eh, yeah, small chance for the attack.

X: Okay. In that case I am sorry for sending a link to you in an email.

Y: It's okay. I put that link in a, in the checker before I went to it. [0:55:14 till 0:55:26 has been omitted].

X: Makes sense.

Y: Okay. It's okay.

X: These were so far my questions, do you have anything that we did not talk about, about VPN?

Y: Eh, yeah, so, eh, well, I do not have questions right now, but it's just more like a remark. So, I know that VPN is kind of the only resource we have right now, especially in a situation like Corona crisis, it is one of the only solutions we have right now. Is to connect through VPN. So, even if it is very eh, how you say, weak, well, not really weak, but if it has vulnerabilities, we have to live with it and we have to make sure that we are as employees or as people who are using VPN, we are responsible with it. Because either way, we do not have an alternative solution to properly authenticate, you give a secure connection in a way that no one else can listen or see what is being transferred, et cetera. Eh, I am not sure if there is eh, another kind of technology that is being developed other than VPN, but this is all we have right now, and I think it works well so far. I am not certain if there are any severe vulnerabilities that have been discovered for it, or if there is any kind of research going on. But I am sure if someone would be able to crack VPN code and coming here, then we will have to move to a new technology. But this is the best we have so far.

X: Okay. Do you have any other questions for me?

Y: Well, I am not certain if my questions were useful to you, because I would not consider myself as a very technical competent eh, individual. But I did my best to share all the insights that I can tell from using the VPN. Eh, but eh, eh, yeah, I mean, I am not certain how I can ask more information. But if I have a need for any questions or anything I will definitely eh, ask you about it. At the moment I do not have a question for you.

X: Okay, then I would like to thank you a lot for your participation.