Micro Focus Reimagining Episode #35 Cyber Chris Abramson

Fri, 5/13 5:42PM • 22:00

SUMMARY KEYWORDS

security, cloud, code, environment, securing, application, encrypt, organization, cyber, teams, walgreens, chris, data, model, reimagining, approach, workloads, companies, secrets, working

SPEAKERS

Rob Aragao, Stan Wisseman, Chris Abramson

Read | Listen

Chris Abramson 00:00
Oh, you know, from a data protection standpoint, the core thing is if you can encrypt the data, encrypt it. At the end of the day, just encrypt the data.

Rob Aragao 00:17
Welcome to the Reimagining Cyber podcast where we share short to the point perspectives on the cyber landscape. It's all about engaging yet casual conversations and what organizations are doing to reimagine their cyber programs, while ensuring their business objectives are top priority. With my co-host, Stan Wisseman, Head of Security Strategist, I'm Rob Aragao Chief Security Strategist. And this is Reimagining Cyber. So Stan, who do we have joining us for this episode?

Stan Wisseman 00:45
Rob, Chris Abramson is the Senior Director of Cloud Security Engineering at Walgreens. Chris' career spans over 20 years while working inside companies from the Fortune 500 to as small as 10 employees. And, Chris, it's great to have you with us today to help us better understand how to take secure cloud computing to large environments. You've been working with Azure defender, for cloud security, as well as helping secure applications as they're doing dev test and rolling out in production. So it's a hands on kind of experience for our listeners that are trying to deal with these issues. Can you expand a little bit on your background for our listeners?

Chris Abramson 01:25
Sure. So interestingly enough, my background actually didn't start in cloud. I'm an app developer by trade. That's where I started. And coming into security was kind of a call it a mishap. I hadn't actually anticipated going into InfoSec, I was on the programming route. And then all of a sudden, you know, things happened in 2008. Rob, you know that period of time, or not 2008. A little sooner than that. That just led me into the security path. And that's where I ended up. And now over the span of the last 20

years, my roles have changed. Governance, technology, governance, back to technology. And today, now it's in the cloud space.

Stan Wisseman 02:12
Gotcha. Well, Chris, in 2019, I believe it was Walgreens inked a deal with Microsoft, with plans to move most of its workloads to Microsoft's Azure public cloud. And I'm sure that is keeping you very busy as the one that's sort of like on-point for securing cloud workloads. So, the consumption of cloud services at that kind of scale, must be pretty daunting in the sense of having to rethink how IT operates in the broadest sense, and how security fits into these new processes? So, how have you navigated this transition?

Chris Abramson 02:55
Well, a good chunk of it has been kind of a Microsoft first approach. We've had to rethink strategy, you know, on-prem has always been about firewalls and IDSs and IPSs and technology that you wrap around an environment, maybe not so much in the environment, even though more companies have trended towards like EDR solutions on their servers and being able to monitor what's happening. But in the cloud, you're working in, what equates to a highly coded environment? And so, the nature of how things communicate with each other and talk to each other. That's been the biggest change for us is, how do we adapt to that type of world? And how do we adapt to securing that type of world?

Rob Aragao 03:44
Well, Chris, one of the things is also focusing on how you are actually shifting these application workloads to the cloud, and as organizations have taken different approaches, right, you have the kind of lift and shift approach versus the, we're gonna go cloud native. And you're going to take advantage of different services from the CSP, in your case with Azure, of course, right. But there's multitudes of different deployment models and is probably some different kind of aspects of that and playing with what you're doing within Walgreens. How have you gone about establishing some of the guardrails to ensure that security really, truly is not being left behind?

Chris Abramson 04:18
Sure. So, a lot of our teams work a lot with ARM a little bit with TerraForm, as well, too. And so what we've done is we've partnered with our cloud COE organization, and we've designed security into that deployment model. So where, we're deploying, I'm trying to think of a good example, but I'll just say we're deploying a VM to an environment. We've built into that CI pipeline, the security model that we want wrapped around that. So as our teams, whether it be an infrastructure team, or even an application team, go to do that deployment. They're hitting the gates of security, not at the end, not after everything's deployed. And then we have to go back and try to figure out okay how are we going to wrap security around this. But they're hitting it as they go. So, they can make the changes, address the configurational issues, and then deploy in a way that is appropriate in our environment that poses the least risk to the environment as well.

