NEWS RELEASE

Cisco Annual Security Report Reveals a Decline in Defender Confidence and the Increased Impact of Industrialized Attackers

2016-01-19

Businesses Make Strides in Advancing Security Posture in the Face of Persistent Attacks That Take Advantage of Aging Infrastructure and Data Leaks Through Browser Extensions
SAN JOSE, CA -- (Marketwired) -- 01/19/16 -- The Cisco® (NASDAQ: CSCO) 2016 Annual Security Report released today, which examines threat intelligence and cybersecurity trends, reveals that only 45 percent of organizations worldwide are confident in their security posture as today's attackers launch more sophisticated, bold and resilient campaigns.

While executives may be uncertain about their security strength, 92 percent of them agree that regulators and investors will expect companies to manage cybersecurity risk exposure. These leaders are increasing measures to secure their organizations' future, particularly as they digitize their operations.

The report highlights the challenges businesses face due to the rapid advancements of attackers. Hackers increasingly tap into legitimate resources to launch effective campaigns for profit-gain. Additionally, direct attacks by cybercriminals, leveraging ransomware alone, put $34 million a year per campaign into their hands. These miscreants continue to operate unconstrained by regulatory barriers.

Businesses are up against security challenges that inhibit their ability to detect, mitigate and recover from common and professional cyberattacks. Aging infrastructure and outdated organizational structure and practices are putting them at risk.

The study sounds a global call-to-arms for greater collaboration and investment in the processes, technologies and people to protect against industrialized adversaries.

Top Research Findings

- ***Decreasing confidence, increasing transparency:*** Less than half of businesses surveyed were confident in their ability to determine the scope of a network compromise and to remediate damage. But, an overwhelming majority of finance and line-of-business executives agreed that regulators and investors expect companies to provide greater transparency on future cybersecurity risk. This points to security as a growing boardroom concern.
- ***Aging infrastructure:*** Between 2014 and 2015, the number of organizations that said their security infrastructure was up-to-date dropped by 10 percent. The survey discovered that 92 percent of Internet devices are running known vulnerabilities. Thirty-one percent of all devices analyzed are no longer supported or maintained by the vendor.
- ***SMBs as a potential weak link:*** As more enterprises look closely at their supply chain and small business partnerships, they are finding that these organizations use fewer threat defense tools and processes. For example, from 2014 to 2015 the number of SMBs that used web security dropped more than 10 percent. This indicates potential risk to enterprises due to structural weaknesses.
- ***Outsourcing on the rise***: As part of a trend to address the talent shortage, enterprises of all sizes are realizing the value of outsourcing services to balance their security portfolios. This includes consulting, security auditing and incident response. SMBs, which often lack resources for an effective security posture, are improving their security approach, in part, by outsourcing, which is up to 23 percent in 2015 over 14 percent the previous year.
- ***Shifting server activity:*** Online criminals have shifted to compromised servers, such as those for WordPress, to support their attacks, leveraging social media platforms for nefarious purposes. For example, the number of WordPress domains used by criminals grew 221 percent between February and October 2015.
- ***Browser-based data leakage:*** While often viewed by security teams as a low-level threat, malicious browser extensions have been a potential source of major data leaks, affecting more than 85 percent of organizations. Adware, malvertising, and even common websites or obituary columns have led to breaches for those who do not regularly update their software.
- ***The DNS blind spot:*** Nearly 92 percent of "known bad" malware was found to use DNS as a key capability. This is frequently a security "blind spot" as security teams and DNS experts typically work in different IT groups within a company and don't interact frequently.
- ***Time to detection faster***: The industry estimate for time to detection of a cybercrime is an unacceptable 100 to 200 days. Cisco has further reduced this figure from 46 to 17.5 hours, since the 2015 Cisco Midyear Security Report was released. Shrinking the time to detection has been shown to minimize cyberattack damage, lowering risk and impact to customers and infrastructures worldwide.
- ***Trust matters***: With organizations increasingly adopting digitization strategies for their operations, the combined volume of data, devices, sensors, and services are creating new needs for transparency, trustworthiness, and accountability for customers.

For a complete copy of the 2016 Cisco Annual Security Research report, and to read more about Cisco's recommendations as to what businesses can do to mitigate against risk, click here.

About the Report

The *Cisco 2016 Annual Security Report* analyzes the most compelling trends and issues in cybersecurity from Cisco security experts on the advances made by both the security industry and by the criminals hoping to break through security defenses. In addition, the report highlights key findings from Cisco's second annual Security Capabilities Benchmark Study, focused on security professionals' perceptions of the state of security in their organizations. Geopolitical trends, insights into perceptions of cybersecurity risk and trustworthiness, and the tenets of an Integrated Threat Defense round out the report.

Supporting Quote

"Security is resiliency by design, privacy in mind, and trust transparently seen. With IoT and digitization taking hold in every business, technology capability must be built, bought, and operated with each of these elements in mind. We cannot create more technical debt. Instead, we must meet the challenge head on today."
-- John N. Stewart, senior vice president, chief security and trust officer, Cisco

Supporting Resources

Cisco Video with Chuck Robbins, John N. Stewart: 2016 Cisco Annual Security Report: Executive Perspectives
Cisco Annual Security Report
Cisco Blog: Forewarned is Forearmed: Announcing the 2016 Cisco Annual Security Report
Cisco Infographic
Follow Cisco on Twitter @CiscoSecurity
Like Cisco Security on Facebook

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize 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

Embedded Video Available

Press Relations
Kayla Bruneau
209-858-8290
kbruneau@cisco.com

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

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

Source: Cisco