Episode 45: Microsoft 365 Security for IT Pros

Wed, 8/5 12:00PM 36:14

SUMMARY KEYWORDS

book, security, chapter, people, defender atp, microsoft, cloud, framework, pages, folks, kemp, writing, updates, build, azure, platform, tony, professionals, author, approach

SPEAKERS

Warren du Toit, Chris Goosen, Nicolas Blank, Michael Van Horenbeeck

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 Hi, and welcome to another episode of the cloud architects podcast my name is Nicolas Blank and I'm here with my co host. Christopher Goosen.

C Chris Goosen 01:04
Hello.

N Nicolas Blank 01:06

Today we have a guest which we featured on the show before Michael Van Horenbeeck

M Michael Van Horenbeeck 01:12
Hi, everyone.

N Nicolas Blank 01:14
Welcome to the show. And thank you so much for appearing again. We are excited that there's something that you are launching fairly soon, and it's a book. So without wanting to spoil too much, why don't you tell us what your book is about and why you've decided to write it?

M Michael Van Horenbeeck 01:37
Sure. So the book is called Microsoft 365 security for IT professionals. And some of you might recognize that the title kind of resembles the office 365 for IT professionals book, um, which is done on purpose. A couple of years back Tony Paul Cunningham and I we started a venture Adventure I should say of writing a book which is kept up to date on a monthly basis, the office 365 for IT professionals book. The reason why we started that journey a couple years back is because the cloud is moving at lightning speed updating you almost on a daily basis. So trying to create a book which isn't outdated from the day that you publish. It was an interesting challenge. And I believe I wrote for the Book Three, four years after original work life got in the way so I kind of dropped off as a as an author and an entire team took over from Paul me. And, you know, there's a whole author team out, but still you I like to write. In the meantime, I also switched over to the security side of things where over the past couple of years, all I've done is security, security, security. And I noticed there wasn't really a security book in the same space or following the same model kind of keeping up to date on a monthly basis. And you know, With the focus from Microsoft on everything, you know, security and compliance, there's a ton of stuff that's changing really like a lot of that. So I figured, you know, let's bring on that challenge. Let's try and write a book and keep it up to date at the same pace. But rather than focusing on the productivity side of things, just focus on the entry 65. and, by extension, a little bit of Azure Security as well. And that's how we got to the book, which, by the way, we should be releasing very shortly.

C Chris Goosen 03:29
That's, that's super exciting, I think, for a number of reasons. Right? I think, one, I think that most people or at least a large part of the audience will understand or know of the office

365 for IT pros venture and the work that you and Tony and everyone have done on that because it really is the standard as far as you know, a book of knowledge around office 365 goes right and I it's something that I've given to customers in the past when when I've worked with customers, and they've said hey, where do I go for free? Knowledge, where do I go to learn more about office 365? What training courses can I go on? I've given them a copy of the book. And on here you go, actually hijacked Tony once at Ignite and made him sign a whole bunch of USB keys for me. He wasn't he wasn't pleased. So I think that that same kind of methodology is is fantastic. Because I think one of the things I've found over the last little while since I've started doing a lot more security focused work as well is sometimes the documentation is not quite where the where the product is. And so all I can say is, you know, hats off, and congratulations, but it seems like a mammoth challenge to me to be kind of taking that on keeping that publishing kind of cycle going on something that is that bleeding edge.

M Michael Van Horenbeeck 04:45

Yeah. So, I mean, you have no idea how much effort it goes into the book. We started writing last year. And you know, the initial effort of writing a chapter is massive, right? But as you're writing the chapter, they keep changing stuff, and you're like finding yourself writing a bit of bits and pieces and then rewriting it and then writing new bits and pieces and rewriting older stuff that you've written a couple of weeks back. So to get to the point where we're, you know, ready to release has been a massive undertaking, but the real challenge starts now, updating the book on a monthly basis. If there's one thing that I've learned is, don't underestimate it. I did in the past a little bit where, you know, sometimes I didn't account for the time to write the chapters, right, which meant that I had to know doing last minute, which added a lot of burden. So I learned a lot from the earlier process. My respect for Tony for, you know, keeping the book up to date for keeping everyone in line and for doing the copy editing is just grown tremendously. Because now I'm taking on that role and I'm like, Oh, god, what do you do, you can start with, right? But at the same time role, so you know, trying to get to the point where we want to be that book of knowledge, right, where we want to centralize everything, get that practical guidance. But it's a journey, right? Even version one that we're releasing, we know their stuff that we should get in there over time. Like, I'll give you a practical example Office ATP, right due to some author challenges, you know, people dropping off halfway, because they, they figured out, hey, this is too much of a word for us. We had to cut that chapter on version one. So we're going to add that word as part of the release, you know, in a couple of months time. But that's a massive chapter, right? Like our Defender ATP chapter, even without practical deployment guide information is 120 pages on that one, I'm not gonna call it a little thing. It's just it's quickly becoming this huge mess of stuff. And I think we'll learn as we go, but it is it is it is interesting to see at the very least.

