Security at Cisco – Part 2

Hello and welcome back to part two of Security at Cisco. I'm Rich Gore, Manager of the Cisco at Work Team and with me today is Laura Kuiper, Consulting Security Engineer in Cisco's Corporate Development Consulting. We'll dive right back into security technology within Cisco and then we'll wrap up with a question and answer period, as well as sharing some additional resources with you for more information on security. Thanks Rich, let's take another look at the agenda and then get right back into the security strategy.

AGENDA

So we've already talked about in the first part who is Cisco and we've already gone through a large chunk of the security technologies here at Cisco. So we're going to move right in and finish up the firewalls and go onto the next technology.

SECURITY STRATEGY: PROACTIVE & REACTIVE

Excellent. So the next thing we're going to talk about is Cisco CSA. So this is where our personal firewall, or host IPS comes in and it's another way that we're being proactive with our security.

CSA 4.5: ADDITIONAL FEATURES

So what is CSA? A lot of people go, "Well, what is CSA?" Sort of like virus protection, but not. Right, and most people in Cisco know what CSA is because we've got it running on all of our machines. But did you know that when we went from CSA 4.0 to 4.5 there was a lot of features that were added because of what IT fed back to our development team? Actually I didn't know. Absolutely, so some of the things were that we wanted to be able to put a single rule into test mode. Previously in CSA 4.0 before 4.5, if you had a new rule you had to put the entire policy into test mode rather than having the individual rule to find out what's going to happen if I implement this rule. So you can test one line at a time as opposed to testing the whole thing – nice. Absolutely, it's a great way to add new rules and find out what's going to happen, that you can have different policies for users when they are in the office and when they're outside of it. I mean, do I really want the same policy when I'm at home as when I'm in the office? Maybe not, so that's something where you can have different policies if you want them. Can I delegate security responsibility to the end user; absolutely, so how much security do they want? I can set what a minimum should be but if they want more security they can go in and adjust that and that actually makes it very nice. We have some very paranoid people within Cisco. I've seen that feature, I haven't used it, but I have seen it. That is what it's for. I'll give it a try. And you can push configuration changes out to the agents, so rather than waiting until CSA says oh wait I need to check in, you can actually push that now to the multiple agents as well, of oh wait, I have a new rule because a new virus came out or something has happened and you can push it instead. Interesting.

END-USER SECURITY DECISIONS

So here's that example of what we were talking about for end-user decisions; centrally define high, medium or low and the other thing is that you can do the personal firewall type and decide what do I want to have. The other big feature that came out with 4.5 is the "remember" feature. Have you ever had a product or application where every single time you went to use it, CSA pops up? As a matter of fact, yes, I do. You could now tell it to remember what your answer is and it won't pop up again because it will remember what your answer was, so that's a very useful feature. It's a very bad feature, also, because if somebody does that when they say. "yes, I want this virus to infect me", it will remember that for the next time as well. Over and over again. Well, so you can also go back in the logs and see if you've done that and go and change it if you need to. But it's very nice for those applications that we don't have a CSA rule for that continually asks for CSA every single time. Remember what my answer is so that I don't have to tell you every time. Makes sense.

AN ROI EXAMPLE

So one of the big things that happens in business is: business wants an ROI, they want a return on investment. Why should I do this? Why should I build up a brick wall? Why should I install a CSA, yes. Absolutely, why should I spend the money to buy CSA to do this? Well, we actually have an ROI example here. How much does it cost you when you have a virus or worm to clean it up? I have no idea. Well, here we've got some examples of how much it costs to clean up each time we have a virus. So if you have a minor incident, a minor incident and it's costing you $250,000 per minor incident. It's costing you up to $2.5 million for a major incident. Where does the cost come from? The cost comes from how many people is it taking and how much of their time is it taking to go and chase down these viruses and image these systems, so that's taking a lot of time. And when we do that type of study you can figure out, as we're seeing the increase in the number of viruses and worms that these types of things are only going to increase. We've seen those types of numbers with SQL Slammer. How much did it cost the world to clean up SQL Slammer? So what you can do is here's what my Opex cost was, total for the year for cleaning up these incidents. How much is it going to cost me to install CSA and then what's CSA going to do, how many incidents is it going to reduce so it reduces my total amount of cost? And as you can see from this ROI example, I reduce my Opex cost by quite a bit and a lot of companies are looking for reducing Opex cost overall. Absolutely, so we have some places where we can say a virus or a worm came at Cisco and CSA blocked it. Absolutely, and we can look at that from our logs and we can say this number of machines didn't have CSA running and it cost us this much money to go and clean those up as well. So we've been able to start tracking that, we've been tracking that for well over a year now and almost two years, so we actually have something to go back on and say, you started deploying CSA here, our cost went down by this much. Nice.

