CEC Internal News

Employee Information

Keeping Our Products Safe from Attack

CEC Posting Date: 2009-Dec-17

All employees are accountable and must do their part to keep Cisco's assets, information, and intellectual property secure. For more information, see the Cisco 2009 Annual Security Report.

Cisco thrives on healthy competition, although sometimes it needs to engage in high-pitched battles for the upper hand. Fewer battles have higher stakes for Cisco than the one to beat cybercriminals in their attempts to undermine the security of our products.

Customers depend on Cisco to be a trusted leader in the cybersecurity realm. When customers encounter security weaknesses in Cisco products, the threat is larger than just tackling the bug or defect at hand. The bigger threat is to Cisco's trusted relationship with customers, which, if it is weakened too often, can erode one of our most precious assets: the value of the Cisco brand in the marketplace.

Cisco's leadership recognizes the seriousness of the war on cybercrime and, as part of the company's internal quality initiative, has called for network and product security to be the job of every product development team and engineer.

At this year's July/August birthday chat event with employees, John Chambers issued this challenge to the engineers in the room: "I'm asking each of you that every product we develop and work on should have security and manageability

Cisco's First Global Security Awareness Event

Every day Cisco employees are faced with security risks that put the company's intellectual and physical property at risk. At Cisco, all employees are accountable and must do their part to keep our company's assets, information, and intellectual property secure.

On December 9, Corporate Security Programs, Safety and Security, Emergency Preparedness and Response, and the Privacy teams hosted the inaugural Global Security Awareness Event in an effort to broaden awareness and educate employees about the best ways to help protect Cisco and keep the company's information—and its employees—safe and secure.

Visit the Virtual Event Site to learn how you can make a difference by properly handling confidential information, preventing tailgating, knowing how to manage risk, and protecting yourself and Cisco's confidential information on social networking sites, among other information and resources.

Join the Keep Cisco Secure movement. The Corporate Security Programs Organization is recruiting a special team of advocates to create the culture of awareness and help

at the initial thought-process stage, not as an afterthought."

President Obama Rallies a Nation, and Cisco Responds

The battle cry is being echoed at the national level. President Obama recently declared October to be National Cybersecurity Awareness Month.

"The cyberthreat is one of the most serious economic and national security challenges we face as a nation," he said.

In October, Cisco showed the determination to continue to meet the security challenge head-on by hosting the second annual SecCon conference for employees. Coinciding with National Cybersecurity Awareness Month, the conference drew approximately 650 participants, the majority of them product development engineers.

The goals of this year's SecCon conference were to impress upon product teams how deep-rooted the cybersecurity threat is and to offer proactive solutions for making Cisco products more secure from hacker attacks and malicious exploits.

To accomplish the first goal and demonstrate to attendees the ingenuity of cybercriminals, conference organizer Erick Lee decided to invite actual hackers to speak. Lee recruited "good" hackers, who help Cisco by providing useful information (as opposed to bad, or black hat, hackers, who do so for profit and to break products).

Says Lee, who is a senior technical leader in the Advanced Security Initiatives Group, "Developers don't tend to go to security conferences where hackers are—they're going to developer conferences instead. So, we decided to make this a 'hackers talking to developers' conference."

Hackers Show Their Stuff

Vulnerability disclosures are areas where Cisco has let customers down by building products that are not as secure as they must be. These disclosures generate a lot of concern from our customer base. Along with putting our customers at risk, they distract those customers from moving forward and delivering their products and services—and, by extension, they impact our ability to sell

Guest speaker Felix "FX" Lindner started things off by revealing how he could exploit a Cisco router simply by examining the physical item and its output. Then, hacker Moxie Marlinspike from the Institute for Disruptive Studies continued to keep attendees unsettled by showing how SSL sessions between a customer and a trusted business, such as a bank, can be attacked despite the presence of the lock icon on the web browser.

Chris Paget shook any remaining conference complacency further with examples of hardware hacking. In one demonstration, he mimicked a base station on a GSM phone network in order to get a Cisco phone to connect through the fraudulent station rather than a legitimate station.

But, rather than leaving SecCon participants

communicate security risks through the Security LEAD program (LEAD stands for Leading, Educating, Advocating, and Demonstrating).

Related Link

- Corporate Security Programs Organization

those products and services.

Russell Smoak, Director of Security Research and Operations

feeling vulnerable without any source of hope, this year's conference offered Cisco a significant step forward in terms of making its network products more impervious to attack and the threat of brand erosion. That step forward was the official launch of the Cisco Secure Development Lifecycle, or CSDL.

According to Lee, CSDL is built upon industry best practices and existing security elements already in use. "It's a product lifecycle methodology that identifies certain tools, processes, and actions that product teams can take to ensure secure and resilient products," he explains.

