Welcome to the Event Tech Podcast where we explore the ever-evolving world of event technology every week. This show is brought to you by Endless Events, the event AV company that doesn't suck. Now, let's talk tech.

Brandt Krueger:
Hello everybody and welcome to another edition of the Event Tech Podcast. He's Will Curran from Endless Events.

Will Curran:
And he is the fried Brandt Krueger.

Brandt Krueger:
You just said that because of our pre-show discussion, you didn't look that up in the adjective generator.

Will Curran:
Well, no. I mean, I realized I didn't have the adjective generator in front of me, so I picked a really good random-

Brandt Krueger:
Oh, for crying out loud.

Will Curran:
I mean, it's still random because we were talking about it.

Brandt Krueger:
Yeah.

Will Curran:
All right.

Brandt Krueger:
I know, I could have let it go.

Brandt Krueger:
I could have let it go, but I want to know what you think out there. Usually we throw that out to the end, but we were having a pre-show discussion about vocal fry. If you know what vocal fry is, let us know your opinions about it, hashtag Event Tech Podcast, but that is not what we are here to talk about, is it Will?

Will Curran:
Not at all. Today we're talking about all the news coming out of two conferences that have happened recently in the tech space, in the tech security space, called DEF CON, and also

Black Hat. Brandt, can you talk a little bit about what are these conferences? And maybe we start off with, yeah, what is DEF CON, and then maybe we talk about what black hat versus white hat, all that sort of stuff.

Brandt Krueger:
Well, it's actually hacker summer camp, right? It's just this wonderful time of year where all the hackers come out and they put on a lot of sunscreen because they might get seen by the sun for a moment as they go from their Uber to the convention center, and we all come out to play. And so actually what it is, so Black Hat and DEF CON happen to be back-to-back security-focused conferences, both taking place in Las Vegas. And they've actually added a third one to the mix called BSides, and the idea is this kind of splintered off I think a couple of years ago and it's kind of all the stuff that people didn't feel fit anymore in Black Hat or DEF CON. They wanted to kind of spin off and do their own thing.

Brandt Krueger:
And I think they're doing those actually all over the world as well, so you've got actually three simultaneous, or roughly simultaneous, conferences all going on at the same time regarding digital security, hacking. As far as the terminology goes, black hat versus white hat, generally ... It's kind of funny because the show is called Black Hat, and usually what we talk about, you think about the Old West, right? You've got the people in the black hats and the people in the white hats.

Brandt Krueger:
And then the white hat hackers are usually the ones that are the security researchers, they're the ones that are trying to break into things to test things, penetration testing, all of those kinds of things. And then the black hats are the ones that are actually being malicious actors, so it's actually kind of ironic that the show, which highlights all of these security issues, is actually called Black Hat when in fact it's acting much more as a white hat in this scenario.

Will Curran:
And I think it's kind of amazing, all of the stuff that comes out of it jampacked in such a short period of time. I mean, it's kind of like anxiety-driven, weak, full of-

Brandt Krueger:
Oh, yeah.

Will Curran:
... Finding out that there's all these exposed issues. And what's really interesting, too, is that similar to I think any conference, as we all know because we put these on, is that they also present findings that they've probably been collecting over the last year, about major apps, major things. And we're going to talk about a lot of those now, but it's not just one of these things where, "Oh, hey. Yeah, I just found this out yesterday. I'm just going to announce it now."

Will Curran:
And it's kind of interesting how you get this foolery of all these exposed issues and things like that, and yeah, it's really interesting because these guys give really big reports on how it happened, how it got exposed and really go into detail. So it is like a security techy guru's dream, because you really get to learn a lot about how they did it, how it happened, all that sort of stuff, right?

Brandt Krueger:
Exactly. We thought we'd kind of go through ... Obviously, Will and I have been kind of in this space of cyber security and events for a while now and really want to make sure that we're keeping our audiences up to date regarding the latest issues that you need to start thinking about. Now, some of these are going to be related and relatable to meetings and events, others are going to be more generally applicable to just businesses and companies in general, especially if you're a higher-end one that might have some corporate secrets. And then some of these are just, "Maybe we need to know these as just being good citizens," things that we need to know are going on in our world today.

Will Curran:
Absolutely, absolutely. And we want to give a shout-out to TechCrunch, they wrote an article called What Security Pros Need to Know About Black Hat and DEF CON, and we're definitely gaining some inspiration from that article. Shout-outs to Zach Whittaker for writing that article, absolutely fantastic. But definitely some ideas coming from there, and then also we'll be pulling from some stuff that just happened this week that not necessarily is related to Black Hat, DEF CON, BSides, but will be more so just things that happen to be happening this week as well that people need to be aware of.