C Chris Goosen 06:53

Yeah, and I think the thing is, and we've said it on the show before it may even have been on the last episode where we you know, we call Microsoft, the security vendor, right? Because At the end of the day, that's kind of where they are right now. And, and a lot of folks, and I'm seeing this firsthand with my recent role change, people don't take Microsoft seriously in the security space yet, or at least a lot of folks don't. But when you're able to look at something like this and go, Well, this is how it all ties together. And the small thing that's just a, just a tiny little endpoint thing is 100 and something pages worth of documentation. It's really stunning to say something and I think it's gonna be a very easy way to quantify the value that the platform brings. Right when you when you when you tie all these services together.

M Michael Van Horenbeeck 07:36

Yeah, I mean, and there is another interesting tidbit, which you're just kind of you mentioned Microsoft cybersecurity vendor, I'm entirely with you. There's things they don't do, right. They don't build firewall. They do build Azure firewalls, but don't build physical firewalls and stuff. But they have a whole plethora of options and solutions that somehow tie in together. They have a vast ecosystem and it's uncovering value. system, which is the interesting part and also the hard part. But at the same time, you know, putting everything together as an author team, we were already facing the, you know, where do we put this in which chapter with this belong? Or like this feature, it belongs to product x, but he really belongs more to this new paradigm. So where do we put it into the book? So why expect that will happen is over the course of the next couple of months when, you know, feedback trickles in when Microsoft, you know, releases new stuff, and God knows what they've got planned for this year. You know, we'll be modifying and updating the book and that's the beauty of dating monthly, right? If something doesn't belong in one chapter, or we can take it off next month and put it somewhere else where it belongs better or where it feels more natural. But we see that today, like, honestly, we've had discussions about you know, Windows Information Protection. Well, you know, do we create a chapter on Windows 10 security and if so, well, what about Defender ATP or attack surface reduction resource protection? Do we keep it in Defender ATP? Or do we put it into Windows? 10 per day? Yeah, it's kind of like, you know, ongoing discussions the entire time.

C Chris Goosen 09:06

Yeah. And I think this is probably this probably is a really good insight into how meetings within the Microsoft marketing department go, right? Because they're constantly, they're constantly like they changing the product names, but also the product name doesn't

always align 100% with the rest of that, the platform, so I could definitely see how that would be a slight, you know, slight challenge.

M Michael Van Horenbeeck 09:27

Well, and you know, it's not just that Microsoft 365 security for IT professionals. So you know, obviously even looks at the 65 side of things. But what we've already committed to and we started writing is an Azure Sentinel chapter now. Better Sentinel? No, it is and it isn't entry 65 because it's Azure workload, but yet we put it there in the book. So you know, you can see the cross the bleed between the two worlds, your productivity and Azure, which is typically infrastructure, kind of converging in becoming one so you know, maybe we should rename The book from the get go to Microsoft Security for IT professionals editor.

C Chris Goosen 10:04

Now that makes sense. I mean, I think where you're at now, I think it, it's definitely gonna resonate with the way that it's named. And I think immediately, when I saw news about the book it immediately I was able to put it together and tie it to, you know, the other author team and the work that Tony is doing. And I think that's really valuable, because I think not only are is it going to be a natural progression for folks who are in the IT pro space, who are now possibly becoming more comfortable with Office 365, and with the 365 workloads, and now starting to think a little bit more security focused. So this is a natural progression for them. But this is also a really good entry point for just pure infosec folks who have not played in the micro space before, right. And there are a lot of people like that there are a lot of people who come out out of the Palo Alto, Cisco, etc. World CrowdStrike world who have never really dipped their toe into the Microsoft ecosystem. I think this is going to be a really, really good entry point for them too. Gotta get involved and see what's what's actually going on.