How the CSDL Helps Beat Cybercrime

The CSDL is divided into six phases: 1) concept, 2) plan, 3) develop, 4) validate, 5) launch, and 6) sustain. Early in the lifecycle, the user is introduced to the product security baseline, which is a list of more than a hundred common security mistakes and how not to make them.

Later on, the CSDL covers threat modeling, which approaches all the different ways that someone can threaten a security mechanism and how to mitigate those threats. "Threat modeling is thinking like a hacker," says Lee.

Further elements in the CSDL help developers to write good code and avoid bad code, prevent a bug from becoming something seriously exploitable, use secure silicon components, test products while attempting to break them, and "sign" a product so that customers can be assured that they are running a Cisco product and not a piece of malware.

One Cisco business unit that has been industriously putting the CSDL to early use is the Unified Communications Business Unit (UCBU).

According to UCBU software engineer Massimo Ramella-Pezza, the UCBU was busy adopting components of the CSDL even before the formal launch, most notably conducting 11 product security baseline evaluations in 2009.

"The CSDL allows us to create a process that lets everything fall into place at the right time. And, it really helps us keep our products in line with each other," says Ramella-Pezza, who is the UCBU's "security advocate." As a security advocate, he works regularly with the Security Evaluation Office to learn about the latest CSDL tools and information, and shares this input with the product developers in his business unit.

UCBU Leads the Cybersecurity Charge

Ramella-Pezza is excited about the upcoming UCBU release of Cisco Unity Connection 8.0 because it has been at the forefront in terms of early incorporation of the CSDL. According to Ramella-Pezza, this fact is allowing Cisco account teams to push the product more energetically into the marketplace—a marketplace where major customers in banking, telecommunications, and the government have started asking Cisco specifically for lifecycle compliance. With the CSDL, Cisco can answer security questions upfront with much greater confidence than before, he adds.

Ramella-Pezza urges other product teams to learn about the CSDL and to adopt it. "By implementing the CSDL, product teams can translate security directly into a competitive advantage for their product," he says.

From his vantage point as Director of Security Research and Operations for Cisco, Russell Smoak can share in Ramella-Pezza's enthusiasm for the CSDL. One of the most visible programs in his organization is Cisco's Product Security Incident Response Team (PSIRT), which receives security vulnerability reports from internal and external parties, classifies them, works with CDO to resolve the issue, and discloses the vulnerabilities to customers.

"Vulnerability disclosures are areas where Cisco has let customers down by building products that are not as secure as they must be," says Smoak. The vulnerabilities, he indicates, can range from network-disrupting events that prevent the delivery of services to those putting government entities at risk for information disclosure to those endangering intellectual property and financial data.

"These disclosures generate a lot of concern from our customer base," adds Smoak. "And along with putting our customers at risk, they distract those customers from moving forward and delivering their products and services—and, by extension, they impact our ability to sell those products and services."

The Challenge Before Us

"What we don't always consider inside of Cisco, especially in the early stages of product development, is the potential install base of the product. If we push out a vulnerability in one of our very pervasive products, you can be looking at hundreds of thousands of devices that have to be addressed," Smoak states.

These disruptive activities cost customers a significant amount of money and impact the delivery of services, which can cause damage to the brand of both the customer and Cisco.

Lee agrees. "At Cisco, luckily, we haven't had that five-alarm fire yet," he says. On the other hand, he notes that more than 50 percent of the security bugs at Cisco are found by customers and hackers. "That's not a good stat," he adds.

Lee, Smoak, and Ramella-Pezza all see the CSDL as helping to come to the rescue of potential fires. The beauty of the CSDL, says Ramella-Pezza, is that "it gives us the tools to secure our products architecturally from cybersecurity threats."

That emphasis on architecture is key. As John Chambers stated in a keynote speech at RSA Conference 2009 in April, "I think you can have innovation and security coexist. ... You have to do it architecturally. You've got to realize that it's going to be a phased-in approach. And, you've got to realize that you're going to be only one or two steps ahead of the bad guys for the next 5 to 10 years."

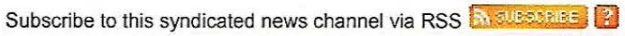
Related Links

- Cisco Secure Development Lifecycle
- Cisco Product Security Incident Response Team
- Cisco Security Intelligence Portal
- Cisco Trusted Systems Group
- Security Technology Business Unit
- Cisco 2009 Annual Security Report

For comments or questions on the above content, please contact CEC News Team.

Please indicate your organization and provide feedback to the author:

Select Your Organization... Rate this article...

Subscribe to this syndicated news channel via RSS 

Managed by: CEC News Team; Last Modified: 2009-Dec-17 | About CEC