A HIGHER STANDARD FOR PATIENT SAFETY

12/06/2018

Brian Contos: Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness.

Brian Contos: I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Tim Waldo. Welcome to the Podcast, Tim.

Tim Waldo: Glad to be here.

Brian Contos: Hey, Tim, before we get started, why don't you tell everybody who you are and what you do.

Tim Waldo: Again, my name's Tim and in the professional realm, I'm a security engineer, mostly emphasizing on best practices for deploying security applications. In my private life, I'm an outdoor geek. I'm all about, you know, white water caving, cave diving, hiking, whatever I can get out of the office and into the outdoors to do.

Brian Contos: I love it. What's the best white water run you've ever done?

Tim Waldo: One that I got tricked into, it ended up being a class 4-5 run, dropped out at about 340 feet per mile, which is very, very steep. The guy that took me on it was like, "Oh, this is an easy class 3 run. You'll do great," and it ended up being the epic run of my life.

Brian Contos: Wow, wow. That was a nice friend!

Tim Waldo: Oh yeah, he's notorious for stuff like that.

Brian Contos: So, Tim, as a security engineer working in the healthcare space, what trends are you noticing?

Tim Waldo: Well the trend that I've noticed the most – and probably because I was doing some research to finish my thesis for my masters – was a trend of, and I was only looking at healthcare organizations, but a trend of healthcare organizations that would embed dozens of email addresses into their website for points of contact, for random reasons that I never could figure out. But I was looking for a project to do for the thesis and I had read a lot of stuff on WannaCry and that it

was an open portal, basically, through email. I wanted to see what kind of exposure certain organizations had for WannaCry. So, I did some research, found some applications that would do scans on websites and report back how many email addresses were found in them. I was finding 30 or 40 per site on every site that I would do a scan on.

Tim Waldo: It became sort of disconcerting for me. I ended up not doing that for my thesis, I didn't feel like I could get enough actual data to support the thesis, but it became a personal interest from that point on. I randomly, when I'm looking at new contracts and stuff, will do scans on their domains just to see how exposed they are in the email realm for getting social engineered or phished for getting deployments for WannaCry or other crypto locker type malware.

Brian Contos: Yeah, it's interesting how malware of many times, you mentioned different crypto lockers and, of course, WannaCry, they get in through email, servers, etc. But let's take WannaCry and, specifically, related to healthcare: are you still seeing WannaCry as being a major issue for healthcare providers, healthcare payers, scientists, what have you?

Tim Waldo: Most definitely. I mean, in the last year there was a hospital in Kentucky that pretty much got taken down completely by WannaCry. More recently, there [have been] some healthcare organizations that [have] had pretty severe outbreaks within the last month. It's still very prevalent.

Brian Contos: I was going to say it always amazes me, but that would be a lie because I know there's just so many archaic attacks and I wouldn't even consider WannaCry one of those still relatively recent that organizations, especially in healthcare where they don't have a massive security team and massive security budgets. As most organizations don't and their primary focus is, you know, the patient experience and every dollar that you're putting into security, for example, isn't a dollar that you're putting into that patient experience. So, hiring more doctors and nurses and more medical equipment.

Brian Contos: But is there a higher standard that you think healthcare organizations need to be held to because of the sensitivity of the data that they're dealing with or because of some of the regulatory mandates that are enacted because of that sensitive data?

Tim Waldo: Oh, most definitely. Healthcare organizations, unlike, say, a large retailer that wants to send you a flier, they have information that could, if released, ruin someone's life. Protected health information is a very big thing. That's the reason we have HIPAA and it's there to protect that, but I think a lot of organizations are looking internally to their networks and not considering the external sources that they might be providing to a hacker to then phish them in

the same process. They need to be more aware of what's outside of their network as opposed to what's going on inside their network.

Brian Contos: Yeah, I think it's an interesting juxtaposition because years ago we said, "Hey, you've gotta really focus on what's happening inside your network because of the insider threat." [There's] not enough focus on things like leaving a bunch of corporate email addresses on your externally accessible web servers. So, what can we do about this? Let's get back into the technical bits and bytes of this. What can a healthcare organization or any organization do to help mitigate this risk?

Tim Waldo: So, the first thing is just exactly what I did and that's to examine their websites with an external application or [create] a Python script that will parse through and look for just open email addresses. Sometimes they're all on a webpage and it's like, "For assistance, email this person and they'll help you," which leads into the second part. Once they find those exposed email addresses, they can replace where they're at with an email address with a web form and just have someone, you know, fill out the web form to get information and then the web form gets redirected to the corporate user, not via email.