M Michael Van Horenbeeck 11:02

Yeah, so and that's, that's really important what you mentioned, because, as you said, there's a whole audience that's familiar with Tony's book, The Office 365 book. And obviously, they, you know, after having read the book, you understand the product really well, the product platform, I should say, really well, I have certain insights. So the jump into the entry 65 security is more natural, but there is a whole, you know, a whole army of people out there that you know, are less familiar with Microsoft products as a whole, but they're now you know, faced with new implementations, new features, you know, Microsoft everywhere these days. So what we try and do is, you know, to keep it

accessible, right, not start up there, but you start slowly and then build up gradually to the book, which is also one of the reasons why the first chapter is not a really a technical chapter. It's more you know, okay. So how to approach it security, because people come from a security background, they have this person in mind if this you know, thinking like their security It and someone who's coming from the productivity side doesn't necessarily have, you kind of have to blend them together to kind of mix and match the both worlds which, in itself, we didn't want to create a 300 page book about process because that's though, everyone, you know, understands why it's necessary, but it's still dull. So we kind of slimmed it down to about 1520 pages to kind of get everyone in that same mindset, and then take them on a journey with identity, Device Management and support and so on. Okay, yeah,

C Chris Goosen 12:26

that makes sense. I think that's a pretty, pretty important way to kind of approach it right. And you kind of have to have a mix of those various components. You can't just be all technical or process because you end up losing out on a bunch of, you know, folks lose out on a bunch of things that they're looking to learn. But also, you're not hold at that point. You're not you know, you can't be completing a job if you don't understand, you know, a little bit of all of those pieces.

M Michael Van Horenbeeck 12:49

Mm hmm. I agree. Yep.

C Chris Goosen 12:51

Okay, well, look, Nick, I think Nick might have a question here.

N Nicolas Blank 12:54

Yeah. I wanted to ask Michael, who is the primary audience for this book is Is this an operations person who needs to add security to the landscape? Or is this for a hardcore security person who needs to add Microsoft to their landscape?

M Michael Van Horenbeeck 13:11

That's a good question, Nick. I think there's value for both right? This is for the none. Well, tech savvy but non security savvy, IT professional that needs to do something with with something and security in Microsoft 365. I mean, we all know how to sale cycle work,

right? Then the Microsoft sales sales guys there and tell them hey, it was a great discount on, you know, the interesting divide the five security bundle, and the company says, Yeah, great, let's do this. And then, you know, it rolls downhill to the security teams or the operational teams or like lowers first time that we touch X, Y, or Z. You know, what can we do with it? How do we do it? What's the best practice? What are the caveats, right? So some of them may have the actual office 365 experience and some of them may be coming from a purely security perspective, like looking In our company, and the projects that we do is we've got exactly that happening. Like I've got one project for customers migrating from McAfee to Defender ATP. And we're dealing with people that have dealt with McAfee for years, they know the product inside out, they have no knowledge whatsoever of Defender ATP. But you know, just looking at defender by itself, you can't because it's part of the holder, your bigger ecosystem. So it kind of ties in together with that whole entry. 65 steps are prevented, super valuable to have secure resource. But the same is true. If you're coming from the other side where, you know, we've come from exchange like all of us, all three of us were hardcore old coal exchange, guys, we turn a link to security, you know, a couple of years back if a book like that would have existed, I would have surely appreciate it that rather than going out and having to figure out everything on my own,

N Nicolas Blank 14:49

completely right, but just like so many other things in the IT landscape, is there a process that I can follow in so Yeah, I'm kind of picking on from an IT professional point of view. I could be ITIL aligned from a security professional, I could be mature aligned. How do I align myself against the knowledge in the book?

