Raymond A. Mason
School of Business
WILLIAM & MARY

LEADERSHIP & BUSINESS PODCAST

EPISODE 59: ANDREW LEETH – CYBER ATTACKS & THE ETHICAL HACKER

Ken White

From the College of William & Mary in Williamsburg, Virginia. This is Leadership & Business. The weekly podcast that brings you the latest and best thinking from today's business leaders from across the world. We share the strategies, tactics, and information that can make you a more effective leader, communicator, and professional. I'm your host Ken White. Thanks for listening. Well, one of the biggest, most expensive, and misunderstood threats to business today is the cyber attack. Where an outsider damages a computer network or website, in today's environment businesses and organizations are constantly at risk of being hacked, and those hacks can cause a company to lose its reputation, money, customers, and more due to a major hack that took place just the week before last. People in the U.S. were unable to access sites like PayPal, CNN, and Twitter. Cyber attacks are on the rise, and they're difficult to predict and stop. But businesses are fighting back. In many cases, they're working with ethical hackers professionals who are brought in to penetrate and assess the security of computer and Internet systems. Our guest today has worked with organizations to identify potential weaknesses in their systems. Andrew Leeth is a security engineer for Salesforce. He joins us on the podcast today to discuss what companies and organizations are doing to minimize the chance of a cyber attack. Here's our conversation with Andrew Leeth.

Ken White

Andrew, thank you for taking the time to join us. You're busy. You're a professional and a graduate student, so thanks for taking the time to be with us today. Tell us what you do what's your job all about.

Andrew Leeth

I've got kind of an interesting role and a interesting way that I've got to where I'm at. To give you some background, I'm a currently a security engineer with Salesforce. I've been in that for two going on three years now. So the short explanation is I'm an ethical hacker. So a company brings me in, and I go perform penetration testing. I do reviews of their configurations and their software, and the tools they're using in their networks and systems. And I look for security holes that could be penetrated by an attacker. So we try and simulate real-world attacks against our customers, against our platforms, and you

know, whatever I'm able to accomplish, we go and fix and remediate, and hopefully, if a real bad guy came along and tried the same tactics they would not be able to get in. Before that, though, I was a consultant, and I did a few years of consulting where I would go from client to client, usually in the financial services or maybe healthcare, where there are a lot more regulations around security a lot more protected data. And I would do risk assessments. I would do penetration testing. So I would go in, and I would say these employees are no longer employees with your company. Why are they still having access to your systems? That's certainly a risk that a company would have, and you wouldn't want a fired employee to be able to see medical records or even the technical things like can somebody from the internet get into your database and see your customer data. So we would recreate those testing events for our customers. And there's also what's kind of the fun or spy-like aspect to that, which is social engineering. So we would actually go to our customers who contracted for social engineering, and we would do all sorts of information gathering on employees. We'd come up with a good story to get ourselves in, and we would walk into, say, a big branch and try and get on their networks.

Ken White
Wow.

Andrew Leeth
So you know we'd be going to Goodwill and looking for a Cisco polo and tell them we're here to fix the internet. And, of course, everyone's got slow internet.

Ken White
Sure.

Andrew Leeth
And trustworthy tellers would let you behind the counter and let you plug in.

Ken White
Wow.

Andrew Leeth
So then you could document that and provide that to management and say, you know. Obviously, your training is not working as well. You know that you have to have a letter from this person to let someone else on the machines.

Ken White
Man, we've got to be on guard, personally and professionally, right?

Andrew Leeth
Absolutely.

Ken White
So when you go in a client brings you in. What ordinarily do you find? Are there certain things that you know you're going to come across?

Andrew Leeth
Yeah, there's a lot of common problems that I think a lot of organizations struggle with. Passwords are definitely really, really tough for organizations to get their hands around. It's mostly because it requires the human factor. And we want passwords when we set them to be easy to remember. We don't want to have to change them all the time. We want to make it as easy for us to get our job done. It's just human nature. But that makes it easier for us as an attacker to get into the systems. Simple things like password guessing using passwords that are most frequently used. It's a common problem out there. So you know, if you think that you're setting your password to winter 2016 exclamation point, nobody's going to think of that. Well, that's how the attackers thinking. So that's one of their first guess.