Tim Waldo: Replacing those email addresses with web forms would be the second thing you would want to do. The third is actually addressing policies that aren't so much related [to] their website but corporate users are bad about going out and signing up for different notifications and you know, email alerts from their banks or following a particular thread that's email driven as opposed to a Facebook group. Those uses of their corporate email addresses also open up exposure. You know, reviewing their policies and making sure their users are aware that they shouldn't be using their email address for those types of situations.

Brian Contos: Yeah, so the takeaways I'm hearing from this is some better coding practices, removing those email addresses, of course. You're replacing it with web forms, to your point. You know, reviewing these third-party policies you have as well, in terms of how people use those email addresses so they're not popping up all over the place.

Brian Contos: What are some other steps organizations can take to utilize preventative solutions to detect and mitigate this threat beyond making the web server more secure?

Tim Waldo: So, leaning towards the technology replacement to validate their email addresses, they can use email gateways that sandbox incoming and outgoing emails. That would protect them from, one, malicious code coming in, and two, protect that health information going out, which is, for a healthcare organization… They don't really want PHI going out to non-authorized users of

that information. That would be a violation of HIPAA and we don't want to violate HIPAA. That's a bad thing.

Brian Contos: Yeah, and that's a good point, you know, when a lot of people think about protecting sensitive data, they default to DLP and sometimes they're not focusing enough on the email gateways where a lot of information can quite easily and often does leak. What an important area for healthcare organizations, especially with non-security savvy employees, probably a lot of people are communicating and sending information back and forth and might not realize the security or privacy ramifications of what they're doing. It's an extra stopgap for potentially careless activity as well, I'm guessing.

Tim Waldo: Oh, most definitely. I mean, you know, back in the day it was all about fax numbers. If you put the wrong fax number in and faxed somebody's health information to the Walmart store, it wouldn't be a good thing. The same thing goes for email. You can easily mistake an email address by one letter and it goes to somebody else that actually has that email address and now you've sent out PHI to someone, again, not authorized. Using gateways and sand boxing technologies for email is definitely a direction that healthcare organizations need to be looking at.

Tim Waldo: I mean, there's always gonna be gaps but the sandboxing technology that's out there now is way better than it was five years ago. I've actually seen some email gateways that worked a little too well sometimes because they would sometimes block actual good email but that's just sort of a tuning process that you have to go through. That's gonna be any product, you know? You have to fine tune them.

Brian Contos: Yeah, yeah, I see that a lot in the DLP area, as well. A lot of folks will deploy DLP but nine times out of ten it's in detection mode and not prevention mode. So, we'll say, "Hey, just wanted to let you know a bunch of sensitive stuff, I think, just left the network." Because, you know, it does take time to get those devices tuned and operating the way you want.

Tim Waldo: Yeah, it's definitely not like a car where you can go buy a car, hop in it, turn the key and start it and drive off. You have to tune your DLP, be that an email gateway or be that, you know, DLP preventing somebody from using the USB key to download data. The software out there now is way smarter than it used to be and it captures that stuff and lets you know about it, but you have to tune it.

Brian Contos: Well the other problem that I often see – and let me know if you see this – I see folks that they'll get something tuned, they'll get it working, it's highly effective and then somebody somewhere, perhaps not even in the security team, maybe in the networking team or the infrastructure group, will make a change to a tap

or a span or something's updated or rule ordering changed or somebody threw a proxy server where it shouldn't be or a million other potential issues and now, all of a sudden your solution that was really chugging along and providing value isn't, right?

Tim Waldo: Totally. I've seen several organizations that, you know, they'll have one person dedicated to doing the tuning for, for example, the DLP and that's just one tenth of their full job. It's not like they're doing daily tuning or weekly tuning on the product. Things do start slipping by.

Brian Contos: Well, Tim, as we wrap things up here, I really just have one final question for you.

Tim Waldo: Okay.

Brian Contos: Who's your favorite superhero or super villain and why?

Tim Waldo: I'd have to go with Captain Caveman. Why? Because he was a very diverse character. I mean, you know, all the other superheroes have their back story and they're all relatively current. Captain Caveman's from the ice age. I think he's a really strong character, actually.

Brian Contos: You know, it's funny, as soon as you said Captain Caveman I started thinking back and I remember this, you know, I know he was like, covered with hair. It was like a long beard or his whole body was hair or whatever but he could pull like, dinosaurs out of it and all sorts of things, which I thought was a pretty cool trick but also reminded me, I think he has a similar backstory to Captain America in that, wasn't he frozen and then somebody rescued him and then he's like, "Okay, now I'm gonna go solve crimes and solve mysteries and things like that." He was kind of thought out just like Captain America.

Tim Waldo: He was.

Brian Contos: That's awesome, what a great character. Well thanks, Tim and hey, thanks everybody for joining us today on the Cyber Security Effectiveness Podcast, sponsored by Verodin. Be sure to check out some others. Take care.