Heather:

Welcome to the Hurricane Labs podcast. I'm Heather, and today we're going to talk about the value of using a VPN for network security purposes for average users, so basically anyone who uses the internet for streaming, email gaming, social media, et cetera. Here to help us with that, I have Tom, Hurricane Labs' Director of Technical Operations, and Miles, one of our Security Analysts. So before we get into the specifics of network security for just average users, let's talk a little bit about what VPNs actually are.

Tom:

So basically, a VPN is a way to connect to a different network and have a secure connection to that network. So it is going to sound weird saying historically, but the main goal of that was companies who had remote employees that needed to have access to resources. They deploy VPNs so that their remote workers and employees are able to access those resources securely from outside of their physical location.

Heather:

Then the value of VPN in professional use is accessing proprietary information and things like that securely. What about with personal use? What's the value that VPNs offer for people to just use as part of their normal internet usage? Is there a value?

Miles:

Oh, I believe so. It gives you a certain level of privacy for browsing the internet.

Tom:

I kind of think the... It's one of those areas that has exploded in, I don't know necessarily popularity, but at least in marketing, where you see a lot of companies advertising, "Hey, you can use our VPN service," and all of that. And I kind of think that they're pushing a narrative that maybe is not all that realistic. That said, I think there are some potential privacy benefits, but I think the way that the VPN industry advertises VPNs kind of makes them seem more important than they actually are.

Heather:

So it's becoming a ping word then, and that you need to know what your goal is with using a VPN?

Tom:

I think we can look at it from the perspective of a couple different things. So you go to a coffee shop, you connect to a public wifi. What are things that you need to be concerned about? Let's assume there is someone on that network that is wanting to intercept what you're doing, and let's say they control the wireless access point of the router. Things that they're going to be able to see, unencrypted traffic. So primarily, that's going to be DNS requests and unencrypted websites. So, anything that's not HTTPS, instead HTTP. So yeah, depending on what you're doing, you can see information about that. If you're worried about your bank account potentially being intercepted when you're using public wifi, I would say either you have a really, really terrible bank, or you don't have to worry about that sort of thing happening, other than people providing that internet connection, whether it be... If you're at a library, for example, the library and the ISP knowing what bank you're using. They're not going to get details about your bank balance, for example, if you don't use a VPN, because that's all transmitted encrypted.

Heather:

Yeah. I read an article on Tom's guide, different Tom, I presume, unless you're that Tom, Tom, where it talks about how coffee shop hacking is a high risk and low payout activity. So if you're going to Panera and you're working from there, and unless you're, like you said, accessing your work content where you have to be more secure with what you access, probably not necessary to use a VPN in that situation. Is that right?

Tom:

I would say generally, yes. And even with the rise of cloud services and such for work, there are different types of ways to access things securely that don't necessarily require a VPN. So if you are a company that has all of your services, for example, in Office 365, you don't necessarily have to have your employees on VPN to access things like SharePoint and email, if that's what they need. They might still need to VPN to access file servers and other internal resources, but it really comes down to what the employees looking to do. And obviously making sure the things that you access are handled in a secure way, that is encrypted.

Miles:

For me, it's kind of a... It's probably not necessary in a lot of cases, but there are going to be cases where having a VPN, especially in that coffee shop situation, could be useful. And it's not something that I want to bother figuring out, so it's easier for me just to... Once I connect to a public wifi, just turn it on, and then I don't have to worry about it all.

Tom:

I actually recall being at a presentation at DEFCON a couple years ago where someone was using the publicly released information out of the DEFCON network to see what was going on. And you can get a ton of information from that about Slack, for example, since every Slack channel uses a unique DNS name. And not every Slack channel, every Slack organization, I guess, is the right way to phrase that. But you can use that to see what Slack organizations are used. And if you're trying to hide where you're discussing things on Slack, having a VPN to protect that would make sense. That said, your VPN provider can then see that information. So it's who do you trust more.

Heather:

Miles, you mentioned that you run your home firewall through VPN. Can you tell us a little more about that setup?

