FEDERAL TECH PODCAST

Ep. 70 How to Manage Machine Identities

00:00
This is John Gilroy from the Federal tech podcast and this is Kevin Bocek from benify. Today we're going to talk about managing machine identities hit the music Manny.

00:08
Welcome to the federal tech podcast where industry leaders share insights on innovation for the focus on reducing cost and improving security for federal technology. If you like the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:37
Well, welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is Kevin Bocek, Vice President security strategy and threat intelligence at a company called venna phi. And today we're gonna talk about non person entities. We're going to talk about non machine entities. We're going to talk about managing machine identities. My first question to you Kevin is, you know, why should we worry about something like this? And I know that's true company does your company has been around a while very successful, and I gotta toss out this Warren Buffett quote, okay. Warren Buffett once said, don't ask a barber if you need a haircut. So I get you on the podcast, I say, Hey, Kev, we worry about machine identities. And you're gonna say, Well, yeah, so why worry about? Here's

01:24
why, John. I mean, if you think about everything we're hearing today, it is all about machines, machine learning, AI cloud, what makes a business valuable, what makes government do its job for citizens better what is even important on the battlefield. We here today, which is all about machines, about AI, cloud. And you know, what, they're only more machines, there's all this cloud software, it's all the web services, all the AI the code the AI is creating, there's a lot more of that than us as humans, only more so to the future, actually, we should maybe consider ourselves the non machines.

02:13
Here we go. Turning to

02:15
so first, what's important, and what you know, really is, you know, differentiating both government services and business. It's all about machines, which, just like people, we got to know which ones are good or bad friend or foe, actually, you know, Aristotle 1000s, of years ago came up with this idea of the rule of identity, the law of identity, which if something exists, it must have an identity. So all of the cloud services, all of the AI machine learning that we're using today, and tomorrow, we got to know whether it's good or bad friend or foe. That's why machine identity management is important.

02:59
Okay, next quick question number two, so it's going to have value for our listeners, because everyone's talking about artificial intelligence and machine oiled machines, right in the whole phrase there, isn't it? And we live in a world where humans have to be identified, and apparently, system processes, non personalities have to be identified. So what role does your company play? So why should my guppies care about what venna phi does?

03:23
Well, you know what you can observe this each and every day, when you log on to your bank website. And when you log on for a government service, you noticed that there's a padlock in your browser? That padlock means that your machine, which is the browser and mobile devices, talk to another machine or web server on the other end, and say, yep, you know, what, I think this is who it says is on the other, I've authenticated it. So we feel this each and every day, already. Now, of course, there are hundreds or 1000s of machines all working in the background, whether I access a government website, whether I log in to order something online. So wow, software and machines are only more and more important. And you know, we've probably experienced problems with this all in our life, you know, we've gone to log on to some website, and it says, yep, can't trust that site. That might because be because it's machine identities misconfigured it might be expired. And that problem is only getting more complex. You might have tried to download an app. And it says, yep, can install that it doesn't come sign which machine doesn't have a machine identity. So it's something we all feel already. And as we live in a world that's more and more digital, you get on an airplane. It's just a big mobile device. Apps are installed. How do you know which ones are good or bad friend or foe? We hear about the federal guard comment about zero trust. What does zero trust mean? It means always authenticated. So it always has to have identity all those machines. So that's what benify does, we help manage the lifecycle of all the identities of this machines, especially the software that makes business and government run, we make sure that all those machines can be authenticated, that they can be authorized. And then finally, of course, really important, it's governed. And a world where developers and engineers are making the future, we have to make sure that there's the governance, they need to focus on new features, speed, especially the security teams make need to make sure they're doing it safely. And I live in

05:47
rural Virginia near the Blue Ridge, and I have this silly house. I got three refrigerators, I've got a pond, and I have a backup generator. And so whenever there's a power outage, hey, I'm in business, you know, everything's working. And let's take that and apply that to the security world. Okay. So you're humming along, everything's fine. All of a sudden you get it. And I guess there's outages with machine identity, sir.

06:10
So first of all, giant all the Virginians out there, I love the Rapidan in the Shenandoah. So, second, yeah, it's a great example, which is, you know, what happens when there's a failure machine identities, it's pretty much like the electricity going off. Because that means just like, your web browser can't talk to another web server. They can't work together. All the software that talks between a cloud a data center, the way that now your car, gets a software update from the cloud, not machine identity isn't working, right. I can't trust that cloud. I can't authenticate, it won't allow it. So this is something that, you know, everyone here is benefiting from. And we

also all just like we have power outages, which we don't have too many of those these days. We do have many more actually machine identities, because it's a lot more complicated. In the machine world, like our brains wrapping our minds around that. It's really difficult. Yeah, everyone's probably experienced it, like LinkedIn has gone down. Spotify has gone down, as yours gone down. I even saw I think Starlink satellites went down. And why just because this one little thing, some to these machine identities are called certificates, just expired. Just imagine, which of course, we could talk more in the hands of an adversary what they could do.