Brandt Krueger:
Sounds good. Well, where do we want to kick this off?

Will Curran:
Well, let us start off I guess with what they also started with the article, because I think it brings up this awareness of the devices and things that we have going on, and they basically highlighted ... A lot of people are talking about at DEF CON and Black Hat about how Internet of Things devices, or IoT devices, are a huge risk factor, and I don't think we really talked about this at all in our cyber security episode, but I think people need to be aware of what's going on because there's so many of these also inside of the events industry. Brandt, what is an Internet of Things device?

Brandt Krueger:
Well, it's any of these now multiple, multiple, multiple connected devices that we're putting in our homes. I mean, as we start to expand into the smart home worlds, we're adding smart light bulbs, and either those bulbs themselves are connected to wifi or they're connected to a hub that is connected to wifi. We're just finding more connected devices, that's where this whole

Internet of Things comes from, that all of these devices are in some way or another connected to the internet. In addition to our phones and our computers and our laptops, we're having all of these other devices connect. I don't know why I said ... It was probably from the pre-show, I've started to do a lot of those, "Oh!" things that we were joking around a lot with our voices.

Will Curran:
Oh!

Brandt Krueger:
But anyway, we're seeing a lot of these other devices being very much so hackable, so they're not putting a whole lot of thought into these light bulbs and temperature sensors and thermostats and all of the security cameras that people are getting that are being pushed out now. Not only by major manufacturers, but as minor manufacturers try and get in the game to push these products out at a significantly reduced price, they're not paying a whole lot of attention to security.

Brandt Krueger:
And so what we're finding out is a lot of these low-end, and even some of the high-end things like security cameras, are being left wide open for hackers to come in and connect to if they know what they're doing, and it doesn't even take that much knowledge. It actually really is, if you can kind of follow a step-by-step tutorial, pretty easy to discover, find and connect to these types of security cameras.

Brandt Krueger:
As far as the other Internet of Things that are things that are being done with the things, they're just starting to use them basically as botnets, so when we talk about a botnet, it's a group of computers or devices that are being used to achieve some kind of goal. And even if that goal is to just mess with things, these devices are perfect for that, because they are connected to the internet, they can be taken over and then can be used as part of a denial of service attack, that basically you get a million different smart bulbs to attack a single site and it's going to bring that site to its knees.

Brandt Krueger:
So, there's a lot of interesting and easy hacks on a lot of these Internet of Things devices that a lot of thought hasn't been put into how do we keep these things secure, so that's kind of the 10,000-foot level of what's happening. And it's going to get worse as we put more and more and more and more of these things in our houses and offices.

Will Curran:
Absolutely, and I think anybody who knows me well enough knows that I am obsessed with smart home technologies, Internet of Things devices, and so much that when you go and you say, "A-word, turn off all the lights," or, "Hey A ..." Yeah, I almost said it. "Google, turn off all my lights," it's like, "Turning off 45 lights."

Brandt Krueger:
Yes, that's a fact. Yeah.

Will Curran:
I'm like, "In a two-bedroom apartment? That's crazy!" But the interesting thing that ... I read another article today, or this week, actually yesterday, was about the head of Google Nest, which is all their smart home products, their cameras, thermostats, everything, basically their Internet of Things kind of device arm. And the lead of that, Rishi Chandra, I think I am saying his name correctly, basically said that we're entering into this fourth-stage computer, we went from basically personal computing to the web, then we went from the web to mobile.

Will Curran:
And now he's saying that we're going to move from mobile to what he's calling ambient computing, the idea that there's sensors in computers and displays all embedded around you, and you don't have to actually have the computing directly in your pocket or in your backpack or whatever it may be, it's going to be there. And I think that's just going to introduce so many more vulnerabilities, because yeah, it's all sensor data, it's all cameras, it's all the things that it provides is basically the Google Homes and the A-words and the S-words of the world that are literally going to be there to kind of collect that data.

Will Curran:
And that's obviously a vector to attack similarly to the way we've talked about it in our cyber security, is that the events industry isn't necessarily the direct attack. No one's going to, "Oh, we're going to take down the events industry." It's all going to come in sideways to get to something else, right?

Brandt Krueger:
Exactly, exactly. So, it's going to be a continuing trend that we just need to keep an eye on what we're bringing into our homes and offices, and really go into it intentionally. And don't just buy the cheapest smart bulb, right? Make sure it's coming from a reputable manufacturer that's going to stand by the product. I know the Philips Hue bulbs are expensive, but they're also constantly getting updates, which is one of the things that I love about it. I forget which bulb it was, it had some brief memability on the internet, that it was basically how to factory reset the bulb, and it was the most ridiculous thing you've ever seen in your life. It was this whole video of, "Turn the bulb on for three seconds, then turn the bulb off. Turn the bulb on. Turn the bulb off. Turn the bulb on."

