Life of an Ethical Hacker with Brad Ammerman

CyberAware Podcast: Season 2, Episode 4

Nathan: Welcome back everybody to the cyberaware podcast. My name's Nathan Sloneker, your resident expert on all things cybersecurity here at Minnesota State University, Mankato. And today I'm joined with Ham again.

Ham: Dude it's so great to be back in the studio once again, as always. Today, we do have an extended episode going on featuring a special guest. In this episode, Nathan sits down with an industry expert, Brad Ammerman who works in the field of ethical hacking.

Nathan: Yes. This week, as you said, Brad Ammerman, we had a great conversation about hacking in general. Brad himself as a penetration tester, if you're familiar with what that is.

Ham: I think we've covered it just a little bit. Why don't you tell the folks at home what it's all about?

Nathan: Yeah. So with hacking, we have ethical hacking, we have unethical hacking. Ethical hacking is legal with permission and stuff. And then unethical, obviously illegal, under the table, bad. So Brad himself is an ethical hacker and he came in and just shared a bunch of stories and some good advice for all of our listeners here.

Ham: Today, Nathan and Brad, will walk through everything you need to know about the world of hacking. So sit back, relax and enjoy what we're about to talk about today folks.

Nathan: Today, we're joined by Brad Ammerman for an episode on hacking a welcome Brad. Thank you. Just a bit of a start here. If you just want to introduce yourself.

Brad: Yeah. So, I'm the manager of an offensive cyber operations team based on Iowa. Basically I run a small team of somewhat nefarious gentlemen who gain access, usually from an external standpoint to an internal standpoint, on 90% of our engagements.

Nathan: You know, we have ethical hacking and we have unethical hacking. What one of those would you say that you do?

Brad: Definitely ethical hacking. We get authorization from the client.

Nathan: Ethical hacking, obviously you're doing things proper, right, legally. Versus unethical. And that would just be, I guess, bad actors, criminals, that sort of thing. When it comes to Ethical hacking I feel like it's not a job or something that a lot of people are actually familiar with.

Brad: Basically a company will pay by company and I'll send a consultant or assign a consultant, you know, as their lead penetration tester. And depending on what the service is that the client needs, whether it's a physical assessment, a virtual assessment where we're actually doing it remotely or an onsite, , internal, external assessment. My guys will, you know, basically accomplish the mission, so to say. We're just trying to act like a threat actor. And we will mimic some of the attacks that they do.

Nathan: Like you mentioned, you run a team and you yourself are a penetration test. You, do you want to explain kind of what that is for the audience?

Brad: Sure. Basically we use manual and automated techniques to exploit vulnerabilities on internal and external networks. Usually it's trying to social engineer our way in and then from that social engineering standpoint, that's kind of like our pivot either into like potentially their email system to look for business critical information or through their VPN. And, you know, once we get in through their VPN, That's all she wrote. It won't take us long to get to what we need, whether it's, again, business critical information, domain credentials the file known as the ntds.did, which is like, you know, the brains of your active directory. It has all users and passwords that are cashed on there.

Nathan: Okay.

Brad: And that's from the networking side. Then we got like web application side where we'll rip a web app apart. Or physical sides where I actually physically try to break in. I mean, you you've seen my grappling hook.

Nathan: So this does go a bit more broad than just online I mean, you can physically try to break into places. That's part of the gig. Okay. So follow up on the grapple hook. What's in your toolkit.

Brad: Oh, geez. Uh, we got under the door tools shove knives. Honestly, what I've been mimicking is there's locksmiths out there, but a lot of those tools really aren't sophisticated enough without the proper training, but there are also tools that people use to like get into cars.

For example You got air wedges. Well, if it can work on a car door on the mirror, it can work on, you know, the door of a building. And there's a lot of firefighter tools that I implement, which are entryways that are perfectly legal to purchase. So I put that in my toolkit and that would be like the shove knife the under the door tool - it's a great way to get into buildings from the interior, but you're sitting on the exterior.