Ken White
Yeah.

Andrew Leeth
So passwords are definitely a huge problem. A lot of times, companies have trouble with detection. So let's say an attack is happening. You would want your IT staff or your security staff to be on guard that, hey, something bad is happening. We need to go fix that, and you can do that through various alerting tools, logging things that are happening, etcetera. But a lot of organizations don't have a really mature process around detection and monitoring.

Ken White
Who is the big case? I mean, from a business standpoint, this affects the bottom line. If this happens, and it does happen, and it will happen, you've got to be ready for this, right?

Andrew Leeth
Absolutely.

Ken White
So what's the case that everybody wants to talk about?

Andrew Leeth
Everyone talks about the big breach. You know when within a company their own culture. Usually, we get brought in when I was a consultant on, you know, hey, we had a breach, and we want to make sure that doesn't happen again. They've felt the pain personally within their company. It had a lot of scrutiny, bad PR attention, and they want to make sure that that doesn't happen again. So they're doing what they can to help protect the money that they've lost. They don't want that to happen again. That's usually a big draw to bring us in. Another issue would be they have some sort of regulatory obligation, and they need some sort of independence. If you're with your own company, you're not going to have a really independent opinion on the state of security at the company. So they need some sort of auditor to come in and say, you know what, they've got these couple issues, but everything looks good to report back that they're compliant with these regulations.

Ken White
I think if we were to ask the average person who does not do what you do, someone like me, you know can you name a company that really was either taken by surprise or took a hit, we think of Target.

Andrew Leeth
Absolutely.

Ken White
What happened? What took place back then?

Andrew Leeth
You know, obviously, Target's got a huge attack surface. They've got lots of different applications, lots of software, lots of servers. They have lots of different stores spread geographically everywhere. So you think they've got a data center somewhere they're interacting with third parties and distributors and suppliers and all these different business connections, and so all this is going somewhere. It's really hard for the IT organization security organization to wrap their hands around all of that and secure every bit of it.

Ken White
Sure.

Andrew Leeth
If we think about Target, they really got in through a third-party supplier portal. It wasn't the e-commerce target.com portal. Their security team knew about that portal, and they secured it really well because they knew that that was extremely important. But this other third-party portal that you know only a few people saw. Nobody thought about it. But it

provided a backdoor right into their system and then their network that hackers were able to go in, and you know, we talked about detection a few minutes ago, the detection Target wasn't maybe as mature as it should be. And so the attackers had time to dump all of their database, including credit card numbers.

Ken White
And so that was one of the things that customers felt they have my credit card. Oh no. Now what. But it really affected the bottom line for Target.

Andrew Leeth
Absolutely. So like you mentioned some of the consequences are reputation and trust. Like, do I really want to go shop at Target because they're losing my credit card, or maybe I should go to the other retailer? We can look at the quarter that that breach happened, and there was a 46 percent drop in revenue that quarter.

Ken White
Wow.

Andrew Leeth
So that's pretty large. And you think of how many credit cards that Target stores. They had 40 million and they believe that one to three million of those credit cards were actually sold on the black market and used. So that's a huge number. You think of other consequences that Target had to go through. They had a hundred million dollars on upgrading their point of sale systems in each of the stores. So that's one of the tasks that they said that will prevent this from happening again because we're going to put in better security. So one of those steps was going to every store and replacing the pin and ship card swipe that you're typically used to using

Ken White
Right.

Andrew Leeth
to make a more secure one. So that cost a lot of money for them. Certainly, they're going to have more regulatory scrutiny. People are going to be looking at them underneath a microscope just to make sure they're doing the right things because they've screwed up. They've got a history of screwing up in the past.

Ken White
Yeah.

