Proactive Remedies for Rising Threats
Transcript

Part 1: The Evolving Threat

Stephanie Losi: Welcome to the CERT Executive Podcast Series. 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. Before we begin, I'd like to let you know that show notes and other supporting materials for today's conversation are available at the podcast website. Please take a few minutes to look them over. My name is Stephanie Losi. I am a journalist and graduate student at Carnegie Mellon working with the CERT program.

Julia Allen: And I'm Julia Allen, also a senior researcher at CERT in security governance and executive outreach.

Stephanie Losi: Today we're pleased to introduce Marty Lindner, a senior researcher at CERT and a recognized expert on Internet-based threats and trends. We'll be discussing how these threats are evolving and how organizations can protect themselves. So Marty, let's start, let's jump right in: What is the biggest threat faced by business leaders right now, and how is this different from a year ago?

Marty Lindner: Well I think a couple of things have changed in recent history, is that the motivated adversary, the bad guy, has learned that they can make money by using the internet as a tool for causing pain to businesses and to individuals. So you can be on the Internet as a business and you can be DDoSed as an attack –

Julia Allen: You mean like Distributed Denial of Service, right?

Marty Lindner: Distributed denial of service, right. And there's extortions going on where you will be threatened, you know, if you don't pay money we will take you off the air, make your website unavailable.

Julia Allen: So, Marty, so this financial gain aspect is something fairly recent?

Marty Lindner: Yeah, it's becoming more and more popular, it was around for a while but only a couple of people realized they could make money, but I think now just everyone realizes that you can make a lot of money. If you go back to 2001 when Code Red hit and things like that, people did that because they could, and they bragged about it.

Julia Allen: So it was more just for fame in their community or their fifteen minutes of recognition?

Marty Lindner: Right. They never told anybody, but they still bragged in their own circles, and that was a cool thing. But now people realize that if they keep their mouth shut about how they do it and go do it, they can profit from it and make lots of money.

Julia Allen: Okay, so it's much more behind the scenes.

Marty Lindner: Much more behind the scenes.

Stephanie Losi: And when would you say that shift really happened, I mean do you think there was some sort of catalyst or was it a gradual thing over time, and when did you really start to see it emerge?

Marty Lindner: A couple of years ago -- I mean probably two, three years ago -- is when it really started shifting. The last worm that we saw that was probably done because you could was probably Blaster, and if you think about it we've had a couple of worms since Blaster but not like we used to before Blaster. Before Blaster you could do it and -- bragging rights. Now people realize if you have a tool that's going to cause pain, target an individual or an organization, make some money doing it, and keep on going.

Julia Allen: maybe you'd be willing to talk about Zero Day Vulnerability and what we should do to take that into account.

Marty Lindner: Yeah, so a Zero Day Vulnerability is a flaw in software that in theory the good guys -- the software manufacturers, the anti-virus companies -- don't know anything about. The bad guys like it because in theory they can write a piece of malware that can get into a computer because of the Zero Day, right.

Julia Allen: But how do they find out about it?

Marty Lindner: Reverse engineering of products. I mean, we all have to understand that there are people out there that are scrutinizing Linuxes, Windows, Mac OS, take your pick, trying to find flaws in the product, and when they find the flaw that no one knows about, they've got their Zero Day. Step two of it is to take that Zero Day and create a piece of malware that is, quote, "profitable" to them.

Julia Allen: That'll take advantage of that vulnerability.

Marty Lindner: Right, however that could be profitable to them, right, and at that point they either use it, they sell it to their friends and neighbors to use it, and there's a lot of money being made not actually using the exploit --

Julia Allen: But threatening to use it, right?

Marty Lindner: Well, threatening it or selling it to someone else who might want to use it and, you know, depending on what country you're in and what the laws are, it's not illegal to write the bad software, it's illegal to use it. So there's a lot of people out there that are writing it but don't want to get in trouble so they sell it in the underground market to someone else who wants to use it.

Julia Allen: You know, you speak of that underground market. Why does it seem like the intruder community, or the hacker community, is so well connected, and those that are trying to protect our networks against that attack always seem to be playing catch-up? Do you have an opinion about that?

Marty Lindner: I'm not sure I have a good opinion, but clearly the cost models are backwards, right? The bad guys don't need a whole lot to generate the badness. I mean, they can do it from a desktop computer, and after they have their desktop computer, what are they using? They're using our computers, other businesses' and other home users' computers, for computing horsepower to continue their badness and to extort people and to steal data. So all they need is a little computer.