Nathan: What are you after, when you try actually go into a location?

Brad: It really depends on the client. I've had clients ask for specific materials where it's not digital equipment. Actually gaining access to a physical server showing proof that we were in taking pictures inside, art, getting inside the vault, things like that, you know, are the, the red flags that they want tested and to make sure that we can or cannot get to, and, you know, 9 times out of 10, the client doesn't want us to get there, but you know, they are pleased to know when we do get there, cause we'll tell them how to fix it.

Nathan: What kind of issues do you run into are dangerous that there are doing these sort of tasks when you're going into a location physically?

Brad: Armed security guards. That's that's a big one. Get on your knees and put your hands behind your head. I've had that happen before.

Nathan: A lot of this job you said is a social engineering. When you, you you're, I guess caught in a way, or like you're approached by a security guard. What's your course of action with that? I feel like a lot of people would fold under that.

Brad: I mean, it's definitely within the scope of just being like, yep. I'm caught, here's my letter of authorization I'm actually allowed to be here, but that could even backfire look at what happened to those Coalfire guys in Iowa, you know, they had letters of authorization, but they got thrown in jail.

Nathan: And I not familiar with that. If you could explain that a bit or at least some that story up.

Brad: I mean, from, from what I know, basically they were getting into, I believe it was a courthouse and there was a disagreement between the police officers and the sheriff. And I believe it was actually more of a political thing than anything, but yeah, these Coalfire consultants were detained and put into jail for quite a long time, before they were actually released.

Nathan: So I, I'm kind of curious on just the overall laws with it.

Brad: We have all those laws that are in place that we don't break. We get authorization from the client and that's basically our legal document that says, yes, we can send these phishing attempts or yes, we can try and break in. If my guys ever feel like uneasy, I'll just tell them to end the engagement right there so they don't go against their personal ethics. Cause some, some people can't lie very easily to others. They potentially could call the project right there.

Nathan: You want to explain , what attacks or ways you guys try to approach a client? We have covered like in previous episodes, you know what fishing is, spam, hacking, ransomware, the whole, whole nine yards. I mean, it's not just hacking for you guys, it sounds like.

Brad: No, not at all. I mean, like for us, when we're doing fishing, we'll do phone phishing calls. Either pointing them to the email that we sent a couple of days previously, or just coming up with a completely different scenario to try and get them to, you know, let us remote into their machine or to go and click on a very nefarious link where they have to enter their credentials and we'll leverage that to get in from the external to the internal. And that's our mimic of, you know, threat actors. Cause that's what they're doing.

Nathan: Yeah, I mean, we talked about fishing here, you know, and what it is. One of the biggest things that we say is, you know, the biggest kind of vulnerability when it comes to just places in general is the people most of the time. I don't know if you agree with that.

Brad: Oh yeah.

Nathan: Yep. And I mean that we, like, we talked about previous episodes, you know, just how important it is to just make sure that all your team or everyone you work with is up-to-date, which is cybersecurity in general. Make sure they're cyber aware, I guess, coming back to the podcast itself. From your standpoint, what are I guess some of the biggest things you think people should look out for from a company or just even personal standpoint, just keep safe?

Brad: A Lot of companies don't do security awareness training right. That's the sad part. It's a check the box exercise. So that way they're either fall in line with their compliance or with the standards that are set forth by the board. And that's where it ends, you know, whether it's quarterly or yearly and a half an hour video and maybe a quiz at the end. And that's not enough. You actually need to like, game-ify the system where it gets ingrained into them on a daily basis where they're taking it home and using those techniques on everyday life, not just at work.

Nathan: Okay. And I, that ties into, I guess, the personal that I was asking you about, you know, what, what steps can someone like me or even our listeners here take, in order to remain safe?

Brad: I mean, most of the time people like just individually, won't be ransomwared. Yeah, you're going to have some pretty high dollar targets that might. However identity theft is huge and if they

can get in and get, you know, information on your identity, That's a big black market thing right now. Credit card numbers, your supposed security numbers, you know, they're going for pennies on the dollar, but when you have 5,000 and put it on the dark web, you know, you going to make a pretty penny.

