FEDERAL
TECH
PODCAST

Ep. 30 How to Outwit the Problem of Federal Identity

SUMMARY KEYWORDS
phishing, identity management, people, trust, identity, christine, phishing email, called, federal government, user, pki, absolutely, emails, federal, organization, policy, cybersecurity experts, products, big, read

00:00
This is John Gilroy from the Federal tech podcast

00:02
and this is Christina from guidehouse.

00:04
Today we're gonna talk about identity management in the federal government hit the music cloud.

00:13
Welcome to the federal tech podcast where industry leaders share insights on innovation, with a focus on reducing cost and improving security for federal technology. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:37
Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. today. We have in person Christine Olin, Director at guidehouse. Christine, how are you?

00:47
I'm doing well. How are you today?

00:49
Well, I used to very scientific approach to invite you today. What I do every time I do these silly interviews, oh, we sit around, have a cup of coffee and go, Oh, who should I have on next? And they'll recommend this company or this agency. And then someone said guidehouse. I said, that sounds like a publishing company or something. And so I contacted you got anyone smart there? And they said, Well, we got Dr. Harry Greenspan I go, I've had him on too many times. How about Chrissy, Chrissy be fine. So that's he got the distinguished invitation to be on federal tech podcast with John Gilroy. So your website and this is great part about your website. The big, big phrases out with complexity is well, we got a lot of complex topics to talk about here. Access Management and identity. That's a complex topic and about five hours of that we can go through, we're

just gonna do about a half hour here and find out your experience, you've got a great experience inside the government outside the government got a legal background there. I've listened to several of you interviews, you certainly know the terminology back and forth. Maybe that's your language background, but your terminology is big and acronyms is something that's real good. So let's set the stage. I think everyone knows COVID hit. And a lot of people start working remotely, all of a sudden, all that kind of hints intimations about identity management org, it's like the frog boiling, got to the point where it boiled up to the top. And so set the stage for us, then we'll dive into some of the big challenges we have with federal identity management, please.

02:14
Sure. So I have to say I think the best thing that could have happened to cybersecurity and identity management is absolutely COVID. So one reason for that is because a lot of the vendors who had been working towards doing some really great advancements, they started accelerating the advancements. So before we had, we had, okay, identity Betty, we now have pretty stellar identity betting vendors, we have a lot of vendors on the marketplace, we didn't have that before. We now also have what I call a zero trust broker, which allows us to do more granular authentication and access control, which is something that we absolutely need to be able to hit that zero trust architecture that we're all trying to do, especially in the federal government. And then the other thing is, is that I feel like every organization in the world finally woke up and said, Oh, my gosh, identity management actually matters, we need to do something about it. So it's, it's been a wild ride, because I started with identity management in the federal government in 2013, where I was supporting an agency that was doing policies on federal ICANN. And at that time, it was really hard to see it any sort of adoption within the government. And now here we are with executive level mandates to really drive better adoption, for more complex things like a back right, which is a part essentially, that's contextual authentication to get you to zero trust. So it's really, really exciting to like be a part of this particular time period, because we're seeing that people are starting to understand it more. And we're also seeing the change of oh, I actually want to protect my systems. How do I do this? Okay, now I need funding. How do I get that? So we're working through all of the challenges we have now with legacy systems and all the other things.

04:15
Some people study foreign languages. As an undergraduate, I studied history. So I look at everything from a historical perspective. And I remember years ago, studying all those acronyms, our back and a back and all this and that, and I got my certifications and all that stuff. And, and back in the day back where you are in UVA, they really liked a back and then it switched somehow to roll baseline and all of a sudden, it's like this big momentum earrings are back. And now we see the moment I'm stopped with COVID and COVID. Everyone's go, no, this doesn't make much sense. Maybe you should be based on access, rather than your role because your role can be faked because of identity. And so now we just use that term very trippingly on the tongue back, but But that's really seems to be the trend here. If this is from 40,000 feet looking at trends in identity management Yeah, so

