Inside Defense-in-Depth
Transcript

Part 1: Defining Defense-in-Depth; Getting Started

Stephanie Losi: Welcome to the CERT 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.

I'm Stephanie Losi, a journalist and graduate student at Carnegie Mellon, and I'm also working at CERT on security, governance, and executive outreach. I'm pleased to introduce Kristopher Rush, a member of the technical staff at CERT, whose focus is on Defense-in-Depth. We'll be discussing the Defense-in-Depth Foundations for Secure and Resilient IT Enterprises, a curriculum that Kristopher played an essential role in developing, and which was recently posted on the CERT website.

Okay, Kris, let's just jump in here, and to start out, I want to ask you what is Defense-in-Depth, and how does it really fit into an enterprise or IT security program?

Kristopher Rush: That's a really good question. Like you mentioned, the curriculum that we just published on the CERT website was really aimed at addressing Defense-in-Depth from kind of a different point of view. Throughout the security world, people a lot of times will talk about Defense-in-Depth, but it's not really explained, and there's no really good way to look at something like a model and determine if you've really achieved it.

So what it is, just in definition, it's multiple controls that are related, addressing different security concerns in an organization. So one instance would be, you know, you've got firewalls to protect you from malicious traffic, but you've also got anti-virus software in case malicious traffic reaches your network. So it's just a layered approach at addressing information security and information insurance, such that if one layer fails, you've got other layers in place to kind of make sure your network is sustainable in the face of attacks and failures.

Stephanie Losi: Okay, and what are the layers? I mean, could you give me sort of a brief overview of that, and touch on some of them?

Kristopher Rush: I could. Defense-in-Depth, as far as I can tell, up to this point, has really just been, you know, one kind of concept, and what we've really done is, we've broken it down into eight different conceptual containers, and what this does is, it really enables an organization, instead of looking at security just to say, "Do we have it?" and trying to measure up what implementations they have, and where they need to be, and what's required, it gave them a framework of these eight containers to look at each one individually, and kind of compare what they have, and determine if they've got the right things in place.

So what the containers actually are: We started with compliance management, and I won't go into a lot of detail with these, because the material's online, and you can look at it, but you've got compliance management, then we move on to risk management, identity management, authorization management, accountability, availability, configuration management, and then incident response, or incident management.

Stephanie Losi: So you've got all these different areas, and you can take a look at, sort of, before you implement Defense-in-Depth, "Where do I stand?" and then you can implement it, and take a look after: "Where do I stand?" And you can sort of make it some sort of iterative process.

Kristopher Rush: Exactly. I mean, it's really not something that should be addressed kind of wholesale, you know, take them all and throw them at your IT staff, and hope that you get something out of it. One of the things that we emphasize is that Defense-in-Depth should really be ingrained in your organizational culture. It's not something that you hand to one person, and hope that it's achieved or it's accomplished.

When you look at something like compliance management, which is really one of the founding concepts of Defense-in-Depth, that's where you really establish your organizational policy, your IA policy that's going to be sort of general, yet specific enough to provide guidance to your IA staff, or your information security, or just even your sysadmin kind of people, and then even be useful to your users as far as how they're expected to conduct themselves in your infrastructure.

Stephanie Losi: Okay, so I'm hearing you say that there are sort of different perspectives on Defense-in-Depth, depending on who you are within the organization. You could be a sysadmin, you could be a user. How about a mid- to senior-level manager? If you're in this role, what can Defense-in-Depth do for you? How would you view it, and also how would you view its pros and cons if you were considering implementing it?

Kristopher Rush: That's a really good question. Any time that you can be provided with some sort of framework or guideline, I think that it's beneficial, as long as you kind of buy into what the framework is leading you towards, and so for a mid- to senior-level manager, what this is providing is, like I said, the framework to kind of move forward, because a lot of times you've got C-level executives, or even mid-level managers that don't really have a lot of the technical experience, or they may be familiar with it, but they've been more in the managerial role for quite a long time.

Stephanie Losi: Right.

Kristopher Rush: So what it does is it provides the framework. I like to think of it, it's kind of a constant in a field where there's really no constant. Security's always changing, the technology's always changing, the regulatory environment's always changing, but with DID, or Defense-in-Depth, you've always got this kind of framework to map it against, and determine, you know, where it fits in your organization, and look at the different controls, and see if you're where you need to be.