Nathan: When people think of like identity theft and whatnot, it's not like someone just selling a single credit card. I mean, you have, you have lists upon lists of thousands of credit cards that you can buy. I don't know how much they go on for, but, and then from there, it's not like they're immediately going to use it. I mean, your credit card number could be sitting for three years before anyone even tries to using it, but it's out there.

Brad: If you have a device connected to the internet, you're vulnerable. I mean, that's all there is to it. When you asked about ways to protect yourself, there's a ton, don't have the same password or that your Facebook and your bank have, you know, use multiple passwords, having strong passwords has always been a recommendation by people. I actually recommend passphrases and then changing out some of the characters or adding characters at the end, like special characters, just to make it one step further.

Nathan: Do you want to explain passphasing to, I guess our listeners here?

Brad: Basically think of it as, you know, like these are not the droids you're looking for, like, that's your password, you know, some famous quote that, you can remember. And then also, with the mutations that you put into place or the, the additional characters you add, you know, that you're always going to remember, but the other sad part is you're going to want one password per every sensitive account.

Nathan: Yeah, I, I feel like that's one of the mistakes so many people they make nowadays, especially in our age, you got the same people for their Instagram or Snapchat, and it's the same password they have for their bank account. As any actor's going to do, if they get one of yours, they're probably going to throw that at the wall to see if it sticks to anything else. And if it does, you're just extremely vulnerable the more they get.

Brad: 100%. Other things that they can do to protect themselves, making sure none of their equipment has default credentials on there, you know, logging in and making sure that they do change their username and password, or at least the password. I know some vendors you're not allowed to change the username. It'll always be admin or root, but if you can get in there and change the default password, that's another layer of protection. There's also using password safes to store your password. So you have one password that could be like 64 characters long that you remember and that is what decrypts, you know, the password safe. And you could also have the password safe on cold storage. So it's on a flash drive or it's on a USB hard drive.

Nathan: Not on your network in any sort of way until it's need to be used. So going back onto passwords, how easy, or I guess difficult, can it be to grab someone's password?

Brad: It's a matter of seconds.

Nathan: When it comes to like cracking and stuff, you know, it's, it's not a matter of. Time it's I guess how fast you can process it, correct?

Brad: Yup, cause you're basically leveraging high end video cards and they're they're CUDA cores and they're GPU processors to basically smash multitudes of passwords at once. I mean, I can easily crack an eight character password in a matter of minutes.

Nathan: I take it, you probably have some sort of cracking machine set up?

Brad: I actually don't know the specs of the machine themselves, but we're using two, high-end like $1,500 video cards.

Nathan: I mean, people I'm sure have some big machines. I guess if you're comfortable, would you mind explaining kind of how the whole password cracking?

Brad: Yeah. I mean, basically you will pull a password hash file off of a network, whether it's, you know, cached credentials you're basically just gaining access to a windows based hash and that hash is pretty much known. And then what you do is you're leveraging a password cracking tool. Once we get this hash file, we'll leverage rule lists and word lists, or we'll just do a brute force attack and/or dictionary attack to try and, you know, basically break that hashed password. Well, our word lists are upwards of gigabytes.

Nathan: Do you wanna explain to what the function of a word list is?

Brad: Yeah, basically it's just dictionary words known passwords that have been identified from the dark web or dumps. There's tons of dumps out there that have, you know, lists upon lists of passwords.

Nathan: The average password for most people is, you know, I'd say under 10 characters, if you'd agree with that?

Brad: Oh yeah. On average people just do eight. I mean the biggest ones that when I do password spraying, I will do the season in a year and I'm pretty likely to get one person fell for the fall 2020, or summer 2021. And then maybe if that doesn't fly, I'll do fall 2021 with an exclamation point. And I'll I'll password spray that and nine times out of 10, there's going to be someone that I identified through my reconnaissance phase that used that password schema.