05:00
I would say the reason why there was that switch. So let's talk about that. So, so back in the day, when I was at UVA actually, after that, I swear, but back in the day, I missed did a really good job of creating the rules around a back they have, I can't remember the publication, but they have an A back publication that's actually

quite good. It's like 116 pages, maybe you're you need to drink a lot of coffee while you're reading it. But it really explains what a back is, right. So it's the whole idea of attribute based access control, to be able to take all of your available attributes for a user, and all the other things surrounding that user and deciding whether or not they should get access to a target application. Right. But the problem was, when they created this, we didn't have the technology in place, right. So there were a couple of couple of things that were there, the technology was there. But it required a lot of integration and are required a lot of coding, which quite frankly, frankly, we don't have that, that workforce of vulnerability in the US because we need faster, easier things that are low code, no code to be able to go through and do the integrations quickly and protect quickly, right. So at the time, for a very long time that wasn't available. I've now seen, more and more vendors come out with products that are allowing, at a back allowing you to be able to put that into the system. But it's also on a low code, no code bases, so that we can have people who aren't developers, but who are still very skilled cybersecurity experts go in and do these integrations. And I think that's really important. The fact that the vendors are now giving us less requirements for developers in their products is allowing us to train up quickly, more people in the cybersecurity world so that we can have more people go and do the work that needs to get done. I mean, I think you probably know this, we have the count right now is at least half a million people. We have in dearth, right, so we need at least a half a million, we probably need more than that. And then on top of that, in the federal government, they need a ton too. So we just have this like stretch, then people. So the fact that vendors are giving us the ability to have people to train up people quickly and have them do the work for us. I think that's a really good place that we're going towards,

07:29
I attend cyber street conferences. And if I if I went to a conference tonight, I could probably get a rope and rope together five guys with big beards and baseball hats, and bring them in a corner and go, Hey, let's talk about this attribute stuff. And it's like, oh, we knew all along is that there was way to go. But we just couldn't it was too expensive and too slow. So that's pretty what it was, is that they weren't taking stupid pills back then the fact is, they kind of knew is the best practice. But there were limitations. And just so who's Christine it half hour? No, we can't wait a half hour to find overseeing this. We have to take and and so what you're saying is that? Well, John, the technology is plenty caught up. And now we can go to the good stuff.

08:07
Yeah, absolutely. It's very exciting. And I think COVID did that right? I think COVID accelerated our technology. I mean, we can say that, because look, we have very clear pictures on this on this call. So it's really great. What has happened in the past couple of years.

08:22
When No, I know you'd like to talk about challenges you've had, let's say got another event. And I get 50 CIOs and federal government, I wrestled 10 in the corner, you probably get 10 Different levels of knowledge of identity management and sophistication. And so if you can, because I know you've been in a lot different areas. So what were the first steps for people who's getting into this? And And what about the other and the spectrum? People really are sophisticated? Are there different levels of approaches they should use? Maybe it's conferences should tender books I should read?

08:56
Yeah. So I think it depends on where you come from. Right? So I came from with a lawyer background. So I actually started in policy. And it made a lot of sense to me, because policy is just basically roles of its I viewed fightcamp policies as something similar to the rules of civil procedure, here's how you must operate within this system, right? And then you have all the guidance on top of it. So then you can pretty quickly say if this that, you also have to memorize it. That's part of the problem. But once you have all that down, then that's really good. So that was my foundation. Then I moved on. And I started working on research and development. And so that's where I learned how to do art, architecture and how things how different vendor products interacted with each other, because I knew is in theory, how it was supposed to work from policy, and then I realized that and then the last step is that I then got to start working in the operations which I find is so much more fun than all the other stuff. And so in the operations, you get to actually build it and then watch it work or watch it fail and then fix it really quickly. So so like that was my journey, I think it depends on where you're coming from. If you're coming from an engineering background and starting, like in starting to do operations, and then slowly working your way backwards to learn policy is the other way to go. If you come from an audit background, and starting by doing audits on systems and learning the controls, and then learning more about policies, and then getting into the operations, if you wanted to do that full stack and get to a point, where an architect are actually hands on, on the vendor product, that those are the different ways to go, I think it really just depends on what your background currently is, and, and what you want to learn, right? I don't want to learn how to do development, like I don't want to actually sit and develop things. So I don't have a coding experience, I am not allowed to get privileged access into the products that I help deploy, I have totally been told by some people that I am not trustworthy enough, because they're afraid I'm going to break things. And that's okay. Because I don't need to have that skill set. I understand how it all works. And I can speak decently intelligently with the engineers so I can understand what they're doing. And then I can ask them to do additional things.