AT CISCO: CSA

So at Cisco we have now fully migrated to 4.5 across the board. We actually were doing the beta testing for the CSA team for 4.5 and so we're able to find some of the issues before it gets rolled out to the rest of our customers. We rolled it out to all production desktop and laptop systems and I clarify that because as you can see from the next bullet, we're working on deploying it out toward DMZ and to our critical servers. So we have it on all desktops today, if anybody gets a desktop at Cisco, it will have CSA already installed. And we're working on Unity servers, so currently any of our Unity servers out there which are over 50, we have CSA deployed on it because they're very critical in our infrastructure and we want to protect them. Makes sense. And we've rolled it out to our CallManagers as well, so CallManagers in the Unity systems, we've already rolled out CSA; we're working on other critical infrastructure servers as well to roll those out, that's our movement forward.

SECURITY STRATEGY: PROACTIVE & REACTIVE

The next thing we're going to talk about is network access control, this is NAC and 802.1x, both big hot buttons that have happened recently. I've heard of them, yes.

NAC LOGICAL COMPONENTS

So let's talk about what is NAC because everyone goes, we want to talk about NAC. Well NAC is network admission control and it's made up of several parts. It's made up of an agent that runs on your machine, it's a very lightweight agent that runs on your PC called CTA, which is Cisco trust agent. It talks to a router, which is a network access device, and that router talks to a AAA server that has where the policies are located. And based on whether or not the information that CTA provides matches up to the policies determines what kind of network access you can have. So let's say, for example we have a policy that says, you must be running CSA, you must be running anti-virus, and you must be running a particular service pack of Windows 2000. Reasonable requests. Absolutely, what happens when you come on the network and you've disabled your anti-virus? Well, how do I know you don't have a virus infection? You wouldn't, yes. Right, and so we talked earlier about how somebody could come from their house, plug into Cisco's network and all of a sudden we've got an infection in Cisco's network. With NAC what would happen is it'd look at the policy and say wait a minute you've got anti-virus disabled, it would put you on what's called a quarantine network. It would give you a little pop-up that says, your anti-virus is disabled, please enable and run

anti-virus and then we'll allow you back on the network. Seems friendly enough, yes. Seems friendly enough. So we're looking at how we're going to deploy that. So that's something where it's a way to help protect networks by how a machine is postured. So this is not user access. So 802.1x does user authentication, NAC does posture validation of a machine.