Julia Allen: Yeah, it kind of reminds me -- not to say that they're equivalent -- but it kind of reminds me of some of the issues we have with terrorism. There are so many points of entry, there's so much to be protected, and yet it only takes one person coming through one entry point to create a huge disaster.

Marty Lindner: Right, and if you take the -- and, you know, in the physical side when you talk about terrorism it's a physical thing, you have to get around our borders. The Internet has no borders, unlike dropping a bomb or something, you have to be local, to cause a cyber attack you can be anywhere on the globe.

Stephanie Losi: Right, and this is I guess where the global aspect comes in, in terms of, you know, the laws are different in every country, and I imagine that causes a whole lot of problems in terms of figuring out even what is a threat, and --

Marty Lindner: Yeah, and the other one is that there's no fear on the bad guys' side because they know that there is no prosecution if they do something bad because there's no way to get to them.

Stephanie Losi: Right, the country that they're in may not even deem this to be an illegal threat.

Marty Lindner: Right, and even if you take the U.S., for example, if the U.S. looks at it as a crime, that doesn't mean that we have the legal relationship with the other country so that they can actually go do something about it. There are many cases where we know where the bad guys are located, we know who they are, but for legal reasons there is no way to go get them.

Part 2: Redundancy and Diversity

Julia Allen: So are there some things that organizations can do -- I mean, granted there are certain types of attacks that are difficult to respond to or protect yourself against -- but in the face of these financially motivated attacks, what kinds of actions should organizations be taking or thinking about taking?

Marty Lindner: Well, I think there's a couple of things, one, you know, there's redundancy and diversity, and redundancy says you have more than one of everything, diversity says you have more than one of everything but they're actually different. I think if you can do some redundancy and some diversity where you distribute your infrastructure not in one building but globally spread it out, then the motivated attacker to really win the battle has to think harder about what part of your organization they're going to target.

Julia Allen: Right, not by surprise?

Marty Lindner: Assume that it's going to happen, right, and decide ahead of time how you're going to respond to it. You know, you can take the weekend off, come back on Monday and when you haven't paid money they're probably going to stop, right?

Stephanie Losi: Right, but what are some of the most cost effective things, do you think, that executives can do to sort of mitigate against this risk?

Marty Lindner: Distributing your workload I still think is the biggest way to defend yourself, and the other one is to do the risk analysis to really understand in advance what it means to your business so that if it does happen, you're prepared. I don't know if that's really a cost effective thing, but you still need to do it so you know.

Julia Allen: So how can business leaders stay up-to-date, there is just -- we're all being inundated with all kinds of advisories and vulnerability reports and Patch Tuesday and, you know, you name it, how does someone stay on top of the issues that they really should be paying attention to?

Marty Lindner: That's hard, but I will break it down to there's probably three issues that if you focus on the three issues -- I'll list them in a second -- you're probably going to do okay. Number one is the fact that a DDoS can occur, and just think about in advance: That's going to happen, what are you going to do about it?

Julia Allen: So it almost becomes like a business continuity disaster recovery type of planning activity?

Marty Lindner: Right, correct. The second one is to assume that not all your employees and contractors are trustworthy, and that there is going to be an attack from the inside.

Julia Allen: Okay, so making sure you're prepared for that?

Marty Lindner: Right, and all the best practice to go along with that. But lastly is, as you said with Patch Tuesday and all these other patches, patching poor software is a problem, so you have to be diligent and have a whole crew that's just paying attention to the infrastructure you have and reading about all the vulnerabilities and best practices with the product set that you operate, and this is sort of backwards, I think. I'm a fan of diversity, which says that if you have two of something you're better off than one, and they're different.

Julia Allen: Right, two different things, right.

Marty Lindner: Two different things, but that requires you--

Julia Allen: So make it, in other words, run Windows one place, run Linux or other variations another place?

Marty Lindner: Linux another place, but that doubles the amount of manpower and expertise you need.

Julia Allen: Right, right, so that becomes a risk trade-off, right?

Marty Lindner: Right, on the other side you can say, “Okay, I'm only going to run Windows, I'm only going to run Linux,” -- pick one. That reduces the manpower you need to pay attention to what's going on, but now you have a different risk -- that any one single product failure will do you in -- so you have to do your whole trade-off analysis as to which way you want to go, and depending on what it is, you make the business decision.

