Episode 44: "Security is a business enabler and a risk reduc...

Tue, 6/2 9:27AM 1:01:43

SUMMARY KEYWORDS

security, team, cloud, microsoft, people, infosec, technology, attacker, organization, company, vendors, customers, fran, secure, breach, hired, built, literally, deploy, aws

SPEAKERS

Warren du Toit, Chris Goosen, Nicolas Blank, Francisco Donoso

C Chris Goosen 00:19

Welcome to the cloud architects podcast, a podcast about cloud technology and the people using it.

N Nicolas Blank 00:26

The cloud architects podcast is sponsored by Kemp technologies. Choose Kemp to optimize your multi cloud application deployments and simplify multi cloud application management. A single pane of glass for application delivery, Kemp provides a 360 degree view of your entire application environment, and even third party ADCs. Download Kemp 360 for free today at Kemptechnologies.com

W Warren du Toit 00:53

Hello, everyone, and welcome to another episode of the cloud architects podcast yet I feel the same as you. It's been a while. It has definitely been a while. It's been a crazy year. And I think that this is like gonna be the first of many Corona episodes where we talk about things that have been happening in sort of how we've been forced to change the way we work. And so I'd like to introduce my co hosts yet again. It's good to see you guys.

N Nicolas Blank 01:28
Hey, Nick.

C Chris Goosen 01:30
Hey, Chris here.

W Warren du Toit 01:31
And today, we have an amazing guest. And we'll introduce him shortly. I think Nick wants to pick on me a little bit.

N Nicolas Blank 01:39
I do. I do. And I want to pick on Warren and Chris both because both of them have had some changes lately. And we want to talk about some of those changes because they do have context for today's show. And I'm going to add a little bit of a mystery by saying that they have both a joint true of the world's large Just security vendors. And so why don't we start with you, Warren, why don't you tell us what have you been doing lately?

W Warren du Toit 02:08
Yeah. So you know, it's strange when you say security vendor, right? Because that's, that's a new thing. I mean, who ever thought that Microsoft would be a security vendor. So yeah, I started working for Microsoft this month. It was was a bit tough because I had to give up my MVP status, but it's okay. I don't have a trophy anymore. I'm more have a blue badge. I mean, it's somewhere here and I could probably show you but yeah, I have cloud solutions architect. I guess. The really cool thing is that I get to use the internal Microsoft tenant now for Azure. Ah, okay.But anyway..

N Nicolas Blank 02:59
for all your hosting requirements. @WarrenDT on Twitter.

W Warren du Toit 03:05
Don't go breaking some new NDAs But still, I think I think it's a beautiful thing. It's a wonderful company to work for. And as Fran was saying a little bit earlier while we were entering Satya as done amazing things, man. He really, really has incredible company to

work for and like parental pandemic leave. Can you believe? So? I get if I wanted to, I mean, provided the workload isn't too hectic I can do. I can teach my child, I can take Lee even teach my child which is which is pretty read. So I think that's that's that's the that's a cool thing. And yeah, like I say, it's it's amazing to be actually sort of in a as an MVP, you sort of delve into it. And you push to sort of create this second career. So with an MVP, many Yeah, you're you really work hard to maintain the two and now I'm lucky enough to be like okay, well the two have merged So not only do I get to promote Microsoft technology, and use Microsoft technology, it's my job. So it's good.

C Chris Goosen 04:09

Yeah, well done. That's awesome, man. Congratulations for that. You know, so yeah. Yeah, I have actually in its it's been probably the biggest change for me in my entire career right for the first time ever. And I've been thinking about this a lot this this week in particular, because for the first time ever, I'm not working for a very large Microsoft gold partner. Right. And so that's been very interesting. And so I made a move a bit of a career change, I guess, if you will, earlier in the year. So right after we recorded the last episode, which was in New Zealand, I joined a company called Kudelski Security. And so I'm gonna be heading up the Microsoft practice, Microsoft Security practice at Kudelski. And we're super excited because, you know, you mentioned before, you know, Microsoft being one of the world's largest security vendors, right. And that's, it's so true. That's the messaging that we're using. And it's exciting to kind of be on the forefront of that. So still working very much in the office 365 space for now in the Microsoft 365 space, but very much focusing and looking at everything through a security focused lens now, as opposed to the productivity focused lens from before. And I guess that's part of why I think this episode kind of came together because I've been immersed in working with some really, really smart people. And one of those people is joining us on the call today. And I was super excited because my head started spinning day one, start, you know, trying to pick up the vernacular and trying to pick up all the new concepts in this new cyber security world. And so we thought it'd be really good idea to bring Francisco Donoso onto the show, to talk a little bit about that world and break it down a little bit so that we can kind of do a, you know, cybersecurity for IT pros, if you will. And so with that, I want to introduce our guest today, Francisco or Fran, welcome to the show.

F Francisco Donoso 05:57

Thank you very much for having me, Chris Warren. Nick, it's a pleasure to be here.

C Chris Goosen 06:02

Yeah. Do you want to just do a quick introduction and sort of tell folks about yourself and what you do? And have done? Yeah.