AT CISCO: NAC

So what are we doing at Cisco with regards to NAC? We're actually, have an ongoing pilot with our remote access, so again those lovely 831 people on the pilot. I'm one of them, yes. So that we can look and how that works, and how it works on a large scale. We're planning and creating a standard for deployment to field sales offices. So what we've done is we've created a architecture for what we believe will work for NAC and we're starting with our field sales offices because they're much smaller and so we have a little more control over what we can do. We have an ongoing pilot also going for field sales offices with sites currently in monitor mode. Now monitor mode is with NAC I can turn NAC on and not have it actually quarantine you but have it send me logs for what it would have done. So these are the people who I would have quarantined, but I let them go this time. Or these are the people that aren't running CTA because you have to be running CTA to do this. If you're not running CTA, it makes it very difficult for it to do anything. So you run it in monitor mode and you can see, okay, if I have a field sales office of 20 people and I only have 10 that are logging onto the network with CTA and I have 10 that aren't, well, if I were to enable NAC fully, those 10 that are not running CTA would have difficulty getting on the network. You'd shut them down. So we're trying to figure out the best migration path for doing some of this. So it's like a dry run with nobody hurt. Correct, absolutely. CTA, what does CTA mean? CTA is Cisco trust agent, so it's the lightweight client that runs on your PC. It's a collector of information. It collects the information about, is this Windows 2000, what service pack are you running, are you running CSA, are you running McAfee, what are you running? Yes, and what levels. Yes, it collects all that information and hands it off. The other big thing that we're doing in IT as a whole is we're working closely with the business units that are doing NAC, especially NAC phase 2. Because phase 2 will involve switches, which means that instead of waiting until it gets to the router, as soon as I plug in my machine to the switch, it will do that posture validation. So we're working with the business units on how that's actually going to work in the future. Makes sense.

SECURITY STRATEGY: PROACTIVE & REACTIVE

So what are we doing from an investigation and forensics standpoint? So mentioned earlier that we're collecting information and most of the tickets that are opened for security incidents are opened through alerts on the SIM system. Well, what do we do with them? Good question, yes, I have no idea.

SIX PHASES OF INCIDENT RESPONSE

So this is our reactive mode. So we've go six phases of what we call incident response. Incident response is, “I've got an incident and now what do I do?” And six phases are, “how do you take care of that?” So the number one phase is something that should be always ongoing, happening, which is preparation. These are doing the best practices, already having the Netflow enabled, collecting the syslogs, already having these things in place. The next is identification. So I'm all prepared and I get an anomaly on Arbor, what do I do? I identify what that problem is. How do I do that, what are my processes for it? Part of preparation might be, who do I contact when this happens? What's the escalation path? When do I get a manager involved? All of this is done ahead of time, as well as who's going to do it and what are the phone numbers to call. So in my preparation I've done that, so I've identified a problem. Now I know who to go contact and then I can do verification of it and the verification of it says, what is it, so I've identified it, verified that it is a problem. I do a trace back, which means I find out where did it come from. I do a reaction, so now I traced it back, what do I do? Some things you want to shut down right away. Maybe, if it's going to be something that needs a legal response, you don't want to shut it down right away because you want to protect yourself, so you may have a different reaction. And then the last thing you're going to do is have a post mortem. And the two phases of this that are the most important are preparation and post mortem. What did I do right, what did I do wrong, what do I need to change in my policies or procedures going forward? Makes sense, yes. So this is six phases of incident response.

PROTECTING CISCO FROM SQL SLAMMER TIMELINE SUMMARY

You have a team of people who do this for a living. We have a virtual team of people that do this on a regular basis. And I'm going to actually walk through an example of how Cisco used incident response to react to an attack. That sounds great. So I'm going to take SQL Slammer because it's the best one to give as an example. It was a big one, yes. Yes, so first thing is that Slammer was launched. Within less than five minutes Cisco had detected it, we had identified that it was a problem and we had started locking it down. And you can see from this timeline that we had already done all of these steps before it had started majorly impacting the rest of the network. So how did we detect it within five minutes? We detected it from using Netflow and Arbor. Right, okay, thank you. So the chart we looked at before that showed the nice peak, we had somebody who was watching that who saw it, who understood that this was a problem and was able to quickly get a hold of our operations team, which is 24 hours and they acted as our central contact. They were able to get the networking operation and the security operations folks on the phone and get them to start actually putting appropriate ACLs in the right places, locking it down to protect Cisco. Very nice. So we went ahead and did that. What we did next was we were able to create a tool to help find machines that may be vulnerable with our own internal network. Find already compromised machines. We didn't have anybody compromised, but machines that could be compromised that needed a patch. Oh, I see. What we were able to do is because we were able to create that because we weren't fighting the worm, we'd already blocked it, we were able to do that. We were also then able to then put that out for the public to be able to use as well to help them find the machines on their network that were infected. Tell them what sorts of machines were being targeted and what they can do to remediate that.