M Michael Van Horenbeeck 15:13

Yeah, yeah, I agree. So I understand what you mean, I'm so this is where the first chapter clinic comes in. I mean, there's so many frameworks out there that you could use to actually, you know, build a build a strategy on what you're going to do. Personally, I am a NIST cybersecurity framework fan, right? With the different phases, but there's organizations that adhere to whole other standards that have built their own standards, in my opinion, and you know, maybe some people will be printed in what I'm going to say, but, you know, I don't care which framework you use, as long as you use a framework, you have a plan that works for you. I'm happy, right? So that's also what we try to explain that first chapter. I do mention meter. And you mentioned ISO, or you mentioned a PCI DSS or you mentioned Mississauga security framework. I explained to the people in here, these are the frameworks look at these are the highlights of these frameworks now go out and figure out what, what's important to you. Obviously, if you're a financial institution, PCI

DSS will come up really quickly. And even there, we try and give some practical examples. Like there's this huge mapping sheet between all the different frameworks that tells you you have the controls in this framework equal the controls in that framework. So we refer to that to that sheet to tell them you know, if you're already compliant with this, but you want to look at the other one, just use that cheat, do the mapping so that you don't do the work twice. But at the same time, we don't want this to become a book on how to use the frameworks. There's plenty of books out there that explain these frameworks into details. You could go on certification on once one framework itself. So we wanted to explain why they're there and where it's important, but we didn't want to go into the detail of, you know, this is how each of them work.

C Chris Goosen 16:57

I think that seems that sounds like a really, really good approach. Honestly, and I, I, for one can't actually wait to get my hands on this so that I could actually have a have a look at that, because I think that's definitely something that I've found particularly challenging kind of entering into this this world is is the fact that everyone has a framework that they look up to, and that is super important to them. But the relationship between them, and then I think it's that's a super important kind of introductory step for sure.

M Michael Van Horenbeeck 17:25

I agree. Yeah. facing the same challenges, right for moving into ISO certification 28 27,001 for our own company. Oh, my gosh, it's like there's a whole avalanche of stuff coming to you. And you're like, Really? So yeah, no, it's getting trying to be practical. I think there's, we could write 100 pages about one of the things but we deliberately kept it, you know, short and sweet, I'd say.

C Chris Goosen 17:49

Yeah, I think that it sounds like it. Right. And so the question I had for you was, I mean, this so much as far as security functionality goes within within the service, right? But I think there's a lot of organizations that still have this mentality that we've given out, we give Microsoft up monthly subscription money, and we've put our data in their service. Why do we have to worry about the security functionality of this? Right? Shouldn't Microsoft be taking care of all of the security functionality for us? Why are we having to care about this? I mean, are you coming across that in Europe as well? Is that something that you've seen?

M Michael Van Horenbeeck 18:25

Yeah, I mean, less than less, to be honest, because people are getting more and more used to the cloud model where, you know, there was a segregation of duties, where, you know, infrastructure, sure, that's Microsoft Word, like physical security. Sure, let them take care of that. But you know, the layer that you build on top of that solutions that you build on top of that, you know, people are starting to understand that that's your responsibility. Now, there's still a whole long way to go. There are still a lot of companies that try and get around why do we need x y, z. But you know, the reality is is that whenever you see today, These days in the news, there is breaches you're far and few in between. Every day there is a breach. There's a leak or something. I think, you know, gradually people will understand. Alright, we need to do this. Like, you need to lock your door a couple of hundred years back, no one locked your doors. There were no locks. Right? The doors are open. Well, today go out and find a house where there's no lock. Hmm. Yeah, I think it's pretty much the same.

C Chris Goosen 19:26

Yeah, I think that that makes sense. I think enable multi factor everyone if you haven't done it MFA. It's just my, my, my PSA for the day. I you know, we got to make sure to pull that out in every episode, just because it's such an important thing. You know, we see, I although I think the last couple of weeks have been very much taken up by f5. And their vulnerability that everyone seems to be bypassing or whatever, but definitely a lot of the things that we're seeing could easily be have been mitigated by just MFA, right? But companies I think are just folks are not being educated and and they're not kind of taking that active decision to, to go, hey, let's see how we can continually improve this. This is not the cloud is not set and forget, right? It doesn't matter what any vendor tells you, you can't just go and throw your data at a service, pay them and forget about it. Like there has to be a continuous improvement model that, you know, you're going to be looking at where the threats can come from, because at the end of the day, the bad actors continue to evolve as well. Right? And you can't, you can't just go Okay, well, this is the assumed knowledge everyone has, and we're gonna we're safe. Yeah, you might be safe today. That doesn't mean you're safe tomorrow. Right? So I think that this whole thing with f5 is really kind of shown. A lot of folks that are, you know, a lot of organizations that are slower to move to the cloud and stay or staying on prem, because security right are now the ones that are targeted by this, you know, this thing in their security, like their, their legacy infrastructure, if you will, right. So this is a very, very interesting thing to be kind of paying attention to