F

Francisco Donoso 06:09

Yeah, absolutely. So, as Chris mentioned, we both work together at a company called Kudelski Security. And it's been a real pleasure, the last few months getting a chance to work closely with Chris, we've been working very closely for the last few months. And that's been great. as Chris mentioned, you know, I've been in cybersecurity for almost the entirety of my professional career. I sort of fell into it. In the very beginning, I got a job at a company like koski years ago, doing like security monitoring for a bunch of different companies. And I fell in love with it. I fell in love with cyber security, even though that wasn't a consideration, you know, when I was in school, but through my career, sorry, guys, I've had an opportunity to actually kind of travel all over the world and work with so The world's largest companies. I've spent a lot of time in the Middle East. After some big breaches of some of the world's most valuable companies, I got a chance to help organizations, but you know, across healthcare or all sorts of different places, kind of recover after some large breaches. And it's, it's been a passion of mine, helping organizations understand how things are changing with the cloud, if you will. One of my favorite things about cybersecurity in general is how quickly we have to adapt to new technology. I think all of us are probably familiar with that stuff as new technology comes out. It's been a blast because I get to learn how to use it from, like, administrative perspective and then have to think through how do we potentially secure this stuff? Kubernetes and cloud environments and office 365,

C

Chris Goosen 07:56

Okay, I was gonna say you said the K word

N

Nicolas Blank 07:59

Somebody, at least it wasn't me.

F

Francisco Donoso 08:04

And, and through my career, you know, I've had the opportunity to work in places like Kudelski building security practice to help our customers. But I've also been security engineer at a company that's now owned by Twilio, that process more traffic per day than Twitter. And I had to learn a lot about how people were managing infrastructure at scale, and how that changed my perspective or my role as a security person. And then I've also worked for a startup where I built all the Kubernetes stuff, because we didn't have anything we needed to deploy code. Kubernetes seemed like a cool project. And then I had to figure out how to secure it. So I've kind of been all over the place and I've enjoyed every second of it.

W

Warren du Toit 08:46

It's not that easy to build Kubernetes from scratch.

F

Francisco Donoso 08:50

No specially when you've never used it before. So it was a it was a really it was a really fun experience, though. And that's really what I love about the industry that we're at technology in general, just like you just get thrown in, and you have to figure it out.

W

Warren du Toit 09:05

How much how much and this this is this, this equation, when I heard you're gonna have you on the show, I was thinking to myself, the first question I'm going to ask is a Mr. Robot question. It's gonna be like, how much like Mr. Robot is being in security? I mean, cuz when you look at it, he, I mean, all of those commands and things that he ran and obviously they did a lot of research into Mr. Robot and what sort of rootkits were being run and Kali, Linux and all that kind of stuff. And like, do you use Kali Linux?

F

Francisco Donoso 09:40

It really depends. The answer is yes, it depends on vironment, right, yeah. Mr. Robot has done the best job that I've seen thus far. It really kind of explaining what cyber security looks like from an attackers perspective. And just recently, actually, I have the opposite. You need to join a company that was built by teams who used to build offensive stuff for people. So I've had a lot of opportunity to work with some of the world's best hackers. It was it was mind blowing, because they would be able to go find a zero day a zero day exploit in technology used across the world in like two days, which I didn't know was possible at the time. But I think the biggest thing that that all of those shows kind of miss is just how much failure there is before that, like, success. And what has to keep you going when you're in that side of the house, which is the attacker side is you have to be okay with the failure but really love the adrenaline of the success. Because it's like 99% failure and banging your head against something that you just don't understand. To get to the point where you're like, Oh my god, I did it. I exploited this thing. And that's amazing. Okay. Let me go back to pounding my head against the wall to figure out how to how to do the next thing. So I think that that's really what's missing

W Warren du Toit 11:07
the emotion. I remember how you did it so that you could protect yourself against it. Yeah, yeah.

C Chris Goosen 11:15
That's fascinating, right. I think. I think part of that is, you know, these conversations, these types of conversations and the fact that we've all thought about and understood the need to be more security focused, especially in the last 10, eight to 10 years, right with, everything's moving into the public domain, if you will, as far as like the cloud and stuff is not as publicly accessible. You can't just wrap your arms around your data center anymore and go Okay, well, we'll just put a firewall and now stuffs protected, right? I remember, man, this would have been probably, I'm thinking probably around 2005, maybe 2004. I was at a teched event, Microsoft tech event. It was in Joburg. So it was the early one did them in, in Sun City. And there was a guy gentleman by the name of Steve Riley, who used to work for Microsoft trustworthy computing group, and went on to AWS and I'm not sure where he is now riverbed, I think at one point too And at that time, he was talking about the concept of perimeter boundary, less data centers, right. And I still remember the talk was called something like, you know, it's 10am. Do you know what your data is? And people just lost their mind, because this guy was like, it's the time is coming, where you're not going to have a perimeter, you're going to have to shift stuff, somewhere, wherever anyone can access it. And you need to rethink what that means to you and your organization. And Fast Forward 15 years, you know, I mean, we've been going down this route for a while now. But Fast Forward 15 years, it has never been more true. So welcome to the cloud. Yeah, welcome to the cloud, right. So So we've all kind of Being This is something that's been on our, I guess, in our minds for a little while, but I think when you start really digging into it, man, it's a whole new world. Right. And so I guess Fran, one of the things I wanted to kind of, I guess, asked you or ask you to unpack for us to break out is the concept of the vernacular and the concepts that kind of float around in cyberspace, right, because you hear people talk about blue team and red team and white hat and black hat. It sounds like people just love colors in the security world. But there's some river they have very specific meanings, though, right, those terms and those phrases.