Nathan: Password spraying, what exactly does that mean?

Brad: I've built a user list. Let's say I'm trying to get into their maybe not office 365, but you know, something similar that has a login and a password. And basically I'll just leverage my user list with a couple of passwords and I'll send an attempt to, you know, throw these passwords out, to actually get authorization to the device without locking out the user. So we'll do this every 45 minutes. We'll send like two attempts. So as to not break that three attempt

Nathan: With hacking, we have different kinds of teams, you know, we got red, we got blue, we got purple. obviously you're on red, which is offensive. Blue on the other side is defensive and then we have purple. Do you kind of want to explain things that you guys have done?

Brad: We just work with the client's monitoring, the network connections and activity on their internal network. And we'll be like trying to emulate a threat actor. So we usually launch a pen test first What we'll do is we'll just start launching attacks and work with the client's to see if they were able to alert on it or even identify the activities that were going on.

And then after that, we will work with the team, sit down and say, okay, these are the, the techniques we're going to be using. And then right before we execute, we alert them. We execute. And then we follow up and ask, you know, were you alerted to this? And did you identify the traffic? If yes. You know, we move on to the next, if no, we got to rinse and repeat until, you know, they tune the tool that they're using, to be able to alert and catch that malicious traffic that we are sending them.

Nathan: What are some of the most fun, I guess, jobs or events that have happened throughout your time being a pen tester?

Brad: Mine are always physical. I just like physically break it into something. And not even like the social engineering of the physical side of it, where we tailgate or something like that. I actually like thinking like a bank robber and, you know, getting into a vault is like so much awesome.

Nathan: Do you have some funny stories from doing physical jobs?

Brad: I mean, the grappling hook is always the best one. People don't think, you know, like when they see my grappling hook, they really think I'm going to scale a wall and that's not what it's used for. If you think about places like. Boston, New York, where they have to build up instead of wide, they have fire escapes and those fire escapes usually are protected.

You know, they don't have it all the way to the ground. Yeah. It might be, you know, like floor up or something like that. Yeah. So basically I just use my nice little handy dandy grappling hook, and I'll throw it up there to try and, you know, catch it and pull that fire escape down. I have used it to descend into places, but I've never scaled a wall like Batman or anything like that.

Nathan: Fair enough. No, I think I, I mean the grappling hooks fun. I mean, I know you handcuffs, you pick, you pick locks for fun, all that sort of thing. what kind of skills do you think are needed for those kinds of field?

Brad: Your soft skills are going to be huge. for social engineering, it's. Impossible to be introverted. But somewhat of an extroverts mentality is kind of a key it's again, it's not 100% required, but it definitely does help. And I wouldn't say you need skills for the job. Those can be taught having a drive and a desire and a passion for the type of work is kind of what I look for as a hiring manager, because from that aspect, You know, I'll bring in as an intern or a junior, and then we'll teach you how to do most of the job.

Nathan: So you hire for the person. I also know you have a lot of certificates.

Brad: Just from my standpoint, it's really hard to get experience if you're not a collegiate kind of person foot in the door is getting those certifications, whether they're the low level, or the more higher end ones, which are like the offensive security certifications.

Nathan: Okay.

Brad: Um, I actually helped write the pen test plus, and that one's geared more towards someone who's got two or three years in the field. But the, good part is, there's so many free training materials out there. Like hack the box volume hub. Just these, try and hack me websites. There's a plethora of them where you can get the skills to, you know, basically challenge these certifications without, even opening a book.

Nathan: But yeah networking at the end of the day. Knowing people is how you're going to get your foot in the door at the end of the day.

Brad: I agree with that. My entire career probably got launched from the connections I made at DEF CON. It's a massive security conference. People come and show crazy new attack platforms, new tools out there, new techniques. Then they got, you know, their own little mini conferences within the big conference where there's like a car hacking village and an election the hacking village where, you know, you're trying to hack voting machines. There's a bio-hacking where people are injecting themselves with magnets and RFID readers and things like that. So, it's a massive, massive get together of people who wear black hoodies.

