NEWS RELEASE

Cisco Annual Security Report Reveals Widening Gulf Between Perception and Reality of Cybersecurity Readiness

2015-01-20

60% of Cisco Security Capabilities Benchmark Survey Respondents Are Not Patching and Only 10% of Internet Explorer Users Run Latest Version; Still 90% of Respondents Are "Confident" in Their Cybersecurity Capabilities

SAN JOSE, CA -- (Marketwired) -- 01/20/15 -- Cisco (NASDAQ: CSCO) -- The Cisco 2015 Annual Security Report released today, which examines both threat intelligence and cybersecurity trends, reveals that organizations must adopt an 'all hands on deck' approach to defend against cyber attacks. Attackers have become more proficient at taking advantage of gaps in security to evade detection and conceal malicious activity. Defenders, namely, security teams, must be constantly improving their approach to protect their organization from these increasingly sophisticated cyber attack campaigns. These issues are further complicated by the geopolitical motivations of the attackers and conflicting requirements imposed by local laws with respect to data sovereignty, data localization and encryption.

Attackers

Cyber criminals are expanding their tactics and adapting their techniques to carry out cyber attack campaigns in ways that make it harder to detect and analyze. The top three trends last year that Cisco's threat intelligence has identified are:

- ***Snowshoe Spam:*** Emerging as a preferred strike method, attackers are sending low volumes of spam from a large set of IP addresses to avoid detection, creating an opportunity to leverage compromised accounts in multiple ways.
- ***Web Exploits Hiding in Plain Sight***: Widely used exploit kits are getting dismantled by security companies in short order. As a result, online criminals are using other less common kits to successfully carry out their tactics -- a sustainable business model as it does not attract too much attention.
- ***Malicious Combinations:*** Flash and JavaScript have historically been insecure on their own, but with advances in security detection and defenses, attackers have adapted by deploying exploits which combine their respective weaknesses. Sharing exploits over two different files -- one Flash

and one JavaScript -- can make it more difficult for security devices to identify and block the exploit and to analyze it with reverse engineering tools.

Users
Users are caught in the middle. Not only are they the targets, but end-users are unknowingly aiding cyber attacks. Throughout 2014, Cisco threat intelligence research revealed that attackers have increasingly shifted their focus from seeking to compromise servers and operating systems to seeking to exploit users at the browser and email level. Users downloading from compromised sites contributed to a 228% increase in Silverlight attacks along with a 250% increase in spam and malvertising exploits.

Defenders
Results from the Cisco® Security Capabilities Benchmark Study, which surveyed Chief Information Security Officers (CISOs) and Security Operations (SecOps) executives at 1700 companies in nine countries* reveals a widening gap in defender perceptions of their likely security capabilities. Specifically, the study indicates that 75% of CISOs see their security tools as very or extremely effective. However, less than 50% of respondents use standard tools such as patching and configuration to help prevent security breaches and ensure that they are running the latest versions. Heartbleed was the landmark vulnerability last year, yet 56% of all installed OpenSSL versions are over four years old. That is a strong indicator that security teams are not patching.

While many defenders believe their security processes are optimized -- and their security tools are effective -- in truth, their security readiness likely needs improvement.

The report findings conclude that it's time for corporate boards to take a role in setting security priorities and expectations. The Cisco "Security Manifesto," a formal set of security principles as a foundation to achieving security, can help corporate boards, security teams and users in an organization better understand and respond to the cybersecurity challenges of today's world. It can serve as a baseline for organizations as they strive to become more dynamic in their approach to security and more adaptive and innovative than adversaries. The principles are:

1. Security must support the business.
2. Security must work with existing architecture -- and be usable.
3. Security must be transparent and informative.
4. Security must enable visibility and appropriate action.
5. Security must be viewed as a "people problem."

For a complete copy of the Cisco Annual Security Research report go to www.cisco.com/go/asr2015

About the Report
The *Cisco 2015 Annual Security Report* is one of the preeminent security reports that examines the latest threat intelligence gathered by Cisco security experts, providing industry insights, trends and key findings revealing cybersecurity trends for 2015. The report also highlights data results from Cisco's *Security Capabilities Benchmark Study* which examines the security posture of enterprises and their perceptions of their preparedness to defend themselves against cyber attacks. Geopolitical trends, global developments around data localization and the importance of making cybersecurity a boardroom topic are also discussed.

Supporting Quote
John N. Stewart, senior vice president, chief security and trust officer, Cisco
"Security needs an all hands on deck approach, where everybody contributes, from the board room to individual users. We used to worry about DoS, now we also worry about data destruction. We once

worried about IP theft, now we worry about critical services failure. Our adversaries are increasingly proficient, exploit our weaknesses and hide their attacks in plain sight. Security must provide protection across the full attack continuum and technology must be bought that is designed and built with that in mind. Online services must be run with resiliency in mind, and all of these moves must happen now to tip the scales and protect our future. It requires leadership, cooperation, and accountability like never seen before in our industry."

Jason Brvenik, Principal Engineer, Security Business Group, Cisco
"Attackers have become more proficient at taking advantage of security gaps. We observed that that 56% of all OpenSSL versions still remain vulnerable to Heartbleed and that major attacks are only leveraging 1% of high-urgency vulnerabilities at any given time. Despite this, we see less than half of the security teams surveyed using standard tools like patching and configuration management to help prevent security breaches. Even with leading security technology, excellence in process is required to protect organizations and users from increasingly sophisticated attacks and campaigns."

Supporting Resources

- John N. Stewart video commentary on the Annual Security Report -- http://youtu.be/ioy5N5d3ugs
- Read Cisco Security Blogs
- Follow Cisco on Twitter @CiscoSecurity
- Like Cisco Security on Facebook http://facebook.com/ciscosecurity

*US, Brazil, UK, Germany, Italy, India, China, Australia, and Japan.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies transform the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. For ongoing news, please go to http://thenetwork.cisco.com.

RSS Feed for Cisco: http://newsroom.cisco.com/rss-feeds

Press Relations
Kelly Cytron
415-271-3638
kcytron@cisco.com

Analyst Relations
Trevor Bratton
949-823-1212
trbratto@cisco.com

Investor Relations
Marty Palka
408-526-6635
mpalka@cisco.com

Source: Cisco