11:15
It sounds like you're dancing with being called a policy wonk. I don't know if that's a phrase or a bad phrase. You're gonna walk away now, if I've used use that phrase, but it sounds like you have all the building blocks for it.

11:28
Yeah, so I think you can like so for example, NIST 863 fours coming out soon. And that is, it's like, I feel very geeky, because those are the things that I talk about with my friends to the community right now. You know, let's talk about how that policy how privacy is going to be instilled within the various levels, especially within the IRL level, how is that going to be able to be solved so that you don't have you know, privacy breaches, when you're doing identity betting, blah, blah, blah. So I definitely have those very geeked out policy, discussion slash arguments. I in fact, I had one late into the night at RSA at a bar this last April, which was absolutely ridiculous, but it was fun.

12:19
This topic comes up constantly, you know, there's a office management buzzer minute executive, there's a Ron Ross and his Merry Pranksters up there coming up with these things all the time. We've, I've talked to Sean Fraser, from Octo, maybe you stumbled him at RSA, Sean Fraser is really bright. That was I think,

Episode 14. In fact, I grabbed him from the floor of the show and dragged him over and put a microphone from He's very shy and quiet. So somehow, sometimes he managed to come up with a word or two. But it everyone's getting bombarded with this. It's almost like people saying to this, to that, to this or that, to this to that. And, you know, when you research this whole transition to zero trust, identity management, there's a group called the National Security Telecommunications Advisory Council, that sounds pretty impressive. And in an article I read last night, they said that zero trust is, is at the risk, risk management at the risk of being an incomplete experience, you know, and they said, there's so much disjointed technical security, they're going out there, it's kind of hard to apply what, you know, the imagine in a commercial company, there may be two or three products trying to do the same thing. And, and no one really knows what they're doing. And the federal government, they getting bombarded by so many do this, do that do that, that they they throw their hands up and said stop the world want to get off? So So So you bring the voice of reason to this? Or how can the typical garden variety agency gets you all this?

13:45
Yeah, so I do think that they absolutely need someone who is an expert in all of those things. So when I saw when the when the AEO came out, last year, I went back and I read the zero trust misguidance to seven. Yes, thank you. And, and so I read it, and I thought, oh my gosh, this is everything we've been working towards. So I will say that identity management people, those are the people who read this, and they totally get it. And it's because the whole thing is based on a foundation of I am of I can't these are that if you don't have that in place, you're kind of you can't do the rest of the pieces, right. So that's number one, you need a strong foundational, ICANN. So if you look at for example, M 2209. If you look at the requirements and M 2209. The identity piece is pretty large, and it's in it's very like regimented. And in fact, that's where they put a lot of the dates is in the identity piece. And then after that there's some other pleat pieces and if you go back down through some of the other pillars kind of refer back up to identity so I think that that is a really good foundation. It's a must have. Right. So how do you as an organization, say, you know, does this thing do zero trust or not? Because literally, every every product out there says we do zero trust. Right? I

15:17
just every, you know, I could play Go to the seventh love and it'll be Slurpee, zero trust Slurpee. Everyone, does it get tires in your car to Costco? Hey, tires, it's just, they slap that label on there. And, you

15:29
know, yeah, now they're now the reality is, is the majority of the products are ancillary. So they don't harm your zero trust architecture. But they don't actually advance your zero trust architecture. And you have to take one step back, and you have to say, alright, what is it that I really want to accomplish with zero trust. And it's not like I want to accomplish this buzzword. It's I want to micro segment my networks, so that every user has to get re authenticated before they get authorized to the next application. So I want to remove lateral movement within the system. So how do I do that? And the answer is you need to get well I affectionately call it a zero trust broker. So it works with your network, it segments off your applications. And it also adds in so you have to have an IDP, an identity provider, that IDP should have strong phishing resistant, multi factor authentication. So what does that mean? Fido tokens, web auth, and or PKI. So that so a user comes in, and then all this other information gets added to that user profile? Right? So you've got I know what my IP address is, I maybe I