Miles:

Yeah, so I have... So the hardware, it's called a Protectli Vault. It's basically... It's just a mini computer basically. And then I have pfSense installed on it. And from there, I have it configured and set up to run the VPN. I use private internet access, PIA, and it just everything that goes out the land port has to go through that VPN. If anyone's interested in doing something like that, all I did was use the instructions out of the Extreme Privacy: What It Takes To Disappear book by Intel Techniques. And it has several pages of instructions on how to set everything up, configure everything, and then... And it also has a VPN kill switch so that nothing... If for whatever reason it failed, then just everything loses internet, and then I would have to fix it, but then that way I know that nothing's going through it that isn't just going through my ISP then. And then there's also... They go through the instructions on how to prevent DNS

leaks, can set up CloudFlare as your DNS, which they do encrypted DNS, which is nice extra bonus. Also. I just, I can set up a wifi access on it as well. So then that way, anything that I connect in my house... Because not every device, especially IoT devices, can just... You can't just set up a VPN on everything, so this is a nice way to... If you want to go the extra mile and just put everything, or as much as you possibly can on a VPN, you can do it this way as well.

Tom:

Doing that at the firewall level and running the VPN there, I think, is a really good idea, because like you mentioned, IoT devices don't support running a VPN client, and you probably wouldn't even want to do that. So having that capability makes a lot of sense to just do it there. Plus you're also deploying that configuration to support all the other users in your environment too. So if you have family members that you don't want to just access the internet directly, you want to have them go out the VPN, you have that option, and they don't have to run any VPN client. The trade off there is that obviously when you're off of that network using wifi somewhere else, you just don't have that. So if you really want to use a VPN everywhere you use the internet, you have to have a combination of running it at the firewall and also a client, because outside of your network, you just don't have that.

Heather:

What was your, I guess, inspiration for going ahead and setting up your firewall that way?

Miles:

It was something that... Because I listened to the podcast, and he's talked about before, referring to the privacy security and OSINT show that he's mentioned, and it sounded like a really cool project. I've also wired up my entire house with Cat 6 cables and installed a network rack, and I just had all this other stuff that I was already doing network-wise in my house, just to try and learn a little bit more about networking do a little more hands on stuff. And it just seemed like a natural fit for a project I can do to get some more hands on experience and learn something. And it's been really cool to do that, because there's stuff that... Because I'd never done anything with pfSense before or anything like that. So it was really cool in that way, but then it just kind of allowed me to just put everything behind my VPN, and then I could just not have to stress about, oh, do I need to use my VPN now or not? And then I do also have it set up so that I do have wifi that is not behind the firewall, because there are things like Netflix, Disney Plus, and other stream services that just won't work with the VPN turned on. So for the purposes of things that don't work when you have the VPN running, I have a way to access what I need that way as well.

Tom:

So basically anything that assumes you have a geolocation in the United States, you have to run that way.

Miles:

Yeah.

Tom:

Do you do that on a per device basis, or do you do it on a destination basis?

Miles:

So basically, for the most part, it's just anything that does any sort of streaming, that's basically the main pain point in my house. And so the TV, the PS4, those are all connected to the... They're basically connected directly to the wifi router that connects directly to my ISP, rather than putting them on the wifi router that's kind of the firewall.

Tom:

Got it. So you basically have a separate segmented network for those sorts of things anyway?

Miles:

Yes.

Tom:

That makes sense.

Heather:

So if someone were inclined to use a VPN, either at a coffee shop or at home, what service would you recommend?

Miles:

The two I would generally recommend are Private Internet Access or ProtonVPN. I like how they do their... They get external audits, so you can kind of... And then they publish those and you can kind of see like what... You can kind of verify the fact. When they say they don't do logging or any of the other benefits that they're claiming on their websites, so you can kind of like back those up. There's also, I believe it was ProtonVPN, they actually did get a subpoena at one point, which they did... The subpoena was to hand over the logs they had. But since they didn't have... So they complied, but they didn't have any logs, which is just also kinds of verifies that their claims are, what they're offering with their VPN, are true. And ProtonVPN has a free tier that you can also use if this is something you want to just try out and see if this is something you like and want to do. That way, you don't have to make a huge financial investment. Not that these things are expensive, but I guess you wouldn't have to make any financial investment if you just want to try it out for a while. So those are usually the two I would recommend.

Heather:

All right. Well, that's all we have for today. So thanks for joining us. And until next time, stay safe.