Andrew Leeth
Theft could happen if they had some sort of IP, intellectual property. You know, certainly, they've got algorithms around who the marketing and things of value, business secrets, trade secrets.

Ken White
Right.

Andrew Leeth
You know a competitor could get that data. Someone else could use that. That's super impressive and something that they want to keep confidential within the company.

Ken White
Absolutely. It's not like we're picking on Target. This could happen to anyone.

Andrew Leeth
And you know it probably is happening to everyone. They just don't know about it.

Ken White
Wow.

Ken White
We'll continue our discussion with Andrew Leeth, security engineer at Salesforce, in just a minute. Our podcast is brought to you by the Center for Corporate Education at the College of William & Mary's Raymond A. Mason School of Business. The Center for Corporate Education helps companies and organizations from all over the world by creating and delivering business and leadership development programs. If your organization is looking to get to the next level, contact the Center for Corporate Education to discuss how we can create and deliver a program that specifically fits your needs and gets results. For more information, visit our website at wmleadership.com. Now back to our conversation with Andrew Leeth.

Ken White
You had talked about right before we started recording the three pillars.

Andrew Leeth
Yeah, so.

Ken White
Can you tell us about that?

Andrew Leeth
We kind of think of it as a triad or a triangle. So when we think about data security, we think of three main topics per se. So you have confidentiality, and when we think of confidentiality, we really think of keeping data private, and only the individuals who need to see that data should see it. Then we talk about integrity, and integrity is really protecting the data itself and making sure that a bad guy isn't going in and modifying data where it shouldn't be modified. And then we can think of the last bit as availability. So we want to make sure our systems are available and online. A lot of attacks you'll see lately are these denial of service attacks where a hacktivist group will be politically motivated to maybe shut down a website because they don't like something that they've done. And we can think of. I believe it was Bank of America a few years ago where they were increasing some ATM fee, and you know, the collective online didn't really agree that they should be doing this. And so they all sent traffic to Bank of America, which took their site offline. You had a e-commerce portal or something that was generating revenue that would certainly stop that flow of money coming in, and that would be devastating to their business, customers satisfaction. If I want to go check my bank balance, I want to do it when I am at my computer, and I pull up the website, and if it doesn't pull up, I'm going to be a little frustrated.

Ken White
Absolutely. What about vandals? Can you give us some examples because again before we start recording you and I were talking about some instances where vandals take it's not about stealing data? It's not about bringing a business to its knees but vandalizing a website.

Andrew Leeth
Absolutely. And this is kind of the classic example that you can think of from when the web was first started, where you'll have people that get access to your website, and they'll put up maybe some inappropriate images or politically motivated statements or various other things. A good example is Sears. A few years ago, had this vulnerability which allowed in its hacker to change a product on their e-commerce site. And so they changed it into a baby grill. So it appeared as though a Sears was promoting barbecuing of babies right, which is absolutely absurd. But it had people concerned. You know, they didn't know if this was real.

Ken White
Right.

Andrew Leeth
The news picked it up, and you know, obviously, it brought a lot of attention to them and not necessarily in a good light either. So we have a lot of issues when it comes to criminals.

Ken White
And then a lot of time and effort that they had to spend just to fix something that probably more of a joke than it was anything else. Right.

Andrew Leeth
Exactly, exactly.

Ken White
It seems like it could almost never end right from the average consumer. It feels like the who's ahead. People like you or the hackers. Is it an arms race? Is it growing and faster and faster? What's going on?

Andrew Leeth
There's really no finish line.

Ken White
Yeah.

Andrew Leeth
There's no being secure. There's no 100 percent complete. There's always something new. There's always new vulnerabilities in everything we do. There's always somebody smarter thinking on the other side. So really, what the goal is for a security department is you want to make it so difficult for an attacker to go after your site that they're easier targets that they'll just go somewhere else. They'll pivot and go after a different target. So if it's going to take a lot of work, a lot of effort, a lot of time, a lot of resources to attack your company. They're going to go to the other company that's got some low-hanging fruit they can get in pretty easily and still accomplish their goals.