have a certificate on my, on my gFV. Laptop, maybe I did, maybe the tool is smart enough it normally is to know what my past user history, is it what the behavior I usually have is, so if I'm entering at three o'clock in the morning, it's gonna say, wait a minute, this doesn't sound right. She's never awake this early. So it goes through and it decides, should I give this person access? Right? So those are decide cited by the organization? What is your risk tolerance? If I want to get into an application that's really rich, and like really good information, I can think of some that some of my clients have, right? I really want that information. They should be saying no, especially if I'm trying to get in at 3am. And that's what zero trust is really created to do. So we've had all of these hacks lately, and like, you know, it's almost Christmas. So we're gonna get another one soon. Every Christmas, we have a different security issue. And SolarWinds has shown the lateral movement is not something we can continue on with it. And so that's like the number one thing to do. And how do we reduce lateral movement, we have to know who is on our network, what it is that they're trying to get you. And we have to say, Well, you can't get to everything just because you got through the front gates. You know, this isn't TSA, you can't just get in and go anywhere in the airport. Actually, you can't do that either. But in theory,

18:10
I was thinking about you in the bar at the RSA. I'll bet in another corner of the bar, they're having fistfights over authentication authorization. And and that's certainly not a recommended go down that rabbit hole here. However, rabbit hole, I think would be popular would be a fishing rabbit hole, maybe a fishing hole? Yes. And because this is really what the objective is, is to increase cybersecurity. And the big attack point is going to be fishing. I mean, it's it's pretty true. Every survey of Red Sox about, hey, it's going to come up to me with emails and I'm happy with emails, you have to email I'm sure that people that hack systems out there, good luck hacking the DOD. But I think it's going to be a phishing attack. And so, so the whole idea with this is is to eliminate phishing and and use that term phishing resistant, you know, and use that Web OS and he said that very fast Web. Web authentication. Whoa, wait a minute. When my wife gets a coffee on the way to work at the Starbucks, that's, that's web off. It's not like it's 50,000. cryptographers talking about quantum and crashing? It

19:09
is you're absolutely right when she when she goes to reload her Starbucks. Web web authentication.

19:18
Don't get scared. Don't get intimidated by Christine. Oh, Christine. I'm scared her. No, she's getting a coffee.

19:25
Yeah, you're absolutely right. So so a couple of things on phishing because I think that there's more than just having phishing resistant. Because a lot of people also just add MFA and they think we're good. Alright, so let's back up. One is I would love to eliminate passwords that of course, all of us in identity management would love to eliminate passwords. It is not actually something that's feasible today. And there's so many reasons why, and I don't want to go into it. But that is not a current. Currently, we can't do that. Right. There's too many applications that use password As on the backend, the passwords are still in the system, and they're going to always be in the system. So that's number one. Number two is we have the ability to teach our users what a phishing attack looks like. And the way we do that is we send monthly phishing emails. Now, if you're like me,

and you have too many emails, you tend to end up dealing, you end up passing all of those emails because you don't get to them. But if you have a user who actually reads all their emails, and then get on a phishing email, and they click the link, then they go to essentially training that says, hey, you just clicked a phishing email, here's what would have happened, if you had complied with what they asked you to do. And we want you to learn a little more about this and what you need to look for. And so I know some organizations do a really good job in their phishing campaigns. And they have gone from really high click rates with these campaigns to much lower. Now, here's the thing, you're always going to get a clicker, you're always going to, it's always going to happen. So you can't you can't say, Okay, well, I have this. I'm good. You're always gonna get a clicker. So all the time. As a cybersecurity expert. All all cybersecurity experts do is say, All right, well, it's always gonna happen. So how do we reduce the risk that they end up getting it like, how do we layer security to make sure that people can't get it? Yeah. So then, because it's always going to happen? How do you how do you fix that? Well, you have a phishing resistant MFA. So this is something that's required by the EPO, it essentially is a phishing resistant MFA. And there are three types. One is are in the federal government, it's a PIV card and any other industry, it would be a PKI certificate. Yep. Yep. So it's PKI. By the way, everybody uses PKI all the time, they just don't know it. When you go to HTTPS. On your web browser, there are PKI certificates talking to each other in the background. So the second one are two things that are based on Fido standards, Fido is fast identity online. And they have created. They were they're creating really good standards for industry to use. So industry in this case for them includes Google that includes apple and includes Amazon, Microsoft, so like all the heavy hitters in US industry are in this organization. And so they are they are like some of the smartest people I know, they get into a room, they do have this fights, I'm sure. Now they made the update. But it would be funny if they were having fist fights over standards. So they talk about things like how do we how do we get more credentials more easily into the hands of consumers or the average person so that they can interact more safely with things online? But on top of that, how do we flip that and give that to our internal users so that we can protect our secret information within our systems. So what they've created from that there's two different Well, there's the same standards, but there's two different products that come from that, essentially, one is called a Fido token. So it is a hard token, you plug it into your USB port, and you touch it. And so it says there is a live human next to this. And therefore you can trust that this is not going to Rp deed into the computer and like it's a bad guy, right. And then the second one is called webauthn, where they tend to use your biometrics. So either you, for me, it's fingerprint, because of, you know, the platform I use, sometimes it can be your face. So it's some sort of biometric and that biometric matches, it says, okay, this person is who they say they are, we can move them through, it is a wonderful way to strengthen your organization's credentials. If you don't use PKI