1. AT CISCO: STOPPING SQL SLAMMER

Right, and the last thing was of course because we weren't fighting that, we were able to help our customers who were fighting it to be able to find ways to get around it, to mitigate it, to clean themselves up. So how did we do all of this? The first thing is we utilized Arbor that works Peakflow DoS anomaly detection, we used that in conjunction with that. That's where we saw that chart that I showed before that showed the huge spike, that's where we saw it. Within minutes, we had our transport and InfoSec teams all networking and our info tech teams responded, locking down the ports at every ingress and egress port globally. We were even able to do a proxy for our folks who are on remote access, so if they had connected, gotten infected at home, they were not going to bring the infection in. And what this really brings to mind is that we had all these tools working, detecting and setting alarms but the part that you said about preparation earlier, what we really had were people who were ready to get the alarms and knew what to do, and knew who to get involved at the moment that the alarms came in. Because if you didn't have that, if you had nobody watching and waiting, or if you had people but they didn't know what to do in response, you would have had people running around and stumbling over themselves. That's amazing. Absolutely, and that's what a lot of people around the rest of the globe had when SQL Slammer happened. We happened to be ready for it, we were very lucky in that sense. How did we get ready for it because it was unusual, it was a once in a lifetime kind of event. We were ready for it because we'd already had some stuff in place for other viruses we had worked on. So that's where we had our preparation already done, we'd already walked through it a couple of times and knew what was going to happen, and they knew how we needed to react. Interesting, okay. So the other thing we did is we created a war room environment so that we could work with PCERT and TAC and our key customers. PCERT? PCERT, this is the incident response team for Cisco externally facing. So if you as a customer have a problem, you're going to open a ticket with TAC. If it's a security-related issue, PCERT may get involved because it may be a vulnerability that they will help address. They ensured best practices, they were able to help with communication and remediation across the globe. And they went and helped our customers after it. Absolutely.

2. AT CISCO: STOPPING SQL SLAMMER (CONT.)

So good experience. Absolutely, so we also scanned Cisco with the in-house tool so we knew what needed to be upgraded, what needed to be patched. So we developed the first scanner, we made it publicly available. We didn't make anybody buy it, we made it available for anybody who wanted to use it. Very nice. And then we performed round the clock monitoring and follow-up on all of the teams that

involved to ensure that no infection had happened and that remediation of servers that potentially could be infected was done. We also had a post mortem that said here's what we did right, here's what we didn't do right, here's what we need to change going forward.

3. AT CISCO: STOPPING SQL SLAMMER – RESULTS

As a result of this, there were no infections found within Cisco of SQL Slammer. That's amazing. It was absolutely amazing. It's one of the reasons why we use this as our example because we did the preparation, we responded, we reacted, we were able to do it going forward. What were the success criteria? As I said, preparation was number one, identification and detection, classification, classified what it was, what needed to be done, communication and empowerment. That was probably, as you pointed out, one of the critical things. Who do you contact, how do you get a hold of them? You empower them to make the decision to put the ACL on there, block it and then we'll move forward. Absolutely, a critical piece to this puzzle as well, we reacted quickly, we knew what to do and then we followed up with a post mortem. We were able to then find out what needed to be done.

SUMMARY

So that's what we have from a technology, policy, process standpoint of what we're doing at Cisco for security.

AT CISCO:

And what I'd like to say in summary is, security at Cisco is important to all aspects. We're not focusing just on our source code, we're not focusing just on our customer data, we consider security important across the board. As you can see, we've done many different things to bring the security technology that Cisco has into our internal network and actually use it and show how important it is. InfoSec and the IT infrastructure work together to deploy these Cisco security features. We don't have two isolated stacks of people. They work together, they work on the architectures together to make security a critical component of the architecture, not just a reliability because with good security, you're more likely to get the reliability. Very true. And we incorporate both proactive and reactive mechanisms. CSA, very proactive, incident response, very reactive, so we incorporate the two together to be able to have the most effective security overall here at Cisco. That's fantastic.