Julia Allen: So have you seen organizations be relatively successful with both strategies -- a diverse strategy versus a "pick one because I only want to have to deal with one platform or one operating system" strategy?

Marty Lindner: Yeah, I know firsthand of several organizations that have the diversity strategy, and they're paying a lot of money for it, but it works.

Julia Allen: I mean, but they're experiencing fewer successful attacks or incidents?

Marty Lindner: Well, I don't know if I can say they're experiencing fewer, because in both cases, if you have two systems and you're running the best practices, you're still going to be targeted. The question is your defenses are higher.

Julia Allen: And maybe your recovery is shorter.

Marty Lindner: And your recovery time is shorter.

Stephanie Losi: Right, and when it happens you still have a backup system for example that wasn't affected, because it wasn't targeted toward that system?

Marty Lindner: Right, so, you know, you said Microsoft Patch Tuesday, so if you have a diverse system and you know that Microsoft Patch Tuesday is coming up, you know, you have the advantage of the diverse system if you're running Windows and something else, that you know it's safe to take down or pay attention to your Windows box to patch it, because your other environment's up and running. Right? If your entire environment was, say, just Windows or just Linux, and a major patch came out for that environment --

Julia Allen: That affects your whole network.

Marty Lindner: It affects your whole network, and it becomes complicated on what you do about it. You know, the backbone providers, the ISPs, are quite forthcoming with the fact that if they have to do an upgrade to their equipment it takes months, right, because they have so much of it and for the most part it's all the same, because it's a cost effective thing for them to do. So before they put anything out they really scrutinize it and test it, and then they start deploying it. It takes months. No matter how bad the problem could be, it takes months.

Julia Allen: So, I mean, you have to do the analysis and the testing and the examination in advance before you actually install the patch.

Marty Lindner: Correct, and I'll give you another argument just to make you think about it. The automated patch distribution is a cool thing for making your labor costs lower, right? But I would argue it gives you a new risk, because if that system works as well as it's supposed to --

Julia Allen: <laughs> It can roll out all kinds of unintended things.

Stephanie Losi: Right, some of them come from outside.

Marty Lindner: Very well, a lot of bad stuff.

Julia Allen: So you get back to your insider threat.

Marty Lindner: Right, insider threat is one, right, but yeah, all those things play into it. So even if you like the patch management solutions that push it all out at once, I wouldn't take my entire organization and put it under one umbrella, right? I'd have a little diversity there so that you can't take out your entire network with one click of a mouse.

Stephanie Losi: Right.

Marty Lindner: Which has happened -- I mean, we've seen numerous occasions where they did the test on the one box and it was fine, so okay, it must be good on all of them, and you click--

Julia Allen: And they're in big trouble.

Marty Lindner: And that one was subtly different than all the rest and you're in trouble. So there's a reason for that, sorry.

Part 3: Other Strategies and Conclusion

Stephanie Losi: No problem. Do you think that the overall security situation will improve or get worse in the future, and I guess what are some trends that you see? I mean, you talked about diversity and redundancy. Do you see organizations moving towards spending more money on diversity, or do you see sort of a balance happening, or are people actually moving away from spending?

Julia Allen: Or maybe even more outsourcing of IT and security services, at least that part of the problem?

Marty Lindner: Yeah, my view is a little skewed, so I don't get to see as broad a range of companies as others do, but outsourcing clearly is a popular trend. I can't really speak to how many people are doing the diversity versus the single path, I just don't know in the big spectrum. The small number of companies I pay attention to I'd say is a 50-50 mix, right. But outsourcing is very popular.

Julia Allen: Well, just, you know, there's a lot to pay attention to, I mean you've mentioned a lot of different issues, risks, concerns, trade-offs… how is, in your opinion, how is any business leader, that's trying to run an organization, let alone think about the security of their network and what might happen, how can they stay on top of this issue or be appropriately educated and know what risks and trade-offs to pay attention to and maybe which ones to delegate? Do you have any thoughts about that? It's just it seems like such a thorny issue.

Marty Lindner: I think it is. I guess the best way to approach it in my opinion is, if you're really running a business, sit down and understand what services you really need to be offering to keep your business up and running, and make sure that that small subset of services is one isolated from anything else you might want to be experimenting with, right? And maintain at the highest level possible, paying attention to patches, best practices, proper training, all that kind of stuff. Make sure your core business works. Sure, go off and experiment with new technologies, but don't test those new technologies on the infrastructure that is your core business, that way if you ever have a flaw, you can turn off those experiments and your core business is still sound.