Nathan: I'm not even a pen test for I'm most days I wear a black hoodie and myself, so I understand. You know, we talk about the typical, hacker voice I'm in sorta thing you see for movies, I'm curious to see your opinion on how most TV shows or movies get it.

Brad: They don't. I mean, so I know the person who helped write Mr. Robot and that definitely went crazy towards the end. But if you think about it, when you have these types of threat actors out there and. Just a collegic, hive mind like anonymous, things like that could potentially happen. The other older things, like the movie hackers where, you know, you see this crazy psychedelic spiral of stuff when you're logging on and yeah

Nathan: he's like, all right, I'm in here's everything. And you're like, well, that's not really how it works, but all right.

Brad: Not in the slightest most of the time, it's just guys with just two liters of mountain Dew in front of them with a terminal with white text on black background. And that's, you know what they're going at are green text on black background, and third, you just type in a way that's the real world. And in the end being a pen, tester is great and all, but that shows no value to a client. What we do gives the client no value. The service is actually in the presentation and the report. And the report is that we deliver has, you know, the recommendations to the client on how to execute, you know, specifically the fixes on the vulnerabilities we identified and the recommendations, if you cannot fix it.

Cause there are things that are baked into windows or on their network that is legacy that they, they can't upgrade or they can't update. Just because it's either A the company's out of business B it's such a business critical asset that they can't afford to have it go down or there's, you know, no way to get it patched.

So we have to take those types of things into account and portray it to the client on the ways to at least. More defense in depth behind it. So that way it's less likely a target if there was someone on their internal network.

Nathan: Okay. Yeah. I mean, at the end of the day, it sounds like it's a team effort between your whole company.

Brad: I would say the big, sad part is a lot of companies don't think they're a target and that's the thing like, they're like, oh, we don't need this because A it costs too much and B you know, we don't have that kind of information. Well, they do. And they are a target. They're just not targeted yet

Nathan: you know, know if your target, why you're a target recognize your vulnerabilities. when you think of big companies, I mean, let's consider Amazon, everyone knows them, but then if you

compare it to a small mom and pop shop car dealership, or something like that. Most people don't think that that they're a target. I guess what goes into that mindset is people think they're two small fish in a big pond or what?

Brad: That right there pretty much sums it up. Why would I be a target when I only make, you know, $30,000 a month where these guys make that in about 10 seconds.

Nathan: And at the same time, you can't afford to go down, but if you have nothing in place to protect yourself from that sort of thing, it's what makes you a target because these big companies, they're the ones who are having, you know, countless things and steps in place.

Brad: Im seeing crazy amounts of school districts get ransomwared, hospitals, legal firms. I mean, you name it. And these they're not big, some are non-profit hospitals that, you know, they don't have a lot of money. And the threat actors are asking for, you know, 10 Bitcoin or a hundred Bitcoin or $500,000 just to get their data back. And that's, that's real life and here's soon, pretty much ransomware as a service is here, but, hacking is going to be in everyday business. And there are all have already been, videos of people gaining access into these facilities where, you know, to the people that are there, it is a business and, the outcome is they get paid or your information gets leaked or deleted.

Nathan: And I guess not even on the business side of things, do you want to talk about state sponsored hackers?

Brad: Think of it like our NSA. I mean, our NSA is there, whether they do state sponsored hacking of Iran or any other place, basically state sponsored, I would say is a team of, highly educated or at least highly smart cyber crime people or even the mob for example, are basically paid by the government to gain access into other people's information, whether it's from a spy standpoint or from a criminal standpoint to either cause disruption or to cause, harm and or to just make a crap ton of money.