Brandt Krueger:
Oh, and it literally was all day. It was like nine cycles of turning the bulb on and off eight times to do a simple factory reset, so clearly nobody put any thought into how that thing should be reset, and much less having updates and things like that. So, I guess what I'm suggesting for our audience is just have some intentionality to it, be sure that you're getting your devices from

reputable manufacturers. I am not one of the ones that's worried that my Google Homes are listening to me. I really don't think they have that capability, to be listening to us all the time 24/7 and then targeting our ads. Someone would notice.

Brandt Krueger:
Exactly the types of people that we're talking about in Black Hat and DEF CON, they would know if this was happening, because they're able to more properly monitor the network traffic that's on there. And if there was a constant feed from every single Google and Madam A device that's out there back to home base, we would see that network traffic, right? It would be there all the time, so it's definitely one of those things. But we do, like I said, just need to have some intentionality when it comes to our Internet of Things devices.

Will Curran:
Yeah, and I think also the awareness to that Internet of Things device isn't just limited to just your home, but also a lot of the devices that we're using in the events industry now, things like for example Beacon Technology to know present sensing when in rooms so you can know how many people are in a single room. Additional things like that continue to be existing inside the events industry as well, so really, really important to know that this isn't just limited to just your home. And that's going to come to the events industry more and more as well.

Brandt Krueger:
Exactly. These devices are going to be everywhere.

Will Curran:
All right. What's the next area that we want to talk about when it comes to the big things coming out at DEF CON and Black Hat?

Brandt Krueger:
Well, this is one that we've touched on in our cyber security stuff, but it's gotten even more complicated. In the past, we've told folks, "Hey, you've really got to be careful where you're plugging in your phones," that maybe you don't just go plug your phone in to any old USB port that you see at the airport or something along those lines. Because for years they've shown the ability that if ... That's a data cable, right? It's USB, it's a USB data cable, so even though you're just using it for charging, it is capable of data, so if you go plugging into a random, "Charge your phone here," station using the USB port, it's definitely been shown that they've been able to plant malicious programs on there, spyware, copy your contacts lists off your phone, all of those kinds of things.

Brandt Krueger:
In fact, I actually just recently read an article that one of the charging station companies is when you click on the terms of service, that basically you're agreeing ... You think you're just saying, "Hey, yeah, I understand that if you blow up my phone it's my fault, not yours," that kind of stuff, but buried in that terms of service was, "We're going to take your contacts and we're going to

send them emails and sell them for advertising purposes." And you agree to it when you click saying that you agree to the terms of service.

Will Curran:
Wow.

Brandt Krueger:
And so that was actually ... So we already kind of knew that, that this was an issue, and so in the past we've always recommended make sure you're plugging into an actual power charger. Plug your charger into an outlet, or make sure that if you are using some kind of power station, you're using your charger and your cable. Well, that just got even more important, because one of the big hacks at ... Let's see which ... I don't remember which one it was, if it was DEF CON or Black Hat.

Brandt Krueger:
But basically a guy worked on it for quite some time creating very official-looking Apple charging cables, so they look exactly like the ordinary charging cables, but he managed to actually make it so that there is an exploit in the cable. So, when you plug in your iPhone into the very real-looking Apple cable, it actually will hack the system right away and you have been owned, or pwned as they say in the biz. So, not only now do you have to make sure that you're not just jacking into any old USB port, now you need to make sure that you're not borrowing some stranger's iPhone cable in order to connect to your phone, because it's the cable itself that actually hacks your phone and steals your data.

Will Curran:
Yeah, this is absolutely crazy, I'm looking at it right now. Yeah, it's at DEF CON, and this looks just like an Apple cable. It's identical, it looks so legit, and basically what it looks like they did essentially is they had a couple of different things. The most common one is that it has a little wifi chip into it, so the idea is that so many people when they charge their iPhone or their phone, they basically plug it right into their computer. Because it has a USB port that's right there, you're already maybe charging your computer, your computer has enough battery life. And what it does, it has a wifi chip that immediately allows someone to connect then to your computer because it's plugged into the USB. Oh my God! And that's what they called the cable, they call it the OMG cable.

Brandt Krueger:
That's insane, isn't it? It's called the OMG cable, yep, exactly. And so what's scary, though, and this is where we get into kind of the gray hat world, is that this guy didn't just make it and go, "Yep, I made it. Isn't that cool? We need to fix it." He made it and then said, "I'm going to make a crap-ton of them and start selling them."