Stan Wisseman 05:24
So for our listeners, ARM is basically the infrastructure as code kind of approach right? For Azure.

Chris Abramson 05:32
Yeah, the Azure Resource Manager platform.

Stan Wisseman 05:36
And can management capability level to be able to actually do those kinds of deployments. And so you're using that as part of your gates. But are you also reviewing the ARM templates that development is using?

Chris Abramson 05:54
We actually go through a process with the teams where we develop the ARM templates alongside them. So instead of a team going off and say we're gonna go build an ARM template to deploy Azure Databricks. Okay, and they go deploy it, and then they gotta like, put it through a process with security. No, we work with them, alongside them to make sure that as it's built as the as the code is being generated, as the checks are being done, all of that is put in there. So, we don't have to do this back and forth with our with our teams. It's inefficient, it takes a lot of time, it takes a lot of effort. So, it's a partnership between the two organizations. And by doing so, we've created this pod model where teams will get together, they'll focus on a past service, and they'll start to build out that that IAC design that infrastructure as a code design, with the security checks available to them.

Stan Wisseman 06:50
And as far as how rigorous do you apply those checks? Is it by risk as far as the risk level? Or how do you? Or is there a differentiator?

Chris Abramson 07:01
How do we make a decision on what checks we're putting in there? You know, we've established our own model of guardrails, things that we know, by experience or by way of industry knowledge. These are the gotchas, these are the things that are going to hit you in a security model. I'm not going to name them off, I don't want to give away the secret sauce to anybody. But we have taken a risk-based approach to things that we've seen in articles that come through CVE data on vulnerabilities in the cloud things that have been experienced by other companies made public, you know, whether through articles or industry groups, etc. And so, we're taking that experience, and we're baking that into our design. So, is it risk-based? Yes, it's more fundamentally though, what's going to prevent bad behavior, things that we don't want to have happen in the environment.

Rob Aragao 08:04
You know, one of the things that we've seen, let's say not taken as seriously previously, were the access controls relative to code repositories, right, kind of loose in the past. But obviously, there's been a lot of changes in specific exploits, at the code repos, that needs to kind of change the way things are approached and actually be more rigid; and access control be more rigid understanding, you know, who has rights back in but access back to pull data back out to pull the details that we're seeing? And one of the obviously the ones that we're all very aware of, as a main kind of light the fire on this was around what happened with SolarWinds, right? It's a prime example of it. So, if you look at what kind of happened back then about now almost a year and a half ago, you know, how has that kind of changed?

And what are some of the thought processes that you have taken in recommending different approaches for how you're really taking in locking down those code repos?

Chris Abramson 09:00
Yeah, this is a tough one, because development teams always want the ability to grab libraries, grab things that that are going to help them move quicker, get things done, deploy code. This is one that, it's still kind of an evolving space, I think, just for anybody, it's still an evolving space. You know, this, and especially in a large company, where you have a lot of development teams that are working. This is one that fundamentally, really takes a lot of interaction between development teams and the security teams make sure that they're thinking about what the impact is going to be if they pull from some rogue repository or just, you know, off the internet and things like that. A lot of education, a lot of back and forth. But there's also tools that that we've implemented, that let us look at particular libraries, you know, things that we feel are going to have major impact in our larger applications and such. So, we do take a hands on approach with them. But I think this is always going to be an evolving space because of the nature of just how software development moves quickly, and things want to get done fast.

Stan Wisseman 10:15
So just a follow up question on that, certainly we're seeing a lot around that whole area around securing the software supply chain, and getting things, you know, one to one areas of trying to lock things down around the code repo, like we're just talking about, but there are other injection points, right, that bad actors can take advantage of. But also, it could be an unintentional kind of insider threats for developers and unintentionally adding risk. You know, are you looking at that or nicely necessarily, you but is your organization looking at, you know, software supply chain risk management as, as an area of focus?

