More Targeted, Sophisticated Attacks: Where to Pay Attention
Transcript

Part 1: The Evolving Threat and What's Driving It

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and software assurance. Today I'm very pleased to welcome back Marty Lindner, a CERT principal engineer. Marty focuses on threat and incident analysis. And today we'll be discussing how the threat has evolved from Marty's vantage point and how business leaders can protect themselves. And this is an update from the podcast Marty and I did back in 2006. So welcome Marty. It's great to have you with us today.

Marty Lindner: Thanks for having me.

Julia Allen: So to get the ball rolling, from your vantage point, given all the things that you see and the people that you talk to, what are some of the significant cyber security threats that most organizations are facing today — and maybe a little bit about how this is different from, say, a year ago.

Marty Lindner: I'll look at it from two vantage points: one is the social engineering vantage point, and then there's the vantage point of just software flaws and the adversary taking advantage of just poorly written software. I think from a poorly written software point of view, the topology really hasn't changed. If the adversary can find a flaw in software, they will try every means at their disposal to take advantage of that flaw. The best laid plans of any security organization are at risk when those things fail. You can't do anything about that. The layered defense works well but there's always that hole that could be exploited.

The other side that I think has changed over the last year to 18 months is the sophistication of social engineering attacks. It used to be we had spam email where you just wailed out messages to as many people as you could find, enticing them to click on a link or something. But it wasn't targeted. It wasn't directed at you. It wasn't directed at your organization.

And I think what we're seeing now is much more focused, much more targeted attacks where you get a message that's personalized. One of the examples that I like to use is there's lots of organizations out there that like to make their email addresses "marty.lindner@place.com." It makes it very convenient to know what my email address is. But it's also helping the adversary know what someone's email address is supposed to be.

So if they get their hands on a list that says that there's a marty.lindner@place.com, they can now customize an email message that says "Dear Marty," make it all look really pretty. And it raises the bar on their ability to socially engineer somebody. So I think it's going down that lane where we're seeing the bigger problems right now.

Julia Allen: So you say that attacks are becoming more targeted. What do you think, or what do you see, are some of the key motivators?

Marty Lindner: Well, I think the simple answer is it's all about money. I mean there's exceptions to everything but this is all about making more money, becoming more profitable. So if you can target someone to get their Social Security number, their bank account, any kind of information that can then be used to turn it into cash, there's a big win there. So that's easily the motivation.

There's other motivations. There's nation state attacks and things like that. But we'll stay out of that. From a business point of view, it's all about money, intellectual property. There are many things that a company can do to minimize the social engineering attack. And I think they're not taking advantage of it as much as they could. For example, signed email. I've been to several conferences where everyone talks about phishing is just getting out of hand and there's nothing we can do about it.

And the answer is there's a lot you can do about it. If you start enforcing policies that require digitally signed email before you accept it, you've raised the bar, because the adversary cannot forge your signature conveniently. So I think people need to start looking at just changing some policies that help reduce the social engineering attacks.

Julia Allen: Are there some examples that you see of this underground economy where identities and various kinds of information are being sold? Can you say anything about that?

Marty Lindner: Oh yeah, absolutely. I mean everything has a value. So in the underground community, and even from the criminal aspect — actually if you divide it in half, there's the underground community and then there's the criminals. And they're actually, I would think, two different categories. But in the underground community, they're trading credit card numbers for calling card numbers. They're using it. It's like a bartering system.

So everything has a value. If someone has a credit card number and they have more than they need, they're happy to trade the credit card number for the telephone calling card number or the Social Security number or the eBay account or whatever they need to continue their bartering process. So everything has a value.

Julia Allen: And it kind of seems to me that these folks are incredibly well connected. Even more so than those of us who are trying to defend against their actions. How do these folks hook up with each other?

Marty Lindner: There's many ways of hooking up but the most common one is just online. I mean, the chat rooms are notorious for finding people with a common theme and the common theme is bartering or trading to make money. When I was a kid, graffiti was the big thing — you went and you painted on a wall. But now, the younger generation, the way that they get enjoyment is by causing internet mischief.

And in their minds, this is mischief, right? And they're just doing it online.

Part 2: Challenges for Law Enforcement; Dealing with External Suppliers

Julia Allen: So moving to perhaps some actions where we can start to do something about this growing situation, what do you see as the trend in law enforcement's ability to deal with the situation? I am seeing more cases being prosecuted. What are you seeing?

Marty Lindner: They're trying much harder. They're prosecuting more cases. We need a couple things. We need to train the investigators on what to really look for and that's coming along slowly. They're getting smarter at it. We need to get prosecutors who are interested in taking on these harder, more complex cases. The number of drug cases versus the number of cybercrime cases — the drug cases still outweigh the cyber cases by leaps and bounds.

And the simple explanation is it's a lot easier to prosecute a drug case — I caught the guy with the drugs — as it is to prosecute someone on a cyber case because it's so much more complex. And we need to educate the prosecutors on that there's a lot of value and it is doable to prosecute these cyber cases.