Will Curran:

Not even. Yeah, he sees, like I'm dropping them over the next few days. I think he's just giving them away for free.

Brandt Krueger:
Yeah, yeah. It's really, really more important than ever. Much like the IoT that you're using, officially branded power charging stuff from companies that you stuff, and knowing where they came from so that you buy them directly from ... It makes me so nervous now thinking about buying stuff off of Amazon and stuff, right? You don't know unless it's coming from Anker, or Aukey, or Apple or something like that. If it's from a third-party seller, man, that's going to make me nervous now too when I start thinking about these types of cables.

Will Curran:
Yeah, like you're going into a charging station at an event, right? Companies have all the ... I won't name any companies that currently rent gear, but you guys all know the soft goods furniture companies that have charging stations built into their sofas. Imagine someone just comes around and is like, "I'm going to replace this cable, and I'm going to replace this cable, I'm going to replace this cable, I'm going to replace this cable."

Brandt Krueger:
Yep. Oh, there's so many.

Brandt Krueger:
Yeah, there's a lot. And then just think about a convention center, right? Where we've got a large event going on, who's going to notice if you just roll in with a charging table, right?

Will Curran:
Uh-huh (affirmative), mm-hmm (affirmative).

Brandt Krueger:
So you just look like another vendor dropping something off. No one's going to stop you, no one's going to pay any attention to it, so I think we need to start keeping track of those kinds of things, it's like, "Where did that come from? Who ordered that?" You know?

Will Curran:
Totally.

Brandt Krueger:
"Was that something that came from the venue?" Because I think that's what would happen, is the venue would assume that the event brought it in, the event would assume that the venue added it, and meanwhile it's nobody's and then all...

Will Curran:
Everyone's utilizing it because they're happy.

Brandt Krueger:
Right, right, right, because yeah, you've got to charge your phones. And so meanwhile, a hacker just has to sit within wifi distance. It's probably not a very powerful chip, but still, I bet it goes ... Especially down a long hall of a convention center, you've just got to sit there and then watch the data roll in.

Will Curran:
Yeah, it's crazy. I mean, I'm not even thinking of that fact. I mean, somebody showing up with a table, you don't need to bring a whole table, literally it's just one cable. I remember, I was at a convention center doing an event last week and they were like, "Yeah, look, we have charging stations for your stuff installed in the venue." But no one goes, I'm sure, and checks that regularly.

Will Curran:
And I'm just thinking, too, for an event, it's such a high-profile target because you're getting so much volume, they're coming in so good, people are plugging in, plugging in, plugging in, plugging in super-duper quick, and you're going to be able to get a lot of people's data very, very quickly. Versus, oh yeah, you just hand it to one person, well you're only needing to ask one person, where an event you might get ... How many people do you think use a charging station, hundreds?

Brandt Krueger:
This literally is making me sick to my stomach the more that I read about it. I mean, it's just, once plugged in, an attacker can remotely control the effected computer to send realistic-looking phishing pages to a victim's screen, or remotely lock a computer screen and collect the user's password when they log back in. Yeah, all right, so we're all hosed.

Will Curran:
Yeah. I'm feeling the anxiety right now, anxiety right now.

Brandt Krueger:
And the fact that this guy is just going to start dumping them on the market just makes me sick. And that's when we give hackers a bad name, because I've always been of the opinion that hackers and the word hacking and all that kind of stuff has received an unwarranted negative connotation, and that there's actually a lot of benefits. We talk about hackathons and things like that.

Brandt Krueger:
All hacking ever was originally was just trying to break stuff to see what you could do with it, and there's a lot of legitimate uses for that. I used to take apart stereo equipment, and that's why I know so much about tech and how things work, because I always just take stuff apart. But

anyway, so cables, stay away from the cables if they're not yours. Make sure, yeah, make sure, and if you get them make sure you're buying them from legit sources.

Will Curran:
Cables.

Brandt Krueger:
But I think we can probably move on from that one. It just makes me sick.

Will Curran:
Yeah, absolutely. Absolutely. All right. So, what are the big things that are coming out of DEF CON? Maybe we talk a little bit about ... I don't think I was at ... Oh, no, it was at DEF CON.

Brandt Krueger:
Oh, yeah.

Will Curran:
Some research brought on about Amazon's storage, should we talk about this a little bit?

Brandt Krueger:
Yeah, I don't know too much about this one, so lay it on. Yeah, go ahead.

Will Curran:
Yeah. So, for those who don't know, Amazon in addition to doing E-commerce, their largest and most profitable center for business is actually the web servers that pretty much run 75% of the internet out there. In fact, probably the recording software we're using right now is probably using Amazon's Web Services as they call it, or AWS. And they also have in addition to AWS, which runs live websites, things like that, they also provide a lot of high-volume storage solutions.