F Francisco Donoso 13:34
Yeah, yeah, absolutely. But before I do that, I'm sorry, I just kind of mentioned something that you reminded me of that talk where you said, Hey, you know, boundary lis networks

and data centers are a real thing. The first time I had an experience like that, that had to kind of shift. My entire mindset was when I was working at a company that got purchased by Twilio. And we were processing so much data that when we started looking at firewall vendors for protecting our data center, he would have literally cost hundreds of millions of dollars to buy hardware powerful enough to secure our environment from like a traditional network segmentation perspective. So we had to shift and say, Okay, well, now we're managing firewalls at every single server. And it was just such an interesting shift that I think most organizations are now having to think about, right? I don't know how many organizations are so large that they literally can't buy enough hardware to, like process the security traffic from a firewall perspective, but that was a that was a really interesting change in kind of mindset for me. But yeah, just like you mentioned, you know, there's a lot of terms. And I think that this is something that's been specially pervasive in cybersecurity, and I'm not sure exactly why it's so bad in this specific section, but we have a lot of terms like blue team, right, which essentially is really just defensive guys. Right? So it actually a lot of the terms that you hear in cyber security come from, like old military backgrounds, because some of the very first, people who started thinking about cyber security came from the like, national security or defense space. So the word red team as an example, which is intended to denote someone who's like trying to attack you in terms of a cybersecurity exercise they're trying to break into your environment. In order to help you see what could happen came from the, from the military world, there would be a red team who would work on a training exercise with a team by I don't know breaking into some compound and seeing how far they get. So the red team in cybersecurity is essentially the same thing. Hey, can we break into your organization? How far can we get? How realistic can we be? And the blue team is sort of the opposite of that right that their defensive team was sitting there trying See if they can find those bad guys, or in the real military,

W

Warren du Toit 16:04

Do they work well together?

F

Francisco Donoso 16:07

Yeah, that's really. Yeah.

W

Warren du Toit 16:11

Because I mean, like the one does the one and the one does the other, but they're essentially trying to achieve the same results. They're trying to find a way to prevent the person from getting in, right? Because obviously, you're not talking in context of a blackhead. Now, you're not talking about hackers trying to do evil. You're talking about two teams trying to achieve the same goal.

F

Francisco Donoso 16:33

Yeah, I think what you're seeing now is more and more of the answer is yes. Previously not so much enough. I've had the opportunity now to be on both sides of the coin, and I love them both. Prior to joining klc security, I spent some time at a company that was trying to build an automated red team, and that was some of the most fun I've ever had in my career. That's where I had to learn Kubernetes To figure out how to have a security environment where we literally had zero and it's like we literally had millions of dollars of zero days that we developed, and I had to figure out how to secure that using some magic. But what I, what I've seen is that a lot of red teams from like your traditional cyber security vendors, they really just feel like they're there to beat up the blue team, right? It just feels like sort of a bully coming in and say, Look at how bad you are, you suck. You didn't find any of this. And that was a lot of pervasiveness around cyber security for a while. But now, a lot of that attitude has luckily shifted right where, Look, guys, the only reason we hired you to be a red team is to help our blue team get better. So you need to work together to do that and accomplish that. And there's some firms out there. In fact, Walmart has some of the best Red and Blue Team guys that I've ever met in my entire career. Both of their teams are fantastic. The reason they've succeeded so much, is because they have this partnership where they're just constantly sparring. The Red Team figures out a really novel way to go after some part of the Walmart environment. And then the blue team does eventually catch them. But it's all about, okay, well, that's really cool. How did you get here? And then what could I do to potentially detect you in this new novel way that you came up with, literally just to break into this environment, and just constantly having that collaboration, because it needs to be a collaboration. And what's what's really interesting in that environment is, you know, a red team engagement, depending on how sophisticated it is, could be a year long, right? And for the first six months of that, the blue team may not even see anything that the red team has done. It's all maybe reconnaissance and staging, to make sure that when they break in, they have a way to control what they've broken into. But a lot of the value out of that comes What did you spend six months doing? What did you do? Oh, you register it A domain that looks just like mine, how could I potentially identify that to see if in the future, someone else's staging something similarly? Or, hey, I responded in a way that actually gave you more access. So this is something that we saw at that company A while ago where a blue team when they're in an environment where there's potentially real breach, right, because the goal of a red team should be the blue team should never be in a position where they're like, Oh, that's just the red team, we'll deal with it later. They need to react as if it is a real attacker, constantly. And often what happens is, for blue teams who haven't had that experience, they react in a way that's actually extremely advantageous to an attacker. An example would be, we've had cases where a blue team person would log into a machine that we had compromised using their privileged domain account, which means Hey, now we've got your credentials. We've got your privileged domain account. Thank you very much blue team, you've made our job significantly easier. So a lot of it is just helping the blue team understand how they should react calmly, in a kind of structured way and think about how they're going to react to an attacker, because reacting correctly, could be disastrous, right? It could give the bad guys exactly what they need. And we see that a lot here at klc security and other firms where blue teams who don't have that experience, React poorly, and cause unfortunately more harm than good when they're reacting. So I think that the most important part of a red team really is not just how do you break into this environment? That's always useful information as a defender, but how did I as a defender make missteps that made it worse, and how do I train my team to prevent that stuff in the future?