Nathan: You mentioned other countries like that. It's, it's a real thing. I don't know how many people are aware of, Russia, China, North Korea, the U.S., Iran. We're just throwing things at each other. You bring up solar winds for instance. Not many general non cybersecurity people understand, the scale of solar winds or why it was scary. Most people , haven't heard of it. They might've heard it on the news for that quick news segment before they showed the cute puppies. But most people, I don't think really grasp how big the situation was.

Brad: Yeah. I mean, to give you an example, a solar winds is a huge, huge piece of software. I would say most of our federal government uses as well as state, local governments and a plethora of the private sector. And there was basically a back door, coded into the software that allowed the threat actors into it and basically sit on the network going undetected. I think right now the speculation is it was Russian state sponsored, but you know, once they got in, they just sat there and goes, we did cyber espionage.

Nathan: When it comes to state sponsor, you know, you just try to get as much dirt on the other persons that you can. I don't know how difficult it would be for someone to say, go after a power grid. I mean, they're already going after hospitals, what's stopping them from going after power grids, communications, you know, like nuclear reactors, those sorts of things.

Brad: I guarantee they're targets. Our power grid is so unsecured that it's only probably going to be a matter of time until the government either takes it into account because as you saw by that gas pipeline that got shut down, you know, that's part of the power grid and you know, really open the

eyes. I would hope it opened the eyes of the house and Senate to actually put forth some legislation. And by what I've seen, Biden is trying and they had a big consortium of cybersecurity. People go and talk to them and hopefully good things come out of it. But, you know, it's all going to be hands tied because of budgetary reasons, because security, isn't something that makes people money in the end. It just protects to not lose as much.

Nathan: Yeah. I don't know about you. I feel like just, for most people, it just doesn't take precedence over a lot of other things when I feel like it should. I mean, think, you know Much technology is in our lives, or I guess used in our daily life and compare that to how much stuff you have tied in with it.

Brad: I always try and again, I gave him a five things and tried to relate it to people as a personal identity instead of as a huge. Sect of, you know, security. I always ask them like, do you lock your door when you leave? Do you lock your car when you get out of it? You know? Well, that's the equivalent of, you know, putting secure passwords on something and making sure that you have a firewall and antivirus and other protections on your home computer, like that, being able to relate it to a person on a layman's terms.

Nathan: No, I got you. But most people aren't as trained or as. Aware as they should be. So I guess that just ties in and, you know, for anyone listening, you know, just be aware with these sort of things, it's always important to do. We were just talking about companies, but then, you know, we also talking about like power grids and stuff like that. How different do jobs get when it comes to hacking?

Brad: Oh crazy amounts. Like there are people who just do open source intelligence on companies. There's, you know, people who try and identify threat actors and then you have like reverse engineers who, you know, rip the piece of malware apart and incident response. Those are the guys who, you know, go and find out what happened and get to the root cause of how a breach occurred. You have actual breach negotiators where they'll come in and basically try and make it cheaper for the company to pay the ransomware. If they ask 500 K and the negotiator it'll get them down to a hundred K and he got my team on the offensive side of the house where, you know, physical, digital, um, web app, uh, IOT hardware, you know, those are all silos within, you know, the offensive side of the house.

Nathan: You're not just a hacker at the end of the day. I mean, you can get so specialized, like you were saying, there's some people who I've heard you speak on it before, you know, there's, this is the only person that you know, who does this sort of thing. You know, it's not just a one size fits all when it comes to this.

Brad: There's a lot of niche targets out there and case in point you could be an IOT hacker and trying to take over someone's Alexa, but you don't know anything about Google home. So like that's your forte is you're just the Alexa person.

Nathan: I am curious. I mean, do you have Alexa, do you trust the Alexas and Google homes and the whole nine yards or?

Brad: I have Alexa all over my house. You know, if it's listening to me the consultant that is listening might have a really good show at the end of the day, but not gonna affect me in any way, shape or form. Yes, is it weak and vulnerable? It is, however I have it behind so many layers of security that potentially will protect me. However, at Def con, just this year, I've met a person who basically said it don't matter what protections you have in place. They wrote a tool that can take it over. He basically said watch this and I watched it and he wasn't kidding. It was behind a firewall. It had some other protections on play in place like EDR and other things. And he was able to take over the guy's Alexa.