Julia Allen: So you're saying to identify those services and the networks that support them and the people that support them as a critical asset?

Marty Lindner: Correct, right.

Julia Allen: And then make sure you put the proper resources and attention on protecting that asset.

Marty Lindner: Yeah, it has number one priority, so, and all businesses run mail, right? I don't know how many places have the mail and the web server and a bunch of other things all on one computer, one server. At that point, if an attacker gets into that box, all your infrastructure is dead, right, it's all gone. If you care about your infrastructure, run mail on one system, run the web server on another system, high level of diligence on best practices, but if one of them gets taken out, the other service is still available for use. And a lot of people don't do that, you know, it's cheaper to buy this really, really big --

Julia Allen: One server, right --

Marty Lindner: Mega computer that does everything, it is your single point of failure both from software quality, from an attacker point of view, from a hardware failure … Buy a bunch of little ones, it's better.

Stephanie Losi: So I hear you talking a lot about separation, you know, separation of services, and also separation of a test network from a production network.

Marty Lindner: Oh yes.

Stephanie Losi: Are there any kinds of defense mechanisms that you think people really should be looking into on their test network to sort of defend against some new threats? I mean, what should people be experimenting with on their test network to ensure that really when something happens they are prepared to respond?

Marty Lindner: I think the bigger defense that people should pay attention to is people buy firewalls, and for the most part people look at a firewall as a device that keeps the bad guy out.

Julia Allen: Right, protect the perimeter, right?

Marty Lindner: Protect the perimeter. The firewall can do a lot more than that, and if you look at a firewall, there is two ways a firewall can operate. It's in a mode that denies things that you know are bad, or it permits things that you know are good, those are the two choices. Most firewalls out there today deny things that are bad, so it's assumed that everything is good, and then when you see something bad, you configure it to block it. I don't like that model. I like the model where you assume everything is bad--

Julia Allen: So basically deny everything?

Marty Lindner: Deny everything, right.

Julia Allen: And then permit.

Marty Lindner: And permit those things you know are good, but more importantly it's not just permit those things coming in that are good, also only permit things that you know that are good to go out.

Julia Allen: So, but sometimes that's called both ingress and egress filtering.

Marty Lindner: Egress, right, and the reason that's, if you take that model for the flash worm, because the thing about a flash worm is it infects the computer and then it starts looking for more people to go infect on the outside. If you have those rules in place, that worm, even though it got on your computer, could not go scanning for more computers because your firewall would not let it, right.

Julia Allen: Right, in other words the firewall would block it from someone on the inside sending it out inadvertently, or intentionally.

Marty Lindner: And then the other big thing, you know, if you talk about corporate espionage, which seems to be a big popular thing nowadays too, it's the exfiltration of data -- taking data from a corporate network and giving it to somebody else. Well, if you have your firewall rules and things in place and you only have authorized connections, the data can't easily leave -- not to say it's not impossible, but you can't just open up an FTP connection and dump it to the bad guy. That just won't work.

Stephanie Losi: Right, so and it seems, you know, firewall rule configuration would be one of those ideal things that would require a lot of testing on the test network I would imagine.

Marty Lindner: Correct, and also, if you do it right, you write the security policy that says this is what you're allowed to do, and then take that policy and apply it to the firewall, and you'll have all your positive rules as opposed to your negative rules.

Stephanie Losi: Got it. Okay, so what advice would you give executives, just to sort of wrap up and sum up everything we've talked about, how can they best protect themselves, and what advice would you give them regarding the threats that are out there today?

Marty Lindner: Well I think the best way to defend yourself is to, you know, identify what your key assets are, right, spend time and money on making sure that those key infrastructure pieces that keep your business running are protected at the highest level possible, step number one. And then step number two is to pay attention to mailing lists and other newsgroups -- to the broader picture of internet security and understanding what's going on there.

Julia Allen: Right, I know there are a lot of market sector-specific groups, financial services sector groups and other trade associations that help particular market sectors pay attention.

Marty Lindner: Right, there's ISACs -- just pay attention to those trade associations and try to keep up. It's an impossible task, I mean, this is my job and there's so many things I know I don’t know anything about.

Stephanie Losi: Well, you’ve helped us a lot, thank you very much, we really appreciate your time.

Marty Lindner: You're welcome.

Julia Allen: Yeah Marty, it's been great, I hope we get a chance to talk again.