Constellations Podcast

Episode 68 – The Cloud, Security and Zero Trust

Guest: Mark McIntyre, Chief Security Advisor, Cybersecurity Solutions, Microsoft– 22 minutes

John Gilroy: Welcome to constellations, the podcast from Kratos. My name is John Gilroy and I'll be your moderator. Our guest today is Mark McIntyre, Chief Security Advisor, Cybersecurity Solutions at Microsoft.

John Gilroy: More and more enterprises are migrating to the cloud and taking their data and applications with them. There are a number of cloud computing setups from public, and private, and multi, and hybrid, and all kinds of combinations of that. The amount of variations leaves a huge amount of complexity for IT departments to monitor cloud services while keeping them secure. Mark, you've got your work cut out for you, don't you?

Mark McIntyre: It's not boring.

John Gilroy: Okay, Mark, I'm going to throw out a fun fact here and you can agree or disagree or throw a chair at me. What do you want to do? Here's the fact. Our recent statistics suggests that insider attacks account for 43% of all data breaches. Do you agree or disagree, or how can even handle something like that?

Mark McIntyre: That could well be true. It's also important to note that the vast majority, let's say 95% or so of incidents out there come from people like us. And so I think what's most important there tying those numbers together is that the vast majority of what we consider to be insider threat really constitutes your employees, or for that matter you and I, trying to do the right thing. We're not consciously trying to hurt our organizations. We're trying to work. Of course, there is malicious insider threat, people motivated by anger toward a company or what have you, but the vast majority of this is really people trying to just still trying to work. And so we have a real chance to help educate our users and create much more secure experiences for them to do their jobs.

John Gilroy: So the phrase in the cybersphere community is just digital hygiene. Is that the word that's used?

Mark McIntyre: Yes.

John Gilroy: Password maintenance, password changes, and understanding what you're allowed and not allowed to handle.

Mark McIntyre: There's no question that if we can help organizations get some of the basics right, the blocking and tackling, the hygiene, we can really make an impact. Certain things, improving patch management, requiring multifactor authentication, and for that matter, do that on your personal devices. Limiting privilege, that's a great place to start. I could go on for five minutes alone about that topic.

Mark McIntyre: There are a variety of recommended best practices out there. You can look at various websites within the U.S., there's a great one from the Australian Defense Department, but generally speaking there are we'll say top five, top 10 steps you can take right now to measurably improve the security of your environment without breaking your budget.

John Gilroy: If you look at companies and you've been all over the world, if you look at companies some will say that to remain safe they have to keep everything closed up, keep it on-premises, keep it behind locked doors here to run their own cloud. Will that keep them more secure?

Mark McIntyre: It might be more, it might provide a sense of assurance and relief but it won't necessarily make you any more secure. For that matter, it fails. Take into consideration the simple fact that the world is changing, that the way that we all interact with IT, the experiences that our employees demand, the richer experiences that customers want require you to innovate and to undergo, which you hear about digital transformation. So yeah, you could try to stay behind your wall, your moat pretty isolated, but we don't think it makes you any more secure. It certainly does not help you address the core issue, which is that yes, security is critical, but security is part of your larger business planning.

John Gilroy: In World War I, they tried to stay behind the walls.

Mark McIntyre: That's right.

John Gilroy: And they brought in new guns that just blew up the walls.

Mark McIntyre: That's right.

John Gilroy: I mean you can try to stick behind your walls, but all kinds of problems with that.

Mark McIntyre: That's right.

John Gilroy: When you look at the cloud from 20,000 feet or 30,000 feet, does cloud mean better security or more vulnerability? Man your stuff is off your premises, isn't it?

Mark McIntyre: Well, I mean obviously I work for Microsoft, I have my own opinions, but my company is investing heavily to the tune of over a billion dollars a year.

John Gilroy: People don't realize that. $1 billion a year. That's a big number.

Mark McIntyre: Yeah, I'll take my 1% of that.

John Gilroy: Any day of the week.

Mark McIntyre: I mean we are a security company and people have not traditionally thought of us in that vein, fair or not, right or wrong, but we're investing heavily now. I think we're starting to see more and more validation of that strategy. Independent analysts putting our products out there saying that we actually are very competitive now, we're industry leading. That's great. But of course, our larger job is to help our customers directly and through our partners transform and help them serve the public taxpayer citizens, help serve their customers better, create new experiences. Security should be part of that conversation. It really should not be considered a separate initiative.