Nathan: What, what's the I guess community, like when it comes to hacking, like, do you share resources or is everyone pretty much like, this is mine. I'm not sharing.

Brad: Its 50/50. I mean, some companies do work together. There's a big open source community to where they'll release their tools to the community. And hopefully the community gives back, you know, whether it's bug fixes or feature recommendations or things like that. It's, it's honestly a 50 50, you're going to have some people who are like mine, you know, they're the what did the seagulls in finding Nemo? You know, they're going to be like that. And then there's going to be others that, you know, try and give back and try and, you know, come to a conglomerate where they're sharing, you know, threat actor, activity, and other, you know, state sponsored, you know, indicators with either the FBI or the CIA or somebody. So that way it gets disseminated.

Nathan: but does that get talked a lot at the cyber summits or what?

Brad: I haven't been to one. So, I don't know usually what the conversations are, but my guest is there's going to be a lot of sidebars and, you know, under the table, dealings on, Hey, you scratch my back, I'll scratch yours. So, you know, we'll share data between each other. It's probably never written in policy or on paper, but I would like, I know our government for the most part, probably disseminates the knowledge down. I mean, from the FBI standpoint, even students can go become a member of InfraGuard if you pay, I think the $70 and get the background check, and you can see the cybersecurity alerts that the FBI are sending out, you know, on a daily or weekly basis.

Nathan: Yup. I mean, there's a lot of tools nowadays that alert you. I mean, not just for hacking it, but you know, just security in general. Um, I think we're at a good point to wrap it up, I would like to get your, top three takeaways for this episode. If you could.

Brad: Keep that security in your mind as an individual and as an employee is probably the biggest one, you know, implement multifactor authentication on all your really high end sensitive things like your bank accounts and things that actually allow you to have a multifactor authentication. I even have it on my PlayStation for when I log in and then. Again, if you can't do really long passwords, just to think of a passphrase and use a password safe to keep it, you know, more secure.

Nathan: Perfect. Well, again, thank you for joining us today, Brad. You know, we learned a lot. I'm hoping our listeners learned a lot too. We appreciate you joining us for this episode.

Brad: Thanks, man.

Nathan: and then we'll pass this off to Mercy for the news.

Mercy: Hey everyone, Mercy Ayesiza here with the news, a student expert on the information security team, I'll be updating you with whats going on in the cybersecurity world. Before I get into the headlines, please make sure to subscribe to our podcast.

First news update, whatsApp provides another security layer for it's over 2 billion users.

On October 15th, the messenger application, WhatsApp announced that we'll provide end to end encryption for message backups for both its Android and iOS users.

When enabled this encryption protects message backups for its users in their desired storage cloud, like iCloud or Google drive with a choice of their own encryption key.

To activate the security setting, open WhatsApp, go to settings. Chat backup and then end to end encrypted backup.

Our second news update, Acer suffers third cyberware attack. Acer a Taiwanese based hardware company was hit with a third cyber attack before it could recover from each previous blows all your, this year in March, when a different group asked for about $50 million in ransom threat actor group called Desorden, confessed its role in the most recent two attacks.

Our third news update hacker responsible for the attack on university of Pittsburgh medical center finally sentenced to seven years.

The healthcare and insurance provider, University of Pittsburgh Medical Center (UPMC), was hacked in 2014 by threat actor Justin Sean Johnson, who also goes by TheDeathStar or dearthy star on the dark web Johnson is said to have stolen personal information of more than 65,000 employees. Data includes names, social security numbers addresses until their information of tens of thousands of employees. This information was sold on the dark web and used for criminal activity, including 1.7 million infected tax returns.

Aside from this incident, Johnson also stole and told about 90,000 sets of personal information between 2014 and 2017 on the dark web. And that wraps up the news for this week. Thanks for listening to the CyberAware Podcast. We'll see you next time.