The weakest link: wireless networks

According to Anton Jacobsz, managing director of value-added distributor Networks Unlimited, the need for network security is evident. Wireless networks are still regarded to be vastly more vulnerable and open to issues such as eavesdropping and authentication risks than their wired counterparts.

OlkerFreeVectorImages via pixabay

Lack of basic wireless security

"A new survey by Fortinet, a reseller partner of ours, has found that nine in 10 CIOs report concerns over insufficient wireless protection and over one-third of enterprises were found lacking basic wireless security. It is an obvious concern in the market and this element of IT infrastructure needs urgent addressing by both business and IT leaders to provide a complete security strategy across both wired and wireless networks," he adds.

According to the Fortinet survey referred to by Jacobz, nearly half (49 percent) of respondents ranked wireless networks as most exposed from a security standpoint, in contrast to just 29 percent for the core network.

With regards to the high number of CIOs being concerned about the vulnerabilities of a wireless network, the survey reveals that this is 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 of the Fortinet survey come from an independent survey of over 1,490 IT decision makers (ITDMs) at 250+ employee organisations around the world. All respondents were sourced from the independent market research company, Lightspeed GMI's online panel.

Other survey highlights include:

• Nearly half of ITDMs (48 percent) consider loss of sensitive corporate and/or customer data the biggest risk of operating

an unsecured wireless environment.

• 72 percent have adopted a cloud approach to managing their wireless infrastructure and 88 percent trust the cloud for future wireless deployment.

• 43 percent of ITDMs polled provide guest access on their corporate wireless networks; 13 percent of these organisations do so without any controls whatsoever.

The survey also showed databases (25 percent), applications (17 percent) and storage (11 percent) infrastructures were considered amongst the least susceptible from a security standpoint.

In addition, 37 percent of global ITDMs polled do not have the most basic wireless security measure of authentication in place. A significant 29 percent and 39 percent 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 percent), application control (37 percent) and URL filtering (29 percent), 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 and authentication, while demand for more security is emerging with 23 percent prioritising complementary technologies - IPS, anti-virus, application control and URL filtering - to guard against the full extent of the threat landscape.

When looking at concerns from a geographical perspective, the survey showed that despite deploying the highest level of security of all the regions surveyed, ITDMs across Asia-Pacific (APAC) are the most concerned about their wireless security, with 44 percent stating they are very concerned, in contrast to 30 percent in the Americas, and 20 percent in Europe, the Middle East and Africa (EMEA).

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

Higher levels of concern

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.

When asked to cite the risks of operating an unsecured wireless network, of the 48 percent of ITDMs who considered loss of sensitive corporate and/or customer data as the biggest risk to their organisation, it was the highest at 56 percent in APAC, in contrast to the Americas at 45 percent and EMEA 42 percent. The next highest risk, industrial espionage, was mentioned by just 22 percent of ITDMs, followed by non-compliance to industry regulations (13 percent), with service interruption and damage to corporate reputation ranked equal last (nine percent).

Cloud-based management set to grow

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

Of the cloud-ready respondents, 58 percent would want to use a private cloud infrastructure for wireless management and 42 percent would outsource to a third party managed service provider. Fourteen percent of those considering outsourcing

would only do so provided it is hosted in the same country, leaving 28 percent happy to embrace wireless management as a public cloud service regardless of geography.

When it comes to inviting guests onto the wireless network, the survey found that the most common form of guest security access on corporate wireless networks is a unique and temporary username and password (46 percent), ahead of a captive portal with credentials (36 percent).

Realising the importance of wireless security

"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 prevalent, it's not an oversight organisations should risk any longer."

"It's positive to see IT leaders beginning to recognise 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."