Will Curran:
And this one's called the Elastic Block Storage snapshots. And the idea behind this is that let's say for example even a company like Endless, we're creating a ton of video content, audio content, when we get done with it, we're done editing it, it needs to kind of go into cold storage, per se, right? And what that does is allows Amazon basically to store something at a very, very cheap rate for pennies per gigabyte to store your data that you might not ever really touch very often but you want to have it backed up somewhere.

Will Curran:
Well, some research just presented at DEF CON reveals basically that Amazon is inadvertently leaking their own files from the cloud, and there's some exposed what they call buckets, or kind of sections of storage, that are packed with data that if you don't configure it properly could be set to public. Wow, so I think the important thing to know about this is that, yeah, sure, maybe

you want to consider what solution you're using to store all your data and all these things like that online and they come in like Amazon, but always making sure that you check all the settings of everything when you're setting it up. Because a lot of times, these things are defaulted for ease and simplicity.

Will Curran:
In this case I'm sure it's set ... It's not necessarily set to public, "Oh, hey, I can Google search your data," per se, but it might be set public where you don't need a secret key that only you have access to, for example to get into that data and upload to it. It might just be like, hey, you just pointed at a URL and it just uploads there and then allows you to download really, really easily. So yeah, I think it's important to ... I'm a settings nerd, I don't know if anyone knows that. Brandt, do you even know that about ...

Will Curran:
First thing I do when I get a new app, I go into all the settings and I see what all the settings and twist and turn them all and things like that, and you'd be surprised, sometimes the most powerful features in addition to ease and functionality are turned off by default and you end up getting to go through it. But make sure that from a security standpoint you always go through all your settings, and make sure it's set to be absolutely secure.

Brandt Krueger:
Yeah, it looks like there's a couple different things going on there. One is like you said, where people have these S3 buckets and they have inadvertently left them public. But then it looks like there's also this other thing that is going on in the article where they're talking about these volume snapshots that Amazon is doing, that Amazon is in itself inadvertently kind of leaving public. And the analogy they use it that when you wipe a hard drive, you really need to shred it.

Brandt Krueger:
But these are basically virtual hard drives, and so they've got data even if you "write over them" that data is still there, and that's true of current regular hard drives as well. That's why you kind of need to shred them, you need to wipe, wipe, wipe that data. But these virtual volumes it looks like are being left kind of unshredded and your people are figuring out how to poke around in them and find data that has been either reformatted or deleted. It's kind of what I'm pulling out of this, both very bad.

Will Curran:
Yeah. Yeah, very, very, very bad. But I mean, this is kind of the interesting part about DEF CON and Black Hat, is that this is something that they're presenting and putting a lot of information out about how it's happening and how to fix it, yada, yada, yada. And what's interesting is that the companies are responding very quickly. I think a lot of them are actually attending these conferences, so Amazon probably was sitting in on that session, their head of security, and was like, "Oh, yep, I know how exactly to ... Oh, okay. Great. This is really great to fix."

Will Curran:
And luckily they're all commenting very, very quickly saying, "Hey, we're going to get this fixed. We know how to get this fixed. Thank you."

Brandt Krueger:
Yeah, yeah. And that's usually what the goal of this stuff is, is to bring it to light so that people can fix it, and honestly that's why you want people hacking on things, that's why we want protections for white hat hackers, because the more we bring stuff to light ... It's also a good reasoning behind open-source software, that the more people you have looking at something, the more likely it is that you'll be able to find a thing. They found some pretty interesting things, I'm looking, continuing to look through. They found actually snapshots that included VPN information for corporations.

Will Curran:
Wow.

Brandt Krueger:
So they'd be able to actually log onto those corporate VPNs. And they actually also found a snapshot of a government contractor that provided data storage for several federal agencies including intelligence gathered from messages sent to and from the so-called Islamic State terror group. And to quote the researcher, "Those are the kinds of things I definitely do not want to be exposed to the public internet." Yeah, I'm going to agree with that.

Will Curran:
Yeah, for sure.

Brandt Krueger:
Definitely going to agree with that, so that was definitely ... Yeah, that was another big one that came out this week. Anymore you want to add on that?

Will Curran:
Yeah, I think one of the interesting ones I'm looking at too, it says WordPress installations. I mean, WordPress pretty much runs almost 95% of the internet nowadays, and the fact that API tokens, password hashes were found for those installs, really, really interesting, and that can definitely affect everybody, for sure. I think another takeaway too for this, I mean in general I think for as we're going through this as well, is that when it comes to these conferences, or obviously there are people kind of poking at it and trying different things. Again, that white hacker kind of mentality.