Julia Allen: Well, and as you said before, particularly since the cases are involving more and more money, which is a tangible asset, even though it's hard to really figure out exactly what happened where and who did it, the consequences are getting bigger, right?

Marty Lindner: Correct. And I think another interesting part about the law enforcement aspect — most of our law enforcement efforts are designed to be geographically small. And I think this is a big change in the FBI in particular. The FBI had local field offices and their role in life was to deal with bank robberies and banks in their area. The problem now is that the things don't actually happen in their area.

If my identity is stolen or if money's stolen out of my bank account, it didn't happen in Pittsburgh, Pennsylvania. It happened who knows where? And what we need to do is get the law enforcement across jurisdictions and across countries to learn how to communicate better so that they can actually connect all the dots.

Julia Allen: Right. Because the internet doesn't recognize any jurisdiction or any boundary, right?

Marty Lindner: Correct. And in some cases, because there is no jurisdiction, the bad guy can be somewhere. No matter how hard we try — we can identify them by name — we can't do anything about it because there's no reciprocity.

Julia Allen: So what are some of the additional issues that pop up when you're dealing with a global supply chain situation or when an organization is outsourcing maybe key applications or services or pieces of its infrastructure? How does that show up in the threat analysis?

Marty Lindner: All right. Well, it gets interesting. You have to look at why people outsource. And not across the board, but in most cases, people are outsourcing because it's a way to save money. By outsourcing to an organization that has a facility with 7 by 24 operations and all that stuff, you actually reduce your cost. The problem is, what is their security posture relative to your security posture? If they get compromised, what are they going to do to protect your information that is different than how you would protect your own information?

So I think what a company needs to think about when they outsource is are the processes in place at that outsourcing organization so that your information is protected and managed at the same level you would do it if you did it internally? And if you look at some of the more recent credit card oopses and things that have taken place, it really is that company A assumed that company B had the same set of processes in place and in reality, they didn't. It was much lower thresholds and information got stolen, and then the bigger company is the one who had the bigger loss.

Julia Allen: So when you're getting ready to engage with a global supply chain partner, a partner that's in another country, it sounds like the up-front vetting and the due diligence, really working hard on getting the right terms and conditions and service-level agreements — are those ways to help insure you've got adequate protection?

Marty Lindner: Oh, absolutely. And I mean, do the auditing also just to make sure what they say they're doing on paper is what they're actually doing.

Part 3: Mitigating Your Exposure; Trends to Pay Attention to Now

Julia Allen: So what advice do you give people, business leaders, government leaders? What advice do you give them to help, recognizing that they can't totally eliminate their risk and their exposure, but to better mitigate it?

Marty Lindner: Well, I think there's a couple things. From a pure, just want to think about the social engineering aspects, there's two sides of that. One is training and education. Your employees need to understand the threat. And clearly they cannot understand the threat as well as the security professional does. But you have to keep reminding everyone that you're taking a risk every time you click on a link. So training goes a long way.

But like I said earlier, I think there are some technology solutions that we need to start looking at to raise the bar. I'm a big fan of signed email and encrypted email. For this discussion, it's really the signed email. If you at your gateway can stop email that isn't digitally signed properly, a lot of this social engineering phishing attacks will just go away because your employees will never see email that is fraudulent. I mean again, that's not perfect but you can raise the bar immensely.

And I think the other thing on the social engineering aspect of it is there's lots of companies that publish, open to the world, their policies, procedures, their forms, and their templates. And what we're seeing is the adversary downloads these forms, these templates, and now they know what these fraudulent documents are supposed to look like. So short of being able to digitally sign them or do something to prove they're authentic, you should also think about not exposing them so people can steal them and then use them to launch a social engineering attack.

Julia Allen: That's pretty interesting. I hadn't thought about the fact that a lot of organizations these days, in the interest of being more transparent are, as you said — policies, procedures, maybe some of their own standards and guidelines — to make it evident to both their customers and their employees how they're protecting information. But that can be turned against you.

Marty Lindner: And with being non-attributional here, there was a set of events where an organization actually advertised what an application for an account on their system looked like. And at the bottom, it required a signature. So they got the application. In another part of the same situation, they had an example of something that this company was doing and it included a pdf with a person's signature. So what the adversary did was took the template for the other form, the signature off of the example, put the two together, submitted it, and it worked perfectly.

Julia Allen: Boy, it does give you pause for thought, doesn't it?

Marty Lindner: Yes. So I mean, and it happened. So that's where you've got to be careful. The adversary is just — social engineering is the way to do it.

Julia Allen: So as part of preparing for or extending our preparation to mitigate against these kinds of risks, what do you see are some of the effective key roles and team structures that should be in place, ready to go when something happens?

Marty Lindner: Well yes, you definitely have to plan and have a response process in place. There's many organizations that when they get compromised, it becomes a fire drill. And the fire drill is who do I need to get involved and all that kind of stuff. I think a good organization should have a response plan in place. All the people that need to be involved are identified in advance so when the compromise occurs, you just go and play your role.