Stephanie Losi: So we discussed these layers, and we discussed looking at it and trying to figure out where you're supposed to be. Where would you start?

Kristopher Rush: It kind of all starts with compliance management. You can't really implement any sort of security unless you've got a reason for having security, unless you've got some sort of idea or concept of what it is you want secure, and with Defense-in-Depth, this really, it's tied to your organizational goals, so IT security or information assurance is not some other separate concept. It's something that really works alongside the objectives of your organization.

Stephanie Losi: Right, the business mission.

Kristopher Rush: Exactly. I mean, that's really what it's all about, is providing continuity of business in the face of threats and failures, so you start with compliance management, or developing a policy, what is it that your goals are in a general enough manner that you don't have

to change your policy all the time, but you've got this document that states what it is you're seeking to achieve, and then you kind of move towards risk management.

So once you've got this overarching goal, as far as IA policy goes, then you move towards risk management, and what that really involves is, number one, it's identifying the critical assets in your organization, because if you've got a business mission, there are of course some sort of assets within your organization that are targeted directly at accomplishing that mission, so once you define the critical assets, you can then determine what the loss to your business might be if those assets were not available. So as part of risk management, you identify your assets, and then you look at the threats that exist in regard to those assets, and then you can determine how important it really is, and what the security requirements are for those assets.

So in compliance management and risk management, you've really got these two key containers, or concepts, of Defense-in-Depth that set everything else up.

Stephanie Losi: Okay, so we're going way beyond the thought process of, "Oh, security is, you know, say, these mechanisms. It's a firewall." And you're kind of taking a big step back, and you're looking at the whole organization, and saying, "Well, security is a concept, and a goal that we have, and so here's how we want to implement it, and these are the assets that we need to protect, so now what do we need to do on the mechanism, low level, to do that?"

Kristopher Rush: Exactly.

Stephanie Losi: Okay, thank you. That makes a lot of sense.

Part 2: Obtaining Buy-In

Stephanie Losi: I do have a question about who should be the point person for a Defense-in-Depth strategy. You know, at what level of the organization should this operate, because it seems to be a big-picture initiative, so it would strike me that it should be some sort of top-level, senior person, as opposed to, you know, a system administrator who might have been tasked with security. Is that accurate?

Kristopher Rush: Sure. Well, I mean, Defense-in-Depth is not really for one specific type of organization, so to say that it's always for your C-level executive, or the main VP of information assurance or IT, that's nice, but in smaller organizations I guess you can't really always expect that there's a CIO or a CISO.

So given that DiD really does rely on sort of an organizational buy-in, and that needs to be driven from the management level in order to be kind of ingrained throughout the organizational culture, it would be best if it was a CIO or a CISO who was kind of the leading person of this initiative, that made it known that this is where we're going to go with our information assurance, and these are the concepts that we're going to be using.

And also, going further, because these are the people that have really the control of putting that into the organizational culture, making sure that there's user awareness -- and also I think it's great that, if there is an organization with a CISO, they can kind of be the bridge between, say, your other C-level executives that aren't real technology oriented or minded, and the staff who are the ones actually implementing this, so that there's kind of a flow through the organization, and everybody at least can be on the same page.

Stephanie Losi: This leads to another thought: How do you get buy-in for Defense-in-Depth? How do you, you know, whatever position you're in, in the organization, if you come in and you want to implement Defense-in-Depth, how do you get buy-in, both above and below your level?

Kristopher Rush: I wish I had a real short answer for that, but I don't think that there really is one. I think one of the keys to information assurance is that a lot of organizations operate in some sort of regulatory environment. You've got Sarbanes-Oxley and various other regulatory mechanisms that many companies are having to look at and become compliant with, so I think that the fact that they're faced with some external force to look at information assurance is one sort of mechanism to achieve buy-in, because once they determine that it has to be done, or there's consequences, it's kind of buy-in by default.

The other thing is just user education. It's just kind of, you know, you don't make them sign a policy document at their hiring, and then expect them to have security in mind all the time. You've got to kind of, you know, make sure that it's ingrained in corporate events, or have separate events, educating your employees, or maybe publications, but I think you really do achieve that buy-in, just in the fact that it addresses it in a framework that can actually be looked at and kind of measured, not specifically, but you can determine if you're meeting at least the general requirements of the framework, so I think that goes a long way toward achieving some buy-in from the employees and the management.