Chris Goosen 20:55

That's fascinating. I you know, you were talking about the sparring and I remember It was early last year, I did a security training course. And I was we were on like a campus where we would, you know, we there the whole day type of thing. And then we would have lunch, and snack breaks and whatnot in the cafeteria on this training campus. And the lunchtime conversations were worth almost more than the course was because I mean, it was a fantastic course. But the lifestyle conversations were great, because the very backgrounds of the people that were on this course, was fascinating, right? We had these, like really hardcore risk and compliance folks. And then we had like, you know, kind of consultant type people like us. And then we had really hardcore, like red or blue team, offensive and defensive folks, right. And so these guys would be talking about someone like the and many of them represented some pretty large and very well known organizations. And so you hear about the ways they try and get in and it's not even only from a from a you know, breaking through network layer type stuff, but like even just physical security penetration testing, right, like trying to sneak in as a pregnant lady, or you know, get through security, physical security controls, because you're pregnant, you can't fit in, you know that all of these like wildly crazy concepts. So you just go people do that and what yeah, we run these types of operations all the time, like, get really, really good looking girl to come in and try and walk back, you know, all that type of stuff. And it's amazing how they, you know, they would target people like target a particular security guard, physical security guard, because, you know, maybe he has a wandering eye. So you bring in an attractive young lady to try and do you know what I mean, like, the social engineering aspect of this is the sound of

W

Warren du Toit 22:39

what's what's the end goal, right? I mean, I think this is also quite important, because, you know, like, if we weren't humans, and we didn't have freewill and they weren't. I don't want to swear... Pierre, I'm saving you here, pal. And I'd like you get really bad people. Okay, then once certain things for certain things, but I mean like to go and hire someone that is going to do that takes a lot of planning a lot of motivation, a lot of money to orchestrate these sorts of social engineering attacks and things like that. What is the end goal? Is it to go haha I got in or is it more of a like, okay, we're actually going to steal stuff. And it's actually corporate corporate corporate espionage and all these conspiracy theorists throughout the world. were absolutely right. And you're thinking,

N

Nicolas Blank 23:44

I can answer that very quickly. For me, based on the last three, four weeks, I think the last four weeks we've had three post breach requests and my last One was from a bank, which I will not name, who on the basis of an email, which came from a domain name, which was one letter away from the production domain. Right, however, had all the rights spam records in place, so SPF and DKIM all checked out, it should a request to accounts payable. With and you can see how much how long this breach has been been in place. I'll tell you in a second and send a request accounts payable to say please will you pay this amount? The person from accounts payable said Hang on, this looks fishy. Should I respond to this? And five minutes later, an email came back from the attacking domain saying yes, this is correct. Go ahead and pay. And what's even worse is that the attacker had crafted a PDF document With three signatures, which they had literally photoshopped on top of a PDF, so at first glance, it looks correct. But the second glance you can see was manufactured in the lost $400,000 on a Friday morning.

C

Chris Goosen 25:18

So yeah, yeah. The the goal, I guess is is trying to secure all the aspects, right, all the elements and is this fascinating? So there's a podcast that I listened to quite a lot called the Darknet diaries. And if you haven't checked it out, well worth listening to. One of the episodes talks about I can't remember the exact firm name but a couple of guys who were hired to do some physical penetration testing by a government entity. I think it was up in Iowa. Actually, it wasn't it definitely was a Dallas, Iowa. I remember because I was like downtown, and they essentially got caught but knowingly got caught they tripped in alarm at a courthouse. They had managed to get into after some recon and whatnot. And so they waited for the cops. And as they normally would, you know, when the cops come and rescue, you give them a, you know, a document that says we were hired to do this, here's the signatures of other people. But that didn't, there was some kind of, I guess, chain of command issue in that process. And these guys ended up getting arrested and prosecuted for doing this. And it was a pretty big, big, big deal. But fascinating story, if you listen to not only the things that they've that they do, to be able to try these things. So you know, I guess the point I'm making is very interesting. It's a it's a very interesting concept, right? The whole kind of blue red team thing.

Nicolas Blank 26:43

Chris.

Chris Goosen 26:44

Yeah.

Nicolas Blank 26:45

I want to challenge you on that because we talking about companies like Walmart writ large enough to have written blue team, right. And obviously, the guarding against and this is where things get super interesting because companies of that size will suffer things like nation state attack and companies or or should we say attackers with literally unlimited budgets. But what I'm finding in in customers both large and small lately who've been breached is that these are not companies with blue and red team. These are just companies who have some really, really basic things that they haven't bothered doing from a security point of view. Like they are still susceptible to things like password sprays, attacks, and they're going to cloud like office 365 that they haven't disabled legacy awesome, then they're surprised because there's an attack and that's the last right guys. Well, I'd love for you guys now who are in the dedicated security space to to pass some commentary on that way. The.. in my mind, and I don't mean this as a scare mongering thing at all. Hear me, right? I think most of the world who doesn't have any kind of security consciousness is so stunning the exposed that we actually beyond what Microsoft says in terms of assuming breach of trust exposed?

Chris Goosen 28:16

That's I mean, that's a that's a great point. And I think that's, that's part of the reason why I think it's important to have these types of conversations, right? Because I think there shouldn't be a, like a silo between the Information Technology Group and the information security group anymore like this has to become, they have to be able to work together a lot more than what's what's fascinating about the middle. No, in this is true, right? Because what's fascinating about the space, and Fran has some really good data on this as well is that historically, the security teams and the infosec guys go and buy the security products separately from the people who are buying productivity product team, right. And so what Microsoft is coming in and done as well with bundling everything together. When the productivity team buys em 365, they're now getting all of the security products, right? And so what I had seen previously with working with large customers is that you go through this massive migration program, and you're, you know, halfway through it, and then all of a sudden, the security guys are like, hang on, what is this conditional access thing you guys are wanting to it? And why would we involve when we told, like, pump the brakes? Because then they're like, well, we don't want to use a Microsoft Security product, or we weren't involved in that decision. So now we need to go and understand what the product can do and go through the whole due diligence process. So there's Microsoft that kind of tipping the space upside down, if you will, in a sense, because you kind of have to, they're forcing those teams to to work together, I think, and I think that's where this thing becomes really, really fascinating. But to your point about being exposed. One of the things that I think is important to mention is that especially in the Microsoft ecosystem, those basic security controls roles exist, folks are just not implementing them. Right. So looking at MFA, like what were the stats, something like, it's like less than 15% of users are actually using MFA every month. Everyone in every tenant has the ability to enable MFA. But not everyone is doing it.