07:42

I'm sure if there are people listening to this, who have sophisticated knowledge of cybersecurity, can contact you and do a three hour dive in PKI. And encryption. I'm sure we're not gonna do that today. I mean, I'm sure you can handle it. I know your technical background. Let's bring it up to the human level here. And here's a human level. Someone who says constant gets a phishing email hits it, and they get hit with ransomware. It has it's happening all the time. We're gonna Google Trends. Ransomware is crazy. There's ransomware as a service now. So let's look at our machines. Can Can these machines be attacked? Can they be could they be compromised?

08:16

Yeah, one of the things that the FBI alerted, especially us as cybersecurity professionals, what they were seeing was that cyber criminals were setting up fake websites to distribute malware ransomware. And it wasn't just that they were fake sites, actually, in, for example, in your browser, they were looking like real ones. The names but also though they had trusted machine identities, which meant your browser said, Hey, this is a good site, you could even enter your username and password. You might know that most web browsers today won't let you do that or enter a credit card unless there's a machine identity. So what do the fraudsters the cyber criminals? Do? We need machine identities. We also see it today. Then when you download ransomware. Basically, now, all software looks to see if that download, does it come with a Trusted Identity? Does the Excel spreadsheet that has a macro in it? Is it signed? is the software that you're going to install on your computer windows or OSX? Does it come signed with an identity? And of course, what are the cyber criminals that hackers do? They say, Yeah, we need to steal them. We need to use them, which the audience will have heard about probably, you know, the prototype of all cyber attacks, which was Stuxnet. And so this will, I think, make it then you know, clear for the audience. So the goal of STUXnet attacks STUXnet was to infect Iranian nuclear centrifuge systems. How do you get software to run everywhere? or even especially to maybe software where there are cyber controls, you make it look like something else. And in the machine world cyber world, that's the machine identity. So the architects of STUXnet actually broke into Taiwanese companies, they stole the identities for building software. In this case, building audio driver software, you know, when you get an update, my audio drivers must be good. And so Stuxnet actually went around looking like it was from the company that was creating audio driver software. And of course, that made it run everywhere, because it had this machine identity. It's a bit like, you know, I show my passport. When I go in through passport control, same things happens as machines at all, whether it's running the software, whether I connect to a website, whether one cloud talks to another, show me your passport, can I authenticate you, we have to keep that safe. That's what we help do with machine identity management.

11:05

Kevin, I looked at your background, kinda interesting. I'm sure you spent many, many hours debating with software developers and solve it. And these guys, they don't care what they do, they'll argue, the most ridiculous details forever and forever. And when I look at software development, now there's this concept called shift left. In other words, take the security considerations and move it more in the early part of the development stuff. And so I would think that there must be a maturation now software development, where they're starting to include these concepts in in the early stages, the shift left, is that is that a target audience for you this whole software development, folks?

11:41
It is. So first of all, as a, you know, where I got my career started in the Department of Transportation, as a software developer, you know, software developers, what do we love, we love to do things fast. Our best friend, you know, what a software developers best friend is,

12:01
it's contrived to do Mountain Dew now. It's that

12:05
maybe Red Bull, but it's actually Ctrl C Ctrl. V. But best engineers are those that know how to copy and paste, which we could talk about a whole nother challenge as we move into the world of generative AI. But let's first talk about software developers. You know, yet their job is to build software, new features, mazing, new features fast, that runs in many ways against if you think whether you're going to build a house, build a road, build a plane, build it fast, doesn't generally mean build it safe. So that's why you know, engineers, please focus on going fast. But there needs to be also, you know, engineers who think about how do you do that safe? That's this whole rise of a security engineer. It's just not me as a as a cybersecurity professional saying no, don't do that. That's not right. Actually, engineers helping other engineers be safe. I mean, same thing we see in the real world, whether you're building a plane or whether you're building a house, there are architects or engineers that think about safety. That's the real emerging role in cybersecurity, not those that can write a policy. Now those that can write code, that's something that's that's changing fast.

13:35
So in the past, many software development, they're they're under the gun to produce something and this quarter, this 90 days, whatever, they have a deadline. And so what it's possible he may have done is that this whole idea with him shins, and he's it can be a laborious process. It's detail oriented. And so if you have a deadline, and you can have to spend two days worrying about machine identities, well, it's possible humans may cut corners. And, and the ones you know, I want it I want a school bus. But I wanted to get 10 miles to gallon, but I want a school bus and have to have it tomorrow. No, and and you get pushed and pulled. And so I think that's perhaps where benify might fit in with the software developers is that, hey, you can get it done on time. Here's a little tool, we can help you with that. Plug it in and bang, and all of a sudden, the shift left actually doesn't delay anyone. It is a shift left and it meets the deadline. So yeah, yeah, that's,