M Michael Van Horenbeeck 21:00

We mentioned it in the book, a little spoiler there, but it's about 68% of all breaches in the cloud originate on premises like 68%. Yes, that's, that's a large number. And again, you know, attackers are people with intent. They'll always take the path of least resistance. If it's easier to get into your cloud through your on prem environment, they'll do that, right? And this is just true. I mean, when a pen test happens, you should know, right? kudelski does these tests, right? Whenever a pen test happens, I rarely seen them go after Azure. At first, they're like, Okay, let's try and get into the device. And we're into Active Directory, then some letter Academy movement, and bam, we've got your domain. And then from there, it's easy to get back back up into the cloud. You know, that's where the challenges lie. So the people that are full traditionally on premises, they have a lot of work to be done there a lot more than, you know, lowering your attack surface in the cloud, but at the same time, it's very different, right, the things that you have to deal with on premises No, they're not the same as in the cloud, which is also one of the messages that we're trying to get across is like, it is changing sure devices device, that doesn't change. But you know, Cloud Platform cloud applications, they operate in a very different way. The your security is a very different way and therefore have different security measures or how to approach that.

C Chris Goosen 22:24

Yeah, and I mean, even getting down to managing those that infrastructure, right, the way that you typically would do that on premises versus the way that you're possibly doing it today, it's very different in the way you approach it. So it's kind of like I think the message really is that you have to be able to adapt to the way that you know, the new modern way of doing things and you can't be stuck in the old world for too long, right. Otherwise, you're gonna you're gonna lag behind. So yeah, that's so. So we've talked, we've talked a lot about the book and honestly, I personally can't wait to get my hands on a copy here. Can you give us some information about where when how all of that?

M Michael Van Horenbeeck 23:02

Sure. So not sure when the podcast is going to be released. But our target is to release July 13. I've got a full weekend of copy editing, building the book and you're getting the PDF ready. We've got the website up. So the entry 65 security book comm where you can get to the book files are actually to the government platform through which we're selling the book, which is the same platform as the office 365 for IT pros book. So money 13th the book will be available, obviously, it will make a big splash on LinkedIn, Twitter, the website itself, we'll make it known and then hopefully people will find their way to the book itself as well.

C Chris Goosen 23:42

Okay, and would you are you gonna be releasing on Amazon as well? Oh,

M Michael Van Horenbeeck 23:45

no, that's a deliberate choice we we've made and actually I'm leaning on Tony's experience of building the book for Amazon. There's a couple of things like the the amount of effort going into building that book or the E pub and making sure that In Amazon, that's one thing. Secondly, Amazon doesn't support monthly updates. gumroad is easy, because it's just changing the PDF like first one to version two and off you go. Right, nothing else changes. And because of that, I didn't want to take on more work. Plus, you know, supporting the authors supporting the marketing, the hosting everything for the book cost money. Amazon, you know, takes a 70% cut on the book. Wow. Which, you know, it's great because you reach a bigger audience. But at the end of the day, I just think that the effort you put into it, and the gains that you get from it, and the gains that people get from it, are too liberal to justify using Amazon as a platform.

C Chris Goosen 24:40

I think that makes sense. I mean, personally, I've, I've always used the, the gumroad platform because I prefer just having the PDF copy of the book, right. It's more portable for me. I know others disagree with that, because I want to use Kindle and whatnot. I you know, it's not my preferred method of reading. So, you know, it is what it is. But yeah, mix. I think that makes sense. And I think it's good Good to get the message out there to folks like this one platform. That's where you can go and get it. And that's also where you get your your updates, right? Because that reminds me how the subscription model works again. So you, you buy an edition of the book and you get all updates that are part of that edition, correct?

M Michael Van Horenbeeck 25:14

Yes, Yes, correct. So there is a yearly cycle. We're starting July of this year, which is coincidentally called the 2026 or 20 2006 edition. But anyway, so the 2020 edition runs up until June of next year, you buy the book, you get all the updates that year and you know, we are committing not just to updates of the chapters, but this year we'll also committed to a practical guidance chapter on the ATP on an Azure Sentinel chapter and Office ATP chapter. So with the book, you know, you'll be getting that. And then up until June, you'll get updates sometime next year, March ish timeframe, will start thinking or building the new book, which means new edition 2021 edition. We may you know, do completely

overhaul we may add more chapters into that really depends on Oh, ever everything, you know, moves along. I mean, we all know that Microsoft is doing shifting in that space as well with the acquisition of cyber x in the OT space. So we're closely monitoring that. And then based on that, we'll build a new book, new edition, and from there on, people who have bought the first book and can get the new one at a discount, you know, kind of your appreciate their, your, their loyalty to the book, and then they get updates for a year as well. So there is no monthly fee, it's just a one off and then you'll get the updates per year.