F Francisco Donoso 30:15

That's why included.

C Chris Goosen 30:17

Yeah, exactly. And so that's why I like Emma's we should start every every episode with like, interface.

N Nicolas Blank 30:25

So let's try this one over to Fran for for some common ci, basic security stuff.

W Warren du Toit 30:33

Is that such a thing?

F Francisco Donoso 30:35

There really, there really is. I think what you'll find is that almost every compromised, larger small if it’s a small community bank or a large multinational happens, because of some small basic kind of misconfigure ation of technology, things that you’ve already mentioned. Maybe organization that doesn’t have any multi factor authentication, or even enabled multi factor authentication, but forgot about legacy protocols that don’t support multi factor authentication, which then gives you access to email which you can use to pivot as an attacker to another, another, you know, method of compromise, I could trick Chris to do something on my behalf if I have access to Kudelski Security email as an example. So I think that a lot of what you see is really the cause of this, in my mind is two things. One, it teams are moving really fast. And they’re constantly under immense pressure to deliver value to an organization, right? Because they need to that’s they’re there to enable an organization to conduct their business. Nobody runs an IT team just because they love it. They’re there to enable an organization and they’re moving very fast, and they don’t have the time to take a second and think about, okay, well how does this change my exposure? I’m about To go and put this thing on the internet, or I’ve just migrated to Office 365? How does that change the way that someone could interact with my environment? And that’s where a red team comes in, right? Because a lot of the defensive guys or even just it guys, they don’t know what they don’t know. They don’t know how a system can be misused. And the reason that hackers or attackers are so successful is because they’re, honestly all the time just being creative. How could I use this thing for what it exactly was not intended to do on my behalf to be able to break into an organization? So I think that a lot of it is the IT team just doesn’t have the time, but they also don’t have the kind of concept of how do I misuse this thing to gain an advantage or break into this organization. And the second half, I think, is security teams kind of all over the place, have built this culture where they’re just the know people. They’re the people That nobody wants to talk to, because they’re gonna cause a project to grind to a halt. Right? They’re not there to enable the business. They’re there to just say no, and tell the IT team too bad, you got to go do this all again. So I think that, that what’s really important for any organization is to build a culture where the security team is an enabler to the ITT, right? An example of this is actually Facebook and some of the big like Silicon Valley companies. The security teams are working directly with the DevOps teams or the IT teams to help enable security and make their lives easier. A perfect example from Facebook is that Facebook security team wrote a piece of code, a library that enabled secure checking of passwords, and they literally went to the development teams and said, Hey, you guys don’t have to worry about this anymore. Just use this thing that we wrote. And you don’t have to worry about it. There’s not a lot of teams that are doing that. A lot of teams take up backseat and they’re there to like I said, say no rather than collaborate with a technology team and say how do we make this project success? successful? But securely? So I think, really it is a lot of companies don’t have the basics, right? Because it administrators too busy. They put something up, they forget about it. Nobody does inventory. Well, nobody, literally any company I’ve ever worked for. None of them do true inventory. Correct. Nobody knows what they own. But at the same time, even if they know what they own, they don't know how they potentially have misconfigured it and how that could be advantageous to an attacker. So yeah.

C

Chris Goosen 34:39

So do you think that slops just changing gears just a little bit here, but thinking about sort of moved on the management side? Do you think that there's a misunderstanding between organizations using a managed service versus it with an expectation and this happens in the cloud to write this have certainly ever been discussions that I've had with folks go, Well, I want permissive environments a mess, but we might, we're going to AWS or we're going to Azure, so it's gonna be perfect and was like, Well, no, that's not quite how this works. Like, you don't just throw stuff up into the cloud. And then now it works. Right. So do you think there's a there's also a bit of a misconception that people go well, we're moving to Microsoft, to the Microsoft, you know, in 365, platform, Mexican to deal with a security now? move on? Yeah, yeah. What are you seeing? Right?

F

Francisco Donoso 35:29

I think so. I think absolutely. I think a lot of organizations are based at the very beginning of cloud, if you will, right, like Infrastructure as a Service. They didn't consider the shared responsibility model, right? They just saw, hey, I'm putting my data in AWS now it's their job, or I'm putting my infrastructure in Azure. Now Microsoft has to deal with it. That's not the case. And I think what you've seen is all of these companies Microsoft and Google and AWS have started to enable their their customers to build some really secure software in some very secure environments, essentially included right for free and their plans are there. They're doing a lot to enable their clients, Microsoft with MFA for free and all of the security features they built into even base enterprise plans for office 365. But organizations aren't taking advantage of them. Because one they either don't know or two, they think it's Microsoft's problem. The Microsoft's problem kind of aspect has changed. I think what you've seen in the security industry over the last few years is a lot of education that just because you put your infrastructure in AWS doesn't mean that you're now hands off and you have kind of no longer responsibility for securing it. So hopefully that seems to be changing slowly but surely. But at the same time, what I've seen that's unfortunate is a lot of traditional IT security guys. They don't know how AWS or Azure works, right? They don't know how office works. So they're put in this position where they're familiar with maybe the on premise, legacy way to do things. But they also need to learn about these technologies to be effective at securing them. And a lot of a lot of organizations are enabling their security teams to go and learn that stuff. So they can be effective. hopefully that answered your question. Yeah, that's a definite. that's a

C

Chris Goosen 37:30

that's a fascinating point. Do you think? I mean, there is obviously a very big difference between your traditional managed services type business, right. And Nick, you know a lot about managed services. It's something that you're involved with every day. And then the concept of managed security services, right. I mean, it's it with us just unpacking the differences, Dave, about what, what customers should expect when they sign up for one or both of those things. Because Because many security services is very different, right? And that's a part of your background too. So, I mean, you know, should we should we go into that just a little bit? I think that'll be fascinating topic.