Stephanie Losi: Right, and then so instead of scrambling to comply, you're approaching it in a structured way, and you're hoping that this will have larger benefits throughout the organization.

Kristopher Rush: Exactly, and through the compliance management step, where you're really tying it to the organizational mission, I mean, I think that goes a long way towards making it real to people, as far as understanding that it's not just a hindrance to employees, or to the management. Because once they know that it's really there to support their job in the organizational mission, I think more people are willing to accept a lot of the IA implementations.

Part 3: A Continuous Process

Stephanie Losi: How will you know when you've achieved Defense-in-Depth? You've set out to implement the program, you're looking at the framework, and you have a goal of where you want to get to. How do you determine that goal, how do you say, "Well, this is the right level for my organization?" And then how do you say, "Well, okay, we've achieved that level?" How do you measure that?

Kristopher Rush: That's a really good question, and I think a lot of people ask that in any sort of security framework, or just security in general. It's, "How much is enough?" and, "Do I have it? Am I secure?"

Well, unfortunately, it's not like a black or white thing. You can't really perform some technical implementation and sit back and say, "I'm secure." It's like implementing a firewall and never touching it again, and hoping that it's just going to keep you safe from the rest of the world.

Stephanie Losi: Right, no matter what else happens from then on.

Kristopher Rush: Yeah, I mean, a lot of people think of security, especially a lot of times from a management level, as sort of a fix-it-and-forget-it. You know, "We've put this initial amount of funding into security, we had our staff do all these things, and why would we want to do more?"

The Defense-in-Depth model -- it really requires a commitment by the organization, an ongoing commitment. Not just an initial commitment to look at it as a framework, and try to match up the things you have in your organization to the framework, and put it in place, and there it is. A lot of it really involves ongoing maintenance or monitoring of your infrastructure, and of your security mechanisms, so rather than think of it like, you know, you've achieved security and now it's good, I like to sort of look at it in a different manner. You're looking at it as, have you implemented or have you followed the framework the best you can, with the resources you have? And then you have to look at it from the risk management perspective. Given the things that you have in place, have you achieved or do you think that you've achieved the level of risk management that you require for those assets?

And one thing about Defense-in-Depth is it involves a lot of monitoring and constant maintenance, like I said. You've got accountability management, which is one of the constructs, which involves looking at monitoring of logs, of access logs, of traffic logs, these sort of things. The staff that you have in place to implement your Defense-in-Depth implementations can look at these things to determine, you know, does the security that you want -- does it kind of match up with what you're seeing in your logs, and your traffic? Do you have people trying to access things that they shouldn't be? It requires kind of a lot of legwork.

Stephanie Losi: So it's a living concept, is what you're saying.

Kristopher Rush: It is.

Stephanie Losi: Now, you mentioned that the curriculum's available on the website. Who would you say is the target audience for the curriculum, and how can that then be used within an organization to familiarize people at different levels with what's required of them?

Kristopher Rush: Well, I'm glad you brought that up, because one of our aims with the curriculum was to kind of -- a lot of times there's a gap between your technical staff, and then the managerial level. For the managerial or the executive -- the C-level executive who has been in the managerial role for a long time -- they may not be that tied to the technical stuff, or the different things that exist today, so for that level of individual, this is a good starting point to kind of reach back into the technical area, and at least familiarize yourself with various concepts that can assist you in achieving information assurance.

And then for the sysadmin, it's also a really good place to look when maybe you're real familiar with the technology, but you're not real familiar with the managerial concepts, or what the policies are really there for, or how it kind of all ties together. I mean, a lot of the people who are the ones with their hands on the keyboards implementing firewalls and security measures lose sight of what it's all for, and so the Defense-in-Depth curriculum is really ideal for both those groups, and achieving kind of a different thing is giving sort of a managerial eye to the technical staff, and letting the managers see what it really means on a technical level.

Stephanie Losi: All right. Well, thank you very much. I've appreciated your time, I've learned a lot, and I hope our audience has as well.

Kristopher Rush: All right, thank you very much.