I think the best example is the NTSB (National Transportation Safety Board). When a plane crashes, there's a whole crew of people, the fly-away team. They go out and they each have their jobs and they go do it. A good organization will have an incident

response team. There's someone responsible for forensics. There's someone for talking about PR. There's someone talking to law enforcement. All the different components of an incident response process — they should have that in place, ready to go, and just execute it.

Julia Allen: Have you seen organizations that you think have really good incident response capability? Do they tend to go through exercises and red team and other types of —

Marty Lindner: Absolutely.

Julia Allen: pseudo-attack situations?

Marty Lindner: Absolutely. Yes. I mean, if you don't practice, you don't know what to do. Again, without being attributional to companies, there's two or three companies out there that spend quite a bit in energy just practicing. Because if something happens in the real world to their company, it's their reputation.

Julia Allen: Sure. Well, as we wrap up our conversation, how about using your crystal ball? What do you see down the road in terms of future threat and attack trends? Anything new shaping up on the horizon?

Marty Lindner: I think we're seeing a little bit of it now. And it really is, there's newer technology coming out every day. Two years ago, did anyone ever think there would be an iPhone and all the neat, cool things you can do with an iPhone? But think about it. All an iPhone is, and I'm just using that as an example, is another place to store information. And if you go look, there's more and more applications that allow you to download user name and password protection tools on a phone.

So it used to be we told people "don't write down your user name and passwords." We told them to protect them on the computer safely. Now we're storing them on our phones. Just think about all the social engineering aspects, the software flaws, and the other things that now you go after the phone. You don't go after the desktop.

So the corporation who's spending all their energy securing their desktop now needs to start securing all of those little gadgets — the iPods, the iPhones, the BlackBerries. All those things are now in play because they all contain information. And that's what I would be thinking about next.

Julia Allen: What about all the social networking sites – the Facebooks and the MySpace, Twitter? Anything percolating there?

Marty Lindner: Well, so YouTube is becoming the poster child for putting out videos of things for people to watch. That's kind of cool but you have to remember that every video that's out there potentially contains malware, right, which can cause you harm. The social engineering sites, the social networking sites — I shouldn't call them the social engineering sites — the social networking sites.

Julia Allen: Although they probably could turn into that, right?

Marty Lindner: Well, that's what they're turning into. They are — that's where a lot of information is being divulged. There's a whole bunch of things, and I don't want to be attributional here, but I think one is like — LinkedIn can kind of be scary because you're advertising a lot of information about your professional career which can now be used against you in a social engineering attack.

And when you start looking at who you're linked with and all that kind of stuff, now you're building this social network of who else you can send messages on behalf of where you'll think they're authentic. So all this stuff where you divulge things about yourself is really dangerous.

And then I think the last thing that is really out there but you've got to start paying attention to is Second Life, the whole Second Life world. Think about that. That's another economy. And people are out there now bartering and selling stuff. There are commercial companies out there that are recruiting off of Second Life.

Julia Allen: Yes, we did a podcast earlier on the subject of virtual communities. And it looks like there is substantial money to be made, both legitimately, and what I hear you say, illegitimately in those environments.

Marty Lindner: Absolutely. Yes. And you've got to start — that to me is really freaky to think about. But it's real.

Julia Allen: Do you think training, awareness raising, not necessarily using the fear, uncertainty, and doubt factor? But how do you — particularly in a business setting because folks are going to go out and visit these sites just in the normal course of business — how do you reach, how do business leaders reach their staff and employees to make sure they're doing their own due diligence?

Marty Lindner: Yes, I mean that's the hard one. That's a hard one. I don't know if I have a good answer to that. But the one thing that I could suggest or recommend, and I think some entities are thinking about it is, we have learned to become accustomed to using the internet for just about everything. And most organizations are not against their employees spending some amount of their day doing, quote, "non-business work, nonofficial work." And that's becoming acceptable.

The problem is that the bigger risk is in that small window where they're doing their nonofficial business of going to eBay at lunchtime or something like that. So I think what some companies are actually doing now is building two networks. And there's a cost to this but they're doing it. They're building the network for business use and they're building the network for sort of not-so-much business use. And they're putting the rules on their business network that are very rigid, right? They're only doing business-related work on that network. It has an expense to it but it takes the risk away.

Julia Allen: Right, because they're basically accepting the fact that folks are going to do this anyway. And so recognizing that they need to invest, particularly with the younger generation.

Marty Lindner: Absolutely.

Julia Allen: These folks come in and they expect to have access to these kinds of resources. And so you just have to plan for it, right?

Marty Lindner: Yes, absolutely.

Julia Allen: Well listen, I really do appreciate your taking the time to give our listeners an update from all of your travels and the various communities that you are involved in. So thanks very much for your time.

Marty Lindner: You're welcome.