F

Francisco Donoso 38:11

Sure. I just want to start by saying that it's really interesting to me because some of the nation state attackers that Nick mentioned earlier, have found that the soft underbelly of these large mega corpse are actually their managed service providers. There was a report put out, if you google the words cloud Hopper, it was literally about how China or Chinese nation state actors, were breaking into companies like IBM or other large managed service providers, not managed security service providers, because this one single company has access to a multitude of different environments for some very large organizations. So they were actually compromising their managed service providers. So that is Pivot into other larger organizations, because that may have been easier. So I think that what you're going to see, and what we're going to continue to see is these really creative, truly nation state actors who have unlimited resources, they're going to target the big guys that have access to a lot of environments as epileps. Because that's, that's really valuable. And what I've seen from a traditional managed service provider, someone who's maybe your outsourced helpdesk, and who's helping you manage Active Directory and helping you, you know, deploy new new servers or what have you. They typically see security as kind of like a full time, right, something they have to charge their customers extra for. And that's where this managed Security Service Provider space came in. And, and what I've seen, unfortunately, I'm going to be totally transparent here is that a lot of managed service providers that are specialized in security, so many security service providers, are actually detrimental to their customer security. I've worked for a lot of msps. And what happens is clients hire this mssp, they no longer feel responsible for their own cyber security. And the mssp is not really built to support them in that mission, right? They're just like, Oh, no, that's fine that mssp will deal with it. I don't have to worry about and these msps a lot of them were built in really interesting ways. I'll give you an example. I used to work for an mssp organization that was built because the company used to sell firewalls. And one day, a sales guy sold a lot of firewalls. And the customer was like, Yeah, but what if I paid you to manage them too? And the sales guys like Yeah, that makes sense. We can make this profitable, and they built this entire mssp that just kind of got bolted on, right? That's like, hey, okay, well, I'm gonna go hire some fresh out of college kids to manage these. I don't know if that's In firewalls for this customer, and it just kind of snowballed. And what happens is these managed security vendors, they never take the time to think about, okay, well, how do I actually provide value to my customer and defend you perspective, rather than just managing a firewall, or managing a web proxy or whatever other security technology? So truly, if I'm being transparent, spending my career in managed services, a lot of managed service providers are a detriment to their customers. And that's, that makes me really sad personally, right? Because we should be helping our customers, but most of them, unfortunately, don't. But I know that that wasn't exactly what's the difference between an MSP and an SSP and the real differences, one of them should hopefully be focused on security. But, but truly, I think a lot of organizations need to kind of take a step back and understand what's the additional risk that I'm introducing to my business by hiring a company that will Absolutely be targeted by threat actors.

W

Warren du Toit 42:05

It's not a one size fits all thing as well. And I think a lot of msps sort of fall short on that too, because I'd say they're vendor specific. And so vendor specific, we only use Palo Alto or we only use fortigate. Whatever the case would be is, it doesn't encompass everything. It's not taking this broader security. Look at it. It's more like, Okay, well, the people that I'm hiring know this, so they will use that. And then what happens is, that's what we are going to sell to the clients. And then at least we know that we've got our bases covered. But the way you do one thing in one technology and the way you do something in another technology are completely different. And it's like you said it just a little bit earlier and moving back to this whole intrinsic versus it thing. And I find that's the biggest issue that I'm exploring Ignore the moment personally is yes. infosec say no, because that's their job. Understood. But also at the same token, they're not very helpful. They're not very, they're more like, how that you redo that and come back to me when it's done. And then I will say yes or no, it's not like, okay, maybe we can do it this way. Or maybe we can do it that way or, because they're just like, nope, come back. Try again. As opposed to that, that helping that you were talking about, and I think it's very, very important, especially in the times where we're like, oh, AWS does this edge. It does that. How about we just put an NVA and then it's the same both? How about No, you know, what I'm saying? And so what happens is you end up with two MBAs vendor specific in two separate clouds, because you're trying to make them The same, but in actual fact that should be okay. Well, there are different technologies, but you will apply similar principles using their technologies and you end up gaining and i think that's that's, that for me is is a is a big issue at the moment. I don't know about you.

C

Chris Goosen 44:17

I think my opinion on this is that it's very much a cultural evolution of cloud computing. Right. So if you think back to when we were deploying Exchange servers on premises, and Nick and I worked the project probably 15 years ago, where this was very evident, right? The messaging guys only looked after the exchange environment. Then you had, you know, guys looking after SharePoint firewall team, their endpoint team yet like you had like 20 different teams looking after all the various aspects of the Productivity Suite, with Office 365 coming in, and these things becoming more tightly connected. I think one of the evolutions I've seen and certainly the organizations that I've worked with who have made The best strides or at least had the best adoption of office 365 have been companies who have looked at this and gone well, that structure doesn't work. We need to have a team of productivity people that yes, maybe some person's skill set is more SharePoint or teams focused. Another person might be, you know, identity person, but they need to work together to make the platform successful. Right. I think that the next part of this evolution is getting the infosec teams and it traditional IT teams working together as well. Because at the end of the day, like all of this stuff has to sort of Mount together for it to become successful and secure deployment, like you can no longer look at just security as a theme. It has to it has to be built into everything that you do, right as a as a default. You know, cloud first, but I almost want to be like new security first, plus second, but it's really

W

Warren du Toit 45:57

Oh, nice.