C Chris Goosen 26:36

Yeah, fantastic. And I think what's what's great about that, and certainly, you know, the way that I've approached this with with the the other book is that the book is so large now, it's gotten so big that it's it's a fantastic reference. And realistically, I you know, I don't read through the whole thing every time I get it. Now, I just like I read the new chapters when I get the new chapters, but I know I have this In a referenceable thing in my in my tool bag, if you will, right where I can rip it out. And, you know, remember back in the day when we had the exchange administrators pocket to get to guide it's something like that.

M Michael Van Horenbeeck 27:12

Yeah, well at the same time though I'm really keen on making sure we don't bloat the book because it's so easy to go over, you know a certain amount of pages. Right now we're not it's five 600 pages, which is sizable by itself. But once you go over that, like it becomes that huge chunk and people start not reading certain chapters or they start being selective which is which is fine, right, but I really want to keep it you know, concise so that it is digestible. You know, obviously some things just take like the unwritten so many pages, we have them Defender ATP, it's just because we need that much, right. We honestly we couldn't have done it with less maybe we could have done 90 pages and you know, cut some redundancy here and there but at the end of the day, you need what you need. My goal is to keep it sizable, but you will see, you know, talk to me in a year and maybe I'll be six 700 pages.

C Chris Goosen 28:09

Yeah, no. I mean, look, I fair enough. And I think the thing is, given your experience in the industry, and given your experience learning things, I think you have a fairly good idea of what it takes to be able to get that message out there in a way that is going to be useful to someone without it being too bloated or to kind of, you know, too wordy, but also, you know, where it's sometimes where it's just not enough, right? Unfortunately, the internet is

full of blog posts that tackle a particular topic, but really just scratch not even scratch the surface. Basically, they just kind of give you a little bit of interest. You know, and you need to like to everyone who has blogs credit, that's great. But but sometimes sometimes you need to dig one level deeper. Right? And I think the what's great about that your history with with the other book, also you Your history as a, you know, blog author and speaker and stuff is I think that you have that balance, you know how to find that balance. And so yeah, really looking forward to what you and the team have kind of come up with here. I can't wait to get get my hands on a copy,

M Michael Van Horenbeeck 29:12

you'll get a copy from me, but only as you get feedback, because this is, you know, one of the messages that we're going to push really hard. Um, that to me, that book is a collaborative effort, right? Yes, the author team has written something, but we can only improve, make it better and make it you know, more suitable if people use the feedback, right? If they email us and tell us we like it, or Hey, you know, we're missing this piece, so that we know maybe we haven't thought about it. Or maybe we didn't prioritize it in the same way that people are asking for. Call it a user voice. If 100 people email us and tell us we really need this piece of information. And we as authors, we didn't prioritize it as high, we might just shift it up in priority and just add it into the book because there was too long for it, right? So I'm really keen to see how that's gonna work. I know that too. He's getting tons of feedback through his feedback channels on the book, you know, even to correct things as wrong because you never want to make mistakes. Because I'm like our tech tech reviewer, he's done an amazing job. But you know, he's going haywire through all the chapters, all the events that we're firing at him all the things that he needs to test. I mean, we're doing our best to make sure that it's you know, without any spelling errors, grammar spelling, even me as a copy editor. I'm not even native English speaker. So, you know, things will slip but we'll, we're counting on that.

C Chris Goosen 30:33

And I was actually just going to touch on that point, right is I'm always amazed by the fact that and I've read some of your works before where I've, you know, we've done I've done you know, we've done work for the same vendor writing vendor or whatever, and we've kind of reviewed each other's stuff and I I'm always amazed that as someone who's not even an English first language speaker, the level at which you managed to crank out this this awesome work, right so you know, Kudos to that. And I think this is something that everyone needs to also understand is that the team and correct me if I'm wrong, and I actually like you to introduce the team that you know, that you're working with, because I actually don't know everyone personally, like, I know you. But you guys are all based in

Europe, right?

