Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Five reasons an organisation’s wireless network could be at risk

The proliferation of wireless and bring your own device (BYOD) endpoints means corporate networks depend more on wireless networks. Securing the wireless network is, therefore, essential, especially as Australian businesses continue to see an explosion in the number and severity of cyberattacks, according to Wavelink.

Hugo Hutchinson, Wavelink’s national business development manager for Fortinet, said, “There is greater awareness of the need for strong cybersecurity than ever although that corresponds with increasing attacks. Legislation in Australia and around the world has brought the importance of data protection into sharp focus and businesses are doing more to protect themselves from cyberattacks. However, wireless security is often overlooked despite the fact that it plays such a pivotal role.”

Wavelink has identified five ways an organisation’s network could be at risk:

1. Phishing attacks

Cyberattackers are getting smarter and their ability to mimic legitimate emails can be astonishing. Busy workers who receive an email that purports to be from their boss don’t necessarily identify the email as a phishing attempt because it seems so realistic. They therefore fall for the scam, which can cost the company both financially and reputationally.

Hugo Hutchinson said, “Employees might be busy and eager to comply with requests from their managers, which means they will comply without really thinking too much about the nature of the request. So it’s important to ensure they’re educated about the risk of a phishing attack and know how to identify a potentially-suspicious email. Proper security infrastructure is important and educating employees is equally crucial to protect the organisation.”

2. Human error

Whether because of phishing attacks or other errors, people tend to be the weakest link in any organisation. They can inadvertently send passwords via email, connect unsecured devices to the network, or bypass security controls to get their jobs done more efficiently without realising that they’ve opened the network up to intrusion.

Hugo Hutchinson said, “Again, education is essential to mitigate the risk posed by unwary employees. It’s important to set policies around what people can and can’t connect to on the network, for example, and then to communicate that clearly and consistently. It’s not enough to run one training session per year; businesses need to continually remind employees of their responsibilities and the risks facing the business so that they can do their part to keep the business safe.

3. The Internet of Things

The Internet of Things (IoT) holds tremendous potential to boost businesses’ capabilities and profitability. However, IoT devices are additional endpoints in the network and, too often, they aren’t adequately secured.

Hugo Hutchinson said, “Device-makers shouldn’t be relied upon to build strong security features into IoT devices, although further legislation to enhance the security of IoT devices in the future would be beneficial and is likely to occur. IT teams need to ensure that all IoT devices have a new username and password allocated to them as soon as they enter the network.”

4. Compliance

Security requirements continue to evolve alongside the increasing sophistication and creativity of cybercriminals' attacks. It's important to stay current with the latest recommendations. Best practice is a good starting point. The Australian mandatory notifiable data breaches (NDB) scheme and Europe's General Data Protection Regulation (GDPR) include recommendations to keep information safe.

Hugo Hutchinson said, "Complying with NDB and GDPR is a good starting point. It's essential to implement firewalls and internal segmentation so that, if an attacker does get through, they can only access one area. This includes physical and virtual segmentation."

5. Lack of planning

The nature of cybersecurity is that most organisations will be targeted at some point. The question is how the organisation will react. It's essential to have a plan in place that includes what to do in an emergency, who is responsible for what actions, and what steps people need to take to mitigate an attack as soon as possible.

Hugo Hutchinson said, "How an organisation reacts to a cyberattack is almost more important than whether they suffer an attack. Responding quickly and appropriately to both mitigate the effects of the attack and notify the people affected can help protect brand reputation and minimise losses.

"It's important to have a strategy for wireless security and follow it just like a commercial strategy. From CEOs down, all employees need to understand what security is, what risks face the organisation, and how to play their part in protecting it. Perfection is likely to be unattainable however it's essential to do everything in the organisation's power to protect the network.

"Coupled with a complete security solution for network access, such as Fortinet's unique Security Fabric, organisations can be sure they are taking every step towards risk mitigation."