F

Francisco Donoso 46:02

Fair enough. Yeah, I totally agree with you on the infosec teams that IT teams need to work together. And I think honestly, the biggest thing that any security team internal to an organization can do is be more approachable and be willing to help more. You're not there to say no. And the more you say, No, the more people will bypass you, right? Like this. If you're just the no guy that's gonna take a critical project, and just halt it, nobody's gonna come to you, and it's gonna make it to production, and you won't even know it exists. And a lot of a lot of a lot of security guys just make that mistake where they're hired top of the tower, and they're just the people who get to say, we do it or no, go do it this way. But at the same time, a lot of what I've seen personally, is some of the older traditional security guys. Maybe they're not familiar with AWS at all, or maybe they've never even written an application, right? A lot of what we're transitioning to is, hey, there's a lot of custom development going around. There's a lot of DevOps going around. There's a lot of how do I deploy things to cloud with like something like terraform, right. And the security teams have never use these tools. So they're in a position where maybe they have, I don't know, a vulnerability scanning tool, and they get the report and they go tell the developer, hey, go fix this, but they don't even know how to fix it themselves. And I think that's the most important part of being a security practitioner, is sure, you should be aware of how attackers are breaking in and maybe you should be aware of security best practices. But maybe, just maybe, you should be aware of how to use the technology that you're trying to protect. Because unfortunately, I've seen a lot of security guys who have never deployed anything to AWS or never deployed anything to Azure. And I think Some of the biggest value that I've ever found, is putting myself in operational positions where I have to figure out, I'm an operations guy now or I'm an IT guy now, how do I deploy this? And then how would I secure it? So I really hope that what we see as a transition, as we're, as a security kind of community that we begin transitioning to, hey, I'm not just here to tell people don't do this, or go redo it. I need to learn about the technologies, I need to test it myself. I need to try it myself. And then I need to collaborate with the IT team based on what I've learned to make them successful and make the business successful. Because no company other than cybersecurity companies is in the business of security. Security is a business enabler and a risk reducer. Nobody does security because they want to be secure. Truly, nobody. They're all there to enable the business

W

Warren du Toit 48:57

There's the title of the episode.

C

Chris Goosen 48:59

That was just thinking that actually, I. So I think a couple of thoughts I have on that which is, which is kind of interesting. And he kind of brought up here is one of the things I've, I've learned in my time and you know, the three of us spend a lot of our time in the community doing community stuff writing vlogs, that vast majority of the last 10 years, for me, at least have been spent doing that for Nick, it's, you know, even longer than that. And there's definitely a difference in the community interactions between, you know, infosec, folks, and then just your traditional IT pro people, right. And you it's very evident if you, if you go on Twitter, and you look at and I think it's changing, I think the younger generation of infosec people are becoming more community focused at least about kind of sharing things and being open to just contributing to the community and taking and give it's a give and take relationship, right. But I certainly have found that there are there's a very guarded approach. In the community in the infosec community, in many aspects, I think, you know, we've we've been very welcoming of inclusivity in the in the IT pro community, I think it's and dev community Sorry, I always say it Pro, but I always include the dev guys into that as well, because, you know, it's very much part of it. Microsoft did a great job of that inclusivity message. But I find that that's still lacking a little bit somewhat in, in infosec. And if you look at, you know, I follow a few female infosec pros on Twitter, and if you look at the abuse that they get from men in particular, it's disgusting, actually. And I'm actually proud that that doesn't really happen in the Microsoft community. But that, you know, it saddens me that that's still happening. And I think as a community, these things need to also be addressed Because ultimately, we all have the same goal here at the end of the day, right, which would you know, as Fran said, it's about enabling productivity and reducing risks. Right. And collectively,

W

Warren du Toit 51:01

I just want to jump in the creek and I want to say like, are you guys not stressed? lack? Because if a hack happens, right, whose fault is it? So we hired you guys to fix this problem and we got hacked. So why infosec so grumpy is because they know that it's their ass on the line if something goes wrong, and I don't know if I'd be able to sleep at night, if that was, you know, my thing.

C

Chris Goosen 51:41

I can tell you from experience that I know Fran doesn't sleep at night.

F

Francisco Donoso 51:47

Well, I think that honestly. Yes and no. I think that most of the really good security people that I know Have this in the back of their minds with everything that they do. Right, which, which drives them to be successful, which means they need to understand the technologies that they're scared. They need to have very strong relationships with the development teams and IT teams and the infrastructure teams. So I think yes or no, I think what you'll find is that a lot of traditional security people will kind of sit back and say, I told you, so I told you this was going to happen. You didn't listen to me. And and never take a moment to reflect and say, have I personally built a culture where nobody wants to talk to me? So maybe that's why they didn't listen to me. Or have I built a culture where if a team comes to me, I'm going to tell them no, so they're just gonna bypass me and put it on the internet anyway, is that not my responsibility? It's not my job, and I fall. So I think that a lot of what you see from traditional security folks, unfortunately, is I told you this was gonna happen. He just didn't listen to me. So I, I hope that there's a mixture of that, but some of the best security folks that I know absolutely we, we stay up at night thinking about oh my god. Okay, so how do I make this better? And a lot of how do I make this better is not technology, it's relationships and it's building a community and it's working closely with teams outside of security. And a lot of people don't do that retrospection.