SECURITY AT CISCO

You can find more information about security in general at the www.cisco.com/security website. It will give you information in general about what's happening in the security world. It has links off of it to other Cisco web pages that will give you more information about either a security product, or a security solution, or potential vulnerabilities that may be out there, so it gives you a wide variety of things going on from a security perspective. Nice to know.

QUESTIONS

Well Laura, before we go, thank you, that was an awesome presentation, I very much appreciate that. We've put together some questions that customers had asked us about this particular topic in previous sessions, so we have just a little bit of time left and I'd like to ask you to answer a couple of them, if that's okay.

Q. So the first question was, it's about Cisco Guard. Cisco Guard looks like a good defense against DDoS attacks, at least, it says, it keeps the server from being overwhelmed but the rest of your network is still buried under all the added traffic. Is there any way of defending against that?

A. So defending against the additional added traffic can become an issue, and we call that collateral damage because that's not the initial intent of the attack. A lot of that is the type of traffic that it is. You can start doing other types of cleaning up that traffic earlier up in the network. So what the Cisco Guard will do is do the initial being able to allow that host to still be available, which allows you the opportunity to start going back and figuring out how to either block the traffic, if it's a particular source, where you might block that,

working with your service provider to potentially block some of that traffic as well. And if you're a service provider, tracing it back to what customer is it coming from. How interesting. So just pushing that blockage further and further back in the network. Absolutely, till it's right in front of the source of where the problem occurred. Fantastic, yes, okay, thank you.

Q. Question number two. How has Cisco dealt, ah, back to IDS and IPS, how has Cisco dealt with all the false positives that are part of any IDS or IPS system?

A. We've taken a long time to actually do what we call tuning of the systems, we started small of where we deployed them to determine what that is. So we still have some concerns with that, it's one of the reasons why we do still verify all of the alarms that we do get. If they're legitimate alarms, we do open a case for them. And you saw that the vast majority of the cases are open through that, but we're still working on how the best way is to get rid of the false positives and right now it's just a continual tuning mechanism working on it going down the road. We're hoping CSMARS will actually help us with that, but we haven't fully implemented it across the board to be able to tell us if that's the case. Makes sense, yes. And I would imagine, especially at Cisco, the environment where we're constantly changing the environment, changing the type of equipment and the type of traffic would make it a little bit more difficult to setup rules. Well, it's not as hard because IDS and IPS is all signature-based, so it's really looking for a particular signature. So changing out the equipment on the backend on either side on IDS won't change the signature if it's a virus or a worm. Oh, that makes sense. So rather than being behavioral-based, like we talked about with Cisco Guard, IDS and IPS is signature-based so it's looking for a particular signature. So it won't be thrown off by new traffic coming in. Interesting, good, thanks. Well, unfortunately, that's all the time that we have, but thank you very much for answering those questions. And what I'd like to do is point out to you watching at home that there's more information that you can find.

MORE SECURITY RESOURCES

At the top of the page you'll see a URL you can go to for more information about Cisco IT deployments of Cisco technology, including Cisco security technology. You can go to the Cisco IT at work website to find Cisco IT case studies about what we do deploy, what benefits we've gained, what lessons we've learned and also there's some operational practices and some presentations to help you learn more. And now you can also find more information on security in general. There are some design guides, and operational practices, and several other documents, and white papers, and presentations on cisco.com in the URL just below that. Below that, you'll see a toll free number that you can call for more information, or if you'd like to place an order and you can also order Cisco resources from the web from the URL at the bottom of the page.

THANKS FOR WATCHING

So I'd like to thank all of you for watching us and for spending this time with us, for being interested in what the global technology seminar series is all about and for being interested in security in general. We hope that you've enjoyed this show and that it has helped answer some of your questions about security and how we do security in Cisco. So thank you, all of you for spending this time with us and sharing your enthusiasm for security. And thank you Laura, very much, for sharing your expertise, we really appreciate it. Rich, it was an absolute pleasure and I do hope that you've all enjoyed this show and that you'll come back and see another one again soon.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C78-337384-00 02/06