June 2, 2015

Wireless Network the Weakest Security Link in Enterprise IT Infrastructure, According to Fortinet Global Survey of IT Leaders

9 in 10 CIOs Report Concerns Over Insufficient Wireless Protection; Over One-Third of Enterprises Found Lacking Basic Wireless Security

SUNNYVALE, CA -- (Marketwired) -- 06/02/15 -- Information Technology decision makers (ITDMs) believe wireless networks to be the most vulnerable element of the IT infrastructure, according to a new survey from Fortinet®(NASDAQ: FTNT), the global leader in high-performance cyber security solutions. Nearly half (49%) of respondents ranked wireless networks as most exposed from a security standpoint, in contrast to just 29% for the core network.

The Fortinet survey also reveals that insufficient wireless security is a concern for almost all (92%) of the CIOs polled; hardly surprising given that more than one-third of the enterprise wireless networks put in place for internal employees, do not have the basic security function of authentication in place.

The findings come from an independent survey of over 1,490 IT decision makers at 250+ employee organizations around the world. All respondents were sourced from independent market research company Lightspeed GMI's online panel.

Other survey highlights include:

- Nearly half of ITDMs (48%) consider loss of sensitive corporate and/or customer data the biggest risk of operating an unsecured wireless environment.
- 72% have adopted a cloud approach to management of their wireless infrastructure and 88% trust the cloud for future wireless deployment.
- 43% of ITDMs polled provide guest access on their corporate wireless networks; 13% of these organizations do so without any controls whatsoever.

Wireless Networks at Risk
According to the survey, wireless networks are ranked as the most vulnerable IT infrastructure, with the highest proportion of ITDMs (49%) placing it in their top two. Respondents positioned wireless as significantly more vulnerable than core networking infrastructure, with just 29% of ITDMs ranking this highly. Databases (25%), applications (17%) and storage (11%) infrastructures were considered amongst the least susceptible from a security standpoint.

In addition, 37% of global ITDMs polled do not have the most basic wireless security measure of authentication in place. A significant 29% and 39% of enterprises respectively, overlook firewall and anti-virus security functions when it comes to wireless strategies.

Other security measures deemed critical to core infrastructure protection, such as IPS (deployed by 41%), application control (37%) and URL filtering (29%), play a part in even fewer wireless deployments.

When considering the future direction of their wireless security strategies, the majority of respondents said they would maintain focus on the most common security features -- firewall & authentication, while demand for more security is emerging with 23% prioritizing complementary technologies -- IPS, anti-virus, application control and URL filtering -- to guard against the full extent of the threat landscape.

Concern High over Insufficient Wireless Security
Of the ITDMs surveyed, 83% are concerned their existing wireless security is not sufficient, with CIOs reporting the highest level of concern at 92%. Despite deploying the highest level of security of all the regions surveyed, ITDMs across APAC are the most concerned about their wireless security with 44% stating they are very concerned, in contrast to 30% in the Americas, and 20% in EMEA.

Globally, ITDMs reported varying confidence levels in wireless security; China tops the board with 71% 'very concerned', compared to just 13% in Japan.

The findings suggest that increased security awareness leads to higher levels of concern, with respondents in the top two 'concerned' countries -- China and India -- deploying more wireless security functions on average, than the two least 'concerned' countries -- Italy and Japan.

Risk of Data Loss Tops Poll
When asked to cite the risks of operating an unsecured wireless network, 48% of ITDMs considered loss of sensitive corporate and/or customer data as the biggest risk to their organization. This was highest at 56% in APAC, in contrast to the Americas at 45% and EMEA 42%.

The next highest risk, industrial espionage, was cited by just 22% of ITDMs, followed by non-compliance to industry regulations (13%), with service interruption and damage to corporate reputation ranked equal last (9%).

Cloud Management Becomes the Norm
Wireless infrastructure governed by a premise-based controller is a thing of the past according to the findings, with on-site wireless controllers the least common form of management (28%).

This trend for cloud-based management looks set to grow further, with only 12% of enterprise ITDMs refusing to trust the cloud for such critical management in the future.

Of the cloud-ready respondents, 58% would want to use a private cloud infrastructure for wireless management and 42% would outsource to a third party managed services provider. 14% of those considering outsourcing would only do so provided it is hosted in the same country, leaving 28% happy to embrace wireless management as a public cloud service regardless of geography.

'Totally Open' Guest Access
Nearly half (43%) of ITDMs polled provide guest access on their corporate wireless networks, with 13% of these organizations doing so without any controls whatsoever.

The most common form of guest security access on corporate wireless networks is a unique and temporary username and password (46%), ahead of a captive portal with credentials (36%).

"The survey findings indicate that despite the growth in mobility strategies, wireless security has simply not been a priority for enterprises to date," said John Maddison, vice president of marketing products at Fortinet. "As advanced persistent attacks increasingly target multiple entry points, and the cloud becomes more prevelant, it's not an oversight organizations should risk any longer."

"It's positive to see IT Leaders beginning to recognize the role wireless security plays in protecting their critical business assets, yet there is more to be done. As IT strives to balance the need for strong network security with ubiquitous connectivity, wireless must be considered as part of a holistic security strategy to ensure broad and consistent protection for users and devices over wired and wireless access."

Note to Editors

The Fortinet Wireless Security Survey was a research exercise undertaken throughout May 2015, by market research company Lightspeed GMI. The survey was conducted online amongst 1,490 qualified IT decision makers -- predominantly CIOs, CTOs, IT Directors and Heads of IT -- at organizations with more than 250 employees around the globe.

12 countries participated in the survey: Australia, Canada, China, France, Germany, India, Italy, Japan, Hong Kong, Spain, UK and USA. For more information about LightSpeed GMI go to: http://www.lightspeedgmi.com

About Fortinet
Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments - be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at http://www.fortinet.com, the Fortinet Blog or FortiGuard Labs.

endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding product releases. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Attachment Available: http://www.marketwire.com/library/MwGo/2015/6/2/11G043443/Global_Wireless_Security_Survey-1284372564257.pdf

Media Contact:

Andrea Cousens
Fortinet
310-270-8903
acousens@fortinet.com

Source: Fortinet