John Gilroy: Satellite communications traditionally has been very, very conservative and resistant to change and doing things very effectively that way and making a transition to the cloud because people can see the flexibility and the scalability that they have there. So what kinds of risks come along with that kind of a cloud adoption?

Mark McIntyre: Well, going to the cloud we think does make you more secure. You can transfer risk in a sense over to a cloud provider. You get more benefits, you get more data, you get more solutions in a marketplace that can help protect you. I think doing nothing really is not a solution. You will not innovate that way. From a security point of view, you will certainly not be able if you stay on-premises, if you just do nothing and think the attackers will go elsewhere, you'll suffer.

Mark McIntyre: And so CloudFirst technologies we think can definitely make you more secure. They do not of course absolve you of responsibility. And so I think really the key here is understanding roles, responsibilities as you go more into the cloud. If you go into infrastructure as a service, platform as a service, software as a service, we as your provider, perhaps integrator or partner working with you, we take on more of that security management for you. Ultimately, of course it is still your job to run your security so we can help you, we can be a partner to you, but you still do have certain accountabilities.

John Gilroy: Mark, people who listen to this podcasts are in Japan, they're in France, all over the place and different approaches in different parts of the world. There are a lot of people in the federal government that listen to this podcast. There's a

term in the federal government now that's kind of trending. It's called zero trust. For the people all over the world listening to this, so what is zero trust and is it a better approach?

Mark McIntyre: Well, zero trust literally means what it says, never trust, always verify. So we think it's a more modern, a more realistic approach to modern collaboration than traditional imaginal line, moat, traditional security, castle, castle walls is a good phrase. It reflects a modern workplace environment and frankly it allows your security teams to set more granular and proactive controls and policies. By the way, we implement zero trust within Microsoft. There's a really good case study on our own website that we can make available that shows how we have been doing this internally, and the process, and the journey that we're on.

John Gilroy: Eating your own dog food, is that what they say?

Mark McIntyre: That's right.

John Gilroy: That's good.

Mark McIntyre: I'm sure we have struggles like anybody else implementing it. We have people who are very headstrong, people who think they're right, people who think they know better, that perhaps they don't want to be managed. But fact is, we've been doing it around the company for a couple of years now and it could be a good reference model for your audience.

John Gilroy: While we're on the topic of the federal government and zero trust, there is a phrase that's getting very, very popular in the Federal Information Technology community. It's called CMMC, or Cybersecurity Maturity Model Certification. So how does Microsoft help people in the DoD achieve this CMMC certification?

Mark McIntyre: Sure. Well, DoD just released the first version of this I think maybe on Monday, Tuesday. This requires DIB members essentially to demonstrate that they've achieved working at a certain level of maturity. I think it's a one to five model. By the way, there are other maturity models out there in cyber. But generally speaking, the idea is that you want to go up from one to five. You want to demonstrate steady progress, more proactive thinking, strategy, more automation, more use of cloud tools frankly so that you can get to an optimized state insecurity.

Mark McIntyre: In our case, for example, I'll throw out one example. Our Azure Sentinel offering, which is a cloud-based pays you go SIEM, which I suspect not many people might know that we have. But Azure Sentinel is our SIEM in the marketplace now. Using something like Sentinel you can demonstrate right there that if you are a DIB member that this essentially correlates to a CMMC Level 4 and gets

you into Level 5 because it automates response, it throws in threat intelligence, it has learning, things like that. So we're definitely committed in our current investments, in our roadmap to making sure that we help the DoD ecosystem be more secure as it prosecutes its mission.

John Gilroy: Now, we have a lot of people from all over the world. Australia, for example, listening to podcasts and you kind of toss out inside baseball terms that they may try to learn, or they're walking their dog listening to podcasts and trying to figure out what is, so DIB and SIEM? If you could define those, please?

Mark McIntyre: That's right. I apologize. Defense Industrial Base, essentially it's a supply chain ecosystem, let's say. By the way, the attackers are very much aware of that they can go after supply chain partners to get into their ultimate target. It happens worldwide and it's logical. If I were an attacker and if I were trying to go after a DoD system, or a bank, or an insurance company, or a retail provider and I could not get into their systems, I will find the weaker link and I'll get into their systems. So DIB reflects the defense ecosystem and SIEM is really, it's Security Incident Event Management. Essentially think of it as a large system that handles your security data. It helps you meet practical security goals and it also helps you meet compliance and reporting goals.