Right. They don't think about, well, why didn't anybody tell me about this project? Is it because maybe I've just I'm not good to talk to when I when I

W Warren du Toit 53:35
say no, that's

F Francisco Donoso 53:37
exactly, exactly, exactly. So I think. I hope that some of that is changing in the community, but I don't know. And then also really, the reality is, a lot of security vendors, unfortunately, have started selling these snake oil, easy solutions. Just buy this thing. It has machine learning. It has AI it uses The cloud, it'll just solve all your problems. Security is super hard. And you need to be methodical, and you need to be detail oriented. And I've never until now, where we had the opportunity to build a managed service practice that I'm proud of, truly, I've never worked for a security company that literally sat our customers down and said, Okay, this is going to be really hard. But we're here to work with you. It's going to take six months to really make sure we understand your business and make sure we methodically approach how we're going to secure your environment. Every other security vendor, every other security guys like rapid time to value, buy this product, it solves every problem. That's never the answer. That never works. And some of the most disillusionment that I've had personally as a cyber security person who truly loves like the security, world and technology and I love learning about things is that There's so many security vendors that are just selling snake oil, and they're just peddling stuff that they know it doesn't work, but they're giving their customers a false sense of security. And it's just so disillusioning, like honestly, I don't know if this is the same for other parts of the IT world because I've been in security so long. But I just constantly feel that if I go to like some of the business conventions within cybersecurity like RSA, I just walk around this space, where vendors are just selling stuff that they know doesn't work. And I don't know how those people sleep at night, right? Like, I don't know that and I don't know if this is a systemic problem in technology, or if cyber security companies are just like pretty scummy, in general, most of them

C Chris Goosen 55:50
i think i've seen we've definitely seen our fair share of that type of stuff in the migration space right wherewhat you know, the expectations beingset by By migration vendors and or and or consultant consultancy companies who who do migrations don't always meet their own match the reality of the of it right? All of this is seamless, your users won't even know. Like, yeah, I mean, is that really true? Like it, you know, there's always going to be

some, when you undertake a migration project of any sort, there's always going to be some pain and hassle with users. Right. And I think that's also why the whole organizational change management movement is has accelerated as much as it has. And you know, we've had some great ocm guests on the show previously, but so I think that exists everywhere. But you know, it's a good point. And I think just, again, just honest, honesty and transparency is just, it's important in every part of, you know, the way we do business, how we interact with our customers. And it's an important thing, we can't lose sight of that, right.

N Nicolas Blank 56:54
I hate to be that guy, but I've got to be that guy.

W Warren du Toit 56:57
So I think we could have gone on for hours dude, but thought it has to happen.

N Nicolas Blank 57:05
But before we go, I'd like for him to leave our listeners with. Okay, I've heard the stuff and I'm really worried I'm not gonna sleep tonight. Yeah.

W Warren du Toit 57:18
Always please.

N Nicolas Blank 57:20
What if if I am a, this is valid right back down. I'm a I'm an overall system. I could be a developer could be an IT pro could be a business person, I could be a C. So I've heard all the stuff. I've heard the show. I'm thinking I'll quit my job. Instead of quitting my job. What are the one two or three or something tangible? What can I do? Now? What could I do tomorrow? What can I do to be safer?

F Francisco Donoso 57:53
Yeah, I'll start with the one thing that nobody does correctly. inventory, the most unsexy We think in security, but the most valuable. So please, whatever you're doing, try to figure out a way to automate inventory, you need to know what you have to know what you need to protect. The other things that I'll say, are all of these vendors, Microsoft, AWS,

Google, they've spent a significant amount of effort and time and money, building security best practices, and enabling your business and your developers and your teams to do things in their environments and their cloud securely. So just take a moment and just go through and read some of the fantastic documentation that all of these vendors have around security best practices. Maybe before you go and roll out office 365 or you go to Azure. Just take a moment and read what those best practices are, and familiarize yourself with how attackers are attacking. And then finally, I would say, help build security teams or hire consultants who are familiar with the technology that you're trying to protect. That's, that's really important. As you look to transition to the cloud or to these environments, you need to have security professionals who have actually used the technologies that you're trying to protect. Either in their personal time in the lab, it doesn't matter. But whoever you're hiring, either internally or externally, make sure they've used it, make sure they've deployed a, you know, an easy to instance or Azure VM or whatever. So that they can help you understand how your team can secure some of those environments. Hopefully, that helps. But really, those are the three things that I would inventory. Nobody doesn't, right. Please try to do that. If you're going to the cloud fresh, figure out how to do automated inventory, all of these, all of these cloud platforms have a way Do inventory in one way or another across subscriptions or accounts, try to use that as much as possible

W

Warren du Toit 60:06

Taggling, man just tag everything stay for a reason.

C

Chris Goosen 60:12

That's very, that's very insightful. I think, you know, in many instances, the, the attacker knows the platform better than you do. Right? So you really need to spend the time making sure that you actually understand what what you what we're working with here. So that's, that's awesome. Fran, it's been awesome talking to you as always. And before we go, is there anything that we can would that you would want to plug? I'm not sure how active you are on social media, things like that. But if there's any way you know if you want to put that out there now feel free to do that now. Guys, any closing thoughts from you?

F

Francisco Donoso 60:48

Yeah, I'll just say, hey, nothing really to plug my Twitter handle is @Francisckrs. ridiculous to find. Don't worry about it. Make sure that Chris has a link to it. But it's been a pleasure, guys. It's been a blast. I really enjoyed talking to you and I hope to be able to do it again.

W

Warren du Toit 61:10

Oh, yes, yeah. Everyone, before you go, we just wanted to say thank you for listening. We really enjoy putting this podcast together for you every two weeks, please visit us at thearchitects.cloud. Alternatively, drop us a tweet. We'd love to hear what you have to say at @thecloudarch.