Ken White
Yeah. But it sounds like it's just a ton of fun for you.

Andrew Leeth
It's a lot of fun.

Ken White
Yeah.

Andrew Leeth
It's exciting. There's it's a relatively new field, and it's super primetime. I mean, if you look at the Wall Street Journal on a given day or any news outlet, they're always talking about the latest breach.

Ken White
Yeah.

Andrew Leeth
It's brand new. And I mean, schools don't really have programs around it yet. I mean, there's programs here and there that are brand new. But if you look at the developers or the IT people that are in companies today, they didn't have security classes when they went through their degree programs.

Ken White
So it's new but prevalent at the same time. It's out there.

Andrew Leeth
It's very important.

Ken White
Yeah. One thing we find interesting and it's nice to have you on the podcast. Because of this, you're actually a student at William & Mary. We've got about 60 podcasts. You're the first student we've had on. You're a graduate student in the Masters of Science in Business Analytics.

Andrew Leeth
Excellent.

Ken White
How does that tie into what you're doing, and what's the program all about?

Andrew Leeth
So the program is all about looking at business decisions and how we can make and support those decisions with data. So if we look how users are interacting with your brand or how you're operating and you can somehow glean some statistics and do some analysis, you know the big buzzword these days is machine learning getting some

intelligence behind why customers are working with you. You can make a lot smarter decisions, and you can really have fact behind those decisions.

Ken White
And how do you think this will help what you're doing in terms of your career?

Andrew Leeth
Yeah, so security just as every other part of the business. You know, we have to articulate risk, and we have to quantify that and provide the business justification that they should do security. So there's definitely a lot of metrics and analysis that has to happen that you can educate your executives who probably don't have a lot of security knowledge as to what the bottom line is for them and why they should invest in security and why they should make their systems and networks and protect their data ultimately. So kind of where my interests lie are, you know, providing those metrics to the company based on their vulnerabilities but also being able to detect anomalies and other bad things that are happening. You know, we talked about that detection a little bit earlier. This is where you know Sally logs and to her banking account once a week pretty regularly. But then we see a flurry of activity that doesn't seem like her. That's where data science and analytics can really help identify that fraudulent activity and really help identify that and make our victims' lives better.

Ken White
So no doubt, two of the hottest coolest items out there in business cyber security and business analytics, and you're right at the intersection.

Andrew Leeth
Right at the intersection.

Ken White
That's really cool. Last question for someone in business whether it's a smaller business a major corporation that hasn't given this a whole lot of thought. Where do you even start to protect you, your customers, and your business?

Andrew Leeth
You really got to identify what all's in play because that's, I think, the biggest problem that companies have is they don't know where all their data is. They don't know what systems are using, how people are accessing it. So really, getting an inventory of this is everywhere we store data. This is everything that's important to us. This is what we want to protect. That's an important first step, and the bigger you get, the harder it is to answer that question. You know, if you have a small four-person shop, you know, you can probably ask

around to all four people and figure out where they're storing the important business data. But once you get to many locations and thousands of employees, it gets really hard, especially with the proliferation of cloud. You know everyone's just taking data and storing it wherever or they sign a contract with a third party. So it's really understanding where your data is and the risk that data. So once you get a handle of that you can better articulate what kind of vulnerabilities you could possibly have.

Ken White

Excellent.

Ken White

That's our conversation with Andrew Leeth, and that's our podcast for this week. Leadership & Business is brought to you by the Center for Corporate Education at the College of William & Mary's Raymond A. Mason School of Business. The Center for Corporate Education can help you, and your organization get to the next level with business and leadership development programs that specifically fit your needs. If you're interested in learning more about the opportunities at the Center for Corporate Education for you or your organization, visit our website at wmleadership.com. That's wmleadership.com. Thanks to our guest this week, Andrew Leeth, and thanks to you for joining us. I'm Ken White. Until next time have a safe, happy, and productive week.