John Gilroy: That's S as in Sam, I-E-M, correct?

Mark McIntyre: Yeah.

John Gilroy: Mark, I mentioned it earlier; thousands of people from all over the world have listened to this podcast. If you are listening, go to Google, type in Constellations Podcast and arrive at our show notes page. You can get transcripts from each one of our previous 67 episodes. It's like a whole book on space. It's great. Also, if you want you can sign up and we can send you notifications via email of other great guests like Mark and people coming up this year. I think this whole idea of CMMC is kind of popping the radar for us as well. Mark, are there certain sets of piles, season standards that should be used for development in the cloud architecture that will help minimize these risks?

Mark McIntyre: First of all, software development continues to evolve. Microsoft for years has been using internally and promulgating, let's say, externally the security development lifecycle, microsoft.com/sdl, this is a language platform agnostic methodology for writing more secure applications. It is applicable as well to cloud. So we think that that's a really good place to start. Just look at as you write your apps or as you think about how you are going to write apps, follow a practice, follow a methodology because right there if nothing else it reflects an ISO standard, ISO 27034, so right there you have an international framework to guide you on how to write more secure code. So we do that definitely internally.

It takes management direction to do it, but we do. It works very well for us. Things like that are really important.

Mark McIntyre: But now, especially as we introduce more and more platform as a service type capabilities, containerization, and microservices, things like that, the industry is also a really, really helping software developers innovate at a much faster pace than ever before.

John Gilroy: Let's take this cloud question, bring it down in the ground, and talk about practical applications here. So when, let's say, one of our listeners here is working in the cloud environment, whose responsibility is it to manage and secure security? Is that the cloud provider or the company utilizing cloud services?

Mark McIntyre: Well, the answer that we hear a lot is: It depends. We think that we're confident that the cloud offers you more security. It frees you up, it helps you transfer risk to a cloud provider to help you focus on your core business. The more you go up into the cloud, let's say, from on-premises into infrastructure service or platform as a service or up into SaaS, we can take on more of that management for you, manage your identity for you, manage your endpoints, your mailboxes, your infrastructure. But you have to get it right and you have to understand who actually owns what.

Mark McIntyre: There's a really good resource out there if you want to really, really grasp it. Picture it being a thousand words, just go online, use Bing, and look up a pizza as a service. Yes, it makes me hungry.

John Gilroy: Pizza as a service. I like it.

Mark McIntyre: In fact, I'm getting hungry right now thinking about it. But it really works. It helps you grasp or visualize what's possible in terms of the cloud, what someone will do for you as a provider but also what you are responsible for ultimately.

John Gilroy: Now we're talking about the cloud and security, I'd be remiss if I didn't talk about the Cloud Security Alliance.

Mark McIntyre: Sure.

John Gilroy: They say that the top threat to cloud computing is misconfiguration, which occurs when computing assets are setup incorrectly. We know that. This can leave them vulnerable to malicious activity. So how do you prevent someone from misconfiguring something?

Mark McIntyre: Well, thank you for asking that. This was not a setup question. I've been blogging on this recently with some colleagues, and so I can make sure that those URLs are available. This is a huge area of concern to our executives. We're seeing steady growth in cloud business. Clearly, if you look at our reporting quarterly we're seeing more and more growth in our Azure Office 365 cloud businesses. But what we're not seeing, and this is broadly around the industry, we're not seeing a commensurate adoption or consumption of built-in security services.

Mark McIntyre: In our case, we really want to help close that gap. For example, within Microsoft our cloud services also offer a variety of no cost security tools, tools that are there for you to use to help you make sure that you get those configuration settings, that you do them right. For example, if you're launching virtual machines, they're not encrypted. You should know that before it constitutes a problem. If they don't have a vulnerability scanning mechanism, if they don't have password controls or privileged access controls, you should know that. Ideally, we can go even further to the left and we can work with you. For example, a blueprint. We can help you launch a service, an app that has all those configuration settings set the way that you need it to be, whether it's for your internal culture, or best practices, or perhaps an industry standard, something like ISO or NIST or CIS or even GDPR, for example, a European privacy regulation. So we're definitely investing heavily in raising awareness about a lot of these built-in security configuration tools that we can help you go to the cloud as securely as possible.