Will Curran:
You should have kind of a white hacker mentality or have someone do it for your events as well, not only from the security standpoint, right? Someone who can kind of poke and try and evaluate and things like that, but also that's how you should think about your own events when

you're planning them as well, is how can we poke at and test and try new and different things that might be a vulnerability so then that way we can fix it? And it's the only way you'll know unless someone just decides to do the black hate side of things, which is what we want to avoid.

Brandt Krueger:
All right, so the next one I want to bring up was the warshipping.

Will Curran:
Oh, yeah, yeah. This one was really interesting. You sent this to me on Slack.

Brandt Krueger:
Yeah, yeah, yeah, we were kind of going back and forth with this on Slack as soon as I saw it. Just so people understand the name, it's not just made up craziness, there's a couple of things going on there. One is wardriving, which was the terminology that was used when people would just drive around looking for open wifi networks or just driving around looking for unsecured wifi networks. And then later as more people secured their networks, you would just literally park on the street and spend all day trying to hack into that network, collecting just enough data to eventually try and figure out what the encryption was. So, that's wardriving.

Brandt Krueger:
And then there was another variation of the war, I forget what it is, but there's another variation. So, that's where this idea of warshipping comes from, and what they figured out in warshipping, and this was actually backed by security researchers at IBM, so this was definitely a well-funded and well-backed thing, but then again so are going to be state-sponsored hacking and things like that. So, what they set out to do and succeeded in doing was, "Okay, how can we use mailing packages to basically hack a corporate network?"

Brandt Krueger:
And so what they put together using pretty much off-the-shelf components was a little device that they could pack into an ordinary shipping package, make it look like it's coming from Amazon or something like that, and that little device would have a very low power mode that would just power up enough to send a GPS signal back to the command and control servers. And so that way the bad guys, the "bad guys", would know where that device is, and then they would know when it arrived at its destination.

Brandt Krueger:
So, let's imagine you're trying to steal secrets from a corporate competitor, you send them one of these packages and you notice when it arrives, and once it arrives you power up the main system and the main battery, and the main system and the main battery then immediately tries to start connecting to wifi networks and use a lot of these kind of wardriving techniques. But the difference is now you're inside, the call is coming from inside the house, so now you're inside a competitor's building able to get access to those networks, and then it just starts banging away on those networks trying to find a way to either find open networks or break the encryption.

Brandt Krueger:
And it's very possible to break the encryption on wifi if you have time and patience, you just need to kind of collect enough packets that eventually you can kind of figure out what the keys are and break in. So, it's something as because security researchers know that, they have a tendency to physically put the most sensitive networks deep inside the physical locations of the buildings to prevent someone from doing exactly that, being able to sit nearby and start hacking on the corporate network, but this gets around that.

Brandt Krueger:
So, the whole device costs about $100 to build, and it is equipped with a 3G modem, so it doesn't have to be a super fast modem, so it could be remote-controlled as long as it had cellphone service. And then again with that onboard wireless chip, it would periodically start scanning for networks, and just like any laptop's going to do, it's going to scan for those networks once it's gotten in that location. So, this is a truly frightening piece of technology that they've ... And pretty devilish, too, because what it's going to force people to do is really take ... We already kind of-

Will Curran:
Insane.

Brandt Krueger:
I mean, there's a certain amount of safety that comes just from being a big business, right? When it comes to packages and safety and you have to watch out for, I don't know, bombs or chemicals or things like that, but now what it means is from the moment that package arrives you either have to open it right away and determine that this thing is there and get rid of it, smash it real quick or whatever, or you have to somehow keep your packages in a protected ... It's called a Faraday cage, that doesn't let any kind of radio signals in or out of the box.

Brandt Krueger:
The ability for companies to do that, especially small companies, is going to be incredibly difficult. This is another one of those things where, "Man, that's devilish," and you know if these guys can figure it out, anybody can figure it out that's got any kind of hacking smarts or state sponsorship. And so it brings, much like the cables and things like that, another whole new level to having to protect your data.

Will Curran:
Totally. One of the ideas I just had, too, because we were talking about this so I had a little bit of a leap head-start on trying to think of a solution, but I almost see this potentially creating a mail room intermediary service where, for example, instead of mail getting directly delivered to the building it gets sent somewhere else. And then almost like a TSA check, checks through all your packages, scans it, all these things, they've got to look for devices that are on and all that sort of stuff.

Will Curran:
Because it's crazy, I'm looking at a video right now that explains how the IBM researchers were doing this, and they stuffed one of them inside of a stuffed animal that cheeks light up. And it looks totally innocent, it looks legit, so if you get a gift and it says, "Hey, thanks for all your awesome hard work. Here you go."