Chris Abramson 11:02
We are, it's, I think, going back to a kind of go back to the days of PCI, where third party risk management kind, I think, started the ball rolling on this for a lot of companies. It's, there's that word, again, it's evolved, it's kind of moved on from just the person that you got to worry about to now you got to worry about the person's person's person in that model, you got to think about software that you're buying from a third party, that now also embedded software from another third party, that likely embeds software from another third party. That's the Russian doll syndrome. It is the Russian doll of software, it's the concept of how do you know that you're comfortable with what's going on what you're bringing in, whether it's, you know, a console application or some SAS platform that you're going to integrate through an API gateway of some kind that you're comfortable with letting those connections happen. And that's really what it comes down to, is where you're connecting, how you're integrating with these with these different platforms. And such, because you likely might buy something that you don't ever plan on integrating into your systems, you are going to use it for something low risk, you may not care, versus you're going to integrate it wholeheartedly into your environment, now becomes a higher risk scenario. I think it still starts with a strong vendor Security Management Program, talking with your partners, understanding their security practices, what they're doing, and how they're managing their code, their releases, their ingest of those same platforms, or same libraries or same third-party integrations as well, too.

Stan Wisseman 12:48
And that's why asset management and some kind of bill of materials associated with consists of that application is very important, right?

Chris Abramson
Yep.

Rob Aragao 12:57
So, Chris the CI pipeline needs secrets to operate because it needs to communicate with other systems to deploy stuff and access multiple things. These secrets don't belong in the code and all the systems to provide smarter ways of dealing with those secrets, but you need to ensure that these methods of securing secrets are being used. So otherwise, if you hard code your secrets, these tools won't stop you from doing so. What methods have you taken? And then what do you recommend using to tech proper sharing of secrets and code and infrastructure as code templates?

Chris Abramson 13:28
So, I think there's a two-pronged approach here on this one, Rob. Number one, is a strong threat modeling design around application environments, and how they're ingesting that material that comes with an upfront architecture review, and/or utilizing tools that allow you to map your environments out to know where you're connecting, why you're connecting, in what fashion you're connecting, are you encrypting? Are you encrypting the traffic things of that nature? And then the second part of that is recursively coming back over time, the secret stash so whether it's a key vault, you're using something from Hashey Corp, you know, to integrate your whatever it is that you're modeling behind. Obviously, the main thing you don't want to do is you never want to put a hard coded password or a hard coded key in your code like that. That's just downright insane in this day and age, because you have no idea who's going to touch that code who's going to see it, which third party is going to have access to it. You want to make sure that you have a strong chain of custody around the password, the certificate, the key, whatever it is that you're trying to secure for whatever purpose, so it does come down to that threat modeling piece. But then also coming back over time and recursively asking: Are you updating? Are you reviewing who has access to those things? Are you looking at what it's being used for still, did you renew it? Does it expire? There's a little bit of what we all kind of refer to I think in the industry of cyber hygiene, you got to come back and look at those parts and pieces over time and decide: Did I do it right today? Did I implement it properly? And is it getting updated? Is it getting replaced? Is it getting renewed? Is it being changed?

Stan Wisseman 15:22
And getting that visibility, that they're actually zero? And sometimes you have to scan that code to find that perhaps they haven't done now.

Chris Abramson 15:29
Yeah, there's some really great products that I see coming out on the market, that help with that threat profiling, even on a recursive basis, where they can identify things like what we're talking about here, like secrets, exposure, or misconfigured systems, lack of TLS, you know, I think teams really need to start thinking about that, especially as their environment start to grow, or they start to expand out

beyond the reach of just a general like, paper review, or something of that nature. So I think there's some really good stuff coming out in that space.