14:27

that's the change in cybersecurity is about making things easy and fast. So give software developers what they need, please. Software developers, don't want you to have to sit and think or create creative ways of using machine identities. Because you've got to use it for zero trust. You've got to use it to be post quantum ready, and more. Well, let's security engineers give that to you in a way that safe. You just build your apps. Yep, precisely right. It's this kind of idea of fast To secure, you know, I do love a Formula One, unfortunately, my team is suffering and really suffering. But if you think about a Formula One engineer, they're building at, you know, they've got two things in their mind. They're building for the extreme of performance. And also the extreme of safety because you can't win a race, unless you've got amazing brakes. Unless you've got a driver. It's the same push pull, isn't it? Yeah, it's the same thing. And it's what we see in cybersecurity, which actually makes cybersecurity really, really cool and fun these days. Yeah,

15:37
I'm trying to come up with a title for this interview. And I bounce all kinds of different things out. I have a lot of test titles here. And I think that your company website, and I'll spell it out here, it's V as in victory en a fi.com. V is victory, tux. So what is the benefit? We orchestrates connections to machines needing certificates? Basically, words, real simple. Well, what do you do? So that's really what you folks do? I'm trying to summarize this for someone who's maybe listening. So what is this? Oh, so that's what they do. They make sure it's secure. And it can be done in a reasonable timeframe.

16:16
Right? You know, if you think about it in the audience, will, you know, there, there are really two actors out there in the world, there are people, and there are machines. And all of us is people, whether that be US citizens, whether that be as customers, whether that be as team members, we all have identities, same thing goes in the machine world, whether that's in the cloud, whether that's in a data center, whether that's flying, all of those need identities to yep, that's what benify does, we make sure that all those have machine identities, so you know, which ones are good or bad, friend or foe.

16:54
And this isn't some topic that's just a obscure corner of a classroom at Georgetown talking about aspects of software development. Now. I mean, there's executive orders. Now, we all know him. One came out in 2021. And they talked about improving the nation's cybersecurity. And the phrase they use is the word you just use trust, trust in digital infrastructure, bank, trust in digital infrastructure. So your company orchestrates what the EO wants, what they want this trust to be orchestrated. So it's reliable, resilient, right. And, and, and, and doesn't suffer outages. That's resilience to me, isn't it?

17:29
Right. And what we've seen is, especially to with zero trust, so we've seen Sisa, release the zero trust 2.0. Guidance. And again, zero trust is just about always authenticate. We think about always authenticating us as humans, always authenticate the machines. And the machine world is a bit different, though, than us as humans, you know it. In the last few minutes, you know, since we've been talking at a cloud data center, not too far from where the audience is, you know, there have been 1000s 10 1000s of virtual machines, or Kubernetes clusters, started. And then maybe even some of them have gone away, you know, the time it takes

to get, you know, 10,000 100,000 citizens or 10,000 or 100,000 customers, it's a very different world and machines, which brings some unique challenges, which, of course, is what vinify helps to do with machine identity management.

18:35

So some people will say, and many commentators have said that the cloud is all about identity. Well, yeah, well, if it's all about identity, then it's about a human identity and a non personal identity. So it may be is really the first step, it's the first step and zero trust every one of those silly pillars, and there's five pillars and six pillars, and every organization has got a different set of pillars, same pillar, it's always identity. That's you guys. Yes,

18:58

it is. Because, you know, as we move to the cloud, it used to be back in the day. Again, when I was the, you know, department transportation, you could go down to a data center, and you could go down and say, yep, that server is helping these customers when it's cloud, I've got no idea, first of all, where it is. So we have to have identity to know what's your cloud, my cloud, the US government's cloud, the UK government's cloud. And also of course, what might the adversary be? So we all that identity is yet at its core, and think about as we you know, head to a world of AI with machine learning of generative AI, which model is good or bad friend or foe? Which code for example, comes out of that generative AI is good or bad friend or foe? So these are all challenges. So, again, the audience has been using machine identities. And we're going to hear more and more about it.

20:08

You know, that reminded me I remember years ago, I would work with software developers, and they would order servers, put them in the server room and load the software on the server. So you could you could watch them do it. And and I've been in a data center, can you imagine a data center and having any idea what's going on? It's loud. You have to talk about identity 52 ideas, even given a data center? Yeah, I'm asked one question that would have to release you from this interview. So I went to your website, I stumbled on something called the Verify Academy. So what's that?

20:38

Yeah, so the Verify Academy is something that's unique. For our customers, it's a learning resource, we, you know, take it really important and upon ourselves to make sure that we are training, the cybersecurity the machine identity management professionals of the future. So the benify Academy is our investment, personal investment in you know, our customer so that they have the skills for today and that their future proof for tomorrow. There's never going to be enough cybersecurity professionals. So we have to become smarter, we have to be able to build code. That's one of the things machines are building machines today. I don't mean robots building cars, that they're building software, whether that's the generative AI, or whether that's building one cloud instance, or 10,000 in the last five seconds. So yep, so bringing education to help everyone become smarter, faster, and then ultimately, as a society, the world that Vin that benify envisions benify envisions a world where machines and humans, we cooperate, we are successful together. And that starts with learning all of us learning.

22:01
Well. Unfortunately, Kevin are running out of time here. You have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Kevin Bocek, Vice President security strategy and threat intelligence at a company called venna phi.

22:16
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.