John Gilroy: People listening to podcasts when they're walking their dog, I don't know, they're going on hikes and everything else, and they may have heard that little reference made earlier. So if people want to read this blog, it's M-C-I-N-T-Y-R-E, Mark and type in blog or misconfiguration. I imagine you can find that information whether its two years from now or next week. That makes a whole lot of sense to find more what Mark has to say.

John Gilroy: I raised three kids and I taught them how to drive and I'm a big believer in insurance. I mean I love car insurance. It is a big winner for me. And maybe this applies to the commercial as well. One way companies are managing risk with cloud-based security breach is to take out cyber-insurance for the commercial sector. Is this something that should be considered? Is it a thing?

Mark McIntyre: It's certainly a growing field. I work primarily with the government, which of course is self-insured, so we don't come across it as much at least from a practitioner perspective. But I can say this, we've worked some of the big insurance companies and reinsurers, and you'll see them offer their clients, enterprise clients discounts for example. I'm aware of one company that provides certain discounts on their cyber lines if their clients use Office 365 E5, which is just, it's a SKU. It's a licensed framework from Microsoft.

Mark McIntyre: So that's the carrot. That also probably means there are sticks or there are hammers somewhere. There was a really good article several months ago, I think it was in WIRED, but anyway, it was about they were profiling a Northern European company that had suffered a ransomware attack and they cleaned it up, they remediated, and then they submitted their bill, submitted their claim to their risk insurance company, one of their European providers. Their provider turned their client down. They wouldn't pay the claim because they produced evidence that said that showed that the client did not carry out recommendations. These were all hygiene recommendations, patch your stuff, do MFA.

John Gilroy: The basics, yeah.

Mark McIntyre: And so they turned them down there. There are other examples of this. What I would say from Microsoft's perspective is we don't do that. However, we do have really cool tools available right now. I'll give you one example. Secure Score. Secure Score is in your Windows 10, your client's environment. It's also in your Azure environment and Office 365. What Secure Score is, it's all incentive. It's a way to show you that based on how you configure your settings, when you launch your service, you have a score. And so we want to show you the number, what could be possible based on if you return every control to 11. We'll also put you in, group you by industry. So we'll say, "Okay. Well, your score might be 400." Maybe you're in the financial services industry. Your industry peers are at 475 so these are things you can consider doing.

Mark McIntyre: We want to incentivize you, give you more points for doing the more basic hygiene steps. So again, the idea is that we can help you do the right thing earlier in your process as you go to the cloud in ways that don't really have to cost much if any money at all. So we definitely are aware that there certainly is an increasing focus in the risk management industry on cyber. Secure Score is a good example of a tool that's out there that we can all use to help drive the right behavior.

John Gilroy: We've got a final question here. I want to harken back to the beginning. Public cloud, private cloud, hybrid cloud, there are a lot of companies out there who are listening who are using multiple cloud service providers in all kinds of different areas. And so how do they manage their security controls with this hybrid environment?

Mark McIntyre: Sure. Well, governments, U.S. government for sure. These are going to be hybrid environments generally. Now, there's definitely major investments in public cloud, but a lot of governments around the world and critical infrastructure are highly regulated industries will likely be in a hybrid model for years to come. That's totally understandable. You should go to the cloud at your own pace. But in our case, we want to make sure that our technologies support

that, those business decisions and multi-cloud environment is entirely reasonable from a risk management perspective. But we make sure that our technologies are interoperable, that they play nice, let's say, with third-party providers.

Mark McIntyre: Some of our tools out there right now, for example, I mentioned Azure Sentinel earlier. Azure Security Center is a good example, built-in tools you can use right now that help you monitor and manage not only your Microsoft systems but also your third-party systems. We have a lot of partner solutions in there as well. So we want to make sure to call out that we do work heavily and closely with security partners from A to Z. And so we think that the proper and the most responsible way to serve our customers globally is to give them tools that help them manage multiple environments.

John Gilroy: Mark, unfortunately, we are running out of time.

Mark McIntyre: Sure thing.

John Gilroy: I'd like to thank our guest, Mark McIntyre, Chief Security Advisor, Cybersecurity Solutions Group at Microsoft.

Mark McIntyre: Thank you.