Will Curran:
And someone's like, "Oh, cute!."

Will Curran:
Boom, right on my desk, cute little stuffed duck. Woo-hoo, you know? And then there you go, just like you said, they have access to everything. Really, really crazy, I mean, absolutely crazy.

Brandt Krueger:
Yeah, and once again, the whole goal of this is education, right? We're educating people to know that this is possible, and so just knowing that it's possible and getting the daylight out there is a really important aspect to these conventions.

Will Curran:
Definitely, definitely. All right, any other ones that we want to kind of highlight from the DEF CON-Black Hat kind of world as well?

Brandt Krueger:
Those are the biggest ones that are going to affect people the most directly, and on the indirect side I think it's worth mentioning it's a little less connected to our industry or to corporate America in general. But just the fact that they continue to have a voter village aspect of this where they actually purchase real live actual voting machines that are being used in the United States and give people an opportunity to hack on them. And it's one of those things that I think we need to be aware of as citizens of this country and other countries to make sure that we're having fair elections, that we need to have ...

Brandt Krueger:
It's great to have technology, it's great to have the ability to tabulate things quickly, but these machines suck. They're absolutely terrible. Last year they were able to hack one using only a USB keyboard, and they were able to do that in less than a minute, so they were able to break out of the voting terminal and affect the memory, crash the machine. And if you can crash a machine, that's when you can start to execute malicious code, so crashing a machine is always the first step toward being able to execute bad code on this, and they were able to do that in less than a minute. Imagine just sending someone into a voter booth, and those USB keyboards now are tiny, right?

Will Curran:

Wow.

Brandt Krueger:
You could fit one in your jacket pocket. And it's going to take some people more than a couple minutes to vote, and so you have to make sure you give them time, but this is really truly frightening stuff, so like I said, I don't want to spend a whole lot of time on this, because it's not directly impacting the industry. But it's something that we as people, as citizens, need to know about and need to know that this is going on, so I personally, this is me Brandt taking off my event icons and Event Tech Podcast hat-

Will Curran:
Event Tech Podcast hat.

Brandt Krueger:
... for just a moment to say personally I believe this is something we need to be much more aware of. And so I strongly encourage folks to talk to their members of congress, because there's been legislation that's been passed that puts in some pretty common-sense stuff for taking care of our elections and making sure that cities and counties and states have the money that they need in order to secure these things. And it being blocked by certain people in the congress for whatever reasons. So again, not without getting too deep into politics, I would just urge folks to please, please contact your congresscritter and let them know that this is something that's important to us as citizens and that we need to be able to trust our democracy.

Brandt Krueger:
The second half of that is that it's cool to use technology, but there needs to be a paper trail, so there's lots of really good voting machines that are out there that still take advantage of making voting easy and simple. But there is a paper trail to make sure that we the human being can use our eyeballs and actually physically count things if we need to do so in case there is a problem. So, getting off the soapbox now, putting the hats back on. I just wanted to throw that out there.

Will Curran:
No, I think it's really, really important that awareness is a huge part of everything that we're doing. And I mean, that's one reason why we're going to do this episode, is that there's a lot of these things you might think to yourself like, "Well, okay, that doesn't necessarily directly impact me and my size of my meetings or the types of meetings I do, or I'm doing maybe weddings or something like that." But the important thing is awareness in general of this sort of stuff, because the last thing you want to do is be caught off guard, because that's where you get taken advantage of 100%.

Will Curran:
Because, for example, I still talk to people who are like, "No, I just use the same password for everything." But then once they're made aware of how easy it is to use a password manager, which we've talked about in that past episode on cyber security, they go, "Oh, wow. I didn't

know that this was possible or this would happen," or, "Oh my gosh, I didn't know that my Instagram account passwords got leaked. I should change all my passwords." Awareness I think is just a huge, huge part of the security trend.

Brandt Krueger:
It is. I've got kind of one more bonus one that like you said is not directly connected to these conferences but has come out more in the last couple weeks, which is something that we've talked about before but it's getting worse. And another example of how we're going to continue to be targets, especially associations. So, if you're working with associations or you work for an association, planning their annual conference or even their in-between meetings and events, just be aware that that, as we predicted, was going to start picking up the targeting of associations, as well as city and state governments.

Brandt Krueger:
So, the commonality between these things, between associations and cities and other government entities, is that they have a tendency to post their structure publicly, so you can see who's the president, who's the past president, who's the vice president, who's the treasurer. All of these local organizations and major associations across the country and across the world have a tendency to do that.