M Michael Van Horenbeeck 31:15

No, no, not really. So we've got a mic on it, or both also, in VPS, do a lot of work in the security space. They're based out of the United United Arab Emirates. There are actually I think I'm our move to Dubai right now. So they're based out of there. I've got a couple of folks in the Netherlands. I've got as you can see, lovely works for me, as well. And, you know, it just so happened that when I started reaching out to folks that they were the first to respond and said, Yeah, sure. We want to do that. But yeah, it's been it's been helpful because, you know, less timezone issues. It's only a couple of hours apart. But we'll we'll see. I mean, reaching out to the For the Office ATP chapter, I think we might actually cross jump over to to the US to onboard someone else. But as far as the team goes, so we've got alarm on a tour doing the NBA TV chapter, we've got Peter who's doing Intune and identity. We've got Thomas was focusing on information protection, which, you know, coincidentally you could say it is more compliance feature rather than security feature, but as you said, to kind of blogs to it. Next to building the book in the the copy editing, I'm doing em Kaz during the introduction, and also doing some work here and there and the other chapters, and then task is doing the all all up review.

C Chris Goosen 32:40

Okay. And I think what's great about having, like an international team like that is everyone has their potentially slightly different market. So there's going to be slightly different point of view and slightly different experience coming into it and blending it all together. I think that's really powerful too.

M Michael Van Horenbeeck 32:55

It's incredibly useful, like in the talks that we've had, that is questions that we've had. I've learned so much like, insights from from Amar in certain things and how to approach it even you marketing the book, but also structuring the book. We've had another meeting last week, where we were just talking, like brainstorming, all of a sudden everyone was like, Yeah, wow, that's a great idea, just by having that interaction. And that's, you know, it's a learning process for each and every one of us. And, you know, it's fun. So, yeah,

C Chris Goosen 33:25

well, that's super exciting. Honestly, I think I can't I can't wait. Like I said, and it's really the timing on this is absolutely perfect. Like you couldn't have picked a better you know, a

better time for it. So I think with that, I mean, just kind of keeping keeping an eye on the on the clock here. I know. We've all got other things to get to. Nick. I just wanted to just to check in that. You're still breathing, buddy. I I'm sorry. I've taken over.

N Nicolas Blank 33:53
If the questions weren't so good. I throw in some more but you're doing great.

C Chris Goosen 33:58
Michael before we let you go As we always kind of do when we when we kind of, you know, tie off the end of the show. How do you want to be found can obviously be great if you want to develop the URL for the book again, how do people find you on social media if you want to be found, but I know you have a fairly fairly active social profile so go ahead,

M Michael Van Horenbeeck 34:19
not as active as I used to be just because I'm writing the book. So but you know, on Twitter I am and then hybrid, I think that's the easiest way to get a hold of me because my last name, you don't even try to pronounce it in English. So advanta hybrid. From there, you've got the URL, you'll have the book title, you'll see my blog post. Obviously, I'm on LinkedIn as well but has my full back name and Vanderbeek. But through Twitter, you'll easily find me I've got my own blog at the vet hybrid calm so you can get to there or the book of website m365securitybook.com as well, but I'll share it with you so that you can post it with the recording as well.

C Chris Goosen 34:58
Yeah, thank you. I think we'll We'll definitely make sure to put all of these in the in the show notes for the for the episode as well so that we can kind of get that out there. But thanks again for for taking the time to speak to us. This is super exciting sort of announcement, I guess. And we're really pleased that you came on to talk to us about that. And I know it's afternoon time for you in Europe, but I'm sure you still got a few things to get on with for the day. So

M Michael Van Horenbeeck 35:20
unfortunately, yes. Like, you know, you've got a whole day and so I'm halfway my well actually done with my day, two more hours a year I can sign off. But yeah, anyway, guys, I

really appreciate you having me on the call inviting me and talk about the book. Really appreciate that as well.

C Chris Goosen 35:34
Hey, no problem. Thank you. We're always happy to have you. So thanks for coming back.

M Michael Van Horenbeeck 35:38
My pleasure. Cheers.

C Chris Goosen 35:40
Go. Okay, guys. Bye!,

W Warren du Toit 35:44
everyone. Before you go, we just wanted to say thank you for listening. We really enjoyed 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 @thecloudarch.