24:01
wish to get a transcript of this because you have the big three. That's a 123. I mean, this is if someone's just confused and wants to federal insurance. How do I prevent phishing? Well take Christine's 123 Maybe a little business card made or something or this is this the three ways to do it. It makes perfect sense. I mean, that's that is and they get a lot of the tools sitting right there.

24:21
Yeah. Now Now, the other thing that organizations do and and I understand why and it's and it's really helpful is that they they add multifactor and when they add multi factor, they may include push to your phone, right?

So that is how they do that second factor. Now, it is not phishing resistant. And there was a hack recently Do you remember

24:43
this hack? Because it's I know it's a public phone system. I know.

24:47
Yeah. There's a hack recently where was trying to get in and they kept putting pushing the push notification to administrators phone and the administrator did the right thing and can have denied it. But then because hackers are getting really good, they call them they said, I'm from your company, and I need you to push. Ah, they did.

25:11
Ah, I know it's public, but of all the things you think it's the one moment you think you're safe, Christine, then the guy comes after with a rifle or whatever out of a shovel. Yeah, what I do some research on this, I think the general accepted numbers for phishing is, is maybe 35% of people click on phishing attempts, and after education, it probably drops down to the single figures. And, and there are some very knowledgeable people that say, no matter what, you could have five PhDs it's gonna be 4% pay to get work in a garage changing tires is 4%. You know, yeah, Harvard, PhD, 4%. Christine, oh, and 4%. Maybe not you. But that seems to be what it is. All we can do is just, it's like, I mean, if you have a seatbelt and airbags to drive real carefully, you generally speaking, you're going to avoid act, but trees can fall. I don't know it can happen. And all we can do is just the reasonable thing, sir.

26:03
Yeah, no, I totally agree. And I mean, you know, I'll be honest, like, in the phishing campaigns, that some of the organizations I worked with, they, I actually got caught lines on them. And I clicked. And the funny thing is, I was actually so upset, because it because it basically it said, and this is a true statement said You almost hit your storage level for Microsoft. Did I believe that? That would be the case? Yeah, then I did the right thing. And I called the security person, the security officer, and I said, Hey, I got this email. I think it's kind of odd. But I it also could be true. Is this the phishing campaign. And He's so mean, to me, he goes, you might need to click. And I was like, now I know never to trust, you know, but the point is, is that, you know, I was tired, I wasn't really looking at the email as well as I should have. I was going through email at this was at the time when I actually read all my emails. So I was going through the email really quickly, and boom, I got it right. And like, and anyone can have that off day, anyone? And it's always, it's kind of interesting, because sometimes, those phishing emails come just right at the right moment where you're like, oh, yeah, this is super important, because I just had this conversation three hours ago. So I absolutely need to click on this link and get this done. Yeah. And then, and then you get hosed. Right. So I totally get it. And that's why it's always gonna be there is going to be a small percentage, or you can just do what I do and not read emails that.

27:40
Well, this has been a fun conversation. If you enjoyed this conversation, share it with friends, called Dr. Harry green spawn and share with him, share it with everybody. Well, we're running out of time, unfortunately, here.

You've been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Christine Olin, Director at guidehouse. Thank you, Christine.

27:59
Thank you, John. It's been so much fun talking with you today.

28:05
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 podcasts.