Brandt Krueger:
And then same with city governments, right? Here's the mayor, here's the city manager, here's the city council, here's the parks manager, we need all that stuff to be publicly accessible. But what it does is it exposes us to these targeted phishing attacks, these spear phishing attacks, where then it's easy for a malicious actor to create an email that looks like it's coming from the treasurer being sent to the president, or vice versa, right? Here's the president of the association sending something to the treasurer, "Hey, I've got this spreadsheet that I just don't understand these numbers. Maybe you can help me explain them, because you're better with numbers than I am."

Brandt Krueger:
And then the treasurer opens up that spreadsheet, and boom, you are pwned, so same thing with city government, same thing with schools. Kind of along the lines of the voter booths, if you have any connections to these organizations, we're seeing hundreds and hundreds and thousands of dollars add up into the millions of dollars being either paid out to hackers that are doing ransomware on these entities. Or at the very least they're having to go back into backups and recover that data. Sometimes that is being covered by insurance. We had a whole episode on backups, just recently came out as we record this show, so it's important to listen to those things, make sure you've got a backup.

Brandt Krueger:
But if you deal at all with your schools, with your city government, with your local government, your state government, or are working for an association where this information is publicly

available, you really need to start paying attention and getting the word out amongst your people that you are a target. I actually reached out to both my city and my schools in the last couple weeks just to say, "Hey, guys, seeing a lot of this as people are coming back to school."

Brandt Krueger:
And they're plowing through their emails, they might not be paying attention that closely, and sure enough our local IT district director was all over it and was like, "Yep, we've already instituted all of these secure measures and all of these things, and we're doing a training program to get people to know how not to click on links in email," and all that kind of good stuff. So, that's my other soapboxy thing for today.

Will Curran:
I love it. I love it when Brandt gets on the soapbox. He's-

Brandt Krueger:
Soapboxy.

Will Curran:
He gets very boxy and very soapy. No, I love it, I love it. I think you're 100% right, for sure. I agree with you.

Brandt Krueger:
All right, let's wrap this papy up ... Puppy up. Papy? Papy. Papy?

Will Curran:
Yeah, I was going to say ... Yeah, just papy, papy. Well, we talked about a paper trail earlier, so let's wrap this papy, pay-pay, up. Yeah, no, awesome stuff. Brandt, do you want to kind of just take us home and kick that outro?

Brandt Krueger:
I'd love to. It's so important, folks, and that's why we like to do these episodes, that we know what's going on in the space even though we're not necessarily cyber security people ourselves. The important thing is to make sure that cyber security is all of our responsibilities, it's not just being taken care of by the white hats and by folks with the glasses down the hall. We need to make sure that we're all doing our part to make sure that we're keeping ourselves, our organizations and our attendees' data safe as possible. So, Will, thank you so much for joining me as always, I really appreciate it.

Will Curran:
Yay.

Brandt Krueger:

Yay, I love it when we can just rock this nerdy stuff out. So, thank you all for listening, really appreciate it as well.

Will Curran:
Thank you, Brandt. Always a pleasure [crosstalk 00:40:59]-

Brandt Krueger:
You can listen as always in all of your favorite podcatchers, whether that's iTunes, Pocket Casts, Google Play, Spotify. We're seeing a lot of interesting data coming from Spotify these days, so that's always fun. But wherever you listen to your podcast, be sure and let us know if we are not on there, because we want to be where you want to listen.

Brandt Krueger:
But of course one of the best ways that you can do that is at EventTechPodcast.com, there you're going to see all the show notes and the links to all the resources that we share, the transcripts. We'll drop some of the links to some of these articles that we're talking about over the course of today so that you can check it out and be just as secure as we are. So, what do you think about what we're learning from these conventions?

Brandt Krueger:
That would be a fantastic episode, by the way, as I'm thinking about this, Will, is I would love to get someone on from one of these hacker conventions, because it's got to bring a whole different level of security, right? Because you've literally got a convention full of people whose whole purpose in life is hacking things, so if anybody knows anybody out there that's related to any of these, whether it's Black Hat or DEF CON or BSides-

Will Curran:
Totally.

Brandt Krueger:
... That is willing to share the experience of being a planner or an IT person related to those events, please do let us know. Contact us. You can do that at hashtag Event Tech Podcast or send us a good old-fashioned email at EventTechPodcast@helloendless.com, so thank you as always for listening to the Event Tech Podcast.

Thanks again for listening to the Event Tech Podcast. Be sure to rate and review us on your favorite podcasting app. Also, be sure to head to EventTechPodcast.com and leave us a comment about this week's episode. We'll see you next week on the Event Tech Podcast.

Brandt Krueger:
Event Tech out.

Will Curran:

Tech it out.

Brandt Krueger:
Event Tech out.