Stan Wisseman 16:12
One of the challenges we always run across is how to protect your sensitive data. Right, and especially when you're dealing with cloud data warehouses, and those kinds of analytic platforms that are large repositories of data, juicy targets, right. You know, I think that the processes that you're probably putting in place to help gain visibility into that data is moving into the cloud and working with your business units to help ensure that they're protecting that data, and how it's being accessed. What kind of approaches are you taking to help ensure that everybody's in line and then sync and have that visibility?

Chris Abramson 16:51
So I think from a data protection standpoint, Stan, the core thing is, if you can encrypt the data encrypt it. I mean at the end of the day, just encrypt the data now. For a lot of companies, and we're included in there, there's times where encryption just, it doesn't work. Whether it's, you're trying to do analytics, you're trying to do stuff that encryption doesn't give you that ability to do. So there's other ways that I think companies need to think about this and other ways that we've thought about it. Wrapping environments, in a model that doesn't allow access to, or very limited access to, it's kind of, I'll call it the vaulted environment, you know, the no ability to touch, change, maneuver through or ingress or egress without somebody watching you do it, that stuff, it's expensive, and it's highly operational, because there's a lot of eyeballs having to do that. Hence why I say if you can encrypt, encrypt it because honestly, fg h is the quickest, easiest way to protect your data. And if somebody can't walk off with the keys, then you're in good shape, and they can't walk off with the data, because it's encrypted. So you know, and in that space, I recommend a bring your own key model, especially when you're in the cloud, because if especially if you're in a hybrid world, your workloads shift, move, go from one environment to another one region to another. And, all the cloud providers, I think, have solid physical security controls, and even logical security controls. But there's always that one off chance. And I recommend, don't take that chance. Don't do it. So if you can bring your own key and encrypt the environment. So that's really your safest bet. But I think in a lot of ways, as companies start to realize that they need data to do business processes, or analytics or marketing or whatever the model is that you got to do, there's going to be times where that just doesn't work. And you got to be prepared for how you're going to approach that. As a security organization, how are you going to partner with the with the business side of the house and IT side of the house and how you're going to help them expose themselves as little as possible to the to the to the rest of the world and how they protect that information.

Rob Aragao 19:36
Well, Chris, thanks for coming on and sharing with us some of the different things you're doing. We really appreciate, I think, you've only been doing this for three years, the aspect of the cloud journey within Walgreens, and just in that time, the progression that you've made, we know a little bit more behind the scenes than what you're hearing. It's pretty impressive.

Chris Abramson 19:59

It's pretty staggering. I gotta give a lot of credit to our cloud organization, as well as you know, our internal security organization. And, actually, the application teams as well, too. It is definitely a team effort when it comes to doing cloud. Because it is highly, highly, highly complex, there's a high number of touch points. And it can go bad very quickly. If you're not careful. If you're not careful, it can go bad very quickly.

Rob Aragao 20:34
Volumes to what you're sharing as far as all the different components to it. But the teamwork that you guys have been able to really pull together and actually get on the same page to make it happen, right, the examples you shared around how you really do have kind of security gates along the way versus let's wait and see at the end what the actual security issues are. And then everybody has to go back. And now we've killed all this time, right. And now people aren't happy about that at the traditional battles that we've had in the past. So great shifting in there. And then my favorite is the new t-shirt that we're making for you, which is 'just encrypt it'. We'll have to maybe talk to Nike about it, but we'll get there.

Chris Abramson 21:15
It sounds good. Rob. I'll be waiting with bated breath for that shirt.

Rob Aragao 21:18
Yes, yes, indeed. We'll have it delivered. So, thanks again for coming on. We truly appreciate your sharing your experiences there.

Chris Abramson 21:24
Absolutely. I appreciate it. Thanks, guys.

Stan Wisseman 21:26
Hey, thanks, Chris.

Rob Aragao 21:28
Thanks for listening to the Reimagining Cyber podcast. We hope you enjoy this episode. If you would like to have us cover a specific topic of interest, feel free to reach out to us and you can find out how in the show notes. And don't forget to subscribe. This podcast was brought to you by CyberRes, a Micro Focus line of business, where our mission is to deliver cyber resilience by engaging people process and technology to protect, detect, and evolve